Identité numérique

Tour de France de la Cybersécurité

Dr. Michel Dubois

michel.dubois@laposte.fr

9 décembre 2020

DIRECTION
CYBERSÉCURITÉ
GROUPE

Plan

DIRECTION
CYBERSÉCURITÉ
GROUPE

Section 1
L'identité numérique

DIRECTION
CYBERSÉCURITÉ
GROUPE

1. L'identité numérique

L'identité numérique

Notions d'identité

Emprunté du bas latin identitas, «qualité de ce qui est le même»,
dérivé du latin classique idem, «le même»

Sens général Exacte ressemblance entre des êtres, des choses qui ont une existence distincte.

Logique Principe d'identité, principe d'évidence selon lequel une chose ne peut être que ce qu'elle est.

Mathématique Relation d'égalité entre deux termes, qui subsiste quelles que soient les valeurs attribuées aux variables. ($a \times 1 = a$ ou $a + 0 = a$)

Biologie Caractère de ce qui, dans un être, reste identique, permanent, et fonde son individualité.

Droit Personnalité civile d'un individu, légalement reconnue ou constatée, établie par différents éléments d'état civil et par son signalement.

Sociologie Ensemble de caractères attribués à une personne et influençant son comportement et ses relations sociales.

https://www.dictionnaire-academie.fr/article/A9I0058 et https://fr.wiktionary.org/wiki/identité

1. L'identité numérique

L'identité numérique

Identification et authentification

Identification

- Action de considérer comme identiques plusieurs êtres, plusieurs choses
- Action d'établir l'identité d'une personne
- Le fait de s'identifier, de s'assimiler à une personne ou à une chose

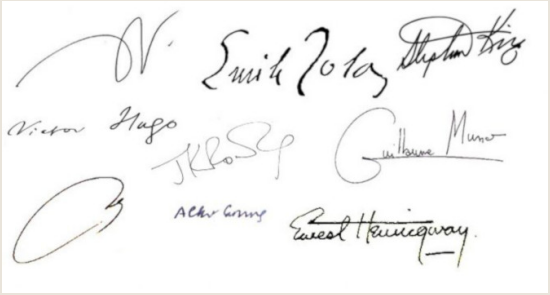
https://www.dictionnaire-academie.fr/article/A9I0054

L'identité numérique

Identification et authentification

Authentification - Le fait d'authentifier

- Donner un caractère légal à un document. Par extension authentifier une signature
- Prouver l'authenticité, déclarer authentique après expertise



https://www.dictionnaire-academie.fr/article/A9A3208

1. L'identité numérique

L'identité numérique

Définition identité numérique

Deux angles de défintion de l'identité numérique

1. l'identité numérique comme reflet des comportements en ligne des individus
   - ensemble des traces laissées en surfant sur Internet
   - utilisé pour catégoriser l'individu
2. l'identité numérique comme identifiant d'accès à un service, choisi pour ou par le détenteur
   - déclarative ou imposée par le service
   - en rapport avec l'état civil ou non

