Direction des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
www.vd.ch

GUIDE AUTHENTIFICATION ADAPTATIVE

Contenu

1.1 Introduction

Pour se connecter à un système de façon sécurisée, il faut prévoir une authentification multifacteur qui peut être composée de:

Quelque chose que l'on **sait**
Ex : un mot de passe

Quelque chose que l'on **a**
Ex : un code envoyé par SMS sur son téléphone

Quelque chose que l'on **est**
Ex : une empreinte digitale

Un nom d'utilisateur et un mot de passe ne sont plus suffisants pour l'authentification des utilisateurs. Pas un jour ne passe sans que l'on entende une nouvelle histoire d'hameçonnage, de vol de mots de passe ou d'usurpation d'identité. La menace est réelle et ne cesse de grandir. La seule réponse efficace contre ce type d'attaque : l'authentification à multifacteur. Elle se base sur l'hypothèse que si votre mot de passe est compromis, car un hacker situé n'importe où dans le monde a réussi à se le procurer, celui-ci devra encore avoir accès à un élément que vous possédez afin de se connecter sur le système sécurisé. L'Administration cantonale s'efforce d'adopter des mesures de sécurité simplifiées, mais néanmoins robustes, pour répondre efficacement aux risques, tout en améliorant l'expérience utilisateur ; dernière en date : **l'authentification adaptative**.

1.2 L'authentification adaptative, c'est quoi ?

L'authentification adaptative permet de remplacer le second facteur d'authentification par des informations disponibles sur l'appareil avec lequel l'utilisateur se connecte. Ainsi, l'appareil (téléphone portable, ordinateur, tablette) avec lequel l'utilisateur accède au portail IAM représente la partie « quelque chose qu'on a » dans la chaîne d'authentification : plus besoin de saisir un code à usage unique transmis par SMS, par exemple.

Illustration

Lorsque l'utilisateur souhaite accéder à une application disponible en authentification forte, après la saisie de son identifiant et de son mot de passe, une nouvelle case à cocher est disponible.

- Si l'utilisateur sélectionne cette option : la prochaine fois qu'il souhaitera accéder à une application en authentification forte à partir de cet appareil, il n'aura pas à ressaisir de code envoyé par SMS.
- Si l'utilisateur ne sélectionne pas cette option : aucun changement par rapport à la situation actuelle ; la prochaine fois qu'il souhaitera accéder à une application en authentification forte, la page de saisie du code envoyé par SMS lui sera à nouveau affichée.

Lorsque l'utilisateur se connecte à une application en authentification forte à partir d'un **autre appareil** (non associé), la page permettant de saisir son second facteur lui sera affichée (avec l'option « se souvenir de mon appareil ») et il aura ainsi la possibilité d'associer, s'il le souhaite, jusqu'à 5 appareils à son compte.

1.3 Fonctionnement

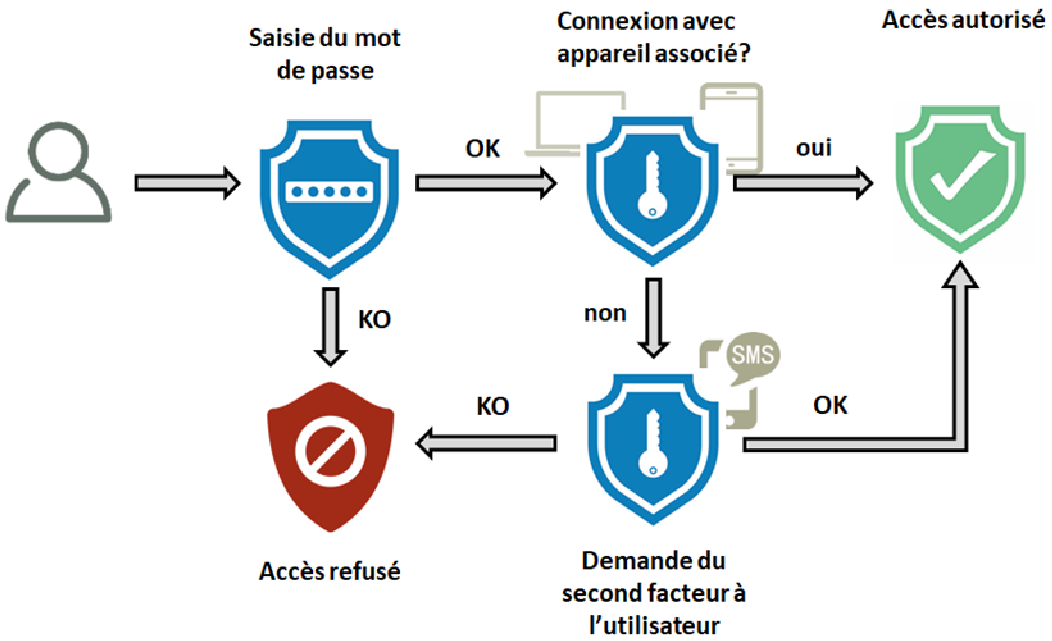
Pour mettre en place ce nouveau dispositif – **qui restera facultatif** –, la Direction des systèmes d'information (DSI) a réalisé un énorme travail sur le paramétrage technique de cette fonctionnalité, en s'efforçant de rendre ce nouveau système le plus sûr possible.

