# < SÉCURITÉ DES DONNÉES DANS LE CLOUD >

**CAMPUS CYBER** 2025

# < SOMMAIRE >

# < SOMMAIRE >

# < INTRODUCTION >

## 1. INTRODUCTION

Le Campus Cyber rassemble les acteurs de la cybersécurité dans une dynamique collaborative visant à renforcer la protection des systèmes numériques et à promouvoir l'excellence française dans ce domaine. Dans ce cadre, le Studio des communs coordonne plusieurs communautés d'intérêt, dont celle dédiée à la "Sécurisation du Cloud". Cette communauté réunit des experts issus de différents secteurs, avec pour objectif de proposer des réponses concrètes et opérationnelles aux risques spécifiques associés à l'usage du Cloud, en particulier la fuite de données, les intrusions ou encore les enjeux de conformité.

Ce guide est le fruit des travaux du groupe « Sécurité de la donnée » (comprenant BNP Paribas, I-Tracing, Lovell Consulting, Red Alert Labs, Wavestone), et s'adresse aux professionnels en charge de concevoir ou de déployer des solutions Cloud – architectes, développeurs, référents sécurité… Il se concentre sur un levier fondamental de la sécurité des données : le chiffrement.

Dans une approche de défense en profondeur, le chiffrement constitue une première ligne de protection. Il repose sur des algorithmes robustes (comme AES) et sur une gestion rigoureuse des clés. Cette protection cryptographique est renforcée par d'autres couches : des politiques d'accès et d'identité strictes, des mesures physiques dans les datacenters, des mécanismes organisationnels (audits, séparation des rôles), ainsi que par des dispositifs de sauvegarde et de surveillance. Ensemble, ces mesures visent à assurer la confidentialité, l'intégrité et la disponibilité des données.

Ce document se focalise spécifiquement sur le rôle central du chiffrement dans cette architecture de défense, en apportant une vision synthétique des menaces, des mécanismes de protection adaptés à chaque état de la donnée (au repos, en transit, en cours d'utilisation), ainsi que des solutions concrètes applicables à différents environnements Cloud. Chaque mesure est décrite de manière opérationnelle, avec un éclairage sur ses prérequis, ses coûts et ses limites de mise en œuvre.

Ce premier volume se concentre sur la confidentialité. Des volets complémentaires aborderont prochainement les dimensions d'intégrité et de disponibilité. Le Campus Cyber remercie chaleureusement les contributeurs pour leur engagement, et espère que ce guide vous apportera un éclairage utile et actionnable.

# 2. LE CONTEXTE

## 2.1 LE MODÈLE DE RESPONSABILITÉ PARTAGÉE

Dans les environnements Cloud (IaaS, PaaS, SaaS), le chiffrement des données est devenu indispensable pour garantir la confidentialité face aux risques croissants d'atteinte à la cybersécurité. Il protège les données contre les accès non autorisés — y compris de la part des fournisseurs Cloud eux-mêmes — et limite les risques liés à la réaffectation de ressources ou à l'accès aux supports physiques.

Ce chiffrement s'inscrit dans un modèle de responsabilité partagée :

- **Les fournisseurs Cloud (AWS, Azure, GCP…) assurent la sécurité physique des infrastructures et proposent des mécanismes de chiffrement intégrés.**
- **Les clients, quant à eux, restent responsables de la mise en œuvre des politiques de sécurité, de la gestion des clés de chiffrement et du contrôle des accès.**

Ainsi, sans configuration et gestion appropriées par le client, les garanties de confidentialité peuvent être compromises.

## 2.2 LA SÉCURITÉ PHYSIQUE

Dans un environnement Cloud, les entreprises n'ont plus de contrôle[1] direct sur les équipements qui stockent leurs données et leurs clés de chiffrement . Elles doivent donc s'appuyer sur les garanties physiques mises en place par les fournisseurs de services.

Même avec des algorithmes de chiffrement robustes, la sécurité des données repose aussi sur celle des infrastructures physiques. Si les serveurs ou les disques sont mal protégés, les données peuvent être compromises via des accès non autorisés ou des manipulations malveillantes.

C'est pourquoi la sécurité physique est un complément indispensable aux protections logicielles et cryptographiques. Elle fait partie des exigences de normes comme ISO/IEC 27001 (annexe A.11) ou SecNumCloud, qui imposent :

- **des contrôles d'accès physiques stricts,**
- **des systèmes de vidéosurveillance,**
- **des enregistrements d'accès,**
- **et des dispositifs d'alerte en cas d'intrusion.**

[1] Sauf dans les cas spécifiques d'utilisation de ses propres HSM, comme dans l'offre HYOK

## 2.3 LE CONTEXTE RÉGLEMENTAIRE

De nombreuses réglementations et normes internationales encouragent ou exigent l'usage du chiffrement des données pour protéger les informations sensibles :

- **Le RGPD (Europe) recommande le chiffrement pour sécuriser les données personnelles.**
- **Aux États-Unis, des textes comme la HIPAA (santé) ou le PCI DSS (cartes bancaires) imposent le chiffrement des données sensibles.**
- **En France, la certification HDS est requise pour l'hébergement de données de santé.**
- **D'autres cadres comme SecNumCloud (France), C5 (Allemagne) ou EUCS (niveau européen) prévoient explicitement des exigences de chiffrement et de bonnes pratiques cryptographiques.**

Même si ces obligations sont optionnelles dans certains cas, elles renforcent l'importance pour les entreprises d'adopter une stratégie de chiffrement robuste pour protéger les données et rester conformes aux exigences légales et contractuelles.

# 3. RISQUES ET MENACES

La sécurité des données dans le Cloud doit être envisagée en tenant compte de leurs trois états : en transit, au repos et en cours d'utilisation. Chacun de ces états expose la donnée à des menaces spécifiques, qu'il convient d'identifier clairement pour mettre en place des protections efficaces.