L'identité numérique

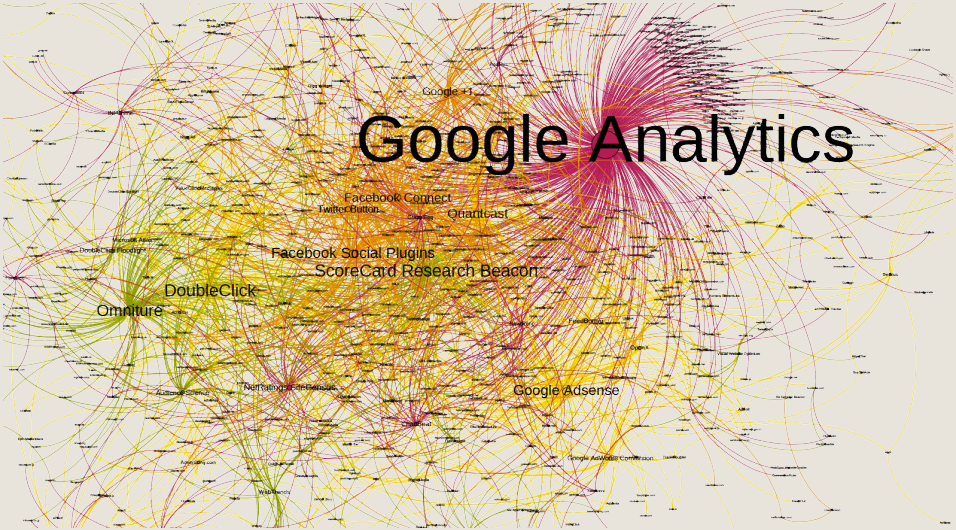
Définition identité numérique

Identité numérique comme reflet des comportements en ligne des individus

L'identité numérique

Définition identité numérique

Identité numérique comme reflet des comportements en ligne des individus

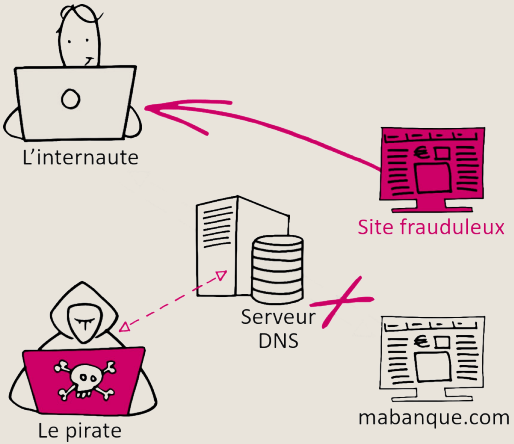


https://www.annehelmond.nl/2012/02/29/track-the-trackers-and-watch-the-watchers/

L'identité numérique

Définition identité numérique

Identité numérique comme identifiant d'accès à un service, choisi pour ou par le détenteur



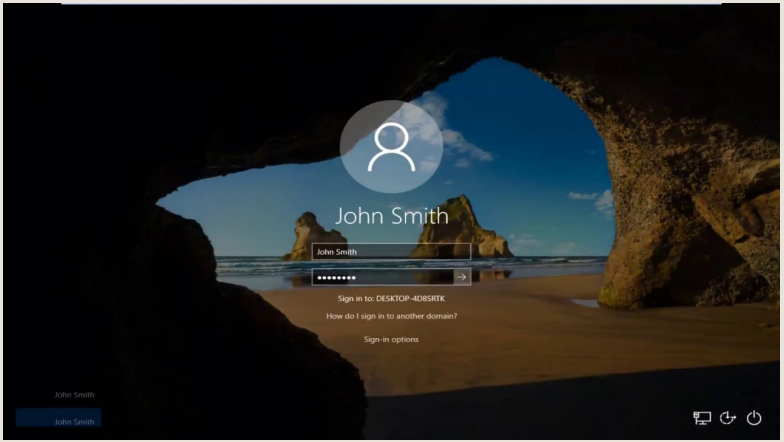
Qui se connecte à quoi ?

L'identité numérique

Définition identité numérique

Identité numérique comme identifiant d'accès à un service, choisi pour ou par le détenteur

- identification
- authentification
- droits d'accès
- audit

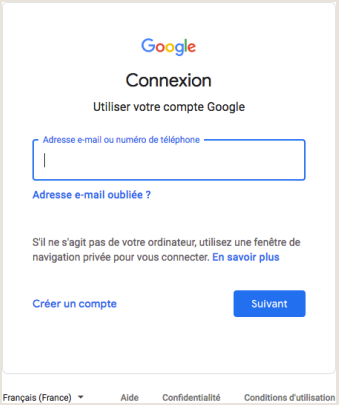


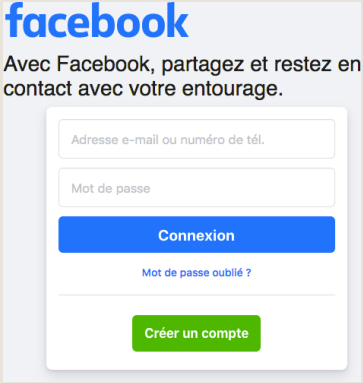
1. L'identité numérique

L'identité numérique

Plateformes et standards

Plateformes de gestion d'identité numérique



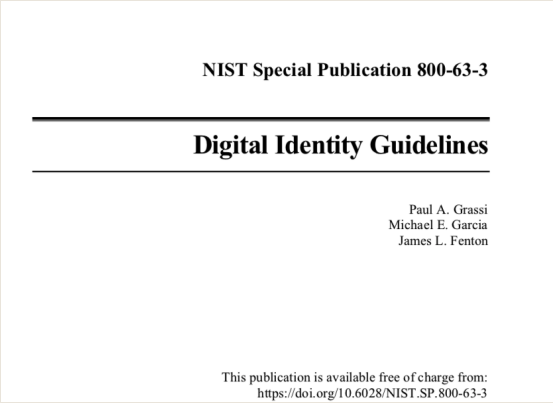


Quelle confiance ?

