Commission nationale de l'informatique et des libertés

Délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés et abrogeant la délibération n° 2017-012 du 19 janvier 2017

NOR : *CNIL2229344X*

La Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 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) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles notamment son article 8-I-2°-*b* ;

Après avoir entendu le rapport M. François PELLEGRINI, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Art. 1er. – Adopte la présente recommandation :

L'article 32 du règlement général sur la protection des données (RGPD) impose que tout traitement de données à caractère personnel soit protégé par des mesures techniques et organisationnelles appropriées aux risques spécifiques que le traitement fait peser sur la protection des données à caractère personnel.

A cette fin, de nombreux traitements utilisent des mots de passe ou autres secrets non partagés afin de protéger l'accès aux données qu'ils contiennent.

La multiplication des attaques informatiques, qui a entraîné la compromission de bases de données contenant notamment les mots de passe associés aux comptes des personnes concernées, a pour conséquence l'amélioration des connaissances des attaquants en matière de mots de passe.

Par ailleurs, l'emploi par les utilisateurs d'un même mot de passe pour différents comptes en ligne, et/ou de mots de passe fondés sur des informations publiques les concernant (date de naissance, prénoms des enfants, etc.) renforce l'obligation pour les responsables de traitement de mettre en œuvre les mesures permettant d'assurer la sécurité des données à caractère personnel qu'ils gèrent.

La Commission estime nécessaire, dans l'objectif d'apporter une plus grande confiance dans les services numériques, de définir des modalités techniques de cette méthode d'authentification à même de garantir un niveau de sécurité adapté. Pour ce faire, la CNIL a décidé d'adopter une recommandation ayant pour objectif de définir les exigences techniques et organisationnelles minimales pour les authentifications par mot de passe ou par tout autre secret non partagé (à l'exception des clés et secrets cryptographiques) mis en œuvre dans le cadre de traitements de données à caractère personnel. Celle-ci constitue une mise à jour de son référentiel technique destiné à apporter un niveau de sécurité minimal, en cohérence avec les bonnes pratiques de sécurité et concrètement applicable Les dispositions de cette recommandation, qui n'ont pas un caractère normatif, correspondent à l'état de l'art auquel tout responsable de traitement devrait se conformer, *a minima*, pour satisfaire aux obligations de l'article 32 du RGPD lorsqu'il utilise une authentification par mots de passe pour protéger un traitement.

Les acteurs peuvent mettre en œuvre d'autres mesures de sécurité que celles décrites dans cette recommandation s'ils sont en capacité de montrer qu'elles garantissent un niveau de sécurité au moins équivalent. La Commission a notamment toujours considéré que d'autres moyens d'authentification, comme par exemple l'authentification à double facteur ou les certificats électroniques, offrent davantage de sécurité que le seul mot de passe. Pour aller plus loin et, notamment, déterminer les mesures nécessaires à mettre en œuvre dans le cas où le niveau minimal décrit est insuffisant, cette recommandation sera utilement complétée par le guide de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) intitulé « Recommandations relatives à l'authentification multifacteur et aux mots de passe ».

Pour l'élaboration de cette recommandation, la Commission a échangé avec ses homologues européens, l'ANSSI et les experts du domaine au moyen d'une consultation publique qui s'est tenue du 21 octobre 2021 au 10 décembre 2021.

1. Recommandations générales en matière de sécurité des mots de passe

Le terme « mot de passe » désigne, dans cette délibération, tout facteur de connaissance (1), c'est-à-dire tout ensemble d'informations révocable, connu uniquement de la personne concernée et permettant ou contribuant à l'authentification de celle-ci ; il inclut, notamment, les « phrases de passe » (réputées plus longues que les mots de passe) et les codes de déverrouillage, et exclut les clés et secrets cryptographiques.

Tout responsable de traitement utilisant des mots de passe doit garantir un niveau minimal de sécurité reposant, d'une part, sur une longueur et une complexité suffisantes, équivalentes à une entropie de 80 bits sans mesure complémentaire et, d'autre part, sur des règles de mise en œuvre et de gouvernance permettant de préserver la sécurité du mot de passe tout au long de son cycle de vie.