## 3.1 DONNÉES EN TRANSIT

Les données en transit, c'est-à-dire lorsqu'elles circulent entre services, utilisateurs ou environnements Cloud, sont particulièrement exposées aux risques d'interception, d'écoute illicite ou de manipulation. Ces menaces peuvent prendre la forme d'attaques passives (comme le sniffing) ou actives (man-in-the-middle), visant à capter ou modifier les flux réseau.

Dans l'environnement Cloud, ces risques sont accentués par la présence de nombreux services intermédiaires – tels que les équilibreurs de charge, les pares-feux applicatifs (WAF), les passerelles API ou les réseaux de diffusion de contenu (CDN) – qui terminent les connexions TLS pour inspecter ou router le trafic. Bien que ces services soient légitimes, ils déchiffrent temporairement les données, ce qui peut exposer des informations sensibles si la configuration est insuffisamment maîtrisée ou si l'un de ces services est compromis.

L'utilisation de protocoles de chiffrement obsolètes, ou mal configurés, constitue également un vecteur de vulnérabilité important. Enfin, certaines erreurs de configuration peuvent exposer des données en clair dans des journaux de diagnostic ou de débogage.

## 3.2 DONNÉES AU REPOS

Les données stockées dans le Cloud – qu'il s'agisse de volumes disques, de bases de données ou d'objets dans un stockage distribué – sont principalement menacées par les accès non autorisés. Ces accès peuvent résulter d'une compromission de compte, d'une mauvaise configuration de droits, ou d'une exposition involontaire (comme un bucket de stockage rendu public).

Même lorsqu'un chiffrement est en place, son efficacité peut être compromise par une mauvaise gestion des clés, notamment si celles-ci sont techniquement faibles, non renouvelées régulièrement, ou si leur cycle de vie n'est pas isolé par rôle. L'absence de politiques d'accès précises (IAM) constitue également un facteur de risque : si les permissions permettant d'utiliser ou de gérer les clés ne sont pas strictement contrôlées, des utilisateurs ou services non autorisés peuvent y accéder ou les exploiter de manière abusive. À cela s'ajoute le risque d'une délégation excessive au fournisseur Cloud, qui peut détenir l'intégralité des droits sur les clés.

Par ailleurs, des éléments souvent négligés comme les sauvegardes, archives ou snapshots mal protégés représentent des vecteurs potentiels de fuite, notamment si le chiffrement ou l'accès à ces ressources ne suivent pas les mêmes standards de sécurité que les données actives.

Au-delà de ces risques structurels, les failles applicatives représentent une menace souvent sous-estimée pour les données au repos. Un contrôle d'accès mal implémenté, une vulnérabilité d'injection (SQL ou NoSQL), ou une API mal sécurisée peuvent permettre à un attaquant d'accéder à des données chiffrées via un canal applicatif légitime. Par ailleurs, certains fichiers temporaires, caches ou journaux techniques peuvent contenir des données en clair si l'application ne gère pas correctement leur suppression ou leur chiffrement.

Ainsi, même lorsque le stockage est chiffré, une faille dans l'application qui y accède peut exposer la donnée.

### 3.3 DONNÉES EN COURS D'UTILISATION

Les données en cours d'utilisation, c'est-à-dire lorsqu'elles sont traitées activement en mémoire par une application ou un service, représentent une zone de risque critique mais souvent mal maîtrisée. En effet, pour qu'une donnée chiffrée puisse être utilisée, elle doit être déchiffrée en mémoire. Pendant cette phase, elle est théoriquement accessible à tout acteur capable de lire cette mémoire : processus malveillant, utilisateur privilégié, hyperviseur compromis, etc.

Dans un environnement Cloud, l'utilisateur ne maîtrise pas les couches d'infrastructure sous-jacentes, telles que l'hyperviseur, le système d'exploitation hôte ou le matériel. Cela crée un espace de confiance réduit, en particulier lors du traitement de données sensibles.

Même dans les modèles avancés de gestion des clés comme BYOK (Bring Your Own Key) ou HYOK (Hold Your Own Key), il est souvent nécessaire que certaines clés intermédiaires — notamment les Key Encryption Keys (KEK) ou les Data Encryption Keys (DEK) — soient chargées en mémoire dans les environnements contrôlés par le fournisseur, ne serait-ce que temporairement, pour permettre les opérations de chiffrement ou de déchiffrement. Cela ouvre plusieurs vecteurs de risque, même si la master key (MK), généralement conservée dans un HSM ou un environnement fortement isolé, reste inaccessible :

- **Accès mémoire à la volée : un processus malveillant, une faille de l'hyperviseur, ou un administrateur compromis pourrait capturer une DEK ou une KEK en clair pendant son utilisation temporaire.**
- **Journalisation involontaire : une clé utilisée dans un processus automatisé peut accidentellement être enregistrée dans un log système ou une trace de débogage.**
- **Usage détourné : si les permissions IAM liées à la clé sont trop larges, un acteur interne peut déclencher des opérations de déchiffrement via l'API du fournisseur (KMS) sans jamais voir la clé, mais tout en accédant aux données en clair.**
- **Shadow key usage : dans certains cas, des composants internes du fournisseur Cloud peuvent faire usage de copies temporaires de clés pour fournir des services intégrés (par exemple l'analyse automatique ou l'indexation), sans que cela soit explicitement visible dans la configuration du client.**

## 4. CLASSIFICATION ET APPROCHE PROPORTIONNÉE

L'un des fondements d'une politique efficace de protection des données dans le Cloud repose sur une classification claire des données. Cette démarche consiste à identifier le niveau de sensibilité de chaque type d'information manipulée ou stockée, puis à lui associer un niveau de protection proportionné.

Classer les données permet de différencier les traitements : toutes les données ne présentent pas les mêmes enjeux en termes de confidentialité, d'intégrité ou de disponibilité. Par exemple, un document interne de travail ne requiert pas le même niveau de sécurisation qu'un dossier contenant des données de santé, des informations financières critiques ou des secrets industriels.