Lors de l'authentification, après que l'utilisateur a saisi son mot de passe, le système compare les informations de l'appareil en cours d'utilisation pour se connecter avec les informations collectées (pour autant qu'il ait cliqué sur le bouton de type « se souvenir de mon appareil »).

- Si les données correspondent, le second facteur (SMS) n'est pas demandé.
- Si les données ne correspondent pas, le second facteur (SMS) est exigé.

Les données collectées depuis votre appareil – telles que l'adresse IP ou la version du navigateur utilisé – font de l'empreinte numérique de votre dispositif une trame unique, qui vous est propre.

Fonctionnement de l'authentification adaptative



1.4 Gestion de ses données

Seules les données techniques que l'utilisateur expose déjà en permanence lorsqu'il navigue sur internet sont collectées. Ces données sont stockées de façon sécurisée et seront uniquement utilisées à des fins d'authentification sur le portail IAM. Voici une liste (non exhaustive) des informations utilisées pour l'authentification adaptative :

- IP source
- Navigateur utilisé
- Les agents utilisateur
- Les polices installées
- …

= 1 appareil associé

Exemple:
«123.123.123.123»
«Chrome v72»
«Mozilla/5 (X11; Ubuntu; Linux x86_64; rv:60.0)»
«cursive;monospace;serif;»

L'utilisateur peut associer jusqu'à 5 appareils (avec leur configuration respective) à son compte. Lors de l'association d'un 6ème appareil (et suivants), l'enregistrement le plus ancien sera effacé.

L'utilisateur peut à tout moment accéder à la section « Authentification forte » du portail self-service IAM, et gérer ses appareils associés.

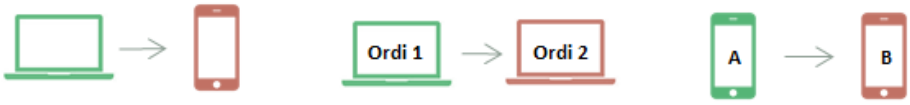
Il peut ainsi voir les appareils associés, les supprimer et également désactiver les notifications envoyées.

1.5 Limitations de l'authentification adaptative

Afin de garantir un niveau de sécurité élevé, les paramètres techniques utilisés pour l'authentification adaptative sont, dans un premier temps, assez stricts. Le chapitre suivant présente les cas d'utilisation de l'authentification adaptative et leur influence sur l'appareil associé.

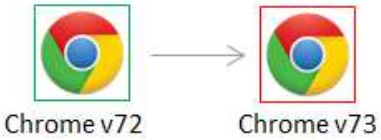
Les situations suivantes induisent un changement de l'empreinte, ce qui nécessite l'association d'un nouvel appareil :

- Changement de poste physique
  L'utilisation d'un poste physique différent oblige l'association d'une nouvelle empreinte à son compte.



