25.082 OCF. Dossier électronique de santé. Loi fédérale
Séance de la CSSS-N des 20 et 21 août 2026

Rapport succinct du 3 août 2026 sur les effets d'un chiffrement de bout en bout pour le DES

Mandat à l'administration – chiffrement de bout en bout

L'administration est chargée de présenter les effets concrets d'un chiffrement de bout en bout dans le cadre du DES. Quelles seraient les conséquences ainsi que les avantages et les inconvénients d'un tel chiffrement notamment au regard du modèle de consentement présumé (opt-out) ?

Contexte

Le dossier électronique de santé (DES) sera l'outil central qui, en Suisse, garantira à la population de disposer d'un accès numérique à ses informations de santé. Il s'agit d'un lieu permettant de stocker les informations pertinentes à long terme pour le traitement afin que les titulaires d'un DES puissent en disposer. Ce dernier contient notamment les informations devant être disponibles indépendamment des différents acteurs ou établissements, ou celles dont on ne sait pas encore au moment de leur mise à disposition qui en aura besoin par la suite.

Parallèlement, le DES fera partie intégrante du futur Espace suisse des données de santé (Swiss Health Data Space ; SwissHDS). Dans cet espace, les professionnels de la santé comme les établissements de santé pourront échanger des données de manière structurée et standardisée (*business-to-business*, B2B), notamment des transferts, des demandes ou des résultats de laboratoire. Alors que la finalité de la communication B2B dans l'espace SwissHDS est le transfert automatisé de données, l'efficience des processus automatisés et l'intégration directe des systèmes, le DES vise la transparence, la souveraineté de ses titulaires et la continuité globale de la prise en charge.

Du fait du caractère particulièrement sensible des données de santé, le Conseil fédéral a visé, dès l'élaboration de la loi fédérale sur le dossier électronique de santé (LDSan), des exigences de protection des données et de sécurité de l'information très élevées, que le DES devra impérativement respecter. Un niveau de protection élevé est déterminant pour la confiance et l'acceptabilité aussi bien de la population que des professionnels de la santé et, par conséquent, d'importance centrale pour le succès du DES. Il sera atteint par l'interaction cohérente de mesures techniques, organisationnelles et juridiques, parmi lesquelles on peut citer des procédures d'identification robustes (processus de vérification de l'identité), des règles d'accès claires et un journal d'accès infalsifiable. Tel qu'il est prévu, ce concept d'architecture de sécurité moderne et résilient correspond à l'état actuel de la technique et sera développé en continu en collaboration avec l'Office fédéral de la cybersécurité (OFCS) et d'autres unités internes et externes afin de garantir à tout moment ce niveau de protection élevé. L'architecture sera conçue selon les principes « zero trust » (confiance zéro), « security by design » (sécurité dès la conception) et « security by default » (sécurité par défaut) et répondra aux exigences strictes de la loi fédérale sur la sécurité de l'information (LSI ; RS *128*) et de la loi sur la protection des données (LPD ; RS *235.1*). Les données du DES seront stockées selon le droit suisse et exclusivement en Suisse. Une analyse devra également établir si l'infrastructure de confiance de l'identité électronique (e-ID) et le Swiss Government Cloud pourront être utilisés à cette fin. Par conséquent, il est prévu que le DES bénéficie d'une architecture de sécurité à plusieurs niveaux, avec des contrôles d'accès clairs ; le chiffrement continu des données, qui correspond à l'état actuel de la technique et qui est déjà utilisé pour le dossier électronique du patient (DEP), sera conservé pour le futur DES.

Dans le même temps, les exigences en matière de protection des données et de sécurité de l'information ne peuvent pas être traitées indépendamment des autres exigences. Elles sont prises

dans un conflit d'objectifs structurel avec d'autres dimensions qu'il est possible de décrire comme un point d'équilibre à trouver entre les coûts, la sécurité, la convivialité d'utilisation et la souveraineté numérique. Ainsi, toute hausse du niveau de sécurité grâce, par exemple, à un chiffrement plus complexe, se fait au détriment de la convivialité d'utilisation et engendre des coûts de développement et d'exploitation supplémentaires. Ces conflits d'objectifs doivent donc faire l'objet d'arbitrages rigoureux.

