# Recommandation

## RELATIVE À L'AUTHENTIFICATION MULTIFACTEUR

*Version adoptée le 20 mars 2025*

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

# Table des matières

# 1. Introduction

L'authentification multifacteur a pour objectif d'atténuer le risque de compromission des ressources informatiques, et *a fortiori* d'accès illégitime ou modification non désirée des données personnelles qui y sont traitées, en demandant à l'utilisateur davantage qu'un simple mot de passe. Les organismes qui souhaitent y recourir, ainsi que les fournisseurs de solutions d'authentification multifacteur eux-mêmes, doivent respecter certaines règles, notamment celles issues du règlement général sur la protection des données (RGPD) et les réglementations sectorielles qui leur sont applicables.

# 2. Présentation de la recommandation et des enjeux

Le présent document détaille les recommandations de la Commission nationale de l'informatique et des libertés (CNIL) pour la mise en conformité au RGPD des responsables de traitement dans leur usage de l'authentification multifacteur. Ce document promeut aussi des approches vertueuses de protection de la vie privée par conception. Ce projet de recommandation, et notamment les exemples qui y sont proposés, a pour seul objectif d'aider les professionnels concernés dans leur démarche de mise en conformité. Il ne prétend pas couvrir de manière exhaustive tous les cas d'usage dans lesquels l'authentification multifacteur est susceptible d'intervenir.

## 2.1. À qui s'adresse cette recommandation ?

Cette recommandation s'adresse aux professionnels de tous secteurs et particulièrement aux délégués à la protection des données (DPD) et aux responsables de la sécurité des systèmes d'information (RSSI) ainsi qu'à leurs équipes. Elle est également destinée aux offreurs de produits, services et solutions d'authentification multifacteur pour leur permettre de mieux connaître la règlementation à laquelle sont soumis les responsables de traitements en matière de protection des données. Elle peut également aider, au travers des exemples, chaque professionnel à déterminer sa qualification juridique au sens du RGPD (responsable, responsable conjoint, sous-traitant, ou le cas échant, aucune) afin de mieux comprendre les obligations qui lui incombent mais également celles de ses partenaires susceptibles de l'impacter de manière incidente.

## 2.2. Qu'est-ce que l'authentification multifacteur ?

L'authentification d'un utilisateur a pour objet de vérifier la preuve de son identité avant de lui donner l'accès aux ressources d'un système d'information (ordinateur, partage réseau, site web, application mobile, etc.). Une **authentification multifacteur,** généralement abrégée par **MFA** (pour *multi-factor authentication* en anglais), a pour caractéristique de s'appuyer sur plusieurs preuves, appelées facteurs d'authentification, appartenant à au moins deux des trois catégories suivantes :

- un **facteur de connaissance** (ce que la personne sait) : un secret à mémoriser, par exemple une phrase de passe (*passphrase* en anglais), un mot de passe ou un code confidentiel, plus communément appelé code PIN (*Personal Identification Number* en anglais) ;
- un **facteur de possession** (ce que la personne a) : un élément secret non mémorisable, tel qu'une clé cryptographique, permettant de prendre part à des protocoles d'authentification (par exemple ceux faisant intervenir un mot de passe à usage unique, généralement nommés protocoles ***OTP*** pour *one-time password* en anglais tel que définis en annexe I) et contenu dans un objet physique unique qui idéalement protège cet élément d'extractions. Il peut s'agir, concrètement :
    - d'un jeton matériel (*hard token* en anglais) à savoir un dispositif matériel dédié, idéalement muni d'un **composant de sécurité** (voir annexe), fourni par le **vérifieur** (voir annexe), tel qu'une carte à puce, une clé USB d'authentification, un authentifieur OTP (composant matériel muni d'un écran affichant un code à usage unique renouvelé régulièrement), une calculette OTP, etc. ;
    - ou d'un jeton logiciel lié (*device-bounded soft token* en anglais) reposant sur une application associée à un **appareil enrôlé** (voir annexe). Ce jeton logiciel ne devrait pouvoir être actif que sur un seul et unique appareil, idéalement équipé d'un composant de sécurité intégré, ou a minima être sécurisé en termes de confidentialité et d'intégrité[1].

[1] Recommandations relatives à l'authentification multifacteur et aux mots de passe, v2.0, p. 38, cyber.gouv.fr

- un **facteur d'inhérence** parfois dit, par abus de langage, facteur biométrique (ce que la personne est ou fait) une caractéristique physique indissociable d'une personne qui peut être :
    - morphologique, par exemple une empreinte digitale, une empreinte rétinienne, la structure du visage, etc. ;
    - comportementale, par exemple la frappe au clavier, la voix, la démarche ou encore l'écriture ;
    - biologique, par exemple l'ADN, le sang, etc.

**L'OTP par SMS, un facteur de possession dont le niveau de confiance reste à évaluer**

L'usage de l'OTP par SMS (par opposition à un authentifieur OTP, une calculette OTP ou une application dédiée d'OTP) peut être considéré comme un facteur de possession dont le niveau de confiance doit être évalué par le responsable de traitement, au cas par cas. En effet, si la carte SIM (SIM physique ou eSIM) est, dans la majorité des cas, personnelle et sous le seul contrôle de l'utilisateur, elle présente plusieurs limites :

- La transmission d'un code OTP par SMS est une méthode d'authentification reposant sur la réception d'une valeur au moyen d'un canal qu'il est difficile de considérer comme apportant une sécurité satisfaisante, c'est pourquoi il est déconseillé par les autorités compétentes[2] [3] ;
- Des solutions existent pour consulter les SMS sur un autre terminal que le téléphone portable de l'utilisateur (par exemple, les solutions opérateurs ou fournisseur de système d'exploitation tel qu'iOS ou Android). Le caractère unique du composant matériel, à savoir l'appareil enrôlé (*device-bounded*), n'est donc pas systématiquement assuré. Dans un scénario où les téléphones sont fournis et gérés par le responsable de traitement, ce dernier peut toutefois prendre des mesures pour que la consultation ne soit possible que sur le terminal lui-même.

Malgré ces limites, l'authentification multifacteur mobilisant l'OTP par SMS et un autre facteur (d'une catégorie distincte) permet d'assurer un **niveau de sécurité supérieur à l'authentification simple**. En cas de recours à ce type d'authentification multifacteur, le responsable de traitement doit s'assurer qu'elle est adaptée aux risques encourus.