Cette classification repose souvent sur des labels ou niveaux de sensibilité, tels que :

- **Public : informations pouvant être diffusées sans restriction.**
- **Interne : données destinées à un usage limité à l'organisation.**
- **Confidentiel : informations sensibles nécessitant des mesures de protection renforcées.**
- **Très confidentiel / Secret : données critiques dont la divulgation aurait un impact majeur (juridique, financier, opérationnel…).**

Sur la base de cette classification, des mesures techniques et organisationnelles différenciées sont mises en œuvre :

- **Pour les données peu sensibles, un chiffrement standard peut suffire. Dans certains cas, un contrôle d'accès strictement défini peut même être considéré comme une mesure de sécurité suffisante.**[2]
- **Pour les données critiques, on privilégiera des algorithmes robustes, une gestion fine des accès, un stockage isolé, voire des solutions de type Confidential Computing ou chiffrement côté client.**

2 A condition :
Que les accès soient limitativement attribués (principe du moindre privilège),
Que les rôles et permissions soient revus régulièrement,
Que les accès soient journalisés et auditables.

# < CLASSIFICATION ET APPROCHE PROPORTIONNÉE >

L'objectif est d'éviter un surdimensionnement coûteux, tout en garantissant un niveau de sécurité adapté à la valeur et aux contraintes associées à chaque catégorie de données.

Cette approche proportionnée permet d'optimiser les ressources de sécurité, de réduire les surfaces d'exposition inutilement complexes et de répondre plus efficacement aux exigences réglementaires, en démontrant que les protections sont alignées avec la nature des données traitées.

# 5. PROTECTION DES DONNÉES EN TRANSIT

Les données en transit sont les informations qui circulent activement entre systèmes — que ce soit via Internet, un réseau privé ou au sein d'un environnement Cloud. Leur protection est essentielle pour éviter les interceptions, notamment lors des échanges entre services ou avec des utilisateurs.

Deux approches complémentaires sont décrites ci-dessous.

## 5.1 CHIFFREMENT DU CANAL (NIVEAU TRANSPORT)

Le chiffrement du canal vise à protéger les données en transit contre l'interception ou l'altération lors de leur transfert entre deux points. Il repose sur des protocoles de sécurité du transport comme TLS ou IPsec, qui assurent la confidentialité, l'intégrité et l'authenticité des échanges réseau.

Le protocole TLS (Transport Layer Security), dans ses versions récentes (1.2 et 1.3), est aujourd'hui la norme pour sécuriser les communications sur Internet et dans les architectures Cloud. Il est recommandé de bannir l'usage de versions obsolètes comme SSL, TLS 1.0 ou 1.1, qui présentent des vulnérabilités connues.

En environnement de production, l'utilisation de certificats wildcard (*.domaine.com) est déconseillée, car la compromission d'un seul certificat compromettrait l'ensemble des sous-domaines. Il est également essentiel de protéger les clés privées associées aux certificats TLS à l'aide de HSM ou de coffres-forts numériques.

Dans certains cas, notamment pour des communications internes entre machines ou pour des environnements hybrides, le protocole IPsec peut être utilisé en complément ou en alternative à TLS. IPsec chiffre les paquets IP eux-mêmes au niveau réseau, ce qui en fait une solution adaptée aux VPN, aux communications inter-VPC ou aux liaisons entre datacenters.

Enfin, pour anticiper les risques liés à l'émergence de l'informatique quantique, il est recommandé d'explorer les protocoles hybrides TLS-PQC (post-quantum cryptography), tels que les combinaisons Kyber + X25519, qui associent un algorithme classique à un algorithme résistant aux attaques quantiques.

## 5.2 CHIFFREMENT DES DONNÉES ELLES-MÊMES

Lorsque le chiffrement du canal ne suffit pas à garantir une protection de bout en bout — par exemple dans des architectures complexes intégrant des composants intermédiaires (load balancers, WAF, CDN) — il devient pertinent de chiffrer directement les données applicatives, indépendamment du transport.

# < PROTECTION DES DONNÉES EN TRANSIT >

Cette approche consiste à chiffrer les champs sensibles des données (comme un numéro de carte bancaire ou un identifiant patient) dès leur création, souvent via des mécanismes de Field-Level Encryption (FLE). Cela permet de conserver une partie de l'utilisabilité des données pour les traitements applicatifs, tout en limitant leur exposition.

Pour les données hautement sensibles, il est recommandé de privilégier des architectures dans lesquelles les données restent chiffrées jusqu'au serveur final ou au contexte de traitement sécurisé. Cela suppose d'éviter tout déchiffrement intermédiaire, y compris par le fournisseur Cloud. Ce principe est particulièrement pertinent dans les environnements traitant des données de santé, financières ou à forte valeur stratégique.

Enfin, pour garantir une réelle protection de bout en bout, toutes les communications internes, y compris celles qui transitent entre services via des réseaux privés ou des API internes, doivent être chiffrées. Cela implique d'auditer régulièrement les configurations des services intermédiaires afin de s'assurer qu'aucun flux n'est exposé en clair, y compris en cas d'erreur de configuration.

# 6. PROTECTION DES DONNÉES AU REPOS

## 6.1 INTRODUCTION

Le chiffrement des données au repos est une mesure de sécurité essentielle dans le Cloud. Il consiste à rendre les données illisibles lorsqu'elles sont stockées sur des supports physiques ou virtuels, comme des disques, bases de données ou stockages objets. Contrairement au chiffrement des données en transit, il s'applique lorsque les données ne circulent pas, mais résident dans un système. Son objectif est de garantir que les informations restent inaccessibles en cas d'accès non autorisé, qu'il soit physique (ex. : vol de disque) ou logique (ex. : fuite de credentials).