La notion de « devinabilité » est une approche alternative pour déterminer la robustesse d'un mot de passe. Elle consiste à évaluer, au moyen de traitements algorithmiques dédiés, la facilité pour un adversaire de retrouver un mot de passe donné. Il s'agit donc, non pas de vérifier le respect d'une politique de mots de passe fixant une complexité formelle minimale, mais d'évaluer dynamiquement la résistance du mot de passe choisi. La littérature sur le sujet recommande une résistance aux attaques minimale de 10^{14} essais. Cependant, au moment de la publication de cette recommandation, les outils pour mettre en œuvre cette méthode, a priori plus fiable que la seule vérification de complexité, ne sont pas encore disponibles pour des utilisateurs francophones ; la Commission ne dispose donc pas actuellement du recul nécessaire pour déterminer le niveau de résistance équivalent aux niveaux décrits dans la présente recommandation. Elle sera attentive aux nouveaux développements dans ce domaine, notamment quant à la disponibilité de solutions librement accessibles qu'elle pourra évaluer.

Les risques spécifiques à certains traitements (par exemple, les traitements de données sensibles au sens de l'article 9 du RGPD, tels que les traitements de données de santé, ou des traitements à large échelle, ou encore dans le cas de traitements particuliers comme la fourniture d'un service de messagerie électronique ou d'un gestionnaire de mots de passe) ou à certaines catégories d'utilisateurs (par exemple, les administrateurs informatiques) nécessiteront des mesures plus contraignantes que celles définies dans cette recommandation, comme par exemple la mise en œuvre d'un processus d'authentification multi-facteurs. Dans certains cas, des réglementations spécifiques peuvent imposer un niveau minimum d'authentification plus exigeant que celui défini dans la présente recommandation.

De plus, les opérations relatives à la gestion des mots de passe confiées, pour tout ou partie, à un sous-traitant, doivent respecter les conditions posées à l'article 28 du RGPD. Dans ces cas de figure, les rôles et responsabilités doivent être précisément définis et formalisés, le niveau de sécurité requis et les objectifs de sécurité assignés au sous-traitant clairement définis, compte tenu de la nature du traitement et des risques qu'il est susceptible d'engendrer.

Enfin, si les simples éditeurs de logiciels ne sont pas soumis au cadre juridique relatif à la protection des données, la documentation relative aux logiciels qui traitent des mots de passe devrait préciser de façon détaillée les modalités de génération, stockage et transmission des mots de passe afin de faciliter la mise en conformité des utilisateurs de ces logiciels.

---

(1) Pour rappel, les mots de passe constituent l'un des trois facteurs possibles d'authentification définis par le guide en matière d'authentification de l'ANSSI et de la CNIL, qui sont : les facteurs de « connaissance » (détention d'une information secrète), de « possession » (détention d'un objet unique, tel qu'une carte à puce) et l'« inhérence » (caractéristique biométrique propre).

2. **Sur la gouvernance**

Tout organisme utilisant une authentification reposant sur des mots de passe définit une politique de gestion de ceux-ci.

Cette politique est rédigée par les acteurs en charge de la sécurité et des moyens informatiques dans l'organisme (RSSI, DSI, DPD/DPO, par exemple) et validée par le responsable de traitement.

Le responsable de traitement doit s'assurer du respect de cette politique par des solutions techniques et organisationnelles. A cette fin, il met en œuvre une revue régulière, par exemple annuelle, des habilitations et de l'application de cette politique afin de vérifier sa bonne mise en œuvre et détecter si une mise à jour est nécessaire.

Les personnes concernées doivent être informées des règles de cette politique qui leur sont applicables. Elles doivent également être sensibilisées aux menaces et aux risques de compromission de leurs mots de passe, ainsi qu'au comportement à adopter en cas de suspicion de compromission de ceux-ci. Les formations ou informations doivent être adaptées aux différents publics, à leurs compétences, à leur niveau de responsabilité et à la sensibilité des données auxquelles ils ont accès. Ces formations pourront utilement inclure un encouragement à l'utilisation de gestionnaires de mots de passe, ainsi qu'une information sur les bonnes pratiques relatives à leur utilisation (notamment sur la nécessité d'un mot de passe maître fort, d'une complexité dépassant les minima définis par cette recommandation et la nécessité de sauvegarder régulièrement la base des mots de passe). Des outils ou indicateurs peuvent être mis à disposition des utilisateurs pour leur permettre d'évaluer, au moment de la création d'un nouveau mot de passe, la robustesse de ce dernier. Dans ce cas, une vigilance particulière devra être portée à la provenance, la sécurité et la pertinence des outils ou indicateurs choisis.

