Les pratiques de chiffrement dans l'informatique en nuage (cloud) public

22 janvier 2024

Le chiffrement est aujourd'hui l'un des mécanismes les plus efficaces pour protéger la confidentialité des données. Pour que l'application du chiffrement soit utile, les clés cryptographiques doivent être correctement gérées et protégées. Quelles sont les différentes approches possibles ?

À retenir

- Le chiffrement des données est une mesure importante de sécurité et de protection des données.
- Selon l'état de la donnée (au repos, en transit, en traitement), **différentes approches sont possibles soit côté serveur, soit côté client**.
- Certaines techniques de chiffrement peuvent être complexes à mettre en place : il est important de connaître les différentes approches pour **appliquer celle qui sera la plus adaptée au traitement de données**.
- Le chiffrement de bout-en-bout n'est pas applicable dans toutes les situations, mais constitue la solution la plus protectrice de la vie privée.

L'émergence de l'informatique en nuage (*cloud computing*), où des données sont confiées à des fournisseurs tiers dans des environnements de stockage, de calcul et de réseaux hors de la maîtrise des clients, renforce **l'intérêt de recourir au chiffrement comme une mesure de sécurité et de protection des données**, non seulement vis-à-vis de tiers malveillants mais aussi des fournisseurs eux-mêmes.

Cette fiche n'a pas pour objet de traiter le sujet de la répartition des responsabilités entre les fournisseurs et leurs clients au titre du RGPD.

Les trois états de la donnée

Le stockage, la communication et l'utilisation des données sont généralement assimilés aux concepts de « *données au repos* », « *données en transit* » et « *données en traitement* ».

Les données doivent être gérées différemment selon leur état (au repos, en transit, en traitement) et leur emplacement (sur site, sur le réseau, dans le *cloud*, etc.). Cette consigne s'applique également au chiffrement des données et la gestion des clés, ces dernières étant elles-mêmes des données soumises à cette classification.

La donnée au repos

Il s'agit de la donnée stockée de manière persistante dans une mémoire non volatile (comme un disque dur ou un disque SSD lorsqu'il n'y a plus d'alimentation électrique). Ces données ne sont pas utilisées ou transmises activement sur un réseau ; elles sont stockées et attendent d'être accédées ou utilisées ultérieurement.

La donnée en transit

Il s'agit de la donnée qui est transmise sur un réseau de communication entre deux endroits d'un même système d'information ou entre deux systèmes d'information. Le contenu d'un courriel, des données envoyées à un serveur web, des données transmises depuis un poste de travail vers un espace de stockage dans le nuage (*cloud*), l'envoi de données dans le *cloud* depuis un serveur de stockage vers un serveur de calcul, des messages échangés par messagerie instantanée, sont autant d'exemples de données en transit.

La donnée en traitement

Il s'agit de l'état de la donnée lorsqu'on y a accès, ou qu'elle est consultée, mise à jour, consommée, analysée, etc. par un utilisateur, une application ou un service. La donnée en traitement fait l'objet de calculs réalisés au sein d'« unités de traitement » telles que les processeurs des ordinateurs, les cartes graphiques, sonores, etc., et ont été pour cela recopiées au sein de mémoires de travail « non-persistantes » (dites aussi « volatiles ») telles que la mémoire vive (la « RAM ») de l'ordinateur ou d'autres mémoires de travail rapides (caches, registres du processeur, etc.).

À retenir

Connaître l'état et l'emplacement de la donnée à chaque étape de son cycle de vie permet d'assurer une gestion efficace et sécurisée des données.

Problématiques du chiffrement et de la gestion des clés dans le *cloud*

Le chiffrement est l'une des principales mesures permettant de garantir la confidentialité des données dans un système informatique. Pour garantir l'effectivité du chiffrement, il est nécessaire que les **clés de chiffrement soient gérées de façon à en garantir la confidentialité et que les algorithmes de chiffrement utilisés soient « à l'état de l'art »**, c'est-à-dire reconnus comme robustes vis-à-vis des techniques de cryptanalyse connues (on parle également « d'algorithme public réputé fort »). Cette fiche part du principe que les algorithmes utilisés dans le *cloud* sont « réputés forts » et se concentre sur les questions de gestion de clés.

La gestion des clés est un processus crucial dans la configuration d'un système cryptographique, d'autant plus complexe que le volume et la répartition des données et le nombre d'acteurs impliqués sont importants. Ce processus est donc particulièrement lourd dans un environnement *cloud* où le contrôle des ressources physiques et logiques est réparti entre les différents participants de l'écosystème (notamment entre le fournisseur et le client).

Ressources physiques et logiques hors du contrôle du client

Le chiffrement permet de garantir la confidentialité des données : les données sont inintelligibles pour toute personne non autorisée (ne disposant pas des clés de déchiffrement). En principe, seuls l'émetteur et le destinataire sont en capacité d'accéder au contenu en clair. En pratique, un client cherche à contrôler d'éventuels accès non autorisés de la part :

- de personnes internes à l'organisme, non malveillantes, mais n'ayant pas le droit d'accéder aux données : une gestion des habilitations est généralement utilisée pour contrôler ces accès ;
- de personnes internes ou externes malveillantes cherchant à accéder aux données : le chiffrement peut être une des mesures efficaces pour limiter ce risque, en complément du contrôle d'accès ;
- du fournisseur du service, de l'infrastructure ou du logiciel lui-même : le chiffrement peut être une des mesures efficaces pour limiter ce risque, s'il est effectué avant d'envoyer les données sur le *cloud*.

Cette fiche se concentre sur les risques présentés par le fournisseur de service de *cloud* vis-à-vis de l'accès et de la lecture des données en clair qu'il stocke et les éventuelles protections apportées par le chiffrement, selon les modalités de sa mise en œuvre.