## 6.2 NIVEAUX DE CHIFFREMENT

Plusieurs niveaux de chiffrement peuvent être mobilisés :

- **Le chiffrement au niveau disque, global, s'applique à un volume complet à l'aide d'outils comme BitLocker ou LUKS.**
- **Le chiffrement au niveau fichier ou objet cible des unités spécifiques, offrant une protection plus granulaire.**
- **Le chiffrement au niveau base de données, via des mécanismes comme TDE, protège les structures de données tout en permettant aux utilisateurs autorisés de les consulter.**
- **Le chiffrement côté application est le plus souverain : l'application chiffre les données avant stockage, assurant que même les couches système ou les services Cloud ne voient jamais les données en clair.**

## 6.3 GESTION DES CLÉS

Dans tous les cas, la gestion des clés est critique. Elle repose généralement sur un Key Management Service (KMS), qui permet de générer, stocker, faire tourner, révoquer et auditer les clés de manière centralisée. Cet aspect est traité plus en détails dans le chapitre dédié.

## 6.4 STRATÉGIES DE CHIFFREMENT

Deux grandes stratégies coexistent :

### 6.4.1. Chiffrement géré par le fournisseur

La plateforme Cloud chiffre les données automatiquement, en gérant également les clés via ses propres outils (ex. : AWS KMS, Azure Key Vault, GCP KMS). Cette approche est simple, efficace et souvent activée par défaut. Cependant, elle nécessite de faire confiance au fournisseur, qui peut théoriquement accéder aux clés.

### 6.4.2. Chiffrement côté client (client-side encryption)

L'organisation chiffre les données en local avant de les envoyer dans le Cloud, en conservant la maîtrise exclusive des clés. Cette méthode garantit que le fournisseur ne peut jamais accéder aux données en clair. Elle est particulièrement adaptée aux environnements à fortes exigences de confidentialité (secteurs réglementés, données sensibles, logique zero trust), mais implique une gestion complexe des clés, une perte potentielle de certaines fonctionnalités Cloud (recherche, IA…) et une charge opérationnelle plus importante.

## 6.5 HIÉRARCHIE DES CLÉS

Les fournisseurs Cloud utilisent une hiérarchie de clés en trois niveaux :

- **La Master Key (MK), stockée dans un HSM ou un service sécurisé, ne sert qu'à chiffrer les clés intermédiaires.**
- **La Key Encryption Key (KEK), gérée par le KMS, chiffre les clés de données et peut être renouvelée indépendamment des données elles-mêmes.**
- **La Data Encryption Key (DEK) est générée à la volée pour chiffrer les données concrètes (fichiers, enregistrements), et reste le seul élément manipulé directement par les services applicatifs.**

Cette architecture permet une séparation des responsabilités, une rotation simplifiée des clés, et une traçabilité fine grâce à des journaux d'audit à chaque niveau.

## 6.6 SOLUTIONS TIERCES CÔTÉ CLIENT

Certaines organisations optent pour des solutions tierces totalement indépendantes du fournisseur Cloud. Elles utilisent des outils locaux pour effectuer le chiffrement/déchiffrement avant toute interaction avec le Cloud. Cette approche renforce l'indépendance et peut répondre à des obligations réglementaires strictes, mais elle introduit des contraintes : complexité d'intégration, surcharge de calcul, et risques accrus en cas de perte des clés. Exemple de technologie : Cosmian covercrypt.

## 6.7 BONNES PRATIQUES CÔTÉ CLIENT

Dans le modèle de responsabilité partagée, le client conserve un rôle essentiel dans la mise en œuvre effective du chiffrement des données au repos. Plusieurs bonnes pratiques doivent être appliquées pour garantir une protection efficace et conforme.

Il est d'abord indispensable de vérifier que le chiffrement est activé sur toutes les ressources pertinentes, qu'il s'agisse de volumes disques, de bases de données, de stockages objets ou de sauvegardes. Cette vérification doit être systématique, notamment lors du déploiement automatisé de nouvelles ressources.

Le choix de la stratégie de chiffrement doit être aligné avec la sensibilité des données. Une solution gérée par le fournisseur conviendra à la plupart des cas d'usage, mais les environnements critiques peuvent exiger un chiffrement côté client, offrant une maîtrise exclusive des clés.

La gestion des clés de chiffrement requiert une attention particulière. Le client doit mettre en place des politiques d'accès strictes, planifier la rotation régulière des clés, auditer leur usage et s'assurer qu'elles sont stockées dans un environnement sécurisé (KMS, HSM).

Lorsque le chiffrement est mis en œuvre au niveau applicatif, il est essentiel d'intégrer les bonnes pratiques de sécurité dans le code lui-même : protection des fichiers temporaires, gestion des caches, sécurisation des secrets, et traitement rigoureux des données avant stockage.

Enfin, la documentation des mécanismes de chiffrement, associée à une traçabilité complète via des journaux d'audit, permet au client de démontrer sa conformité en cas de contrôle ou d'incident.

# 7. PROTECTION DES DONNÉES EN COURS D'UTILISATION

## 7.1 INTRODUCTION

Alors que les mesures de sécurité traditionnelles ciblent les données au repos (stockées sur disque) ou en transit (circulant sur un réseau), les données en cours d'utilisation – c'est-à-dire présentes en mémoire vive (RAM), dans les caches ou les registres processeur – restent souvent non chiffrées. Cette vulnérabilité, longtemps négligée, devient critique dans un contexte de généralisation du Cloud computing et de mutualisation des ressources, où les couches d'infrastructure (hyperviseur, OS, CPU) ne sont plus maîtrisées par l'utilisateur.

Pour combler cette faille, un nouveau paradigme de sécurité s'impose : le Computing on Encrypted Data. Il désigne l'ensemble des techniques permettant de traiter des données sans jamais les exposer en clair durant l'exécution. Deux grandes familles d'approches émergent :

• Crypto-based Secure Computation : repose sur des mécanismes purement cryptographiques, tels que le chiffrement homomorphe ou le Secure Multi-Party Computation (SMPC), permettant de réaliser des calculs directement sur des données chiffrées.

