RECOMMANDATIONS RELATIVES À L'AUTHENTIFICATION MULTIFACTEUR ET AUX MOTS DE PASSE

GUIDE ANSSI

ANSSI-PG-078
08/10/2021

PUBLIC VISÉ :

Développeur Administrateur RSSI DSI Utilisateur

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations relatives à l'authentification multifacteur et aux mots de passe »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`. Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [19].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	2012	Version initiale
2.0	08/10/2021	Réécriture complète du guide

Avant-propos de la CNIL

L'authentification des utilisateurs accédant un système informatique est un des fondamentaux de la sécurité informatique. Ce guide de portée très large, élaboré par l'ANSSI avec la contribution de la CNIL, constitue une référence pour l'élaboration de mesures d'authentification, essentielles pour garantir la sécurité des traitements de données personnelles, en application des articles 5 et 32 du RGPD.
Il sera nécessaire d'adapter ces mesures aux risques propres à chaque application ou traitement selon le contexte, en étant particulièrement vigilant sur la biométrie, spécifiquement encadrée par le RGPD.
La CNIL s'appuiera sur ce guide pour recommander des bonnes pratiques en matière d'authentification et encourage tous les acteurs du numérique à s'en saisir afin de progresser dans leur conformité à l'obligation de sécurité du RGPD. Dans ce cadre, une mise à jour de sa recommandation sur l'usage des mots de passe sera rendue publique en 2022.

En savoir plus : `https://www.cnil.fr/fr/mot-de-passe`

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

1 Introduction **4**
- 1.1 Objectifs du guide . . . 4
- 1.2 Organisation du guide . . . 5
- 1.3 Convention de lecture . . . 5
- 1.4 Glossaire et acronymes . . . 6

2 Authentification **8**
- 2.1 Authentification et premières définitions . . . 8
- 2.2 Menaces et attaques sur l'authentification . . . 9
- 2.3 Aperçu des limites de l'authentification par mots de passe . . . 11
- 2.4 Qu'est-ce que l'authentification multifacteur ? . . . 13
- 2.5 Authentification forte : distinction avec l'authentification multifacteur . . . 15
- 2.6 Éléments supplémentaires à considérer dans le choix des moyens d'authentification en fonction du contexte . . . 16

3 Recommandations concernant le cycle de vie des facteurs d'authentification **19**
- 3.1 Création et renouvellement des facteurs d'authentification . . . 19
- 3.2 Transmission et utilisation des facteurs d'authentification . . . 20
- 3.3 Révocation des facteurs d'authentification . . . 24

4 Facteur de connaissance (« ce que je sais ») **26**
- 4.1 Politique de sécurité de mots de passe . . . 26
- 4.2 Longueur des mots de passe . . . 27
- 4.3 Règles de complexité des mots de passe . . . 29
- 4.4 Délai d'expiration des mots de passe . . . 30
- 4.5 Contrôle de la robustesse des mots de passe . . . 31
- 4.6 Stockage des mots de passe . . . 32
- 4.7 Recouvrement d'un accès . . . 34
- 4.8 Coffre-fort de mots de passe . . . 34
- 4.9 Recommandations à destination des utilisateurs . . . 35

5 Facteur de possession (« ce que je possède ») **37**
- 5.1 Recommandations relatives à l'utilisation d'un facteur de possession . . . 37
- 5.2 Utilisation d'un facteur de possession pour une authentification multifacteur . . . 39

6 Facteur inhérent (« ce que je suis ») **40**
- 6.1 Avantages et inconvénients des facteurs inhérents . . . 40
- 6.2 Recommandations relatives à l'utilisation d'un facteur inhérent . . . 41

Liste des recommandations **43**

Bibliographie **45**

1
Introduction

1.1 Objectifs du guide

L'authentification des différents utilisateurs d'un système d'information (allant des simples utilisateurs aux administrateurs) joue un rôle important dans la gestion de la sécurité d'un système d'information.

L'objectif de ce guide est de proposer des recommandations de sécurité relatives à l'authentification en général (recommandations sur le cycle de vie d'un moyen d'authentification quel qu'il soit) et relatives à l'authentification par mots de passe en particulier.

Ce guide traite de l'authentification pour tout type d'accès, c'est-à-dire du déverrouillage d'un terminal (poste Windows, Linux, etc.), de l'accès à des comptes à privilèges (par des administrateurs par exemple), de l'accès à des applications web (privées ou publiques), etc.

Les recommandations de ce guide doivent être analysées vis-à-vis du contexte dans lequel l'authentification s'effectue. En effet, l'authentification sur un site de réservation d'un terrain de tennis et l'authentification sur un réseau contenant des données sensibles ne font pas face aux mêmes menaces et n'ont donc pas les mêmes besoins de sécurité.

Ce guide a donc également pour objectif de constituer un support technique pour accompagner une analyse de risque sur l'authentification.

Ce guide se focalise uniquement sur le cas de l'authentification de personnes vis-à-vis de machines. En comparaison de l'authentification de machines entre elles, l'authentification de personnes vis-à-vis de machines est plus exposée aux attaques et plus vulnérable à des erreurs humaines, ce qui augmente la probabilité d'une compromission de divers secrets et donc d'une usurpation d'identité. L'authentification de personnes vis-à-vis de machines et celui de machines entre elles partagent de nombreuses problématiques communes, certaines recommandations de ce guide sont donc également valables pour ce dernier cas. Des éléments de réponse supplémentaires peuvent être trouvés dans les annexes B1 [13], B2 [12] et B3 [11] du RGS, en particulier concernant le choix et le dimensionnement des mécanismes cryptographiques impliqués dans l'authentification.

Les principales recommandations qui sont mises en avant dans ce guide sont résumées ci-après.

- Mener une analyse de risque lors de la mise en place de moyens d'authentification.
- Privilégier l'utilisation de l'authentification multifacteur (cf. section 2.4).
- Privilégier l'utilisation de l'authentification reposant sur un facteur de possession (cf. section 2.4).
- Adapter la robustesse d'un mot de passe à son contexte d'utilisation.

- Utiliser un coffre-fort [1] de mots de passe.

Le guide de recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection [8] traite les problématiques liées à l'authentification dans le cadre du contrôle d'accès physique.

Ce guide est complémentaire de l'ensemble des recommandations émises par la CNIL [23, 26] concernant l'authentification de personnes et la gestion des authentifiants comme les mots de passe.

Ce guide est à destination d'un large public :

- des personnes ayant un rôle de développement ou d'intégration dans le cadre de la mise en place d'une solution d'authentification ;
- des personnes ayant un rôle d'administration dans le cadre de la configuration des divers outils permettant l'authentification sur le système d'information placé sous leur responsabilité ;
- des personnes ayant une responsabilité (par exemple DSI ou RSSI) dans le cadre de la définition des objectifs de sécurité en matière d'authentification ;
- des utilisateurs finaux des divers moyens d'authentification, en particulier les mots de passe.

1.2 Organisation du guide

Le chapitre 2 définit ce qu'est l'authentification, l'authentification forte et l'authentification multifcateur, les différentes menaces et attaques pesant sur l'authentification et présente des éléments de contexte à prendre en compte lors de la mise en place d'un moyen d'authentification.

Le chapitre 3 présente le cycle de vie générique d'un facteur d'authentification (de la création à la révocation en passant par l'utilisation des facteurs d'authentification) et formule des recommandations associées.

Les chapitres suivants présentent des recommandations liées à l'utilisation d'un facteur de connaissance tel qu'un mot de passe (chapitre 4), à l'utilisation d'un facteur de possession tel qu'une carte à puce (chapitre 5) et à l'utilisation d'un facteur inhérent telle qu'une empreinte digitale (chapitre 6).

1.3 Convention de lecture

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* est volontairement plus prescriptive que la formulation *il est recommandé*.

Pour certaines recommandations de ce guide, il est proposé plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

1. Dans ce guide, le terme de coffre-fort est préféré au terme de gestionnaire (plus couramment rencontré) afin de mettre en avant la protection des mots de passe stockés que ces outils offrent.

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

R -

Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

R --

Recommandation alternative de second niveau

Cette recommandation permet de mettre en œuvre une seconde alternative, d'un niveau de sécurité moindre que les recommandations R et R -.

La liste récapitulative des recommandations est disponible en page 43.

1.4 Glossaire et acronymes

Analyse de risque. Ensemble du processus permettant l'identification, l'évaluation et le traitement des risques.

Attaque de l'homme-du-milieu. Une attaque où un attaquant est positionné entre deux parties communicantes (entre le prouveur et le vérifieur [2] dans le contexte de l'authentification) dans le but d'intercepter ou de modifier des informations transitant entre les deux parties. On parle de *man-in-the-middle attack* en anglais.

Attaque par rejeu. Une attaque où un attaquant parvient à récupérer des informations d'authentification (comme un mot de passe ou son empreinte) et à utiliser ces informations pour les rejouer afin d'usurper l'identité du prouveur.

Authentification. Processus consistant à vérifier la preuve d'une identité précédemment annoncée grâce à un moyen d'authentification.

Authentification multifacteur. Authentification mettant en œuvre plusieurs facteurs d'authentification appartenant à des types différents.

CC. Critères Communs (*Common Criteria* en anglais).

CNIL. Commission nationale de l'informatiques et des libertés.

Code PIN. *Personnal Identification Number*, code d'identification personnel en français.

2. Voir la section 2.1 pour la définition des termes prouveur et vérifieur.

Coffre-fort de mots de passe. Logiciel permettant de centraliser le stockage chiffré et la gestion des mots de passe.

Compte à privilèges. Compte disposant de droits élevés sur le système d'information comme un compte administrateur.

CSPN. Certification de sécurité de premier niveau.

Facteur d'authentification. Un facteur (lié à une personne dans le contexte de ce guide) appartenant à l'un des types de facteur suivant : *facteur de connaissance*, *facteur de possession* et *facteur inhérent*.

FIDO U2F et FIDO 2. Norme d'authentification visant à simplifier l'utilisation de l'authentification multifacteur, actuellement géré par la *FIDO Alliance*.

Hameçonnage (*phishing* en anglais). Technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (identifiants, mots de passe, etc.) ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

IPsec. *Internet Protocol Security* est une suite de protocoles de communication sécurisée permettant la protection des flux réseau (couche 3 du modèle *OSI*).

Kerberos. *Kerberos* est un protocole d'authentification très répandu reposant sur un mécanisme de tickets.

Moyen d'authentification. Élément qui est généralement connu ou possédé uniquement par l'utilisateur et qui permet de l'authentifier de manière unique (comme un mot de passe, une clé privée d'un certificat électronique, etc.). Il s'agit d'une preuve utilisée pour démontrer son identité.

OTP. *One-Time Password*, dont la traduction est mot de passe à usage unique en français.

Protocole d'authentification. Protocole au moyen duquel un vérifieur s'assure de l'authenticité de l'identité d'un prouveur.

RGPD. Règlement général sur la protection des données.

RGS. Référentiel général de sécurité.

TLS. *Transport Layer Security* est un protocole de communication sécurisé permettant la protection des flux réseau (couche 5 du modèle *OSI*).

2
Authentification

Objectif

Ce chapitre va tout d'abord donner une définition de l'authentification et des éléments qui y sont associés. Après avoir défini l'utilisation d'une authentification simple (c.-à-d. au moyen d'un seul facteur comme un mot de passe), les définitions liées à l'authentification multifacteur sont introduites. Enfin, ce chapitre explicite les distinctions entre l'authentification forte (c.-à-d. employant un protocole cryptographique considéré fort) et l'authentification multifacteur.

2.1 Authentification et premières définitions

L'authentification est un mécanisme faisant intervenir deux entités distinctes : un **prouveur** et un **vérifieur** comme illustré par la figure 1.

- Le **prouveur** cherche à prouver son identité au vérifieur. Il s'agit par exemple pour le prouveur de démontrer sa connaissance d'une donnée secrète comme un mot de passe.
- Le **vérifieur** doit être capable de s'assurer de la validité de l'identité du prouveur. Il s'agit par exemple pour le vérifieur de contrôler l'exactitude du mot de passe fourni par le prouveur.

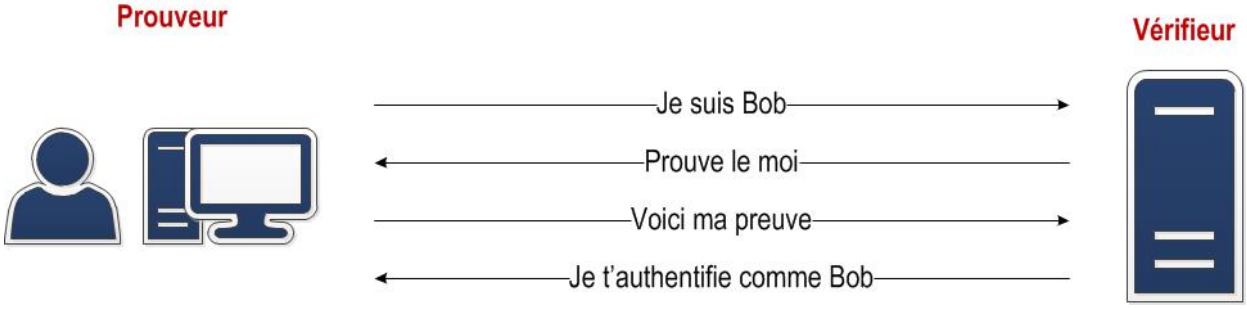

FIGURE 1 – Représentation générique d'une authentification

Un prouveur est un utilisateur du système d'information cherchant à s'authentifier. Le vérifieur est quant à lui classiquement un serveur du système d'information qui a la charge de vérifier l'identité d'un utilisateur.