À retenir

Le chiffrement est une mesure efficace et essentielle pour réduire le risque d'accès illégitimes aux données. Il est indispensable dans de nombreuses situations courantes (flux de données circulant au travers internet, stockage, poste de travail, etc.).

Dans le *cloud*, en comparaison au modèle traditionnel « sur site », le client va déléguer une partie des responsabilités de sécurité au fournisseur de *cloud*, notamment en ce qui concerne le chiffrement et la gestion des clés.

Or **le fournisseur de *cloud* lui-même peut être une source de risques ou un vecteur d'attaque** :

- un fournisseur mal intentionné pourrait « fouiller » dans les données du client ;
- des employés du fournisseur pourraient accéder aux données ;
- un fournisseur pourrait réutiliser des données en dehors du contrôle du responsable de traitement, notamment pour des opérations de maintenance et de sécurité (p. ex. : des données de télémétrie) ou d'amélioration de ses services ;
- le fournisseur pourrait devoir répondre à des demandes des autorités judiciaires et de renseignement de pays tiers, exigeant le transfert ou la divulgation de données (notamment personnelles) vers ces pays ;
- enfin, le fournisseur pourrait être victime d'intrusions par des acteurs malveillants.

En pratique, un fournisseur de service *cloud* peut accéder aux données de différentes manières :

- pour les données au repos :
    - via un accès local, c'est-à-dire dans le centre de données, directement sur les supports de stockage utilisés par le service,
    - via un accès distant en « mode administrateur » du service fourni, permettant de consulter les données à distance,
    - si elles sont chiffrées par le serveur, via un accès aux clés qui permettent au fournisseur de déchiffrer les données et d'y accéder ;

- pour les données en transit :
    - via un accès local, dans le centre de données ou à proximité, sur les équipements réseau utilisés par les machines servant à fournir le service ;

- pour les données en traitement :
    - via un accès local ou distant en « mode administrateur » sur la machine (réelle ou virtuelle) hébergeant le service fourni, permettant de consulter les données (par exemple, en effectuant une requête directe sur la base de données utilisée – sans passer par le logiciel applicatif utilisant la base, et susceptible de tracer de tels accès – ou une copie de certains éléments du service),
    - via des outils de surveillance (« *monitoring* ») et de journalisation qui permettent de consulter les données en cours de traitement.

Le fournisseur de service de *cloud* s'appuie en général lui-même sur d'autres fournisseurs : de couches dites « inférieures » (machines virtuelles, services PaaS ou IaaS), du centre de données lui-même (colocation d'espace de stockage, etc.) et d'équipements et de composants (systèmes d'exploitation, processeurs, etc.).

Détention, contrôle, possession, accès et usage des clés

Lorsqu'il décide d'avoir recours à un service de *cloud*, il est impératif que le client comprenne la répartition des rôles entre lui et le fournisseur en ce qui concerne la sécurité et la protection des données. Du point de vue de la protection des données personnelles, les obligations de chaque partie doivent être formalisées dans un contrat clair, tel que le prévoit l'article 28.3 du RGPD.

En effet, le choix du déploiement des clés cryptographiques est déterminé par le niveau de détention, de possession, d'accès, de contrôle et d'utilisation des clés que le client doit adopter en fonction de ses exigences en matière de sécurité et de conformité :

- la **titularité** des clés répond à la question : « qui est le détenteur des droits sur les clés, sur le plan juridique ? » ;
- le **contrôle** des clés répond à la question « qui gère le cycle de vie des clés » ;

Note : les deux notions de titularité des droits et de contrôle des clés peuvent être rapprochées, dans le sens où la titularité des droits sur les clés implique qu'une entité a le droit d'accéder aux clés, de déchiffrer les données chiffrées avec elles et de contrôler les accès aux clés ;

- la **possession** des clés répond à la question : « qui détient un exemplaire des clés ? » ;

Note : il est important de distinguer la notion de titularité de celle de possession : la possession sous-entend une conservation des clés, sur un support physique. Ces droits peuvent être détenus par deux entités différentes.

- l'**accès** aux clés répond à la question : « qui a accès aux clés ? » ;
- l'**usage** des clés répond à la question : « qui peut utiliser les clés ? ».

Dans le domaine du *cloud computing*, ces différents attributs peuvent être répartis entre le fournisseur des services *cloud* et le client. Par exemple :

- le client peut être le titulaire des clés, les détenir et les utiliser complètement sans que le fournisseur de *cloud* n'ait accès aux clés (voir le chiffrement côté client dans les sections suivantes) ;
- le fournisseur peut être le titulaire des clés, les détenir et les utiliser complètement sans que le client n'ait la main sur la gestion de ces clés (voir le chiffrement côté serveur avec gestion côté serveur) ;
- le client peut être le titulaire des clés. Il peut les stocker et les gérer dans un service de gestion de clés offert par le fournisseur de *cloud*, qui donc possède les clés. Le contrôleur des clés peut dans ce cas être le client si celui-ci a la faculté d'envoyer ses instructions via le service de gestion des clés qui est proposé sur l'infrastructure du fournisseur ;
- un fournisseur peut générer les clés de chiffrement à la demande et les transmettre au client, qui donc les possède et les contrôle ;
- le client peut alternativement avoir recours à un service de tiers de confiance pour la gestion des clés, indépendant du fournisseur de *cloud*.

Le client doit aussi **maîtriser les outils qui sont mis à sa disposition pour utiliser au mieux** les clés de chiffrement. En particulier, le client doit être certain que :

- les services, logiciels ou programmes qui utilisent ces clés sont sains ;
- ces services utilisent les bonnes clés (c.-à-d. les siennes et pas d'un autre client) ;
- les algorithmes de chiffrement et déchiffrement sont correctement mis en œuvre ;
- ces outils sont correctement distribués et vérifiables par lui-même.