Il faut par ailleurs souligner que l'actuel DEP (tout comme le DES en projet) est un système secondaire. Les données de santé continueront d'être stockées de manière décentralisée là où elles ont été saisies à l'origine, c'est-à-dire dans les systèmes des professionnels de la santé ou des établissements de santé (systèmes d'information des cabinets médicaux ou des cliniques). Il leur incombe de gérer ces données de manière sûre et dans le respect de la protection des données. La sécurité des données de la totalité d'un système se mesure, en définitive, au degré de sécurité du plus faible maillon de la chaîne : lorsque des données sont enregistrées ou traitées à plusieurs endroits, un niveau de protection élevé du DES ne parviendra pas à compenser une sécurisation plus basse ailleurs, dans la mesure où les accès non autorisés et les fuites de données ont tendance à se déporter là où la résistance est la plus faible. Une architecture de sécurité efficace nécessite par conséquent un niveau égal de protection, tous lieux de traitement et de stockage confondus, dont la mise en œuvre relève de la responsabilité de chacun des établissements ou des acteurs compétents.

Chiffrement de bout en bout (E2EE)

Le chiffrement sert en premier lieu à protéger les informations, voire à empêcher des personnes non autorisées d'accéder à des contenus sensibles. Pour ce faire, un procédé mathématique rend les données illisibles. Ces dernières ne peuvent plus être reconverties sans la clé correspondante. Un tel chiffrement des données transmises et stockées est chose courante et un pilier essentiel d'une architecture de sécurité moderne : il constitue le fondement de la sécurité, de la souveraineté et de la confiance et, donc, bien plus qu'une option technique. Aujourd'hui, pratiquement toute consultation d'un site internet intervient de manière chiffrée. Dans le présent contexte, deux objectifs immédiats de protection de la sécurité de l'information revêtent une importance particulière : premièrement, la garantie de la confidentialité afin que les données de santé ne puissent être accessibles qu'aux seules personnes autorisées ; deuxièmement, la limitation des dommages potentiels causés par des cyberattaques afin que les données interceptées ou détournées de manière illégitime ne soient d'aucune utilité aux pirates, faute de disposer de la clé correspondante.

En fonction de l'entité qui possède la clé et du lieu où interviennent le chiffrement et le déchiffrement, on distingue différents types de cryptage, présentant chacun un niveau de protection et des prérequis en matière de confiance spécifiques. Le chiffrement de bout en bout (*end-to-end encryption, E2EE*) ne constitue qu'une des nombreuses déclinaisons possibles. Lui-même n'est pas un concept techniquement uniforme, répondant à une définition unique ; il s'agit plutôt d'un terme générique désignant une série de possibilités de mise en œuvre. Fondamentalement, il se caractérise par le fait que les clés cryptographiques se situent et sont conservées aux deux extrémités, c'est-à-dire entre les mains des personnes physiques ou plus précisément, sur les appareils qui leur sont attribués, les intermédiaires (notamment l'exploitante de l'infrastructure) n'ayant pas accès à une information lisible et compréhensible.

En soi, ce concept dévoile surtout ses atouts lorsque l'expéditeur et le destinataire sont identifiés avec certitude au préalable, c'est-à-dire en cas de communication ciblée. Typiquement, ses champs d'application sont donc les services de messagerie tels que WhatsApp, le cryptage des courriels ou la transmission sécurisée de données entre deux systèmes définis comme c'est notamment le cas pour l'e-ID. Dans les situations où il n'y a pas de cercle de destinataires prédéfini, le chiffrement E2EE n'est pas applicable, dans son principe, sans autres développements. Les groupes de discussion en ligne illustrent ce phénomène : pour des raisons techniques, les membres nouvellement ajoutés à la discussion n'ont pas accès aux messages échangés avant

leur arrivée dans la mesure où ces derniers ont été cryptés exclusivement pour les destinataires connus à ce moment-là.