Une étape préalable à l'authentification est l'étape de l'**enregistrement**. Cette étape consiste à enregistrer un prouveur (son identité, son moyen d'authentification, etc.) auprès d'un vérifieur. Cela correspond par exemple à la création d'un compte sur un site Web.

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

La fonction d'**authentification** en tant que telle a pour objectif de permettre au prouveur de démontrer son identité (souvent annoncée lors de la phase d'identification).

Le prouveur va ainsi prouver son identité au vérifieur grâce à un **moyen d'authentification**, élément qui est généralement connu ou possédé uniquement par le prouveur et qui permet de l'authentifier de manière unique. Ce moyen d'authentification peut prendre par exemple la forme d'un mot de passe, d'une donnée biométrique ou bien de la clé privée associée à un certificat électronique contenu dans une carte à puce. Le moyen d'authentification est créé lors de l'enregistrement.

Une fois l'authentification réalisée, cette dernière (ou un autre service) va permettre d'**autoriser l'accès** d'un utilisateur (selon des critères propres à chaque utilisateur) à des ressources (données, services, applications, etc.).

Prenons l'exemple d'une authentification basique comme l'utilisation du couple nom d'utilisateur/-mot de passe pour accéder à une application Web. Cette authentification met en jeu un nom d'utilisateur qui est utilisé pour identifier l'utilisateur. Le moyen d'authentification est ici la connaissance du mot de passe qui sert ainsi à prouver l'identité précédemment annoncée. Une fois l'authentification vérifiée, l'accès à l'application Web est autorisé.

2.2 Menaces et attaques sur l'authentification

Menaces et attaques génériques

La prise de contrôle de comptes utilisateurs avec peu de privilèges voire de comptes administrateurs avec de nombreux privilèges, est un des objectifs majeurs des attaquants. Elle peut avoir des conséquences variées allant de la récupération d'informations personnelles à la compromission d'un système d'information.

La principale menace contre laquelle l'authentification cherche à se protéger est l'usurpation d'identité, qui consiste pour un attaquant à se faire passer pour un utilisateur légitime auprès du vérifieur.

Il est possible de distinguer deux grands types d'attaquants.

- Attaquant *en ligne* : l'attaquant peut uniquement interagir avec le serveur d'authentification pour tenter de retrouver une valeur secrète (un mot de passe ou une clé privée par exemple). Il doit par exemple être capable d'interagir avec un serveur Web afin de réaliser son attaque.
  Se protéger contre des attaquants en ligne nécessite de mettre en place des mesures spécifiques, comme le blocage temporaire de l'accès au compte pendant plusieurs secondes, voire minutes, après un certain nombre d'essais infructueux (cf. recommandation R10).
- Attaquant *hors ligne* : l'attaquant peut interagir avec le serveur d'authentification, et a également accès aux données permettant au vérifieur de contrôler l'identité du prouveur (par exemple des empreintes de mots de passe ou une clé publique). L'attaquant n'a pas besoin d'interagir avec le serveur pour réaliser son attaque et a alors accès à une puissance de calcul potentiellement très importante.
  Se protéger contre des attaquants hors ligne nécessite que le vérifieur protège correctement les données permettant de contrôler l'identité des utilisateurs lors de l'authentification, par

exemple en utilisant des fonctions de hachage dédiées pour le stockage des mots de passe (cf. section 4.6) ou en utilisant des protocoles d'authentification considérés comme forts (cf. section 2.5).

De nombreux types d'attaques peuvent être menés contre un protocole d'authentification pour parvenir à usurper une identité. Voici une liste non exhaustive de ces attaques et des illustrations de leur mise en pratique :

- les attaques par force brute : tests automatisés de tous les mots de passe et de toutes les clés cryptographiques possibles ;
- les attaques sur le protocole d'authentification : attaques de l'homme-du-milieu, attaques par rejeu, exploitation de vulnérabilité de l'implémentation, etc. (voir section 2.5 pour plus de détails) ;
- le vol du moyen d'authentification : vol d'une carte à puce, récupération d'un mot de passe par hameçonnage, manipulation par l'ingénierie sociale, etc.

Certains protocoles d'authentification prennent en compte ces différentes attaques alors que d'autres méthodes nécessitent des mesures complémentaires afin d'en atténuer les conséquences.

Des menaces spécifiques pesant sur les différents facteurs d'authentification d'une authentification multifacteur (cf. la définition en section 2.4) sont présentées dans la suite de cette section.

Menaces et attaques sur les facteurs de connaissance

Les principales menaces pesant sur les facteurs de connaissance sont la déduction (au moyen d'attaques par recherche exhaustive ou par dictionnaire par exemple), l'hameçonnage, l'écoute (dans le cas où l'envoi du facteur de connaissance est effectué au travers d'un canal non protégé), etc. Les mots de passe, souvent choisis par les utilisateurs, font ainsi face à des attaques spécifiques.

- **Attaque par recherche exhaustive.** Cette attaque consiste à choisir un ensemble de caractères et à tester automatiquement toutes les combinaisons possibles de ces caractères. Une variante de cette attaque, désignée par l'expression anglaise *password spraying*, consiste à effectuer des tests automatisés d'un nombre réduit de mots de passe (par exemple à partir d'une liste de mots de passe très utilisés) mais pour un grand nombre d'identifiants possibles (ou de comptes de différents service web par exemple).
- **Attaque par dictionnaire.** Cette attaque consiste à faire l'hypothèse que le mot de passe recherché est un mot du dictionnaire d'une langue donnée et à tester automatiquement chacun de ces mots. Des dictionnaires plus aboutis intègrent également des variations courantes sur les mots du dictionnaire (transformation de a en @ par exemple), une liste des mots de passe ou des phrases de passe les plus utilisés ou bien encore une combinaison (concaténation, etc.) de mots connus.
- **Attaque par tables pré-calculées (par exemple les *rainbow tables*).** Cette attaque consiste à calculer à l'avance [3] les empreintes cryptographiques d'un très vaste ensemble de mots de passe

3. Le calcul des empreintes est consommateur de ressources de calcul, à plus forte raison si le nombre de mots de passe considéré est important.

afin d'accélérer leur recherche, puis de comparer automatiquement chacune d'entre elles à une empreinte volée jusqu'à trouver une égalité qui prouvera que le mot de passe recherché a été trouvé.

- **Attaque par ingénierie sociale.** Cette attaque consiste à récupérer un mot de passe par des moyens détournés comme l'hameçonnage ou bien l'usurpation d'identité.

Le tableau 1 résume les différentes menaces pesant sur la gestion des mots de passe ainsi que les contre-mesures possibles associées.

Menace	Contre-mesures
Recherche exhaustive	Limite temporelle entre chaque essai (contre les attaquants en ligne) et fonctions de hachage itératives dédiées (contre les attaquants en ligne et hors ligne)
Recherche par dictionnaire	Mots de passe robustes et aléatoires et coffre-fort de mots de passe
Tables pré-calculées (*rainbow table*)	Sel aléatoire long
Hameçonnage, ingénierie sociale	Authentification multifacteur

TABLE 1 – Récapitulatif des menaces et contre-mesures sur les mots de passe

Menaces et attaques sur les facteurs de possession

Les principales menaces pesant sur les facteurs de possession sont le vol, la perte, la duplication, la falsification ou bien encore la compromission totale de l'équipement qui porte le facteur de possession. Afin de réaliser une usurpation d'identité, les attaquants vont chercher à récupérer les secrets cryptographiques contenus dans le facteur de possession via par exemple des attaques par canaux auxiliaires.

Menaces et attaques sur les facteurs inhérents

Les principales menaces pesant sur les facteurs inhérents (couramment appelés facteurs biométriques) visent à leurrer le mécanisme de reconnaissance biométrique en usurpant l'identité de la personne physique, par exemple par la présentation d'une photographie ou d'une séquence vidéo préenregistrée ou altérée, ou d'un moulage de l'empreinte digitale.

2.3 Aperçu des limites de l'authentification par mots de passe

Le couple identifiant et mot de passe est le moyen d'authentification le plus répandu, une des raisons principales étant sa facilité de mise en œuvre et d'utilisation. En effet, du point de vue de l'utilisateur, il s'agit simplement de mémoriser un mot ou une phrase de passe, et de saisir cet élément secret mémorisé au moment d'une authentification. Du point de vue de l'administration

ou du développement, la gestion se révèle également plutôt simple : cela consiste à calculer des empreintes cryptographiques des mots de passe et à les comparer avec celles présentes dans une base de données afin de valider ou invalider l'authentification.

Cette simplicité d'utilisation est néanmoins contrebalancée par des limitations en termes de sécurité. La mémorisation des mots de passe est une des principales limitations de cette méthode d'authentification ayant de forts impacts en matière de sécurité. Une des bonnes pratiques concernant la gestion des mots de passe est d'utiliser des mots de passe différents pour chaque service ou compte (cf. recommandation R33). Le nombre de mots de passe à retenir pouvant alors devenir élevé, le comportement des utilisateurs est généralement de choisir des mots de passe facilement mémorisables, par exemple provenant d'informations personnelles (date de naissance, nom de famille, etc.), de mots provenant du dictionnaire de leur langue, ou encore des mots de passe très utilisés (« motdepasse », « azerty », « 123456 », etc.). Les mots de passe créés de cette manière sont très facilement exploitables par des attaquants : un mot de passe appartenant à ces catégories sera « cassé » (c.-à-d. retrouvé par un attaquant) en quelques minutes.

Une autre bonne pratique est de choisir des mots de passe dits robustes (cf. recommandation R32) : ils doivent être suffisamment longs, suffisamment complexes (avec l'utilisation de minuscules, majuscules, chiffres et caractères spéciaux). Un mot de passe sera d'autant plus robuste qu'il aura été généré de manière aléatoire. Néanmoins, étant donné le grand nombre de comptes et de services pour lesquels un utilisateur doit s'authentifier à des fréquences variables, mémoriser un grand nombre de mots de passe robustes peut s'avérer difficile, voire impossible s'ils sont aléatoires. La gestion et la mémorisation d'un grand nombre de mots de passe aléatoires et robustes étant difficilement envisageable sans l'aide d'un outil de gestion de mots de passe comme un coffre-fort de mots de passe, les personnes soumises à ce type de contraintes auront la fâcheuse tendance à utiliser un même mot de passe pour s'authentifier sur plusieurs services ou comptes différents.

L'utilisation d'un même mot de passe sur plusieurs services peut devenir très problématique en cas d'incident de sécurité impliquant les serveurs où le vérifieur stocke les données (c.-à-d. les empreintes cryptographiques des mots de passe) lui permettant de valider l'authentification. L'accès à ces données très sensibles n'est parfois pas correctement protégé, ce qui peut conduire à d'importantes brèches de sécurité : par exemple la fuite d'une base de données pouvant contenir des millions de mots de passe d'utilisateurs. La réutilisation d'un même mot de passe devient ainsi problématique lors de tels incidents et va impacter les différents services ou comptes partageant un même mot de passe, que le mot de passe soit robuste (et même aléatoire) ou non.

L'utilisation d'un coffre-fort de mots de passe est une solution intéressante aux problèmes de mémorisation de multiples mots de passe robustes (cf. recommandation R34). Un coffre-fort de mots de passe permet de stocker des mots de passe sans que l'utilisateur ait besoin de les mémoriser. De nombreux coffres-forts de mots de passe offrent également la possibilité de générer des mots de passe robustes. Ces mots de passe sont alors conservés dans une base de données dédiée et chiffrée par un mot de passe dit « maître », le seul qui doit alors être mémorisé par l'utilisateur.

Néanmoins, ce type d'outil ne permet pas d'empêcher les attaques d'ingénierie sociale comme l'hameçonnage. Ce genre d'attaque permet de récupérer en particulier les mots de passe en usant de moyens détournés : convaincre une personne par téléphone ou courriel d'envoyer son mot de passe, inciter une personne à cliquer sur un lien frauduleux falsifiant une vraie page d'authentification, etc. Également, ces outils restent assez sensibles à la compromission par des logiciels

malveillants (comme des enregistreurs de frappe ou *keylogger* en anglais) des équipements sur lesquels ils sont installés.

Le dispositif d'assistance aux victimes d'actes de cybermalveillance [16] propose de nombreuses ressources afin de prévenir ou de réagir face à ce genre de menaces.

Au vu du large déploiement des mots de passe ainsi que de leur facilité d'utilisation et de gestion, il convient de comprendre les limites liées à leur emploi et d'atténuer ces limites grâce à d'autres mécanismes.

