Projet de recommandation

RELATIVE À L'AUTHENTIFICATION MULTIFACTEUR

Version soumise à consultation publique

jusqu'au : 31/05/2024

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

1.Introduction

L'authentification multifacteur a pour objectif de prévenir la compromission de ressources informatiques en demandant plus qu'un simple mot de passe, pour en conditionner l'accès. Les organismes qui souhaitent y recourir, ainsi que les fournisseurs de solutions d'authentification multifacteur eux-mêmes, doivent respecter certaines règles, notamment le règlement général sur la protection des données (RGPD) et les réglementations sectorielles qui leurs sont applicables.

2.Périmètre de la recommandation

La présente recommandation détaille les préconisations 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, et promeut 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 toutefois pas couvrir de manière exhaustive tous les cas d'usages dans lesquels l'authentification multifacteur est susceptible d'intervenir.

2.1. À qui s'adresse cette recommandation ?

Cette recommandation vise à rappeler le droit applicable et à guider les professionnels dans leur démarche de conformité à la réglementation relative à la protection des données. Elle s'adresse aux professionnels de tous secteurs. Cette recommandation s'adresse particulièrement aux délégués à la protection des données (DPD), 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 personnelles. Elle a notamment vocation à aider 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. Les obligations et recommandations pratiques découlant de ces qualifications sont détaillées dans les parties dédiées à chaque acteur. Toutefois, chaque acteur est invité à se référer non seulement aux recommandations qui le concernent mais également à celles s'adressant à ses partenaires, celles-ci étant susceptibles 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** (*multi-factor authentication*), 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**[1] (ce que la personne sait) : un secret à mémoriser, par exemple une **phrase de passe** (*passphrase*), un mot de passe ou un code confidentiel ;
- un **facteur de possession** (ce que la personne a) : un moyen de conserver des secrets non mémorisables par un humain, par exemple une carte à puce, un dispositif USB contenant une clé privée, un élément matériel (jeton ou *hard token*) ou une application (*soft token*) permettant de générer des codes à usage unique (basés sur un protocole de type **OTP**), une **clé d'accès logicielle** (*passkey*), ou encore une **carte de clés personnelles** ;
- un **facteur d'inhérence** (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. ;

[1] Voir Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité, cnil.fr et la 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, legifrance.gouv.fr

- comportementale, par exemple la frappe au clavier, la voix , la démarche ou encore l'écriture.

Certains types d'information contextuelle (telle que la localisation géographique de l'utilisateur), bien que susceptibles d'apporter des éléments de réassurance, ne peuvent en principe être considérés comme suffisants pour constituer une preuve pour l'authentification.

Terminologie

Plusieurs concepts liés à l'authentification multifacteur existent et peuvent recouvrir des techniques ou approches différentes. En voici quelques définitions pour permettre de les distinguer.

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

Double authentification ou **authentification à deux facteurs** (**2FA** pour *two-factor authentication*) : authentification multifacteur reposant sur exactement deux facteurs de catégories distinctes.

Vérification à 2 étapes *(2SV pour two-step validation) :* authentification basée sur la vérification séquentielle de deux facteurs. Ce terme est parfois utilisé pour signifier une authentification multifacteur mais elle n'a cependant pas ce caractère lorsque les deux étapes font appel à la même catégorie de facteurs (connaissance, possession ou inhérence).

Authentification forte (*strong authentication*) : le sens de cette appellation varie selon le contexte. Elle est parfois utilisée pour désigner une authentification multifacteur dans certains cadres sectoriels (par exemple la deuxième directive sur les services de paiement, appelée aussi DSP2[2], ou encore la politique de sécurité des systèmes d'information de l'État, dénommée PSSI-E[3]). Elle peut également être définie, dans la pratique (formalisée dans la dernière recommandation de l'ANSSI[4] relative à l'authentification multifacteur[5]), comme « une authentification reposant sur un mécanisme cryptographique dont les paramètres et la sécurité sont jugés robustes ». Cette authentification peut, s'il y a lieu, reposer sur un seul facteur.

L'authentification multifacteur doit, comme tout traitement de données à caractère personnelle, respecter le cadre légal notamment le RGPD. Pour ce faire, les responsables de traitement doivent appliquer les principes essentiels du RGPD, en particulier la minimisation des données et le respect des droits des personnes. Cela se traduit notamment par la mise en œuvre de mesures techniques et organisationnelles permettant de concilier l'authentification multifacteur avec les droits et libertés des personnes concernées.

Selon les cas, l'authentification multifacteur peut être considérée comme un traitement accessoire, visant à sécuriser un traitement auquel elle est adossée, ou un traitement spécifique, qui peut contribuer de manière transverse et commune à la sécurité de plusieurs traitements au sein d'un système d'information. La présente recommandation a vocation à s'appliquer à ces deux types de situation.