L'identité numérique

Plateformes et standards

Standards et réglementation

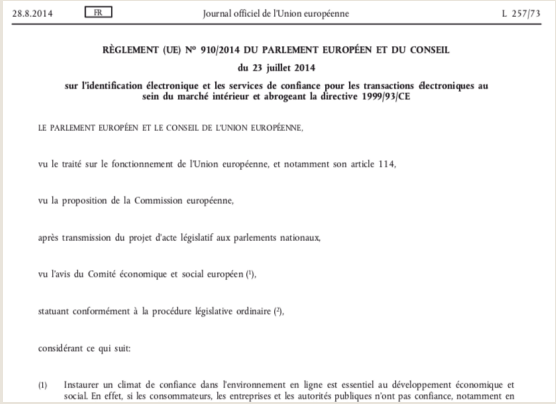


NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3



28.8.2014 FR Journal officiel de l'Union européenne L 257/73

RÈGLEMENT (UE) Nº 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 23 juillet 2014

sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen (1),

statuant conformément à la procédure législative ordinaire (2),

considérant ce qui suit:

(1) Instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique et social. En effet, si les consommateurs, les entreprises et les autorités publiques n'ont pas confiance, notamment en

L'identité numérique

Plateformes et standards

Plateformes de gestion d'identité numérique

Plateforme de confiance!

France Connect

Section 2

Comment s'authentifier ?

DIRECTION
CYBERSÉCURITÉ
GROUPE

2. Comment s'authentifier ?

Comment s'authentifier ?

Les algorithmes

Les services cryptographiques

Service		Algorithme	
Nom	Détail	Cryptographie symétrique	Cryptographie asymétrique
Confidentialité	Protection de l'information par le chiffrement des données lors du stockage ou de la transmission	Chiffrement par bloc ou par flot	Chiffrement à clé publique
Intégrité	Protection contre les modifications invalides de l'information lors du stockage ou de la transmission	Fonction de hachage cryptographique	Signature numérique
Authentification de données	Garantir l'identité de l'émetteur de l'information	Code d'authentification de message	Signature numérique
Authentification d'entités	Prouver l'identité d'une entité (humain ou machine)	Défi-réponse	Signature numérique
Non-répudiation	Protection contre le déni d'action sur des informations par une entité	Code d'authentification de message	Signature numérique
Génération d'aléa	Création de clés cryptographiques et de vecteurs d'initialisation	Générateur de nombres pseudo-aléatoires	

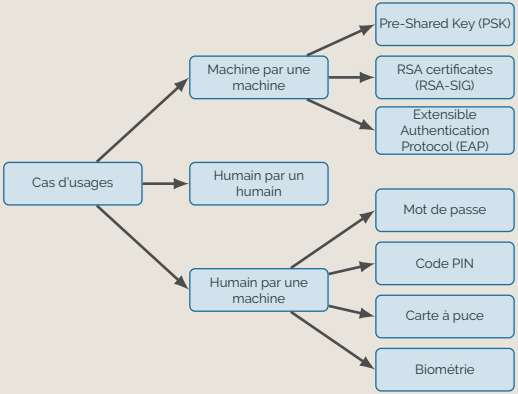
Comment s'authentifier ?

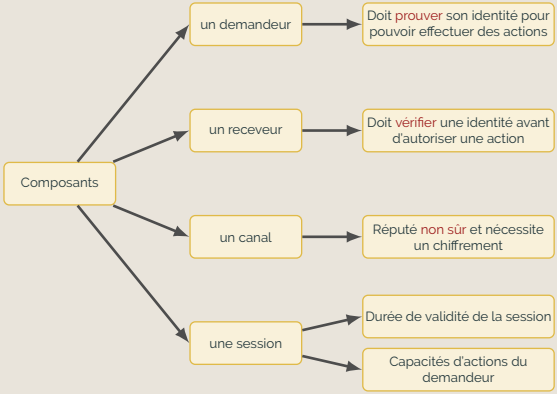
Les algorithmes

L'authentification d'entités

Définition

L'authentification a pour but de vérifier l'identité dont une entité se réclame





2. Comment s'authentifier ?

Comment s'authentifier ?

Méthodes d'authentification

Identification

L'identification a pour fonction de définir l'identité d'une entité.

Authentification

L'authentification a pour fonction de vérifier de manière certaine l'identité d'une entité.

Autorisation

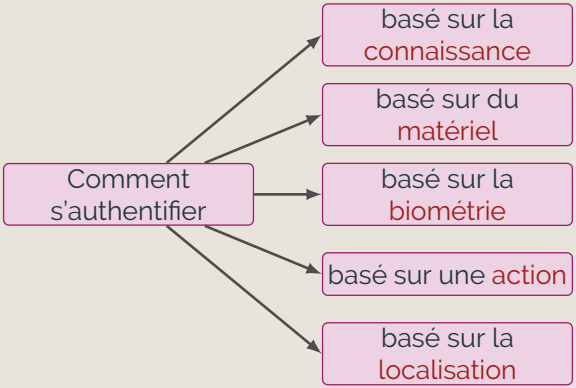
Ensemble des droits accordés à une entité après identification et authentification.