Un des mécanismes permettant d'augmenter la sécurité des authentifications par mots de passe est d'ajouter un ou plusieurs éléments d'authentifications supplémentaires, ayant une forme différente du mot de passe : il s'agit de **l'authentification multifacteur** (cf. recommandation R1). Pour valider l'authentification, chacun des facteurs d'authentification la composant doit être validé. Un des buts de ce guide est en particulier de proposer des recommandations concernant l'utilisation de l'authentification multifacteur.

2.4 Qu'est-ce que l'authentification multifacteur ?

L'authentification multifacteur découle de la nécessité de renforcer la sécurité apportée par l'utilisation d'un unique facteur d'authentification, particulièrement lorsqu'il s'agit d'un mot de passe utilisé seul. Ainsi même si ce dernier est compromis, un facteur supplémentaire d'un type différent est requis afin de s'authentifier.

Un facteur d'authentification est donc un facteur lié à une personne, relevant de diverses catégories :

- facteur de connaissance : « ce que je sais », il s'agit d'une connaissance devant être mémorisée telle qu'une phrase de passe, un mot de passe, un code, etc ;
- facteur de possession : « ce que je possède », il s'agit d'un élément secret non mémorisable contenu dans un objet physique qui idéalement protège cet élément de toute extraction, tel qu'une carte à puce, un *token*, un téléphone, etc ;
- facteur inhérent : « ce que je suis », il s'agit d'une caractéristique physique intrinsèquement liée à une personne et indissociable de la personne elle-même, telle qu'une caractéristique biologique (ADN), morphologique (empreinte digitale, empreinte rétinienne) ou comportementale [4] (voix, frappe au clavier).

Attention

Un type de facteur parfois rencontré est le facteur « où je suis », permettant de détecter la localisation géographique d'une personne grâce à la connexion à un ordinateur au sein d'un réseau spécifique (par l'adresse IP par exemple) ou via un signal GPS. Au vu des possibilités de contournement et de la faible maturité des technologies pouvant exploiter cet autre type de facteur, il convient d'être prudent vis-à-vis de

4. Comme l'authentification reposant sur des comportements est une technologie récente, elle dispose de moins de maturité et est moins maîtrisée qu'une technologie utilisée depuis de nombreuses années comme la biométrie.

leur utilisation au sein d'un mécanisme d'authentification.

Authentification multifacteur

Une authentification multifacteur permet de prouver l'identité d'un utilisateur par la vérification de plusieurs éléments, appelés **facteurs d'authentification**. Chacun des facteurs d'authentification mis en œuvre doit appartenir à une catégorie de facteur différente. L'absence d'un des facteurs nécessaire à une authentification multifacteur doit faire échouer l'authentification.

L'appartenance à une catégorie différente pour chacun des facteurs utilisés est un point important de cette définition. Une authentification qui nécessiterait un code PIN et un mot de passe ne peut pas être considérée comme multifacteur : les deux facteurs utilisés appartiennent à la même catégorie (facteur de connaissance) et sont donc sujets aux mêmes menaces. En revanche, selon le contexte de la mise en œuvre et, bien que l'on ne puisse pas considérer cela comme de l'authentification multifacteur, l'utilisation de plusieurs facteurs appartenant à la même catégorie peut permettre d'améliorer la sécurité apportée par l'authentification par rapport au cas d'un unique facteur. On parle alors de double authentification.

R1

Privilégier l'authentification multifacteur

Il est recommandé de privilégier l'utilisation d'une authentification multifacteur, c'est-à-dire une authentification mettant en œuvre plusieurs facteurs d'authentification appartenant à une catégorie de facteur différente parmi les facteurs de connaissance, de possession et inhérent.

Le contrôle de l'authentification par le vérifieur peut se faire de deux façons différentes :

- le vérifieur vérifie directement l'ensemble des facteurs d'authentification (par exemple un mot de passe et une authentification FIDO U2F) ;
- le vérifieur ne vérifie directement qu'une sous-partie des facteurs d'authentification (par exemple dans le cas d'un code PIN déverrouillant une carte à puce, le code PIN n'est vérifié que localement sur la carte).

Ces deux méthodes de vérifications sont considérées comme de l'authentification multifacteur mais doivent être étudiées minutieusement lors de l'analyse de risque. En effet, elles comportent des risques différents qui doivent être couverts par des moyens différents (augmentation de la surface d'attaque lorsque plusieurs facteurs doivent être vérifiés, confiance de la bonne vérification des facteurs qui ne sont pas directement vérifiés par le vérifieur, etc.).

Pour chacun de ces types de facteurs, le prouveur doit démontrer au vérifieur la connaissance, la possession ou l'attribut physique correspondant au facteur. Dans la suite, des précisions sont données concernant les définitions et les emplois de ces différents types de facteurs.

- Un facteur de connaissance, comme un code PIN ou un mot de passe, ne doit être connu que de son propriétaire. Le vérifieur ne doit pas connaître le facteur de connaissance, mais uniquement une version *non réversible* de ce facteur, comme l'empreinte d'un mot de passe calculée au moyen d'une fonction de hachage cryptographique dédiée au stockage des mots de passe

(cf. section 4.6). Des mesures et bonnes pratiques doivent être mises en place afin de limiter les risques qu'un adversaire ne puisse deviner le facteur de connaissance, à la fois pour le prouveur et le vérifieur (voir chapitre 4).

- Un facteur de possession doit être un équipement attribué à un unique utilisateur. Afin de garantir la sécurité apportée par ce facteur, il est essentiel que des moyens de protection et de détection contre les tentatives de reproduction ou de falsification du facteur soient mis en place. Un facteur de possession peut être une carte à puce contenant une clé privée, une carte SIM d'un téléphone mobile comportant des données d'identification, ou un dispositif permettant de générer des codes à usage unique (OTP).
- Un facteur inhérent doit permettre d'identifier une personne de façon unique au moyen d'attributs physiques comme les empreintes digitales, les empreintes palmaires, la forme du visage, la forme de l'iris, etc. Ainsi ces facteurs inhérents doivent être différents d'une personne physique à l'autre, y compris lorsque des personnes physiques présentent des caractéristiques similaires (par exemple des jumeaux ou jumelles).

L'un des avantages du point de vue de la sécurité apportés par l'authentification multifacteur est qu'un attaquant, afin d'usurper une identité, doit avoir accès à tous les facteurs d'authentification pour réussir son usurpation. Ainsi, lors d'une authentification à l'aide d'un mot de passe et d'un autre facteur, même si le mot de passe est compromis, un attaquant doit encore récupérer le ou les autres facteurs afin d'usurper l'identité du prouveur lors de la phase d'authentification.

2.5 Authentification forte : distinction avec l'authentification multifacteur

En langue française, l'authentification multifacteur est souvent confondue avec l'appellation authentification forte (ou robuste), ce qui laisserait entendre qu'une authentification multifacteur est nécessairement plus robuste qu'une authentification avec un unique facteur.

Il convient ainsi de différencier authentification multifacteur et authentification forte. D'une part, une authentification multifacteur est une authentification faisant intervenir plusieurs catégories de facteurs. Néanmoins, ces facteurs, pris indépendamment ou ensemble, ne sont pas forcément considérés comme étant forts (un exemple typique étant un mot de passe associé à un code temporaire reçu par SMS). D'autre part, une authentification forte (qui repose généralement sur un facteur unique) est une authentification reposant sur un mécanisme cryptographique dont les paramètres et la sécurité sont jugés robustes (l'élément secret est alors généralement une clé cryptographique).

Les protocoles d'authentification que l'on peut considérer comme forts reposent souvent sur des protocoles dits *défi-réponse*. Le message envoyé par le prouveur pour s'authentifier dépend à la fois d'une clé secrète, mais aussi d'un défi variable envoyé par le vérifieur. Lorsqu'un prouveur souhaite prouver son identité à un vérifieur, ce dernier lui envoie alors un défi (une valeur aléatoire par exemple) et le prouveur doit lui transmettre une réponse calculée à partir de ce défi spécifique (une signature de ce défi par exemple).

Afin d'être considérée comme forte, une authentification doit reposer sur un protocole cryptographique permettant de résister à certaines attaques comme :

- l'écoute clandestine (*eavesdroppping* en anglais), qui consiste pour un attaquant à passivement écouter le canal de communication entre le prouveur et le vérifieur ;
- les attaques par rejeu, qui consistent pour un attaquant à récupérer des informations d'authentification (comme un mot de passe ou son empreinte) et à utiliser ces informations pour les rejouer afin d'usurper l'identité de la cible (l'attaque *pass-the-hash* [21] en est un exemple) ;
- les attaques de l'homme-du-milieu, qui consistent pour un attaquant à intercepter et modifier les communications se déroulant entre le prouveur et le vérifieur lors de l'authentification sans être détecté ;
- la non-forgeabilité : l'observation par un attaquant de plusieurs échanges d'authentification d'un prouveur ne doit pas lui permettre d'usurper son identité dans un nouvel échange d'authentification.

Parmi les exemples d'authentification forte reposant sur un facteur de possession, on peut citer :

- l'authentification par certificats (stockés dans des cartes à puce par exemple) ;
- les protocoles FIDO2 et FIDO U2F [4] ;
- les protocoles d'OTP (*One-Time Password*) comme HOTP (HMAC-based OTP [32]), TOTP (Time-based OTP [34]) ou OCRA (OATH Challenge-Response Algorithm [33]).

Dans chacun de ces cas, le prouveur prouve son identité au vérifieur en démontrant indirectement la possession d'une clé cryptographique qui doit rester secrète.

Parmi les exemples d'authentification forte reposant sur un facteur de connaissance, on peut citer :

- le protocole *Kerberos* [27] ;
- les protocoles de type PAKE (Password-Authenticated Key Agreement) comme SPAKE2 [3] ou OPAQUE [20].

On peut ainsi différencier une authentification multifacteur « faible » d'une authentification multifacteur forte lorsque cette dernière fait intervenir au moins un facteur d'authentification considéré comme fort.

R2

Privilégier l'utilisation de moyens d'authentification forts

Il est recommandé de privilégier l'utilisation de moyens d'authentification forts reposant sur des mécanismes cryptographiques conformes au RGS et à ses annexes B1 [13], B2 [12] et B3 [11].

2.6 Éléments supplémentaires à considérer dans le choix des moyens d'authentification en fonction du contexte

L'authentification est un mécanisme fortement dépendant du contexte dans lequel il est mis en œuvre. Ce contexte peut être varié et de nombreux paramètres entrent en jeu comme le niveau

de sensibilisation des utilisateurs à la sécurité, le niveau de sensibilité des données ou des services à protéger, l'importance des menaces pesant sur les données à protéger, le niveau de compétence des différentes personnes impliquées dans la gestion du système d'information ou le niveau de complexité d'utilisation des différents moyens d'authentification mis en place, etc.

Le tableau 2 présente des cas permettant d'illustrer les différences qui peuvent exister concernant l'authentification en fonction du contexte d'utilisation. Ces différents cas d'usage n'ont pas les mêmes besoins de sécurité. Ainsi toutes les recommandations de ce guide ne s'appliquent pas nécessairement à tous ces cas.

Exemple de contexte	**Sensibilité des données ou du service**	**Importance de la menace**	**Moyen d'authentification**
Plate-forme de réservation de terrain de tennis	Peu sensible	Faible (modification de la réservation)	Mot de passe
Site Web publicitaire	Moyennement sensible	Moyenne (interruption ou défiguration du site)	Mot de passe robuste
Messagerie professionnelle	Sensible	Moyenne (interruption du service, compromission d'informations métier sensibles, qui peuvent être d'ordre industriel, financier, concurrentiel, etc.)	Mot de passe robuste + second facteur possible
Système d'information d'administration	Très sensible	Importante (compromission complète du système d'information)	Multifacteur fort (ex. : carte à puce et code PIN)

Table 2 – Différents contextes d'utilisation de l'authentification

Ainsi les recommandations de ce guide sont d'ordre général et doivent être adaptées selon le contexte d'utilisation. Pour cela, il est recommandé de recourir à une méthodologie d'analyse de risque éprouvée (par exemple la méthode EBIOS *Risk Manager* [7]) permettant, au terme du processus et selon des critères prédéterminés, d'identifier la meilleure solution d'authentification à mettre en œuvre. Ces critères doivent notamment tenir compte des menaces potentielles, de la criticité du service ou des informations traitées par ce dernier et de son niveau d'exposition aux menaces. Par exemple, comme illustré dans le tableau 2, dans le cas d'une plate-forme de réservation de terrain de tennis, il n'est sans doute pas pertinent de mettre en place une authentification multifacteur au vu de la faible sensibilité des données en jeu. À l'inverse, utiliser un mot de passe seul lorsque des données ou services fortement sensibles sont en jeu n'est pas suffisant.

R3

Conduire une analyse de risque

Il est recommandé de mener une analyse de risque pour déterminer les moyens d'authentification à mettre en œuvre en fonction du besoin de sécurité.

