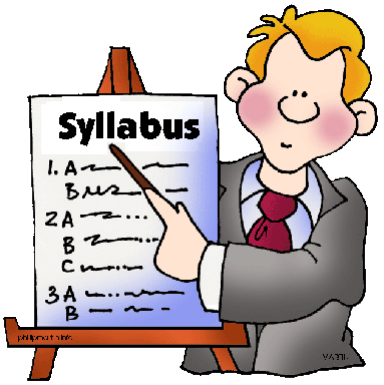
En 2022 60 % des grandes entreprises et 90 % des PME n'utiliseront plus de mots de passe pour la moitié de leurs applications informatiques (Gartner)

Sommaire



La catastrophe sécuritaire des mots de passe

- Les utilisateurs font vraiment n'importe quoi (statistiques DataProt)
- 53% font confiance à leur mémoire pour gérer leurs mots de passe (Ponemon Institute).
- 26 % les inscrivent dans un tableur et 26 % en postits sur l'écran (Ponemon)
- 37 % reconnaissent faire appel au TI une fois par mois pour regénérer un mot de passe oublié pour l'un de leurs sites…(Entrepreneur)
- 51% se servent des mêmes mots de passe pour leurs applications professionnelles et personnelles (First Contact)
- 57% des usagers qui ont déjà été attaqués continuent de se server des mêmes "credentials" (First Contact) : "on ne change pas une équipe qui perd"…
- 71% des comptes sont protégés par des mots de passe utilizes sur plusieurs sites (Lawless Research, TeleSign)
- 29% ont plus de comptes protégés dont ils ont perdu la trace (Digital Guardian)
- 90% craignent que leurs comptes soient hackés (Guardian)
- Le mot de passe "123456" est utilisé dans 23 millions de comptes (First Contact).
- 33% des victimes de compromission de comptes par les mots de passe, ont cessé toute activité avec les services fautifs (Lawless Research, TeleSign)

Le comportement contestable des usagers

- Attaques par dictionnaires
  - Si l'on connait le login, il est possible d'en déduire le mot de passe correspondant, si celui-ci a un "sens" (une chance sur deux)
  - Des dictionnaires sont disponibles qui effectuent la relation…en différentes langues
- Selon Imperva (éditeur spécialisé en détection d'intrusion), 20 % des utilisateurs ont recours à un mot de passe qui figure dans un dictionnaire des 5.000 mots les plus populaires
- NIST : National Institute of Standards and Technology, un employé américain moyen doit se souvenir de 23 identités distinctes. Ils utilisent leur adresse courriel en tant que login, le même mot de passe sur l'ensemble des applications (61 % sont dans ce cas), des mots de passe structurellement trop simples qu'ils copient dans un tableur, dans un agenda papier, là où on est sûr que tout le monde pourra les trouver…
- D'autres sont plus pessimistes (Dashlane) : 200 mots de passe à se souvenir, 300 en 2023

Le « buddy punching » est cette mauvaise habitude qui consiste à s'indiquer les mots de passe…pour des raisons de commodité

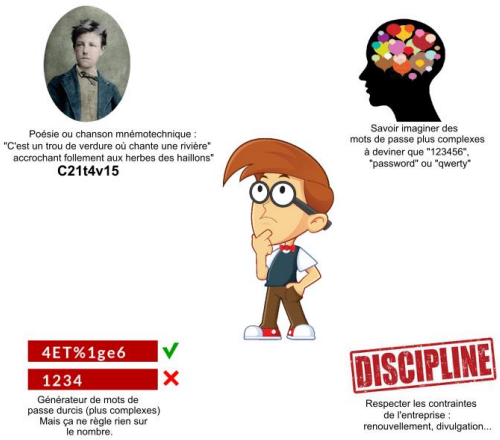
Rang	Mot de passe
1	123456
2	password
3	12345678
4	qwerty
5	abc123
6	123456789
7	111111
8	1234567
9	iloveyou
10	adobe123
11	123123
12	sunshine
13	1234567890
14	letmein
15	photoshop
16	1234
17	monkey
18	shadow
19	sunshine
20	12345
21	password1
22	princess
23	azerty
24	trustno1
25	000000