Il doit également effectuer une veille régulière sur les évolutions des services et des outils de son fournisseur, afin de maîtriser les risques résiduels engendrés par ces évolutions permanentes.

À retenir

Les organismes clients d'un fournisseur de *cloud* doivent déterminer le niveau de **titularité**, de **contrôle** et de **possession des clés** dont ils ont besoin. Cette décision doit être prise compte tenu des enjeux de sécurité, de conformité et de maîtrise des données.

Le client doit impérativement se demander qui détient les clés et gère leur cycle de vie, qui y a accès et les utilise, en particulier lorsqu'il a recours des services fournis par des fournisseurs soumis à des législations extra-européennes.

Sur le plan technique, l'élimination de la possibilité d'accès aux données par le fournisseur n'est garantie que par la titularité, le contrôle, la possession, l'accès et l'usage exclusifs des clés par le client.

Pas ou peu de standardisation de la gestion des clés dans le *cloud*

Il existe des standards internationaux pour la gestion des clés cryptographiques (p. ex. : NIST SP 800-57, FIPS 140-2, Common Criteria) mais les standards, les recommandations et bonnes pratiques, spécifiques à la gestion des clés dans le contexte du *cloud* sont encore peu nombreux. Certains commencent toutefois à émerger, par exemple l'initiative du NIST (le guide *Cryptographic key management issues and challenges in cloud services* de 2013).

Scénario 1 : Données au repos

Le chiffrement des données au repos consiste à chiffrer les données stockées afin de les protéger contre tout accès illégitime. Dans le contexte du *cloud*, **le chiffrement au repos permet de se prémunir contre les accès non autorisés aux données en clair**, qu'il s'agisse de pirates informatiques ou même de personnes ayant un accès physique aux serveurs. Les données compromises sont alors inintelligibles pour les sources de risque.

Pour ce scénario il existe quatre niveaux de chiffrement :

- chiffrement de disque ;
- chiffrement au niveau du fichier ;
- chiffrement de base de données ;
- chiffrement au niveau de l'application.

Plus le chiffrement est de bas niveau (notamment, au niveau du disque), moins sa mise en œuvre est complexe pour le client. **Le chiffrement au niveau de l'application est donc plus complexe à déployer mais est généralement plus efficace** pour protéger la confidentialité des données.

Lorsqu'un client de service *cloud* stocke des données dans le *cloud*, le chiffrement des données peut être opéré par le fournisseur de service ou par le client lui-même. Un chiffrement par le fournisseur implique que celui-ci ait accès, ne serait-ce que de façon transitoire, à la clé de chiffrement et aux données en clair.

Le chiffrement de disque (IaaS)

Le chiffrement de disque est un chiffrement des données, opéré par le serveur, au niveau matériel. Il permet de chiffrer les données avant qu'elles ne soient inscrites sur les disques du fournisseur et de les déchiffrer quand elles sont chargées à partir de ces disques.

Le chiffrement de disque protège les données contre le vol ou la perte physique des supports de stockage.

En revanche, le chiffrement de disque seul ne permet pas de se prémunir contre un accès du fournisseur de service *cloud*, puisque ce dernier possède les clés de (dé-)chiffrement.

À retenir

Le chiffrement de disque seul ne convient pas pour éliminer la possibilité d'accès aux données par le fournisseur de *cloud*, y compris dans le cadre d'une demande d'une autorité étrangère en application d'une législation ayant un effet extraterritorial.

Figure 1 - Chiffrement de disque opéré par le serveur

Pour des raisons de clarté, ce schéma ne fait pas figurer les autres mesures de sécurisation comme l'utilisation d'un tunnel chiffré pour la communication entre le poste de l'utilisateur et le cloud. Cette mesure est néanmoins standard dans les services cloud.

Le chiffrement au niveau du fichier (IaaS, Paas, SaaS de stockage)

À ce niveau, les fichiers sont chiffrés individuellement lorsqu'ils sont inscrits sur le disque. Pour lire le contenu d'un fichier, il suffit de déchiffrer ce fichier particulier, laissant les autres fichiers chiffrés.

Concernant la gestion du chiffrement et des clés, les services de stockage proposent deux configurations principales :

Le **chiffrement côté client**, avec des clés gérées par le client lui-même (ou par un tiers de confiance), consiste à chiffrer les fichiers avant qu'ils ne soient transférés vers le serveur de *cloud* et à les déchiffrer lorsqu'ils sont récupérés par le client. Les clés restent en la possession du client (ou de son fournisseur de gestion de clés). Les fichiers restent chiffrés au repos dans le service de stockage. Sauf si le client transmet les clés de déchiffrement au fournisseur de *cloud*, celui-ci n'a jamais accès aux clés et donc aux fichiers en clair. En d'autres termes, le service de *cloud* joue le rôle d'un simple stockage distant de données déjà chiffrées.

Figure 2 - Chiffrement de fichier côté client

À retenir

Le chiffrement côté client au niveau des fichiers avec des clés dont le client détient les droits exclusifs de titularité, de possession et de contrôle permet d'éliminer la possibilité d'accès aux données par le fournisseur de *cloud*, y compris dans le cadre d'une demande d'une autorité étrangère en application d'une législation ayant un effet extraterritorial.

Les métadonnées techniques servant à l'identification individuelle des fichiers au sein des serveurs sont aujourd'hui quasiment toujours conservées en clair. De telles métadonnées, et notamment les noms des fichiers, peuvent contenir des informations personnelles (p. ex. un fichier nommé « RH_projet_licenciement_faute_grave_Durant_Alain »).

