Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Services de coffre-fort numérique

Cahier des charges pour la certification

Version 1.0 du XX XXXXXX XXXX

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
14/10/2016	0.1	*Version de travail pour commentaires*	ANSSI
28/11/2016	0.2	*Version consolidée à partir des commentaires reçus (ANSSI et DGE)*	ANSSI
19/12/2016	0.3	*Version finalisée à partir des commentaires reçus sur la version 2.0*	ANSSI
02/07/2018	0.4	*Version modifiée à partir des commentaires reçus sur la version 3.0 (consultations externes)*	ANSSI
31/10/2018	0.5	*Version modifiée à partir des commentaires reçus sur la version 4.0*	ANSSI
21/08/2019	0.6	*Version finalisée avec la prise en compte des commentaires*	ANSSI
02/10/2019	0.7	*Version finalisée avec les commentaires de BQA*	ANSSI
06/01/2020	0.8	*Version finalisée avec des corrections mineures*	ANSSI
16/06/2020	0.9	*Version finalisée avec des corrections mineures*	ANSSI
09/02/2021	1.0	*Version publiée*	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

SOMMAIRE

I. Introduction

I.1. Objet

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, modifiée par l'ordonnance n° 2017-1426 du 4 octobre 2017, complète le code des postes et des communications électroniques par un article L. 103, en définissant un service de « coffre-fort numérique ».

L'ANSSI, désignée comme autorité nationale de la sécurité des systèmes d'information par le décret n° 2009-834 du 7 juillet 2009, a la charge de certifier des services de coffre-fort numérique selon un cahier des charges approuvé par arrêté du ministre chargé du numérique après avis de la Commission nationale de l'informatique et des libertés.

Le présent document constitue ce cahier des charges.

I.2. Cadre juridique

Les services de coffre-fort numérique certifiés conformément au présent cahier des charges bénéficient d'une présomption de conformité aux obligations définies aux 1° à 5° de l'article L. 103 du code des postes et des communications électroniques.

I.3. Mise à jour

L'opportunité de la mise à jour de ce document est évaluée par l'ANSSI et peut être le fait d'une évolution du cadre réglementaire ou normatif lié au service de coffre-fort numérique ou d'une modification du processus de certification.

Chaque mise à jour est soumise à l'avis de la Commission nationale de l'informatique et des libertés, et fait l'objet d'une approbation par arrêté du ministre chargé du numérique.

L'ANSSI précise les modalités de transition et date d'effet pour chaque mise à jour.

I.4. Acronymes

Les acronymes utilisés dans le présent document sont les suivants :

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
PASSI	Prestataire d'Audit de la Sécurité des Systèmes d'Information
RGS	Référentiel Général de Sécurité

II. Exigences relatives aux services de coffre-fort numérique

II.1. Définition du service de coffre-fort numérique

L'article L. 103 du code des postes et des communications électroniques définit le service de coffre-fort numérique comme un service ayant pour objet :

- « *la réception, le stockage, la suppression et la transmission de données ou documents électroniques dans des conditions permettant de justifier de leur intégrité et de l'exactitude de leur origine* ; »
- « *la traçabilité des opérations réalisées sur ces documents ou données et la disponibilité de cette traçabilité pour l'utilisateur* ; »
- « *l'identification de l'utilisateur lors de l'accès au service par un moyen d'identification électronique respectant l'article L. 102* [du code des postes et des communications électroniques] ; »
- « *de garantir l'accès exclusif aux documents électroniques, données de l'utilisateur ou données associées au fonctionnement du service à cet utilisateur, aux tiers autres que le prestataire de service de coffre-fort numérique, explicitement autorisés par l'utilisateur à accéder à ces documents et données et, le cas échéant, au prestataire de service de coffre-fort numérique réalisant un traitement de ces documents ou données au seul bénéfice de l'utilisateur et après avoir recueilli son accord exprès dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* ; »
- « *de donner la possibilité à l'utilisateur de récupérer les documents et les données stockées dans un standard ouvert aisément réutilisable et exploitable par un système de traitement automatisé de données, sauf dans le cas des documents initialement déposés dans un format non ouvert ou non aisément réutilisable qui peuvent être restitués dans leur format d'origine, dans des conditions définies par décret.* »

II.2. Exigences spécifiques aux fonctions du coffre-fort numérique

II.2.1. Disponibilité, pérennité et intégrité et exactitude de l'origine des données et documents reçus, stockés, supprimés ou transmis

Le service de coffre-fort numérique garantit l'intégrité, la disponibilité du service de coffre-fort numérique ainsi que la pérennité des données.

Par exemple :

- *l'intégrité des communications peut être mise en œuvre par l'utilisation de mécanisme de calculs d'empreintes conformes aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques spécifiées dans l'annexe [RGS_B1] ;*
- *la disponibilité du service peut être assurée par la mise en œuvre de mécanismes de redondances des équipements ou de répartition de charge ;*
- *la pérennité des données peut être assurée par la définition et la mise en œuvre d'une politique de sauvegarde.*

La Perte de données maximale admissible (PDMA)[1] ne peut dépasser quatre heures. Le prestataire doit expliciter dans ses plans de continuité d'activité et de reprise d'activité les mesures permettant d'atteindre cet objectif. En cas de pertes de données, le fournisseur doit notifier les utilisateurs de son service de l'incident.

Le fournisseur s'engage également sur la disponibilité du service ; ainsi :

- la durée maximale d'indisponibilité en cas de panne ou de maintenance du service ne peut excéder deux heures consécutives ;
- la durée maximale totale d'indisponibilité par mois du service ne peut excéder huit heures.

Il est recommandé que le composant sur lequel s'appuie le service de coffre-fort numérique respecte les spécifications fonctionnelles définies dans la norme [NF Z42-020]. À défaut, ce composant doit justifier d'une couverture fonctionnelle équivalente.

Par exemple, les données permettant d'identifier l'utilisateur doivent être transmises à chaque opération.

II.2.2. Traçabilité des opérations

Le service de coffre-fort numérique intègre des fonctions de traçabilité permettant aux utilisateurs de consulter l'activité récente sur leur coffre-fort (*par exemple en journalisant et en horodatant les réussites et échecs de connexion, l'adresse IP et le protocole utilisé, ainsi que les opérations effectuées sur les répertoires et les fichiers, l'utilisateur ayant effectué une opération, l'objet sur lequel une opération est effectuée et la nature de l'opération effectuée*).