Certains types d'informations contextuelles (telles que la localisation géographique de l'utilisateur, l'adresse IP du terminal, etc.), bien que susceptibles d'apporter des éléments de réassurance, ne peuvent pas, en principe, être considérés comme suffisants pour constituer des facteurs d'authentification.

L'authentification multifacteur reposant sur exactement deux facteurs de catégories distinctes est appelée **authentification à deux facteurs** (**2FA** pour *two-factor authentication* en anglais). Seul le terme authentification multifacteur sera employé dans la présente recommandation.

Par exemple, le paiement traditionnel par carte de paiement sur un terminal de paiement est conditionné à une authentification multifacteur. En effet, l'utilisateur doit être :

1) en possession de sa carte de paiement (qui est une carte à puce) ;
2) saisir son facteur de connaissance, à savoir le code PIN.

## 2.3. Notions connexes à distinguer de l'authentification multifacteur

Lorsqu'il est question d'authentification reposant sur une vérification séquentielle de deux facteurs, il ne s'agit pas forcément d'authentification multifacteur (si les deux facteurs sont de même catégorie) mais de **vérification en 2 étapes** (**2SV** pour *two-step validation* en anglais).

Par exemple une mire d'authentification qui demande la saisie d'un mot de passe puis d'un code reçu par mail est une vérification en 2 étapes et non une authentification multifacteur. En effet, un lien ou un code OTP transmis par courrier électronique ne peut être considéré comme un facteur de possession dans la mesure où il ne permet pas de prouver avec un niveau de confiance suffisamment élevé au vérifieur la possession d'un objet physique unique. En effet, il ne peut être supposé *a priori* que l'accès aux courriers électroniques d'une personne implique l'utilisation d'un facteur de possession car cette pratique ne peut pas, à ce jour, être considérée comme généralisée. La 2SV est donc hors du périmètre de cette recommandation.

[2] Recommandations relatives à l'authentification multifacteur et aux mots de passe , v2.0, p. 21, cyber.gouv.fr
[3] NIST Special Publication 800-63B, Digital Identity Guidelines, version du 02/03/2020, p. 17, nvlpubs.nist.gov

Enfin, l'authentification multifacteur ne doit pas être confondue avec l'**authentification cryptographiquement robuste**[4] qui, indépendamment du nombre ou des catégories de facteurs qu'elle implique, doit reposer « sur un mécanisme cryptographique dont les paramètres de sécurité sont jugés robustes » contre les principales attaques (écoute, rejeu, homme-du-milieu, manipulation/falsification).

Ainsi, plusieurs cas de figure existent :

- une authentification peut être cryptographiquement robuste et multifacteur. C'est par exemple le cas de l'authentification par carte à puce et code PIN ;
- une authentification cryptographiquement robuste n'est pas forcément multifacteur. C'est notamment le cas des solutions impliquant une **clé d'accès logicielle** (*passkey* en anglais, voir annexe I). Ces solutions pourraient être multifacteur dans le cas où la **clé d'accès logicielle** est associée à un terminal spécifique et verrouillé par code PIN ;
- une authentification multifacteur n'est pas forcément une authentification cryptographiquement robuste. C'est par exemple le cas de l'authentification par saisie d'un mot de passe et d'un code OTP reçu par SMS.

L'authentification cryptographiquement robuste n'est pas l'objet de cette recommandation.

## 2.4. Périmètre de la recommandation

Cette recommandation couvre l'étape de l'authentification utilisateur au sens strict. Elle n'a pas vocation à développer les autres phases ou processus importants liés à la gestion des identités et des accès, à savoir :

- la gestion du cycle de vie des identités numériques (enregistrement de l'utilisateur, création du compte et des informations associées, délivrance, activation et/ou enrôlement des facteurs d'authentification, suspension ou révocation de compte, réactivation ou renouvellement du compte, remplacement des facteurs d'authentification) ;
- la gestion d'annuaire avec les mécanismes de fédération d'identité qu'ils soient par exemple :
  - professionnels avec l'authentification unique (SSO pour *single sign-on* en anglais) ;
  - administratifs avec les téléservices nationaux d'identification et d'authentification électronique ;
  - liés à des comptes de médias sociaux via la fonctionnalité « se connecter avec » aussi connue comme *social login* en anglais

Elle n'a pas non plus vocation à couvrir les traitements en aval de l'authentification tels que l'**identification** (voir annexe) et la gestion de session utilisateur.

Plus spécifiquement, **cette recommandation se concentre sur l'usage de l'authentification multifacteur**, à savoir la mobilisation d'au moins deux facteurs d'authentification de catégories distinctes pour une authentification utilisateur. **Cette recommandation limite le champ d'application du facteur d'inhérence aux seules caractéristiques morphologiques.** La biométrie comportementale (par exemple, la frappe au clavier) et la biométrie biologique sont hors périmètre ; elles demeurent peu adoptées pour les solutions d'authentification multifacteur à date de publication.

Cette recommandation peut être utile aux responsables de traitements soumis à des textes comprenant des exigences liées à l'authentification multifacteur telles que eIDAS[5], PGSSI-S[6] ou DSP2[7].

---

[4] L'ANSSI lui préfère le terme **d'authentification forte** au chapitre 2 .5 des Recommandations relatives à l'authentification multifacteur et aux mots de passe, v2.0, cyber.gouv.fr

[5] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil 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 1999/93/CE, europa.eu

[6] Référentiel d'identification électronique des usagers et Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social [personnes physiques], esante.gouv.fr

[7] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE (Texte présentant de l'intérêt pour l'EEE), europa.eu

## 2.5 Données personnelles impliquées dans une authentification multifacteur

Les données à caractère personnel impliquées dans une authentification multifacteur sont généralement :

- les données du traitement d'identification, à savoir l'identifiant utilisateur, comme un numéro de compte attribué par le responsable de traitement, un pseudonyme choisi par l'utilisateur, une donnée personnelle préexistante utilisée comme identifiant (par exemple une adresse mail, un n° de téléphone) ou encore un identifiant technique si l'identifiant est géré par un service de tierce-partie de type fédération d'identité ;
- les données propres à l'authentification, qui diffèrent selon les catégories de facteur utilisées :
    - dans le cas de la connaissance : le mot de passe ou son **empreinte cryptographique** (voir annexe) en fonction du protocole retenu, le code confidentiel, etc. ;
    - dans le cas de la possession : l'élément secret, un identifiant du matériel enrôlé comme le numéro de téléphone portable, l'identifiant universel unique (UUID pour *universally unique identifier* en anglais) de téléphone, l'identifiant de carte réseau d'un appareil (adresse MAC pour *Media Access Control address* en anglais), et/ou les éléments techniques liés aux protocoles d'authentification (secret à usage unique comme un OTP ou une **graine** (voir annexe), certificats, défi-réponse, etc.) ;
    - dans le cas de l'inhérence : les **gabarits biométriques** (voir annexe) (ceux de référence et ceux calculés à la volée lors du contrôle pour comparaison) venant d'une empreinte digitale, faciale, etc. ;
- les données de journalisation des succès et échecs d'authentification multifacteur.