Attention

L'authentification multifacteur ne doit pas donner un faux sentiment de sécurité dès lors qu'elle est mise en place. Son intérêt principal est d'éviter qu'un attaquant ne puisse se connecter directement au service ciblé lorsque l'un des secrets d'authentification a été compromis. Cela n'empêchera nullement un attaquant d'utiliser un canal de connexion déjà ouvert vers ce service si jamais, par exemple, le poste est compromis. Les postes de travail, les services s'assurant de la vérification de l'authentification et les différents services protégés par l'authentification ne doivent pas s'affranchir des autres mesures de sécurisation nécessaires pour garantir un niveau de sécurité en adéquation avec le niveau visé. Le chapitre 3 propose des recommandations sur de telles mesures liées au cycle de vie d'une authentification.

De nombreux autres éléments pouvant avoir un impact sur la sécurisation de l'authentification doivent être pris en compte dans l'analyse de risque.

- **L'expérience utilisateur et la facilité d'utilisation.** Mettre en place des moyens d'authentification trop contraignants par rapport à l'information ou au service à protéger pourrait se révéler contre-productif puisque les utilisateurs chercheraient à contourner les moyens mis en place. Par exemple, un renouvellement de mots de passe trop fréquent pourrait inciter les utilisateurs à noter les mots de passe sur une feuille, qui ne sera pas nécessairement conservée en lieu sûr.
- **La complexité de gestion et d'administration.** La mise en place d'une authentification multifacteur implique une augmentation de la charge de travail d'exploitation du fait de devoir gérer le déploiement et le cycle de vie de plusieurs facteurs.
- **Le contexte opérationnel.** Certains services, bien que critiques et soumis à d'importantes menaces, comme le réseau électrique ou bien des systèmes industriels sensibles, doivent réagir de manière rapide en cas d'incident de production. Dans ce cadre opérationnel particulier et pour des besoins de réactivité importants, il peut être justifié de mettre en place une authentification simple (un code PIN), et ce malgré la criticité du service. Dans ces cas particuliers, cet affaiblissement consenti du niveau d'authentification doit être compensé par d'autres mesures de sécurité (par exemple des mesures physiques ou organisationnelles).
- **L'augmentation de la surface d'attaque.** Dans de nombreux cas d'usage, la gestion des nouveaux facteurs d'authentification est réalisée grâce à l'utilisation de divers outils qui doivent être intégrés au sein du système d'information. Ces outils, s'ils sont mal configurés, peuvent considérablement augmenter la surface d'attaque du système d'information.

3
Recommandations concernant le cycle de vie des facteurs d'authentification

Objectif

Le but de ce chapitre est de décrire de manière générique le cycle de vie d'un facteur d'authentification, quel qu'il soit, et de formuler des recommandations allant de sa création jusqu'à sa révocation, en passant par son utilisation au cours de sa durée de vie.

Le cycle de vie d'un facteur d'authentification peut se décomposer en trois phases : sa création (et sa remise à l'utilisateur), son utilisation et sa révocation.
De nombreuses recommandations de ce chapitre proposent des mécanismes ayant pour objectif de limiter l'impact d'une usurpation d'identité (par la compromission d'un facteur d'authentification) et de favoriser la détection d'une telle usurpation d'identité. Des recommandations d'ordre général vis-à-vis de ce cycle de vie sont proposées dans ce chapitre. Des recommandations spécifiques à chaque catégorie de facteurs sont détaillées dans les chapitres 4, 5 et 6 et concernant respectivement les facteurs de connaissance, les facteurs de possession et les facteurs inhérents.

3.1 Création et renouvellement des facteurs d'authentification

Les phases de création et d'enregistrement d'un facteur d'authentification sont des étapes primordiales et critiques pour toute authentification. Un attaquant qui parviendrait à récupérer ou modifier des informations d'authentification lors de l'enregistrement, ou bien encore des éléments cryptographiques qui ne seraient pas générés correctement (voir par exemple le retrait de certains facteurs matériels d'authentification présentant un défaut de générateur aléatoire [35]) sont autant de vecteurs d'attaque qui peuvent alors compromettre le reste de l'authentification.

R4

Créer les facteurs d'authentification dans un environnement maîtrisé

Il est recommandé de créer les facteurs d'authentification dans un environnement maîtrisé par l'entité chargée de sa création. Les méthodes d'enregistrement et de remise du facteur d'authentification doivent être cohérentes avec le niveau de sécurité attendue de l'authentification.

Par exemple, la création et l'initialisation d'une carte à puce pourrait s'effectuer sur un poste déconnecté avec une remise en main propre à l'utilisateur pour procéder à une vérification d'identité en face-à-face.

R5

Générer les éléments aléatoires avec un générateur de nombres aléatoires robuste

Il est recommandé de générer les éléments aléatoires nécessaires à l'authentification (comme des clés cryptographiques par exemple) au moyen d'un générateur de nombres aléatoires robuste conforme à l'annexe B1 du RGS [13].

R6

Remettre les facteurs d'authentification au travers de canaux sécurisés

Dans le cas où le facteur d'authentification est remis à l'utilisateur (cas d'une carte à puce par exemple), il est recommandé de privilégier la remise en main propre car elle rend possible la vérification d'identité présentant le meilleur niveau d'assurance.
Dans le cas d'une remise à distance, il est recommandé que les canaux et moyens de transmission utilisés pour délivrer le facteur d'authentification soient protégés en intégrité, authenticité et confidentialité.
La vérification de l'identité à distance est également possible et est réglementée par le référentiel d'exigences applicables aux prestataires de vérification d'identité à distance (PVID) [2].

Le renouvellement d'un facteur d'authentification consiste pour un utilisateur à modifier lui-même (ou à pouvoir faire la demande de modification de) son facteur d'authentification, en utilisant le fait que son facteur d'authentification actuel est toujours valide. Par exemple pour un mot de passe, le renouvellement consiste à s'authentifier grâce à son mot de passe actuel (qui est toujours valide) puis à le modifier.

Le processus de renouvellement peut être plus allégé qu'un processus complet de création d'un facteur d'authentification. En effet, l'utilisateur effectuant cette demande est toujours de confiance vis-à-vis du système d'information et son facteur d'authentification actuel est toujours valide. Une fois le renouvellement effectué, l'ancien facteur d'authentification est révoqué.

R7

Mettre en place un processus de renouvellement des facteurs d'authentification

Il est recommandé de mettre en place un processus de renouvellement des facteurs d'authentification.

3.2 Transmission et utilisation des facteurs d'authentification

Cette section a pour objectif de proposer des recommandations relatives à l'utilisation d'un facteur d'authentification sur des sujets variés tels que : les méthodes de transmission, la journalisation des évènements liés à l'authentification, la limitation du nombre d'essais, la sensibilisation des utilisateurs, etc.

Transmission d'un code par SMS

La majorité des SMS transitent grâce à l'ensemble de protocoles de signalisation SS7[5]. Malheureusement, ces protocoles présentent de nombreuses vulnérabilités intrinsèques et peuvent être aisément interceptés [22]. Il serait alors possible pour un attaquant de récupérer un code d'authentification envoyé par SMS et de l'utiliser afin d'effectuer une authentification frauduleuse.

L'attaque d'ingénierie sociale appelée *SIM Swapping* (que l'on peut traduire par transfert de SIM) permet à un attaquant de récupérer le contrôle du numéro de téléphone de la victime. L'attaquant se fait passer pour la victime auprès du service client de l'opérateur téléphonique en prétextant avoir perdu sa carte SIM et tente de convaincre l'opérateur d'envoyer une nouvelle carte SIM (affectée au numéro de téléphone de la victime) à l'adresse postale de l'attaquant. L'attaquant aura alors le contrôle de la ligne téléphonique de la victime. Enfin dans certains cas, il est possible d'exploiter une réutilisation des numéros de téléphone afin de contourner une authentification multifacteur utilisant la réception d'un code par SMS [28].
Il est alors difficile de considérer la réception d'un code temporaire comme un facteur d'authentification apportant une sécurité suffisante.

Attention

Une méthode d'authentification reposant sur la réception d'une valeur (comme un code à usage unique) au moyen d'un canal peu ou pas sécurisé (comme le SMS) est à proscrire.

En l'absence d'alternative, la réception d'un code temporaire par SMS, au même titre que d'autres mécanismes comme les alertes de connexion à partir d'une nouvelle adresse IP, sont autant d'outils qui permettent de limiter ou détecter des tentatives d'authentification frauduleuses.

R8

Ne pas utiliser le SMS comme moyen de réception d'un facteur d'authentification

Il est recommandé de ne pas utiliser le SMS comme moyen de réception d'un facteur d'authentification.

Conservation des historiques

La conservation des historiques des évènements liés à l'authentification (autrement appelée journalisation) a pour objectifs une supervision de la sécurité et une investigation *a posteriori* en cas d'incidents de sécurité.

R9

Conserver les historiques d'utilisation des facteurs d'authentification

Il est recommandé de conserver les historiques des évènements liés à la vie des facteurs d'authentification afin de faciliter la détection de comportements anormaux qui présagerait d'une compromission d'un facteur d'authentification. Parmi ces évènements, on peut citer : la date de création, les tentatives d'authentification (réussies

5. *Signal System # 7*

ou échouées), les demandes de renouvellement, la date de révocation, etc. Il est recommandé de suivre le guide de recommandations de sécurité pour la mise en œuvre d'un système de journalisation [6] appliqué au contexte de l'authentification.

Limitation des tentatives d'authentification

Pour améliorer la sécurité, on peut mettre en place un blocage temporairement des tentatives d'authentification pendant plusieurs secondes voire minutes (de façon linéaire ou exponentielle) après un certain nombre d'essais infructueux. Par exemple, au sein d'un environnement Windows, il est possible de définir un blocage d'accès au compte pendant Y minutes à la suite de X échecs d'authentification successifs. Des outils comme les CAPTCHA [6] permettent également de limiter les tentatives d'authentification automatique par des attaquants sur une application Web.

R10

Limiter dans le temps le nombre de tentatives d'authentification

Il est recommandé de mettre en œuvre un mécanisme limitant le nombre de tentatives d'authentification sur une période de temps donnée, afin de réduire les probabilités d'authentifications frauduleuses par force brute.

Utilisation d'un canal sécurisé

Si le mécanisme d'authentification nécessite l'envoi direct du secret d'authentification (comme par exemple un mot de passe), il est essentiel de protéger le canal de transmission utilisé pour s'authentifier afin de réduire les risques d'usurpation (par une attaque de l'homme-du-milieu par exemple).

R11

Réaliser l'authentification au travers d'un canal sécurisé

Il est recommandé de réaliser l'authentification au travers d'un canal sécurisé (comme un flux encapsulé par les protocoles TLS ou IPsec) permettant de garantir des propriétés de confidentialité, d'intégrité et d'authenticité.

Limitation de la durée de validité d'une session

Afin de réduire la durée d'exploitation par un attaquant d'une session authentifiée, il est recommandé d'en limiter la durée de validité. Par exemple, la durée d'une session d'authentification pour accéder à des informations sensibles (telles que des informations bancaires) doit être très réduite (quelques minutes tout au plus). Autre exemple, dans le cadre d'une authentification par Kerberos sur un réseau interne, la durée de validité de la session peut être de plusieurs heures.

6. Marque déposée par l'université de Carnegie-Mellon, dont le rétroacronyme signifie *Completely Automated Public Turing test to tell Computers and Humans Apart*, soit en français, test public de Turing complètement automatique ayant pour but de différencier les humains des ordinateurs.

R12

Limiter la durée de validité d'une session authentifiée

Il est recommandé qu'une session authentifiée ait une durée maximale de validité. Les secrets temporaires de sessions (comme des *cookies* par exemple) doivent avoir une durée de vie limitée. Il est ainsi recommandé de forcer la ré-authentification des utilisateurs après une période adaptée au cas d'usage.
Des recommandations concernant la bonne gestion d'une session authentifiée (en particulier concernant les *cookies*) peuvent être trouvées dans le guide *Recommandations pour la mise en oeuvre d'un site Web : maîtriser les standards de sécurité côté navigateur [9]*.

Limitation des données d'authentification

En cas de compromission de la base de données contenant des informations d'authentification nécessaires au vérifieur, il ne doit pas être possible pour un attaquant d'utiliser directement ces informations afin d'usurper une identité. Par exemple, dans le cas d'une authentification par mots de passe, ces derniers doivent être conservés sous la forme d'empreintes cryptographiques (voir le chapitre 4 pour les recommandations spécifiques à ce cas) afin de ne pas être directement exploitables par des attaquants. Autre exemple, dans le cas d'une authentification par OTP, le prouveur et le vérifieur partagent une clé secrète en commun. Cette clé doit être suffisamment protégée afin de limiter les conséquences d'une éventuelle compromission du vérifieur.

R13

Protéger les données d'authentification stockées par le vérifieur

Lorsque des données d'authentification doivent être conservées par le vérifieur, il est recommandé d'assurer la protection en confidentialité et en intégrité de ces informations. Il est également recommandé de protéger les accès à ces données sensibles.

Information de l'échec de l'authentification

Au cours d'une authentification multifacteur, les différents facteurs sont généralement demandés à l'utilisateur l'un après l'autre. Afin de ne pas donner d'information supplémentaire à un attaquant, il est recommandé de notifier l'échec ou la réussite de l'authentification uniquement lorsque tous les facteurs ont été demandés.

