FORMULAIRE DE DEMANDE

DE DELIVRANCE D’UN LABEL

POUR UN SERVICE DE COFFRE-FORT NUMERIQUE

*Délibération n° 2014-017 du 23 janvier 2014 portant adoption d’un référentiel pour la délivrance de labels en matière de services de coffre-fort numérique*

*Version du formulaire décembre 2016*

# Modalités de candidature

1. Le demandeur, candidat au label, doit être à la fois opérateur technique du service et fournisseur de ce service auprès des particuliers.

Lorsque l’opérateur technique fournit le service à un organisme qui va jouer le rôle de fournisseur auprès des particuliers, ce dernier ne pourra pas être seul demandeur. Dans cette hypothèse, la demande devra être formulée conjointement par les deux personnes morales, l’opérateur et le fournisseur, afin d’apporter ensemble les justifications et preuves de conformité au référentiel nécessaires à la satisfaction totale des exigences.

1. Le présent formulaire doit être dûment rempli pour demander la délivrance d’un label à un service de coffre-fort numérique. Il permet d’expliquer comment chaque exigence du référentiel d’évaluation est satisfaite et de présenter ou de référencer les éléments permettant de le justifier.
2. Il est ainsi possible de compléter le formulaire par des éléments de justification, en respectant les conditions suivantes :

* tout document joint en tant que justification doit respecter la convention de nommage suivante (personnaliser les libellés entre crochets et retirer les crochets) :

LabelsCNIL-CFN-[nom du demandeur]-[libellé court désignant le document]-[année]-[mois]-[jour].[suffixe]

* tout document électronique doit être lisible par les logiciels de bureautique ou multimédia courants (.doc, .pdf, .txt, .rtf, .jpg…).

1. Le formulaire dûment rempli doit être envoyé à la CNIL avec l’ensemble des éléments de justification en pièces jointes :

* [soit par le biais du formulaire de dépôt en ligne](https://www.declaration.cnil.fr/label/label/formation/initiale/label.action)
* soit par courrier postal à l'adresse suivante :

Commission Nationale de l'Informatique et des Libertés

3 Place de Fontenoy

TSA 80715

75334 Paris cedex 07

Les informations recueillies font l’objet d’un traitement informatique destiné à permettre à la CNIL l’instruction des demandes de label qu’elle reçoit. Elles sont destinées aux membres et services de la CNIL. Vous pouvez exercer votre droit d’accès et de rectification aux informations qui vous concernent en vous adressant à la CNIL : 3 Place de Fontenoy - TSA 80715 - 75334 Paris cedex 07.

# Informations administratives[[1]](#footnote-1)

Les informations suivantes sont nécessaires pour échanger avec la CNIL dans le cadre de l’évaluation du service de coffre-fort numérique, notamment en cas de compléments d’informations nécessaires à l’instruction de la demande.Organisme demandeur

|  |  |
| --- | --- |
| N° SIREN[[2]](#footnote-2) + NIC[[3]](#footnote-3) |  |
| Code NAF[[4]](#footnote-4) |  |
| \*Nom de l’organisme |  |
| Sigle (le cas échéant) |  |
| \*Adresse |  |
| \*Code postal |  |
| \*Localité |  |

## Contact[[5]](#footnote-5)

|  |  |
| --- | --- |
| Civilité |  |
| \*Nom |  |
| \*Prénom |  |
| Service |  |
| \*Adresse |  |
| \*Code postal |  |
| \*Localité |  |
| Téléphone |  |
| Télécopie |  |
| \*Adresse électronique |  |

# Informations relatives aux services de coffre-fort numérique[[6]](#footnote-6)

Les informations suivantes sont nécessaires pour identifier le service de coffre qui fait l’objet de la demande de délivrance de label et délimiter son périmètre.

|  |  |
| --- | --- |
| Nom commercial du service de coffre |  |
| Présentation du service de coffre |  |

# Satisfaction des exigences du référentiel

L’évaluation des services de coffre-fort numérique sera faite au regard des tableaux suivants. Elle pourra être complétée via des échanges entre les évaluateurs et le demandeur.

## Référentiel d’évaluation de la démarche de conformité du demandeur[[7]](#footnote-7)

| **Exigences** | **Moyens mis en œuvre (500 caractères maximum)** | **Éléments de justification[[8]](#footnote-8) (100 caractères maximum)** |
| --- | --- | --- |
| **Exigences relatives à la démarche de conformité du demandeur** | | |
| 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. |  |  |
| 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. |  |  |

## Référentiel d’évaluation des aspects de protection des données du service de coffre-fort numérique [[9]](#footnote-9)

| **Exigences** | **Moyens mis en œuvre (500 caractères maximum)** | **Éléments de justification (100 caractères maximum)** |
| --- | --- | --- |
| **Exigences relatives aux données traitées** | | |
| 1. 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). |  |  |
| 1. 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. |  |  |
| 1. Le demandeur informe l’utilisateur de l’interdiction de stocker des contenus illicites (exemple : incitation au meurtre, incitation à la haine raciale, pédopornographie…). |  |  |

| **Exigences** | **Moyens mis en œuvre (500 caractères maximum)** | **Éléments de justification (100 caractères maximum)** |
| --- | --- | --- |
| **Exigences relatives à l’accès aux données** | | |
| 1. 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…). |  |  |
| **Exigences relatives à la conservation des données** | | |
| 1. 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). |  |  |
| 1. 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. |  |  |
| 1. 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.). |  |  |
| **Exigences relatives à l’information des personnes** | | |
| 1. 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. |  |  |
| **Exigences relatives à la gestion des risques et à la conformité** | | |
| 1. 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. |  |  |
| 1. 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. |  |  |
| 1. 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. |  |  |
| 1. 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). |  |  |
| 1. 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). |  |  |
| 1. 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. |  |  |
| 1. 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. |  |  |
| **Exigences relatives aux mécanismes cryptographiques** | | |
| 1. 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. |  |  |
| 1. 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. |  |  |
| 1. 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. |  |  |
| 1. 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. |  |  |
| 1. 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). |  |  |

1. Les champs précédés d'un astérisque sont obligatoires. [↑](#footnote-ref-1)
2. Système d’Identification du Répertoire des Entreprises. [↑](#footnote-ref-2)
3. Numéro Interne de Classement. [↑](#footnote-ref-3)
4. Nomenclature des Activités Françaises. [↑](#footnote-ref-4)
5. À même de communiquer à la CNIL les compléments d’information nécessaires à l’instruction de la demande. [↑](#footnote-ref-5)
6. Tous les champs sont obligatoires. [↑](#footnote-ref-6)
7. Tous les champs sont obligatoires. [↑](#footnote-ref-7)
8. Référence à un document ou référence à un passage précis d’un document. [↑](#footnote-ref-8)
9. Tous les champs sont obligatoires. [↑](#footnote-ref-9)