Le palmarès des mots de passe les plus employés (SplashData)

Les motivations

- Aucune technique d'authentification n'est sûre à 100 %, il faut impérativement trouver autre chose, un autre formalisme
- Un mot de passe, c'est un "morceau" de l'entreprise que l'on confie à un usager : il doit en avoir conscience
- Progression de la biométrie, il faut en profiter
- SSO et WebSSO : il y a toujours un mot de passe, mais il n'y en a qu'un
- Les protections sont souvent dérisoires (John The Ripper…)
- La plupart des mots de passe sont faibles et réutilisés
- 80 % des fuites de données importantes sont dues aux mots de passe faibles et compromis (Verizon, 2019)
- L'authentification forte se justifie
  - Le coût associé à la perte de données confidentielles, peut aller jusqu'à 30 % de celui des centres d'appels
  - Un prestataire peut être jugé responsable des conséquences d'une attaque : pertes financières et dégradation de l'image
  - L'authentification forte est largement fondée sur les technologies les plus innovantes, de sorte qu'avec le temps elles seront de moins en moins coûteuses à mettre en place et de plus en plus efficaces

Ce que pourrait être un mot de passe



Les critères de choix des mots de passe

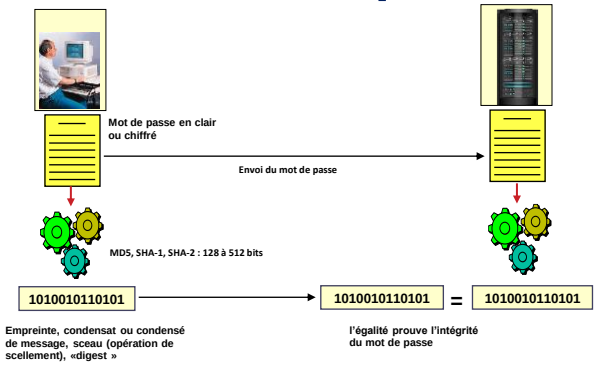
- Une longueur minimale obligatoire prédéfinie, 8 caractères
- Etre composé d'un mélange de caractères numériques, minuscules, majuscules et spéciaux
- Ne doivent pas se trouver dans un dictionnaire
- Impossibilité de réutiliser les n derniers mots de passe (n > 5)
- Nombre limité de tentatives possibles avant verrouillage de compte : au maximum 3, avec augmentation des intervalles de temps de saisie
- Prévoir des tests de fragilité des mots de passe : nombreuses solutions, gratuites ou non.

Les mots de passe forts

- Un mot de passe est dit renforcé lorsqu'il est difficile à deviner (merci les prestataires...)
- Il doit comporter au moins 6 caractères, une combinaison de lettres, chiffres et symboles : @, €, $, #, %... (308 millions de combinaisons), 8 c'est mieux
- Il est sensible à la casse
- Selon la Texas A&M University's Research Foundation
- Avec 8 caractères et sensibilité à la casse : 53.000 milliards de combinaisons
- Mais :
  - Il est impossible de se souvenir des mots de passe complexes. La plupart des utilisateurs choisissent des choses simples dont ils se souviennent aisément.
  - Le nom d'un animal familier, une date de naissance, une adresse de domicile, un nom de ville, le nom d'un enseignant ou d'un sportif.
  - Souvent on utilise le même mot de passe fort pour plusieurs ressources, ce qui multiplie les risques.
- Donc, ça ne sert à rien.
- Sauf…si l'on transforme le mot de passe (hash, chiffrement)

On peut aussi indiquer le code secret de notre carte bancaire…

Hashage pour garantir l'intégrité d'un mot de passe



- Avantage : seul le hash est stocké dans la base de données et il est impossible de revenir au mot de passe en clair
- Il faut veiller à ce que TOUS les services pratiquent ce mécanisme de hashage, sinon en cas de vol d'un mot de passe en clair mettrait à mal l'ensemble du système
- Tous les langages disposent d'une API de hashage
- Le temps de calcul du hash est négligeable

