Min2RIEN

Métiers de l'Informatique
Réunis en Réseau
Inter-Etablissement du Nord

SYNETIS

Les mots de passe ne suffisent plus, adoptez l'authentification-forte !

État de l'art, concepts et facteurs

Yann CAM – yann.cam@(synetis|gmail).com

08 Novembre 2018

Présentation de votre interlocuteur

PRO

SYNETIS

IAM / GRC / SecOps / Audit

Yann CAM

- Security Consultant
- Lead auditor
- Pentester

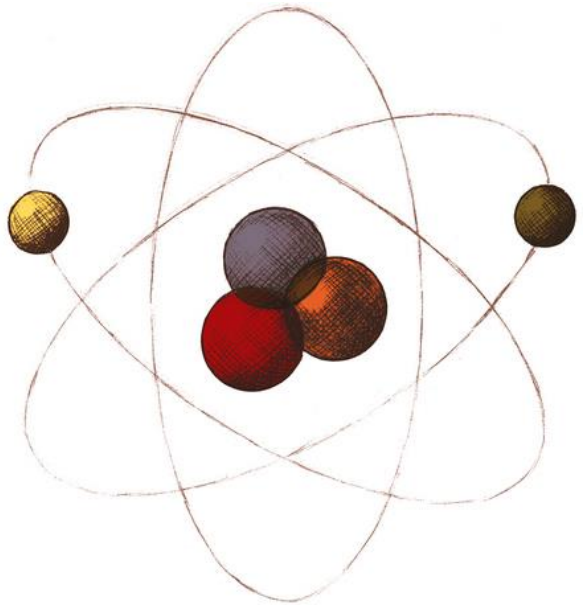
PERSO

Ycam (ASafety.fr)

- Security Researcher
- Bug Hunter
- Contributor
- Blogguer / writer
- Challenger

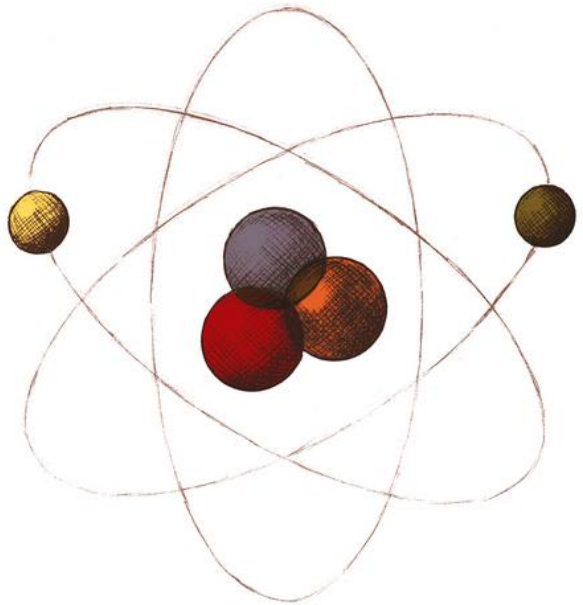
L'authentification forte ?

PLAN



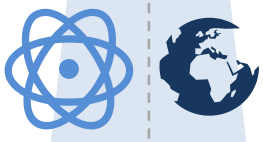
- Bref historique et introduction contextuelle
- Vocabulaire et acronymes
- Pourquoi ajouter des facteurs ?
- Quels sont ces facteurs ?
  - Les hard-tokens physiques
  - Les soft-tokens (smartphones)
  - Les facteurs et critères comportementaux
  - Les facteurs biométriques : apparences physiques et morphologiques
  - Les facteurs biométriques : caractéristiques biologiques
  - Le marquage volontaire…
  - Les facteurs encore plus originaux / atypiques
- Implémentations, solutions, services

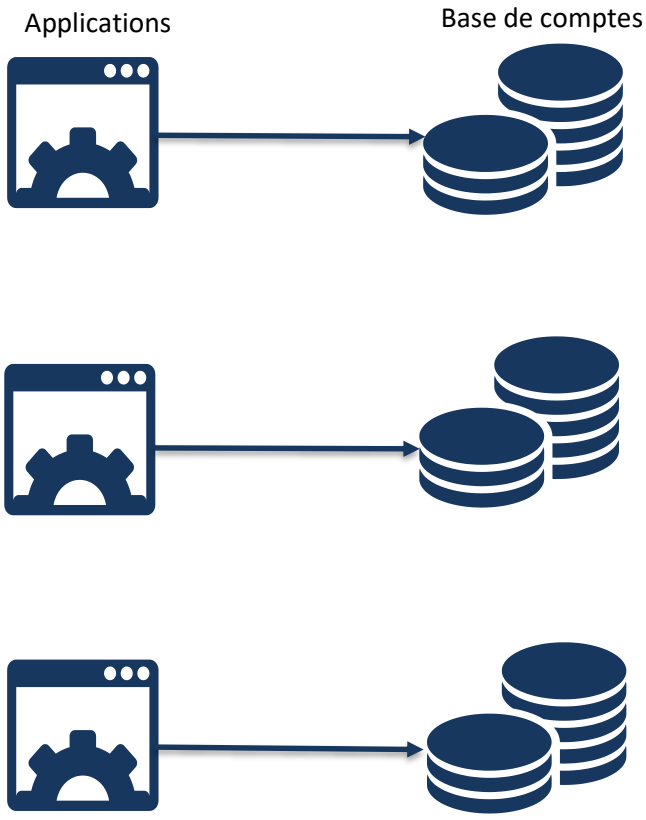
PLAN



- **Bref historique et introduction contextuelle**
- Vocabulaire et acronymes
- Pourquoi ajouter des facteurs ?
- Quels sont ces facteurs ?
  - Les hard-tokens physiques
  - Les soft-tokens (smartphones)
  - Les facteurs et critères comportementaux
  - Les facteurs biométriques : apparences physiques et morphologiques
  - Les facteurs biométriques : caractéristiques biologiques
  - Le marquage volontaire…
  - Les facteurs encore plus originaux / atypiques
- Implémentations, solutions, services

Bref historique et introduction contextuelle

Gestion	Applications		Populations	Devices
Gestion locale des comptes		1970	 Salariés	 Station
Gestion centralisée des identités et de leurs comptes		Internet 1990 	 Salariés et prestataires internes	 Poste de travail et clients lourds
Contrôle d'accès centralisé		Mobilité et ouverture 2005 réseau 	 Salariés, Prestataires internes et **externes**	 Poste de travail et clients légers
Gestion centralisée des habilitations		2008	 Salariés, Prestataires, Fournisseurs **Clients**, Partenaires	
Recertification et audits		 Réglementation  Attaques		
		2018		



Une gestion des comptes par application

- Est devenue source de confusion pour l'utilisateur qui perd ou oublie son mot de passe
- A engendré un besoin de simplification de la gestion des comptes et de leurs accès.
- L'administrateur doit gérer de nombreux référentiels utilisateurs (traitements manuels et répétés)