Traçabilité

Ensemble des informations récoltées pendant toute la durée de la session d'une entité identifiée et authentifiée.

Comment s'authentifier ?

Méthodes d'authentification



DIRECTION
CYBERSÉCURITÉ
GROUPE

2. Comment s'authentifier ?

Comment s'authentifier ?

Le mot de passe

TODAY I FOUND OUT
FEED YOUR BRAIN

HOME | SURPRISE | STORE | OUR BOOK! | ARTICLES | PODCAST | QUICK FACTS

FOR NEARLY TWO DECADES THE NUCLEAR LAUNCH CODE AT ALL MINUTEMAN SILOS IN THE UNITED STATES WAS 00000000

KARL SMALLWOOD NOVEMBER 29, 2013 102

Today I found out that during the height of the Cold War, the US military put such an emphasis on a rapid response to an attack on American soil, that to minimize any foreseeable delay in launching a nuclear missile, for nearly two decades they intentionally set the launch codes at every silo in the US to 8 zeroes.

We guess the first thing we need to address is how this even came to be in the first place. Well, in 1962 JFK signed the *National Security Action Memorandum 160*, which was supposed to ensure that every nuclear weapon the US had be fitted with a *Permissive Action Link (PAL)*, basically a small device that ensured that the missile could only be launched with the right code and with the right authority.

Des réseaux informatique, des services & applications

↓

nécessité d'authentifier et de tracer les entités connectées

Comment s'authentifier ?

Le mot de passe

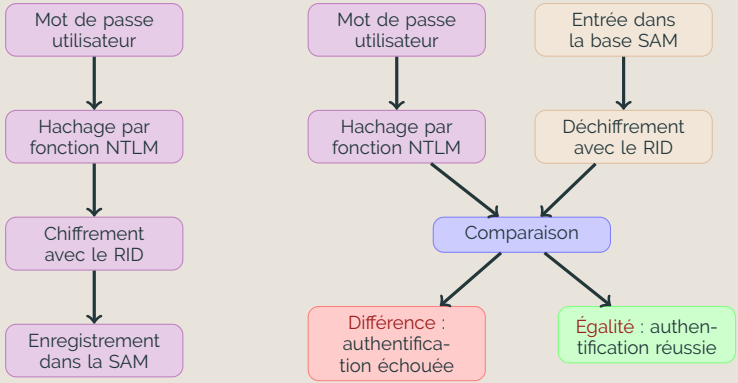
Principe de base

La sécurité d'un système d'information est aussi bonne que celle des mots de passe d'authentification.

Comment s'authentifier ?

Le mot de passe

Processus d'authentification local sous Windows



Source : `http://www.hsc.fr/`

Comment s'authentifier ?

Le mot de passe

Techniques pour casser un mot de passe

Deviner le mot de passe

Utilisation du social engineering (canulars téléphoniques, fouille des poubelles, recherche sur Internet…).

Se faire passer pour le système

Avec des outils de spoofing (Un faux logiciel de connexion imitant le vrai enregistre le mot de passe dans un fichier accessible par le pirate).

Espionner le système

Avec des outils keylogging ou de sniffing des protocoles réseaux.

Attaquer le fichier de mot de passe

Utilisation de l'attaque par dictionnaire ou par force brute.

Comment s'authentifier ?

Le mot de passe

C'est l'empreinte, ou hash, du mot de passe qui est stockée dans l'ordinateur.

Le hashage est une fonction mathématique qui, à partir d'un texte d'origine, calcule une empreinte unique, de taille fixée et de manière irréversible.

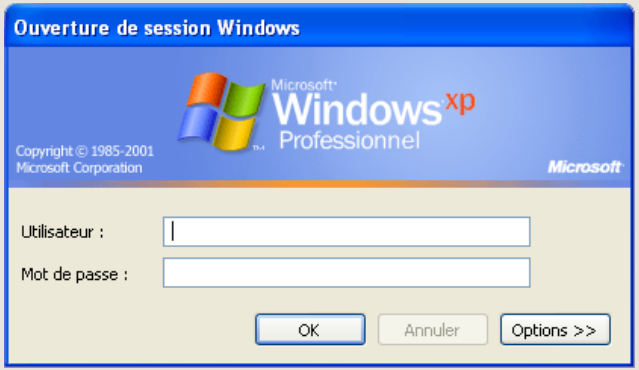
- TOTO $\Longrightarrow$ `04c1d7cd203ef496f200ee5a096b5764`
- ToTo $\Longrightarrow$ `3cca12013a4f82de305ba73b01a84509`
- Toto $\Longrightarrow$ `998db284485ec6c227f8dc34086128e1`
- toto $\Longrightarrow$ `f71dbe52628a3f83a77ab494817525c6`
- Le ciel est rouge demain il fera beau $\Longrightarrow$ `caf7a1f03adc02afe3ef1dd51bd3e8b1`

Comment s'authentifier ?

