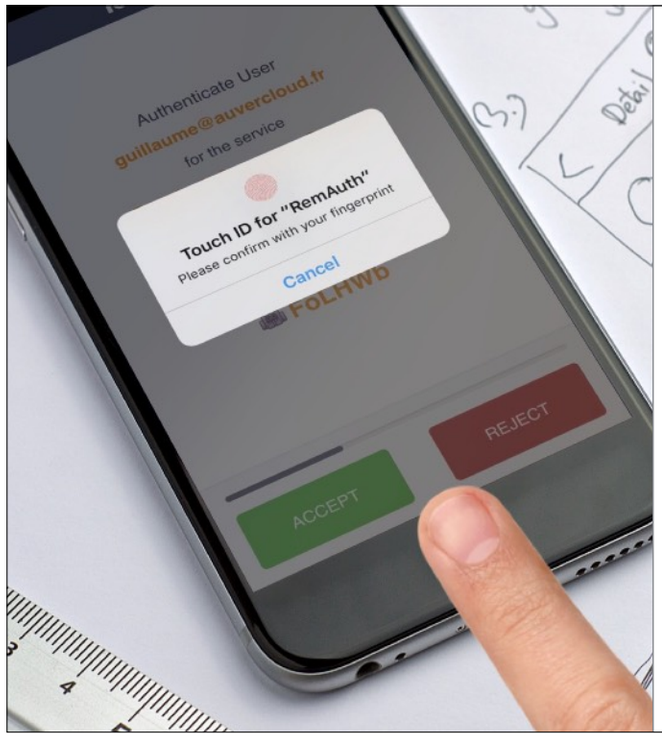


La vérification biométrique comme alternative aux mots de passe ?

Guillaume DORBES
- PDG AUVERCLOUD
- créateur de remauth.com

A propos d’authentification et d’identité dans le monde des applications.
Aujourd’hui le mot de passe est le Sesame de notre monde connecté, mais, comme nous le verrons plus loin, il est également une menace très significative.
Alors, comme nous nous sommes rassemblés ici pour parler biométrie, nous allons voir dans quelle mesure la biométrie représente une alternative crédible aux mots de passe.

Les mots de passe sont un mal..
… pas forcément nécessaire

credit : garfield.com

On l’a tous vécu ! Et pourtant, il faut bien s’assurer de l’identité d’un utilisateur, généralement définie par une adresse email. Adresse email qui est d’ailleurs la position de repli quand le mot de passe est perdu ou volé avec les procédures dites de « reset ». C’est en effet le cas pour la quasi totalité des services grand public, même si certains sont « durcis » avec un deuxième facteur d’authentification.

63%
des violations
de données
mettent en cause
les mots de passe

Source : Verizon Data Breach Investigations Report 2016

Il s’agit bien sûr des violations de données avérées !

- Les causes du problème : Les mots de passe sont souvent trop simples et mal protégés tant du côté des utilisateurs que des fournisseurs de service.
- La cause de la cause : Les mots de passe sont perçus comme un mal nécessaire par les utilisateurs qui ne veulent pas y consacrer d’effort pour les mémoriser et les gérer.
- La multitude des services est un facteur d’aggravation puisque idéalement il faudrait choisir un mot de passe différent et complexe pour chaque service et que bien sûr on ne le fait pas.

La chaine de confiance qui relie l'utilisateur au fournisseur de service est constitué de 3 maillons :

1) l'utilisateur
2) l'appareil (matériel+logiciel) qui permet d'accéder au service
3) le service

En orange, la vérification par mot de passe
En bleu, la vérification biométrique

Tout se joue au niveau de l'utilisateur et de sa relation avec l'appareil :

- dans le cas de la biométrie l'information de vérification et le transmetteur ne font qu'un et le capteur est plus complexe.

A l'arrivée, la question est : « A qui peut-on ou doit-on faire confiance » ?