Suivant le cas, le client peut déléguer la gestion des clés cryptographiques à un tiers de confiance situé dans l'espace économique européen (EEE) ou dans une juridiction offrant un niveau de protection essentiellement équivalent à celui garanti dans l'EEE (voir point 6 du paragraphe 84 des recommandations du CEPD du 18 juin 2021).

Le **chiffrement côté serveur** chiffre les fichiers après leur transfert vers le *cloud* puis les déchiffre avant leur récupération par le client. Les fichiers sont donc transférés en clair (indépendamment d'un chiffrement du flux de transmission) et sont ensuite chiffrés par le serveur. Le fournisseur voit donc transiter en clair les données arrivant dans son environnement, avant d'effectuer lui-même leur chiffrement. Par ailleurs, si le fournisseur doit effectuer des opérations sur les fichiers, comme l'indexation des fichiers pour une recherche, alors le fournisseur doit avoir accès aux clés et doit pouvoir les utiliser pour déchiffrer les fichiers et exécuter lesdites opérations.

Concernant la gestion des clés cryptographiques pour le chiffrement côté serveur, différentes options sont proposées par les fournisseurs :

1. la gestion par le fournisseur (tout est géré par défaut par le fournisseur, comme illustré en **Figure 3 A**) ;
2. la gestion par le client au travers d'un service de gestion des clés du fournisseur (Key Management System – KMS, comme illustré dans la **Figure 3 B**) ;
3. la gestion par le client via des modules matériels (appelés en anglais « *Hardware Security Module* » – HSM) hébergés au sein des serveurs du fournisseur.

Pour les options 2 et 3, le client a la possibilité de fournir sa propre clé et de la stocker dans le KMS ou le HSM dans le *cloud* (modèle dit « *Bring Your Own Key* » – BYOK), comme décrit dans la **Figure 3 C**. Concernant l'utilisation d'un HSM hébergé et géré par le fournisseur, ce dernier pourrait conserver techniquement les accès au module et donc aux clés.

D'autres possibilités sont offertes au client, à savoir la gestion des clés cryptographiques sur site (dans un HSM, par exemple) ou via un tiers de gestion des clés (modèle dit « Hold Your Own Key » – HYOK) via un KMS tiers (voir la **Figure 3 D**).

Néanmoins pour toutes ces options, les clés doivent être, à un moment ou à un autre, accessibles au fournisseur afin de chiffrer les fichiers avant leur stockage au repos ou de les déchiffrer quand ils sont récupérés par le client.

Figure 3 - Chiffrement de fichier côté serveur, selon 4 modèles de gestion de clés

À retenir

Étant donné que le fournisseur possède les clés de chiffrement et a donc accès à la donnée en clair, le chiffrement côté serveur ne permet pas d'éliminer les possibilités d'accès aux données par le fournisseur de *cloud*, notamment dans le cadre d'une demande d'une autorité étrangère en application d'une législation ayant un effet extraterritorial, quelle que soit la méthode de gestion des clés.

Le chiffrement de bases de données (PaaS)

Dans cette fiche, le terme « base de données » désigne les données structurées sous forme de tables (SQL par exemple).

Certains systèmes de bases de données dans le *cloud* font appel au mécanisme de Transparent Data Encryption (TDE) pour chiffrer les données dans la base. TDE chiffre les données avant qu'elles ne soient inscrites sur le disque et les déchiffre lorsqu'elles sont lues en mémoire à partir du disque (quand la donnée est transmise, elle l'est en clair). Ce mécanisme fournit un chiffrement granulaire : chiffrement individuel des enregistrements dans la base, ou chiffrement d'un champ particulier (éléments d'une colonne d'une table). Il s'agit d'un chiffrement côté serveur, équivalent en pratique au chiffrement des fichiers côté serveur présenté en section 2 : c'est le serveur de base de données qui possède les clés cryptographiques et qui effectue les opérations de chiffrement et de déchiffrement.

Concernant la gestion des clés cryptographiques pour le chiffrement côté serveur, les mêmes options que pour le chiffrement de fichiers mentionnées dans la section 2 sont disponibles, à savoir le KMS, le HSM, le BYOK et le HYOK.

Dans le cas d'un chiffrement de bases de données, **le fournisseur possède les clés de chiffrement et a donc accès à la donnée en clair**. Ce chiffrement ne permet donc pas d'éliminer la possibilité d'accès aux données par le fournisseur de *cloud*, notamment dans le cadre d'une demande d'une autorité étrangère en application d'une législation ayant un effet extraterritorial, quelle que soit la méthode de gestion des clés.

Le chiffrement au niveau de l'application (PaaS, SaaS)

Ce chiffrement protège les données d'une application lorsqu'elles sont au repos. L'application (la partie cliente ou la partie serveur) chiffre les données avant écriture dans le système de stockage et déchiffre les données après lecture depuis le système de stockage et avant traitement. Les fonctions de chiffrement / déchiffrement sont mises en œuvre au sein du logiciel applicatif.

Le fait d'avoir accès au système de stockage sous-jacent ne donne pas à un tiers malveillant la possibilité de déchiffrer les données. L'accès aux données ne peut se faire que par le biais de l'application appropriée.

Le **chiffrement applicatif côté client**, avec les clés gérées par le client, chiffre les données avant qu'elles ne soient transférées vers le serveur *cloud* et les déchiffre quand elles sont récupérées par le client. Les clés restent en la possession du client (qui en est le titulaire) ou de son fournisseur de gestion de clés (s'il en a fait le choix). Les données restent chiffrées au repos dans le système de stockage. Le fournisseur n'a jamais accès aux clés et donc aux données en clair, sauf si le client partage les clés de déchiffrement avec lui.