Le mot de passe

Attaque par dictionnaire

1. pour chaque mot d'un dictionnaire
2. calcul du hash
3. comparaison avec celui du système




```
151349 michaella
151350 michaelmas
151351 michaelmastide
151352 michail
151353 michal
151354 michale
151355 miche
151356 micheal
151357 micheil
151358 michel
151359 michelangelesque
151360 michelangelism
151361 michelangelo
151362 michele
151363 michelia
151364 michelin
151365 michelina
151366 micheline
151367 michell
151368 michelle
151369 michelson
151370 micher
```

Comment s'authentifier ?

Le mot de passe

Attaque par force brute

- parcours exhaustif de l'espace des mots de passe
- plus le mot de passe est long plus il est difficile à trouver
- plus l'espace des mots de passe est grand plus le temps nécessaire à la parcourir sera grand

	Lettres minuscules (26)	Caractères alphanumériques (62)	Caractères ASCII (256)
4 caractères	$26^4 = 460000$	$62^4 = 1,5 \cdot 10^7$	$256^4 = 4,3 \cdot 10^9$
5 caractères	$26^5 = 1,2 \cdot 10^7$	$62^5 = 9,2 \cdot 10^8$	$256^5 = 1,1 \cdot 10^{12}$
6 caractères	$26^6 = 3,1 \cdot 10^8$	$62^6 = 5,7 \cdot 10^{10}$	$256^6 = 2,8 \cdot 10^{14}$
7 caractères	$26^7 = 8,0 \cdot 10^9$	$62^7 = 3,5 \cdot 10^{12}$	$256^7 = 7,2 \cdot 10^{16}$
8 caractères	$26^8 = 2,1 \cdot 10^{11}$	$62^8 = 2,2 \cdot 10^{14}$	$256^8 = 1,8 \cdot 10^{19}$

Comment s'authentifier ?

Le mot de passe

Caractéristiques d'un bon mot de passe

- est secret
- contient plus de 9 caractères
- est changé régulièrement
- est dédié à une application
- caractères choisis parmi : $[A \cdots Z]$, $[a \cdots z]$, $[0 \cdots 9]$, [@&$#§+*=]

Comment s'authentifier ?

Le mot de passe

Construire un bon mot de passe

Dictionnaire	→	bateau
Mnémonique	→	Mon code est très Secret
Phrase	→	Je prefere les phrases
PIN	→	1234
Challenge	→	Comment s'appelait votre premier animal de compagnie ?

Comment s'authentifier ?

Le mot de passe

Construire un bon mot de passe

Exemple 1

- Tant va la cruche à l'eau qu'à la fin elle se casse
- Tvlcàlqlfesc

Exemple 2

- J'ai trois enfants, un chat, un oiseau et trois poissons nommés riri, fifi et loulou !
- G3e1c1o&3pnrf&l!

Comment s'authentifier ?

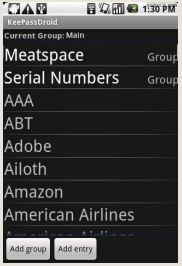
Le mot de passe

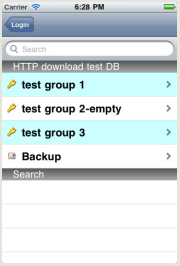
Problème

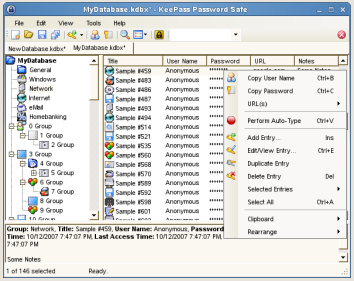
- Un mot de passe par application ou service
- beaucoup de mots de passe !

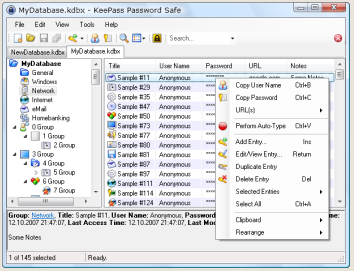
Solution

- Le gestionnaire de mot de passe
- KeePass `http://keepass.info/`









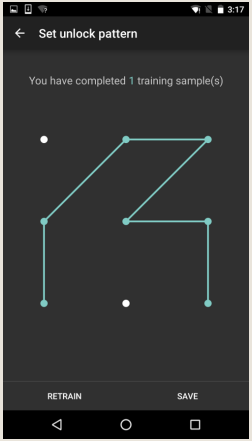
2. Comment s'authentifier ?