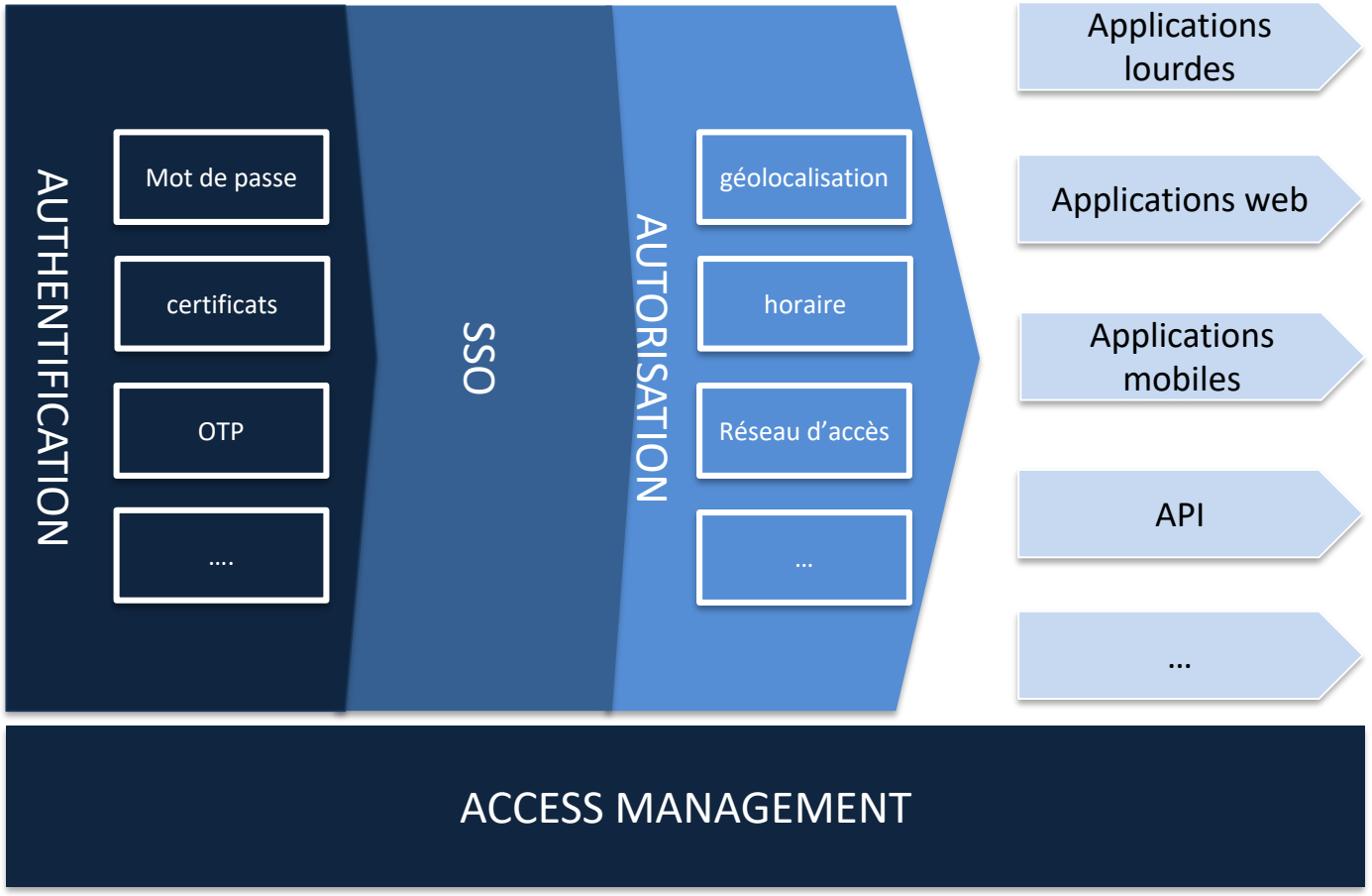
Problèmes rencontrés

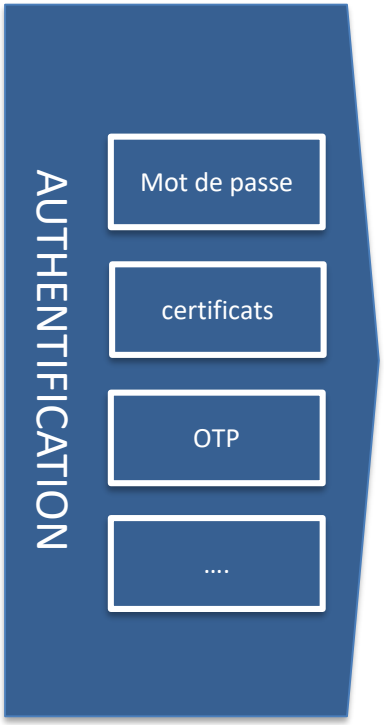
- Niveau de sécurité faible (prolifération de mot de passes)
- Perte de productivité
- Charge importante d'administration
- Manque de traçabilité
- Difficulté d'audit

Enjeux et objectifs

- Vision globale de la gestion des identités et des droits d'accès
- Couverture des exigences fonctionnelles et métiers
- Prise en compte de tout type de population

Bref historique et introduction contextuelle





L'authentification est un mécanisme permettant d'obtenir la preuve de de l'identité de l'utilisateur.

Pour s'authentifier, un utilisateur fournit en général au moins 2 éléments :

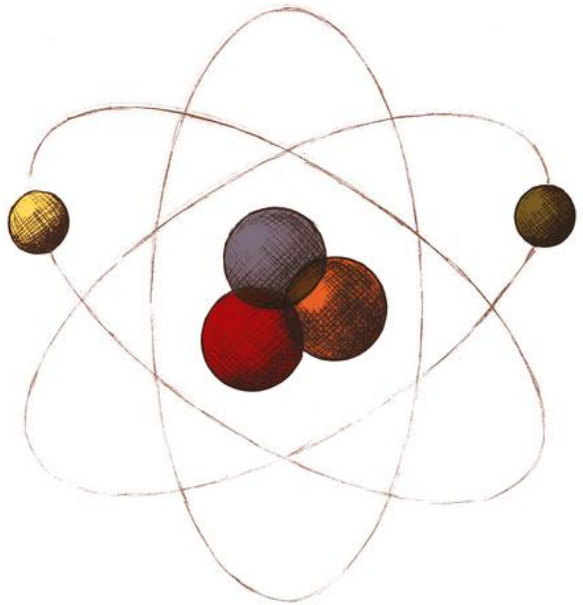
- Son identifiant qui permet son identification
- Un ou plusieurs éléments permettant d'assurer l'authentification elle-même.

Afin d'accroître le niveau de sécurité d'une authentification peuvent être employés suivant les besoins et la criticité :

Des **critères d'authentification** :

Des **facteurs d'authentification** :

PLAN



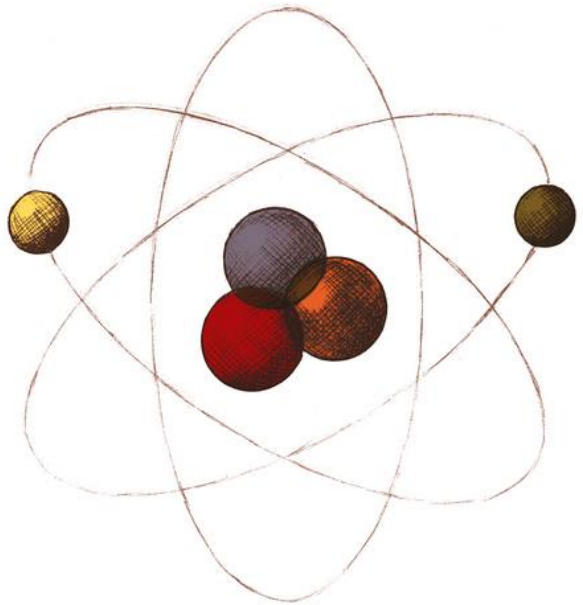
- Bref historique et introduction contextuelle
- **Vocabulaire et acronymes**
- Pourquoi ajouter des facteurs ?
- Quels sont ces facteurs ?
  - Les hard-tokens physiques
  - Les soft-tokens (smartphones)
  - Les facteurs et critères comportementaux
  - Les facteurs biométriques : apparences physiques et morphologiques
  - Les facteurs biométriques : caractéristiques biologiques
  - Le marquage volontaire…
  - Les facteurs encore plus originaux / atypiques
- Implémentations, solutions, services

Clarifions le vocabulaire et les acronymes :

- **Identification** : Indiquer une identité (étape initiale), tel un login ou une adresse email
- **Authentification / authentication** : prouver cette identité (avec un secret ou une donnée personnelle biométrique par exemple)
  - **1FA** : 1 Factor Authentication (généralement un mot de passe)
- **Authentification-forte / Strong-authentication** : renforcement des mécanismes d'authentification avec de nouveaux critères / facteurs
  - **2FA** : 2 Factor Authentication
  - **3FA** : 3 Factor Authentication
  - …
  - **MFA** : Multi-Factors Authentication – dynamique, personnalisation de la chaîne d'authentification
- **OTP** : One-Time Password, password à usage unique (généralement 6 à 8 chiffres)
- **Authentification adaptative** : ajuster les demandes d'authentification en fonction de critère de criticité ou de contexte de connexion.
- **SSO** : Single Sign-On
- **IdP** : brique d'authentification centralisée (fournisseur d'identités / Identity Provider)

PLAN

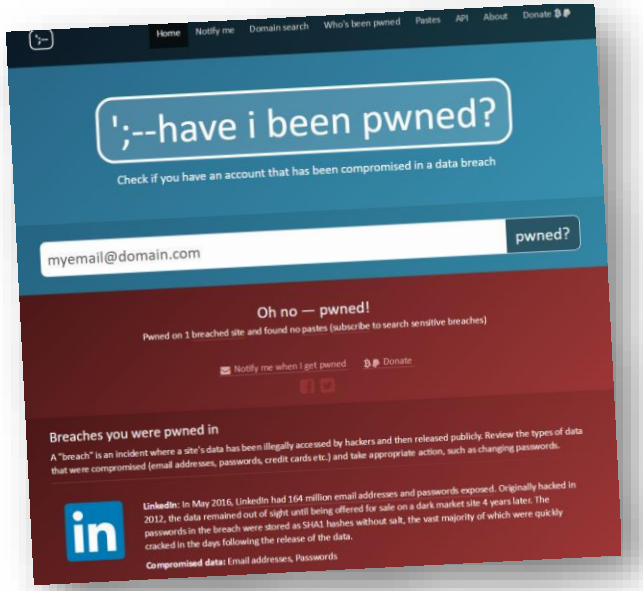
- Bref historique et introduction contextuelle
- Vocabulaire et acronymes
- **Pourquoi ajouter des facteurs ?**
- Quels sont ces facteurs ?
  - Les hard-tokens physiques
  - Les soft-tokens (smartphones)
  - Les facteurs et critères comportementaux
  - Les facteurs biométriques : apparences physiques et morphologiques
  - Les facteurs biométriques : caractéristiques biologiques
  - Le marquage volontaire…
  - Les facteurs encore plus originaux / atypiques
- Implémentations, solutions, services



Pourquoi ajouter des facteurs ?

Le mot de passe n'est plus auto-suffisant !

- Trop simple
- Jamais changé
- Pas unique, même mot de passe pour de nombreux services
- Tout le monde dit de les complexifier, mais comment s'en souvenir ?
  - => Password manager… Oui, mais le master password reste le point de faiblesse ?
- Et les procédures de mots de passe oubliés avec « question / réponse » ? (OSINT / réseaux sociaux)
- Et les leaks massifs médiatisés dans tout ça ?