Cette recommandation couvre l'étape de l'authentification au sens strict, elle n'a pas vocation à développer les processus liés à la gestion des identités et des accès (par exemple la gestion de comptes, la gestion des droits et habilitations, etc.). Elle présente des encadrés explicatifs afin de préciser des thématiques aux enjeux particuliers, tels que la biométrie ou l'authentification basée sur les risques, et d'illustrer en pratique les sujets abordés.

2.3 Pourquoi l'authentification multifacteur ?

La mise en place d'une authentification multifacteur permet d'atténuer significativement les risques d'accès illégitime aux fonctionnalités et aux données d'un système d'information suite à la compromission d'un mot de passe utilisateur, par exemple. C'est pourquoi, la CNIL en recommande l'usage, tout comme l'ANSSI qui met en avant l'authentification multifacteur parmi l'une des cinq mesures prioritaires à déployer de manière préventive[6]. Une telle authentification peut donc être privilégiée par le responsable de traitement pour sécuriser

[2] Voir article 18 du règlement délégué de la DSP2, EUR-Lex

[3] Politique de sécurité des systèmes d'information de l'État, legifrance.gouv.fr

[4] Agence nationale de la sécurité des systèmes d'information

[5] Recommandations relatives à l'authentification multifacteur et aux mots de passe, cyber.gouv.fr

[6] Les Mesures Cyber Préventives Prioritaires disponibles, cyber.gouv.fr

l'accès aux ressources de ses systèmes d'information en fonction de ses objectifs de sécurité. Dans ce cas, la mise en place d'un dispositif d'authentification multifacteur est susceptible de participer au respect de l'obligation de sécurisation de tout traitement de données à caractère personnel, en application des articles 5 et 32 du RGPD.

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

Plusieurs règles doivent être respectées par les organismes qui décident de recourir à l'authentification multifacteur afin de mettre en place des pratiques respectueuses du RGPD.

Les principales actions à mener préalablement à la mise en place d'une authentification multifacteur sont :

1. vérifier si la mise en place d'une authentification multifacteur résulte d'une obligation légale ;
2. si cela n'est pas le cas :
    1. évaluer l'opportunité de mettre en place une authentification multifacteur ;
    2. justifier d'une base légale au traitement d'authentification multifacteur ;
3. choisir la solution en prenant en compte les risques relatifs aux personnes concernées ;
4. préciser la qualification des acteurs et leurs obligations ;
5. minimiser la collecte de données ;
6. définir les modalités de conservation des données ;
7. documenter et encadrer les potentiels transferts de données ;
8. prévoir l'exercice des droits des personnes concernées ;
9. S'assurer que le niveau de sécurité associé à chaque facteur est approprié par rapport aux risques.

3.1 Vérifier si la mise en place d'une authentification multifacteur résulte d'une obligation légale

La mise en place d'une authentification multifacteur peut être explicitement imposée, dans certains cas, par des dispositions nationales ou européennes. Il est alors dans ce cas nécessaire de la mettre en œuvre en portant l'attention sur les choix de la solution comme développé en partie 3.3.

Exemples de réglementations applicables en date de la parution de la recommandation :

- **Les réglementations exigeant des schémas d'identification électronique aux niveaux de garantie substantiel ou élevé tels que définis dans le règlement européen eIDAS[7] ;**
- La directive européenne DSP2[8] pour certaines opérations telles que l'accès au compte bancaire en ligne, la réalisation d'opérations de paiement ou encore l'exécution d'actions susceptibles de comporter un risque de fraude ;
- La PSSI-E[9] pour l'accès à des informations sensible de l'administration ;
- **Le code de la santé publique qui fait référence à des référentiels d'identification, d'interopérabilité et de sécurité pour les services numériques en santé. Parmi ces référentiels, la PGSSI-S[10] (politique générale de sécurité des systèmes d'information de santé) impose l'authentification multifacteur aux professionnels de santé et patients pour l'accès à certains traitements de données de santé ;**
- Le référentiel d'exigences SecNumCloud[11], par exemple pour l'accès aux interfaces d'administration de services cloud.

3.2 Si cela n'est pas le cas :

3.2.1 Evaluer l'opportunité de mettre en place une authentification multifacteur

L'authentification multifacteur est une mesure de sécurité préventive, elle permet de réduire significativement la vraisemblance du risque d'accès illégitime à des systèmes d'information, a fortiori à des données à caractère personnel, par rapport à une authentification simple. Ainsi, la mise en place d'un dispositif d'authentification multifacteur peut participer au respect de l'obligation de sécurisation des traitements de données à caractère personnel soumis à l'application des articles 5.1.f et 32 du RGPD, sans qu'il ne puisse toutefois être considéré que ces articles constituent une obligation générale d'utiliser une telle modalité.

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 lorsque la connexion au système d'information est établie depuis l'extérieur du réseau de l'organisme. En effet, l'authentification basée sur ces deux facteurs permet généralement d'améliorer de manière importante la sécurité du système d'information. Il est cependant toujours nécessaire de procéder à une analyse au cas par cas en prenant en compte les spécificités du traitement considéré et des personnes qu'il concerne ou qui y accèdent.