## 2.6 Authentification multifacteur et RGPD

L'authentification multifacteur est un ensemble d'opérations sur des données à caractère personnel (listées à la section précédente) comprenant la collecte des identifiants de comptes et facteurs d'authentification, la transmission ou non au système du vérifieur, la comparaison avec les valeurs de référence, etc. Elle peut donc, au titre de l'article 4.2 du RGPD, être qualifiée de traitement de données à caractère personnel.

Par rapport à une **authentification simple** (voir annexe), l'authentification multifacteur constitue une mesure de sécurité ayant pour objectif de réduire significativement la vraisemblance du risque d'accès non autorisés à des systèmes d'information, et *a fortiori* à des données à caractère personnel. Ainsi la finalité du traitement d'authentification multifacteur est la sécurisation de l'authentification utilisateur.

# 3. Comment respecter les obligations de protection des données personnelles ?

L'authentification multifacteur doit, comme tout traitement de données à caractère personnelle, respecter le RGPD. **À ce titre, il est nécessaire de mener préalablement à la mise en place d'une authentification multifacteur les actions suivantes,** développées dans les sections ci-après :

3.1. évaluer l'opportunité de mettre en place une authentification multifacteur ;
3.2. justifier d'une base légale pour le traitement d'authentification multifacteur ;
3.3. identifier une exception permettant l'usage du facteur d'inhérence le cas échéant ;
3.4. choisir la solution en prenant en compte les risques relatifs aux personnes concernées ;
3.5. qualifier les acteurs et préciser leurs obligations ;
3.6. minimiser la collecte de données ;
3.7. définir les modalités de conservation des données ;
3.8. documenter et encadrer les potentiels transferts de données ;
3.9. prévoir l'exercice des droits des personnes concernées ;
3.10. sécuriser l'authentification multifacteur.

## 3.1 Evaluer l'opportunité de mettre en place une authentification multifacteur

Comme toute mesure de sécurité, l'authentification multifacteur doit présenter un niveau de protection adapté au contexte et aux risques auxquels est exposé le traitement dont elle conditionne l'accès. Le responsable de traitement pourra choisir cette mesure au moyen d'une analyse de risque intégrant, entre autres, les contraintes du cadre réglementaire et normatif en vigueur. Pour cette analyse le responsable de traitement prend en considération ses objectifs de sécurité en termes de disponibilité, d'intégrité et de confidentialité. En plus des domaines d'impact classiques (financier, image, etc.), une attention particulière devra être portée à l'impact sur les personnes (sécurité et santé, vie privée, droits et libertés, etc.), tant pour les personnes dont les données sont traitées que pour les utilisateurs des services à sécuriser.

Pour les traitements de données sensibles, au sens de l'article 9 du RGPD (par exemple le traitement de données de santé), et les traitements ou les opérations à risque pour les personnes concernées (sans qu'il ne soit nécessaire d'atteindre la criticité du risque élevé au sens de l'article 35 du RGPD tels que précisés dans les lignes directrices du CEPD [8]), la CNIL recommande le recours à l'authentification multifacteur. L'administration systèmes et réseaux, la connexion au système d'information de l'employeur établie depuis l'extérieur du réseau de l'organisme ou, en général, l'accès à une messagerie électronique professionnelle sont des traitements pour lesquels la CNIL recommande de mettre en œuvre l'authentification multifacteur. De fait, si l'accès à ces traitements et opérations est compromis cela a généralement un impact notoire sur les personnes concernées - que ce soient les personnes sur lesquelles portent les données à caractère personnelles (par exemple violation du secret médical pour les patients) ou les accédants au service (par exemple usurpation d'identité des employés, usagers, clients, etc. permettant de faire des actions en leur nom).

Dans tous les cas, il est nécessaire de concilier la sécurité apportée par l'authentification multifacteur et les conséquences qu'elle pourrait engendrer pour les utilisateurs concernés (notamment la dissuasion d'accès au service, la collecte de données supplémentaires, l'impossibilité ponctuelle ou permanente de mobiliser un des facteurs, etc.). Ainsi, pour les traitements ou opérations à faible risque, il convient de permettre l'usage de l'authentification multifacteur, sans l'imposer, ce qui permet d'avoir un impact positif sur les droits des utilisateurs.

Par ailleurs, il conviendra de veiller à prendre en compte les questions d'accessibilité au numérique de certaines populations spécifiques lors de cette analyse.

La mise en place d'une solution d'authentification multifacteur participe au respect de l'obligation de sécurisation, en application des articles 5.1.f et 32 du RGPD, sans qu'il ne puisse toutefois être considéré que ces articles imposent systématiquement d'utiliser une telle modalité. En effet, le recours à l'authentification multifacteur ne doit pas être considérée comme une mesure de sécurité générale et systématique. La banalisation de l'usage de cette solution dans des contextes qui ne le nécessitent pas (par exemple pour une plateforme de réservation de terrain de tennis) peut engendrer une perte de vigilance des utilisateurs (voir Exemple #6 : Des mesures contre la lassitude liée à la MFA), ce qui peut réduire son efficacité dans les contextes où elle est nécessaire.

## 3.2 Justifier d'une base légale pour le traitement d'authentification multifacteur

En pratique, deux cas de figure différents peuvent se présenter. Dans le premier cas, l'authentification multifacteur peut être une mesure de sécurité, au sens de l'article 32 du RGPD, rattachée au traitement principal. Dans ce cas, la fonction d'authentification multifacteur suit la base légale du traitement principal, et n'a pas besoin d'avoir une base légale propre. Dans le second cas, le responsable de traitement peut mettre en œuvre une authentification multifacteur comme une brique de sécurité transversale et commune aux applications de son système d'information. Dans une telle hypothèse, la CNIL recommande de la considérer comme un traitement en propre avec une finalité de sécurisation des systèmes d'information. La présente recommandation a vocation à s'appliquer à ces deux types de situations.