Mot de Passe vs Biométrie

	Mot de Passe	Biométrie
Source d'information	Données mémorisées	Données corporelles
Capteur d'information	Clavier	Lecteur d'empreinte / caméra
Vecteur d'identification	Généralement simple	Plutôt complexe
Interception de données	Assez simple	Variable selon algorithme

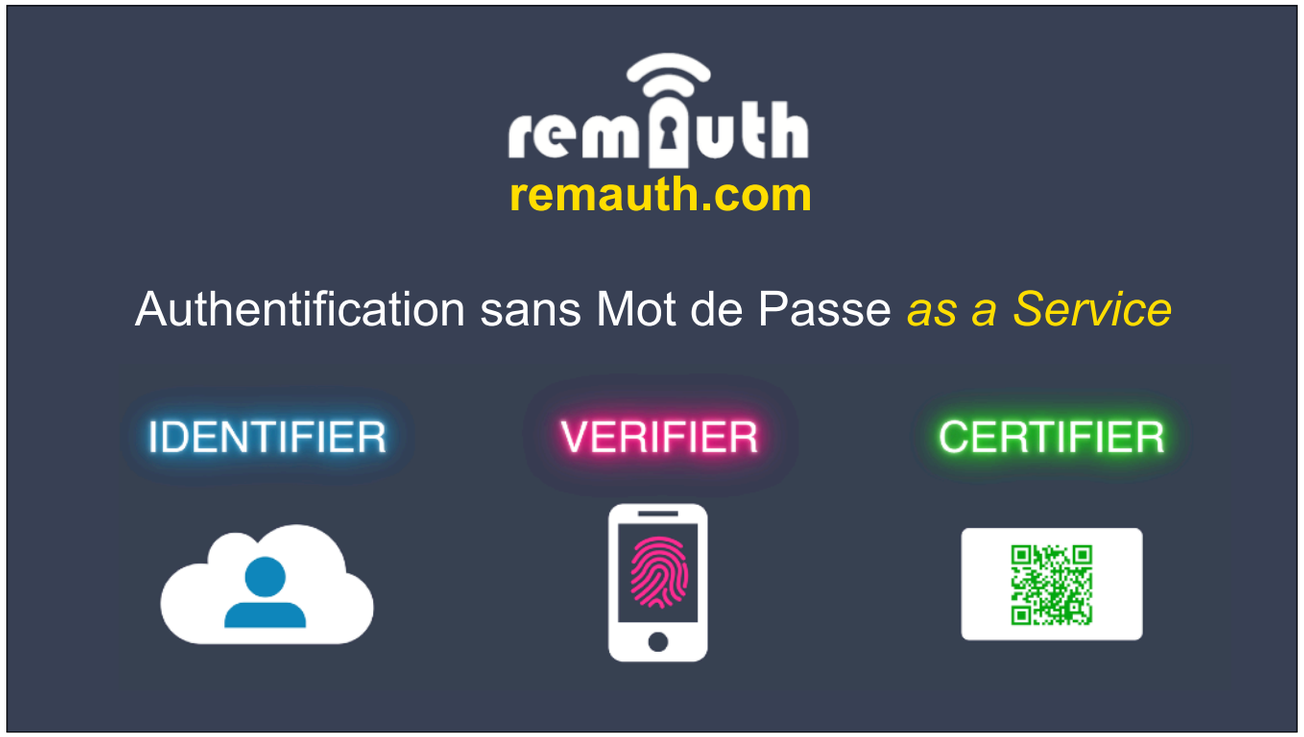
- Données corporelles sont aussi fiables que données mémorisées
- Simplicité du capteur vs dépendance à un vendeur de composant complexe. Le capteur d'empreinte digitale constitue une première approche intéressante, mais le caméra a le bénéfice d'être un composant standard, banalisé, disponible sur tous smartphones et beaucoup d'ordinateurs et dont les performances sont en croissance permanente.
- Les mots de passe sont généralement trop simples et/ou répétitifs alors que les vecteurs d'identifications biométriques peuvent être complexes et multiples.
- Attention à l'interception de mot de passe par keylogger ! Attention aux bases de données mal « salées »… La qualité de la biométrie tient dans la qualité de ses algorithme et de ses implémentations, mais est globalement largement moins sensible à l'interception de données que le sont les mots de passe.

En matière de reconnaissance digitale sur smartphone, aujourd'hui les services subissent une dépendance totale des API Android et iOS ou de solutions propriétaires. Open Source est la solution qui devra s'imposer !
Résultat : La vérification biométrique est meilleure, pas 100% sûre (rien de l'est jamais), mais en constant progrès.

« Se connecter à un service devrait toujours être simple et sûr »

- Guillaume DORBES, 2017

Est-ce que les mots de passe sont simples ? NON
Est-ce que la biométrie permet de se connecter simplement ? OUI
Est-ce que les mots de passe sont sûrs ? NON !
Est-ce que la biométrie est sûre pour authentifier un individu ? OUI mais cela dépend également des capteurs et des algorithmes, mais en tous les cas beaucoup plus sûre que les mots de passe !