• Hardware-based Secure Computation, plus connue sous le nom de Confidential Computing : s'appuie sur des environnements d'exécution isolés matériellement et attestés (Trusted Execution Environments – TEE), dans lesquels les données peuvent être déchiffrées et traitées en toute confidentialité, même dans un Cloud non totalement fiable.

Dans cette section, nous allons nous concentrer principalement sur le Confidential Computing, en tant que solution déjà mature, intégrée aux offres des principaux fournisseurs Cloud, et soutenue par un écosystème technologique en pleine expansion (Intel SGX/TDX, AMD SEV-SNP, AWS Nitro Enclaves, etc.).

Nous aborderons également, de manière plus succincte, les principes du chiffrement homomorphe, technologie encore émergente mais prometteuse, qui ouvre la voie à des traitements véritablement zero-trust, y compris dans des environnements multi-cloud ou hostiles.

## 7.2 CONFIDENTIAL COMPUTING

Selon le Confidential Computing Consortium, cette approche repose sur l'utilisation d'un Trusted Execution Environment (TEE) matériel, garantissant :

- **Confidentialité des données : aucune entité non autorisée ne peut lire les données en cours d'utilisation.**
- **Intégrité des données : aucune modification possible par des entités extérieures au TEE.**
- **Intégrité du code : le code s'exécutant dans le TEE ne peut être modifié.**
- **Attestabilité : capacité à prouver de manière cryptographique que l'environnement est sécurisé.**

Cette technologie réduit la taille du Trusted Computing Base (TCB), en limitant le nombre de composants auxquels faire confiance.

### 7.2.1 Implémentations matérielles du Confidential Computing

Plusieurs technologies matérielles ont émergé depuis les années 2010 pour concrétiser le modèle du Confidential Computing, en créant des environnements d'exécution isolés capables de protéger les données en cours de traitement, même en cas de compromission de l'infrastructure sous-jacente.

**Intel SGX** (Software Guard Extensions), introduit en 2015 avec les processeurs Intel Skylake, crée des enclaves sécurisées directement dans la mémoire, permettant ainsi de protéger les données même dans le cas où le système d'exploitation ou le BIOS serait compromis. Cette solution offre une isolation très granulaire, mais elle requiert une réécriture partielle du code applicatif et peut avoir un impact significatif sur les performances.

**Intel TDX** (Trust Domain Extensions), présenté en 2021, s'adresse principalement aux machines virtuelles (Trusted Domains) et ne nécessite pas de modification du code applicatif. Il propose de meilleures performances que SGX, bien que l'isolation soit moins fine, car elle s'effectue au niveau de la VM. Intel TDX vise à sécuriser les environnements virtualisés de manière plus flexible.

# < PROTECTION DES DONNÉES EN COURS D'UTILISATION >

**AMD SEV-SNP**, déployé à partir de 2021 dans les processeurs EPYC de 3e génération (Milan), fournit une protection mémoire pour les machines virtuelles, en garantissant à la fois l'intégrité et l'isolation matérielle. Fonctionnant selon des principes similaires à ceux d'Intel TDX, mais dans l'écosystème AMD, cette technologie permet une exécution sécurisée même si l'hyperviseur est compromis.

**NVIDIA Confidential Computing**, annoncé en 2023, s'applique quant à lui aux GPU, notamment les modèles A100 et H100, utilisés pour les charges de travail en intelligence artificielle et en machine learning. Il garantit une isolation efficace des traitements sans compromettre les performances, et son fonctionnement est totalement transparent pour les applications, ne nécessitant aucune refactorisation.

### 7.2.2 Approches spécifiques

**AWS Nitro Enclaves** propose une implémentation logicielle d'un environnement d'exécution de confiance (TEE), sous forme d'enclaves isolées rattachées aux instances EC2. Cette solution est plus souple à déployer que les alternatives matérielles, bien qu'elle offre un niveau de sécurité généralement inférieur. L'attestation de l'enclave est assurée par l'hyperviseur Nitro d'AWS, et peut être intégrée de manière transparente aux services de gestion de clés comme AWS KMS.

**Confidential Containers (CoCo)** repose sur une isolation au niveau des conteneurs, en s'appuyant sur des technologies comme Kata Containers et AMD SEV-SNP. Cette approche permet d'exécuter des applications de manière confidentielle, sans nécessiter de modification du code. Porté par la Cloud Native Computing Foundation (CNCF), le projet bénéficie d'une adoption croissante, notamment chez Microsoft Azure. La société Edgeless Systems propose par ailleurs une version enrichie de cette solution, incluant des mécanismes d'attestation renforcés et une isolation plus fine entre les conteneurs.

### 7.2.3 Vérification de l'attestation

L'attestabilité est l'un des piliers du Confidential Computing : elle permet de vérifier qu'un environnement d'exécution de confiance (TEE) est bien sécurisé, conforme, et qu'il n'a pas été altéré. Si cette vérification peut être réalisée localement, elle reste insuffisante dans un contexte Cloud – et a fortiori dans un environnement multi-cloud – où les machines virtuelles, conteneurs ou enclaves peuvent être instanciés dynamiquement sur des infrastructures partagées.

Dans ce cadre, une attestation à distance devient indispensable. Elle permet à un système externe, tiers de confiance, de valider cryptographiquement l'intégrité de l'environnement, indépendamment de l'hébergeur Cloud. Cette séparation est cruciale pour éviter tout conflit d'intérêts, notamment lorsque le fournisseur d'infrastructure est aussi celui qui génère les preuves d'attestation.