[8] Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 adoptées le 4 octobre 2017, cnil.fr

Quelle que soit l'analyse juridique retenue par le responsable de traitement, l'authentification multifacteur repose donc sur une base légale au sens de l'article 6 du RGPD. Cette base légale peut notamment être :

- l'obligation légale s'il existe une disposition imposant une authentification multifacteur. Il est important de souligner ici que cette base légale n'est mobilisable que pour des textes prévoyant cette obligation de manière explicite. En particulier, les articles 5.1.f et 32 du RGPD qui prévoient une obligation de sécurité n'engendrent pas à eux-seuls une obligation légale de mettre en place une authentification multifacteur dans le cadre de traitements de données à caractère personnel ;

- l'intérêt légitime du responsable de traitement pour garantir la sécurité de ses systèmes d'information. C'est la base légale la plus commune pour mener des opérations de sécurité informatique impliquant le traitement de données personnelles. Dans ce cas le responsable de traitement doit veiller à mettre en balance son intérêt propre avec les intérêts ou libertés et droits fondamentaux des personnes concernées ;

- le consentement des personnes concernées, par exemple lors de la souscription et de l'utilisation de services en ligne Si cette base légale est mobilisée, le responsable de traitement doit prévoir une alternative[9] et prendre en compte ses implications en termes de protection de la vie privée. Cette base légale est donc moins adaptée aux opérations de sécurité. Il est à noter que cette base légale ne peut pas, en règle générale, être mobilisée dans le cadre d'une relation de travail.

**Choix de base légale dans le contexte professionnel**

Dans le contexte professionnel, l'existence du lien hiérarchique entre l'employeur et ses subordonnés crée de fait un déséquilibre dans les relations susceptible d'affecter le caractère libre du consentement. Dès lors, le consentement ne peut que rarement être retenu en tant que fondement juridique d'un traitement de données sur le lieu de travail, sauf à garantir le respect de son caractère libre, spécifique et éclairé. L'une de ces garanties implique notamment l'existence d'alternatives, accessibles sans contraintes.

Ainsi, en l'absence d'obligation légale (article 6.1.c), **la base légale la plus adaptée dans le contexte professionnel apparaît être celle de l'intérêt légitime de l'employeur** (article 6.1.f du RGPD). Cette base légale, qui exige une mise en balance des droits, des intérêts et des libertés respectifs de l'employeur et de l'employé, est étroitement liée au sujet de la minimisation des données traitées.

Concernant l'inscription au registre des activités du responsable de traitement, tel que prévu par l'article 30 du RGPD, la CNIL considère que celle-ci peut être réalisée de manière alternative au sein de l'entrée du registre relative au traitement auquel l'authentification multifacteur est adossée, ou bien dans une entrée spécifique du registre dans le cas d'une authentification multifacteur transversale et commune à différentes opérations de traitement.

## 3.3 Identifier une exception permettant l'usage du facteur d'inhérence le cas échéant

Le RGPD qualifie les données biométriques de sensibles lorsqu'elles visent à identifier une personne physique de manière unique : leur traitement est par conséquent interdit sauf à bénéficier de l'une des exceptions prévues par l'article 9 du RGPD.

Dans ce contexte, **la CNIL estime que le recours à la biométrie n'est possible qu'avec l'exception fondée sur le consentement des personnes** (article 9.2.a), sauf si une norme juridique le rend obligatoire ou autorise explicitement son utilisation. Tel est par exemple le cas du règlement type relatif à l'accès par authentification biométrique sur les lieux de travail, pris sur le fondement de l'article 44 de la loi « Informatique et Libertés » qui permet aux employeurs de mettre en place des dispositifs de contrôle d'accès basés sur l'utilisation d'un facteur inhérent morphologique en en encadrant strictement les modalités.

[9]Le consentement doit être libre, spécifique, éclairé et univoque : il ne doit donc être ni contraint ni influencé. La personne doit se voir offrir un choix réel, sans avoir à subir de conséquences négatives en cas de refus.

Les deux conditions – l'existence d'une base légale au sens de l'article 6.1 du RGPD et l'existence d'une exception permettant de traiter des données sensibles au sens de l'article 9 du RGPD sont bien distinctes : il est donc possible pour un dispositif d'authentification multifacteur ayant recours au facteur inhérent d'être fondé sur une base légale autre que le consentement (par exemple, l'intérêt légitime) lorsque l'exception mobilisée permettant de traiter des données sensibles est celle du consentement des personnes concernées.

## 3.4 Choisir la solution en prenant en compte les risques relatifs aux personnes concernées

En vertu de l'article 25 du RGPD, le responsable de traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir la protection des données dès la conception et par défaut.

Ainsi, la CNIL recommande de privilégier l'authentification multifacteur **basée sur des facteurs de connaissance et de possession** lorsque cela est possible, en particulier dans le cadre professionnel.

L'usage d'un **facteur inhérent** entraîne des risques spécifiques pour les personnes ; par conséquent, son usage devrait être entouré de précautions particulières. Sans préjudice d'autres dispositions, il est recommandé de manière générale de proposer une alternative au facteur inhérent (par exemple un facteur de possession) aux utilisateurs, notamment dans un cadre professionnel.

Il faut également noter que le choix d'un facteur d'authentification des catégories inhérence ou possession, dans le cadre professionnel, peut avoir des conséquences négatives s'agissant de la protection de la vie privée, notamment si la mise en place du facteur d'authentification repose sur des équipements personnels de la personne concernée (voir Section 3.6) ou des facteurs relevant de ses comptes à usage privé. Il sera, dans ce dernier cas, nécessaire d'accorder une attention particulière à la mise en balance de l'intérêt de l'employeur avec les intérêts ou libertés fondamentaux de l'employé. Ces conséquences négatives peuvent aussi se traduire par une moindre maîtrise de la sécurité du dispositif par le responsable de traitement dont ce dernier devra aussi tenir compte dans son évaluation du dispositif.

De manière générale, le responsable de traitement devra prendre en compte les impacts en termes de respect de la vie privée induits par le facteur de possession envisagé. Par exemple, un code OTP envoyé par SMS repose sur la collecte par le vérifieur du numéro de téléphone portable de l'utilisateur, ce qui est potentiellement plus intrusif que l'usage d'une application de **OTP** (voir annexe) dédiée ne reposant que sur le partage d'une graine.