Dans certains cas, le chiffrement E2EE peut présenter l'avantage d'atteindre un niveau de protection et de confiance plus élevé, s'agissant notamment des accès de personnes travaillant pour l'exploitante ou des fuites de données internes à celle-ci. En revanche, il a pour inconvénient de compliquer significativement, voire d'empêcher, les fonctions proposées par l'infrastructure telles que la détection des logiciels malveillants, la recherche plein texte ou les résultats automatisés, dans la mesure où le système lui-même ne peut pas lire ces données. Le chiffrement de bout en bout qualifié de E2EE peut complexifier les processus existants et les rendre fastidieux, car cette méthode requiert une gestion des clés très exigeante sur les terminaux. Ceci accroît sensiblement la complexité de l'implémentation, de la restauration et de l'utilisation sur plusieurs appareils par rapport à d'autres méthodes. Il en résulte des coûts supérieurs récurrents. Si l'on perd une clé (en égarant, par exemple, le smartphone sur lequel elle était enregistrée), toutes les données qu'elle a permis de chiffrer sont inaccessibles, à moins qu'une procédure de restauration de la clé n'existe. Toutefois, l'existence d'une procédure de ce type serait en contradiction avec le principe de strict chiffrement E2EE puisqu'elle présuppose qu'il existe une instance ayant accès à la clé ou à une copie de cette dernière. En matière de stockage de longue durée, la perte d'une clé peut, en l'absence d'une procédure permettant de la restaurer, être synonyme de perte définitive de l'ensemble des données archivées, un risque inacceptable dans de nombreux cas d'application.

Les comparaisons internationales le montrent, en effet, aussi : il n'existe aucun système de DES, qu'il soit public ou national, qui utilise un chiffrement E2EE strict pour les informations auxquelles différentes unités de traitement ont accès.

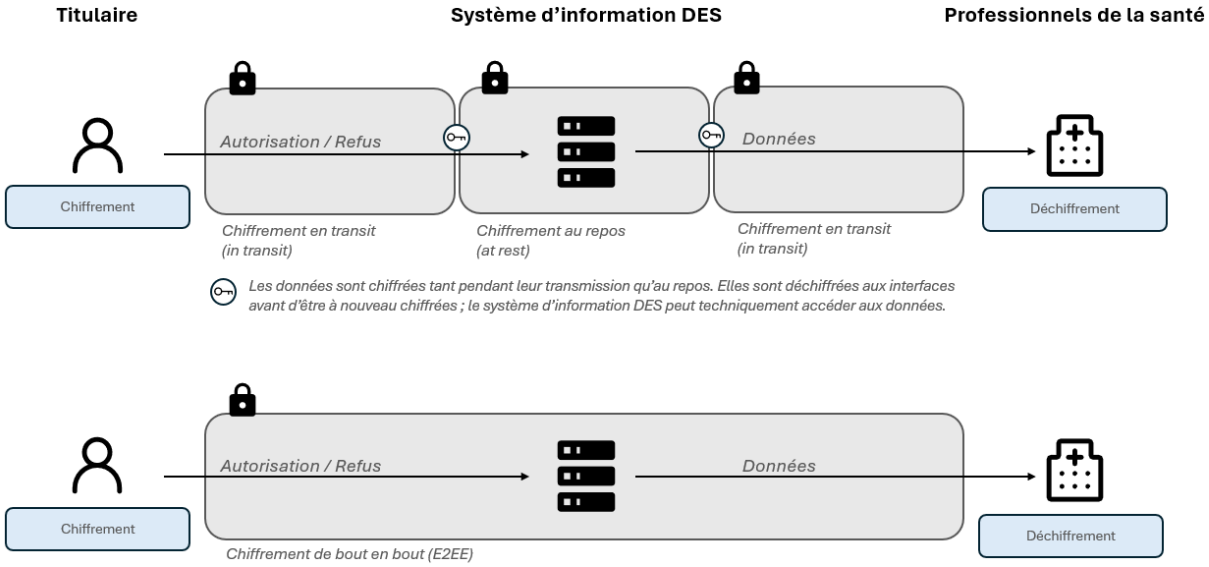
Dans le cas du DES, le principal défi réside dans le fait que les données ne sont pas simplement transmises mais stockées à long terme, souvent sans que l'on sache clairement au préalable qui y accédera plus tard. Il s'agit d'une différence notable par rapport aux applications comme WhatsApp ou le courrier électronique. Par ailleurs, le chiffrement E2EE remet en question des fonctions essentielles comme l'accès d'urgence ou l'ouverture automatique du DES, car chaque titulaire devrait, pour ce faire, générer une clé cryptographique pour son DES. Finalement, dans le contexte du DES, le chiffrement E2EE implique des exigences nettement supérieures s'agissant des compétences numériques des titulaires (mots clés : inclusion numérique et accessibilité) ainsi que des professionnels de la santé, qui sont déjà fortement sollicités par des tâches administratives croissantes.