Pour l'usage de facteur d'inhérence, des précautions particulières doivent être prises comme illustré par l'exemple 1 : « Biométrie et consentement » ci-après en partie 3.2 et à l'encadré « Le cas particulier de la biométrie morphologique » en partie 3.3 de la présente recommandation.

Comme toute mesure de sécurité, l'authentification multifacteur requiert d'adapter le niveau de sécurité visé au contexte et aux risques auxquels est exposé le système d'information concerné. Outre les risques liés à la confidentialité et à l'intégrité des données, ceux liés à l'indisponibilité de l'accès pour les utilisateurs ne doivent pas être oubliés. Pour les systèmes ou opérations à risque élevé (par exemple l'administration système et réseau, l'accès aux traces de journalisation et le traitement de données sensibles comme un dossier patient informatisé ou encore l'accès au gestionnaire de mots de passe ou à une messagerie électronique professionnelle), le recours à l'authentification multifacteur est fortement recommandée.

Dans tous les cas il est nécessaire d'effectuer une mise en balance entre la sécurité apportée par l'authentification multifacteur et les conséquences qu'elle pourrait engendrer pour les utilisateurs concernés (notamment la

[7] Règlement (UE) No 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (PDF, 1 Mo), EUR-Lex

[8] Directive (UE) 2015/2366 sur les services de paiement, legifrance.gouv.fr

[9] Politique de sécurité des systèmes d'information de l'État, legifrance.gouv.fr

[10] Corpus documentaire PGSSI-S, esante.gouv.fr

[11] Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences (Version 3.2), cyber.gouv.fr

dissuasion d'accès au service, la collecte de données supplémentaires, l''impossibilité de mobiliser un des facteurs, etc.). Ainsi, pour les systèmes ou opérations à faible risque, il convient de permettre l'usage de l'authentification multifacteur sans forcément l'imposer, ce qui permet d'avoir un impact positif sur les droits des utilisateurs.

3.2.2 Justifier d'une base légale au traitement d'authentification multifacteur

L'authentification multifacteur nécessite de traiter des données à caractère personnel au sens du RGPD. Les opérations de traitement liées à l'authentification doivent reposer sur une base légale au sens de l'article 6 du RGPD.

Cette base légale peut être :

- L'obligation légale s'il existe une disposition imposant une authentification multifacteur (en principe cette obligation aura été identifiée en étape 1). Il est important de souligner ici que cette base légale n'est mobilisable que pour des textes réglementaires prévoyant cette obligation de manière explicite. En particulier, l'article 32 du RGPD qui prévoit une obligation de sécurité n'engendre pas à lui seul une obligation légale de mettre en place une authentification multifacteur dans le cadre de traitements de données à caractère personnel ;
- Le contrat, s'il existe une relation contractuelle entre l'organisme mettant en œuvre l'authentification multifacteur et les personnes concernées, ou pour l'exécution de mesures précontractuelles prises à la demande de la personne concernée. Dans ce cas, le responsable de traitement devra s'assurer que le contrat est licite en droit français et que l'authentification multifacteur est objectivement nécessaire à l'exécution du contrat ;
- L'intérêt légitime du responsable de traitement pour garantir la sécurité du réseau et des informations de ses systèmes d'informations. 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 devrait prévoir une alternative (par exemple, l'authentification simple par identifiant et mot de passe ou bien sans traitement biométrique) et prendre en compte ses implications en termes de sécurité. Cette base légale est donc moins adaptée aux opérations de sécurité. A noter que lorsque le dispositif de sécurisation utilise des données biométriques, qui sont des données sensibles au sens de l'article 9 du RGPD, le dispositif ne pourra être mis en œuvre qu'avec le consentement des personnes, sauf à ce à ce qu'il soit rendu obligatoire par une norme juridique. Dans ce cas, le responsable de traitement doit proposer une alternative, et le consentement constitue la base légale la plus naturelle.

Les caractéristiques des mesures de sécurité des traitements sont distinctes de celles des traitements qui sont sécurisés : même dans le cas où les mesures de sécurité s'adossent au traitement principal, les données utilisées peuvent être spécifiques, leur durée de conservation est propre, les accédants sont généralement distincts et plus réduits, etc. Il convient donc d'assurer une information spécifique aux personnes concernées. De plus, une mention de ces traitements de sécurisation doit en principe figurer dans le 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 est adossée, ou bien dans une entrée spécifique du registre dans le cas d'une authentification transversale et commune à différentes opérations de traitement.

Exemple #1 : Biométrie et consentement

Un fournisseur de service en ligne, tel qu'une plateforme d'achat/revente entre particuliers par exemple, peut proposer à ceux-ci 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 veut proposer de renforcer l'authentification par mot de passe par un mécanisme de reconnaissance biométrique. En pratique, le fournisseur introduit une option activable par les utilisateurs.