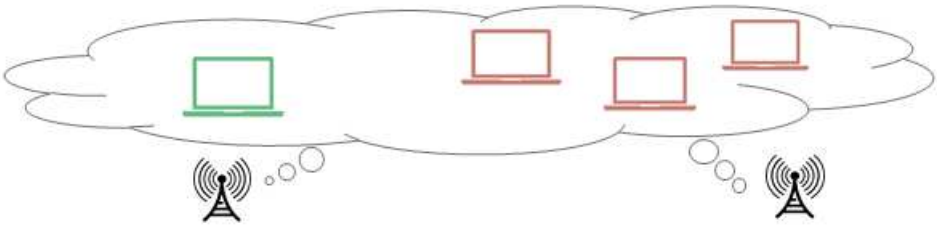
- Changement de navigateur
  L'utilisation d'un navigateur web différent oblige l'association d'une nouvelle empreinte à son compte.

- Changement de version du navigateur
  La mise à jour majeure du navigateur web oblige l'association d'une nouvelle empreinte à son compte.



Information : les versions majeures de Chrome sont mises à jour environ tous les 1.5 mois.

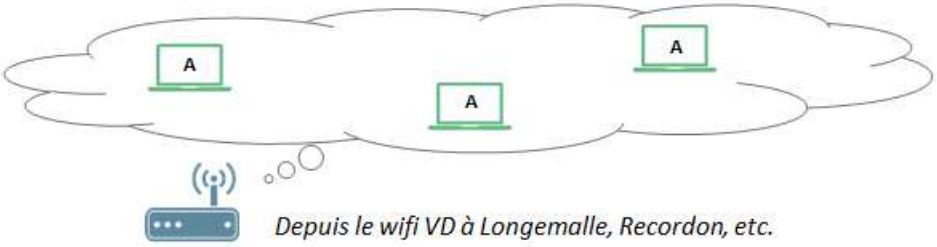
- Connexion 3G ou 4G
  L'adresse IP varie très fortement lorsque l'utilisateur se connecte à travers la 3G, 4G ou 5G. **Nous recommandons de ne pas** associer une empreinte à son compte à travers ce type de connexion.



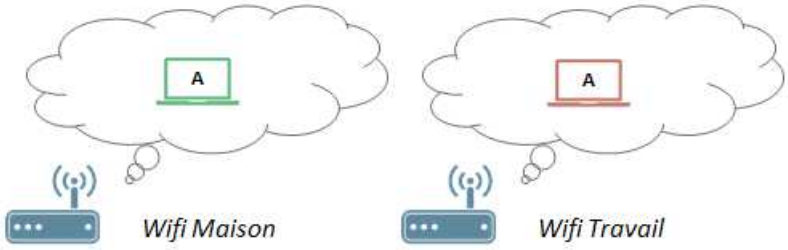
Les situations suivantes ne conduisent pas de changement de l'empreinte

- Reconnexion depuis le même réseau filaire
  Lorsque l'utilisateur se connecte depuis un même réseau filaire, l'adresse IP est stable. Le niveau de stabilité dépend de la configuration du réseau à partir duquel on se connecte. Sur le Réseau cantonal vaudois (RCV), il peut rester le même plusieurs mois.

- Reconnexion depuis le même wifi
  Lorsque l'utilisateur se connecte depuis un même réseau wifi, l'adresse IP est stable. Le niveau de stabilité dépend de la configuration du réseau à partir duquel on se connecte. Sur le wifi de l'Administration cantonale, il peut rester le même plusieurs mois.



Par contre, le changement de réseau wifi oblige l'association d'une nouvelle empreinte à son compte.



1.6 Recommandations d'utilisation

Afin d'utiliser de façon efficace et sécurisée l'authentification adaptative, l'utilisateur doit respecter les recommandations suivantes :

- Ne jamais cliquer sur l'option « se souvenir de mon appareil » sur un poste non personnel
  - Poste de travail public
  - Poste de travail partagé (poste de guichet ou poste en libre-service)
  - Poste de travail d'un collègue
- Ne jamais utiliser cette option sur un poste non sécurisé :
  - Ordinateur, téléphone ou tablette qui n'a pas de verrouillage / déverrouillage par un mot de passe
- Le changement d'adresse IP ayant une influence sur votre empreinte numérique, utilisez cette fonctionnalité de préférence à travers un réseau filaire ou un réseau Wifi.