Toutefois, ce type de chiffrement implique plusieurs limitations. En effet, si l'application côté serveur ne peut pas avoir accès aux clés de déchiffrement et donc aux données en clair, alors :

- toutes les opérations sur les données sont effectuées par la partie cliente ;
- le serveur ne sert que de stockage de données ;
- de nombreuses fonctionnalités peuvent être limitées (notamment, les fonctionnalités collaboratives).

Par ailleurs, dans tous les cas, le serveur conserve l'accès en clair à des métadonnées, comme les noms de fichiers, pour servir correctement le client.

À retenir

Le chiffrement côté client au niveau de l'application, dans le périmètre du client, avec les clés du client, qui en garde la titularité, le contrôle et la gestion, permet d'éliminer la possibilité d'accès aux données par le fournisseur de *cloud*, y compris dans le cadre d'une demande d'une autorité étrangère en application d'une législation ayant un effet extraterritorial.

Toutefois, ce chiffrement comporte plusieurs limitations : métadonnées toujours en clair, fonctionnalités restreintes et opérations sur les données à effectuer côté client.

Pour ce type de chiffrement, le client peut déléguer la gestion des clés cryptographiques à un tiers de confiance situé dans l'EEE ou dans une juridiction offrant un niveau de protection essentiellement équivalent à celui garanti dans l'EEE.

Le **chiffrement applicatif côté serveur** chiffre les données au niveau du serveur d'application. Le serveur d'application chiffre les données avant qu'elles ne soient stockées dans le *cloud*.

À retenir

Si, dans le cas du chiffrement applicatif côté serveur, le fournisseur de *cloud* voit les données en clair, la possibilité d'accès aux données par le fournisseur de *cloud*, notamment dans le cadre d'une demande d'une autorité étrangère en application d'une législation ayant un effet extraterritorial, n'est pas éliminé.

Résumé

Le tableau ci-dessous permet d'évaluer les choix que le client doit opérer pour les cas où il souhaite se prémunir contre un accès aux données par le fournisseur et contre une communication des données à des tiers.

Ces protections peuvent être nécessaires, en fonction des risques, même lorsque le fournisseur est soumis exclusivement à la législation européenne (par exemple, pour limiter les accès en mode administrateur non autorisés ou si le fournisseur prévoit de traiter certaines données du client pour ses propres finalités).

Recommandations générales pour les clients

Il est recommandé de :

- procéder à une analyse des risques liés au recours à un service de *cloud* en matière de protection des données ;
- déterminer les options et configurations de chiffrement des données au repos mises en place par le fournisseur de *cloud* (en dialoguant avec le fournisseur, en examinant sa documentation, etc.) ;
- déterminer si ces options assurent un niveau de protection des données qu'ils estiment adéquat, sur la base de l'analyse des risques (il est donc possible, sur la base de cette évaluation, de devoir renoncer à un service *cloud* particulier, ou de renoncer de migrer un traitement dans le *cloud*).

Le chiffrement comme mesure supplémentaire pour les transferts hors UE

Concernant la question des transferts de données hors de l'Union européenne et des possibilités d'accès par des autorités de pays tiers, le CEPD recommande la mise en œuvre d'un chiffrement comme mesure supplémentaire efficace pour certains cas d'usage particuliers. Toutefois, comme illustré dans le tableau ci-dessous, ce chiffrement techniquement approprié ne permet en revanche pas de se prémunir contre un accès aux données de la part du fournisseur, quand il est chargé d'appliquer le chiffrement aux données (c'est-à-dire une fois que les données ont été envoyées dans le *cloud*) ou lorsque celui-ci est en possession des clés de chiffrement et de déchiffrement (rendant ainsi le chiffrement inefficace).

Ainsi, pour atteindre cet objectif, **il est recommandé d'appliquer le chiffrement au niveau du client** (« approche 5 », dernière colonne du tableau ci-dessous).

Le chiffrement comme mesure de sécurité pour la confidentialité des données

Si la question des transferts et des possibilités d'accès par des autorités de pays tiers ne sont pas des objectifs visés par l'application d'une mesure de chiffrement, celle-ci reste une bonne mesure de sécurité afin de protéger la confidentialité des données.

Il est néanmoins recommandé aux clients ayant recours aux services de *cloud* :

- d'identifier différents degrés de sensibilité des données et de classifier leurs données en conséquence ;
- de déterminer pour chaque degré de sensibilité le niveau de garantie nécessaire qui devra être assuré par le chiffrement. Par exemple, un chiffrement côté client sera privilégié pour des données hautement sensibles ;
- de mettre en œuvre une gestion des clés appropriée à la sensibilité des données. Par exemple, pour chiffrer des données à caractère personnel peu sensibles, le client peut envisager une gestion des clés de type « BYOK », en combinaison avec des contrôles d'accès aux données chiffrées et aux clés bien définis et tracés ;
- d'effectuer des audits réguliers, non seulement des accès éventuels aux données et aux clés, mais aussi des mécanismes de chiffrement et de gestion des clés utilisés.

Chacune des approches identifiées dans les quatre premières colonnes du tableau (approches 1 à 4) présente des avantages et des inconvénients résumés dans le tableau ci-dessous.

En résumé :

- les approches qui impliquent une gestion plus complète des clés par le client (approches 3 et 4) nécessitent une expertise plus avancée en gestion des clés et en sécurité mais offrent un niveau plus élevé de contrôle sur les clés de chiffrement par rapport aux approches où le fournisseur de services *cloud* est impliqué dans la génération et la gestion des clés (approches 1 et 2) ;

- les approches avec une gestion des clés par le fournisseur (approches 1 et 2) sont généralement plus simples à mettre en œuvre, car le client délègue une partie ou la totalité de la gestion des clés au fournisseur, ce qui nécessite une confiance accrue vis-à-vis du fournisseur et des lois auxquelles il peut être soumis ;
- en conservant la gestion des clés de chiffrement (approche 4), le client peut garantir une confidentialité plus élevée de ses clés et de ses données, réduisant le risque d'accès non autorisé aux données en clair.