Le fournisseur de la plateforme peut alors procéder d'au moins deux manières :

- **Il propose de recourir à un dispositif qui effectue la comparaison des données biométriques localement sur l'ordiphone personnel de l'utilisateur. Ce dispositif conserve le gabarit biométrique dans le composant de sécurité[12] de l'appareil sans qu'il ne soit traité pour une autre finalité[13] que l'authentification. Dans ce cas, le fournisseur du service en ligne n'est pas considéré comme responsable du traitement de données biométriques.**

  Au titre du RGPD, 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.

- Il propose, sur la base du consentement, un second facteur reposant sur un traitement de données biométriques effectué côté serveur, dont il est responsable de traitement. Une telle approche peut lui permettre de proposer des services additionnels tels que, par exemple, la synchronisation sur plusieurs appareils des données biométriques permettant l'authentification. Elle nécessitera cependant de la réalisation d'une analyse d'impact relative à la protection des données.

Dans les deux cas, le recours à la biométrie ne peut être imposé sans alternative. Le fournisseur doit donc, par exemple, proposer l'utilisation d'un facteur de possession ou garantir le maintien d'une authentification simple, sans que ce choix n'entraîne de restriction sur les services fournis à l'usager.

3.3 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.

De manière générale, il est préférable que le mécanisme d'authentification multifacteur ne collecte aucune information supplémentaire, contribuant à relier le compte à une autre identité de la personne, que le responsable de traitement n'ait déjà. Si une telle collecte s'avérait nécessaire, le responsable de traitement devrait, pour assurer la transparence, informer spécifiquement les personnes concernées de ce risque de corrélation après une mise en balance de ce dernier avec la sécurité supplémentaire apportée à l'utilisateur. Cela est en particulier le cas pour les services pour lesquels il est raisonnable de supposer que les utilisateurs puissent s'enquérir davantage de rester sous couvert de pseudonymat que du renforcement de la sécurité de l'accès.au service.

Si le recours à une authentification multifacteur protège les personnes, l'usage d'un facteur inhérent entraîne des risques spécifiques pour celles-ci. Par conséquent, son usage devrait être entouré de précautions particulières. D'une manière générale, il est recommandé de proposer une alternative au facteur inhérent (par exemple un facteur de possession) aux utilisateurs, notamment dans un cadre professionnel.

[12] Recommandations relatives à l'authentification multifacteur et aux mots de passe, cyber.gouv.fr

[13] Biométrie dans les smartphones, cnil.fr

Le cas particulier de la biométrie morphologique

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 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.

Pour le cas particulier de l'authentification reposant sur un traitement de données biométriques pour le contrôle d'accès aux lieux de travail ainsi qu'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[14].

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[15].

En outre, une attention particulière devra être portée aux durées et modalités de conservation des gabarits biométriques de référence et ceux servant à la comparaison. La CNIL recommande que les gabarits biométriques de référence ne soient stockés que sur des dispositifs sous le contrôle exclusif des personnes concernées.

Enfin, la sécurisation du dispositif biométrique nécessite des mesures particulières destinées à empêcher notamment l'usurpation d'identité : à cet égard, l'utilisation de données biométriques ne laissant pas de traces (comme le réseau veineux des doigts ou de la main plutôt que l'empreinte digitale) ou la qualification de la performance des capteurs utilisés contre certaines attaques par présentation (détection de vivant, etc.) sont nécessaires.

Il sera nécessaire de documenter et être en mesure de justifier, de manière très concrète, le 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.

Le responsable de traitement devrait également considérer, lors du choix de la solution d'authentification multifacteur, le risque d'accès empêché (*lockout*) 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.

[14] Contrôle d'accès biométrique au travail, cnil.fr

[15] Biométrie dans les smartphones, cnil.fr

Le cas particulier de l'usage additionnel de techniques basées sur les risques

Initialement conçue dans une perspective de lutte contre la fraude dans le secteur bancaire, la technique dite d'authentification basée sur les risques (RBA pour *risk-based authentication*), peut aujourd'hui être utilisée dans les solutions d'authentification pour renforcer les contrôles.

La technique consiste à calculer dynamiquement un score pouvant être basé sur des règles logiques, des informations contextuelles, une analyse liée à l'appareil (*device intelligence*), l'historique des incidents de sécurité lié au compte ou encore des comportements de personnes utilisatrices pour détecter des comportements anormaux. Ce calcul peut également faire intervenir de l'intelligence artificielle (à travers des modèles agrégés, ou spécifiques, de personnes utilisatrices légitimes). Il permet alors de définir les niveaux de risque pour un accès ou une action sollicitée par l'utilisateur. Le score résultant conditionne dans ce cas le niveau d'authentification exigé (simple, multifacteur et/ou cryptographiquement robuste) ou peut entraîner un rehaussement de l'authentification pour chaque fonctionnalité jugée à risque (par exemple pour l'accès à une interface d'administration, une transaction à montant élevé ou l'ajout d'un compte bénéficiaire sur un site de banque en ligne).