3. **Sur les modalités opérationnelles de l'utilisation de mots de passe**

3.1. *Préambule et définitions*

Les règles et recommandations décrites dans les annexes B1 et B2 du référentiel général de sécurité (2) (RGS) ainsi que dans le guide des mécanismes cryptographiques de l'ANSSI (3) font référence pour ce qui doit être considéré comme un « algorithme public réputé fort ». Pour assurer que « *la mise en œuvre logicielle est exempte de vulnérabilité connue* », la Commission recommande de ne choisir que des logiciels ou composants logiciels faisant l'objet d'une maintenance de sécurité régulière, de n'utiliser que les versions à jour de ceux-ci et d'effectuer une veille sur leur sécurité.

On appelle « entropie » la quantité de hasard contenue dans un système. Pour un mot de passe ou une clé cryptographique, cela correspond à son degré d'imprédictibilité, et donc à sa capacité de résistance à une attaque par force brute. Dans le cadre de cette recommandation, le terme d'entropie, appliqué à un mot de passe,

correspond à son entropie idéale dans l'hypothèse où il serait généré aléatoirement. En informatique, on mesure couramment l'entropie en nombre de « bits », c'est-à-dire en nombre de chiffres binaires (valant soit « 0 », soit « 1 ») permettant d'exprimer la même quantité de hasard. Ainsi, un code de carte bancaire à quatre chiffres décimaux pris au hasard, valant chacun de « 0 » à « 9 », donne dix mille combinaisons possibles (10 à la puissance 4, noté 10^4). Pour obtenir un nombre de combinaisons binaires équivalent, il faut utiliser 13 bits, car 2 à la puissance 13 (ou 2^{13}) vaut 8 192, qui est du même ordre de grandeur que 10^4. On dira donc qu'un code de quatre chiffres décimaux aléatoires possède une entropie de 13 bits. Ces calculs peuvent s'appliquer à tout ensemble de caractères : 26 choix possibles par caractère pour des lettres majuscules, 52 pour des lettres majuscules et minuscules, 62 si l'on y ajoute les chiffres, etc.

Toute règle de construction d'un mot de passe conduit à limiter l'espace des choix possibles, et donc à limiter son entropie pour une longueur donnée. Par exemple, choisir un mot de passe parmi les mots d'une langue revient à limiter très fortement le nombre de combinaisons de lettres possibles en pratique. En effet, chaque langue n'admet qu'un nombre limité de suites de lettres, servant à former les syllabes des mots. La tentation, pour de nombreux utilisateurs, de choisir des mots de passe « simples à retenir » facilite les attaques dites « par dictionnaire » dans lesquelles, au lieu de tester par force brute l'intégralité des combinaisons possibles, n'en sont testées qu'un nombre très limité, comprenant des mots du dictionnaire, des prénoms ou des dates, ainsi que leurs dérivations « classiques » (par exemple, du mot « kangourou », seront dérivées et testées des combinaisons telles que « k4ng0urou », « kangourou01 », « KaNgOuRoU », « Kangourou_1969 », etc.).

De fait, lorsque les utilisateurs ont la liberté de choisir comme mot de passe des combinaisons qui ne sont pas strictement aléatoires, il est nécessaire, pour conserver un niveau d'entropie donné, de choisir une politique de mots de passe privilégiant la longueur des mots de passe par rapport à leur complexité, voire, en fonction des risques, d'augmenter le nombre de bits d'entropie cible pour la politique de mots de passe. En effet, pour les utilisateurs employant généralement des mots du dictionnaire, il est préférable d'imposer des mots de passe les amenant à choisir une série de mots plutôt qu'un seul. Il est recommandé de les guider dans ce choix, en leur rappelant notamment qu'il est préférable de choisir des mots qui n'ont pas de liens entre eux.

A ce propos, le décompte des caractères qui seront utilisés pour la création d'un mot de passe devra être réaliste. Ainsi, il conviendra de ne prendre en compte que les caractères habituellement intégrés par les utilisateurs dans leurs mots de passe et, notamment, uniquement les caractères spéciaux disponibles sur les claviers habituellement accessibles et utilisés par les utilisateurs concernés. Dans le cas d'un usage dans différents environnements (ordinateur, ordiphone), les jeux de caractères considérés doivent être accessibles dans l'ensemble des environnements des utilisateurs.