Le composant sur lequel s'appuie le service de coffre-fort numérique est réputé satisfaire à cette obligation lorsqu'il respecte les exigences définies au chapitre 5.5 de la norme [NF Z42-020].

L'ensemble des actions liées aux fonctions d'administration et d'exploitation de l'infrastructure supportant le service de coffre-fort numérique doivent également être journalisées.

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Pour dater ces évènements, il est possible de recourir :

- soit à un service d'horodatage électronique tel que prévu par le règlement [eIDAS], interne ou externe ;
- soit à l'heure du système et en assurant une synchronisation des horloges des systèmes entre elles, au minimum à la seconde près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Pour les opérations faites hors ligne, cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les évènements avec une précision suffisante. Pour la synchronisation par rapport au temps UTC, il est recommandé de se référer à un système comprenant au moins deux sources indépendantes de temps.

[1] La PDMA (ou *Recovery point objective* (RPO)) est le point à partir duquel les informations utilisées par le service de coffre-fort doivent être restaurées afin de permettre son fonctionnement à la reprise (ISO/CEI 22300:2018).

II.2.3. Identification et authentification de l'utilisateur

Le fournisseur doit collecter, dans le cadre de la création d'un compte, l'ensemble des données nécessaires pour garantir l'identification univoque de l'utilisateur (*en particulier, les données collectées doivent permettre de distinguer les homonymes*).

Cette collecte doit cependant rester proportionnée au regard de la finalité. Conformément à l'article 30 de la loi du 6 janvier 1978 modifiée, l'identification du détenteur du coffre ne peut, en aucun cas, être réalisée au moyen du numéro de sécurité sociale (RNIPP).

Les données sont conservées pour une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

a) Règles applicables aux mécanismes d'identification et d'authentification

L'identification de l'utilisateur lors de l'accès au service de coffre-fort numérique doit être assurée par un moyen d'identification électronique[2] répondant aux exigences retenues dans le [REFERENTIEL eID] pour le niveau de garantie « substantiel ».

L'emploi : *- d'un moyen d'identification électronique répondant aux exigences du niveau « élevé » du règlement [eIDAS] et certifié conformément aux dispositions de l'article L. 102-III du code des postes et des communications électroniques ; ou bien* *- d'un moyen d'identification électronique répondant aux exigences du niveau « substantiel » du règlement [eIDAS] et certifié conformément aux dispositions de l'article L. 102-IV du code des postes et des communications électroniques ;* *- d'un moyen d'identification électronique notifié et répondant aux exigences du niveau « substantiel » ou « élevé » prévu par le règlement [eIDAS] ; ou bien* *- d'un certificat d'authentification de personne qualifié au niveau RGS ** ou *** ;* *permet d'apporter une présomption de conformité à cette exigence.*

Le prestataire peut mettre en œuvre lui-même l'identification d'un utilisateur en fournissant son propre moyen d'identification électronique ou en déléguant cette tâche à un service externe. Dans le cas d'une identification déportée (*par exemple, sur un serveur de fédération d'identités)*, le prestataire devra s'assurer du respect par le service externe :

- des règles associées à l'identification et l'authentification d'un utilisateur précédemment décrites ;
- de l'utilisation d'un standard permettant de sécuriser la communication de la preuve d'authentification *(par exemple SAMLv2, ou OAuth2 (complété éventuellement par OpenID Connect (OIDC)))* ;
- de l'implémentation de mesures de sécurité à même de prévenir toute tentative d'usurpation d'identité, par exemple par une attaque du type « homme du milieu » en provenance du système d'information où est hébergé le service.

[2] Ce moyen d'identification électronique sert également à l'authentification de l'utilisateur.

Si l'authentification comprend l'utilisation de mots de passe, ces règles font l'objet d'une information des utilisateurs (*par exemple, affichage du niveau de sécurité du mot de passe choisi*) et d'un contrôle de bonne application.

b) Règles applicables à l'accès au coffre-fort numérique par des tiers autorisés

Les règles applicables à l'identification et l'authentification de l'utilisateur décrites au paragraphe II.2.3.a ci-dessus s'appliquent à l'ensemble des tiers autorisés à accéder au coffre-fort, incluant notamment :

- les personnes physiques ou morales spécialement autorisées par l'utilisateur ;
- les tiers auxquels les utilisateurs ont recours pour importer des données depuis un espace de dépôt vers le coffre ;
- le cas échéant, les personnels du fournisseur de service de coffre-fort numérique réalisant un traitement au seul bénéfice de l'utilisateur avec l'accord exprès de celui-ci ;
- ainsi que les administrateurs en charge des opérations techniques de gestion du coffre.

Le service de coffre-fort numérique intègre des outils (*par exemple, verrouillage du compte, refus de connexion depuis l'adresse malveillante*) permettant de bloquer les tentatives de connexions illégitimes.

II.2.4. Confidentialité des documents et données de l'utilisateur

Le service de coffre-fort numérique ne permet la consultation des documents dématérialisés stockés que par l'utilisateur concerné, et le cas échéant, par les tiers spécialement autorisés par ce dernier dans les conditions prévues par l'article L. 103 du code des postes et des communications électroniques. Le choix doit-être donné à l'utilisateur d'autoriser la consultation de tout ou partie des documents stockés à ces tiers.

Des mesures de sécurité doivent être mises en place pour garantir la confidentialité des documents et données stockés, ainsi que des métadonnées suivantes :

- Nom des répertoires et leurs dates de création ou de modification :
- Nom des fichiers et leurs dates de création ou de modification ;
- Identité des personnes accédant au coffre-fort numérique ;
- Type de fichier et taille du fichier

Le service de coffre-fort numérique doit assurer le chiffrement de l'ensemble des éléments stockés. En complément, le service de coffre-fort numérique doit assurer le chiffrement des transmissions vers ou depuis celui-ci.

Les mécanismes impliqués dans le chiffrement doivent être conformes aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques spécifiées dans l'annexe [RGS_B1], et doivent permettre une évolution de la taille des clés et des algorithmes utilisés.