Une variante de l'authentification basée sur les risques est l'authentification continue qui consiste à appliquer le calcul du score de manière continue tout au long d'une session utilisateur. Lorsque qu'une anomalie est détectée le mécanisme prend des mesures en temps réel perceptible ou non de l'utilisateur : ajout de règles, sollicitation d'une action utilisateur pour réassurance par analyse comportementale, demande de présentation d'un facteur d'authentification supplémentaire voire demande de réauthentification complète.

L'usage des techniques basées sur les risques requiert de considérer l'exactitude des informations utilisées pour le calcul de ce score. Par exemple, l'ANSSI indique, concernant la localisation, qu'« [a]u vu des possibilités de contournement et de la faible maturité des technologies pouvant [l']exploiter, il convient d'être prudent vis-à-vis de leur utilisation au sein d'un mécanisme d'authentification ». Si ce dispositif repose sur des données biométriques, leur traitement à des fins de vérification, identifiant de manière unique une personne physique, est à considérer comme une authentification et relève donc du cadre particulier de l'article 9.

Dans le cas où la solution d'authentification multifacteur met additionnellement en œuvre une technique basée sur les risques, des données supplémentaires peuvent être collectées telles que l'horaire, l'identifiant de l'appareil ou la géolocalisation. En cas d'utilisation d'une telle technique, le responsable de traitement devrait veiller à ce que la collecte de données soit proportionnée au but poursuivi et être en mesure de justifier cette collecte, en particulier concernant ses performances au regard du principe d'exactitude du RGPD.

Aussi, le responsable de traitement devrait veiller à ce que les mécanismes utilisés ne privent pas les personnes concernées de l'accès aux services si celles-ci utilisent des systèmes amoindrissant la capacité à accéder à leurs traces de navigation, tels que des bloqueurs de traceurs (*cookies*).

Enfin cette technique, en ce qu'elle consiste à analyser le comportement de l'utilisateur pour lui attribuer un score de risque, pourrait être considérée comme un profilage de l'utilisateur au sens de l'article 4 du RGPD.

Si tel est le cas, le responsable de traitement devra déterminer si un tel profilage est soumis au régime de l'article 22 du RGPD. Ainsi, dans le cas où l'échec de l'authentification ou de son maintien affecterait de manière significative la personne légitime concernée ou aurait des effets juridiques et proviendrait d'une décision automatisée, y compris du profilage, les dispositions de l'article 22 s'appliqueraient.

3.4 Préciser la qualification des acteurs et leurs obligations

Si un organisme utilise un produit permettant une authentification multifacteur sans avoir recours à un prestataire pour son installation, sa configuration, son hébergement, son exploitation, sa maintenance ou toute autre opération entraînant un traitement de données personnelles, cet organisme est en principe seul responsable du traitement.

L'organisme qui décide de recourir à un fournisseur de **service** ou de solution (cette dernière étant entendue comme la combinaison d'un **produit** logiciel ou matériel **et** d'un **service** d'intégration ou de tierce maintenance applicative, par exemple) afin d'effectuer une authentification multifacteur au sein de son système d'information sera qualifié en principe de responsable de traitement, tandis que le fournisseur agira généralement en tant que sous-traitant. Les sous-traitants peuvent par exemple être les prestataires d'infogérance ou les fournisseurs de solutions d'informatique en nuage (*cloud*).

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 de l'article 28.3 du RGPD.

Pour rappel les acteurs qui vendent un produit sans prestation de service associée (ce qui exclut par exemple les services en *SaaS*) ne sont pas, en principe, concernés par les dispositions de sous-traitances du RGPD. Ils peuvent alors être considérés comme des tiers au sens du RGPD (de tels prestataires peuvent, le cas échéant, être responsables de traitement de données issues de leurs produits, qu'ils collectent et exploitent pour leurs finalités propres).

Exemples de recours à un fournisseur pour la mise en place d'une authentification multifacteur

Exemple #2 : Une application installée sur un terminal professionnel

Cette solution est pertinente pour mettre en place un second facteur d'authentification lié à un terminal mobile 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 (cf. Exemple 5 en partie 9), un code à usage unique. La synchronisation est opérée ab initio et, en principe, aucun échange de données n'est nécessaire entre le terminal et le serveur OTP qu'il soit sous le contrôle de l'employeur ou du fournisseur de l'application (ce qu'il appartient à l'employeur, en tant que responsable de traitement, de vérifier). Dans ce cas de figure, le fournisseur de l'application n'est pas considéré comme sous-traitant.