Enfin, il convient également de recommander aux utilisateurs de ne pas utiliser, pour construire leurs mots de passe, d'informations personnelles (date de naissance, prénoms des proches, etc.), ces inclusions étant à même de faciliter des attaques ciblées les concernant.

---

(2) https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/.

(3) https://www.ssi.gouv.fr/entreprise/guide/mecanismes-cryptographiques/.

3.2. *Modalités de l'authentification par mot de passe*

Lorsque l'authentification par mot de passe s'effectue au moyen d'une connexion réseau, et *a fortiori* si cette dernière est opérée par un tiers, la Commission recommande :

- qu'une mesure de contrôle de l'identité du serveur d'authentification par le client soit mise en œuvre, au moyen d'un certificat d'authentification de serveur ;
- que le canal de communication entre le serveur authentifié et le client soit chiffré à l'aide d'une fonction de chiffrement sûre (c'est-à-dire mettant en œuvre un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue) ;
- que des mesures de sécurité renforcées soient mises en œuvre afin de garantir la confidentialité des clés privées utilisées ;
- que les mots de passe n'apparaissent pas dans les adresses des ressources distantes, ni en clair, ni sous forme hachée.

Les deux premiers points peuvent notamment être mis en œuvre par l'utilisation du protocole TLS dans une configuration respectueuse des recommandations de l'ANSSI en la matière, exposées dans son document SDE-NT-35/ANSSI/SDE/NP1 intitulé « Recommandations de sécurité relatives à TLS ».

Lorsque l'authentification par mot de passe s'effectue sur une page web, il est recommandé que cette page ne contienne pas de code réalisant des appels externes (publicités, briques logicielles et contenus tiers, etc.), afin de limiter les vecteurs d'attaques pouvant mener à la compromission des mots de passe.

Dans les champs de saisie des mots de passe, les caractères saisis ne doivent pas être visibles par défaut ; ils doivent rester invisibles ou être représentés par un caractère neutre tel qu'un point ou une étoile.

En cas d'échec de l'authentification, le message d'information affiché devrait indiquer l'échec sans fournir d'information susceptible d'aider un attaquant potentiel.

Tout dispositif mettant en œuvre des mots de passe par défaut (qu'ils soient générés automatiquement ou par une personne initialisant le compte pour l'utilisateur) ne doit fournir que des mots de passe à usage temporaire et/ou

doit imposer leur modification à la première connexion. Idéalement, le système devrait contraindre l'utilisateur à effectuer cette modification avant de lui permettre de réaliser d'autres actions.

S'agissant des modalités de création d'un mot de passe requis pour l'authentification à un compte, le responsable de traitement doit s'assurer que les mots de passe utilisés sont d'un niveau de sécurité suffisant, par exemple en imposant une taille et une complexité minimales. La personne ayant recours à une authentification par mot de passe doit être préalablement informée de l'ensemble des éléments de la politique mise en œuvre par le responsable de traitement qu'elle doit respecter et, notamment, le cas échéant, les tailles minimale et maximale des mots de passe si celles-ci sont susceptibles de ne pas être naturellement respectées par l'utilisateur.

En dehors du cas des codes de déverrouillage (voir cas n° 4), dès lors que le responsable de traitement identifie un risque lié à la soumission abusive de mots de passe (notamment, si le traitement est accessible depuis internet), il convient de fixer une taille maximale pour les champs des mots de passe. Celle-ci doit être suffisamment grande pour permettre l'utilisation de phrases comme mots de passe, tout en évitant les attaques par déni de service résultant du traitement d'un mot de passe abusivement long. Leur taille maximale ne saurait en principe être inférieure à 50 caractères pour une authentification par mot de passe avec ou sans restriction de compte (cas n° 1 et 2). Elle pourra être, par exemple, de l'ordre de quelques centaines de caractères.

Afin d'encourager l'utilisation des gestionnaires de mots de passe et d'améliorer l'accessibilité numérique, des mécanismes ayant pour objet ou effet d'interdire aux utilisateurs de coller un mot de passe dans les champs de saisie ne doivent pas être mis en œuvre, tant lors de la création du mot de passe que de sa modification ou de son utilisation lors de l'étape d'authentification.

