AUTHENTIFICATION PRIVÉE

NOTE D'INTERPRÉTATION

Mai 2018

Association Française des Hébergeurs Agréés de Données de Santé à caractère personnel

NOTE D'INTERPRÉTATION – AUTHENTIFICATION PRIVÉE

Version du 21 mars 2018

Avant-propos

Ce document est une note d'interprétation telle que prévue par le code de l'AFHADS. Elle porte sur les exigences de contrôle des applications hébergées en matière d'authentification.

C'est un guide pratique fondé sur l'expérience. Il ne se substitue pas aux éventuelles exigences qui seraient applicables au titre des futurs référentiels opposables, mais n'est en rien contradictoire avec l'état de ces référentiels tel qu'il est connu à la date de rédaction.

Il s'adresse à un public d'experts, et ne rappelle pas des éléments de l'état de l'art comme l'usage de fonctions cryptographiques sûres. Le but est seulement de s'accorder sur les options possibles.

Le sujet de l'identification n'est abordé ici qu'indirectement, au travers des besoins de désignation des utilisateurs ou techniciens de maintenance de l'application hébergée (pour l'authentification). Notamment l'utilisation de référentiels nationaux ou régionaux d'identité à des fins d'interopérabilité n'est pas traitée ici.

De même, on s'abstient ici de traiter de l'authentification dite publique, au sens de la PGSSI-S. L'immense majorité des applications hébergées ne relève en effet que de l'authentification privée, dans laquelle il existe une relation contractuelle établie entre les utilisateurs et l'offreur de service.

Terminologie

Les systèmes hébergés sont accessibles à deux populations :

- Les utilisateurs, y compris les administrateurs fonctionnels de la solution, qui accèdent via des interfaces qui leurs sont dédiées.
- Les techniciens de maintenance, qui ont un accès au système sous-jacent.

Les uns comme les autres sont connus au travers d'une identité numérique, plus ou moins complexe dans la forme (simple identifiant, adresse mail, DN d'un certificat, etc.)

Les crédits sont les éléments présentés par un utilisateur ou un technicien de maintenance pour attester de son identité numérique. Les procédés d'authentification visent à apporter un niveau de confiance sur le fait que ces crédits ne peuvent être présentés que par le titulaire légitime de l'identité numérique.

La corrélation est l'action d'associer une identité numérique à une personne physique ou un dispositif physique donné.

Authentification

Niveaux d'authentification requis

Le niveau d'authentification requis dépend du réseau depuis lequel les crédits sont présentés et d'éventuels accords entre les participants à ce réseau.

Si les crédits sont présentés depuis Internet ou un réseau ouvert, l'authentification forte est requise.

Si les crédits sont présentés depuis un réseau privé, trois cas de figure se présentent :

- Le réseau privé et l'application sont dédiés à un unique responsable de traitement, qui s'engage sur la maîtrise des accès physiques et logiques à son extrémité du réseau privé. En ce cas, l'authentification faible est acceptable pour les utilisateurs. C'est par exemple le cas de systèmes déportés via un VPN pour un établissement.
- Le réseau privé et l'application sont partagés entre plusieurs responsables de traitement, mais ils ont établi entre eux, ainsi qu'avec l'hébergeur, une convention de reconnaissance de leurs engagements mutuels sur la maîtrise des accès physiques et logiques. En ce cas l'authentification faible est encore acceptable pour les utilisateurs. Ce peut être le cas d'un VPN Santé régional.
- Si aucune des deux conditions ci-dessus n'est remplie, l'authentification forte est requise pour les utilisateurs.
- Dans tous les cas de figure, l'authentification forte est requise pour les techniciens de maintenance.

Procédés d'authentification

L'authentification par identifiant et mot de passe est une authentification faible. Dans ce cas de figure le mot de passe doit respecter la règle de complexité usuelle : au moins 8 caractères de 3 types différents parmi les quatre types majuscules, minuscules, chiffres et caractères spéciaux. Cette règle de complexité peut être relâchée dans le cas où le mot de passe n'est qu'un des facteurs d'une authentification forte.

Pour que l'authentification soit forte, elle doit être basée sur un second facteur de nature différente du premier et répondant aux critères suivants :

- Il ne doit pas être public ou facilement accessible à un tiers : le numéro RPPS ou le numéro de carte CPS, l'adresse IP du poste de travail ne sont pas recevables.
- Il doit être soit personnel, soit attribué à une structure ayant une autorité hiérarchique directe sur l'utilisateur. Un certificat attribué à un établissement est recevable ; un certificat générique embarqué dans une application mobile ne l'est pas.
- La méthode utilisée pour démontrer sa possession ne doit pas être vulnérable au rejeu. Un OTP reçu par un canal précédemment validé est recevable ; un cookie ne l'est pas.

A titre d'exemple, les procédés d'authentification suivants sont recevables :

- La présentation d'un certificat client individuel issu d'une carte CPS ou d'un autre support sécurisé
- La présentation d'un certificat client logiciel individuel et la saisie d'un mot de passe (le seul certificat ne suffit pas car son confinement côté client n'est pas démontrable)

- La présentation d'un certificat client de structure, d'un identifiant et d'un mot de passe.
- La présentation d'un identifiant, d'un mot de passe, puis d'un code à usage unique reçu par mail ou par SMS.
- La présentation d'un identifiant, d'un mot de passe, puis d'un code basé sur le temps et un secret obtenu lors d'une connexion précédente (TOTP selon la RFC 6238)
- La présentation d'un identifiant, d'un mot de passe, puis d'un code issu d'une grille de codes communiquée précédemment par un canal sûr
- La présentation d'un identifiant, d'un mot de passe, puis de la réponse à un challenge exigeant la connaissance d'une clé privée associée à cet identifiant (jetons FIDO U2F)

Authentification par un tiers

L'authentification par un tiers est possible dans la mesure où :

- Cette authentification est reconnue comme valide par l'ensemble des responsables de traitement utilisant l'application hébergée.
- Elle est effectuée selon une méthode acceptable pour une authentification directe dans le contexte où elle est effectuée. Ceci signifie notamment qu'une authentification faible effectuée dans un réseau local sécurisé d'un établissement est acceptable si tous les responsables de traitement utilisant la même application en ont accepté le principe.
- Le mécanisme de propagation de l'authentification tierce à l'hébergeur est sûr, tant dans l'identification de l'origine de l'authentification que dans l'inaltérabilité de son contenu.

Ce peut être par exemple le cas :

- D'une authentification par un annuaire d'établissement propagée via un jeton SAML
- D'une authentification par un portail régional de santé
- D'une authentification France Connect de niveau substantiel

Corrélation

L'authentification telle que détaillée ci-dessus permet de s'assurer de l'identité numérique de l'utilisateur. À elle seule, elle peut permettre de lui donner accès aux données qu'il a lui-même déposées, mais pas d'accéder à des données déposées par des tiers.

Pour pouvoir accéder à des données tierces, son identité numérique doit avoir été corrélée à une personne ou un dispositif physique. Cette corrélation peut être effectuée implicitement ou par une personne habilitée précédemment corrélée.

La corrélation implicite est possible lorsque l'authentification est effectuée par une carte CPS ou par un système tiers.

Le principe de corrélation exige que chaque identité numérique soit univoque. Les cas particuliers ou cela serait impossible (remplacement d'urgence, interne de garde, etc…) doivent être identifiés et une méthode palliative organisationnelle mise en place pour que l'identité physique puisse être retrouvée à posteriori en cas de besoin.

En aucun cas l'utilisation d'une identité générique n'est acceptable pour un technicien de maintenance.