Le responsable de traitement devra prendre en compte, lors du choix de la solution d'authentification multifacteur, le risque d'accès empêché (*lockout* en anglais) lié à l'oubli, au vol ou à la perte du composant matériel dans le cas d'un **facteur de possession**, et mettre en place les mesures organisationnelles et techniques appropriées, sans que le processus de réémission d'un nouveau facteur n'affaiblisse la sécurité.

**Exemple #1 : Une application mobile de TOTP déverrouillée par code PIN**

De nombreuses solutions d'authentification multifacteur utilisent comme facteur de possession une application mobile de TOTP, basé sur la synchronisation temporelle entre le serveur d'authentification et l'application fournissant l'OTP.

Le vérifieur (responsable de traitement de l'authentification) n'a pas toujours la possibilité de maîtriser la sécurité du mobile et donc de l'accès à l'application. Pour réduire le risque d'usurpation d'identité par vol du mobile, l'application vérifie en local que la personne est l'utilisateur légitime, par le contrôle d'un code PIN, avant de générer la preuve de possession : le code à usage unique (OTP). L'utilisateur saisit alors l'OTP sur la mire d'authentification et le vérifieur en réalise la vérification.

**Protection dès la conception**

Dans cet exemple, le facteur de possession est déverrouillé par l'autre facteur. L'entité qui vérifie les preuves d'identité n'a alors pas besoin de rapatrier les données liées au facteur de connaissance qui restent traitées localement. La solution minimise les données qui transitent lors de l'authentification à des données purement techniques :

- l'identifiant du compte utilisateur ;
- l'horodatage ;
- la preuve de possession (l'OTP). Cet élément de preuve est collecté mais seul le verdict (« succès » ou « échec ») doit être conservé dans les traces de journalisation.

D'un point de vue sécurité, la notion de déverrouillage permet d'atténuer le risque d'usurpation d'identité lié à la perte ou au vol du matériel : celui-ci est inutilisable sans l'autre facteur. Cependant, en cas de découverte d'une vulnérabilité du composant de sécurité du matériel, l'effet peut être similaire à celui d'une compromission des deux facteurs. C'est pourquoi, dans les solutions multifacteur où seul le facteur de possession est directement vérifié, le composant de sécurité doit impérativement présenter des garanties de robustesse suffisantes.

L'usage d'un **facteur inhérent** d'authentification, à savoir l'usage de données biométriques aux fins d'identifier une personne physique de manière unique, est, sauf en cas d'exemption domestique, soumis, en tant que traitement de données sensibles, au respect de l'une des conditions de l'article 9.2 du RGPD et en particulier au consentement de la personne.

Lorsque ce traitement biométrique est réalisé par une personne physique dans le cadre d'une activité strictement personnelle ou domestique conformément à l'article 2.2 du RGPD, il n'est pas soumis aux obligations de protection des données. Cela peut être le cas lorsqu'il s'agit d'un **usage privé, pour accéder à un service à des fins personnelles, et que le gabarit est stocké dans l'appareil, sous le seul contrôle du particulier**.

Pour le cas particulier de l'authentification reposant sur un traitement de données biométriques pour le contrôle d'accès aux appareils et aux applications utilisés **dans le cadre des missions professionnelles**, le responsable de traitement devra prendre en compte les dispositions du règlement type relatif à l'accès par authentification biométrique sur les lieux de travail. Il sera alors nécessaire de documenter et de pouvoir justifier du besoin d'une authentification basée sur la biométrie lorsqu'elle est mise en œuvre par un responsable de traitement, par rapport à d'autres mécanismes d'authentification moins intrusifs.

En outre, la CNIL recommande que les gabarits biométriques de référence ne soient stockés que sur des dispositifs sous le contrôle exclusif des personnes concernées.

**Exemple #2 : Une authentification relevant de l'exemption domestique basée sur un facteur d'inhérence**

Un fournisseur de service en ligne, tel qu'un service de messagerie personnelle en ligne, peut proposer à ses clients d'utiliser une authentification multifacteur en mettant en avant la sécurité offerte vis-à-vis de risques de vol de comptes et d'usurpation d'identité.

Le fournisseur du service veut proposer de renforcer l'authentification simple par une authentification multifacteur avec facteur biométrique. En pratique, le fournisseur introduit une option activable par les

utilisateurs, sans que ce choix n'entraîne de restriction sur les services fournis à l'usager. En effet, **le recours à la biométrie ne peut être imposé sans alternative.**

Le fournisseur d'un service peut dès lors proposer de recourir à un dispositif qui effectue **la lecture-comparaison des données biométriques localement** sur l'ordiphone (*smartphone* en anglais) personnel de l'utilisateur. Ce dispositif conserve le gabarit biométrique de référence dans le composant de sécurité[10] de l'appareil sans qu'il ne soit traité pour une autre finalité que l'authentification. Dans un tel cas, la vérification du facteur d'inhérence elle-même peut entrer dans l'exemption domestique inscrite à l'article 2.2.c du RGPD. Ainsi, le fournisseur du service en ligne n'est pas considéré comme responsable du traitement de données biométriques, ce dernier n'ayant pas accès aux gabarits biométriques.

Le responsable de traitement pourra en outre se référer à la précédente communication de la CNIL dédiée au cas du recours aux systèmes d'authentification reposant sur des équipements personnels relevant de l'exemption domestique.

Dans le cas où un facteur d'inhérence est mobilisé, cette modalité, qui allège la responsabilité du fournisseur, est à privilégier dans la mesure où elle réduit l'atteinte à la vie privée des usagers.

## 3.5 Qualifier les acteurs et préciser leurs obligations

Un organisme qui déploie une solution d'authentification multifacteur au sein de son système d'information est en principe seul responsable du traitement.

L'organisme qui décide de recourir à un fournisseur d'authentification multifacteur en mode *SaaS* sera en principe qualifié de responsable de traitement, tandis que le fournisseur de la solution en mode *SaaS* agira, en principe, en tant que sous-traitant. Pour rappel les acteurs qui vendent un produit sans prestation de service associée (par exemple de déploiement d'une solution standard en propre chez le responsable de traitement) ne sont pas, en principe, concernés par les dispositions de sous-traitance du RGPD. Ils peuvent alors être considérés comme des tiers au traitement[11], n'ayant aucun accès aux données à caractère personnel.

La sous-traitance doit être encadrée par un contrat liant l'organisme client qui commande l'opération (le responsable du traitement) et l'entreprise prestataire qui met en œuvre celle-ci (le sous-traitant). Le responsable devra être vigilant sur les « *garanties suffisantes* » apportées par le sous-traitant en vertu de l'article 28.1 du RGPD. Le contrat de sous-traitance devra contenir *a minima* les clauses prévues à l'article 28.3 du RGPD.