L'utilisateur et l'ensemble des tiers autorisés doivent être en capacité de déchiffrer et visualiser les documents, données et métadonnées stockées dans le coffre-fort numérique, sauf pour les tiers disposant uniquement du droit de dépôt dans le coffre-fort de l'utilisateur.

Dans le cas où un tiers, non expressément autorisé par l'utilisateur, aurait accédé aux données et documents stockés dans le coffre-fort numérique, le fournisseur en notifie l'utilisateur en précisant les causes de cet accès (*par exemple, intrusion par un pirate informatique, ou accès par un personnel du prestataire en application d'une décision de justice, etc…*), ainsi que les données dont il est présumé ou confirmé qu'elles ont été divulguées.

Le service de coffre-fort numérique efface les documents et les métadonnées supprimés définitivement par l'utilisateur de tous les endroits où ils sont stockés :

- sans délai pour les espaces de stockage courants et les éventuelles copies répliquées en ligne (synchronisées en temps réel ou en miroir) ;
- dans un délai maximum d'un mois pour les sauvegardes (incrémentales, complètes… réalisées à fréquence donnée).

Toutefois cette obligation ne concerne pas les journaux de preuve produits par le service de coffre-fort numérique pour garantir les opérations réalisées ou pour répondre à une procédure judiciaire.

De plus, il est possible de conserver brièvement un document qu'un utilisateur souhaite supprimer, notamment afin de détecter une éventuelle anomalie quant à l'utilisation de son espace personnel, ou de lui permettre de revenir sur sa décision en cas de mauvaise manipulation.

Le service de coffre-fort numérique prévoit des mécanismes de révocation et de renouvellement des secrets cryptographiques en cas de perte par l'utilisateur, de suspicion d'accès non autorisé à ses documents et données ou de mise à l'état de l'art des mécanismes cryptographiques (*par exemple, augmentation des tailles de clé ou modification des algorithmes*). En particulier, lorsque les secrets cryptographiques sont détenus par le seul utilisateur, le service de coffre-fort numérique prévoit des mécanismes de copie de sauvegarde de ces secrets. Dans le cadre de son devoir de conseil, le fournisseur de service de coffre-fort numérique recommande à l'utilisateur de confier la copie de sauvegarde de ces secrets à un tiers de confiance (*par exemple, un proche, un cabinet d'avocat voir à un ou une notaire*).

II.2.5. Récupération des documents et données stockés

Le service de coffre-fort numérique doit permettre à l'utilisateur de récupérer, sans surcoût, les documents et les données qui y sont stockés conformément à l'article D. 537 et suivants du code des postes et des communications électroniques.

Le fournisseur de service de coffre-fort numérique doit rendre disponible les interfaces permettant d'assurer l'interopérabilité. Ces interfaces doivent être documentées de façon ouverte et gratuite. Lorsque le composant « coffre-fort numérique » respecte les spécifications fonctionnelles définies dans la norme [NF Z42-020], le fournisseur de service de coffre-fort numérique est réputé satisfaire à cette obligation.

II.3. Exigences générales

II.3.1. Considérations légales

Le fournisseur met en place une démarche visant à s'assurer de la conformité à la réglementation relative aux données à caractère personnel ([RGPD][LIL]) de l'ensemble des traitements mis en œuvre par le service de coffre-fort numérique. En particulier, le fournisseur recueille le consentement de l'utilisateur préalablement aux traitements des documents ou données déposés sur le service de coffre-fort numérique par ce dernier et réalisés à son seul bénéfice.

De plus, le fournisseur de service de coffre-fort numérique respecte les recommandations de la délibération n° 2013-270 du 19 septembre 2013 portant recommandation relative aux services de coffre-fort numérique, reprises dans le présent cahier des charges comme indiqué dans l'annexe 2.

De manière générale, le fournisseur doit s'assurer de la conformité aux exigences réglementaires spécifiques à la nature des services qu'il propose. En particulier, le fournisseur devra détenir un certificat d'hébergeur de données de santé valide s'il est amené à héberger de telles données.

II.3.2. Information préalable à l'utilisation du service

Le fournisseur de service de coffre-fort numérique informe au préalable les utilisateurs, au moins à travers la publication de conditions générales d'utilisation faisant l'objet d'une acceptation explicite :

- de l'identité de l'opérateur du service de coffre-fort numérique et de celle du fournisseur du service, le cas échéant ;
- de la finalité poursuivie par les traitements auxquels les données sont destinées ;
- des obligations et responsabilités des différentes parties ;
- des garanties en termes d'indemnisation et limites de garanties du service (en particulier, la perte maximale de données admissible et la durée maximale d'interruption admissible) ;
- des éventuels destinataires des données conservées, incluant les documents stockés et leurs métadonnées ;
- de tout transfert de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne, en indiquant si cet État, sur la base de sa propre législation, pourrait effectuer des demandes visant à accéder directement aux données conservées ;
- des droits d'accès, de rectification et d'opposition des utilisateurs ainsi que des modalités d'exercice de leurs droits ;
- de la possibilité de mandater des personnes (par exemple pour permettre à l'utilisateur de récupérer ses données en cas de perte de sa clef, ou à ses ayants droits en cas de décès) ;
- du type d'espace mis à leur disposition et de ses conditions d'utilisation. En particulier, le fournisseur informe l'utilisateur de l'interdiction de stocker des contenus illicites ainsi que, le cas échéant, de l'interdiction de stocker les données relatives à la santé (si le fournisseur ne remplit pas les conditions légales) ;
- des mécanismes techniques utilisés, notamment les mécanismes de chiffrement ;
- des modalités de résiliation du service ;
- des modalités de révocation, de renouvellement ou de copie des secrets d'authentification ;
- des modalités de récupération à tout moment des données stockées dans un format électronique ouvert (sauf dans le cas des documents initialement déposés dans un format non ouvert qui peuvent être restitués dans leur format d'origine) ;
- de la durée de conservation des dossiers d'enregistrement des journaux d'événements ;
- des procédures pour la résolution des réclamations et des litiges ;
- de la loi applicable au contrat ;
- de la politique de confidentialité ;
- de la définition des directives relatives au sort des données après la mort de l'utilisateur ;
- de la durée de conservation des données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée ;
- en cas d'offre de service associé de récupération de documents auprès de services tiers, des conséquences de l'utilisation par le fournisseur de service de coffre-fort numérique des identifiants et mots de passe des utilisateurs pour se connecter en son nom à ces services tiers ;
- des éventuels agréments ou certifications dont le fournisseur dispose en matière de stockage et d'archivage de données.