MD-5, SHA-1, SHA-2

c'est un trou de verdure où chante une rivière, accrochant follement aux herbes des haillons
`14AA5379629ABE883905DC25C7FFAB8D2AB0140A`
soiscourageuxmaisprudentenvolgardeintelligencehabilitédiscipline
`DB25D884ED3F2BB5B1309FD0DC3ABC4C9B34EC84`

Ne pas confondre avec le chiffrement

Les recommandations que l'on n'applique pas

- Utiliser des mots de passe différents pour s'authentifier auprès de systèmes distincts (pas évident dans la pratique).
- Choisir un mot de passe qui n'est pas lié à notre identité (mot de passe composé d'un nom de compagnie, d'une date de naissance, etc.).
  - Les hackers se focalisent en premier lieu sur ce qui peut caractériser leur cible
- Ne jamais demander à un tiers de créer un mot de passe pour nous.
- Modifier systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en comportent.
- Renouveler les mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
- Ne pas stocker les mots de passe dans un fichier sur un poste exposé au risque (exemple : en ligne sur internet), encore moins sur un document papier facilement accessible.
  - Le minimum est alors de chiffrer le contenu du fichier
- Ne pas s'envoyer à nous-mêmes nos mots de passe sur notre messagerie personnelle.
  - La messagerie est l'une des applications les plus faciles à pénétrer du fait de la faiblesse conceptuelle du protocole SMTP
- Configurer les logiciels, y compris le navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.
  - A l'usage, cette règle s'avère contre productive

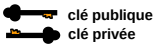
Il faut distiller un minimum de paranoïa dans le comportements des usagers et leur faire comprendre que « cela n'arrive pas qu'aux autres »…

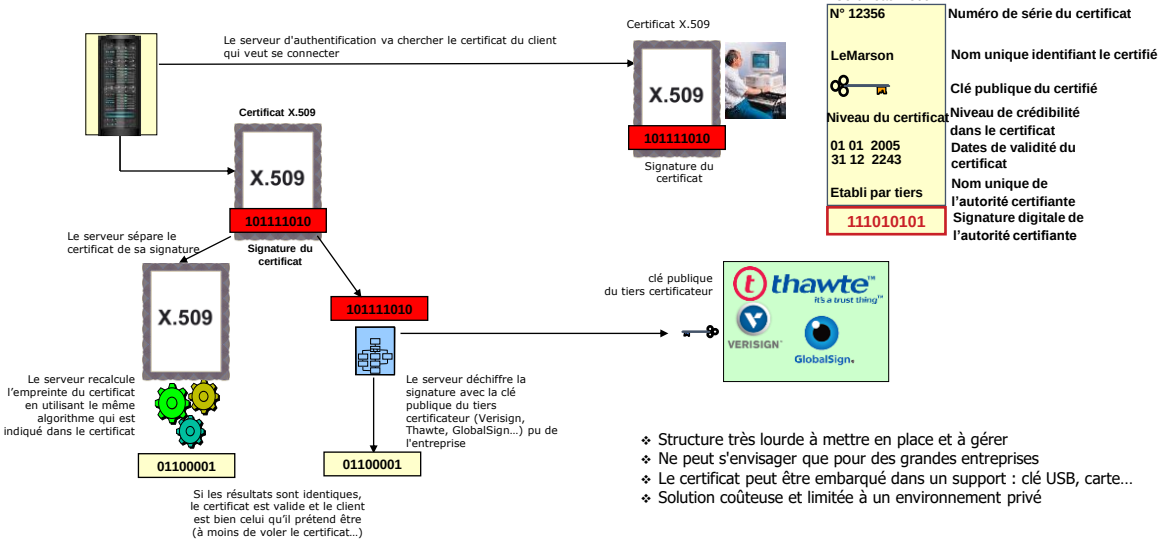
L'identification sans mot de passe

- Combinaison des données multi-facteurs (MFA)
  - Données biométriques
  - Contrôle de l'adresse courriel
  - OTP : On-Time Password (le token remplace le mot de passe)
  - Certificats
  - Géolocalisation
  - Clés publiques et privées
  - Comportements
- L'objectif est d'associer plusieurs éléments d'authentification, logiques et physiques, pour conforter la qualité de la reconnaissance
  - Avec ou sans mot de passe