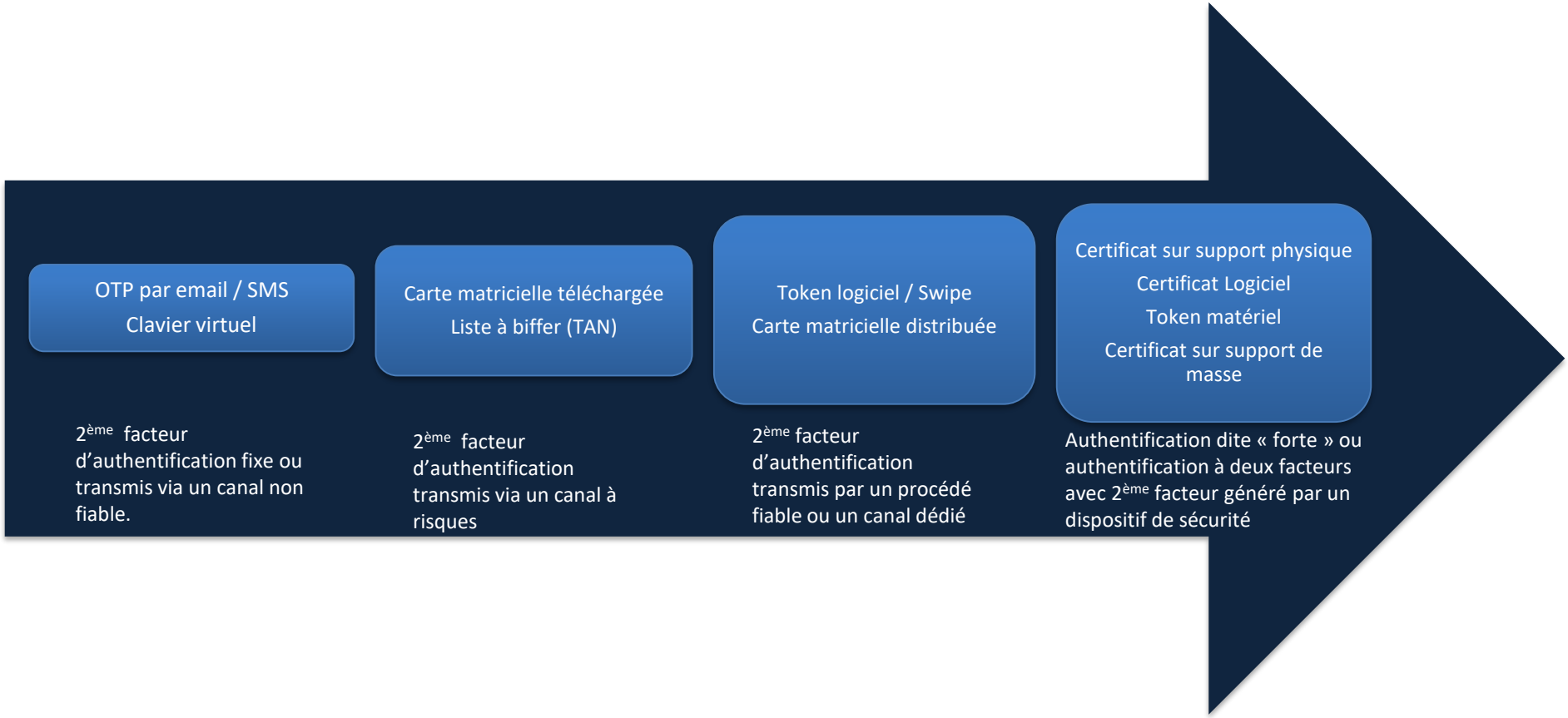
Pourquoi ajouter des facteurs ?

Authentification-forte = au moins 2 facteurs servant à l'authentification

Principaux intérêts :

- Complexifier la tâches des pirates : ils doivent à la fois voler votre mot de passe (facteur n°1) + dérober votre téléphone qui reçoit ou génère des OTP (facteur n°2) + … (MFA)
- S'assurer de la légitimité d'actions critiques sur un SI : les administrateurs peuvent utiliser un second facteur pour accéder à des serveurs en SSH, à des consoles d'administration web, SaaS, etc.
- Rassure quand à l'utilisation de service forçant l'utilisation de mots de passe « simple ».
- Accompagne voire remplace petit à petit les mots de passe…

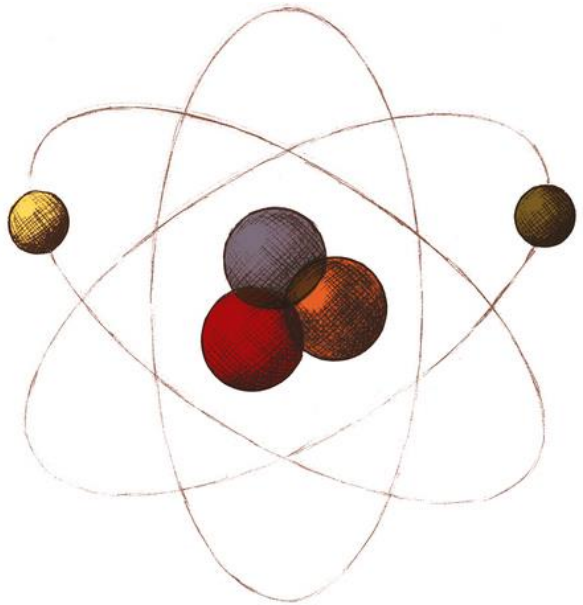
Pourquoi ajouter des facteurs ?



Niveau de sécurité plus faible

Niveau de sécurité plus élevé

PLAN



- Bref historique et introduction contextuelle
- Vocabulaire et acronymes
- Pourquoi ajouter des facteurs ?
- **Quels sont ces facteurs ?**
  - **Les hard-tokens physiques**
  - **Les soft-tokens (smartphones)**
  - **Les facteurs et critères comportementaux**
  - **Les facteurs biométriques : apparences physiques et morphologiques**
  - **Les facteurs biométriques : caractéristiques biologiques**
  - **Le marquage volontaire…**
  - **Les facteurs encore plus originaux / atypiques**
- Implémentations, solutions, services

Une « question » de facteur…

Le mot de passe, traditionnel exemple du 1er facteur, répond à la question :

« Qu'est ce que l'on sait ? »

Mais bien d'autres facteurs / questions permettant de vérifier une identité peuvent être employés :

- ***Que possède-t-on ?*** (une carte magnétique, un hard-token, une clé USB, un smartphone,…) ;
- ***Qu'est ce que l'on est ?*** (utilisation de l'empreinte digitale, empreinte rétinienne,…) ;
- ***Que savons-nous faire ?*** (un *selfie* avec grimace, de la reconnaissance vocale,…).

- ***Où nous trouvons-nous ?*** (géolocalisation depuis des lieux jugés « de confiance ») ;
- ***A quelle date / heure sommes-nous ?*** (accès autorisé en jours / heures ouvrés uniquement) ;
- ***Qu'entendons-nous ?*** (bruits ambiants) ;
- ***Que portons-nous ?*** (vêtements intelligents, bijoux, babioles…) ;
- ***Qu'avons-nous fait récemment ?*** (SMS reçus, activités des réseaux sociaux, etc.).

Une « question » de facteur…

Ces différentes « questions » disposent toutes à l'heure d'aujourd'hui d'une implémentation existante (au stade de R&D / PoC, solution opensource / commerciale, éprouvée ou non) avec des taux de réussite / d'erreur et de faux-positifs tout à fait convenables.

Découvrons ensemble certains de ces facteurs communs comme atypiques…

Des hard-tokens physiques

Left to right: Smart card (phone SIM), PayPal 2FA token, Yubikey

RSA SecurID SD600

RSA SecurID SD200

RSA SecurID SD520

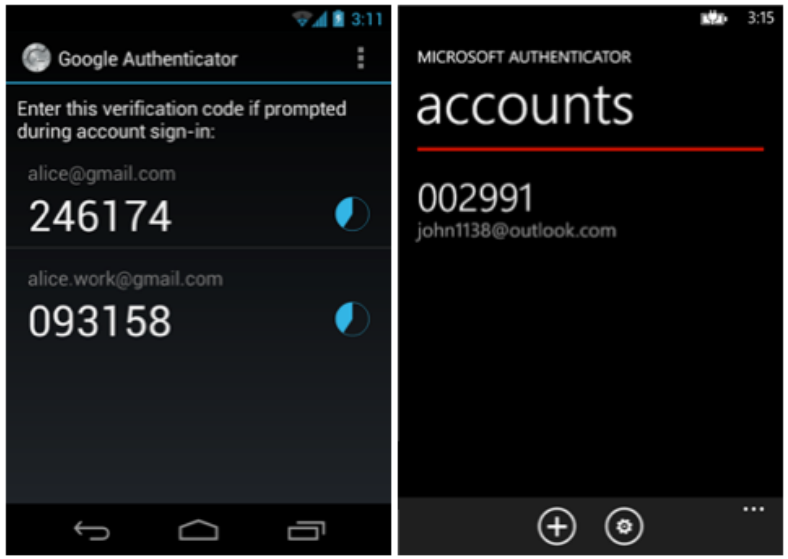
RSA SecurID SID700

RSA SecurID SID800

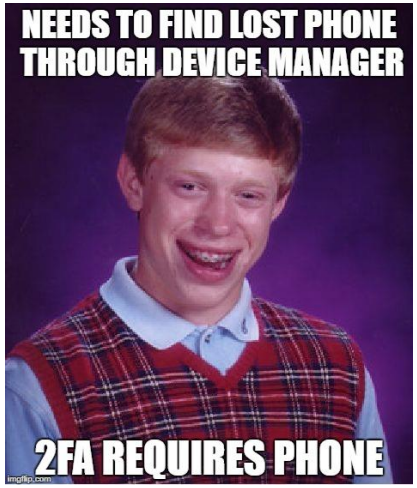
BlackBerry with
RSA SecurID software token

Quels sont ces facteurs ?