R14

Ne pas donner d'information sur l'échec de l'authentification

Il est recommandé que l'échec d'une authentification multifacteur ne donne pas d'information sur le facteur ayant conduit à l'échec de l'authentification.

Définition d'un délai d'expiration

En cas de compromission non détectée d'un facteur d'authentification, ce dernier ne pourra alors pas être utilisé à des fins malveillantes au-delà de sa date de validité. Par exemple, la norme X.509 impose la présence d'une date de fin de validité des certificats numériques. Un délai d'expiration permet aussi de limiter les impacts que pourraient provoquer l'oubli de la suppression d'un compte

d'un utilisateur (après son départ de la structure par exemple). Il faut néanmoins faire attention à conserver un délai d'expiration cohérent avec le niveau de sécurité visé pour ne pas trop dégrader l'expérience utilisateur (pour le cas particulier des mots de passe, voir la section 4.4), ce qui risquerait de dégrader la sécurité globale.

R15

Définir un délai d'expiration des facteurs d'authentification

Il est recommandé de mettre en place un délai d'expiration des facteurs d'authentification, permettant de limiter une éventuelle période d'utilisation frauduleuse.

R16

Définir une politique d'utilisation des facteurs d'authentification

Il est recommandé d'établir une politique définissant les conditions d'utilisation du ou des facteurs d'authentification mis en place. Il peut par exemple s'agir de définir les conditions d'utilisation d'un facteur d'authentification de possession, de définir les procédures qu'un utilisateur doit suivre dans les cas de perte ou de compromission de son facteur d'authentification.

R17

Sensibiliser les utilisateurs à la sécurité de l'authentification

Il est recommandé de mettre en place des campagnes de sensibilisation des utilisateurs aux risques liés à l'authentification (par exemple des campagnes de sensibilisation au hameçonnage). Les utilisateurs doivent être également informés des différentes conditions d'utilisation des facteurs d'authentification mis à leur disposition.

3.3 Révocation des facteurs d'authentification

La révocation d'un facteur d'authentification est l'action consistant à bloquer spécifiquement son utilisation. Par exemple, dans le cas des certificats électroniques, leur statut de révocation est diffusé au moyen de listes de révocation (*Certificate Revocation List* ou CRL en anglais) ou de répondeur OCSP (*Online Certificate Status Protocol*). De nombreux cas (la compromission, l'oubli, la perte, la fermeture d'un compte, etc.) nécessitent de devoir révoquer un facteur d'authentification en particulier pour empêcher sa réutilisation à des fins d'usurpation d'identité.

La révocation est un processus essentiel pour la sécurité de l'authentification et fait partie intégrante du cycle de vie d'un facteur d'authentification.

Le processus de révocation doit être suffisamment complet et maîtrisé, de manière à ce qu'une compromission ou une suspicion de compromission d'un secret entraîne une réaction rapide et des actions concrètes (désactivation, audit spécifique, etc.) sur tous les éléments en lien avec ce secret (par exemple tous les serveurs utilisant les comptes associés).

R18

Mettre en place un processus de révocation des facteurs d'authentification

Il est recommandé de mettre en place un processus dédié permettant de révoquer des facteurs d'authentification et de diffuser l'information de révocation.

Les utilisateurs doivent pouvoir faire une demande de révocation, particulièrement en cas de perte ou de vol.

R19

Définir des délais adaptés de prise en compte des révocations

Les délais pour la prise en compte et l'application de la révocation doivent faire partie de l'analyse de risque et doivent être adaptés aux menaces pesant sur le système d'information.

Des délais de prise en compte courts auront l'avantage de limiter les impacts en cas de compromission par usurpation d'identité, mais de tels délais s'accompagnent généralement d'un dimensionnement organisationnel adapté.

4
Facteur de connaissance (« ce que je sais »)

Objectif

Ce chapitre a pour objectif de présenter des recommandations relatives à la bonne utilisation des mots de passe.

Un facteur de connaissance concerne tous les secrets d'authentification dont la connaissance doit être démontrée par un prouveur (comme les mots de passe). Sauf mention contraire et par souci de simplicité, la notion de « mot de passe » fera référence à un secret devant être mémorisé par un utilisateur, quelle que soit la forme de ce secret (mot de passe, phrase de passe ou code PIN).

4.1 Politique de sécurité de mots de passe

Comme déjà énoncé dans la section 2.3, les mots de passe présentent de nombreuses limites à la fois du point de vue de leur utilisation et de leur gestion.

Les différentes menaces et attaques détaillées dans la section 2.2 permettent de catégoriser les mots de passe suivant leurs usages et leur sensibilité à ces attaquants. On peut distinguer trois catégories de mots de passe.

- Les mots de passe devant être mémorisés (sensibles aux attaques en ligne et hors ligne) : concerne les mots de passe ne pouvant pas facilement être gérés par un coffre-fort de mots de passe, comme le mot de passe maître de ce dernier, le mot de passe d'une session Windows, etc. Ces mots de passe doivent être mémorisés et suffisamment robustes au vu de leur criticité, mais ils sont peu nombreux à retenir. Cette catégorie de mot de passe étant la plus critique, il est pertinent qu'elle soit associée à un second facteur d'authentification.
- Les mots de passe pouvant ne pas être mémorisés (sensibles aux attaques en ligne et hors ligne) : concerne les mots de passe pouvant être générés et conservés par des coffres-forts de mots de passe, comme les mots de passe associés à des comptes de récupération.
- Les numéros d'identification personnels, autrement appelés codes PIN sont vérifiés localement au sein d'un composant physique de sécurité. Les codes PIN que l'on retrouve dans les cartes à puce dont les cartes SIM sont également accompagnés de mesures très restrictives sur le nombre d'échecs d'authentification autorisés (par exemple, la carte se bloque après trois échecs successifs d'authentification).

Cette catégorisation permet de mettre en lumière le fait que parmi tous les mots de passe utilisés au quotidien, il n'y en a qu'un nombre limité qui doivent être mémorisés par un humain. Cette catégorisation peut alors servir de base pour mener une analyse de risque.

La sécurité des mots de passe est souvent réduite à l'estimation de leur « force », c'est-à-dire l'estimation de leur entropie exprimée en bits. Néanmoins, cette estimation ne vaut que si chaque caractère (respectivement chaque mot) du mot de passe (respectivement de la phrase de passe) est choisi de manière uniformément aléatoire. Dans le cas contraire, c'est-à-dire dans le cas où les utilisateurs choisissent eux-mêmes leur mot de passe, ils sont habituellement facilement mémorisables comme un mot du dictionnaire, une date, une citation, etc. L'entropie de tels mots de passe se retrouve fortement réduite et son estimation réelle devient très difficile.

L'entropie est une métrique simple d'utilisation mais qui ne permet pas de capturer la sécurité apportée par les nombreuses autres mesures additionnelles qui doivent être définies dans une **politique de sécurité des mots de passe** comme la limite du nombre d'essais, la méthode de conservation des mots de passe, etc.

Politique de sécurité des mots de passe

Une politique de sécurité de mots de passe est caractérisée par la définition de certains éléments associés à la gestion des mots de passe (liste non exhaustive) :

- catégorie de mots de passe ;
- longueur des mots de passe ;
- règles de complexité des mots de passe (c.-à-d. les types de caractères utilisables) ;
- délai d'expiration des mots de passe ;
- mécanismes de limitation d'essais d'authentification (cf. la recommandation R10) ;
- mécanismes de contrôle de la robustesse des mots de passe ;
- méthode de conservation des mots de passe ;
- méthode de recouvrement d'accès en cas de perte ou de vol des mots de passe ;
- mise à disposition d'un coffre-fort de mots de passe.

R20

Mettre en place une politique de sécurité des mots de passe

Il est recommandé de mettre en place une politique de sécurité des mots passe adaptée au contexte et aux objectifs de sécurité du système d'information.

La liste d'éléments présentée dans cette définition n'est bien sûr pas exhaustive, mais a pour objectif d'en traiter les principaux. Dans la suite, certains de ces éléments vont être précisés.

4.2 Longueur des mots de passe

La robustesse d'un mot de passe est généralement mesurée au moyen de l'entropie, exprimée en bits. L'entropie d'un mot de passe peut être estimée en calculant l'ensemble des mots de passe

possibles pour une longueur donnée et une complexité donnée. La longueur est une composante importante de la sécurité d'une authentification par mots de passe. Il est souvent plus efficace d'allonger un mot de passe que de chercher à le rendre plus complexe [5] pour en augmenter l'entropie. Définir une longueur minimale permet d'avoir un certain contrôle sur le niveau de sécurité apporté par les mots de passe lors de leur création par les utilisateurs.

R21

Imposer une longueur minimale pour les mots de passe

Il est recommandé de définir une longueur minimale pour les mots de passe lors de leur création en fonction du niveau de sécurité visé par le système d'information.

Dans la suite, des exemples de longueurs minimales pour une même complexité fixée à un jeu de caractères composé de 90 caractères (minuscules, majuscules, chiffres et certains caractères spéciaux) sont donnés. Ces exemples proposent des niveaux de sensibilité (faible, moyen, fort, très fort) correspondant à une certaine valeur d'entropie. La définition de ces niveaux de sensibilité dépend fortement du contexte de mise en œuvre de l'authentification et doit être accompagnée d'une analyse de risque. Les recommandations de longueurs minimales en fonction du niveau de sensibilité sont résumées dans le tableau 3.

Niveau de sensibilité	**Longueur minimale en nombre de caractères**	**Taille de clé équivalente en bits** [5]
Faible à moyen	Entre 9 et 11	≈ 65
Moyen à fort	Entre 12 et 14	≈ 85
Fort à très fort	Au moins 15	≥ 100

TABLE 3 – Recommandations concernant les longueurs minimales des mots de passe

Dans des contextes de sensibilité forte à très forte, il est recommandé d'utiliser l'authentification multifacteur (cf. R1).

Ces exemples de longueurs minimales concernent surtout les mots de passe devant être mémorisés par un humain. Pour ceux ne devant pas être mémorisés, il est recommandé que la longueur minimale soit très grande (supérieure à 20 caractères par exemple).

Néanmoins, ces valeurs minimales de longueur peuvent être adaptées en fonction des diverses mesures complémentaires mises en place. C'est le cas par exemple pour les codes PIN dont la longueur et la complexité sont souvent bien plus réduites, mais qui sont accompagnés de fortes mesures complémentaires (comme une désactivation d'accès définitive au compte au bout de trois échecs d'authentification) afin de compenser ce risque. Un autre exemple pourrait être d'adapter certaines mesures complémentaires (comme imposer des caratères spécifiques) en fonction de la taille du mot de passe choisi par l'utilisateur : un utilisateur choisissant un mot de passe très long (comme une phrase de passe de 20 caractères et plus) ne se verrait pas imposer de contraintes sur les caractères à utiliser alors qu'un utilisateur choisissant un mot de passe court (une dizaine de caractères) se verrait imposer l'utilisation de chiffres et de caractères spéciaux.

Une mauvaise pratique observée consiste à fixer une longueur maximale faible (8 ou 10 caractères par exemple) lors de la création d'un mot de passe : cette pratique empêche l'utilisation de phrase de passe. Les phrases de passe constituent une méthode alternative de construction de mots de

passe. Elles consistent à choisir aléatoirement un certain nombre de mots parmi un corpus déterminé (comme le dictionnaire de la langue française). À entropie égale, les phrases de passe sont souvent bien plus longues que les mots de passe « classiques », mais sont aussi pour certains utilisateurs plus simples à mémoriser.

R22

Ne pas imposer de longueur maximale pour les mots de passe

Selon les systèmes, il est recommandé de ne pas fixer de limite à la longueur maximale d'un mot de passe afin de permettre aux utilisateurs d'avoir recours à des phrases de passe ou longs mots de passe.

En pratique selon les systèmes utilisés (application Web ou Windows par exemple) il paraît néanmoins raisonnable de fixer une valeur limite (plusieurs centaines de caractères par exemple) afin de ne pas s'exposer à de potentielles attaques en déni de service (qui consisterait à soumettre des mots de passe de plusieurs Mo au vérifieur et pouvant prendre plusieurs minutes à traiter).

4.3 Règles de complexité des mots de passe

La notion de complexité d'un mot de passe désigne usuellement le choix du jeu de caractères dans lequel les caractères composant un mot de passe sont choisis. Ces jeux de caractères peuvent être assez variés concernant leur taille et composition (caractères numériques, alphanumériques, en minuscules, en majuscules, comprenant des caractères spéciaux, etc). Plus la taille du jeu de caractères est grande plus le nombre de mots de passe possibles est grand.

Afin d'éviter que les utilisateurs ne choisissent des mots de passe trop simples (des mots du dictionnaire français par exemple), une règle fréquemment utilisée lors de la création d'un mot de passe afin d'en augmenter la robustesse est d'imposer des contraintes sur les types de caractères qu'il doit contenir. Par exemple, il peut être imposé que les mots de passe contiennent au moins une majuscule, un chiffre et un caractère spécial.