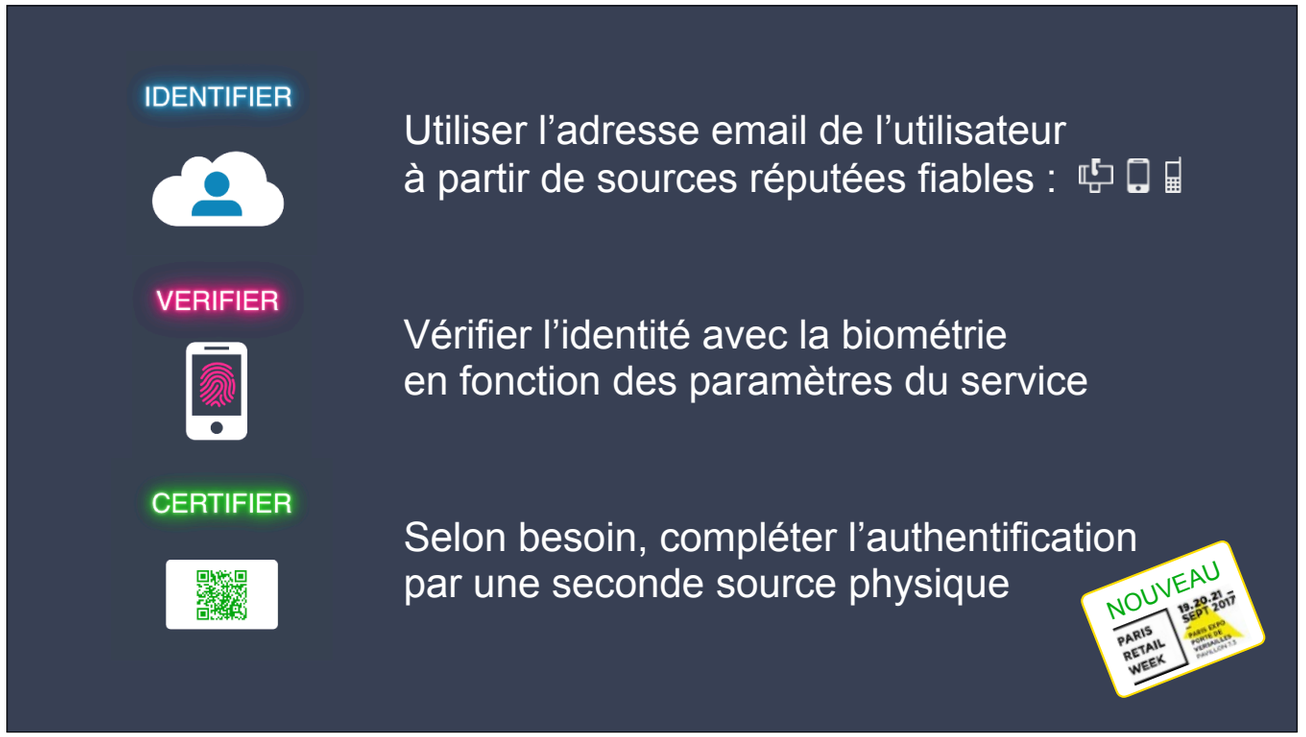


Fort du constat précédent, RemAuth se propose de résoudre les problèmes d'authentification par un service en mode cloud constitué de 3 fonctions:

- Identifier l'utilisateur de façon simple et sans mot de passe.
- Vérifier l'identité avec des méthodes biométriques.
- Certifier l'utilisateur par une seconde source physique.

En mode « cloud » signifie :

1) Pas d'investissement lourd, ni financier, ni technique.
2) Une mise en oeuvre rapide
3) Une solution accessible à tous => Ce n'est pas réservé aux grandes sociétés qui en ont les moyens.



Fonctions simples à mettre en oeuvre grâce au mode cloud qui permet un paramétrage simple et une intégration à faible cout grace à une API HTTP standard.
L’extension « CERTIFICATION » de remauth.com avec utilisation de certificats physiques sera dévoilée en septembre à la Retail Week de Paris.

« Biometrics beat passwords
for 93% of UK consumers »

- Mastercard and University of Oxford, June 13, 2017

L’attente des utilisateurs est forte même si les décideurs peinent à passer à l’acte.
RemAuth peut aider à assurer cette transition.

remauth

remauth.com

Guillaume DORBES
guillaume@auvercloud.fr
+33 (0) 777 99 88 33