Comment s'authentifier ?

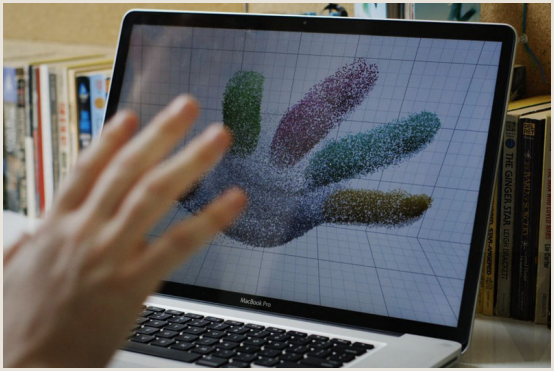
Autres moyens d'authentification

Authentification basée sur une action

Gestes 2D



Gestes 3D



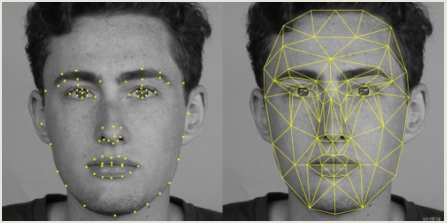
Comment s'authentifier ?

Autres moyens d'authentification

Authentification basée sur la biométrie

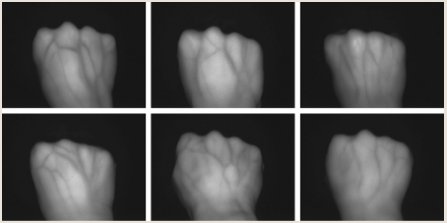
Géométrie de la main

Reconnaissance faciale



Scan rétinien

Triangulation des veines de la main

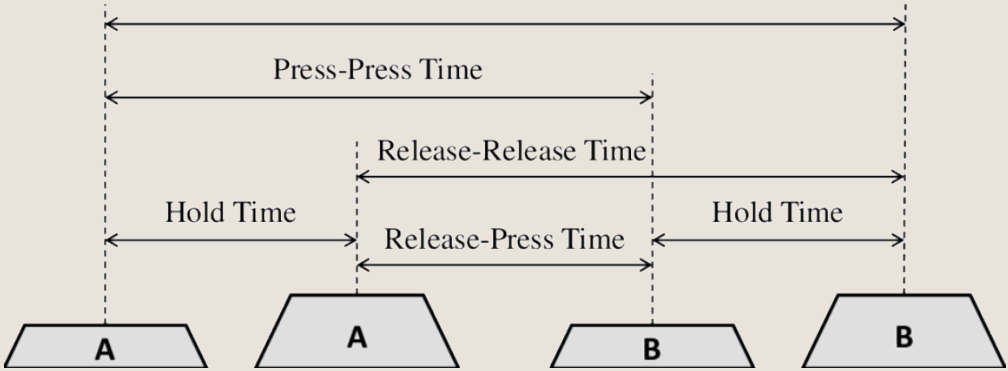


Comment s'authentifier ?

Autres moyens d'authentification

Authentification basée sur la biométrie

Dynamiques de la frappe clavier



Comment s'authentifier ?

Autres moyens d'authentification

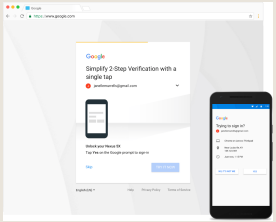
Authentification basée sur du matériel

Token OTP

Token multi-protocole

Carte à puce

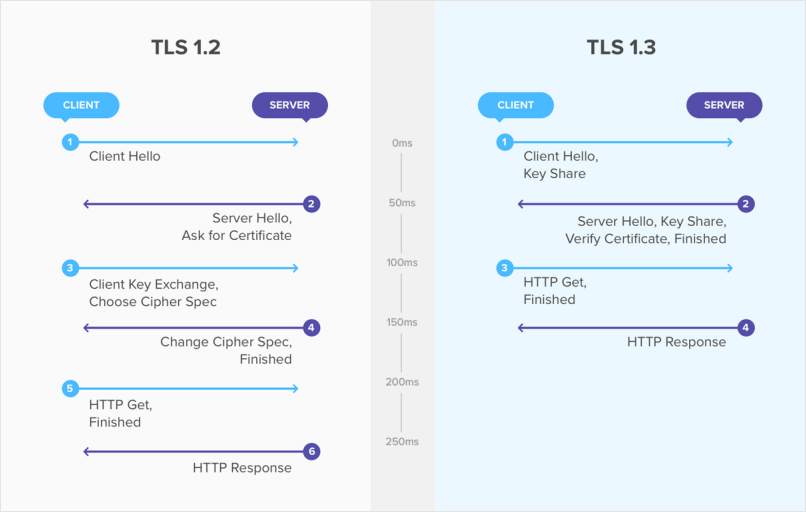
Utilisation du smartphone



Comment s'authentifier ?