Les soft-tokens dématérialisés :

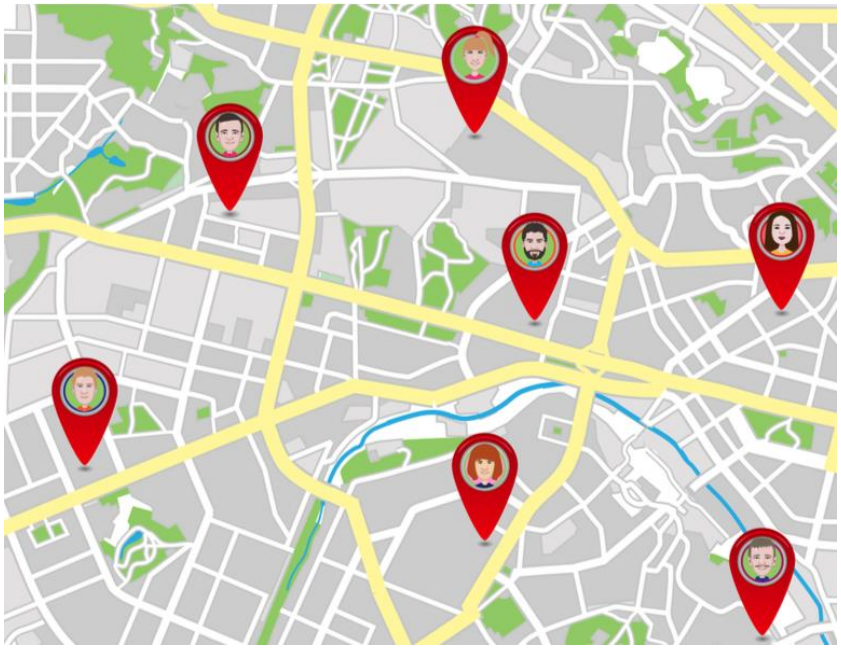


Login codes from authenticator apps for Android (left) and Windows Phone



Les facteurs et critères comportementaux

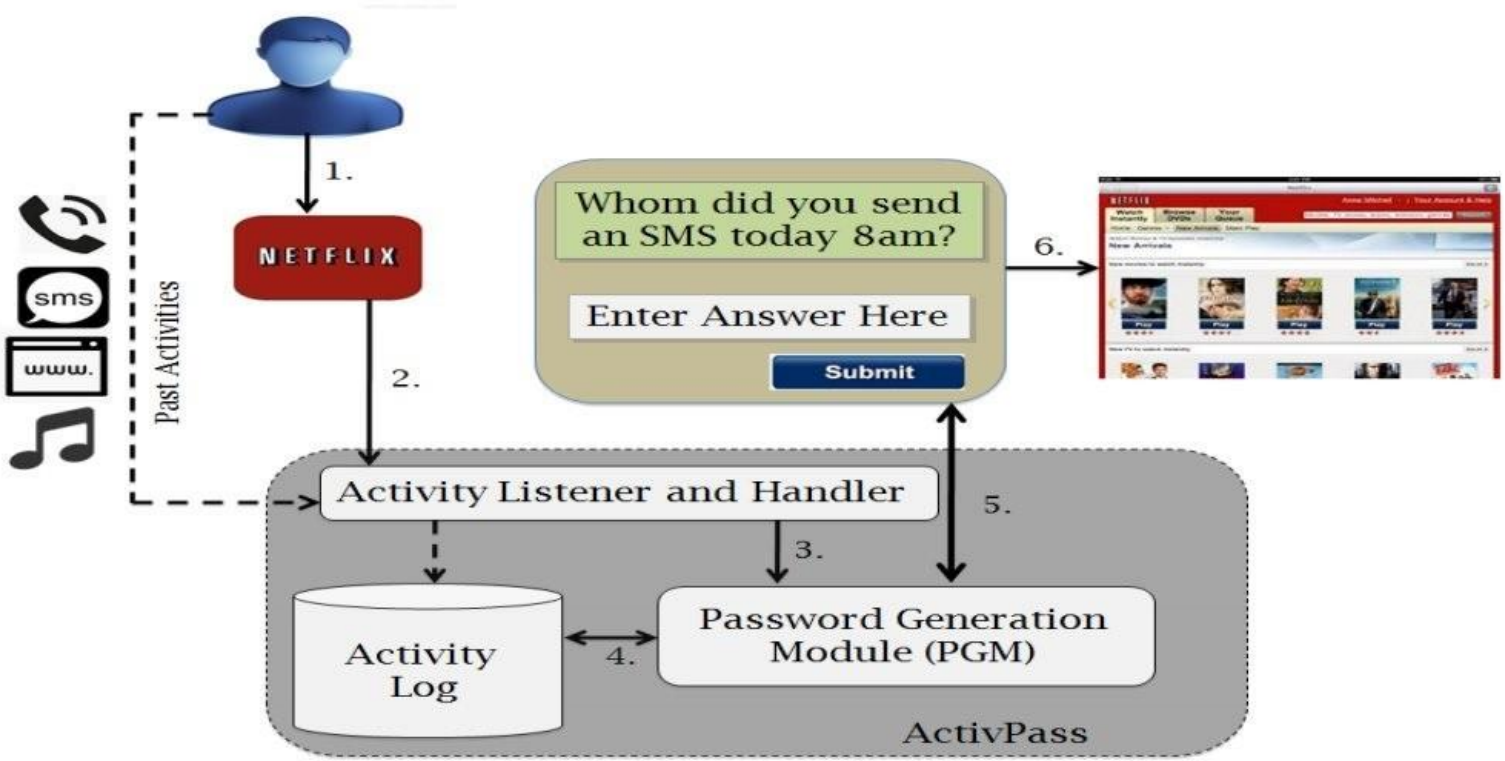
Géolocalisation



Créneaux temporels

Les facteurs et critères comportementaux

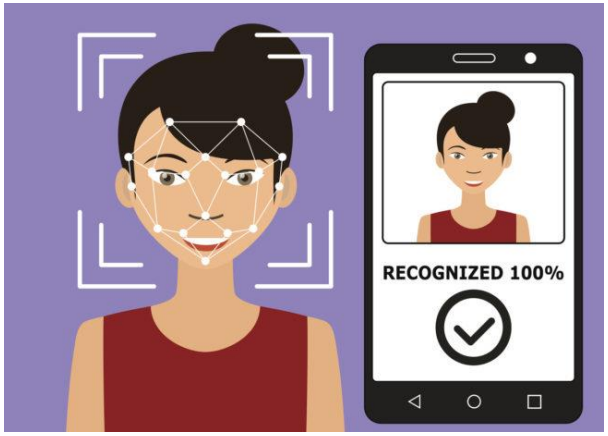
L'activité passée (ActivPass) : Ce système consiste à collecter quotidiennement divers journaux et logs en provenance d'un tas de ressources autorisées par l'usager, puis génère un mot de passe qui se traduira comme la réponse à une question de sécurité pour le lendemain.



Les facteurs biométriques : apparences physiques et morphologiques

Les traditionnels et ultra-connus :

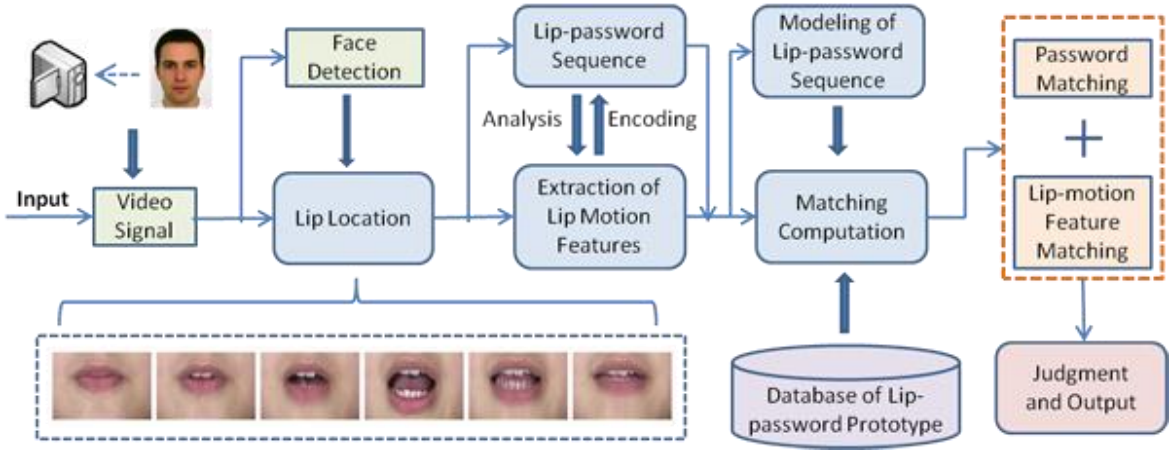
- **Reconnaissance d'empreintes digitales**
- **Reconnaissance de la main**
- **Reconnaissance oculaire**
- **Reconnaissance faciale**
  - Comment déjouer des « photos » présentées à la caméra ?
    - Amazon avec le paiement par « selfie »
    - Funny faces de Google : Souriez ! Grimacez !
    - Liveness check de Google : clignement des yeux, tirer la langue…
    - Head tracking : suivi des mouvements
    - Image thermique ? Détection infra-rouge ?...