Exemple #3 : Un service d'authentification multifacteur en SaaS

Cette solution consiste à recourir à un fournisseur de service tiers qui inscrit les utilisateurs, gère les comptes, gère la délivrance et l'activation des facteurs et des informations d'authentification associés et enfin 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 ou à la journalisation des flux d'authentification par le prestataire ;
- veiller au bon encadrement d'éventuels transferts de données personnelles hors Union européenne, qui peuvent concerner les flux d'authentifications eux-mêmes mais 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.

3.5 Minimiser la collecte de données

Les données collectées par les solutions d'authentification multifacteur varient selon les facteurs d'authentification mis en œuvre. De manière générale et en fonction de leur besoin, ces solutions peuvent collecter :

- Un identifiant utilisateur, comme une adresse email, un numéro de compte, etc. ;
- Un identifiant technique si l'identifiant est généré par un service de tierce-partie ;
- Des données différentes selon les catégories de facteurs utilisées
  - Dans le cas de la connaissance : le mot de passe ou son **empreinte cryptographique** en fonction du protocole retenu, le code confidentiel, etc. ;
  - Dans le cas de la possession : un identifiant universel unique (*UUID*) de téléphone, une adresse MAC (de l'anglais, *Media Access Control*) d'une carte réseau d'un ordinateur, un certificat, un OTP ou la réponse dans le cas d'un protocole défi-réponse etc. ;
  - Dans le cas de l'inhérence : un gabarit biométrique venant d'une empreinte digitale, rétinienne, etc.

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

Exemples de minimisation dans le cas du facteur de possession

Exemple #4 : Une carte de paiement protégée par code PIN

Le paiement traditionnel par carte sur un terminal de paiement, avec insertion de la carte et saisie du code PIN, est une authentification multifacteur.

Concernant le facteur de connaissance, le code PIN permet de vérifier que le payeur est bien le détenteur légitime de la carte, cette vérification est normalement faite directement sur la carte de paiement au sein de son composant de sécurité : la carte à puce. Le terminal de paiement sert alors uniquement d'interface de saisie sans autre action à cette étape.

Pour ce qui est du facteur de possession, son authenticité est vérifiée à travers un procédé cryptographique appelé DDA (Dynamic Data Authentication) : cela permet de vérifier que la carte de paiement n'est pas contrefaite.

Au sein de la carte à puce sont stockés un couple de clés asymétriques, un certificat et une clé symétrique unique. L'authentification se base sur un échange défi-réponse entre le terminal et la carte à puce :

1) le terminal transmet à la carte un nombre aléatoire (le défi) ;
2) la carte génère, à partir de ce nombre, une signature électronique (la réponse) ;
3) Le terminal vérifie cette signature et, si elle est valide, cela atteste que la carte contient bien la clé privée et donc que la carte n'est pas contrefaite.

Exemple #5 : Une application mobile d'OTP déverrouillée par empreinte digitale

De nombreuses applications d'authentification multifacteur utilisent comme second facteur un TOTP, basé sur la synchronisation temporelle entre le serveur d'authentification et l'application fournissant l'OTP. Pour que cela constitue bien une authentification multifacteur, il faut qu'en plus de saisir l'OTP sur la mire d'authentification, l'utilisateur présente un second facteur soi de connaissance, soit d'inhérence.

Le vérifieur (responsable de traitement de l'authentification) est souvent dans l'impossibilité 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 il devra limiter l'accès à l'application ou à la visualisation de l'OTP aux personnes légitimes. A cette fin, certaines personnes préfèrent utiliser une authentification par empreinte digitale ou reconnaissance faciale plutôt que des méthodes basées sur un facteur de connaissance. Dans ce cas, le recours à la biométrie doit cependant se faire, en principe, au moyen d'un dispositif biométrique dont le gabarit est stocké et comparé à l'empreinte présente dans le composant sécurisé du mobile. Cela conditionne, de fait, l'usage d'une telle solution au fait que les utilisateurs possèdent des appareils mobiles compatibles, à savoir avec un composant de sécurité.

Comme pour la carte bancaire, l'authentification biométrique permet à l'application de vérifier que la personne est l'utilisateur légitime en local 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.

Minimisation par conception

Dans ces deux exemples de solution, le facteur de possession est déverrouillé par l'autre facteur. L'entité qui vérifie les preuves d'identité n'a alors pas besoin de collecter les données liées au facteur de connaissance ou d'inhérence. La solution minimise les données collectées lors de l'authentification à des données purement techniques :

- l'identifiant du compte utilisateur ;
- l'horodatage ;
- la preuve de possession (la réponse dans le cas du défi-réponse pour la carte de paiement et l'OTP pour l'application mobile). Notons que cette preuve est collectée mais que 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 d'un composant de sécurité, 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 fortes garanties de robustesse (en s'appuyant par exemple sur une qualification ou une certification).

3.6 Définir les modalités de conservation des données

Pour rappel, ne sont considérées ici que 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.