Autres moyens d'authentification

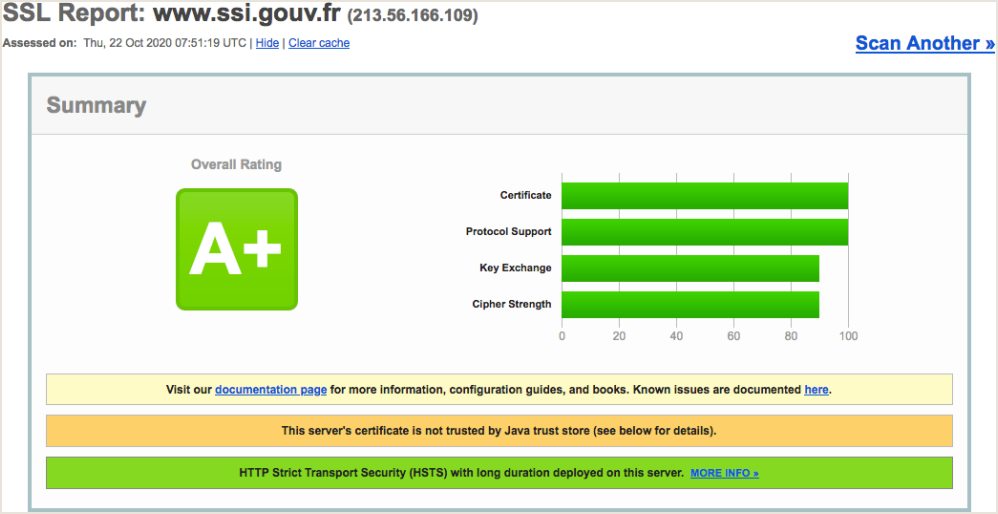
Authentification protocolaire



Comment s'authentifier ?

Autres moyens d'authentification

Authentification protocolaire

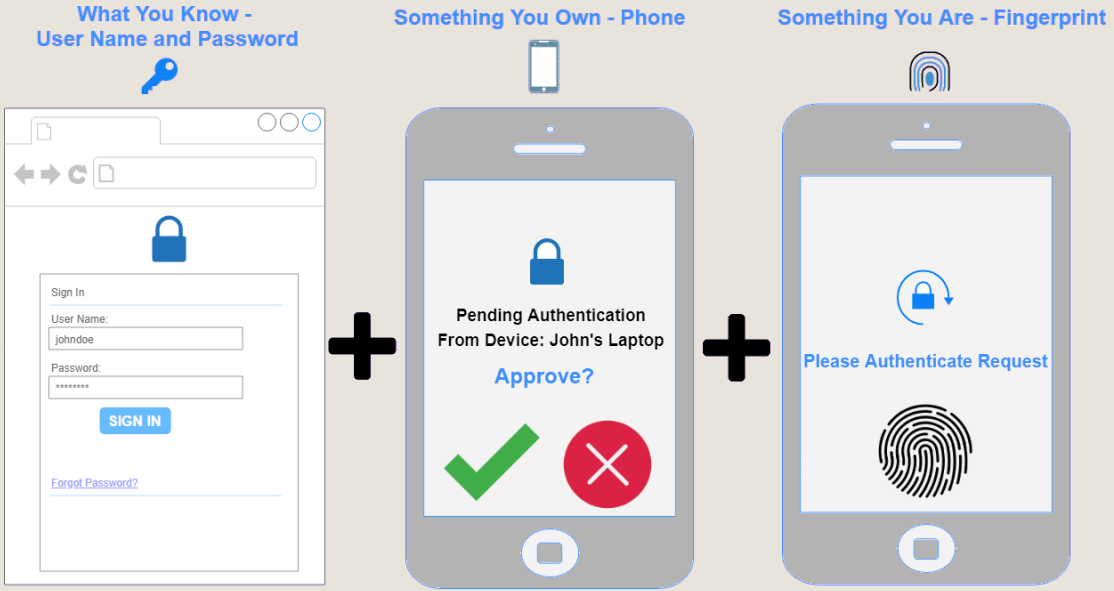


https://www.ssllabs.com/ssltest/

2. Comment s'authentifier ?

Comment s'authentifier ?