R23

Mettre en œuvre des règles sur la complexité des mots de passe

Au moment de la création ou du renouvellement d'un mot de passe par un utilisateur, il est recommandé de mettre en œuvre des règles de complexité tout en proposant un jeu de caractères le plus large possible.

Ce type de règles se trouve en pratique souvent détourné par les utilisateurs : transformation de a en @, de o en 0, rajout d'une majuscule en début de mot de passe, rajout d'un chiffre en fin de mot de passe, etc. Les attaquants ayant connaissance de tels comportements, ce genre de mesure n'apporte en pratique qu'assez peu de sécurité contre des attaques hors ligne, où il est possible de créer des dictionnaires dédiés. En revanche, contre les attaques en ligne, ce type de mesure reste très efficace, en particulier couplé avec des limitations temporelles de connexion en cas d'échec d'authentification (cf. recommandation R10). En effet dans ce contexte, imposer une complexité sur les mots de passe augmente suffisamment le nombre de possibilités pour un mot de passe donné (par exemple le mot de passe « password » va être remplacé par « Passw0rd », « P@ssw0rd », « PaSSword1 », « p4ssw0rd » et des dizaines d'autres possibilités), ce qui permet d'augmenter significativement la protection contre des attaques en ligne.

4.4 Délai d'expiration des mots de passe

Le choix d'imposer ou non un délai d'expiration fixe est un sujet qui a évolué ces dernières années. Fixer un délai d'expiration sur des moyens d'authentification est une bonne mesure en général mais s'avère souvent contre-productif dans le cas des mots de passe. En effet, en imposant un délai d'expiration trop réduit sur les mots de passe, les utilisateurs ont tendance à créer des itérations sur leurs mots de passe (par exemple rajouter « +1 » sur un nombre contenu dans le mot de passe comme Toto1, Toto2, etc.) ou à créer des liens logiques triviaux entre les différents mots de passe. Les attaquants étant bien évidemment conscients de tels comportements chez les utilisateurs, l'entropie des mots de passe « itérés » va être très faible en cas de compromission d'un précédent mot de passe.

Ce choix va aussi dépendre de la sensibilité du compte concerné. Une distinction peut être faite entre les comptes dits à privilèges qui sont très sensibles (c'est-à-dire les comptes disposant de droits élevés sur le système d'information comme un compte administrateur) et les comptes sans privilège particulier qui sont peu sensibles (comme les comptes utilisateur).

Pour des comptes peu sensibles, imposer un délai d'expiration trop court (3 à 6 mois par exemple) peut se révéler contre-productif étant donné les comportements des utilisateurs observés lorsqu'ils sont soumis à ce type de contrainte. En revanche, pour les comptes très sensibles comme les comptes à privilèges, conserver un délai d'expiration des mots de passe reste une bonne mesure à mettre en œuvre.

De nombreux moyens permettent de s'assurer que les utilisateurs choisissent des mots de passe robustes (contrôle de leur robustesse à la création, utilisation de coffre-fort de mots de passe, etc.) qui, lorsqu'ils sont mis en œuvre, ne justifient plus le besoin d'imposer un délai d'expiration. En revanche, si aucun de ces moyens ne peut être mis en place ou que le contexte le justifie, il peut être pertinent d'imposer un délai d'expiration (par exemple d'une durée de l'ordre d'une année).

R24

Ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles

Si la politique de mots de passe exige des mots de passe robustes et que les systèmes permettent son implémentation, alors il est recommandé de ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles comme les comptes utilisateur.

Pour les comptes à privilèges (comme les comptes d'administration) le guide d'administration sécurisée [10] recommande de privilégier l'utilisation d'authentification à double facteur. Lorsque l'authentification choisie pour les comptes à privilèges est une authentification simple par mot de passe, imposer un délai d'expiration sur les mots de passe de ces comptes à privilèges est une bonne mesure.

R25

Imposer un délai d'expiration sur les mots de passe des comptes à privilèges

Il est recommandé d'imposer un délai d'expiration sur les mots de passe des comptes très sensibles comme les comptes administrateurs. Ce délai d'expiration peut par

exemple être fixé à une durée comprise entre 1 et 3 ans.

En cas d'incidents de sécurité (comme une suspicion de compromission de la base de données contenant des mots de passe), une expiration immédiate des mots de passe des comptes concernés doit être imposée.

R26

Révoquer immédiatement les mots de passe en cas de compromission suspectée ou avérée

En cas de compromission suspectée ou avérée d'un système d'authentification, tous les mots de passe concernés par ce système doivent être renouvelés immédiatement (de l'ordre de la journée). Au-delà de ce délai, les comptes concernés doivent être désactivés et une procédure de réactivation pour les utilisateurs doit être mise en œuvre.

4.5 Contrôle de la robustesse des mots de passe

Définir des règles de constitution des mots de passe est d'autant plus pertinent que des contrôles sont mis en place afin de s'assurer que ces règles sont respectées dans les faits et qu'il est impossible, pour les utilisateurs, de les contourner. Contrôler la constitution des mots de passe au regard de règles pré-définies permet de garantir le niveau de robustesse des mots de passe.

R27

Mettre en place un contrôle de la robustesse des mots de passe lors de leur création ou de leur renouvellement

Il est recommandé de procéder à un contrôle automatisé et systématique de la robustesse des mots de passe au moment de leur création ou de leur renouvellement.

De nombreux contrôles permettent de s'assurer que les mots de passe ainsi créés offrent une robustesse en accord avec le niveau de sécurité souhaité, par exemple :

- mettre en place des mécanismes automatiques et systématiques permettant de vérifier que les mots de passe respectent bien les règles définies dans la politique de sécurité des mots de passe ;
- comparer les mots de passe lors de leur création à une base de données répertoriant les mots de passe les plus utilisés ou bien ceux qui ont été compromis (par exemple les dictionnaires recensant les mots de passe les plus utilisés ou bien encore les dictionnaires inclus dans les outils de « cassage » de mots de passe comme *JohnTheRipper* [1]) ;
- repérer les mots de passe contenant des motifs (ou des répétitions de motifs) spécifiques (comme une suite de chiffre telle que « 12345 », la suite des premières lettre des claviers comme « azerty », etc) ;
- repérer les mots de passe contenants des informations personnelles saisies lors de la création du compte, comme les noms et prénoms ou encore les dates de naissance ;
- lors d'un renouvellement du mot de passe, interdire la réutilisation d'un mot de passe parmi les X derniers mots de passe déjà utilisés.

Néanmoins, les produits logiciels actuellement disponibles pour la mise en pratique de cette recommandation sont rares.

De plus, il convient d'être prudent quant à l'utilisation de ces produits lorsqu'ils sont à l'extérieur du système d'information (comme une solution dans le *cloud*). Dans ce cas, un lien, par lequel des informations très sensibles vont transiter (c.-à-d. les mots de passe), est alors créé entre le système d'information et une solution extérieure. Il est important de prendre en compte les risques supplémentaires ajoutés par l'utilisation de telles solutions dans l'analyse de risque.

Afin de pouvoir donner aux utilisateurs les moyens nécessaires au respect des contraintes imposées lors de la création de leurs mots de passe, il est important de les sensibiliser à la nécessité de créer des mots de passe dont la robustesse respecte les règles de la politique de mots de passe. Il est également important de fournir aux utilisateurs des ressources leur permettant de générer des mots de passe robustes comme des coffres-forts de mots de passe (voir section 4.8) ou bien des outils d'assistance à la génération et mémorisation de mots de passe robustes (comme l'outil de la CNIL [25]).

Attention

Une pratique, qui pourrait sembler pertinente au premier abord, consisterait à analyser la robustesse des mots de passe *a posteriori* de leur création. C'est-à-dire d'effectuer une analyse de la base de données contenant les mots de passe au moyen d'outils de « cassage » de mots de passe comme *JohnTheRipper* [1]. Les utilisateurs employant des mots de passe faibles repérés avec ces outils seraient alors prévenus qu'il doivent le modifier pour en choisir un plus robuste. Néanmoins, une telle pratique est délicate à mettre en œuvre de manière sécurisée car elle présente de nombreux risques : la base de mots de passe doit être extraite d'une zone protégée et journalisée vers une autre zone potentiellement moins bien protégée, les personnes responsables de ce traitement pourraient être malveillantes et tirer profit des informations extraites, etc.

4.6 Stockage des mots de passe

Le stockage des mots de passe des utilisateurs par le vérifieur doit être réalisé de manière sécurisée. En effet, en cas de compromission de cette base (cette base a été récupérée ou rendue publique par un attaquant), les mots de passe seront directement révélés s'ils sont stockés en clair. Ainsi, ce sont les empreintes des mots de passe qu'il faut conserver plutôt que les mots de passe eux-mêmes. Le stockage des mots de passe en clair doit être absolument proscrit. Ces empreintes, aussi appelées hachés, sont le résultat d'une fonction de hachage cryptographique (comme les familles SHA2 ou SHA3) appliquée aux mots de passe. Ces fonctions de hachage cryptographique semblent au premier abord de bons outils pour stocker les mots de passe, car elles ont, en particulier, la propriété d'être à sens unique : retrouver le mot de passe originel à partir d'une empreinte est extrêmement difficile.

Les fonctions de hachage cryptographique qui permettent de calculer ces empreintes sont déterministes. Autrement dit, l'empreinte d'un même mot de passe calculée avec la même fonction de hachage sera toujours la même. Comme un même mot de passe se retrouve généralement utilisé pour de nombreux services, la compromission des empreintes des mots de passe d'un seul de ces

services compromet les mots de passe sur l'ensemble des services. Les attaquants peuvent alors précalculer des tables de correspondance entre les mots de passe courants et leurs empreintes respectives pour différentes fonctions de hachage, ce qui accélère fortement le « cassage » des mots de passe. L'ajout d'une valeur aléatoire unique (communément appelée un sel) lors du calcul de l'empreinte du mot de passe permet de se prémunir contre des attaquants utilisant des tables précalculées.

R28

Utiliser un sel aléatoire long

Il est recommandé d'utiliser un sel choisi aléatoirement pour chaque compte et d'une longueur d'au moins 128 bits.

Les fonctions de hachage cryptographique recommandées, comme la famille SHA2, sont des fonctions très rapides à exécuter, ce qui, dans le contexte du stockage des mots de passe, est un avantage pour les attaquants, leur permettant de tester (c.-à-d. de calculer des empreintes) de nombreux mots de passe. Afin de ralentir les attaquants, il est recommandé d'utiliser des fonctions de dérivation de mots de passe dites *memory-hard* permettant à la fois d'augmenter le temps d'exécution mais aussi l'espace mémoire lors du calcul d'une empreinte. L'utilisation de telles fonctions correctement paramétrées permet un important ralentissement des attaques par force brute tout en ayant un impact négligeable sur les services légitimes ne devant exécuter qu'un petit nombre de calculs d'empreintes. En particulier les fonctions de dérivation de mots de passe *memory-hard* permettent de se protéger contre des attaquants profitant des accélérations matérielles apportées par l'utilisation de cartes graphiques ou de *hardware* dédié.

La liste des fonctions recommandées dans les recommandations R29 et R29- n'a pas vocation à être exhaustive.

R29

Utiliser une fonction de dérivation de mots de passe memory-hard pour conserver les mots de passe

Pour conserver les mots de passe, il est recommandé d'utiliser des fonctions de dérivation de mots de passe *memory-hard* comme scrypt ou Argon2.
Il est conseillé de paramétrer ces fonctions de manière à proposer le niveau de sécurité le plus élevé possible tant que cela n'affecte pas un usage légitime.

R29 -

Utiliser une fonction de dérivation de mots de passe itérative pour conserver les mots de passe

Pour des contextes où il est difficile de faire usage de fonctions *memory-hard*, il est recommandé d'utiliser la fonction de dérivation de mots de passe PBKDF2.
Il est conseillé de choisir le nombre d'itérations de PBKDF2 le plus grand possible, tant que cela n'affecte pas un usage légitime.

L'usage seul de fonctions de dérivation de mots de passe bien paramétrées n'est pas suffisant : l'ensemble des éléments de la politique de mots de passe sont nécessaires pour garantir un bon niveau de sécurité avec cette méthode d'authentification.

4.7 Recouvrement d'un accès

Pour pallier l'oubli ou l'expiration d'un mot de passe, un mécanisme de recouvrement d'accès (au compte, au service, à la ressource, etc) doit être mis en place. De nombreuses méthodes existent et sont dépendantes du contexte d'utilisation. Parmi les plus courantes, on peut citer : la réception d'un mot de passe temporaire autogénéré (qui doit alors être changé sans tarder), la réception d'un lien temporaire à usage unique de réinitialisation, le contact du support informatique, etc. Ces méthodes viennent avec leurs problématiques propres : le choix du mode de réception (par courriel, SMS, envoi postal, téléphone, etc), le choix du temps de validité de liens temporaires, la complexité de ces méthodes pour l'utilisateur, l'ajout ou non de vérificateur humain, etc. Cela rend très difficile la recommandation d'une méthode en particulier. En revanche, la transmission du mot de passe originel en clair est à éviter.