De plus, le fournisseur de service de coffre-fort numérique ne doit pas inciter les utilisateurs à leur confier leurs identifiants et mot de passe permettant d'accéder au service de coffre-fort numérique sans les avoir préalablement informés quant aux conséquences de cette collecte.

Enfin, le fournisseur de service de coffre-fort numérique doit faire figurer, de façon lisible, sur l'ensemble des pages du service, une mention rappelant aux utilisateurs, au minimum, les informations relatives à la localisation des données et au droit applicable en cas de litige.

Par exemple : « Les données que vous stockez sur ce coffre-fort numérique sont hébergées sur nos serveurs en Irlande et le droit applicable en cas de litige est le droit irlandais. »

II.3.3. Garanties pour l'indemnisation de l'utilisateur

Le fournisseur de service de coffre-fort numérique s'assure des garanties en termes d'indemnisation de l'utilisateur en cas de défaillance du service de coffre-fort numérique à remplir les exigences du présent cahier des charges (*par exemple en souscrivant à une assurance dans le but de couvrir les dommages imputables à des manquements au présent cahier des charges ou à ses engagements*).

II.3.4. Documentation

Le fournisseur du service de coffre-fort numérique doit documenter son service. Cette documentation doit notamment comprendre :

- Un dossier technique permettant de connaître et comprendre le fonctionnement du service de coffre-fort numérique ainsi que des options ou possibilités permises par celui-ci :
- Les manuels :
    - d'installation et de paramétrage ;
    - d'administration et d'exploitation ;
    - d'utilisation.

Le fournisseur du service de coffre-fort numérique est réputé satisfaire à cette obligation lorsqu'il respecte l'ensemble des exigences définies au chapitre 6 de la norme [NF Z42-020].

II.3.5. Homologation de sécurité

Le fournisseur doit effectuer une analyse de risques sur le système d'information utilisé pour mettre en œuvre le service de coffre-fort numérique et définir une organisation de gestion des risques en vue de procéder à une homologation conformément au guide [HOMOLOGATION].

Cette homologation est réalisée préalablement à l'ouverture du service puis révisée au moins tous les deux ans. Elle se base sur une analyse des risques qui comprend au minimum :

- l'ensemble des menaces auquel le service de coffre-fort numérique est exposé, c'est-à-dire tous les scénarios de risques qui rendent possibles des atteintes à la disponibilité, à l'intégrité et à la confidentialité des données stockées, du fait de l'exploitation de vulnérabilités informatiques, physiques, humaines et organisationnelles, par des sources internes et externes, humaines et non humaines, de manière accidentelle et délibérée ;
- les politiques de sécurité et mesures techniques ou non techniques s'y rattachant, mises en place ou prévues *(par exemple, dans le cadre d'un plan d'amélioration continu)*, pour traiter chacune de ces menaces, en agissant avant, pendant ou après qu'elles se concrétisent ;
- une estimation de la vraisemblance résiduelle de chacune de ces menaces.

II.3.6. Notification des incidents

Le fournisseur du service de coffre-fort numérique notifie dans les meilleurs délais, et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, à l'Agence nationale de la sécurité des systèmes d'information :

- les incidents pouvant entraîner la réalisation des scénarios de risques identifiés dans l'analyse de risques préalable à la mise en service de coffre-fort numérique ayant un impact important ou critique sur la sécurité du service ou sur les données à caractère personnel conservées par le fournisseur du service de coffre-fort numérique ;
- la désactivation d'origine malveillante ou accidentelle des mesures préventives mises en place pour se protéger des scénarios ci-dessus.

À titre indicatif, une liste non exhaustive de type d'incidents de sécurité à notifier figure en Annexe 0 du présent cahier des charges.

De plus, à compter du 25 mai 2018, le [RGPD] impose, dans le cas de violations concernant les données à caractère personnel, de notifier la CNIL et, en cas d'atteinte à leurs droits et libertés, de notifier les utilisateurs concernés.

II.3.7. Veille relative aux vulnérabilités et aux incidents

Une veille relative aux vulnérabilités pouvant affecter le service de coffre-fort électronique doit être effectuée.

De plus, une veille relative aux incidents affectant les services auxquels recourt le coffre-fort numérique doit être effectuée.

II.3.8. Veille relative aux exigences applicables et bonnes pratiques

La décision d'homologation prend également en compte les résultats d'une analyse de la conformité aux références applicables au service de coffre-fort numérique, réalisée préalablement à l'ouverture du service puis révisée au moins tous les trois ans. Cette analyse comprend au minimum :

- un recensement des exigences (communautaires, légales, réglementaires, sectorielles, contractuelles...) ;
- un recensement des bonnes pratiques (normatives, référentiels sectoriels, règles internes...) que le prestataire s'engage à respecter ;
- une explication de la manière dont chaque référence applicable est respectée, ou une justification du fait qu'elle ne l'est pas.

II.3.9. Sous-traitance

Lorsque le fournisseur du service de coffre-fort numérique est amené à sous-traiter certaines activités dans le cadre de la fourniture de ce service, il doit répercuter dans ces contrats de sous-traitance ultérieurs les obligations qui lui incombent en matière de sécurité des données et documents stockés.

II.3.10. Sécurité organisationnelle

La norme [ISO_27001] représente une norme réputée et éprouvée en matière de gestion de la sécurité de l'information, et il est recommandé de la mettre en œuvre. À défaut, il est nécessaire de démontrer que le système de gestion de la sécurité de l'information adhère à des normes ou principes apportant un niveau de sécurité similaire.

II.3.11. Sécurité des matériels et logiciels

Les fonctions cryptographiques sensibles, relatives au chiffrement et à l'authentification des utilisateurs, doivent être mises en œuvre dans des équipements cryptographiques qualifiés au moins au niveau élémentaire par l'ANSSI, utilisés conformément aux conditions d'utilisation définies dans leurs attestations de qualification.