Les techniques biométriques en support

PKI et la certification X.509





Certificat X509

N° 12356	Numéro de série du certificat
LeMarson	Nom unique identifiant le certifié
	Clé publique du certifié
Niveau du certificat	Niveau de crédibilité dans le certificat
01 01 2005 31 12 2243	Dates de validité du certificat
Etabli par tiers	Nom unique de l'autorité certifiante
111010101	Signature digitale de l'autorité certifiante

- Structure très lourde à mettre en place et à gérer
- Ne peut s'envisager que pour des grandes entreprises
- Le certificat peut être embarqué dans un support : clé USB, carte…
- Solution coûteuse et limitée à un environnement privé

Un début : le mode MFA

- Une méthode d'authentification forte exploite au moins deux techniques d'identification
- Elle permet de contrôler efficacement les accès et constitue un bon moyen pour se protéger contre la non répudiation : « non, ce n'est pas moi… »
- Il faut veiller à ne pas perturber gravement l'usager
- L'authentification fondée sur un seul facteur est traditionnellement effectuée de trois manières différentes :
  - Sur un élément que l'on possède : clés USB, cartes token, téléphone, messagerie, identifiant FIDO…
    - Avantage : plus difficile à voler à distance
    - Inconvénient : une alternative est nécessaire s'il se casse ou se perd
  - Sur un élément que l'on connaît : mots de passe, PIN, nom d'un animal favori (KBA : Knowledge Based Authentication)…
    - Avantage : facile à installer
    - Inconvénient : facile à oublier ou à voler
  - Sur un élément qui nous caractérise : empreintes digitales, empreinte vocale, iris de l'œil, forme du visage, empreinte vocale, EEG (Encéphalogramme)…
    - Avantage : impossible à oublier
    - Inconvénient : dépendant d'un appareil associé

Méthode	Exemples	Caractéristiques
Ce que vous savez	User ID PIN Mots de passe	Partagés Facile à deviner Souvent perdu
Ce que vous possédez	Clés USB Cartes Badges	Partagés Peuvent être dupliqués Perdus ou volés
Ce que vous savez et ce que vous possédez	ATM + PIN	Partagés PIN est peu sûr (écrit dans des endroits visibles, faciles à récupérer et à oublier)
Quelque chose d'unique sur l'utilisateur	Empreinte digitale, visage, empreinte vocale, iris	Impossible à partager Impossibilité de non répudiation Ne peut pas être volé ou perdu Imitation difficile

L'usage des clés de sécurité

- Une clé de sécurité est un dispositif externe qui se connecte au terminal
- La clé est active, car elle est peut générer les informations supplémentaires de sécurité : clés privées ou publiques, données biométriques, certificats… C'est un mini-ordinateur
- Protégée par … mot de passe, mécanisme biométrique…
- La clé se présente sous le format USB traditionnel, sauf qu'au lieu de stocker des fichiers, elle contient une puce sécurisée qui renferme un code chiffré connu uniquement du fabricant
- Plusieurs usages
  - Authentification simple : c'est l'information confidentielle stockée qui sert de sésame (procédure de déclaration préalable)
  - Déclaration à un service : on se connecte au service, puis on insère la clé et on appuie sur un petit bouton (par exemple) : dès lors la clé est associée au service
  - Authentification double : la clé génère une biclé, publique et privée, peut stocker jusqu'à 1024 "credentials" et participer au protocole FIDO2
- Inconvénients
  - Pertes et vols
  - Compatibilité pas toujours garantie des browsers et des applications

L'authentification MFA dans Windows 10 et OKTA

Microsoft Windows 10 Hello (mise à jour 2004)