R30

Proposer une méthode de recouvrement d'accès

Afin de permettre aux utilisateurs de retrouver un accès à leur compte, il est recommandé de mettre en place une méthode de recouvrement d'accès adaptée au contexte d'utilisation.

4.8 Coffre-fort de mots de passe

Afin de permettre aux utilisateurs l'emploi de mots de passe robustes, il est important de mettre à leur disposition des outils dédiés, comme les coffres-forts de mots de passe. Les coffres-forts de mots de passe (*Keepass* [29] est un exemple) permettent, entre autres, de générer des mots de passe longs et complexes (sans avoir besoin de les mémoriser ni même d'en prendre connaissance) et de les stocker de manière sécurisée.

R31

Mettre à disposition un coffre-fort de mots de passe

Il est recommandé que les responsables du système d'information mettent à disposition des utilisateurs un coffre-fort de mots de passe et les forment à son utilisation.

Le moyen d'authentification permettant de déverrouiller l'accès aux mots de passe contenus dans le coffre-fort a évidemment une importance majeure. Il prend souvent la forme d'un mot de passe, dit mot de passe « maître », qui doit être robuste et mémorisé par un humain. Ce mot de passe est très critique et sa compromission entraînerait la compromission de tous les mots de passe contenus dans le coffre-fort. De nombreuses solutions de coffres-forts de mots de passe proposent également l'ajout d'un second facteur d'authentification afin de mieux protéger l'accès au coffre-fort de mots de passe.

Attention

Les alternatives consistant par exemple à utiliser un fichier bureautique protégé par un mot de passe sont à proscrire dans la mesure où elles n'apportent pas du tout le même niveau de protection qu'un coffre-fort de mots de passe conçu à cette fin.

4.9 Recommandations à destination des utilisateurs

Cette section à destination des utilisateurs rappelle des bonnes pratiques quant à l'utilisation des mots de passe au quotidien.

Il est recommandé d'utiliser des mots de passe différents pour chaque service afin de limiter les conséquences en cas de compromission d'un mot de passe (un seul service sera impacté au lieu d'une multitude). L'utilisation d'un coffre-fort de mots de passe permet de mettre en pratique une telle recommandation et d'éviter le stockage non sécurisé des mots de passe.

R32

[Utilisateur] Utiliser des mots de passe robustes

Il est recommandé d'utiliser des mots de passe (ou phrases de passe) robustes, c'est-à-dire suffisamment longs et complexes pour résister aux attaques par recherche exhaustive et n'étant pas un mot du dictionnaire (ou une citation ou phrase connue) pour résister aux attaques par dictionnaire.

R33

[Utilisateur] Utiliser un mot de passe différent pour chaque service

Il est recommandé d'utiliser un mot de passe différent pour chaque service auquel l'utilisateur est inscrit.

R34

[Utilisateur] Utiliser un coffre-fort de mots de passe

Il est recommandé d'utiliser un coffre-fort de mots de passe permettant facilement de générer des mots de passe robustes et différents pour chaque service, facilitant la mise en œuvre de la recommandation R33.

R35

[Utilisateur] Protéger ses mots de passe

Il est recommandé d'adopter les bons réflexes de protection des mots de passe. Par exemple, il est impératif de ne pas écrire ses mots de passe sur une note sous le clavier, de ne pas créer un fichier « mot de passe » sur le poste utilisateur, de ne pas s'envoyer ses mots de passe par courriel, etc. L'utilisation d'outils comme les coffres-forts de mots de passe est à privilégier.

Les messageries électroniques sont actuellement des éléments centraux et critiques dans les mécanismes d'authentification. En effet, leur compromission permet très généralement d'accéder dans un second temps à tous les comptes associés à cette messagerie électronique.

R36

[Utilisateur] Utiliser un mot de passe robuste pour l'accès à sa messagerie électronique

Il est recommandé d'utiliser un mot de passe robuste pour accéder à sa messagerie électronique. En particulier, il faut privilégier l'utilisation d'une méthode d'authentification multifacteur lorsque cela est disponible.

Un attaquant verra son action de « cassage » de mot de passe facilitée si celui-ci est constitué pour tout ou partie par des informations de nature publique et personnelle (nom, prénom, date de naissance, nom d'un animal domestique, ville de résidence, etc.), particulièrement celles visibles sur les réseaux sociaux.

R37

[Utilisateur] Choisir un mot de passe sans information personnelle

Il est recommandé de ne pas construire son mot de passe à partir d'informations personnelles comme les noms et prénoms ou encore la date de naissance.

Des comptes natifs (d'administration ou d'équipements connectés) possèdent généralement des mots de passe par défaut, consultables dans la documentation de l'éditeur de la solution ou sur Internet. Il convient donc de les modifier dès l'installation.

R38

[Utilisateur] Modifier les mots de passe par défaut

Il est recommandé de modifier les mots de passe par défaut.

5
Facteur de possession (« ce que je possède »)

Objectif

Ce chapitre a pour objectif de fournir des recommandations de sécurité sur l'utilisation des facteurs de possession.

5.1 Recommandations relatives à l'utilisation d'un facteur de possession

Un facteur de possession est un moyen de stocker des secrets non mémorisables par un humain (et n'ayant pas vocation à être mémorisés par un humain). Il s'agit typiquement des clés cryptographiques qui permettent de réaliser des opérations de chiffrement, de signature ou d'authentification. Les menaces principales pesant sur le facteur de possession étant le vol et la duplication des secrets cryptographiques, l'équipement physique qui fait office de facteur de possession doit être équipé d'un composant de sécurité, permettant de stocker et manipuler ces clés cryptographiques de manière sécurisée.

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.

Le composant de sécurité permet notamment d'offrir des garanties de protection contre l'extraction et la duplication des éléments cryptographiques qu'il contient. Des mesures de défense contre les attaques par canaux auxiliaires (mesure du temps d'exécution, de la consommation électrique, des émanations électromagnétiques, etc.) et les attaques par injection de fautes sont également intégrées au sein du composant de sécurité.

Les facteurs de possession, manipulant généralement des clés cryptographiques, permettent l'authentification forte (comme définie dans la section 2.5) : authentification par certificat X.509, protocole FIDO2 [4] ou bien encore les différents protocoles d'OTP comme HOTP [32]. La protection de ces clés cryptographiques au sein d'un composant de sécurité constitue ainsi un objectif important afin de garantir l'usage légitime de l'authentification.

Parmi les facteurs de possession intégrant un composant de sécurité, on peut citer les cartes à puce, les cartes SIM ou bien encore les facteurs matériels d'authentification (par exemple les « *tokens* » FIDO). L'utilisation d'un matériel physique ayant subi une évaluation de sécurité (par exemple une qualification de sécurité [7] ou un processus de certification Critères Communs [14]) est à privilégier, particulièrement dans le cas où la vérification d'un des facteurs s'effectue localement au sein du composant de sécurité. Un composant dont la sécurité à été évaluée offre des garanties de robustesse aux menaces identifiées lors de la procédure d'évaluation de sécurité.

R39

Utiliser un facteur de possession intégrant un composant de sécurité qualifié ou certifié

Il est recommandé de recourir à l'utilisation d'un facteur de possession dont le composant de sécurité a reçu un visa de sécurité de l'ANSSI.

R39 -

Utiliser un facteur de possession intégrant un composant de sécurité

Lorsqu'une authentification, simple facteur ou multifacteur, utilise un moyen d'authentification reposant sur un facteur de possession, il est recommandé qu'il possède un composant de sécurité intégré.
Il est recommandé d'utiliser un protocole d'authentification conforme au RGS.

R39 - -

Utiliser un facteur de possession même sans composant de sécurité

L'utilisation d'un facteur de possession permet l'utilisation de protocoles d'authentification conformes au RGS. Son utilisation reste recommandée même si les éléments secrets ne peuvent pas être stockés dans un composant de sécurité. Dans ce contexte, il est essentiel de mettre en œuvre des mesures de protection supplémentaires comme le chiffrement des éléments cryptographiques, des restrictions d'accès, etc.

Les deux situations typiques où un facteur de possession sans composant de sécurité est utilisé sont :

- le cas du stockage d'éléments cryptographiques (une clé privée SSH par exemple) sur un poste de travail ; ces éléments ont des besoins de sécurité en confidentialité et en intégrité, qui peuvent être assurés par exemple par le chiffrement de ces éléments au moyen d'un mot de passe ;
- le cas du stockage d'éléments cryptographiques dans un mobile (de type *smartphone*) par exemple dans le cas de l'utilisation d'une authentification par OTP ; les besoins de sécurité en confidentialité et en intégrité de ces éléments cryptographiques peuvent être assurés par chiffrement ou par stockage dans une portion protégée de la mémoire (comme l'Android *keystore* ou l'iOS *keychain*).

7. Plus d'information à cette adresse : https://www.ssi.gouv.fr/administration/qualifications/

5.2 Utilisation d'un facteur de possession pour une authentification multifacteur

Lorsqu'un facteur d'authentification de possession est mis en œuvre pour une authentification multifacteur, il est très souvent associé à un autre facteur d'authentification, par exemple une carte à puce protégée par un code PIN. Deux cas de composition des facteurs existent lorsqu'un facteur de possession et un second facteur (qui est généralement un facteur de connaissance) sont mis en œuvre.

1. Le vérifieur ne vérifie directement qu'un seul des facteurs (généralement le facteur de possession). La vérification du second facteur s'effectue alors au sein du composant de sécurité, qui permet de déverrouiller l'utilisation du facteur de possession (cas de la carte à puce protégée par un code PIN).
2. Le vérifieur vérifie directement les deux facteurs d'authentification (cas lors de l'utilisation du protocole FIDO U2F ou FIDO 2 qui associe un *token* à un mot de passe).

Dans le cas 1, la sécurité de l'authentification repose essentiellement sur le composant de sécurité, puisque les deux facteurs d'authentification sont conservés au sein de ce composant, et l'authentification est uniquement effectuée par la vérification du facteur de possession. Ainsi, en cas de découverte de vulnérabilités du composant de sécurité, les deux facteurs d'authentification risquent d'être compromis. Dans ce cas, il est important d'utiliser un composant de sécurité évalué. En revanche, la notion de déverrouillage du facteur de possession par un autre facteur permet de se protéger contre la perte ou le vol du facteur de possession : celui-ci est inutilisable sans l'autre facteur.

Dans le cas 2, une faiblesse du composant de sécurité n'entraînerait la compromission que du facteur de possession puisque le second facteur ne serait pas connu du composant de sécurité. Néanmoins, le vérifieur doit alors gérer et assurer directement la protection de deux facteurs d'authentification au lieu d'un seul. De plus, en cas de perte ou de vol du facteur de possession, celui-ci reste utilisable par un attaquant. Enfin, le second facteur est ici alors sensible aux attaques en ligne et hors ligne alors qu'il n'est sensible qu'aux attaques en ligne dans le cas 1 grâce au composant de sécurité.

Lorsqu'il n'est pas possible d'avoir accès à un composant de sécurité évalué pour protéger un facteur de possession, il est préférable de privilégier le cas 2 où le vérifieur vérifie directement les deux facteurs d'authentification. Ainsi, un attaquant ayant réussi à récupérer le facteur de possession (par exemple en cas d'une vulnérabilité du composant de sécurité) a tout de même besoin de l'autre facteur pour réaliser une authentification illégitime.

Ces deux cas présentent certaines différences en matière de menaces (sensibilité ou non aux attaques hors ligne) et de confiance (niveau de confiance accordé dans le composant de sécurité) qui doivent être prises en compte lors d'une analyse de risque.

6
Facteur inhérent (« ce que je suis »)

Objectif

Ce chapitre a pour objectif de fournir des recommandations de sécurité sur l'utilisation des facteurs inhérents.

6.1 Avantages et inconvénients des facteurs inhérents

La biométrie, signifiant étymologiquement la mesure du vivant, consiste à vérifier ou déterminer l'identité d'un individu à partir de ses caractéristiques biologiques (comme l'ADN, le sang), morphologiques (comme l'empreinte digitale, la forme de l'iris ou la forme du visage) ou comportementales (comme la voix, la vitesse de frappe au clavier).

L'usage d'un facteur biométrique pour l'authentification, comparé aux autres types de facteurs, présente deux avantages principaux.
Le premier est sa simplicité d'emploi. En effet, par rapport à un facteur de connaissance il n'y a pas d'information secrète à mémoriser et par rapport à un facteur de possession il n'y a pas d'objet physique à conserver. Dans les deux cas, la biométrie permet de se prémunir des risques liés à l'oubli ou à la perte des moyens d'authentification et d'améliorer l'expérience utilisateur.
Le deuxième est l'authentification directe d'un individu apportée par la biométrie, au contraire des facteurs de connaissance et de possession qui vont authentifier uniquement un élément secret.

Néanmoins, l'emploi d'un facteur biométrique présente de nombreux désavantages et limitations.

Un de ces désavantages concerne la problématique de la révocation du moyen d'authentification. En effet, pour les facteurs de connaissance et de possession, la révocation des moyens d'authentification (en cas de compromission par exemple) est une procédure relativement aisée à effectuer. Le vérifieur ne doit plus accepter d'authentification provenant d'un moyen révoqué et le prouveur doit générer de nouveaux éléments secrets. Dans le cas de la biométrie, la révocation d'un moyen d'authentification consiste alors en la révocation d'une mesure d'une caractéristique physique unique à un individu. Ce trait physique unique peut devenir alors difficilement utilisable comme moyen d'authentification.