Les facteurs biométriques : apparences physiques et morphologiques

Et d'autres bien moins connus…

- **Reconnaissance labiale, avec « lip motion password » :** Cette méthode innovante se base sur les mouvements des lèvres de l'individu, jugés uniques. En corrélant ces mouvements vis-à-vis du mot de passe indiqué textuellement, un *framework* appliquant une série d'algorithmes de reconnaissance permet de prouver ou non l'identité de l'usager tout en l'authentifiant.
  - **Résistant au mimétisme (autre interlocuteur le prononçant)**
  - **Non-pollué par les bruits environnements (par rapport à la reconnaissance vocale)**
  - **Utilisable par des muets**
  - **Sans frontière de langue !**

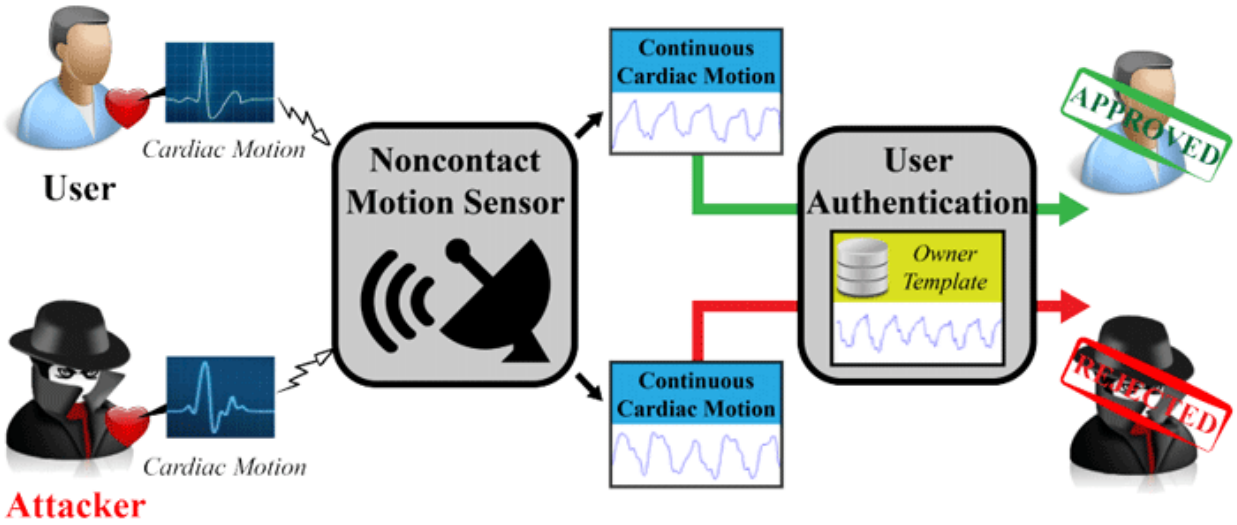


Les facteurs biométriques : caractéristiques biologiques

- **Reconnaissance vocale**
  - La simple répétition d'une phrase « Bond, James Bond », pré-enrôlée et falsifiable via un magnétophone ;
  - La lecture à l'instant T d'une phrase soumise par le système authentifiant, qui sur la base de la réponse (et d'un certain nombre de mots / sons pré-enrôlés) permet de valider l'authentification : bien plus robuste.
- **Reconnaissance cognitive** (Neurosky Mindset) : électro-encéphalographie

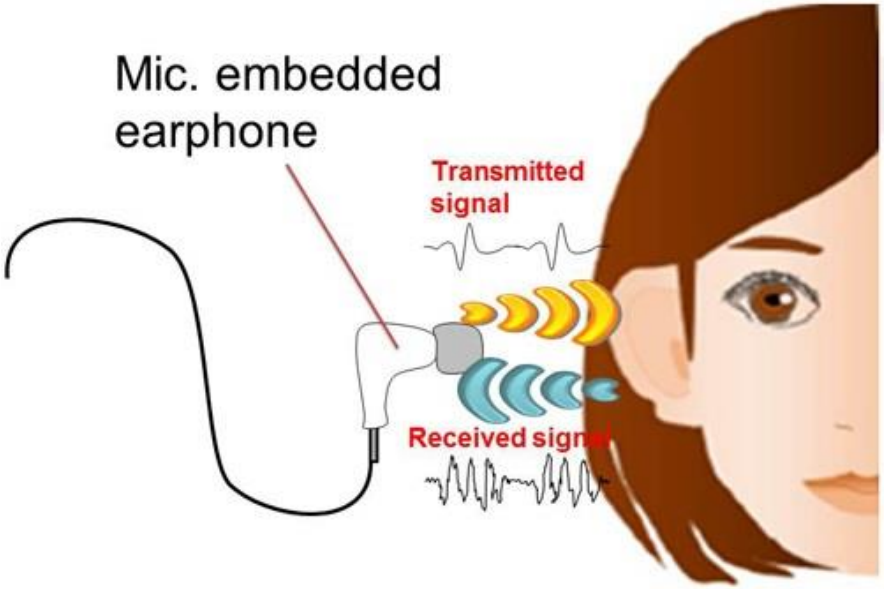
Les facteurs biométriques : caractéristiques biologiques

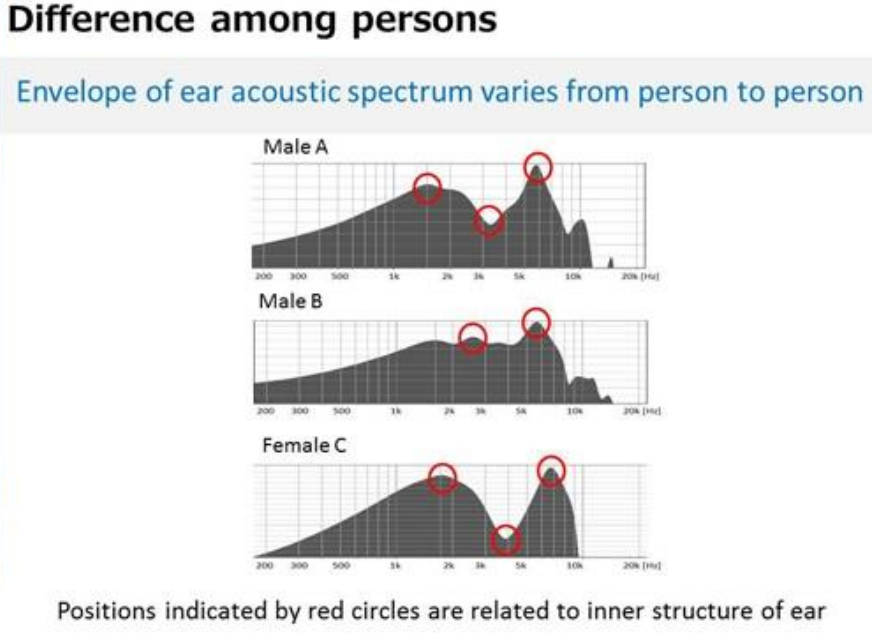
- **Reconnaissance cardiaque :**
  - **Cardiac Scan :** ce système d'authentification utilise un radar Doppler bas-niveau pour analyser par onde et cartographier continuellement les dimensions de votre cœur, vous autorisant en conséquence l'accès à une application, un équipement ou à une zone restreinte dès lors que vous êtes suffisamment proche du capteur
  - **Bracelet Nimy**



Les facteurs biométriques : caractéristiques biologiques

- **Cavité auditive :** Des chercheurs de l'entreprise NEC ont mis en place ce tout nouveau mécanisme d'authentification auditif avec plus de 99% de précision, via les cavités auditives qui diffèrent entre chaque individu. En émettant un signal audio et en enregistrant le signal retour (l'écho), l'appareil est capable de déterminer l'identité du porteur.



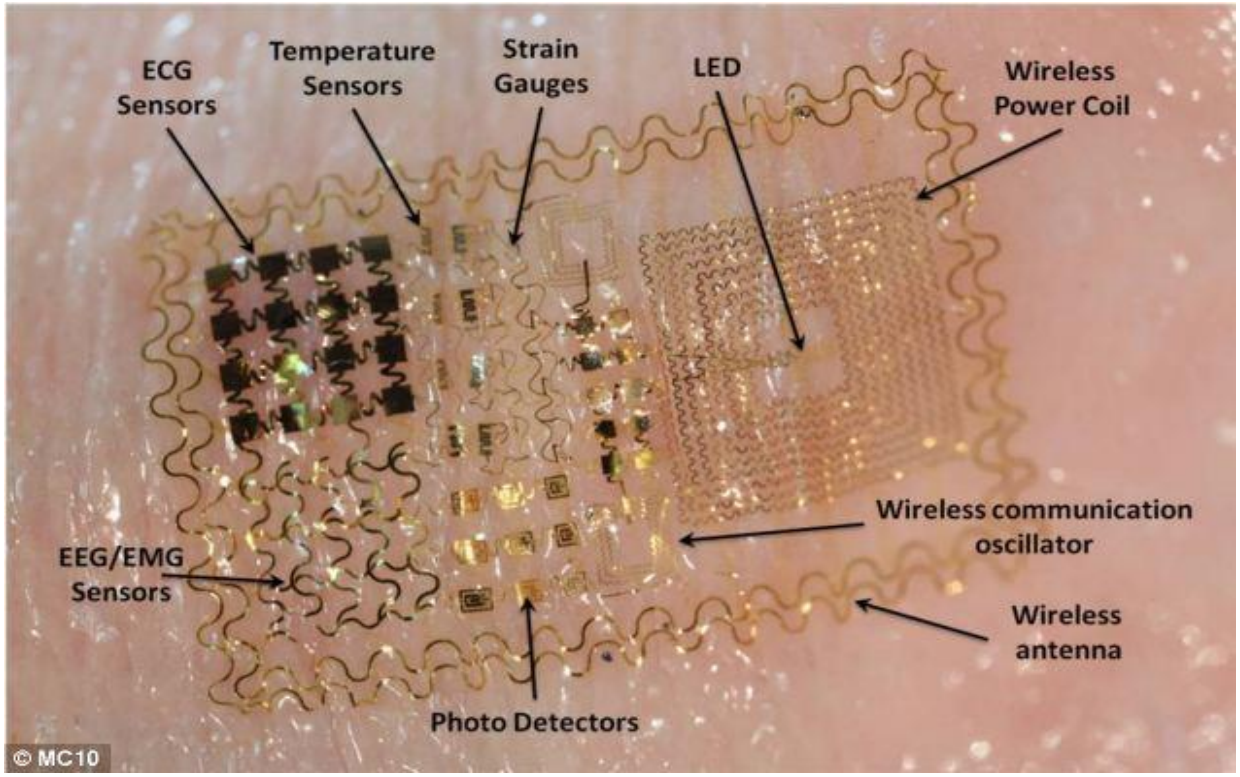


Le marquage volontaire…

- **Pilule bleue ou pilule rouge ? :** Une alternative plus expérimentale a été mise en avant lors de la conférence WSJ/All Things Digital, Google et Motorola ont présenté une pilule à avaler permettant de vous transformer en mot de passe humain pour votre smartphone ou autres applications. La bien-nommée « *vitamin authentication* » pilule s'active dans l'estomac via les acides contenus dans celui-ci.