Concernant la conservation des données utilisée lors de l'authentification, les responsables de traitement peuvent par exemple se référer à la recommandation « mots de passe » [16]pour les modalités de conservation des données liées aux facteurs de connaissance et 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 ce contexte particulier. Les modalités de conservation des données relatives aux facteurs de possession dépendent de la technologie employée. De manière générale, les secrets et paramètres stockés devront être régulièrement mis à jour en fonction des risques et avancées technologiques. Un chiffrement au repos des données les plus critiques est également recommandé.

Concernant les traces de journalisation des systèmes d'authentification, elles doivent être conservées selon des durées limitées. Il est conseillé de se référer à la recommandation journalisation[17] de la CNIL qui recommande une durée entre 6 mois et 1 an dans le cas général.

La prise en compte de dispositions spécifiques au contexte d'usage peut amener à fixer des durées de conservation particulières, notamment liées aux caractéristiques des traitements, tels 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 en raison de l'importance du risque pour les personnes en cas de détournement de finalité par exemple.

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

3.7 Documenter et encadrer les potentiels transferts de données

Le déploiement d'une solution d'authentification multifacteur est susceptible d'entraîner des transferts de données 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 d'informatique en nuage[18], même si le service principal offert par le responsable de traitement est hébergé sur le territoire de l'Union européenne. En effet, il existe des fournisseurs de service d'authentification multifacteur tiers utilisables de manière générique et compatible avec un grand nombre d'autres services.

De manière générale, il est recommandé au responsable de traitement d'apporter une attention particulière aux flux de données engendrés par l'authentification multifacteur et, le cas échéant, de bloquer tout flux non nécessaire à la fourniture du service.

3.8 Prévoir l'exercice des droits des personnes concernées

L'information des personnes concernées devra être prévue conformément aux articles 13 et 14 du RGPD. Cette information devrait être accessible (le cas échéant au moyen d'un lien hypertexte) aux différentes étapes d'une gestion de compte dont l'accès se base sur une authentification multifacteur, et notamment :

- lors de l'inscription de la personne, c'est-à-dire à la création du compte et des informations associées ;
- lors de la délivrance ou lors de l'activation des facteurs d'authentification (comme par exemple l'enrôlement du 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

---

[16] Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité, cnil.fr et la 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, legifrance.gouv.fr

[17] La CNIL publie une recommandation relative aux mesures de journalisation, cnil.fr et la délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation, legifrance.gouv.fr

[18] Les outils de sécurisation d'applications web dans l'informatique en nuage (cloud), cnil.fr

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 ou informations associées à celui-ci.

Lors de l'inscription de la personne au service, avec potentiellement création d'un compte, l'information sur le traitement de données à caractère personnel résultant des mécanismes d'authentification peut être intégrée dans la politique de confidentialité générale lorsque le contexte le permet. En pratique, 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 fin de sécurité (authentification, journalisation, chiffrement…), 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 4 (profilage), 22 (décision individuelle automatisée), 9 (données sensibles) et 35 (relevant d'une AIPD) du RGPD.

Les droits des personnes concernées dépendront de la base légale choisie par le responsable de traitement. L'exercice de ces droits pourra être facilité par la mise à disposition d'une interface de gestion en libre-service pour les personnes concernées. Il conviendra de veiller à prendre en compte les problématiques d'accès au numérique pour certaines populations.

Il faut par ailleurs noter que le choix d'un facteur d'authentification peut avoir des conséquences sur la vie privée de la personne concernée, notamment si la mise en place du facteur d'authentification peut reposer, dans le cadre professionnel, sur l'accès aux équipements personnels de la personne. Les responsables de traitement devraient ainsi prendre en compte ces problématiques dans le choix des facteurs d'authentification pouvant être déployés, par exemple en évitant de recourir à des facteurs relevant de l'identité privée d'une personne dans un cadre professionnel.

3.9 S'assurer que le niveau de sécurité associé à chaque facteur est approprié par rapport aux risques

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 »[19] de la CNIL dédiée à ce sujet.

Pour les solutions faisant intervenir un facteur de possession, le responsable de traitement devra veiller à ce que ces solutions :

- soient basées sur protocoles de vérification de preuves cryptographiquement robustes (type OTP ou défi-réponse) lorsque les enjeux le justifient ;
- prouvent la possession d'un dispositif matériel spécifique, y compris pour les solutions logicielles (*soft token*). Dans ce cas, l'utilisateur devra, dès l'inscription, enrôler son appareil (au sens d'une association de l'appareil avec le compte de la personne auprès du responsable de traitement) ;
- fassent intervenir des preuves de possession dynamiques (pour garantir une vérification systématique de l'authenticité du dispositif matériel) lorsque les risques le justifient.

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 et de faux rejet), ainsi que la robustesse aux **attaques par présentation**.

[19] Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité, cnil.fr

Exemple #6 : La sécurisation des applications mobiles d'authentification multifacteur par notification push (soft token)

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 la valider, ce qui déclenche le mécanisme cryptographiquement robuste d'authentification (OTP ou *challenge-response* 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 fatigue ou par manque d'attention, par en accepter une. Cette attaque est nommée « accoutumance à la MFA », aussi connue comme *MFA fatigue*.