Plusieurs exemples illustrent cette évolution :

- **Azure Attestation Service permet d'attester des environnements SGX, TPM et AMD SEV-SNP, mais reste un service dépendant du CSP.**
- **Intel Trust Authority propose une attestation indépendante pour SGX et TDX, garantissant une séparation entre le fournisseur Cloud et le validateur.**
- **Google Cloud collabore avec Intel pour assurer l'attestation des machines virtuelles confidentielles basées sur TDX.**

Dans une architecture Cloud critique, la mise en place d'une attestation à distance indépendante renforce significativement la confiance dans les traitements effectués, en permettant à l'utilisateur final de s'assurer que les opérations sensibles se déroulent bien dans un environnement isolé, non modifié, et reconnu comme tel par une autorité extérieure.

## 7.3 CHIFFREMENT HOMOMORPHE (HE)

Le chiffrement homomorphe constitue une approche innovante et complémentaire au Confidential Computing. Il permet d'effectuer des traitements directement sur des données chiffrées, sans jamais devoir les déchiffrer, ce qui ouvre la voie à des modèles de calcul réellement « zero-trust ».

Il existe deux principales variantes de cette technologie. Le chiffrement homomorphe partiel autorise une seule opération sur les données chiffrées (par exemple l'addition ou la multiplication), ce qui le rend adapté à certains cas d'usage ciblés. Le chiffrement homomorphe total – ou Fully Homomorphic Encryption (FHE) – permet quant à lui de réaliser l'ensemble des opérations applicatives directement sur des textes chiffrés, sans restriction. Toutefois, cette approche reste extrêmement coûteuse en ressources de calcul et en temps d'exécution, ce qui en limite encore les usages en production à grande échelle.

Les algorithmes de chiffrement homomorphe reposent généralement sur des fondements mathématiques considérés comme résistants aux attaques quantiques, notamment le problème du Ring Learning With Errors (RLWE). Conscients de son potentiel stratégique, plusieurs acteurs du secteur – parmi lesquels Microsoft, IBM, NIST, Duality, et des universités comme le MIT – participent aujourd'hui à des travaux de standardisation internationale pour encadrer son usage et en favoriser l'adoption.

## 7.4 CONCLUSION

Le Confidential Computing apporte une réponse opérationnelle et désormais industrialisée au défi de la sécurisation des données en cours d'utilisation, en complétant efficacement les protections déjà existantes pour les données au repos et en transit. En confinant les traitements sensibles dans des environnements matériellement isolés et attestés (TEE), il réduit la nécessité de faire confiance à l'infrastructure cloud sous-jacente — tout en introduisant de nouveaux points de confiance, notamment le matériel et les services d'attestation.

Des solutions comme Cosmian VM, qui s'inscrit pleinement dans ce paradigme, proposent un modèle de traitement confidentiel enrichi par des mécanismes de vérifiabilité continue, renforçant la traçabilité et l'intégrité des environnements d'exécution.

À plus long terme, le chiffrement homomorphe constitue une approche complémentaire: bien qu'encore limité en pratique, il permet de traiter directement des données chiffrées sans les exposer, offrant des perspectives intéressantes pour les environnements zero-trust.

Ces deux modèles peuvent coexister, selon les besoins en performance, en souveraineté ou en résilience.

# 8. GESTION DES CLÉS

## 8.1 INTRODUCTION

Avec la migration massive des systèmes d'information vers le Cloud, la question de la gestion des clés de chiffrement est devenue centrale. La confidentialité des données sensibles et le respect des exigences réglementaires (RGPD, DORA...) passent par un contrôle strict des clés, y compris vis-à-vis du fournisseur de services Cloud (CSP).

## 8.2 RÔLE ET USAGE DES CLÉS DANS LE CLOUD

Les clés de chiffrement sont utilisées pour protéger les données au repos (disques, bases de données, objets). Les opérations de chiffrement/déchiffrement sont généralement effectuées directement par les services Cloud eux-mêmes, que les clés soient gérées par le CSP ou fournies par le client.

Le chiffrement, même réalisé avec les clés du fournisseur, offre une protection de base contre l'accès non autorisé. Toutefois, pour garantir une véritable souveraineté, il est essentiel de contrôler tout ou une partie du cycle de vie des clés.

## 8.3 BONNES PRATIQUES DE GESTION DES CLÉS

Parmi les bonnes pratiques en matière de gestion des clés, la première consiste à assurer une génération sécurisée, en utilisant un HSM (ou à défaut un Software Security Module) garantissant un haut niveau de protection contre l'exfiltration. Il est essentiel de veiller à l'isolement des clés, soit par client dans le cas d'un HSM mutualisé ou partitionné, soit par usage pour les traitements particulièrement critiques.

La rotation périodique des clés permet de limiter l'impact d'une éventuelle compromission, en réduisant la durée pendant laquelle une clé compromise reste exploitable.

Enfin, un contrôle d'accès strict doit être mis en place à l'aide de politiques IAM complété par une traçabilité systématique des actions sur les clés via des mécanismes d'audit.

## 8.4 MODÈLES DE GESTION DES CLÉS

| Modèle | Description | Avantages | Contraintes | Exemples |
|---|---|---|---|---|
| CSP Managed Keys | Le fournisseur gère tout | Simplicité, faible coût | Aucun contrôle, non-conformité possible | AWS KMS, Azure Key Vault |
| Customer Managed Keys (CMK) | Le client pilote la politique dans le KMS du CSP | Contrôle[3], conformité | Complexité accrue | AWS CMK, Azure CMK |
| BYOK | Le client génère et importe ses clés | Origine maîtrisée, Conformité[4] | Rotation manuelle, import complexe | AWS BYOK, GCP External Key |
| Client-Managed HSM | HSM dédié ou partition gérée par le client | Flexibilité, conformité[4] | Coût, compétences requises | AWS CloudHSM, Azure Dedicated HSM |
| HYOK | Clés hébergées hors du Cloud | Souveraineté maximale, Conformité[4] | SPOF réseau, configuration complexe | AWS XKS, GCP EKM |

## 8.5 CLÉ ≠ ENVIRONNEMENT D'EXÉCUTION : UNE DISTINCTION ESSENTIELLE

Même si une organisation maîtrise l'origine et le stockage de ses clés (via BYOK ou HYOK), les opérations de chiffrement/déchiffrement ont lieu dans les services du CSP.