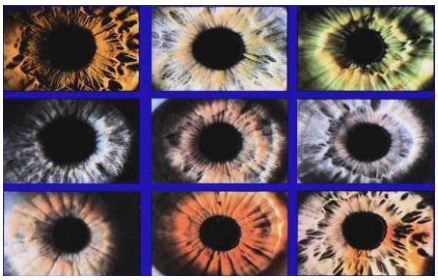
- Nouvelles dispositions de reconnaissance multi-facteurs, nécessite pour certaines un mot de passe à la connexion (MFA)
- Reconnaissance du visage
- Empreinte digitale PIN
- Clé de sécurité (USB)
- Mot de passe

La solution OKTA FastPass

- Service de connexion sans mot de passe sur les appareils, applications et systèmes d'exploitation tels que iOS, iPadOS, MacOS, Android et Windows.
- Pour fonctionner sans mot de passe, l'utilisateur doit se connecter une première fois à ses outils et applications de travail pour que le service Verify ajoute le terminal utilisé dans la base de données des appareils vérifiés de l'entreprise.

MFA avec Windows 10 : plusieurs possibilités dont certaines nécessitent un mot de passe

Le scan de l'iris pour les mobiles



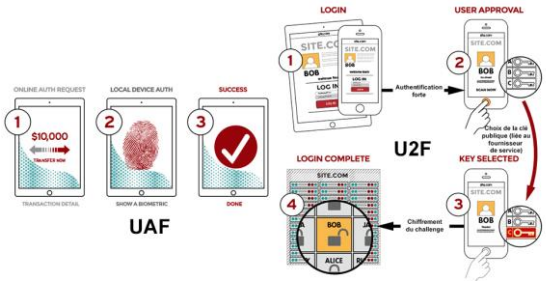
Système de scan de l'iris de l'oeil

- Le mobile est doté dans la face avant d'un émetteur LED qui génère un faisceau lumineux et une petite caméra à infrarouges.
- Après avoir enregistré l'image de son iris, l'utilisateur qui demande à se servir du mobile, l'allume, ce qui met en route une petite application d'attente, avec deux cercles que l'usager est invité à fixer, pendant que le LED éclaire ses yeux par un faisceau de lumière approprié.
- La caméra infrarouge enregistre l'image de son iris éclairé par les LED et le logiciel de reconnaissance le compare à celui ou ceux qui ont été enregistrés dans le smartphone. Si la correspondance est établie, le smartphone se « débloque ».
- Le processus ne demande pas plus de 150 ms et le taux d'erreur est estimé à 1 pour 10 millions…d'autres fabricants estiment ce taux à 1 pour 10 milliards
- Le système fonctionne même si les yeux ne sont pas bien alignés, si l'utilisateur bouge, si la pupille est dilatée et si les conditions ambiantes ne sont pas bonnes, avec beaucoup de luminosité.

Nombreuses solutions MFA et "passwordless"

Les nouveaux venus de l'authentification mobile

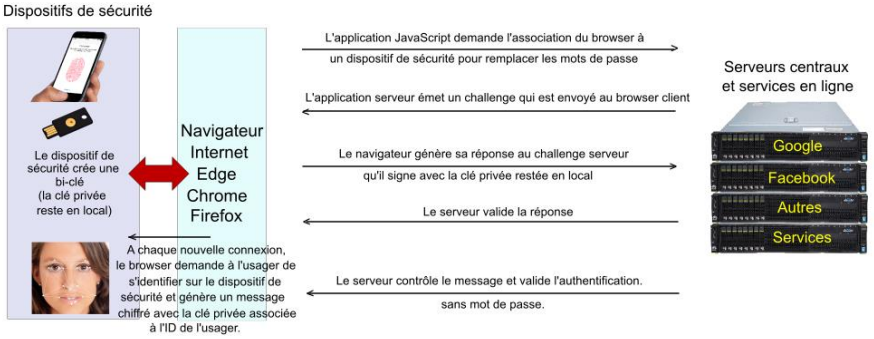
- FIDO et Mobile Connect, qui enrobent les mots de passe dans des mécanismes plus sûrs d'authentification forte
- FIDO (Fast IDentity Online) : ce n'est pas un serveur distant qui valide l'identité de l'usager, mais son mobile.
- Deux méthodes : UAF (Universal Authentication Framework) et U2F (Universal Second Factor).
  - UAF remplace le mot de passe par un système d'authentification forte alors qu'U2F introduit un deuxième facteur d'authentification.
  - L'utilisateur UAF choisit un mécanisme d'authentification sur son mobile : « swiping » (balayage) de doigt sur l'écran, une reconnaissance de visage par caméra, une séquence sonore à prononcer dans le micro, la saisie d'un PIN, etc, qui sera déclaré par le propriétaire du mobile auprès d'un service en ligne. On peut cumuler les processus (Google, eBay).