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

- l'utilisation d'informations complémentaires selon une logique d'authentification basée sur les risques, comme l'emplacement géographique, le type de terminal et la dernière heure de tentative de connexion, qui facilite la détection par l'utilisateur légitime des tentatives de connexions frauduleuses ;
- **la limitation de fréquence des notifications *push* (par exemple : pas plus d'un certain nombre de notifications, ou de tentatives, par heure) est simple à mettre en œuvre et efficace. Néanmoins, elle n'empêche pas que l'attaquant ait recours à l'ingénierie sociale pour tromper une cible, par exemple en lui téléphonant ;**
- **l'usage de la correspondance de numéros ou de symboles qui envoie une requête sur l'application mobile et demande à l'utilisateur de saisir le code affiché sur l'écran de connexion. Dans ce cas, l'usurpateur voit le code alors que l'utilisateur légitime, qui n'est pas à l'origine de la tentative de connexion, ne le voit pas. L'intérêt de la notification *push*, qui est de faciliter l'expérience utilisateur de connexion, peut se retrouver alors fortement réduit.**

Il est possible de se référer au guide de l'ANSSI Recommandations relatives à l'authentification multifacteur et aux mots de passe[20] pour identifier et mettre en œuvre d'autres mesures de sécurité informatique. Il conviendra de prendre en compte les impacts sur les personnes concernées dans le choix et l'implémentation de ces mesures.

[20] Recommandations relatives à l'authentification multifacteur et aux mots de passe, cyber.gouv.fr

4. À ne pas faire

- Confondre authentifications répétées et authentification multifacteur : des demandes d'authentifications successives portant sur des catégories de facteurs différents mais liées à des comptes disjoints (par exemple un compte local d'ordinateur puis un compte de service en ligne) ne peuvent, a priori, pas être considérées comme une authentification multifacteur.
- Demander plusieurs fois la saisie d'un même facteur : cela ne constitue pas une authentification multifacteur.
- Journaliser des informations secrètes telles que l'empreinte d'un mot de passe, un OTP ou une empreinte biométrique.
- Utiliser les données contextuelles à l'authentification (par exemple, adresse IP ou géolocalisation) comme un facteur d'authentification à part entière (l'authentification basée sur les risques et l'authentification multifacteur peuvent être combinées mais ne doivent pas être confondues).
- Utiliser des méthodes d'authentification non fiables ou déconseillées par les autorités compétentes comme :
- la transmission d'un code OTP par SMS car il s'agit d'une méthode d'authentification reposant sur la réception d'une valeur au moyen d'un canal peu ou pas sécurisé[21] ;
- la transmission d'un lien ou d'un code OTP par courrier électronique car elle ne peut pas être considérée comme un facteur de possession dans la mesure où elle ne permet pas de prouver la possession d'un objet spécifique[22].

Pour les deux derniers points, en l'absence d'alternative, l'usage d'un code à usage unique par SMS ou par courrier électronique peut constituer une mesure de réassurance de l'authentification, au même titre que les mécanismes d'alerte de connexions suspecte qui permettent de détecter ou empêcher les tentatives d'usurpation de comptes.

[21] Recommandations relatives à l'authentification multifacteur et aux mots de passe, p. 21, cyber.gouv.fr

[22] NIST Special Publication 800-63B, Digital Identity Guidelines, p. 17, nvlpubs.nist.gov

Annexe I : Définitions

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

- **Authentification multifacteur**
- **Facteur d'authentification** (facteur de connaissance, facteur de possession, facteur d'inhérence)
- **Authentification simple**
- **Double authentification** ou **authentification à deux facteurs**
- **Authentification forte**
- **Vérification à 2 étapes** (2SV pour *two-step validation*)
- **Authentification basée sur les risques**
- **Authentification continue**

Carte de clés personnelles : aussi désignée comme carte matricielle, il s'agit d'une carte matérielle en papier plastifié contenant une grille de codes. L'utilisateur doit détenir la carte pour pouvoir saisir le second facteur, à savoir un code de la case de coordonnées (X,Y) indiquées sur la mire d'authentification.

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 :

TOTP (*Time-based OTP*), basé sur la synchronisation temporelle entre le serveur d'authentification et le matériel ou l'application fournissant l'OTP ;

HOTP (*HMAC-based OTP*), basé sur un compteur et HMAC, un algorithme de hachage cryptographique à clé secrète ;

OCRA (*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 (*token*) 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.

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

Analyse liée à l'appareil : Recherche d'anomalies dans les informations liées à l'appareil de l'utilisateur telles que l'identifiant d'appareil, l'adresse IP, les traceurs (*cookies*) enregistrés, la géolocalisation, la langue, la taille de l'écran, la version du navigateur, l'empreinte numérique (*fingerprint*) du navigateur, etc.

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).