Al'exception des envois par voie postale, les mots de passe ne doivent pas être communiqués à l'utilisateur en clair, notamment par courrier électronique. Seuls des mots de passe temporaires ou à usage unique devraient être communiqués aux utilisateurs.

Dans le cas d'un envoi par voie postale, l'usage de mesures complémentaires destinées à détecter son interception (par exemple : enveloppes dont l'intérieur est noirci pour éviter la lecture par transparence, cases à gratter) ou à en empêcher l'usage (par exemple : renouvellement forcé lors de la première utilisation du mot de passe envoyé) devraient être mis en œuvre.

Dans le cas de l'envoi de liens de création ou de renouvellement de mot de passe, une durée d'expiration courte est définie, dans la plupart des cas de quelques heures et d'au plus de 24 heures. Cependant, dans le cas d'un envoi par courrier, la durée de validité pourrait être plus longue.

Lorsqu'un mot de passe est refusé lors de sa création, un message d'information clair rappelant la politique de l'organisation en termes de mot de passe et explicitant la raison du refus doit être affiché à l'utilisateur. Dans la mesure du possible, le responsable de traitement doit conseiller et guider l'utilisateur dans la création de son mot de passe.

Les mots de passe connus comme étant couramment utilisés ne devraient pas être acceptés. La taille et le contenu de la liste de mots de passe à refuser doivent être proportionnels aux risques et, le cas échéant, adaptés au contexte d'usage (par exemple, en incluant des listes de mots de passe interdits spécifiques au service utilisé). Dans tous les cas, l'utilisateur doit être informé que les mots de passe les plus courants ne sont pas acceptés.

En cohérence avec les recommandations de l'ANSSI en matière d'authentification décrites dans le guide intitulé « *Recommandations relatives à l'authentification multifacteur et aux mots de passe* », la Commission décrit trois possibilités d'exigences minimales pour une authentification par mot de passe. Le cas d'usage et le public ciblé doivent être pris en compte dans le choix des critères à imposer dans la politique de gestion des mots de passe.

Le premier cas fait reposer la sécurité principalement sur le mot de passe ; il impose par conséquent des exigences importantes en termes de niveau d'entropie, et donc de taille et de complexité du mot de passe. Dans les cas suivants, l'existence de mesures complémentaires visant à assurer un niveau de sécurité similaire permet le recours à des mots de passe d'entropie plus faible.

Dans tous les cas, comme indiqué en introduction, les niveaux d'entropie décrits ci-dessous sont des limites basses. En fonction des risques, un niveau minimal plus élevé peut être nécessaire.

– *Cas n° 1 : mot de passe seul*

La robustesse de cette authentification reposant exclusivement sur la qualité intrinsèque du mot de passe de l'utilisateur, la complexité à fixer dans la politique de mots de passe doit permettre d'assurer l'équivalent d'une entropie d'au moins 80 bits. Les trois exemples ci-dessous correspondent à cette entropie.

Exemple 1 : les mots de passe doivent être composés d'au minimum 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles.

Exemple 2 : les mots de passe doivent être composés d'au minimum 14 caractères comprenant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire.

Exemple 3 : les phrases de passe fondées sur des mots de la langue française doivent être composées d'au minimum 7 mots.

– *Cas n° 2 : mot de passe et restriction d'accès au compte*

Quand l'authentification prévoit un mécanisme de restriction de l'accès au compte (voir exemples ci-dessous), la complexité à fixer dans la politique de mots de passe doit permettre d'assurer l'équivalent d'une entropie d'au moins 50 bits.

Exemple 1 : la taille du mot de passe doit être au minimum de 8 caractères et comporter 3 des 4 catégories de caractères (majuscules, minuscules, chiffres et caractères spéciaux), les caractères spéciaux devant être pris dans un ensemble d'au moins 11 caractères.

Exemple 2 : les phrases de passe fondées sur des mots de la langue française doivent être composées d'au minimum 5 mots.

Exemple 3 : les mots de passe doivent être composés d'au minimum 16 chiffres.

L'authentification doit alors faire intervenir un mécanisme de restriction d'accès au compte. Celui-ci peut prendre une ou plusieurs des formes suivantes :

- une temporisation de l'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement en fonction du nombre de tentatives dans un laps de temps déterminé ; cette durée soit supérieure à une minute après cinq tentatives échouées, et permette de réaliser au maximum 25 tentatives par 24 heures ; et/ou
- un mécanisme déterminant un nombre maximal de tentatives autorisées dans un délai donné (par exemple, 10 essais par heure) ; et/ou
- un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (par exemple : mise en œuvre de « captcha ») ; et/ou
- un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10, assorti d'un mécanisme de déblocage proportionnel aux risques que les personnes fassent l'objet d'une usurpation d'identité.