**Exemple #3 : Un jeton matériel**

Un jeton est un composant matériel porteur d'une partie des éléments secrets contribuant au processus d'authentification. Le jeton affiche un mot de passe à usage unique pendant une durée limitée. Côté serveur, chaque mot de passe n'est accepté qu'une fois. La synchronisation entre le jeton et le serveur, qu'il soit sous le contrôle du responsable de traitement ou sous celui du fournisseur de solution, est établie *ab initio*. Dans ce cas de figure, le fournisseur de jeton n'est pas considéré comme sous-traitant au sens du RGPD, car aucun échange de données à caractère personnel n'est nécessaire.

**Exemple #4 : Une application TOTP installée sur un terminal professionnel**

Cette solution est pertinente pour mettre en place, en plus du mot de passe (connaissance), un second facteur d'authentification lié à un terminal mobile (possession) confié par l'employeur. Une application est installée par l'employeur sur le terminal et activée par ses soins. Celle-ci permet de générer, sur demande du possesseur uniquement, un code à usage unique. La synchronisation permettant de générer les codes à usage unique est opérée *ab initio* entre le terminal et un serveur TOTP sous le contrôle de l'employeur (sans que le fournisseur de la solution ne traite ni n'accède aux données). L'application elle-même n'effectue pas d'échange de données avec un tiers dans son fonctionnement courant. Dans ce cas de figure, le fournisseur de la solution de TOTP n'est ni responsable de traitement ni sous-traitant au sens du RGPD.

[10] Recommandations relatives à l'authentification multifacteur et aux mots de passe, v 2.0, p37, cyber.gouv.fr
[11] Tiers est ici utilisé au sens commun du terme et non au sens défini à l'Art. 4(10) du RGPD.

**Exemple #5 : Un service d'authentification multifacteur en mode SaaS**

Cette solution consiste à recourir à un fournisseur de service tiers qui contrôle les preuves fournies par les utilisateurs au moment de leur authentification. Dans ce cas de figure, le fournisseur hérite de la qualification de sous-traitant au regard du RGPD. Le responsable de traitement, dans le cadre de ses obligations, devra être particulièrement vigilant aux aspects suivants :

- vérifier (et idéalement auditer) les garanties de sécurité offertes par le prestataire, en termes de confidentialité, d'intégrité et de disponibilité ;
- prendre en compte les risques spécifiques liés à l'enregistrement et à la journalisation des flux d'authentification par le prestataire ;
- veiller au bon encadrement d'éventuels transferts de données personnelles hors de l'Union européenne, qui peuvent concerner les flux d'authentifications eux-mêmes et également tout service périphérique, concernant par exemple la sécurité ou la performance du dispositif ;
- vérifier l'existence d'éventuels sous-traitants de second rang et les engagements de ces derniers vis-à-vis des points ci-dessus.

## 3.6 Minimiser la collecte de données

En vertu du principe de minimisation des données, le responsable de traitement doit s'assurer que les données collectées, stockées et traitées pour l'authentification sont bien nécessaires à la fourniture du service.

**Utilisation de l'équipement privé d'un employé**

L'utilisation de l'équipement privé d'un employé soulève des questions ayant trait à la fois à la législation du travail qui encadre les relations de travail (1) et au RGPD (2).

**(1) La législation du travail**

La législation du travail prévoit que les employeurs doivent, par principe, fournir aux employés les moyens et outils dont ils ont besoin pour accomplir leur travail, notamment pour accéder au système d'information. Tel serait par exemple le cas d'un jeton matériel remis par l'employeur au salarié (composant USB dédié, composant matériel muni d'écran affichant un code à usage unique, carte à puce, etc.).

Par dérogation à ce principe, le recours aux matériels et équipements personnels des salariés (notamment pour mettre en place des procédures d'authentification) est dans certains cas possible. Il appartient alors aux employeurs de s'assurer de leur conformité au droit du travail et d'intégrer dans cette réflexion la question d'égalité de traitement et d'existence d'alternatives pour les employés ne possédant pas d'appareils personnels compatibles, ou ne souhaitant pas, pour des raisons personnelles, les utiliser à des fins professionnelles.

**(2) Le régime général résultant du RGPD**

Dans le cas où les conditions issues de la législation du travail sont satisfaites, l'employeur devra veiller au respect de l'ensemble des règles générales du RGPD, particulièrement sur deux points spécifiques.

***a) Minimisation des données***

Conformément à l'article 5.1.c du RGPD, les données traitées doivent être « (…) limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ».

En prenant l'exemple d'un facteur de possession tel que le téléphone mobile personnel d'un employé, on constate qu'il existe plusieurs manières de l'utiliser à des fins d'authentification de l'employé.

- L'une d'elles pourrait reposer sur l'envoi d'un SMS OTP, cette option-là nécessitant, pour l'employeur, de connaître et d'utiliser le numéro de téléphone de l'employé.
- Une autre manière consiste à installer sur le terminal de l'employé une application de TOTP qui stockera une clé fournie par l'employeur pour afficher ensuite les codes OTP à la demande de l'employé. Dans cette seconde option et contrairement à la précédente, l'employeur n'a pas à collecter ni à utiliser le numéro de téléphone du salarié.

La seconde option nécessitant moins de données, elle devrait pour cette raison être privilégiée en vertu du principe de minimisation. Le choix, par l'employeur, de l'application de TOTP à utiliser doit privilégier les solutions ne procédant à aucune collecte des données personnelles de l'utilisateur (par exemple, à des fins publicitaires, etc.).

***(b) Protection des données par conception et mesure de sécurité***

Enfin, le RGPD impose à l'employeur des obligations en matière de sécurité des données traitées, notamment dans ses articles 5.1.f, 25 et 32.

Ainsi, l'employeur doit mettre en place des « mesures techniques et organisationnelles appropriées », à même de garantir le respect des principes du RGPD en fonction des risques encourus par les personnes concernées. Ces mesures devraient en particulier comprendre un cloisonnement des données traitées par l'application TOTP, d'une part, et des autres données personnelles de l'employé, d'autre part, sur son équipement privé. Par ailleurs, la CNIL rappelle au responsable de traitement la nécessité d'inclure dans son analyse les risques présentés par l'usage d'un équipement personnel dont il n'a pas la maîtrise physique ou juridique[12].