- La FIDO Alliance est une association industrielle ouverte lancée en février 2013 dont la mission est de développer et de promouvoir des normes d'authentification qui contribuent à réduire la dépendance à l'égard des mots de passe (Wikipedia)
- Un "board" de 42 membres
  - Amazon, American Express, Apple, ARM, Avast, Bank of America, Facebook, Google, Infineon, Intel, Lenovo, Mastercard, Microsoft, NTT Docomo, Paypal, Qualcomm, RSA, Samsung, Thales, Visa, VMWare, Wells Fargo, Yahoo, Rubico…
  - Très nombreux sponsors

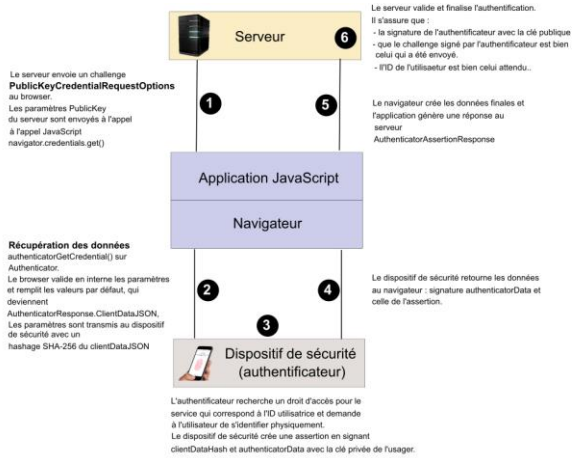
FIDO 2 (WebAuthn)

- Implémentation des standards WebAuthn et CTAP
- WebAuthn : protocole d'authentification du W3C depuis un browser
- CTAP ("Client To Authenticator Protocol") est la specification qui décrit le lien entre le navigateur et le système d'exploitation et le dispositive de sécurité additionnel : clé, carte…



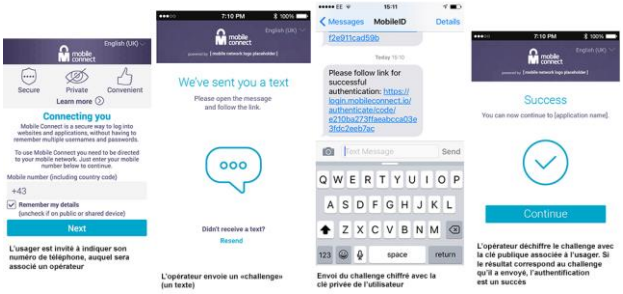
L'API FIDO2

- Pour ceux que le développement intéresse, FIDO2 est fondé sur l'API WebAuthn
- Cette API étend les méthodes JavaScript `navigator.credentials.create()` et `navigator.credential.get()` de Credential Management, de manière à lui faire accepter un paramètre publicKey
  - create() est utilisé pour associer des moyens d'authentification à un compte.
  - Get() est utilisé pour la procédure d'authentification proprement dite.
  - Pour vérifier la compatibilité de votre navigateur, le script JavaScript doit s'assurer que l'interface window.PublicKeyCredential est bien définie.