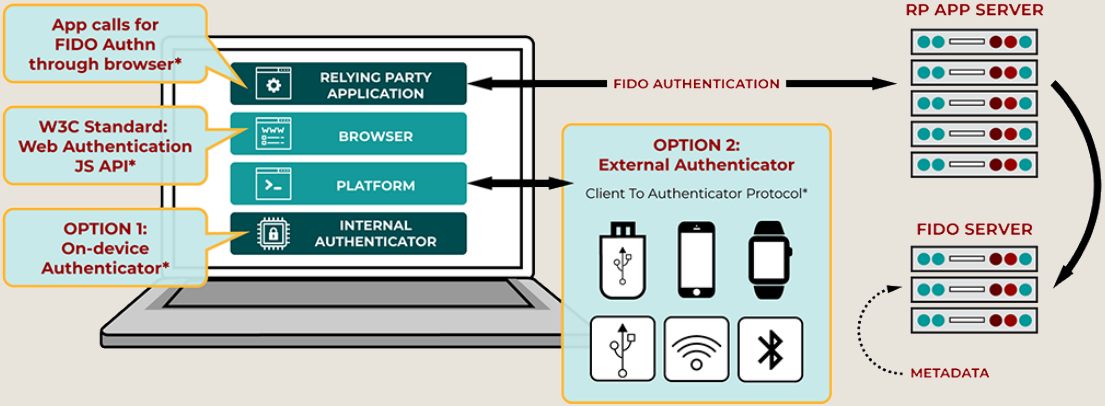
Authentification multi-facteurs



Comment s'authentifier ?

Authentification multi-facteurs

FIDO 2 : authentification sans mot de passe

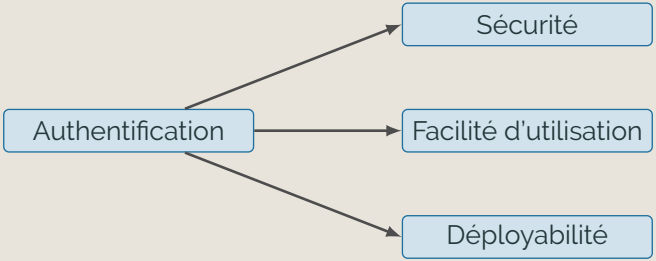


2. Comment s'authentifier ?

Comment s'authentifier ?

Comment choisir ?

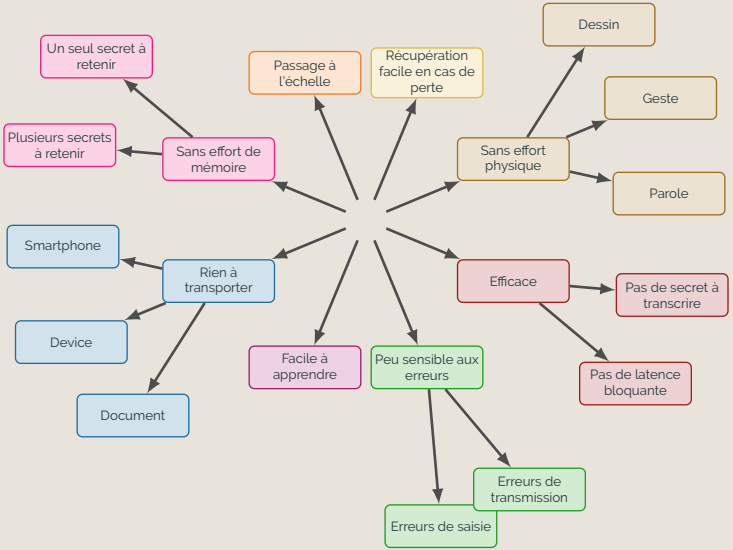
Méthode pour choisir une méthode d'authentification ?



Comment s'authentifier ?

Comment choisir ?

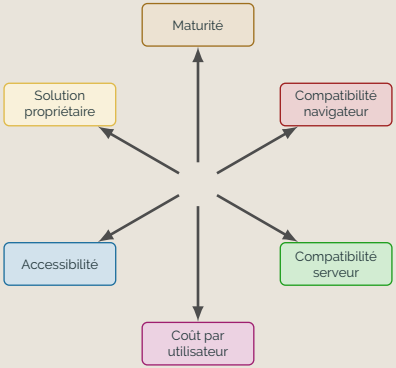
Facilité d'utilisation



Comment s'authentifier ?

Comment choisir ?

Déploiabilité



Comment s'authentifier ?

Comment choisir ?

Sécurité