L'approche 4 offre donc un niveau de protection des données plus élevé par rapport aux autres approches (1 à 3), sans toutefois constituer une mesure permettant d'annihiler les possibilités d'accès par le fournisseur, de lui-même ou à la demande d'un tiers.

Chiffrement au repos	**Chiffrement côté serveur**				**Chiffrement côté client**
Approche pour la gestion des clés	**Approche 1** **Clés générées et gérées par le fournisseur**	**Approche 2** **Clés générées par le fournisseur et gérées par le client dans le KMS du fournisseur**	**Approche 3** **Clés générées par le client, stockées et gérées par le client dans le KMS du fournisseur** **« BYOK »**	**Approche 4** **Clés générées et gérées par le client sur site ou dans un KMS tiers (de confiance)** **« HYOK »** **« EKM »**	**Approche 5** **Clés générées et gérées par le client sur site ou dans un KMS tiers de confiance**
Simplicité de mise en œuvre	Simple le client n'a rien à faire.	Plutôt simple, car le client gère les clés via le KMS du fournisseur, qui propose une automatisation des processus. Le client n'a pas à gérer les mises à jour, la maintenance ou le déploiement de correctifs de sécurité.	Un peu plus complexe que l'approche 2 car le client génère et gère lui-même les clés. Il doit mettre en place en local son système de gestion de clés, servant notamment à la génération et à l'import des clés dans le KMS.	Plus complexe que les approches précédentes car le client doit mettre en place son propre système de gestion des clés.	Complexe car le client doit mettre en place son propre système de gestion des clés en interne ou dans un KMS tiers.

Investissement et expertise	Pas d'expertise spécifique, toutes les opérations de gestion de clés sont prises en charge par le fournisseur.	Niveau d'expertise plutôt modéré. Le client doit comprendre les fonctionnalités du KMS pour gérer les clés selon ses besoins. Le client peut avoir besoin de connaissances en matière de sécurité et de bonnes pratiques de gestion des clés pour configurer correctement le KMS.	Niveau d'expertise plutôt élevé. En complément de l'expertise nécessaire pour l'approche 2, le client doit avoir une expertise approfondie en gestion des clés de chiffrement, car il est responsable de la génération, de l'importation et de la gestion de ses propres clés de chiffrement en dehors du fournisseur (avant leur import).	Le client doit investir dans son propre système de gestion des clés nécessitant une expertise idoine.	Le client doit investir dans son propre système de gestion des clés nécessitant une expertise idoine.
Niveau de contrôle des clés par le client	Aucun, le client n'a pas de contrôle direct sur la génération, le stockage ou la gestion des clés.	Le client a un certain contrôle sur l'accès aux clés, il peut définir les autorisations d'accès aux clés pour limiter qui et quel service peut les utiliser.	Le client a plus de contrôle que pour les approches précédentes, en particulier car il gère la génération des clés.	Le client est responsable de la gestion complète du cycle de vie des clés, y compris la rotation régulière des clés, la révocation des clés compromises et la création de nouvelles clés selon les besoins.	Le client détient le contrôle total sur les clés de chiffrement, car il les génère et les gère localement ou les confie à un tiers de confiance qu'il choisit.
Niveau de contrôle des clés par le fournisseur	Total, le fournisseur prend en charge tous les aspects de la gestion des clés.	Le fournisseur a accès au KMS et à son contenu mais n'a pas un contrôle total sur les clés, comme pour l'approche 1.	Le fournisseur a accès au KMS et à son contenu mais n'a pas un contrôle total sur les clés, comme pour l'approche 1.	Le fournisseur a accès au KMS et à son contenu mais n'a pas un contrôle total sur les clés, comme pour les approches précédentes.	Le fournisseur n'a aucun contrôle sur les clés, car dans cette approche le client ne les partage jamais avec le fournisseur.

Niveau d'accès aux clés par le fournisseur	Accès complet	Le fournisseur a un certain niveau d'accès aux clés stockées dans le KMS pour pouvoir effectuer des opérations telles que le chiffrement et le déchiffrement des données pour le compte du client quand celui-ci utilise les services de *cloud*.	Le fournisseur peut encore avoir un certain niveau d'accès aux clés stockées dans le KMS, car il doit être en mesure d'effectuer des opérations de chiffrement et de déchiffrement pour le compte du client quand celui-ci utilise les services de *cloud*.	Le client doit fournir les clés au fournisseur pour qu'il puisse effectuer les opérations de chiffrement et de déchiffrement côté serveur, car les données doivent être accessibles et utilisables par les services de *cloud* utilisés par le client.	Les clés ne sont jamais partagées avec le fournisseur.
Possibilités d'accès par le fournisseur aux données en clair	Ayant accès aux clés, le fournisseur pourrait techniquement les utiliser pour déchiffrer les données du client et y accéder	Étant le gestionnaire du KMS, le fournisseur pourrait techniquement accéder aux clés, les utiliser pour déchiffrer les données du client et y accéder	Étant le gestionnaire du KMS, le fournisseur pourrait techniquement accéder aux clés, les utiliser pour déchiffrer les données du client et y accéder	Il existe toujours un risque d'accès par le fournisseur aux données en clair, principalement en raison des opérations de chiffrement et déchiffrement côté serveur nécessaires pour que le fournisseur puisse offrir ses services.	Le fournisseur ne voit jamais les données en clair (*)
Transparence des accès aux clés par le fournisseur	Transparence faible. Le client a peu d'informations sur l'accès aux clés utilisées pour chiffrer ses données	La transparence dépend du fournisseur, mais le client peut auditer les accès via le KMS	La transparence dépend du fournisseur, mais le client peut auditer les accès via le KMS	Le fournisseur ne peut pas accéder aux clés du client sans que le client ne les fournisse spécifiquement pour chaque opération. Cela offre un niveau de contrôle élevé au client sur les accès aux clés par le fournisseur.	N/A