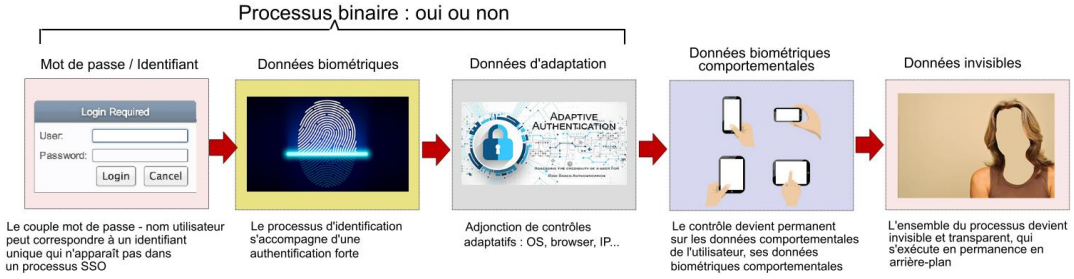
D'autres solutions plus confidentielles

- Mobile Connect est basé sur OpenID Connect
  - C'est l'opérateur qui va assurer l'authentification, en contrôlant le PIN de l'usager
    - Le client clique sur l'onglet « Mobile Connect » de sa page d'accueil
    - Il saisit son numéro de téléphone et l'opérateur auquel ce numéro est associé lui demande de saisir un texte secret, qui peut aussi être le PIN du mobile sur 4 ou 6 caractères maintenant.
    - Ce code est chiffré avec la clé privée de l'usager
    - Chez l'opérateur, le code est déchiffré avec sa clé publique

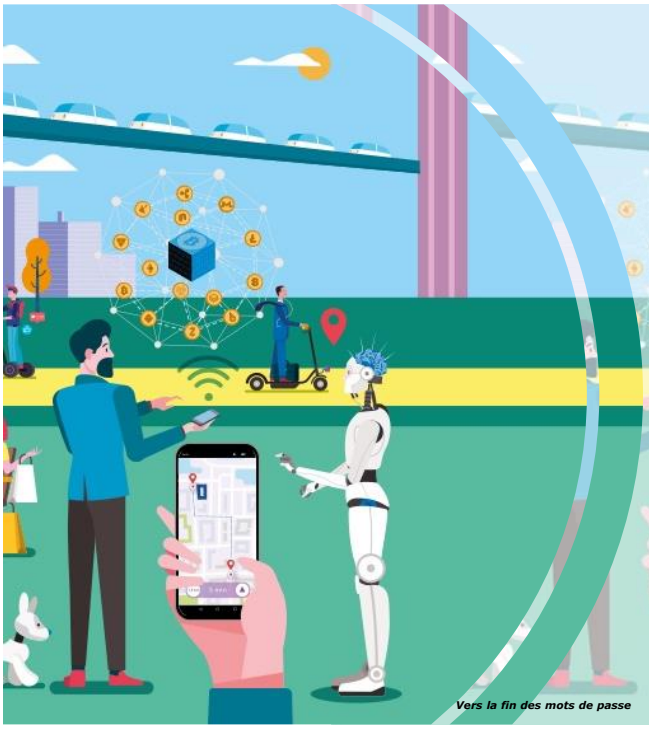


Le cheminement vers l'authentification invisible

L'avenir



L'authentification va devenir invisible, qui sera fondée sur la biométrie comportementale



Vers la fin des mots de passe

4 septembre 2020

Nos prochains rendez-vous

Vendredi 11 septembre	**: IBN et la programmation des réseaux**
Vendredi 18 septembre	**: Le "machine learning", c'est quoi au juste**
Vendredi 25 septembre	**: Les secrets du "deep learning"**
Vendredi 2 octobre	**: Le grave danger que représentent les GAFAM**
Vendredi 9 octobre	**: Au cœur des backbones Internet, comprendre...**
Vendredi 16 octobre	**: Cyberguerre, entre fantasmes et réalités**
Vendredi 23 octobre	**: Les avancées concrètes des villes intelligentes**
Vendredi 30 octobre	**: Les algorithmes de chiffrement, ces inconnus**
Vendredi 6 novembre	**: L'IA et la fin de la démocratie**
Vendredi 13 novembre	**: Les certifications pour remplacer les diplômes**
Vendredi 20 novembre	**: IA et la démocratie**
Vendredi 27 novembre	**: La médecine du futur, les barrières explosent**
Vendredi 4 décembre	**: La transformation digitale, mythe ou réalité**
Vendredi 18 décembre	**: Panorama des architectures globales du TI**
Mercredi 23 décembre	**: Une journée comme les autres en... 2070**