Conséquences :

- **Les données sont visibles en mémoire au moment du traitement.**
- **L'environnement d'exécution (OS, hyperviseur, CPU) reste sous contrôle du fournisseur.**

Il subsiste donc un risque de compromission (attaque en RAM, compromission interne).

Le Confidential Computing est une réponse émergente à ce problème, en confinant ces opérations sensibles dans des enclaves matérielles attestées (SGX, TDX, SEV-SNP...).

3 Définir les politiques d'utilisation des clés ; restreindre les permissions IAM sur les opérations de chiffrement/déchiffrement; auditer les accès aux clés (logs d'usage) ; décider de la rotation, de la révocation, ou de la suppression d'une clé.

4 Capacité à se conformer à des exigences réglementaires ou normatives internes

## 8.6 RISQUES ET LIMITATIONS

Bien que les solutions de chiffrement dans le Cloud offrent un haut niveau de sécurité, elles présentent également certaines limites et points de vigilance qu'il convient d'anticiper, tant sur les plans techniques qu'opérationnels ou réglementaires.

Sur le plan technique, les clés de chiffrement restent accessibles en mémoire vive (RAM) au moment de l'exécution, ce qui constitue une surface d'exposition potentielle. Par ailleurs, les modèles HYOK (Hold Your Own Key), qui reposent sur une infrastructure de clés externe, peuvent subir des latences ou des indisponibilités en raison de leur dépendance à la connectivité réseau.

Les limitations spécifiques aux modèles HYOK sont également notables. Le lien entre l'environnement Cloud et le HSM du client constitue un point de vulnérabilité critique. Une panne ou une latence excessive peut entraîner l'échec des opérations de chiffrement ou de déchiffrement, rendant nécessaire la mise en place d'une architecture de haute disponibilité pour garantir la résilience du système.

Sur le plan opérationnel, ces approches requièrent des compétences techniques avancées en matière de HSM et imposent souvent un double inventaire des clés,[5] notamment dans les modèles BYOK (Bring Your Own Key), ce qui augmente la complexité de gestion.

Enfin, certaines contraintes réglementaires doivent être prises en compte. Les clés mutualisées peuvent ne pas être conformes aux exigences du RGPD ou du règlement DORA.[6] De plus, les clés gérées exclusivement par les fournisseurs Cloud (CSP-managed) sont souvent non exportables, ce qui limite la flexibilité pour répondre à certaines politiques de souveraineté ou d'interopérabilité.

5 Le double inventaire de clés dans les modèles comme BYOK (Bring Your Own Key) s'explique par la coexistence de deux environnements de gestion :

1. L'environnement interne du client, où la clé d'origine est générée, stockée, documentée et potentiellement utilisée à d'autres fins internes (chiffrement sur site, sauvegarde locale, etc.).
2. L'environnement du fournisseur Cloud, où cette même clé (ou une version encapsulée/importée) est injectée dans un KMS (Key Management Service) pour être utilisée dans les services Cloud (S3, EBS, Azure Blob, etc.).

6 RGPD – Maîtrise des moyens de traitement : L'article 28(3)(c) du RGPD (UE 2016/679) impose que les sous-traitants garantissent la maîtrise exclusive des moyens de traitement, ce qui inclut les clés de chiffrement. L'article 32 renforce cette exigence par la mise en œuvre de mesures de sécurité adaptées au risque.
DORA – Exigences en matière de résilience cryptographique : Le règlement (UE) 2022/2554 impose aux entités financières de protéger les données sensibles avec des schémas cryptographiques robustes (art. 9) et d'anticiper la compromission des clés dans les tests de résilience (art. 24).

## 9. CONCLUSION ET PERSPECTIVES

La protection des données dans le Cloud repose sur une **stratégie de sécurité cohérente, couvrant l'ensemble de leur cycle de vie :** en transit, au repos, et en cours d'utilisation. À chaque étape, le chiffrement joue un rôle central, à condition d'être correctement configuré, associé à une gestion rigoureuse des clés et intégré dans une gouvernance appropriée.

Pour **les données en transit,** les protocoles comme TLS ou IPsec offrent une protection efficace contre les interceptions, à condition de respecter les bonnes pratiques (versions modernes, protection des clés privées, fin des certificats faibles). Dans certains cas, un chiffrement complémentaire des données applicatives est nécessaire pour garantir une confidentialité de bout en bout.
**Les données au repos** bénéficient généralement d'un chiffrement activé par défaut. Néanmoins, l'efficacité de cette protection dépend largement de la maîtrise des clés : choix des modèles (BYOK, HYOK), politiques IAM strictes, rotation périodique, et auditabilité. Une mauvaise configuration ou une délégation excessive au fournisseur peut sérieusement affaiblir la sécurité. La hiérarchie des clés (MK, KEK, DEK) et la classification des données constituent des piliers structurants.
Pour **les données en cours d'utilisation,** le chiffrement classique atteint ses limites : dès qu'une donnée est déchiffrée en mémoire, elle redevient vulnérable. Le Confidential Computing répond à ce défi en assurant l'exécution dans des environnements isolés matériellement (TEE) et vérifiables, comme Intel SGX, AMD SEV-SNP ou AWS Nitro Enclaves.

**La gestion des clés** doit concilier simplicité, contrôle, performance et conformité. Si les modèles avancés (HYOK, HSM dédiés) offrent une souveraineté maximale, ils introduisent aussi des défis techniques et opérationnels, notamment en termes de disponibilité et d'intégration.
Une distinction essentielle doit être faite entre la possession des clés et le contexte d'exécution : une clé bien protégée ne suffit pas si les opérations de chiffrement se déroulent dans un environnement non maîtrisé (hyperviseur, OS, CPU partagés).