Les modalités de transmission de la graine à l'application doivent aussi être prises en compte ; il est préférable d'utiliser un canal direct comme un code-barres à deux dimensions (tel qu'un QR-code) généré par l'employeur et affiché par un dispositif sous son contrôle, plutôt qu'une transmission d'une graine sous forme d'un fichier via une connexion filaire ou sans fil « traditionnelles ».

[12] Guide de la sécurité des données personnelles version 2024, p20, cnil.fr

## 3.7 Définir les modalités de conservation des données

Pour rappel, seules sont considérées ici les données liées à l'authentification. Les informations en lien avec les autres étapes d'une gestion de compte et les processus annexes de gestion d'identité et des accès ne sont pas couverts.

Les données d'authentification seront conservées par le vérifieur de façon sécurisée et pour une durée appropriée au regard des risques, sans excéder la durée de vie du compte utilisateur. Les responsables de traitement peuvent se référer :

- à la recommandation « mots de passe » pour les modalités de conservation des données liées aux facteurs de connaissance ;
- au règlement type relatif à l'accès par authentification biométrique sur les lieux de travail pour les modalités de conservation des données relatives à la biométrie dans le cadre professionnel. Pour les usages dans le cadre personnel (contractuel, administratif, etc.), une attention particulière devra être portée aux durées et modalités de conservation des gabarits biométriques de référence.

Les modalités de conservation des données relatives aux facteurs de possession dépendent de la technologie employée (par exemple, l'OTP n'est pas conservé après utilisation, alors que les certificats sont conservés jusqu'à expiration ou révocation).

Les traces de journalisation des systèmes d'authentification doivent être conservées pour une durée limitée. La prise en compte de dispositions spécifiques au contexte d'usage peut amener à fixer des durées de conservation particulières, liées aux caractéristiques des traitements, telles que le règlement type relatif à la biométrie sur les lieux de travail, des obligations règlementaires, ou une utilisation à des fins de contrôle interne ou plus généralement de sécurité en raison de l'importance du risque pour les personnes en cas de détournement de finalité par exemple. En cas d'absence de dispositions particulières, il est recommandé de se référer à la recommandation journalisation de la CNIL, qui préconise dans le cas général une durée de conservation de 6 à 12 mois.

Dans tous les cas, les données biométriques et les informations secrètes, telles qu'une empreinte cryptographique de mot de passe ou un OTP, ne devront pas faire partie du contenu des journaux. Aussi seul le résultat « succès » ou « échec » devra être tracé, sans jamais l'associer aux informations secrètes.

## 3.8 Documenter et encadrer les potentiels transferts de données

Le déploiement d'une solution d'authentification multifacteur est susceptible d'entraîner des transferts vers des pays tiers qui doivent être effectués dans le respect de la réglementation existante. Ce cas de figure est particulièrement vraisemblable lorsque la solution d'authentification repose sur des services en mode *SaaS*, même si le service principal offert par le responsable de traitement est hébergé sur le territoire de l'Union européenne.

De manière générale, il est recommandé au responsable de traitement d'apporter une attention particulière aux flux de données engendrés par l'authentification multifacteur ainsi qu'à son éventuelle soumission à des lois extra-européennes et, le cas échéant, de bloquer tout flux non nécessaire à la fourniture du service.

## 3.9 Prévoir l'exercice des droits des personnes concernées

Les droits des personnes concernées dépendront de la base légale retenue par le responsable de traitement.

L'information des personnes concernées devra être prévue conformément aux articles 13 et 14 du RGPD. En pratique, pour la sécurisation d'un traitement contribuant à la mise en conformité à l'exigence de l'article 32 du RGPD, la CNIL fait preuve d'une certaine souplesse dans les modalités d'application des obligations d'information. En particulier, si plusieurs utilisations des données sont faites à des fins de sécurité (authentification, journalisation, chiffrement, etc.), la finalité indiquée peut être désignée comme, de façon générale, la sécurisation du traitement, sans avoir à détailler les différents moyens de sécurité employés lorsqu'elles ne relèvent pas des articles 9 (traitement de données sensibles) ou 35 (traitement relevant d'une analyse d'impact relative à la protection des données) du RGPD.

Cette information peut être précisée à différentes étapes de la gestion du compte dont l'accès est conditionné à une authentification multifacteur :

- lors de l'inscription de la personne, c'est-à-dire lors de la création du compte et des informations associées (possibilité d'intégrer cette information dans la politique de protection des données) ;

- lors de la délivrance ou lors de l'activation des facteurs d'authentification (comme par exemple l'enrôlement d'un facteur de possession) ;
- lors de l'usage pour s'authentifier proprement dit. Une telle information des personnes concernées pourra par exemple se matérialiser par un lien vers une notice d'information complète présentée sous forme de menus dépliants pour ne pas surcharger la personne d'informations tout en faisant apparaître clairement les moyens d'accéder à l'information recherchée ;
- lors de la suspension ou de la révocation du compte ;
- lors de la réactivation ou du renouvellement du compte ou bien lors du remplacement des facteurs d'authentification.

## 3.10 Sécuriser l'authentification multifacteur

Les mesures de sécurité pouvant être mise en œuvre pour l'authentification multifacteur sont fortement corrélées à la solution choisie et aux catégories de facteurs mobilisées.

Pour les solutions faisant intervenir un facteur de connaissance, le responsable de traitement devra respecter la recommandation « mots de passe » de la CNIL dédiée à ce sujet.

Pour les solutions faisant intervenir un facteur de possession, la CNIL recommande au responsable de traitement de veiller à ce que ces solutions :

- soient basées sur des protocoles de vérification de preuves cryptographiquement robustes[13] ;
- fassent intervenir des preuves de possession dynamiques (pour garantir une vérification systématique de l'authenticité du dispositif matériel).

Enfin, pour les solutions faisant intervenir un facteur d'inhérence, le responsable de traitement devra prendre en compte les performances (notamment les taux de fausse acceptance pour les accès non autorisés et de faux rejet pour les accès empêchés) en fonction du contexte d'usage, ainsi que la robustesse aux **attaques par présentation**.

S'agissant de la sécurisation de l'authentification multifacteur, il est aussi possible de se référer au guide de l'ANSSI *Recommandations relatives à l'authentification multifacteur et aux mots de passe*[14] pour identifier et mettre en œuvre d'autres mesures de sécurité dont notamment « R11 Réaliser l'authentification au travers d'un canal sécurisé » et « R39 Utiliser un facteur de possession intégrant un composant de sécurité qualifié ou certifié. ».