Utilisation des services de *cloud*	Les fonctionnalités du *cloud* sont préservées	Les fonctionnalités du *cloud* sont préservées	Les fonctionnalités du *cloud* sont préservées. Néanmoins, cela peut entraîner des ajustements spécifiques dans l'utilisation des services du *cloud*. Le client doit configurer correctement les services pour utiliser les clés importées dans le KMS.	Les fonctionnalités du *cloud* sont préservées. Néanmoins, cela peut entraîner des ajustements spécifiques dans l'utilisation des services du *cloud* qui ne sont pas tous compatibles avec cette approche.	Les fonctionnalités du *cloud* sont restreintes. En effet, le chiffrement côté client peut avoir des implications sur certaines fonctionnalités du *cloud* qui dépendent du traitement en clair des données par le fournisseur.

(*) les limitations évoquées dans les « À retenir 6 » et « À retenir 9 » sont toutefois à prendre en considération

Scénario 2 : Données en transit

Cette notion couvre notamment :

- les données transitant entre un terminal utilisateur vers un service web dans le *cloud* ;
- les données transitant entre différentes machines dans le *cloud*, y compris entre différents services/fournisseurs de *cloud* (p. ex. : entre un serveur web applicatif et une base de données).

Le chiffrement des données en transit repose conceptuellement sur la création d'un tunnel sécurisé entre le client et le serveur *cloud*, ou entre différentes machines du *cloud* : dans le tunnel, les données sont chiffrées ; hors du tunnel, elles sont en clair. Les données sont chiffrées à l'envoi (entrée du tunnel) et sont déchiffrées à la réception (sortie du tunnel).

À retenir

Les données personnelles transitant sur un réseau public tel qu'Internet **doivent être protégées par un chiffrement de données** afin de préserver leur confidentialité en cas d'interception ou d'écoute par des tiers malveillants lors de leur transit sur le réseau.

Le chiffrement des données en transit ne correspond pas à la notion de chiffrement de bout en bout : le service *cloud*, qui peut servir d'intermédiaire entre deux entités qui souhaitent communiquer, peut avoir accès aux données en clair.

Figure 4 - Chiffrement de données en transit

Les protocoles les plus utilisés pour le chiffrement des communications sont TLS, SSH, IPSec et MACSEC.

D'un point de vue cryptographique, le chiffrement des données en transit fait généralement intervenir un chiffrement à clé publique pour l'établissement du tunnel sécurisé et l'échange de clés « de session » entre les parties, en conjonction d'un chiffrement symétrique pour le chiffrement effectif des données échangées à l'aide de la clé de session. La présentation, par au moins une des parties, de certificats électroniques signés par une autorité de certification reconnue de confiance est le standard pour prouver la validité et l'authenticité des clés publiques et éviter l'interception par un tiers malveillant usurpant l'identité de cette partie (attaques de type « homme au milieu » ou « man-in-the-middle »).

Scénario 3 : Données en traitement

Protéger la confidentialité de la donnée en traitement comporte plus de défis que les deux scénarios précédents. **Deux propriétés a priori incompatibles** de la donnée doivent être vérifiées simultanément :

1. la donnée doit être en clair pour pouvoir être traitée par le service, et donc connue du fournisseur responsable de ce service ;
2. la donnée doit être chiffrée pour en assurer la confidentialité vis-à-vis du fournisseur du service.

En effet, les méthodes traditionnelles de chiffrement ont pour objectif de rentre inintelligibles les données chiffrées pour quiconque ne détient pas la clé de déchiffrement. Or, l'état « en traitement » requiert par définition que la donnée soit accessible afin d'effectuer les opérations de traitement (recherche, consultation, analyse, mise à jour, etc.). Par conséquent, soit la donnée est exploitable, mais sans que sa confidentialité ne soit protégée, soit la confidentialité de la donnée est respectée, au prix de son exploitabilité.

À retenir

Si les données ne sont pas chiffrées lors du traitement par le service (ce qui est typiquement le cas pour des services SaaS), alors le chiffrement au repos et/ou en transit par le fournisseur ne constituent pas des mesures techniques supplémentaires efficaces vis-à-vis d'un accès par le fournisseur, puisqu'il doit avoir accès aux données en clair lorsque le service effectue les traitements.

Figure 5 - Combinaison du chiffrement au repos et en transit

Scénario 4 : Chiffrement de bout en bout

Le chiffrement de bout en bout (ou de client à client) est une solution permettant de protéger une communication en chiffrant les données de sorte que seules les parties engagées dans la communication puissent les déchiffrer. Avec le chiffrement de bout en bout, toutes les opérations cryptographiques (chiffrement, déchiffrement, génération et gestion des clés) sont strictement effectuées à la source ou à la destination. Dans ce scénario, le fournisseur de *cloud* n'a, à un aucun moment, accès aux données en clair. Ainsi, le chiffrement de bout en bout permet aux clients de garder le contrôle de la gestion des clés et du chiffrement.

Ce type de chiffrement est particulièrement adapté à des communications bilatérales entre deux personnes ou entités et requiert généralement l'installation de logiciels dédiés sur le terminal de chaque utilisateur. Il est nettement plus complexe à mettre en œuvre sur une architecture dite « client-serveur ». Ainsi, les types

de services concernés par le chiffrement de bout en bout sont les services de communications électroniques, à savoir la visioconférence ou la messagerie (instantanée ou courriel), mais aussi les services de partage de fichiers ou encore les services de travail collaboratif.