Résultats de l'analyse externe de l'EPF Lausanne

Dans le cadre d'un partenariat avec l'OFSP, le Center for Digital Trust (C4DT) de l'EPFL a élaboré quatre variantes d'architectures de sécurité possibles pour le futur dossier électronique de santé (cf. annexe). Le temps disponible pour ce faire était compté au vu de la très haute complexité technique et organisationnelle de la matière, de sorte que les travaux se sont concentrés sur des concepts généraux, accompagnés d'analyse de faisabilité. Le développement d'architectures de sécurité détaillées a été abandonné, et l'analyse s'est attachée à évaluer les effets des différentes variantes sur les éléments centraux du système au niveau fonctionnel et réglementaire, à savoir la convivialité d'utilisation, la gestion des clés, la complexité du système (= coûts) et la capacité d'évolution à long terme.

La variante I esquisse une solution principalement organisationnelle, dans laquelle les données seraient effectivement chiffrées selon l'état actuel de la technique, l'exploitante du DES aurait un accès purement technique aux données et la protection serait, par conséquent, assurée notamment par des mesures organisationnelles, la conformité au droit et la confiance envers l'exploitante. La variante II est techniquement plus complexe. Elle consiste en un modèle hybride qui utilise la technologie du *confidential computing*[1] et dans le cadre duquel les clés sont stockées dans un espace de confiance. Les variantes III et IV décrivent des modèles basés sur un chiffrement E2EE strict reposant sur une gestion des clés soit assumée par les titulaires eux-mêmes soit distribuée de manière entièrement décentralisée entre des instances de confiance.

Figure : différences entre la variante I (en haut) et l'E2EE (en bas)



Source : d'après l'analyse « Data Security in the Swiss Electronic Health Records (E-GD): Four possible architectures » ; Imad Aad, Linus Gasser, JP Hubaux Center for Digital Trust (C4DT), EPFL ; juillet 2026

[1] Le *confidential computing* est un concept de sécurité qui protège les données non seulement lors de leur transmission, mais également durant leur traitement. Il utilise des environnements d'exécution de confiance sécurisé par le matériel (*trusted execution environments, TEEs*) permettant d'isoler le traitement des données du reste du système.
Ceci permet d'éviter que les exploitants d'une infrastructure, les administrateurs de cette dernière ou des logiciels malveillants ne puissent accéder aux données sensibles pendant leur traitement. Contrairement au chiffrement E2EE, il est ainsi possible de procéder au traitement de données protégées en apportant tout de même de fortes garanties en matière de protection des données. Cette approche est souvent utilisée pour la sécurisation du *cloud computing*, pour les données de santé ou dans le secteur financier.