La CNIL recommande que toute opération d'administration ou de gestion d'une solution d'authentification multifacteur soit conditionnée à une authentification multifacteur ayant elle-même au moins la même robustesse, afin d'assurer un niveau de sécurité cohérent.

Il conviendra de prendre en compte les impacts sur les personnes concernées dans le choix et l'implémentation de ces mesures de sécurité.

[13] Recommandations relatives à l'authentification multifacteur et aux mots de passe, v2.0, chapitre 2.5, cyber.gouv.fr
[14] Recommandations relatives à l'authentification multifacteur et aux mots de passe, v2.0, cyber.gouv.fr

**Exemple #6 : Des mesures contre la lassitude liée à la MFA**

De nombreuses applications d'authentification multifacteur utilisent des notifications *push* afin d'améliorer l'expérience utilisateur. La cinématique de connexion est la suivante :

1. L'utilisateur saisit son identifiant et son mot de passe sur la mire d'authentification ;
2. Il reçoit une notification *push* sur son mobile enrôlé ;
3. Il clique dessus pour ouvrir l'application et valider la demande, ce qui déclenche le mécanisme cryptographiquement robuste d'authentification (défi-réponse entre le composant sécurisé du téléphone et le serveur d'authentification).

Si un attaquant a réussi à récupérer le mot de passe de l'utilisateur, il peut réaliser l'étape 1. Dès lors, l'utilisateur légitime reçoit sur son mobile une notification non sollicitée.

En pratique la plupart des utilisateurs refusent les notifications d'authentification dont ils ne sont pas à l'origine. Néanmoins, si l'attaquant réitère l'opération plusieurs fois avec insistance, l'utilisateur pourrait finir par en accepter une, par agacement de la répétition ou par manque d'attention. Cette attaque est nommée « lassitude liée à la MFA », aussi connue comme *MFA fatigue*.

**Il existe différentes mesures pour réduire ce risque d'attaque par *MFA fatigue* :**

- l'affichage à l'utilisateur d'informations contextuelles complémentaires comme l'emplacement géographique, le type de terminal et l'horaire de la dernière tentative de connexion, ce qui facilite la détection par l'utilisateur légitime des tentatives de connexion frauduleuses ;
- la limitation de la fréquence des notifications *push* (par exemple : pas plus d'un certain nombre de notifications, ou de tentatives, par minute) ;
- la correspondance de numéros (*match number* en anglais) ou de symboles consistant à utiliser l'application mobile d'authentification, sur laquelle l'utilisateur est déjà authentifié par ailleurs, en lui demandant de confirmer le code affiché.

# Annexe : définitions

Notons que les définitions déjà formalisées dans le corps de la recommandation ne sont pas reprises dans cette annexe :

- **Authentification multifacteur**
- **Facteur d'authentification** (facteur de connaissance, facteur de possession, facteur d'inhérence)
- **Authentification à deux facteurs**
- **Authentification cryptographiquement robuste**
- **Vérification en 2 étapes** (2SV pour *two-step validation*)

**Identification :** « L'authentification utilisateur est précédée par une phase d'identification (parfois implicite) qui consiste, pour [l'utilisateur], à annoncer son identité sans prouver cette dernière. Par exemple, il peut s'agir d'un nom d'utilisateur à renseigner »

Source : Recommandations relatives à l'authentification multifacteur et aux mots de passe, v2.0, p. 8, cyber.gouv.fr

**Vérifieur :** Le vérifieur s'assure de la validité de l'identité de l'utilisateur au moyen des facteur d'authentification. Il s'agit par exemple pour le vérifieur de contrôler l'exactitude du mot de passe saisi par l'utilisateur.

**Appareil enrôlé :** Appareil associé avec un compte utilisateur auprès du vérifieur

**Composant de sécurité :** Un composant de sécurité est un composant physique indépendant, équipé d'un contrôleur dédié et d'une mémoire protégée, destiné à effectuer des opérations sensibles dans un environnement de confiance. Les cartes à puce sont des exemples de facteurs de possession possédant un composant de sécurité intégré.

Source : Recommandations relatives à l'authentification multifacteur et aux mots de passe, v2.0, p. 37, cyber.gouv.fr

**OTP :** L'acronyme OTP signifie *One-Time Password* ou *One-Time PIN*, mot de passe ou code à usage unique en français. C'est un code ou un mot de passe défini dynamiquement qui n'est valable que pour une session ou une transaction sur un système informatique. Il existe plusieurs protocoles OTP tels que :

- TOTP (pour *Time-based OTP*), basé sur la synchronisation temporelle entre le serveur d'authentification et le matériel ou l'application fournissant l'OTP ;
- HOTP (pour *HMAC-based OTP*), basé sur un compteur et HMAC, un algorithme de hachage cryptographique à clé secrète ;
- OCRA (pour *OATH Challenge-Response Algorithm*), basé sur un mécanisme de défi-réponse.

**Clé d'accès logicielle** (*passkey*) **:** Il s'agit d'une paire unique de clés privée et publique, générée dans un dispositif matériel ou logiciel (**jeton**) lors de l'inscription à un service en ligne. La clé privée est conservée de manière sécurisée dans ce dispositif sur un ou plusieurs terminaux de l'utilisateur et synchronisée dans un environnement cloud. La clé publique est enregistrée auprès du service en ligne. Chaque clé d'accès est liée à un compte utilisateur pour lequel elle a été générée.

**Empreinte cryptographique :** Une empreinte cryptographique, aussi appelée haché ou condensat, est le résultat d'une fonction de hachage cryptographique (comme les familles SHA2 ou SHA3).

**Gabarit biométrique :** Résultat du traitement de l'enregistrement brut (photographie, enregistrement audio, etc.) de la caractéristique biométrique par un algorithme rendant impossible la reconstitution de celle-ci. Les gabarits constituent des données biométriques dérivées et doivent ainsi être distinguées des données dont sont issues les caractéristiques biométriques.

Source : Règlement type relatif à l'accès par authentification biométrique sur les lieux de travail, Article 1, CNIL.

**Authentification simple :** Authentification reposant sur un seul facteur, le plus souvent un mot de passe

**Graine :** Donnée utilisée en entrée d'une fonction cryptographique concourant à l'aléa en sortie. Dans le cadre d'un protocole **OTP**, des graines différentes garantissent, idéalement que des codes **OTP** différents sont générés.

**Attaque par présentation :** Présentation d'un artefact ou de caractéristiques humaines à un système biométrique dans l'intention d'influer illégitimement sur son verdict.