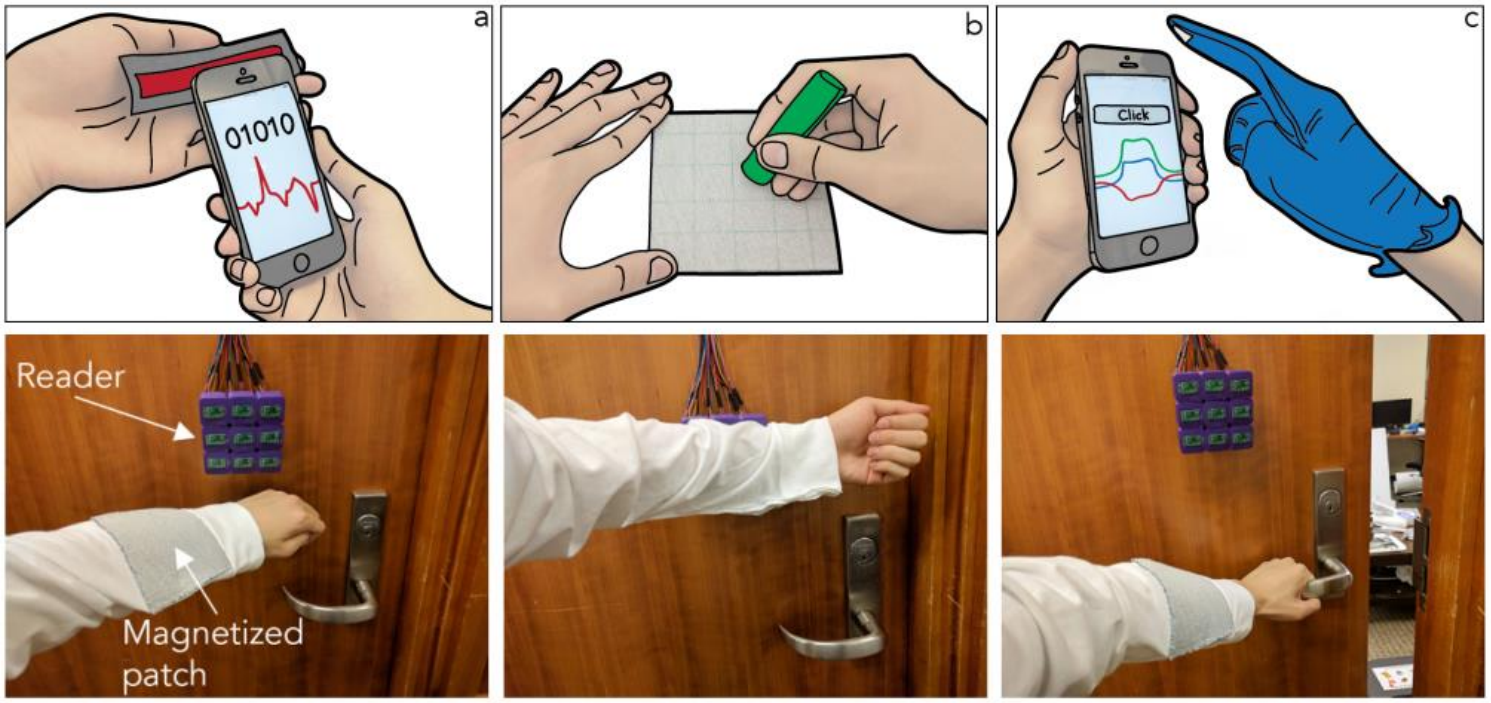
Le marquage volontaire…

- **Tatouage biométrique :** Cette autre technique d'authentification, généralement appelée « BioStamps » est principalement destinée au monde médical pour faciliter l'authentification des patients.



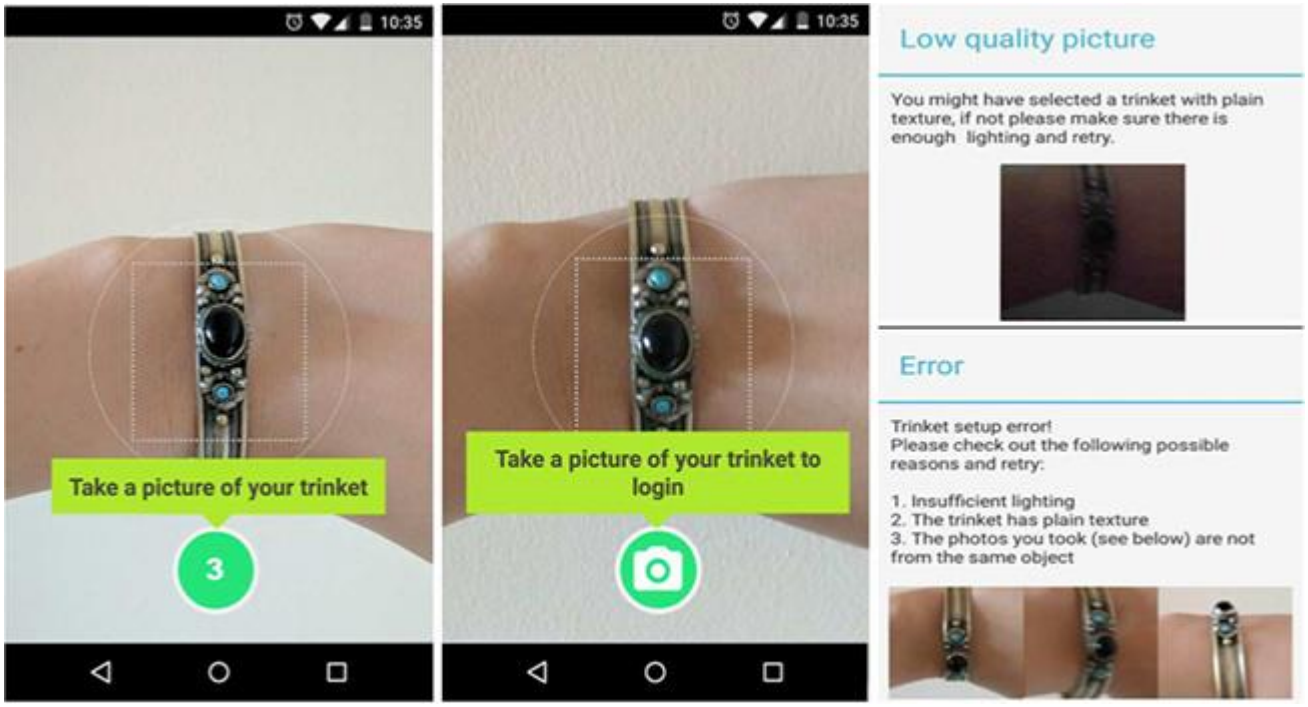
Les facteurs encore plus originaux / atypiques :

- **Les vêtements:** Les « SMART textiles » se démocratisent, notamment dans les défilés de mode. Des chercheurs de l'Université de Washington arrivent à présent à manipuler la polarité de tissu magnétisé dans le but d'y stocker de la donnée ou des informations visuelles.



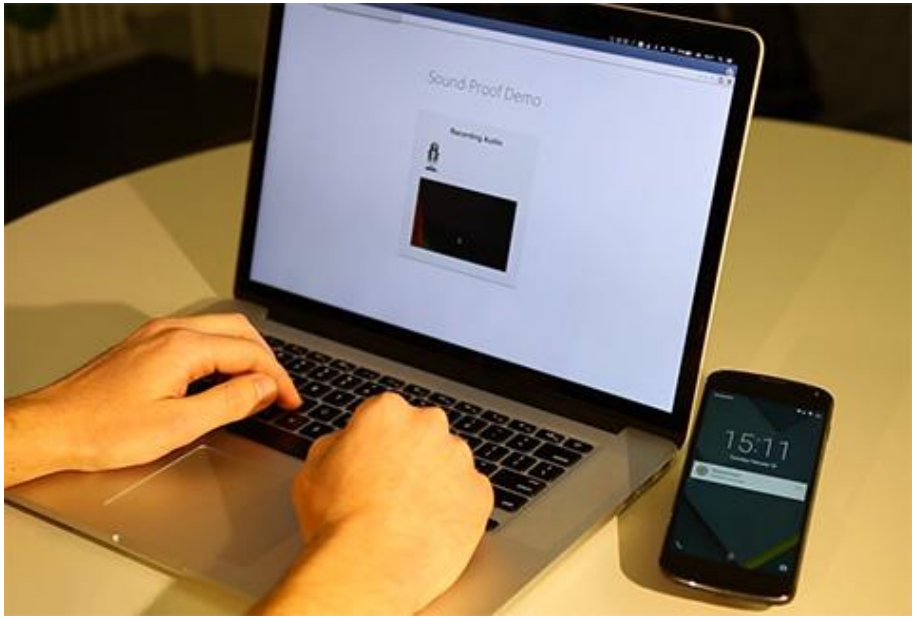
Les facteurs encore plus originaux / atypiques :

- **Bijoux et babioles :** Un groupe de chercheurs de la *Florida International University* et Bloomberg LP a créé Pixie, une solution basée sur une caméra (smartphone) qui se fonde sur ce que l'utilisateur porte : il est question de *trinket* (babiole) et sur ce que l'utilisateur sait (quelle babiole photographier/filmer, quel angle de visibilité, quel point de vue, etc.).