Tableau : aperçu des variantes

	Description	**Confiance cryptographique**	**Niveau de maturité technologique**[2]	**Inconvénients majeurs**
I	Chiffrement continu et protection d'ordre organisationnel	basse	productif (très élevé, 9)	tributaire de mesures de sécurité organisationnelles
II	Chiffrement faisant appel au *confidential computing*	moyenne	capacité fonctionnelle attestée (élevé, 8)	Fortes complexité et dépendances : sur le marché, rares sont les composantes matériel répondant aux exigences.
III	Chiffrement et gestion des clés par les utilisateurs	moyenne	prototype (moyenne, 6-7)	L'entière responsabilité de l'infrastructure comme de la restauration de la clé incombe aux seuls utilisateurs, en l'absence de toute garantie institutionnelle.
IV	Gestion des clés entièrement décentralisée	forte	structure expérimentale (rudimentaire, 4-5)	Absence de standardisation ; seules des réalisations expérimentales, n'ayant pas encore atteint la phase productive, sont connues.

Source : analyse « Data Security in the Swiss Electronic Health Records (E-GD): Four possible architectures » ; Imad Aad, Linus Gasser, JP Hubaux Center for Digital Trust (C4DT), EPFL ; juillet 2026

Ces résultats indiquent tout d'abord que les variantes ne correspondent pas toutes à la définition *stricto sensu* de l'E2EE évoquée ci-avant et que l'E2EE se décline également en différentes configurations techniques. Selon l'architecture choisie, les effets sur la sécurité, l'exploitation et la réglementation divergent considérablement, raison pour laquelle une évaluation globale de la méthode de chiffrement en tant que telle ne semble pas appropriée. Une augmentation du niveau de protection des différentes architectures sur le plan technique va entraîner une progression du degré de sécurité des données atteint, mais également une hausse au niveau de la complexité de la mise en œuvre et des coûts. Dans le même temps, la convivialité d'utilisation et le niveau de maturité des technologies requises diminuent.

Appréciation et conclusion intermédiaire

L'analyse montre clairement qu'une administration des clés par les seuls titulaires (variantes III et IV) pose des défis techniques qui n'ont pas pu être résolus de manière satisfaisante jusqu'à présent, notamment au vu des exigences correspondantes en lien avec l'ouverture automatique, la restauration des clés, l'accès d'urgence et les fonctions essentielles. La convivialité d'utilisation et l'accès à bas seuil ne seraient pas garantis par cette mise en œuvre. Le rapport de l'EPFL souligne par ailleurs que ces solutions, dans la mesure où elles n'ont pas encore été assez testées, standardisées et qu'elles n'ont pas fait leurs preuves à grande échelle, dans des environnements réels, ne présentent actuellement qu'une maturité technique moyenne à basse, soit insuffisante pour une infrastructure critique qui sera déployée sur l'ensemble du territoire Suisse. En particulier, ces variantes ne proposent aucune solution aboutie, même au niveau international, pour la mise en œuvre du modèle opt-out.

A contrario, le recours à une architecture hybride (variante II) intégrant le *confidential computing* et un espace de confiance semble possible à certaines conditions. Cependant, au sens strictement technique de la définition du terme, cette solution ne constitue pas un chiffrement E2EE, bien

[2] Selon l'échelle *Technology Readiness Level (TRL)* : www.sbfi.admin.ch > Recherche et innovation ; consulté le 10 juillet 2026

qu'elle puisse atteindre un niveau de protection équivalent ou semblable sur le plan fonctionnel. Toutefois, dans cette variante aussi, la conception architecturale concrète s'avère ambitieuse.