De nombreuses caractéristiques inhérentes, comme la forme du visage ou les empreintes digitales ne sont pas confidentielles et ne peuvent pas être protégées en confidentialité, au contraire de facteurs de connaissance ou de possession.

En raison de la nature même de la biométrie, la vérification de l'identité par le vérifieur est probabiliste : un compromis doit toujours être trouvé entre sécurité (maintenir un taux bas de fausse acceptation) et la fonctionnalité (maintenir un taux bas de faux rejet). La qualité de la vérification va aussi dépendre de la qualité du capteur physique utilisé pour mesurer les données biométriques, qui peut varier d'un constructeur à l'autre. Certaines des caractéristiques mesurées pour une authentification biométrique vont également s'altérer avec le temps, à cause du vieillissement des individus, de blessures, etc. L'obsolescence du matériel servant à mesurer ces caractéristiques peut également poser problème.

Enfin, la conservation de données biométriques pose des problèmes vis-à-vis du respect de la vie privée. En effet, le vérifieur doit conserver les modèles (ou gabarits) biométriques des différents prouveurs. Ces modèles, établis lors de l'enregistrement d'un individu, contiennent des informations caractérisant de manière unique un individu et doivent donc être protégés de manière adéquate. La CNIL propose des fiches de conseils [24] relatives à la gestion réglementaire des données biométriques (comme imposé par le RGPD par exemple).

De plus, de nombreuses études scientifiques montrent que les technologies utilisées pour l'authentification biométrique restent pour la plupart sensibles à la contrefaçon (reconnaissance d'empreintes digitales : MasterPrint [30] et DeepMasterPrint [15], reconnaissance faciale : [17], reconnaissance vocale : [18], reconnaissance des veines palmaires : [31], etc.).

6.2 Recommandations relatives à l'utilisation d'un facteur inhérent

La prise en compte des limites et des risques liés à la biométrie est essentielle lors de l'intégration de ce type d'authentification au sein d'un système d'information.

R40

Ne pas utiliser un facteur inhérent comme unique facteur d'authentification

Il est recommandé de ne pas utiliser un facteur d'authentification inhérent lorsqu'il s'agit d'une authentification avec un unique facteur.

R41

Utiliser un facteur inhérent uniquement associé à un facteur d'authentification fort

Dans le cadre d'une authentification multifacteur, si un facteur d'authentifcation inhérent est utilisé, alors il est recommandé de l'accompagner d'au moins un autre facteur d'authentification reposant sur un mécanisme cryptographique conforme au RGS.

La biométrie permet l'authentification directe d'individus au travers de certaines caractéristiques physiques uniques. Lorsque ces caractéristiques doivent être révoquées, elles deviennent inutilisables. La phase d'enregistrement devient une phase très critique et doit être protégée en conséquence.

R42

Favoriser une rencontre en présence lors de l'enregistrement d'un facteur inhérent

Lors de la phase d'enregistrement d'un moyen d'authentification inhérent, il est recommandé de procéder à la vérification de l'identité par une rencontre en présence afin de limiter les risques d'usurpation d'identité lors de cette phase.

Liste des recommandations

R1	Privilégier l'authentification multifacteur	14
R2	Privilégier l'utilisation de moyens d'authentification forts	16
R3	Conduire une analyse de risque	18
R4	Créer les facteurs d'authentification dans un environnement maîtrisé	19
R5	Générer les éléments aléatoires avec un générateur de nombres aléatoires robuste	20
R6	Remettre les facteurs d'authentification au travers de canaux sécurisés	20
R7	Mettre en place un processus de renouvellement des facteurs d'authentification	20
R8	Ne pas utiliser le SMS comme moyen de réception d'un facteur d'authentification	21
R9	Conserver les historiques d'utilisation des facteurs d'authentification	22
R10	Limiter dans le temps le nombre de tentatives d'authentification	22
R11	Réaliser l'authentification au travers d'un canal sécurisé	22
R12	Limiter la durée de validité d'une session authentifiée	23
R13	Protéger les données d'authentification stockées par le vérifieur	23
R14	Ne pas donner d'information sur l'échec de l'authentification	23
R15	Définir un délai d'expiration des facteurs d'authentification	24
R16	Définir une politique d'utilisation des facteurs d'authentification	24
R17	Sensibiliser les utilisateurs à la sécurité de l'authentification	24
R18	Mettre en place un processus de révocation des facteurs d'authentification	24
R19	Définir des délais adaptés de prise en compte des révocations	25
R20	Mettre en place une politique de sécurité des mots de passe	27
R21	Imposer une longueur minimale pour les mots de passe	28
R22	Ne pas imposer de longueur maximale pour les mots de passe	29
R23	Mettre en œuvre des règles sur la complexité des mots de passe	29
R24	Ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles	30
R25	Imposer un délai d'expiration sur les mots de passe des comptes à privilèges	31
R26	Révoquer immédiatement les mots de passe en cas de compromission suspectée ou avérée	31
R27	Mettre en place un contrôle de la robustesse des mots de passe lors de leur création ou de leur renouvellement	31
R28	Utiliser un sel aléatoire long	33
R29	Utiliser une fonction de dérivation de mots de passe *memory-hard* pour conserver les mots de passe	33
R29-	Utiliser une fonction de dérivation de mots de passe itérative pour conserver les mots de passe	33
R30	Proposer une méthode de recouvrement d'accès	34
R31	Mettre à disposition un coffre-fort de mots de passe	34
R32	[Utilisateur] Utiliser des mots de passe robustes	35
R33	[Utilisateur] Utiliser un mot de passe différent pour chaque service	35
R34	[Utilisateur] Utiliser un coffre-fort de mots de passe	35

R35	[Utilisateur] Protéger ses mots de passe	35
R36	[Utilisateur] Utiliser un mot de passe robuste pour l'accès à sa messagerie électronique	36
R37	[Utilisateur] Choisir un mot de passe sans information personnelle	36
R38	[Utilisateur] Modifier les mots de passe par défaut	36
R39	Utiliser un facteur de possession intégrant un composant de sécurité qualifié ou certifié	38
R39-	Utiliser un facteur de possession intégrant un composant de sécurité	38
R39- -	Utiliser un facteur de possession même sans composant de sécurité	38
R40	Ne pas utiliser un facteur inhérent comme unique facteur d'authentification	41
R41	Utiliser un facteur inhérent uniquement associé à un facteur d'authentification fort	41
R42	Favoriser une rencontre en présence lors de l'enregistrement d'un facteur inhérent	42

Bibliographie

[1] *Jonh The Ripper password cracker*.
https://www.openwall.com/john/.
Dernier accès le 15/07/2020.

[2] *Référentiel d'exigences applicables aux prestataires de vérification d'identité à distance (PVID)*.
Référentiel Version 1.1, ANSSI, avril 2021.
https://www.ssi.gouv.fr/actualite/publication-du-referentiel-dexigences-applicables-aux-prestataires-de-verification-didentite-a-distance-pvid/.

[3] Michel Abdalla and David Pointcheval.
Simple Password-Based Encrypted Key Exchange Protocols.
In Alfred Menezes, editor, *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*, volume 3376 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2005.

[4] FIDO Alliance.
FIDO2 : WebAuthn & CTAP.
https://fidoalliance.org/fido2/.
Dernier accès le 12/07/2020.

[5] ANSSI.
Calculer la force d'un mot de passe.
https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/, 2020.
Dernier accès le 26/10/2020.

[6] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[7] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.0, ANSSI, octobre 2018.
https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide.

[8] *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection*.
Guide ANSSI-PA-072 v2.0, ANSSI, mars 2020.
https://www.ssi.gouv.fr/controle-acces-videoprotection.

[9] *Recommandations pour la mise en oeuvre d'un site Web : maîtriser les standards de sécurité côté navigateur*.
Guide ANSSI-PA-009, ANSSI, avril 2021.
https://www.ssi.gouv.fr/guide/recommandations-pour-la-securisation-des-sites-web/.

[10] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://www.ssi.gouv.fr/securisation-admin-si.

[11] *RGS Annexe B3 : Règles et recommandations concernant les mécanismes d'authentification*.
Référentiel Version 1.0, ANSSI, janvier 2010.
https://www.ssi.gouv.fr/rgs.

[12] *RGS Annexe B2 : Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[13] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[14] *Certification Critères Communs*.
Page Web Version 1.0, ANSSI, mars 2016.
https://www.ssi.gouv.fr/certification.

[15] Philip Bontrager, Aditi Roy, Julian Togelius, Nasir D. Memon, and Arun Ross.
*DeepMasterPrints : Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution**.
In *9th IEEE International Conference on Biometrics Theory, Applications and Systems, BTAS 2018, Redondo Beach, CA, USA, October 22-25, 2018*, pages 1–9. IEEE, 2018.

[16] cybermalveillance.gouv.fr : Assistance et prévention du risque numérique.
L'hameçonnage (phishing).
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing, 2020.
Dernier accès le 10/07/2020.

[17] Nesli Erdogmus and Sébastien Marcel.
Spoofing Face Recognition With 3D Masks.
IEEE Trans. Information Forensics and Security, 9(7) :1084–1097, 2014.

[18] Serife Kucur Ergunay, Elie el Khoury, Alexandros Lazaridis, and Sébastien Marcel.
On the vulnerability of speaker verification to realistic voice spoofing.
In *IEEE 7th International Conference on Biometrics Theory, Applications and Systems, BTAS 2015, Arlington, VA, USA, September 8-11, 2015*, pages 1–6. IEEE, 2015.

[19] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

[20] Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu.
OPAQUE : An Asymmetric PAKE Protocol Secure Against Pre-computation Attacks.
In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 456–486. Springer, 2018.

[21] Microsoft.
Mitigating pass-the-hash and other credential theft, version 2.

https://www.microsoft.com/en-us/download/details.aspx?id=36036.
Dernier accès le 12/07/2020.

[22] Hassan Mourad.
The fall of SS7 : how can the critical security controls can help ?
https://www.sans.org/reading-room/whitepapers/critical/fall-ss7-critical-security-controls-help-36225.
Dernier accès le 12/07/2020.

[23] Commission nationale de l'informatique et des libertés (CNIL).
Authentification par mot de passe : les mesures de sécurité élémentaires.
https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires, 2018.
Dernier accès le 10/07/2020.

[24] Commission nationale de l'informatique et des libertés (CNIL).
Biométrie.
https://www.cnil.fr/fr/biometrie, 2018.
Dernier accès le 12/07/2020.

[25] Commission nationale de l'informatique et des libertés (CNIL).
Générer un mot de passe solide.
https://www.cnil.fr/fr/generer-un-mot-de-passe-solide, 2018.
Dernier accès le 04/11/2020.

[26] Commission nationale de l'informatique et des libertés (CNIL).
De « azerty » à « Pa$$word », une revue des pratiques de gestion des mots de passe.
https://linc.cnil.fr/de-azerty-paword-une-revue-des-pratiques-de-gestion-des-mots-de-passe, 2021.
Dernier accès le 03/08/2021.

[27] Dr. Clifford Neuman, Sam Hartman, Kenneth Raeburn, and Taylor Yu.
The Kerberos Network Authentication Service (V5).
RFC 4120, juillet 2005.

[28] Wladimir Palant.
Yahoo ! and AOL : Where two-factor authentication makes your account less secure.
https://palant.info/2020/03/09/yahoo-and-aol-where-two-factor-authentication-makes-your-account-less-secure/, 2020.
Dernier accès le 10/07/2020.

[29] Dominik Reichl.
Keepass.
https://keepass.info/.
Dernier accès le 15/07/2020.

[30] Aditi Roy, Nasir D. Memon, and Arun Ross.
MasterPrint : Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems.
IEEE Trans. Information Forensics and Security, 12(9) :2013–2025, 2017.

[31] Pedro Tome and Sébastien Marcel.
On the vulnerability of palm vein recognition to spoofing attacks.

In *International Conference on Biometrics, ICB 2015, Phuket, Thailand, 19-22 May, 2015*, pages 319–325. IEEE, 2015.

[32] Mountain View, David M'Raihi, Frank Hoornaert, David Naccache, Mihir Bellare, and Ohad Ranen.
HOTP : An HMAC-Based One-Time Password Algorithm.
RFC 4226, décembre 2005.

[33] Mountain View, David Naccache, Johan Rydell, Siddharth Bajaj, and Salah Machani.
OCRA : OATH Challenge-Response Algorithm.
RFC 6287, juin 2011.

[34] Mountain View, Johan Rydell, Mingliang Pei, and Salah Machani.
TOTP : Time-Based One-Time Password Algorithm.
RFC 6238, 2011.

[35] Yubico.
Reduced initial randomness on FIPS keys.
https://www.yubico.com/support/security-advisories/ysa-2020-01/.
Dernier accès le 12/07/2020.

ANSSI-PG-078
Version 2.0 - 08/10/2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN