DOSSIER DOCUMENTAIRE ACTIVITÉ MFA

PRÉSENTATION DE LA CLÉ D'AUTHENTIFICATION YUBIKEY

La yubikey est un dispositif d'authentification électronique qui supporte les mots de passe à usage unique (HOTP, TOTP), le chiffrement et l'authentification par paire de clés publique, privée (PGP), le protocole Universal Second Factor (U2F) ainsi que la norme FIDO 2 développés par l'alliance FIDO.

Il permet aux utilisateurs de mettre en place une authentification multifacteur forte, s'affranchissant ainsi des limites de l'authentification par mot de passe.

> ⚠ **Information :** En 2016, l'entreprise Yubico, créatrice des clés yubikey, décide de remplacer tout son code open-source par du code propriétaire fermé. Les yubikey ne peuvent plus être auditées de façon indépendante. En 2017, des chercheurs en sécurité ont notamment découverts une faille dans l'implémentation des clés RSA générées dans les yubikey 4. L'utilisation de technologies ouvertes permet un meilleur contrôle et une meilleure capacité d'audit.

Il existe ainsi des clés de sécurité alternatives qui misent justement sur un code et un matériel totalement ouverts et libre comme la « nitrokey » produite en Allemagne.

Source : Wikipédia

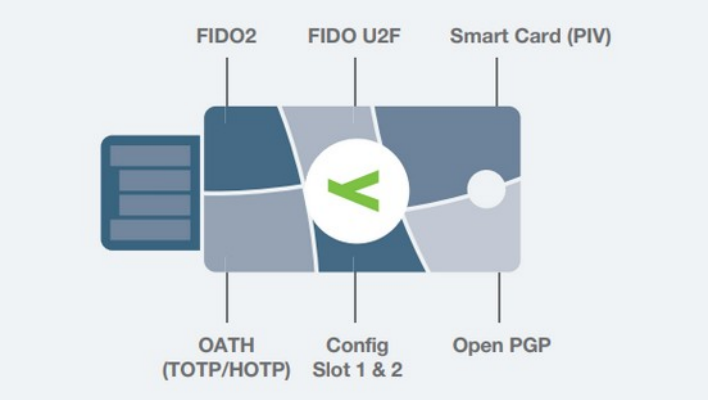


Figure 1: Image issue du site officiel yubico

LES DIFFÉRENTES MÉTHODES D'AUTHENTIFICATION PROPOSÉES AVEC LA YUBIKEY

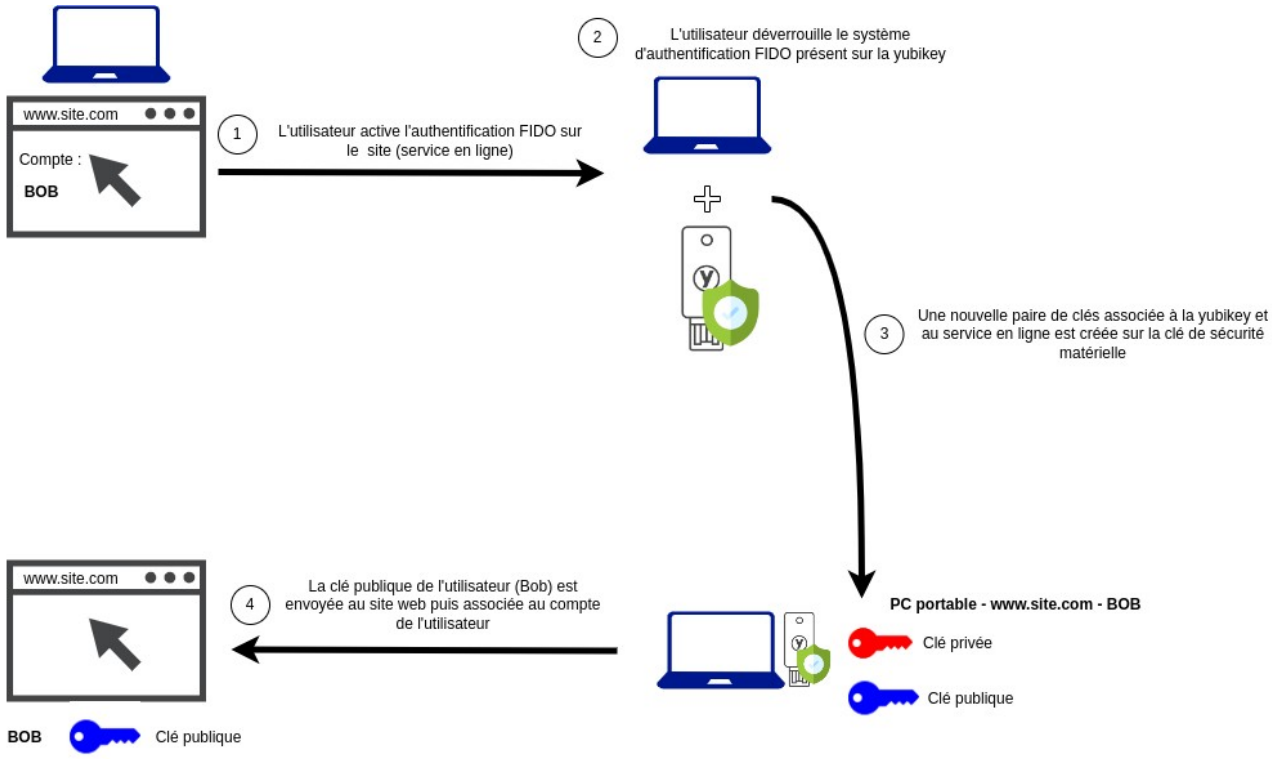
FIDO 2

FIDO 2 est un protocole d'authentification forte développé et promu par la Fido Alliance, un consortium industriel ouvert créé en 2013 dans le but de fournir un standard d'authentification interopérable.

La plupart des services web utilisant le protocole FIDO 2 utilise la méthode d'authentification **WebAuthn (Web Authentication)**. Cette dernière est un standard du World Wide Web Consortium avec la contribution de la FIDO Alliance qui propose une interface d'authentification des utilisateurs aux applications Web à l'aide de clés asymétriques.

Phase d'enregistrement WebAuthn

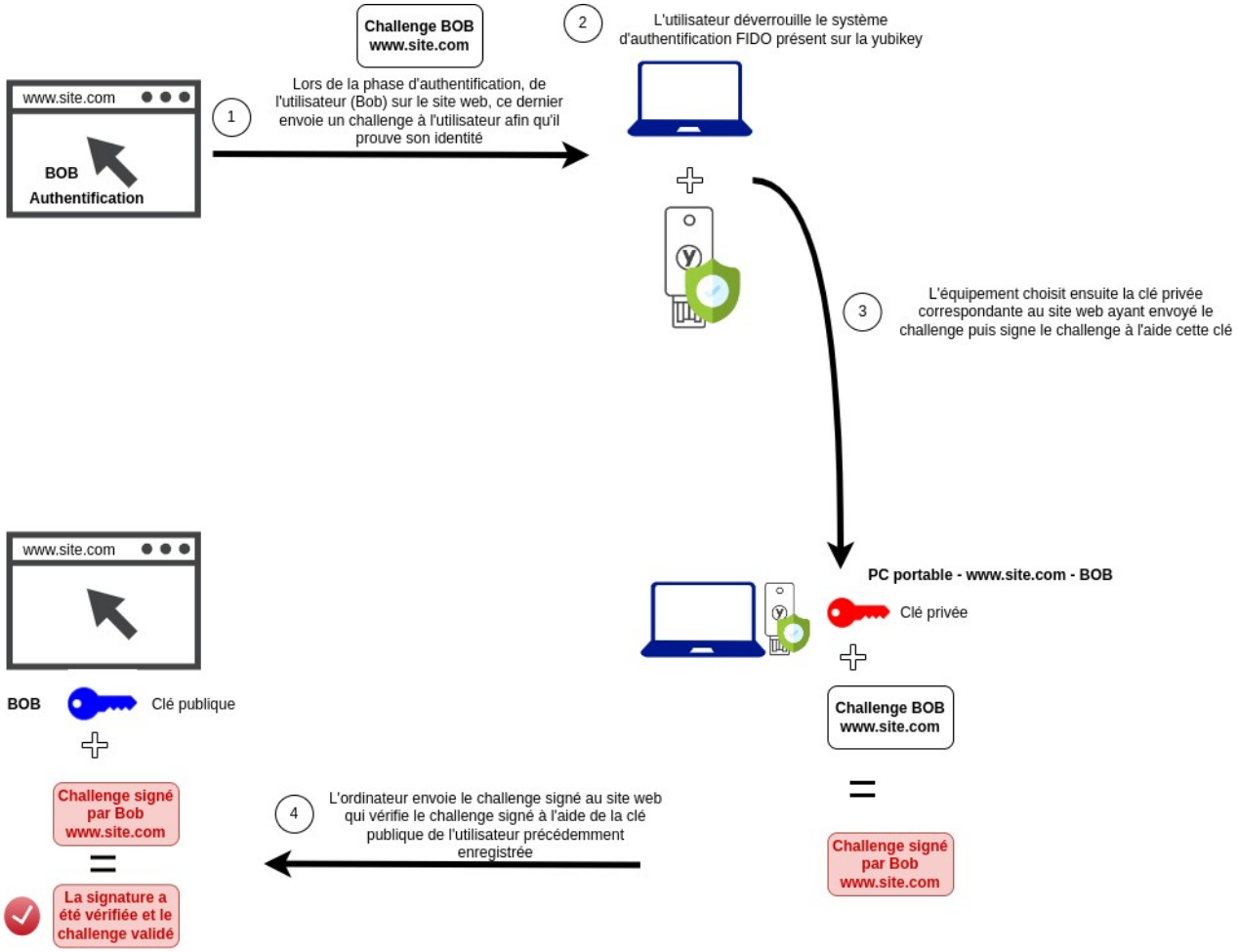
1. Lors de la phase de création ou de paramétrage d'un compte sur un site web compatible, il est nécessaire de choisir une authentification FIDO 2.
2. L'utilisateur approuve la demande de mise en place de FIDO 2 sur son appareil local (ordinateur ou smartphone) à l'aide de la yubikey.
3. L'appareil local génère alors une paire de clés publique/privée unique à la clé de sécurité, et au service en ligne choisis au préalable[1].
4. La clé publique est envoyée au site web (service en ligne) et elle est associée au compte utilisateur. La clé privée est gardée précieusement sur la yubikey en local.



1 *La clé publique peut être la source de l'identifiant d'un compte (i.e. le compte est potentiellement nommé à partir d'un dérivé de la clé publique).*

Phase d'authentification WebAuthn

1. Lors de l'authentification sur le site web, celui-ci envoie un challenge à l'utilisateur.
2. L'utilisateur doit déverrouiller l'accès à la clé privée présente sur la yubikey.
3. La yubikey sélectionne la clé privée correspondante au site web ayant envoyé le challenge puis signe ce dernier à l'aide cette clé.
4. Le site web vérifie la signature du challenge à l'aide de la clé publique de l'utilisateur qui a été stockée lors de la phase d'enregistrement.



Différences entre FIDO 2 et FIDO U2F

FIDO U2F est FIDO 2 utilise tous les deux un système de cryptographie à clés publiques.

FIDO U2F est le plus ancien (2014) des deux standards. C'est un protocole qui impose un second facteur d'authentification (en plus d'un mot de passe généralement). U2F signifie Universal 2nd Factor. Cette méthode permet à l'utilisateur d'accéder à une ressource informatique après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification.

FIDO 2 est une norme datant de 2019 qui permet de mettre en œuvre une authentification forte par simple facteur[2], ou par multifacteur.

2 *Le site web valide une seule authentification forte qui combine de façon transparente deux facteurs. Dans le cas de la yubikey, le deuxième facteur correspond au code PIN s'il a été défini correctement au préalable.*

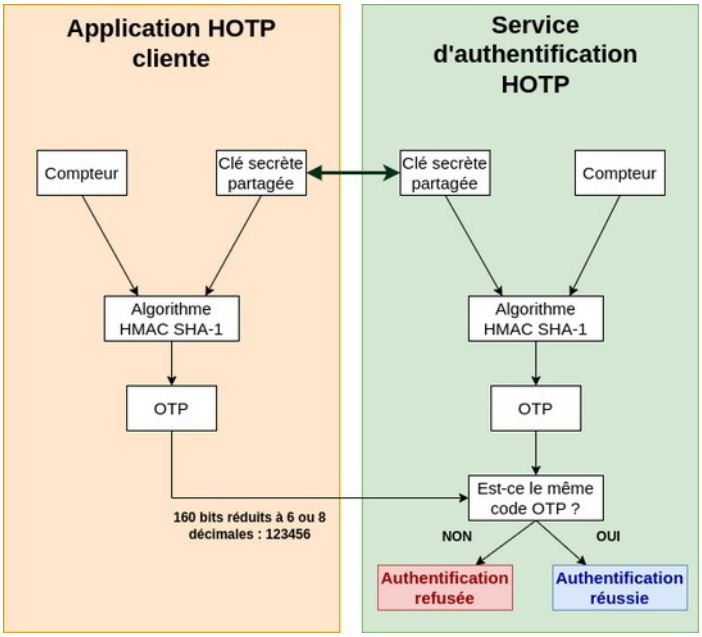
Mot de passe à usage unique basé sur le temps (HOTP / TOTP)

HOTP

HOTP (pour HMAC One Time Password) est un mécanisme d'authentification reposant sur l'utilisation d'une clé secrète et d'un compteur commun entre le client et le serveur. HOTP ne nécessite donc pas l'utilisation d'une horloge.

Il se base sur HMAC. HMAC est un type de code d'authentification de message qui combine l'utilisation d'une fonction de hachage (SHA-256) avec une clé secrète dans le but de vérifier simultanément l'intégrité des données et l'authenticité du message.

Toutefois, HOTP est susceptible de perdre la synchronisation du compteur entre le client (par exemple la clé de sécurité) et le serveur. Il peut ainsi s'avérer difficile de maintenir un compteur commun.



TOTP

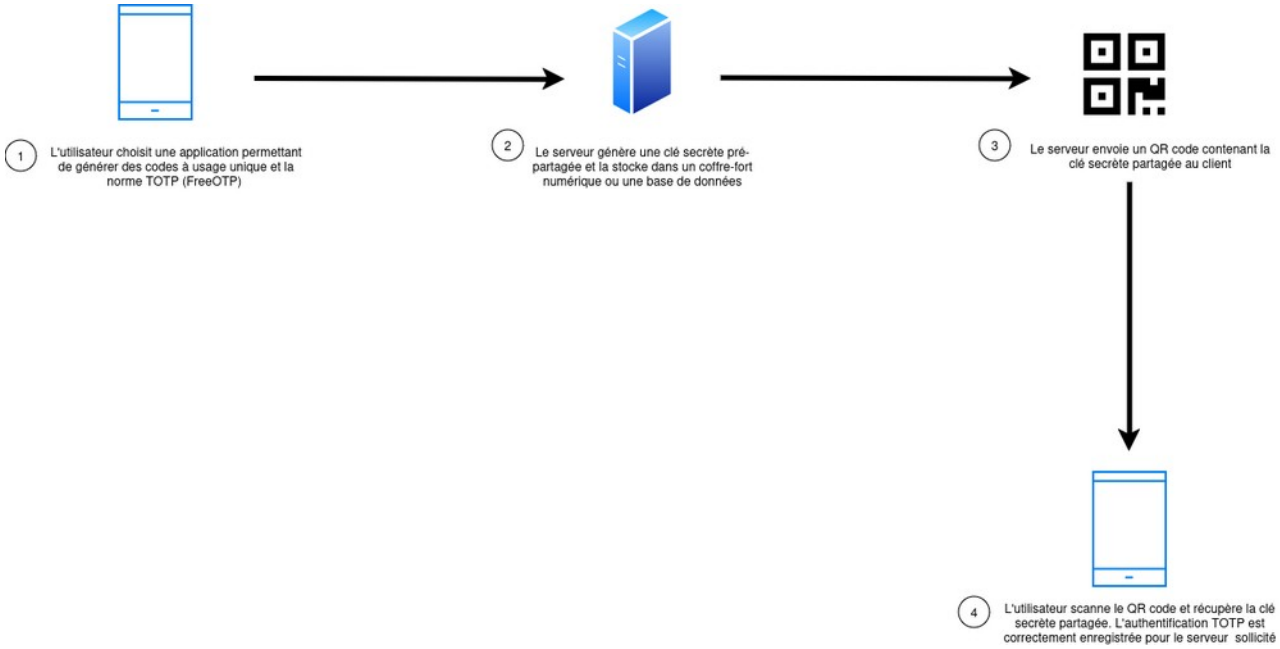
Un mot de passe à usage unique basé sur le temps (TOTP, Time based One Time Password en anglais) est un algorithme permettant de générer un mot de passe à usage unique.

Ainsi, TOTP permet la génération d'une séquence de caractères valable seulement pendant un intervalle de temps limité afin de constituer un mécanisme de double authentification. C'est une extension du mot de passe à usage unique basé sur HMAC. Contrairement à HOTP qui nécessite un compteur incrémental partagé entre les deux entités pour garantir l'utilisation unique, TOTP utilise l'heure[3] et un secret partagé. Un intervalle de temps de validité est défini pour tolérer une désynchronisation des horloges.

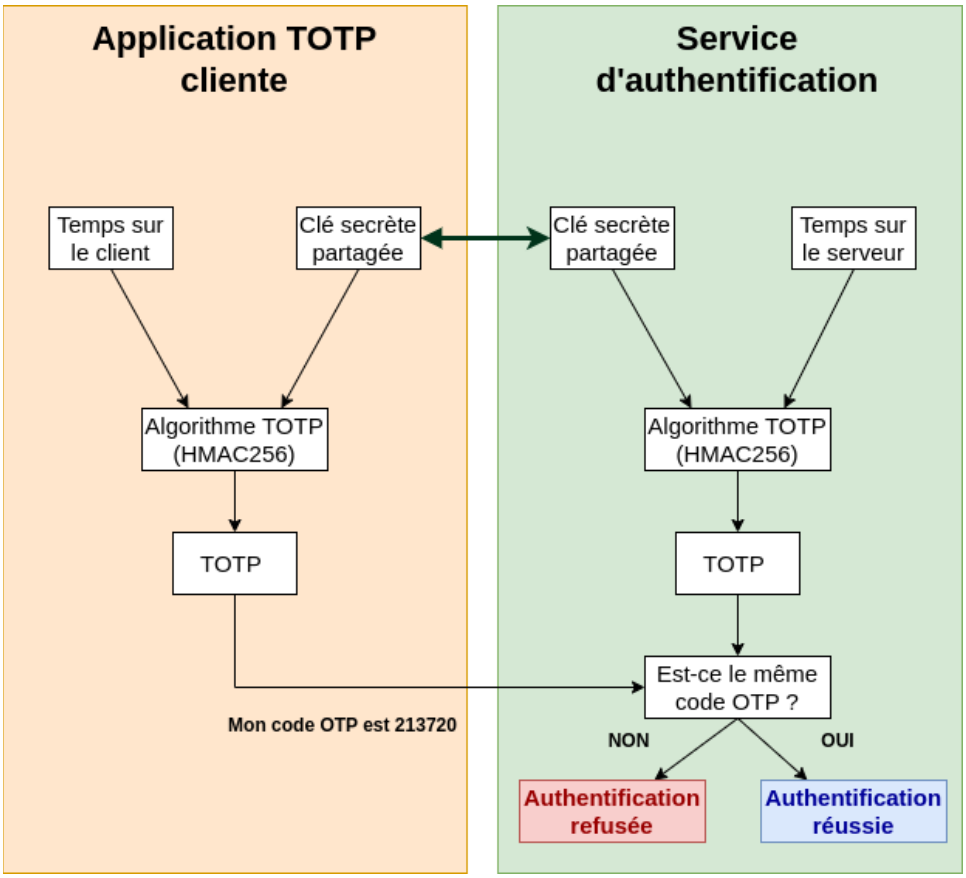
Source : Wikipédia

3 *Sous réserve que les horloges soient synchronisées.*

Phase d’enregistrement



Phase d’authentification



Dans le schéma ci-dessus, nous constatons que la clé secrète est commune et qu’elle a été transmise au client lors de la phase d’enregistrement. L’avantage de passer par une clé de sécurité est de pouvoir stocker cette clé secrète sur un matériel spécifique et non directement sur le smartphone ou sur l’ordinateur client.

> ⚠ **Attention !** Contrairement à la norme FIDO 2, TOTP ne protège pas d'un certain nombre d'attaques (phishing, fuite du secret commun sur le serveur). Cette méthode d'authentification est donc moins robuste que FIDO 2 et ne respecte pas l'état de l'art.