La présente analyse de l'EPFL fournit une première appréciation globale et comporte encore des imprécisions concernant les évaluations de la fonctionnalité, de la sécurité d'exploitation et de l'évolutivité. De nouvelles clarifications approfondies sont indispensables pour notamment établir si les fonctionnalités et la convivialité d'utilisation peuvent être assurées par la mise en œuvre de la variante II. Cette dernière nécessite, pour une part, des composants matériels spécifiques, notamment pour l'espace de données de confiance, ce qui est susceptible de créer des dépendances vis-à-vis de certains fabricants et d'entraîner une augmentation significative des coûts pour le développement comme pour l'exploitation courante. Pour décider de la variante applicable, il faut par ailleurs mettre cette question en perspective avec des interrogations générales, dont celle de l'interaction avec le SwissHDS.

Il est essentiel de reconsidérer la vue d'ensemble : dès que les données quittent le domaine de responsabilités du système DES, elles sont soumises à la structure technique et organisationnelle de chacun des systèmes primaires où, selon les circonstances, elles sont ensuite traitées de manière non chiffrée. Sur le plan technique, le DES doit être intégré de manière fluide à l'Espace des données de santé SwissHDS. Cette exigence vaut également pour le chiffrement. Si le DES utilise un chiffrement E2EE qui ne peut pas être déployé à l'échelle de l'ensemble de l'espace de données, les professionnels de la santé comme les établissements de santé ne pourront pas utiliser les données du DES. Il est également à craindre que les données de santé ne soient pas archivées dans le DES si leur mise à disposition dans le dossier en question est perçue comme trop complexe ou fastidieuse en raison du chiffrement E2EE. Les patients continueraient alors, comme c'est le cas aujourd'hui, d'envoyer aux professionnels de la santé des informations médicales, par courriel et sans chiffrement. Pour cette part du traitement des données, seules s'appliquent les dispositions générales des lois sur la protection des données de la Confédération et des cantons (pour ce qui est des établissements cantonaux).

Les résultats disponibles ont également été discutés avec l'OFCS. Celui-ci indique à ce sujet que les modèles d'architecture décrits s'attachent en particulier à protéger les données d'un accès de l'exploitante de l'infrastructure DES. Cette protection ne s'étend toutefois qu'à l'intérieur du DES. D'autres points d'attaque, comme une importante fuite de données due, par exemple, à une violation par une partie autorisée, ne sont, selon l'OFCS, pas suffisamment pris en compte alors qu'il s'agit probablement du plus grand risque pour le DES. Cet aspect devrait être davantage considéré lors du développement des variantes.

Suite de la procédure et recommandations d'action

Élaboration de l'architecture de sécurité

Dans le cadre des travaux en cours sur l'architecture de sécurité, l'analyse de l'EPFL propose des repères supplémentaires. L'OFSP recommande, en toute logique, d'approfondir ces aspects et de les intégrer dans le concept détaillé. Dans le cadre de ces travaux, il convient d'analyser de manière plus poussée des questions telles que la procédure d'opposition, l'accès d'urgence, le règlement des représentations ou les fonctions de recherche et de filtrage, d'en prévoir l'élaboration pour une utilisation à grande échelle et, le cas échéant, de les tester au cas par cas. Des thématiques telles que l'accessibilité et l'inclusion numérique seront également traitées dans ce contexte. La conception de l'architecture de sécurité du DES doit, par conséquent, trouver un juste équilibre entre sécurité, convivialité d'utilisation, coûts et souveraineté numérique. La prise en compte disproportionnée d'un de ces objectifs au détriment des autres ne favoriserait ni l'aspect pratique ni l'acceptance du système. Par ailleurs, en plus d'un haut niveau de maturité, il convient également de laisser la porte ouverte à de futures évolutions : l'architecture du système doit éviter toute dépendance vis-à-vis de certains fournisseurs ou de technologies spécifiques. L'intégration d'évolutions futures, comme de nouvelles normes d'interopérabilité, des applications basées sur l'IA ou des exigences de sécurité revues en lien avec les évolutions dans le domaine des

ordinateurs quantiques, doit rester possible à tout moment. Enfin, il faut également s'assurer qu'un concept cryptographique détaillé soit aussi compatible avec le SwissHDS.

Considérations législatives

Un chiffrement des données tout au long de la chaîne de traitement correspond à l'état actuel de la technique et est également envisagé pour le DES. Le présent projet de LDSan offre, par conséquent, une base légale suffisante pour le chiffrement des données traitées[3]. Celle-ci est par ailleurs complétée par les dispositions pertinentes d'autres actes législatifs applicables, notamment celles de la LSI et de la LPD, qui fixent, pour leur part, des exigences en matière de confidentialité, d'intégrité et de disponibilité des données traitées.

À la lueur du rapport de l'EPFL, il n'apparaît pas non plus adéquat de fixer à l'échelon de la loi une procédure cryptographique concrète ou une architecture de sécurité précise pour le DES, comme le chiffrement E2EE sous une forme spécifique. Le Conseil fédéral a délibérément fait le choix d'une réglementation neutre du point de vue de la technologie, fidèle au principe selon lequel la loi définit de manière contraignante le « quoi », c'est-à-dire le niveau de protection à atteindre, alors que la mise en œuvre technique concrète (le « comment ») est réglée dans le droit d'exécution ainsi qu'à l'échelon de l'exécution, par exemple dans le cadre de prescriptions techniques destinées aux normes à mettre à jour. Lors de l'élaboration du droit d'exécution, les cercles intéressés sont associés à divers comités et peuvent également faire valoir leur point de vue dans le cadre de la consultation. Le projet de l'ordonnance concernée est par ailleurs naturellement soumis aux commissions compétentes, qui en font la demande.

Cette approche est ancrée dans l'ordre juridique suisse, précisément dans le domaine de la sécurité de l'information et de la protection des données. La plupart du temps, il est fait référence à des notions qu'il convient de préciser au cas par cas, tels que « état de la technique » ou « mesures organisationnelles et techniques appropriées » afin de concilier, d'une part, la sécurité juridique liée au niveau de protection visé et, d'autre part, la souplesse technique requise. Ainsi, le droit fédéral ne contient à ce jour aucune disposition, au niveau législatif, concernant des technologies de chiffrement spécifiques. Ce point est également corroboré par les législations actuelles qui abordent des questions de chiffrement : tant la loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques (LeID) que la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ ; RS *172.023*) renoncent à prescrire des normes ou procédures cryptographiques spécifiques, se limitant, au contraire, à formuler des objectifs de protection neutres du point de vue de la technologie, dont la mise en œuvre et la garantie seront transposées à l'échelon de l'ordonnance ou de l'exécution.

Si la protection cryptographique était explicitement inscrite dans la loi au titre d'exigence générale, l'OFSP propose une formulation neutre du point de vue de la technologie, qui ne préjuge pas de la conception concrète retenue pour le DES :

Ajout à l'art. 5, al. 7

La Confédération est responsable de la protection et de la sécurité des données du système d'information DES, **notamment par chiffrement**. Elle conserve ces données en Suisse conformément au droit suisse.

Il est ainsi possible de préciser et de définir, en étroite concertation avec les services spécialisés de la Confédération et les experts en sécurité externes, si le chiffrement E2EE doit être utilisé, et si oui, sous quelle variante. Ceci permet de garantir que l'implémentation concrète suivra le rythme des évolutions techniques et pourra être adaptée avec souplesse aux futures solutions développées.

---

3 L'art. 5, al. 7, inclut l'obligation de garantir un niveau de protection approprié lors du traitement des données personnelles sensibles, en particulier, sans prescrire de procédure technique précise ; l'art. 7 concrétise cette obligation de protection en lien avec la sécurité des données, laissant suffisamment de champ libre pour une architecture de chiffrement continu.