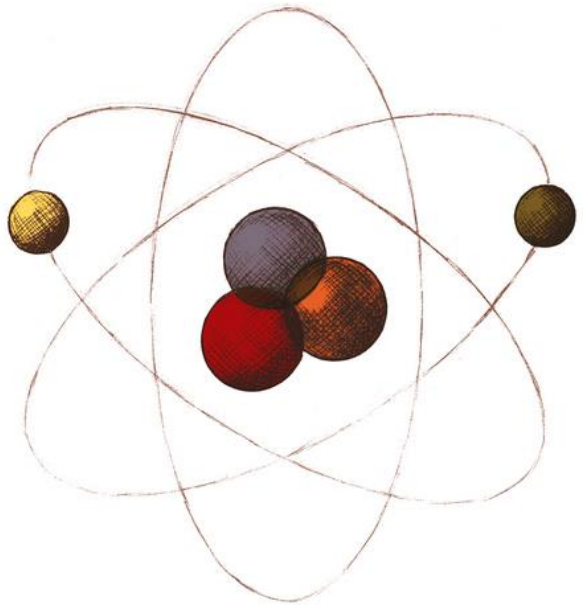


Les facteurs encore plus originaux / atypiques :

- **Ambiance sonore : SoundProof,** lorsqu'une ressource sur un poste est protégée par l'authentification forte « *Sound-Proof* », le micro du poste s'active automatiquement pour détecter les sons ambiants. En parallèle, une notification est envoyée sur le smartphone de l'individu identifié, qui de son côté (doté de l'application « *Sound-Proof* »), active également son micro pour comparer les sons ambiants.



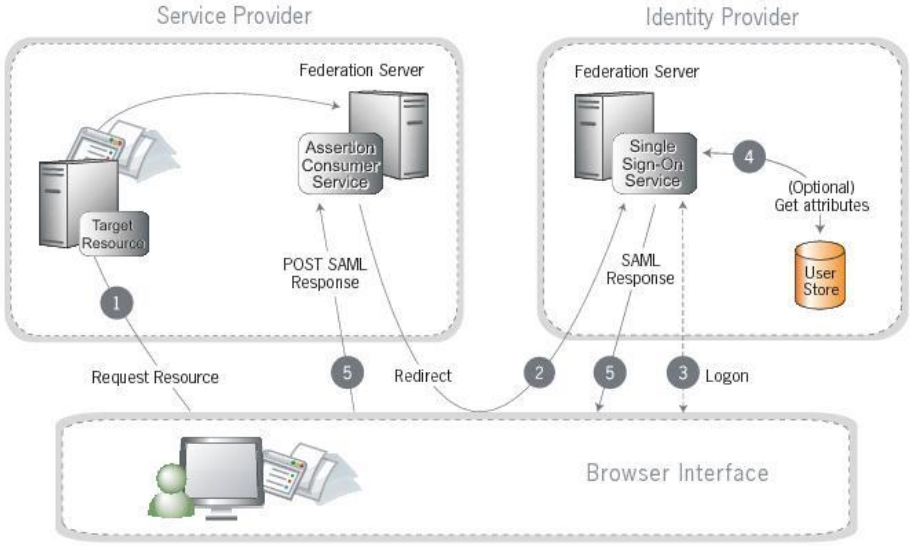
PLAN

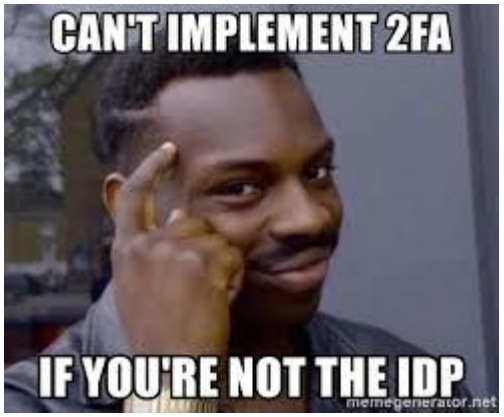


- Bref historique et introduction contextuelle
- Vocabulaire et acronymes
- Pourquoi ajouter des facteurs ?
- Quels sont ces facteurs ?
  - Les hard-tokens physiques
  - Les soft-tokens (smartphones)
  - Les facteurs et critères comportementaux
  - Les facteurs biométriques : apparences physiques et morphologiques
  - Les facteurs biométriques : caractéristiques biologiques
  - Le marquage volontaire…
  - Les facteurs encore plus originaux / atypiques
- **Implémentations, solutions, services**

Et maintenant ?

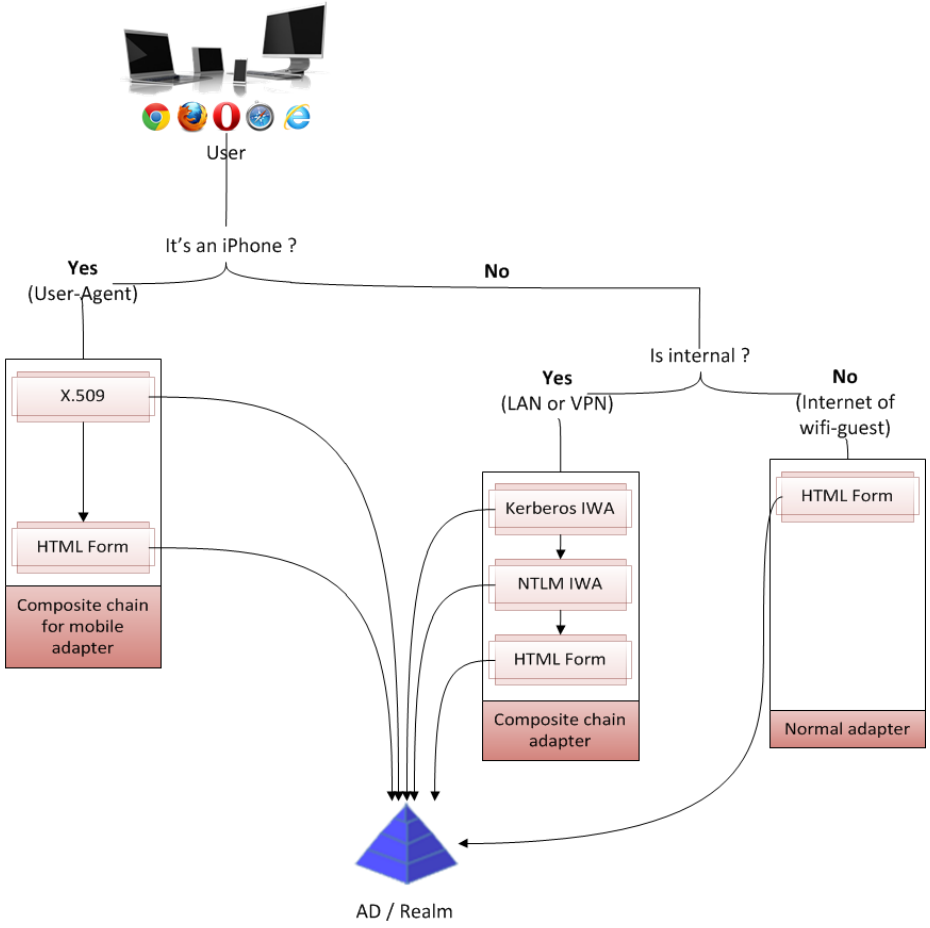
- **Comment ça s'implémente ? Tout dépend des facteurs…**
  - Pour 90% des cas : **opter pour la fédération des identités** (web / mobile)
    - Mettre en place un fournisseur d'identité (IdP) (Ping, ILEX, Keycloak, CAS, OpenAM, Google, Microsoft, Okta, SaaS…)
    - Référentiel unique de compte, authentification centralisée
    - Protocoles standardisés : **SAML, OAuth2, OIDC**…
    - **Plus de mots de passe qui transitent sur le réseau !**
    - Schéma d'authentification et facteurs configurables.