Avec **la montée du multi-cloud,** les organisations doivent harmoniser leurs politiques de sécurité, assurer une interopérabilité entre fournisseurs, et maintenir une gouvernance unifiée des clés à travers des outils compatibles (KMS, HSM fédérés, API standardisées).

Enfin, **la tendance va désormais au-delà du chiffrement** : l'enjeu est de mettre en place des modèles vérifiables, capables de prouver que les traitements ont été effectués dans des environnements sûrs, conformes, et intègres. Des solutions comme Cosmian VM, Edgeless Systems ou Azure Confidential Ledger incarnent cette nouvelle génération d'approches, en intégrant attestation cryptographique, traçabilité, et preuves de conformité de bout en bout.

# < GLOSSAIRE >

**AES (Advanced Encryption Standard)** : Algorithme de chiffrement symétrique largement utilisé, recommandé dans ses variantes 128 ou 256 bits pour la protection des données.

**Attestation (Confidential Computing)** : Mécanisme cryptographique permettant de prouver qu'un environnement sécurisé (TEE) n'a pas été altéré avant d'y exécuter du code sensible.

**BYOK (Bring Your Own Key)** : Modèle dans lequel le client génère ses propres clés de chiffrement et les importe dans l'environnement du fournisseur Cloud.

**CDN (Content Delivery Network)** : Réseau de serveurs répartis géographiquement permettant une diffusion optimisée de contenu, souvent utilisé dans le Cloud.

**Chiffrement homomorphe** : Technique permettant d'effectuer des calculs sur des données chiffrées sans les déchiffrer, préservant ainsi leur confidentialité.

**CMK (Customer Managed Key)** : Clé de chiffrement dont la gestion est assurée par le client, via le KMS d'un fournisseur Cloud.

**Confidential Computing** : Paradigme de sécurité visant à protéger les données en cours d'utilisation via des enclaves matérielles sécurisées.

**FHE (Fully Homomorphic Encryption)** : Forme avancée de chiffrement homomorphe permettant tout type de calcul sur des données chiffrées.

**HSM (Hardware Security Module)** : Matériel spécialisé utilisé pour générer, stocker et manipuler des clés cryptographiques de manière sécurisée.

**HYOK (Hold Your Own Key)** : Approche dans laquelle les clés de chiffrement sont conservées exclusivement hors de l'environnement Cloud.

**KMS (Key Management Service)** : Service proposé par les fournisseurs Cloud pour gérer le cycle de vie des clés de chiffrement (création, rotation, révocation…).

**RLWE (Ring Learning With Errors)** : Problème mathématique utilisé dans la cryptographie post-quantique, notamment pour le chiffrement homomorphe.

**SaaS / PaaS / IaaS** : Modèles de services Cloud. SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service).

**TLS (Transport Layer Security)** : Protocole cryptographique assurant la confidentialité et l'intégrité des communications réseau.

**TEE (Trusted Execution Environment)** : Environnement d'exécution sécurisé, isolé du système principal, utilisé pour protéger les données et le code sensible.

**XKS (External Key Store)** : Mécanisme proposé par AWS pour permettre l'utilisation de clés stockées en dehors du Cloud, dans un modèle HYOK.

# < BIBLIOGRAPHIE >

## NORMES ET RÉGLEMENTATIONS


• Règlement général sur la protection des données (RGPD) – Règlement (UE) 2016/679.
https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4
• Digital Operational Resilience Act (DORA) – Règlement (UE) 2022/2554.
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022R2554


## RÉFÉRENTIELS TECHNIQUES ET GUIDES


• ANSSI – Guide des mécanismes cryptographiques (v2.04).
https://cyber.gouv.fr/sites/default/files/2021-03/anssi-guide-mecanismes_crypto-2.04.pdf
• CNIL – Les pratiques de chiffrement dans l'informatique en nuage (Cloud) public.
https://www.cnil.fr/fr/les-pratiques-de-chiffrement-dans-linformatique-en-nuage-cloud-public
• ENISA – Post-Quantum Cryptography: Current state and mitigation (v2).
https://www.enisa.europa.eu/publications/enisa-report-post-quantum-cryptography
• RFC 8446 – The Transport Layer Security (TLS) Protocol Version 1.3.
https://datatracker.ietf.org/doc/html/rfc8446
• RFC 4301 – Security Architecture for the Internet Protocol (IPsec).
https://datatracker.ietf.org/doc/html/rfc4301


## PUBLICATIONS DE CONSORTIUMS ET FOURNISSEURS


• Confidential Computing Consortium – Common Terminology for Confidential Computing (2023).
https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/Common-Terminology-for-Confidential-Computing.pdf
• AWS – Introduction to External Key Store (XKS).
https://github.com/aws/aws-kms-xksproxy-api-spec/blob/main/xks_proxy_api_spec.md
• AWS post-quantum cryptography migration plan
https://aws.amazon.com/blogs/security/aws-post-quantum-cryptography-migration-plan/
• Azure – Confidential Ledger Overview.
https://learn.microsoft.com/en-us/azure/confidential-ledger/
• Cosmian – Confidential VM & Covercrypt documentation.
https://docs.cosmian.com/encrypt/covercrypt/
https://docs.cosmian.com/compute/cosmian_vm/overview/
• Edgeless Systems – Confidential Kubernetes with Constellation.
https://docs.edgeless.systems/constellation

< Studio des Communs >

CAMPUS CYBER

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : **COMMUNAUTES@CAMPUSCYBER.FR**
5 - 7 RUE BELLINI 92800, PUTEAUX



CE PROJET A ÉTÉ FINANCÉ PAR LE GOUVERNEMENT
DANS LE CADRE DU PROGRAMME D'INVESTISSEMENTS D'AVENIR