Mauvaises pratiques

Le chiffrement seul des données en transit ne peut être considéré comme du chiffrement de bout en bout, sauf si le fournisseur est l'unique destinataire des données échangées.

La combinaison du chiffrement des données en transit avec le chiffrement de données au repos ne peut être considérée comme du chiffrement de bout en bout si, à un point donné de la chaîne de transmission, il y a rupture du chiffrement, permettant au fournisseur d'accéder aux données en clair. Cette solution n'est pas une mesure efficace pour éliminer le risque d'accès aux données par le fournisseur de *cloud*.

Bonne pratique

Le chiffrement de bout en bout (de client à client), avec les clés du client, qui en garde la titularité, le contrôle et la gestion, permet d'éliminer la possibilité d'accès aux données par le fournisseur de *cloud*, y compris dans le cadre d'une demande d'une autorité étrangère en application d'une législation ayant un effet extraterritorial.

Pour ce type de chiffrement, le client peut déléguer la gestion des clés cryptographiques à un tiers de confiance situé dans l'Espace économique européen (EEE) ou dans une juridiction offrant un niveau de protection essentiellement équivalent à celui garanti dans l'EEE (sans nécessité de mesures additionnelles).

Pour des raisons pratiques, la gestion des clés (génération, diffusion, renouvellement en cas de perte) est souvent confiée au fournisseur. Cette gestion est certes effectuée sur le terminal ou le client d'une application, mais avec un logiciel (application) maîtrisée par le fournisseur.

Figure 6 - Chiffrement de bout en bout

Étape 1 : Alice chiffre son message pour Bob avec la clé publique de Bob

Étapes 2 et 3 : Le message chiffré est envoyé à Bob, sans que le fournisseur de *cloud* ait accès au contenu en clair

Étape 4 : Bob déchiffre le message en utilisant sa clé privée

Étapes 5 et 6 : Réponse de Bob à Alice chiffrée de bout en bout

À retenir

Les techniques avancées de chiffrement et les technologies d'informatique confidentielle semblent prometteuses pour permettre d'effectuer dans le *cloud* des traitements complexes sur les données chiffrées. Cependant, ces techniques sont, pour l'instant, limitées à des fonctions de base, et ne sont pas applicables à des traitements complexes comme ceux mis en œuvre dans le SaaS.

Étant donné que les données apparaissent en clair dans l'enclave, dans une mémoire réputée protégée et isolée du système, il convient de s'assurer que le fournisseur ne peut pas avoir accès aux données en clair traitées ou aux clés cryptographiques utilisées dans l'enclave, ni quelles opérations ont été effectuées sur

ces données (via les fonctionnalités d'attestation à distance offertes par les technologies d'informatique confidentielle).

Focus

Les techniques avancées de chiffrement que sont le calcul multipartite sécurisé (SMPC), le chiffrement totalement homomorphe (FHE) et le chiffrement fonctionnel (FE) ont pour but de réconcilier chiffrement et traitement sur données chiffrées. Avec ces technologies, les données sont chiffrées côté client avant d'atteindre le serveur *cloud*, mais peuvent tout de même être traitées par ce dernier. Ces techniques sont très prometteuses pour contribuer à la protection des données personnelles traitées dans le *cloud*. Toutefois, même si elles ont franchi la frontière de la recherche, ces techniques ne sont pas encore pratiques pour des applications complexes, notamment dans le SaaS. Il est essentiel d'assurer une veille technologique pour suivre de près les avancées dans ce domaine. La CNIL de son côté suit attentivement les progrès dans les techniques avancées de chiffrement.

Les technologies d'informatique confidentielle basées sur des composants matériels offrant un environnement d'exécution de confiance (« *Trusted Execution Environments* » ou TEE), s'attaquent également à la problématique de la confidentialité des données en traitement. Ces composants matériels fournissent en leur sein même un environnement sécurisé (appelé « enclave sécurisée ») pour opérer sur les données en clair, de telle sorte qu'aucun élément extérieur ne peut pénétrer l'enclave. Il s'agit d'une région sécurisée de la mémoire, protégée de tout programme extérieur à l'enclave, qui permet non seulement d'isoler les données mais aussi le code informatique prévu pour les traiter. Schématiquement, les opérations sur les données chiffrées s'effectuent en :

1. déchiffrant les données dans une zone isolée et protégée du reste du processeur ;
2. effectuant toutes les opérations sur les données en clair dans cette zone sécurisée ; et
3. chiffrant les résultats des opérations avant qu'ils ne quittent l'enclave.

Cependant, la technologie d'enclaves sécurisées est encore limitée à certains micro-services (comme des opérations cryptographiques). Par ailleurs, le code des applications s'exécutant dans l'enclave doit être écrit de telle sorte que l'application soit compatible avec l'enclave. Si un fournisseur ou un tiers fournit l'application dont certaines opérations sensibles doivent être effectuées dans l'enclave, alors le risque que ce fournisseur ou ce tiers ait accès aux données en clair reste présent. En outre, les technologies TEE peuvent comporter des vulnérabilités et de défauts, tant logiciels que matériels, comme celle mise à jour en août 2023 (baptisée « Downfall »), qui pourraient exposer, de façon accidentelle ou délibérée, les données en clair à un attaquant ou au fournisseur.

Vous souhaitez contribuer à l'amélioration de cette fiche ?

Écrivez à retours-cloud[@]cnil.fr

Articles en relation

- Comprendre les grands principes de la cryptologie et du chiffrement
- Cloud computing : les conseils de la CNIL pour les entreprises qui utilisent ces nouveaux services
- Référentiel général de sécurité (RGS) de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

- Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE

Sommaire
Les outils de sécurisation d'applications web dans l'informatique en nuage (cloud) >