Challenge-réponse

Certaines applications ou certains systèmes nécessitent que l'utilisateur configure l'authentification par challenge-réponse sur un slot particulier de la clé de sécurité.

Deux algorithmes sont supportés par la yubikey :

- Yubico OTP
- HMAC SHA1

Le système d'authentification basé sur HMAC-SHA1 fonctionne de la manière suivante :

1. L'application (ou le système) et la yubikey dispose de la même clé secrète.
2. La yubikey doit être connectée sur l'hôte.
3. L'application ou le système présent sur l'hôte envoie un challenge sur le slot défini dans la yubikey.
4. La yubikey reçoit le challenge et génère une signature symétrique (appelée aussi motif d'intégrité) à l'aide de la clé secrète et de l'algorithme cryptographique type HMAC SHA-1 présents sur le slot.
5. La yubikey renvoie cette empreinte à l'application ou au système.
6. Cette dernière réalise la même opération sur le challenge d'origine à l'aide de la même clé secrète et du même algorithme. Elle compare ensuite l'empreinte qu'elle vient d'obtenir avec celle envoyée par la yubikey. Si les deux empreintes sont identiques, l'authentification est validée.

Source : https://docs.yubico.com/yesdk/users-manual/application-otp/challenge-response.html

> ⚠ **Attention !** L'algorithme de hachage SHA-1 est considéré comme déprécié. L'ANSSI préconise l'utilisation de SHA-2 et SHA-3. La CNIL, quant à elle, pourra sanctionner l'usage de cet algorithme obsolète dans des mécanismes d'authentification.

OpenPGP

Pretty Good Privacy, plus connu sous le sigle PGP, est un outil mettant en œuvre des algorithmes cryptographiques hybrides (asymétrique et symétrique) permettant entre autres de chiffrer et signer des données. Il a été développé et diffusé aux États-Unis par Philip Zimmermann en 1991.

Source : Wikipédia

Le dernier standard de PGP est défini dans la RFC 4880. Il a connu de nombreuses évolutions et ne correspond plus au standard originel créé par P. Zimmermann. OpenPGP est un standard alors que PGP et GnuPG en sont des implémentations logicielles.

La génération d'une paire de clés PGP peut se faire sur n'importe quelle machine à l'aide d'outils spécifiques tels que GnuPG. La problématique du chiffrement à clé publique est la conservation de la clé privée. En effet, si cette clé est dérobée par un attaquant, c'est l'ensemble du système de chiffrement ou de signature qui est compromis.

La yubikey permet ainsi de stocker la clé privée en dehors de l'ordinateur et de la rendre accessible par l'intermédiaire d'un code PIN à saisir. Après 3 échecs dans la saisie du code PIN,

l'accès à la clé privée est verrouillée. Le fait de stocker la clé privée sur une clé de sécurité réduit de manière considérable les risques de compromission.

Smart Card (PIV)

PIV est une norme ouverte couramment utilisée dans les organisations commerciales et gouvernementales pour l'identification à deux facteurs, la signature numérique et le chiffrement. Elle repose sur l'utilisation de certificats et le stockage de la clé privée sur la yubikey. Elle se rapproche ainsi des principes exposés précédemment avec OpenPGP.

RAPPEL CONCERNANT LES FACTEURS D'AUTHENTIFICATION

Voici les catégories de facteur d'authentification :

- **facteur de connaissance** : « ce que je sais », il s'agit d'une connaissance mémorisée ;
- **facteur de possession** : « ce que je possède », il s'agit d'un élément secret non mémorisable contenu dans un objet physique qui protège cet élément de toute extraction ;
- **facteur inhérent** : « ce que je suis », il s'agit d'une caractéristique physique indissociable d'une personne (ADN, empreinte digitale, empreinte rétinienne).

> Selon l'ANSSI, le facteur inhérent n'est recommandé qu'avec l'usage d'un facteur de possession dans le but du déverrouillage d'un élément permettant l'authentification forte.

RAPPEL CONCERNANT LA DIFFÉRENCE ENTRE AUTHENTIFICATION MULTIFACTEUR ET AUTHENTIFICATION FORTE

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).

Source : Guide de « Recommandations relatives à l'authentification multifacteur et aux mots de passe » publié par l'ANSSI