Il est recommandé que le composant « coffre-fort numérique », et toute autre application intervenant dans le processus de chiffrement ou d'authentification (*par exemple, une application installée sur le téléphone mobile de l'utilisateur*), fassent l'objet d'une qualification par l'ANSSI au niveau élémentaire du [RGS]. À défaut, il doit être démontré la mise en place de mesures techniques et organisationnelles permettant de réduire les risques pesant sur eux.

II.3.12. Certification et audits

Le coffre-fort est certifié par l'Agence nationale de la sécurité des systèmes d'information. Cette certification se fait conformément aux dispositions des articles R. 55-7 et suivants du code des postes et des communications électroniques.

Annexes

Annexe 1 – Références documentaires

	Document
[LIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée Disponible sur https://www.legifrance.gouv.fr/
[RGS]	Référentiel général de sécurité, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[RGS_B1]	Annexe B1 au [RGS] : Mécanismes cryptographiques Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques
[RGS_B3]	Annexe B3 au [RGS] : Authentification Règles et recommandations concernant les mécanismes d'authentification
[NF Z42-020]	NF Z42-020 (juillet 2012) : Spécifications fonctionnelles d'un composant Coffre-fort numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps.
[eIDAS]	Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n° 1999/93/CE. Disponible sur http://www.europa.eu
[ISO_27001]	ISO/CEI 27001:2013 (octobre 2013) Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information - Exigences
[HOMOLOGATION]	*L'homologation de sécurité en 9 étapes simples*, version en vigueur Disponible sur http://www.ssi.gouv.fr
[REFERENTIEL eID]	Moyens d'identification électronique – Référentiel d'exigences de sécurité, version 1
[RGPD]	Règlement n° 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Disponible sur http://www.europa.eu

Annexe 2 - Couverture des recommandations techniques de la délibération n° 2013-270 du 19 septembre 2013 portant recommandation relative aux services dits de « coffre-fort numérique ou électronique » destinés aux particuliers

Recommandation de la délibération n° 2013-270	Chapitres applicables du présent document
3. Formalités préalables à la mise en œuvre d'un service de coffre-fort numérique	
Le fournisseur d'un service de coffre-fort numérique détermine les moyens et les finalités dans la mise en œuvre du traitement. Il est ainsi, à la lecture de l'article 3-I de la loi du 6 janvier 1978 modifiée, le responsable du traitement et il lui appartient en cette qualité d'accomplir les formalités auprès des services de la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre du service.	II.3.1
Un service de coffre-fort numérique ou électronique doit faire l'objet, avant sa mise en œuvre, d'une déclaration normale auprès des services de la Commission nationale de l'informatique et des libertés.	II.3.1
La déclaration doit préciser, notamment, les catégories de données à caractère personnel traitées par le prestataire pour assurer son service (données d'identification des utilisateurs et données de connexion), à l'exception des catégories de données stockées par les utilisateurs du service de coffre-fort numériques.	II.3.1
En application de l'article 69 de la loi du 6 janvier 1978 modifiée, si les données stockées par les utilisateurs d'un service de coffre-fort numérique doivent être transférées en dehors de l'Union européenne par le prestataire, ce dernier doit obtenir une autorisation préalable de la Commission nationale de l'informatique et des libertés.	II.3.1
1. S'agissant des données traitées	
Un fournisseur de service de coffre-fort numérique de documents est amené à traiter au minimum des données permettant d'identifier de façon certaine les utilisateurs, d'une part, ainsi que les données de connexion nécessaires au fonctionnement de son service, d'autre part. Ces catégories de données doivent figurer dans la déclaration du traitement accomplie auprès de la Commission nationale de l'informatique et des libertés.	II.3.1
2. S'agissant des destinataires	
Lorsqu'un service de stockage numérique est présenté comme un service de coffre-fort numérique, les documents stockés ne doivent être consultables que par l'utilisateur concerné et les personnes spécialement mandatées par ce dernier.	II.2.3
Le contenu d'un coffre-fort numérique doit ainsi être protégé par des mesures techniques les rendant incompréhensibles aux tiers non autorisés.	II.2.4
3. S'agissant des durées de conservation	
Lorsqu'un utilisateur souhaite supprimer l'un des documents de son espace personnel, cette opération doit être immédiatement prise en compte.	II.2.4
Les copies répliquées en ligne du document supprimé doivent également être supprimées sans délais. Les éventuelles sauvegardes dans lesquelles peuvent figurer ces données ne doivent quant à elles pas être conservées au-delà d'un mois.	II.2.4
Il est toutefois possible de conserver brièvement un document qu'un utilisateur souhaite supprimer, notamment afin de détecter une éventuelle anomalie quant à l'utilisation de son espace personnel, ou de lui permettre de revenir sur sa décision en cas de mauvaise manipulation.	Non couvert
Lorsqu'un service de stockage numérique est présenté comme un service de coffre-	Décret n° 2018-853 du 5 octobre

fort numérique, le fournisseur du service s'engage quant à la pérennité du stockage. Par conséquent, la fermeture de ce type de service nécessite d'en informer les utilisateurs suffisamment en avance, afin de leur laisser le temps nécessaire pour récupérer les documents stockés.	2018 relatif aux conditions de récupération des documents et données stockés par un service de coffre-fort numérique
4. S'agissant de l'information des personnes	
De façon générale, en application de l'article 32 de la loi du 6 janvier 1978 modifiée, les personnes concernées par un traitement de données à caractère personnel doivent être notamment informées de l'identité du responsable du service, de la finalité poursuivie, des destinataires des données, des éventuels transferts de données à destination d'un pays non membre de l'Union européenne, ainsi que de l'existence et des modalités d'exercice des droits d'accès, de rectification et d'opposition.	II.3.1 II.3.2
Par ailleurs, lorsque que le fournisseur propose à ses utilisateurs un service de récupération de documents auprès de services tiers, basé sur la collecte des identifiants et mots de passe de l'utilisateur pour se connecter en leur nom à ces services tiers, il doit informer ses utilisateurs quant aux conséquences pouvant résulter de la collecte de leurs identifiants et mots de passe. En effet, une telle collecte peut constituer une violation des conditions générales d'utilisation de ces services tiers et des conséquences dommageables peuvent en résulter, telles que la perte du bénéfice d'une garantie ou d'une assurance.	II.3.2
La Commission nationale de l'informatique et des libertés recommande ainsi que les fournisseurs d'espaces de stockage numérique élaborent des solutions techniques permettant d'offrir des services de récupération de documents dématérialisés sans procéder à la collecte d'informations confidentielles.	Décret n° 2018-853 du 5 octobre 2018 relatif aux conditions de récupération des documents et données stockés par un service de coffre-fort numérique
5. S'agissant des mesures de sécurité	
Le fournisseur d'un service de coffre-fort numérique ne doit pas être en mesure d'accéder aux données ou de les réutiliser. Des mesures techniques doivent être mises en place pour rendre les données incompréhensibles aux tiers non mandatés par l'utilisateur.	II.2.3 II.2.4
Les données doivent être chiffrées avec une clef, maitrisée uniquement par l'utilisateur, conforme aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques éditées par l'Agence nationale de sécurité des systèmes d'information (ANSSI) dans son référentiel général de sécurité à l'annexe B1.	II.2.4
Lorsqu'un coffre-fort numérique a vocation à conserver des données à long terme, une copie de sauvegarde de la clef de déchiffrement doit être confiée à un tiers de confiance, afin de permettre à l'utilisateur d'accéder à ses données en cas de perte de sa clef.	II.2.4
Toute utilisation d'une sauvegarde de la clef de déchiffrement doit faire l'objet d'une traçabilité et d'une information de l'utilisateur concerné.	II.2.2
Lorsqu'un coffre-fort numérique a vocation à conserver des données à long terme, le fournisseur du service doit prévoir une évolution de la taille des clefs et des algorithmes utilisés, afin de garantir la confidentialité des données stockées dans le futur.	II.2.4
Tous les transferts d'information vers et depuis un coffre-fort numérique doivent être chiffrés lorsqu'ils sont réalisés par un canal de communication non sécurisé.	II.2.4
Les fournisseurs doivent utiliser dans la mesure du possible des produits cryptographiques certifiés ou qualifiés par l'Agence nationale de sécurité des systèmes d'information (ANSSI)	II.3.11
Les fournisseurs doivent communiquer auprès de leurs clients sur les mécanismes de chiffrement utilisés de la façon la plus transparente possible	II.3.2

Les fournisseurs doivent utiliser des mécanismes d'authentification robustes, de préférence des mécanismes d'authentification forte (mots de passe à usage unique, envoi de codes par SMS, ...) et respecter les recommandations de la Commission nationale de l'informatique et des libertés dans ce domaine. En cas d'utilisation de mots de passe, des mécanismes réduisant les risques liés aux choix de mots de passe faibles doivent être mis en place	II.2.3
Les fournisseurs doivent mettre en place des mesures visant à garantir l'intégrité et la disponibilité des données (centre de stockage redondant, sauvegardes régulières, ...) et apporter des garanties en termes d'indemnisation des personnes en cas d'ineffectivité de ces mesures.	II.2.1 II.3.3
Les fournisseurs doivent apporter des garanties fortes pour prévenir toute perte de données en cas de cessation d'activité.	Décret n° 2018-853 du 5 octobre 2018 relatif aux conditions de récupération des documents et données stockés par un service de coffre-fort numérique
Les fournisseurs doivent rendre accessible, sans surcoût, un outil permettant aux utilisateurs de récupérer l'intégralité du contenu de leur coffre-fort de façon simple, sans manipulation complexe ou répétitive, et ce, afin de faciliter le changement de fournisseur.	Décret n° 2018-853 du 5 octobre 2018 relatif aux conditions de récupération des documents et données stockés par un service de coffre-fort numérique
Les fournisseurs ne doivent pas inciter les utilisateurs à leur confier leurs identifiants et mot de passe permettant d'accéder en ligne à des services de la société de l'information sans les avoir préalablement informés quant aux conséquences de cette collecte.	II.3.2
Lorsqu'un coffre-fort numérique permet d'échanger des données avec des tiers, le fournisseur doit mettre en place des mécanismes d'authentification de ces tiers.	II.2.3
Les fournisseurs doivent proposer des fonctionnalités de traçabilité permettant aux utilisateurs de visualiser l'activité récente sur leur coffre-fort numérique, afin de détecter les éventuelles intrusions non souhaitées	II.2.2
Les fournisseurs doivent mettre en place des outils permettant de détecter et bloquer les connexions illégitimes aux coffre-fort numériques	II.2.3
L'effacement d'un fichier par un utilisateur doit être immédiatement pris en compte. Les copies répliquées du document supprimé doivent également être supprimée sans délai. Les éventuelles sauvegardes ne doivent pas être conservées au-delà d'un mois, ce délai apparaissant suffisant pour palier une mauvaise manipulation de l'utilisateur ou corriger une anomalie.	II.2.4
Les fournisseurs doivent informer leurs utilisateurs sur les mécanismes techniques qu'ils mettent en œuvre, afin de leur permettre de juger du niveau de sécurisation du service proposé.	II.3.2 II.3.4
Les utilisateurs doivent être informés quant aux modalités de résiliation du service et de récupération des données stockées	II.3.2
A défaut d'obtention d'une autorisation préalable de la Commission nationale de l'informatique et des libertés, les données collectées dans le cadre d'un service de coffre-fort numérique doivent rester sur le territoire de l'Union européenne, ou sur le territoire d'un État non membre de l'Union européenne garantissant aux données un niveau de protection suffisant au sens de l'article 68 de la loi du 6 janvier 1978 modifiée	II.3.1 II.3.2

Annexe 3 – Couverture des exigences du référentiel pour la délivrance par la CNIL de labels en matière de services de coffre-fort numérique

Le référentiel pour la délivrance de labels en matière de coffre-fort numérique, adopté par la délibération 2014-017 du 23 janvier 2014, a été abrogé par la délibération 2018-102 du 15 mars 2018 mettant un terme à l'activité de labellisation de services de coffre-fort numérique. Néanmoins, le tableau ci-dessous a pour objectif de montrer l'adéquation des exigences du présent cahier des charges avec les exigences du référentiel mentionné ci-dessus.

Exigence du label CNIL	Chapitres applicables du présent document
ED01 Le demandeur a mis en place une démarche visant à s'assurer de la conformité à la loi « Informatique et Libertés » de l'ensemble des traitements qu'il met en œuvre pour l'ensemble de ses activités, dont le service de coffre-fort numérique.	II.3.1
ED02 Les traitements du demandeur, incluant sa gestion des utilisateurs du coffre, ont fait l'objet de formalités préalables adéquates auprès de la Commission Nationale de l'Informatique et des Libertés.	II.3.1
ES01 Le service de coffre-fort numérique collecte, dans le cadre de la création d'un compte, des données d'identification pertinentes et proportionnées au regard de la finalité. L'identification du détenteur du coffre ne peut, en aucun cas, être réalisée au moyen du numéro de sécurité sociale (RNIPP).	II.2.3
ES02 En l'absence d'agrément ministériel pour l'hébergement de données de santé, le demandeur informe l'utilisateur de l'interdiction de stocker des données relatives à la santé. Il ne prévoit pas la création par défaut de dossiers relatifs à la santé.	II.3.1 II.3.2
ES03 Le demandeur informe l'utilisateur de l'interdiction de stocker des contenus illicites (exemple : incitation au meurtre, incitation à la haine raciale, pédopornographie…).	II.3.2
ES04 Le service de coffre-fort numérique ne permet la consultation des documents dématérialisés stockés que par l'utilisateur concerné, et le cas échéant, par les personnes spécialement mandatées par ce dernier (par exemple un notaire, pour permettre aux ayants droits d'accéder à ses données, le conjoint lorsqu'un espace partagé est créé au sein du coffre-fort numérique…).	II.2.4
ES05 Le service de coffre-fort numérique efface les documents supprimés définitivement par l'utilisateur, ainsi que leurs métadonnées, de tous les endroits où ils sont stockés : - sans délai pour les espaces de stockage courants et les éventuelles copies répliquées en ligne (synchronisées en temps réel ou en miroir) ; - dans un délai maximum d'un mois pour les sauvegardes (incrémentales, complètes… réalisées à fréquence donnée).	II.2.4
ES06 Le demandeur garantit la pérennité du stockage, notamment en informant les utilisateurs au moins un mois avant la date de fermeture du service pour leur permettre de récupérer leurs documents stockés.	II.2.5
ES07 Le demandeur rend accessible, sans surcoût, un outil permettant aux utilisateurs, de récupérer l'intégralité du contenu de leur coffre-fort de façon simple, sans manipulation complexe ou répétitive, et dans un format électronique structuré et couramment utilisé, afin de faciliter le changement de fournisseur, et ce sans collecter d'informations confidentielles (telles que les identifiants bancaires, les mots de passe de service en ligne, etc.).	II.2.5

Exigence du label CNIL	Chapitres applicables du présent document
ES08 Le demandeur informe au préalable les utilisateurs : - de l'identité de l'opérateur du service de coffre-fort numérique et de celle du fournisseur du service ; - de la ou des finalité(s) poursuivie(s) ; - de l'absence de destinataire des données conservées, incluant les documents stockés et leurs métadonnées ; - de tout transfert de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne, en indiquant si cet État, sur la base de sa propre législation, pourrait effectuer des demandes visant à accéder directement aux données conservées ; - des droits d'accès, de rectification et d'opposition des personnes et les modalités d'exercice de ses droits ; - de la possibilité de mandater des personnes (par exemple pour permettre à l'utilisateur de récupérer ses données en cas de perte de sa clef, ou à ses ayants droits en cas de décès) ; - du type d'espace mis à leur disposition et de ses conditions d'utilisation ; - des mécanismes techniques utilisés, notamment les mécanismes de chiffrement ; - des modalités de résiliation du service et de récupération des données stockées ; - en cas d'offre de service associé de récupération de documents auprès de services tiers, des conséquences de l'utilisation par le demandeur des identifiants et mots de passe des utilisateurs pour se connecter en leur nom à ces services.	II.3.2
ES09 Le service de coffre-fort numérique fait l'objet d'une analyse de la conformité aux références applicables au service de coffre-fort numérique, préalablement à sa mise en place puis tous les trois ans. Elle comprend au minimum : - un recensement des exigences (communautaires, légales, réglementaires, sectorielles, contractuelles...) ; - un recensement des bonnes pratiques (normatives, référentiels sectoriels, règles internes...) que le demandeur s'engage à respecter ; - une explication de la manière dont chaque référence applicable est respectée, ou une justification du fait qu'elle ne l'est pas.	II.3.8
ES10 Le service de coffre-fort numérique fait l'objet d'une étude des menaces, révisée au moins tous les trois ans. Elle comprend au minimum : - l'ensemble des menaces auquel le service de coffre-fort numérique est exposé, c'est-à-dire tous les moyens qui rendent possibles des atteintes à la disponibilité, à l'intégrité et à la confidentialité des données stockées, du fait de l'exploitation de vulnérabilités informatiques, physiques, humaines et organisationnelles, par des sources internes et externes, humaines et non humaines, de manière accidentelle et délibérée ; - les mesures techniques ou non techniques, mises en place ou prévues, pour traiter chacune de ces menaces, en agissant avant, pendant ou après qu'elles se concrétisent ; - une estimation de la vraisemblance résiduelle de chacune de ces menaces.	II.3.5
ES11 Le service de coffre-fort numérique intègre des outils permettant de bloquer des connexions faites par des robots et de retarder et/ou de bloquer les connexions illégitimes faites par des personnes.	II.2.3

Exigence du label CNIL	Chapitres applicables du présent document
ES12 Le service de coffre-fort numérique intègre des mesures visant à garantir l'intégrité et la disponibilité des données (centre de stockage redondant, sauvegardes régulières…). Le demandeur s'assure des garanties en termes d'indemnisation des personnes en cas d'ineffectivité de ces mesures (par exemple en souscrivant à une assurance dans le but de couvrir les dommages relatifs à ses engagements).	II.2.1 II.3.3
ES13 Le service de coffre-fort numérique intègre des fonctions de traçabilité permettant aux utilisateurs de consulter l'activité récente sur leur coffre-fort (par exemple en journalisant et en horodatant les réussites et échecs de connexion, l'adresse IP et le protocole utilisé, ainsi que les opérations effectuées sur les répertoires et les fichiers, l'utilisateur ayant effectué une opération, l'objet sur lequel une opération est effectuée et la nature de l'opération effectuée).	II.2.2
ES14 Le service de coffre-fort numérique fait l'objet d'une vérification indépendante (par exemple par un auditeur externe, par un service de contrôle interne…) de l'effectivité et de l'efficacité des mesures choisies, au moins une fois tous les trois ans, et le cas échéant des mesures correctives.	II.3.9
ES15 Le demandeur procède à une notification à l'utilisateur en cas d'accès à ses données par un tiers non mandaté par l'utilisateur, même si ces données sont chiffrées.	II.2.4
ES16 Le service de coffre-fort numérique intègre une fonction de chiffrement / déchiffrement des données conservées, incluant les documents stockés et leurs métadonnées. Cette fonction : - permet de rendre les données incompréhensibles aux tiers non mandatés par l'utilisateur, y compris au demandeur ; pour ce faire, le demandeur peut par exemple spécifier et/ou fournir un logiciel à mettre en œuvre sur le poste client de l'utilisateur, en précisant les règles de sécurité que ce dernier doit appliquer, pour lui permettre de chiffrer localement des documents et les métadonnées associées, et de les envoyer ensuite sous forme chiffrée au service de coffre-fort numérique, de telle sorte que le demandeur ne soit pas techniquement en mesure de les déchiffrer ; - permet à l'utilisateur et ses mandataires de déchiffrer et de visualiser les données conservées, incluant les documents stockés et leurs métadonnées ; - est conforme aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques du référentiel général de sécurité de l'Agence nationale de sécurité des systèmes d'information ; - repose sur des clefs maîtrisées par l'utilisateur et ses mandataires ; - permet une évolution de la taille des clefs et des algorithmes utilisés, afin de garantir dans la durée la confidentialité des données stockées.	II.2.4
ES17 Le service de coffre-fort numérique intègre une fonction qui facilite la sauvegarde et la récupération des clefs de chiffrement/déchiffrement pour permettre à l'utilisateur de continuer à accéder à ses données en cas de perte de ses clefs : - soit chez l'utilisateur, de manière sécurisée ; - soit chez un tiers de confiance, non lié au demandeur et choisi par l'utilisateur ; on note dans ce cas que le tiers de confiance devrait assurer la sécurité de la sauvegarde des clefs, garder une trace de toute utilisation de la sauvegarde des clefs et informer l'utilisateur de toute utilisation de la sauvegardes des clefs.	II.2.4

Exigence du label CNIL	Chapitres applicables du présent document
ES18 Le service de coffre-fort numérique intègre une fonction de chiffrement de tous les transferts d'informations vers et depuis le coffre-fort. Cette fonction est conforme aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques du référentiel général de sécurité de l'Agence nationale de sécurité des systèmes d'information.	II.2.4
ES19 Le service de coffre-fort numérique met en œuvre des mécanismes d'authentification pour : - les utilisateurs ; - les personnes physiques spécialement mandatées par ces derniers ; - les tiers auxquels les utilisateurs ont recours pour importer des données depuis un espace de dépôt vers le coffre ; - ainsi que les administrateurs informatiques pour la seule gestion du coffre.	II.2.3
ES20 Le service de coffre-fort numérique ne permet de s'authentifier que par des mécanismes d'authentification robustes (mots de passe à usage unique, envoi de codes par SMS…). Il assure que l'utilisateur, et les personnes physiques spécialement mandatées par ce dernier, sont authentifiés par le serveur hébergeant les données. Tous ces mécanismes sont conformes aux règles et recommandations du référentiel général de sécurité de l'Agence nationale de sécurité des systèmes d'information. Si l'authentification comprend l'utilisation de mots de passe, ces règles font l'objet d'une information des utilisateurs (affichage du niveau de sécurité du mot de passe choisi par exemple) et d'un contrôle (système de blocage si insuffisant).	II.2.3

Annexe 4 – Liste non exhaustive de type d'incidents de sécurité

La liste suivante indique, de manière non exhaustive, des exemples d'incidents de sécurité devant être notifiés à l'ANSSI, s'ils ont un impact sur le service fourni.
De manière générale, tout incident de sécurité lié à un scénario de risque de gravité importante ou critique dans l'analyse de risques doit être notifié.

Perte et vol de supports
Perte ou vol d'un support papier ou de stockage d'informations confidentielles relatives au service
Perte ou vol d'un support papier ou de stockage d'informations confidentielles relatives aux utilisateurs du service
Perte ou vol d'un support de stockage de la clé privée d'une autorité de certification racine
Perte ou vol d'un support de stockage de la clé privée d'une autorité de certification intermédiaire

Perte et vol de postes
Perte ou vol d'un poste d'un administrateur
Perte ou vol d'un poste d'un opérateur

Intrusion physique
Intrusion physique dans les locaux hébergeant le service

Intrusion logique
Intrusion logique dans les systèmes d'information du service

Disponibilité du service
Indisponibilité de tout ou partie du service
Indisponibilité de la fonction de prise en compte des révocations
Indisponibilité de la fonction d'information du statut de révocation des certificats

Atteinte à la confidentialité
Atteinte à la confidentialité de la clé privée d'une autorité de certification racine
Atteinte à la confidentialité de la clé privée d'une autorité de certification intermédiaire
Atteinte à la confidentialité de la clé privée d'un service
Atteinte à la confidentialité de la clé privée d'un utilisateur
Atteinte à la confidentialité de données relatives aux utilisateurs du service
Atteinte à la confidentialité des données à caractère personnel relatives aux utilisateurs du service

Atteinte à l'intégrité
Atteinte à l'intégrité de tout ou partie du service
Atteinte à l'intégrité d'un service de conservation de signatures ou cachets électronique
Atteinte à l'intégrité de la fonction d'information du statut de révocation des certificats
Atteinte à l'intégrité de la source de temps d'un service d'horodatage électronique

Usurpation d'identité
Usurpation d'identité d'un administrateur
Usurpation d'identité d'un opérateur

Abus de privilège
Abus de privilège par un administrateur
Abus de privilèges par un opérateur
Délivrance frauduleuse de certificats électroniques
Émission frauduleuse de jetons d'horodatage électronique

Code malveillant
Détection de la présence d'un code malveillant dans le système d'information du service