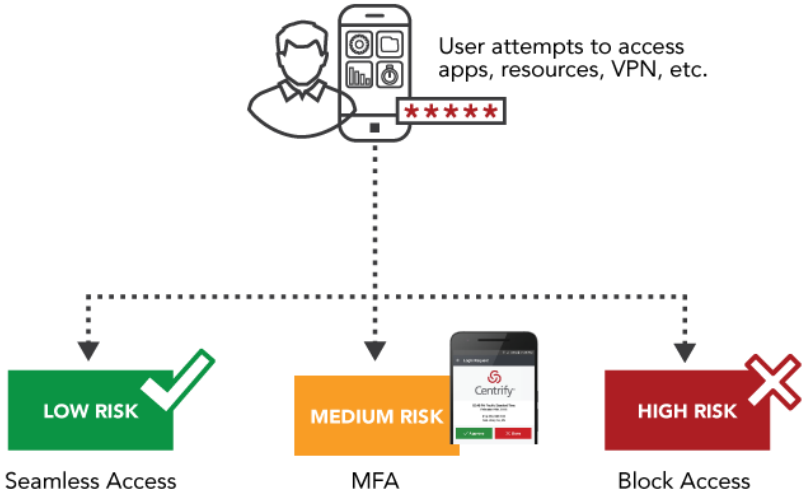




L'authentification adaptative

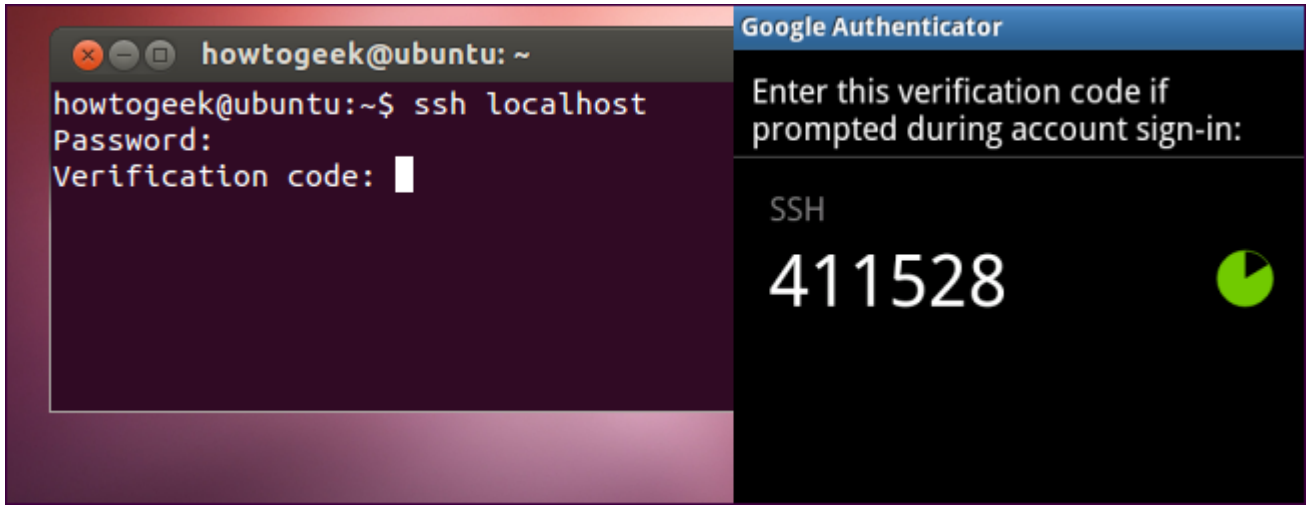
- Ajuster l'authentificateur approprié en fonction du contexte et de la criticité





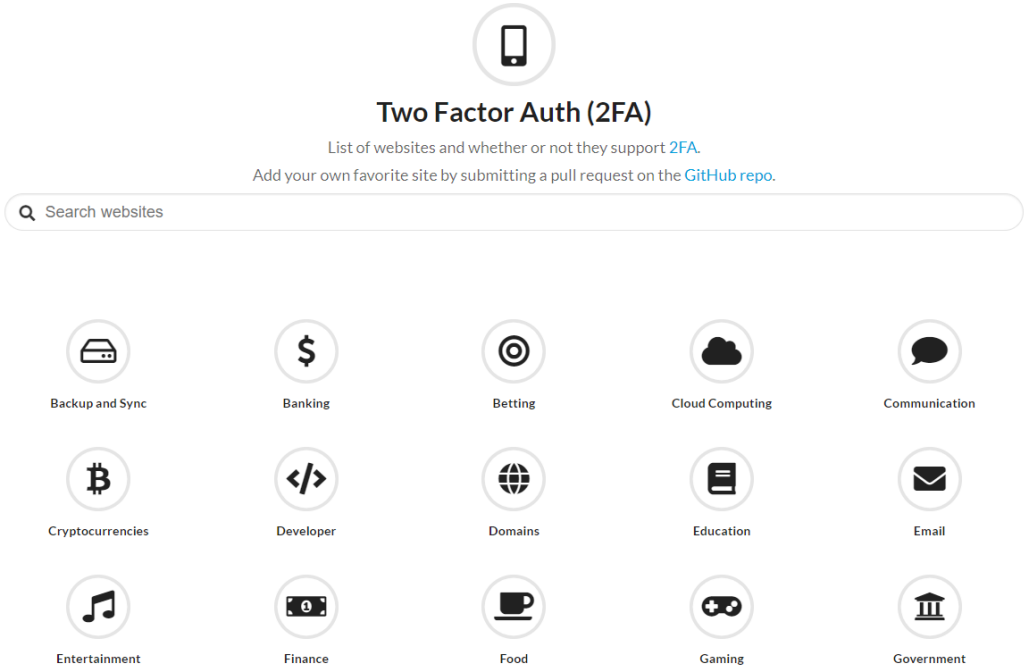
Et maintenant ?

- **Comment ça s'implémente ? Tout dépend des facteurs…**
  - Radius (VPN, etc.)
  - Module PAM Unix (OTP Google Authenticator)



Et maintenant ?

- **Quels services sont compatibles ?**
  - Certains services proposent leur propre compatibilité 2FA (OTP)
  - D'autres peuvent être fédérés, donc dépendent de ceux implémentés via votre IdP
  - Des kits de développement dans divers langages existent (PHP, ASP .Net, Java, etc.)



Et maintenant ?

- **Quel(s) facteur(s) choisir ?**
  - C'est la grande question du choix de la solution…
    - Être portatives voir s'intégrant avec les équipements que vous portez habituellement sans induire de surcoût d'achat ou de gestion (le hard-token se voit délaissé par rapport aux soft-tokens ces dernières années) ;
    - Limiter les actions de l'usager pour impacter le moins possible son expérience utilisateur et le temps consacré à ses phases d'authentification : recopier un code reçu par SMS ou généré par un soft-token se voit remplacé par un simple « *swipe* ».
    - Être totalement transparent, sans nécessiter d'action de l'usager (pilule ingurgitée, analyse du son ambiant entre le smartphone et l'ordinateur, port de vêtements intelligents, etc.).
    - Assurer une sécurité à toute épreuve, tâche la plus complexe.
    - Être acceptable par les usagers, RGPD *compliant*…

Sources & ressources

- **[TFA]** TwoFactorAuth, *List of websites and whether or not they support 2FA*, **https://twofactorauth.org/**
- **[PIX]** Pixie, *Camera Based Two Factor Authentication Through Mobile and Wearable Devices*, **https://users.cs.fiu.edu/~carbunar/pixie.pdf**
- **[LIP]** Lip-password for Personal Identity Verification (Yiu-ming Cheung et al.), **https://www.comp.hkbu.edu.hk/v1/proj/hkpfs/ymc/1/**
- **[CAR]** CardiacScan, **http://www.buffalo.edu/news/releases/2017/09/034.html**
- **[VET]** Data Storage and Interaction using Magnetized Fabric, **http://smartfabrics.cs.washington.edu/smartfabrics.pdf**
- **[ACT]** ActivPass, *Your Daily Activity is Your Password*, **http://synrg.csl.illinois.edu/papers/activpass.pdf**
- **[NIS]** NIST Special Publication 800-63B, **https://pages.nist.gov/800-63-3/sp800-63b.html**
- **[AMA]** Amazon wants you to pay by face, **https://nakedsecurity.sophos.com/2016/03/16/amazon-wants-you-to-pay-by-face/**
- **[NEC]** NEC develops biometrics technology that uses sound to distinguish individually unique ear cavity shape, **https://www.nec.com/en/press/201603/global_20160307_01.html**
- **[SOU]** Sound-Proof, *Usable Two-Factor Authentication Based on Ambient Sound*, **https://arxiv.org/pdf/1503.03790v3.pdf**
- **[HOT]** HOTP: An HMAC-Based One-Time Password Algorithm, **https://tools.ietf.org/html/rfc4226**
- **[TOT]** TOTP: Time-based One-time Password Algorithm, **https://tools.ietf.org/html/draft-mraihi-totp-timebased-08**
- **[HST]** Hacking soft tokens, Bernhard MUELLER, **https://gsec.hitb.org/materials/sg2016/whitepapers/Hacking%20Soft%20Tokens%20-%20Bernhard%20Mueller.pdf**
- **[PIL]** Proteus Digital Health, **https://www.proteus.com/**
- **[BST]** BioStamp, **https://www.mc10inc.com/**
- **[BRA]** Neurosky MindSet, *Forget your password: The future is 'passthoughts'*, **https://phys.org/news/2013-04-password-future-passthoughts.html**
- **[NIM]** Nimy bracelet, **https://nymi.com/**
- **[FAK]** How clever social engineering can overcome two-factor authentication… or not?, **http://www.sorinmustaca.com/how-clever-social-engineering-can-overcome-two-factor-authentication/**
- **[FBK]** Here is how to hack Facebook using SS7 flaw, **https://www.techworm.net/2016/06/hack-facebook-using-ss7-flaw.html**
- **[BYP]** Hacker Kevin Mitnick shows how to bypass 2FA, **https://techcrunch.com/2018/05/10/hacker-kevin-mitnick-shows-how-to-bypass-2fa/**
- **[HIB]** HaveIBeenPwned ?, **https://haveibeenpwned.com/**
- **[MIS]** MISC n°98 - Tour d'horizon de l'authentification forte (MFA)

Questions et remerciements