Le choix de la solution doit être opéré en prenant en compte la vraisemblance d'une attaque par déni de service, qui aurait pour objet de rendre les comptes inaccessibles, et de sa gravité pour les utilisateurs.

– *Cas n° 3 : code de déverrouillage*

Quand l'authentification s'appuie sur un matériel détenu par la personne, la complexité à fixer dans la politique de mots de passe doit permettre d'assurer l'équivalent d'une entropie d'au moins 13 bits.

Exemple : la taille du code personnel doit être au minimum de 4 chiffres décimaux.

L'authentification ne peut concerner qu'un dispositif matériel détenu en propre par la personne, à savoir uniquement les cartes à puce et dispositifs contenant un certificat électronique ou une paire de clés déverrouillable par mot de passe, ou tout autre mécanisme technique apportant un même niveau de sécurité.

Un blocage du dispositif doit être mis en œuvre après un nombre d'authentifications échouées consécutives au plus égal à 3.

3.3. *Modalités de conservation des mots de passe*

Le mot de passe ne doit jamais être stocké en clair par le responsable de traitement. Lorsqu'il est conservé, tout mot de passe utile à la vérification de l'authentification doit être préalablement transformé au moyen d'une fonction cryptographique spécialisée, non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant un « sel » et des paramètres relatifs aux coûts en temps et/ou en mémoire nécessaires à son attaque. On entend par « sel » une donnée supplémentaire ajoutée systématiquement aux données devant être hachées (ici, les mots de passe) afin d'empêcher que deux informations identiques donnent la même valeur hachée sur deux systèmes informatiques différents. Utiliser un sel limite la possibilité qu'un attaquant déduise le mot de passe d'un utilisateur en consultant l'une des nombreuses bases de données de couples « mot de passe sans sel/valeur hachée » précalculés qui sont disponibles sur internet.

Le sel devrait être généré aléatoirement et avoir une longueur minimale de 128 bits. Il est généré pour chaque utilisateur et stocké dans la même base de données que les mots de passe. Les différents éléments (taille de sel, algorithmes et paramètres) devront être régulièrement mis à jour en fonction des risques et avancées technologiques.

La mise en œuvre d'un protocole de type PAKE (« *Password Authenticated Key Exchange* »), public et prouvé sûr, garantissant la vérification du mot de passe sans qu'il soit transmis en clair au serveur pour vérification est conseillée : ce type de solution permet, d'une part, de ne jamais exposer le mot de passe lors de la transaction et, d'autre part, de ne pas stocker les mots de passe sur le serveur, seule une fonction de vérification étant conservée à leur place.

Dans le cas particulier des mots de passe stockés dans une application, leur stockage devrait être limité aux applications de gestion de mots de passe (ou remplissant ce rôle). Les mots de passe devraient alors être stockés sous une forme chiffrée et un mécanisme de déverrouillage (par exemple via une phrase de passe maître) devrait être proposé. Dans les autres cas, un mécanisme de jeton à durée de vie limitée et révocable à tout moment par l'utilisateur est conseillé.

3.4. *Modalités de changement du mot de passe et d'information des personnes*

Le responsable de traitement doit permette à la personne concernée de procéder elle-même, de façon autonome, au changement de son mot de passe. Dans ce cas, les règles afférentes à la création de mots de passe s'appliquent.

Les modalités décrites plus haut quant à l'envoi de mots de passe à l'utilisateur par voie postale ou électronique, s'appliquent également à son renouvellement.

3.4.1. Renouvellement périodique du mot de passe

Les responsables de traitement ne devraient plus imposer de modification périodique des mots de passe à l'ensemble de leurs utilisateurs. Une procédure de modification périodique reste cependant nécessaire pour les comptes à privilège (comptes d'administration) ; une périodicité pertinente et raisonnable sera à définir en fonction des risques.

3.4.2. Renouvellement du mot de passe sur demande de l'utilisateur

Si le renouvellement implique l'envoi d'une information (par exemple : lien web, mot de passe temporaire communiqué par courriel ou téléphone), celui-ci doit s'effectuer via un canal préalablement validé (par exemple : adresse courriel, moyen d'identification électronique de secours). Afin d'empêcher la compromission du mot de passe par un usage malicieux de la phase de renouvellement, il ne doit pas être possible d'envoyer le nouveau mot de passe sur un canal de communication récemment modifié. La durée d'embargo sur les canaux récemment modifiés doit être proportionnée aux risques d'usurpation. Toute modification du canal doit être notifiée à l'utilisateur sur l'ensemble des canaux de communication validés, y compris celui ayant fait l'objet d'une modification, afin qu'il puisse être alerté si cette modification n'est pas de son fait.

Lorsqu'une réinitialisation demandée par l'utilisateur déclenche l'envoi d'une information sur un canal préalablement validé, l'utilisateur devrait simplement être informé du fait qu'une demande de validation sera envoyée, sans lui confirmer l'existence du compte la validité du canal.

Si le renouvellement fait intervenir un ou plusieurs éléments supplémentaires (numéro de téléphone, adresse postale, réponse à une question, etc.), il convient que :

– les modalités permettant d'identifier que la personne demandant le renouvellement est la personne détentrice du compte ne reposent pas sur une réponse à une question relative à des informations habituellement publiques (par exemple : des informations accessibles à de nombreuses personnes sur les réseaux sociaux telles que le nom des parents, le lieu d'études, le nom des animaux de compagnie, etc.) ;
– ces éléments ne sont pas conservés dans le même espace de stockage que l'élément de vérification du mot de passe, à moins d'être conservés sous forme chiffrée à l'aide d'un algorithme public réputé fort, et que la sécurité de la clé de chiffrement soit assurée ;
– afin de prévenir les tentatives d'usurpation s'appuyant sur le changement de ces éléments, la personne doive être immédiatement notifiée de leur modification par les moyens de communications identifiés.

La personne concernée devrait avoir accès à une interface lui permettant de saisir un nouveau mot de passe. La validité de la session de cette interface ne doit pas excéder 24 heures, et les liens de renouvellement doivent être à usage unique. Tout nouveau lien généré devrait révoquer les liens précédents.

3.4.3. Renouvellement des mots de passe et information des usagers en cas de compromission

Lorsqu'une atteinte à la confidentialité des mots de passe ou, plus généralement une atteinte à la sécurité susceptible d'engendrer la compromission de comptes utilisateurs, a été détectée, le responsable de traitement informe sans délai la personne concernée et lui permet de renouveler son mot de passe immédiatement.

Le responsable de traitement doit évaluer le risque d'usurpation de compte et ses impacts afin de décider de la nécessité de mesures particulières (par exemple : blocage temporaire des comptes concernées ou mise en œuvre d'un mécanisme supplémentaire d'identification de l'usager).

Dès lors qu'il existe une suspicion de violation de son mot de passe, le responsable de traitement doit imposer à la personne concernée de le modifier lors de sa prochaine connexion, et lui recommander de veiller à changer les mots de passe des éventuels services pour lesquels elle aurait utilisé ce même mot de passe.

Lorsqu'une information complémentaire est utilisée (cas n° 3), celle-ci doit également être renouvelée dès lors que sa confidentialité n'est plus garantie.

Enfin, concernant les données de renouvellement, les questions secrètes et leurs réponses doivent également être renouvelées en cas d'atteinte à leur confidentialité.

3.5. *Journalisation*

Les activités d'authentification des utilisateurs et de manipulation de leurs secrets, par eux-mêmes ou des tiers, doivent normalement faire l'objet d'une journalisation respectant les recommandations de la CNIL en la matière. Les mots de passe ainsi que les identifiants non reconnus ne doivent pas apparaître dans les journaux.

Art. 2. – La délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe est abrogée.

Le cas d'usage n° 3 qui y était prévu (c'est-à-dire, le cas correspondant à une information secrète de 7 caractères et un mot de passe d'au moins 5 caractères) n'est plus recommandé par la Commission. Les responsables de traitement qui auraient mis en œuvre ce cas d'usage devraient faire évoluer leur politique de mots de passe vers un autre cas. La Commission tiendra compte du délai nécessaire pour mettre en œuvre les changements nécessaires.

La présente délibération sera publiée au *Journal officiel* de la République française.

La présidente,
M.-L. Denis