Panorama des approches pour la vérification d'âge en ligne

Olivier Blazy

Saclay, 25 ans du CRANS

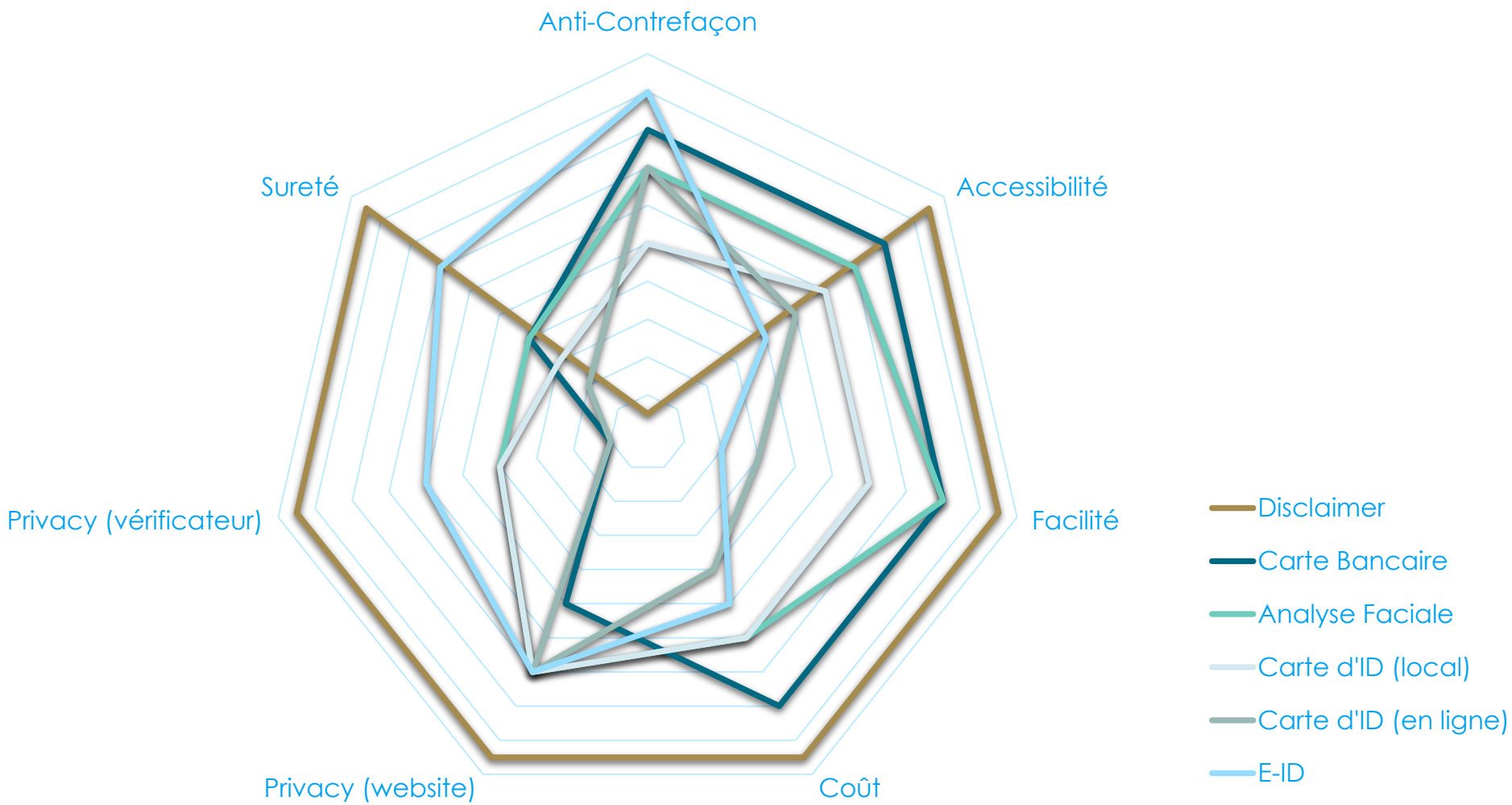
2023

Vérification d'âge en ligne

De plus en plus présente dans le débat public

- Internet ne doit pas être un endroit hors des lois
  - Veut-on/Peut-on avoir les mêmes limites que dans le monde réel
- Plusieurs soucis
  - Qui est derrière l'écran ?
    - 1 utilisateur = 1 login = 1 personne ?
  - Quelles fonctionnalités veut-on ?
    - Bloquer tous les mineurs ? Laisser accès aux utilisateurs légitimes ? Les deux ?
  - Veut-on copier le monde réel ? Faire mieux ?
    - Doit-on protéger l'identité des gens ? Auprès de qui ?
    - Est-ce que les vérificateurs doivent apprendre qui consultent quoi ?

Un équilibre très complexe



Anti-Contrefaçon : Unforgeability

Il doit être impossible de :

- produire un token valide, si on est sous la limite
  - ➡ Utilisation de mécanisme de signature / certification
    Par défaut une signature n'est pas anonyme / pseudonyme

- Rejouer un token
  - ➡ Les interactions sont nécessaires
    Il doit y avoir un nonce pour éviter des rejeux

Protection face au site web

Le site web ne doit pas apprendre :

- Notre identité

  Différence avec le monde physique: Attribut sélectif

- Notre âge (Savoir que +18, ne veux pas dire savoir 37)

  ➡ La réponse ne doit être qu'un bit et pas l'âge. (RGPD: Minimisation)

- L'autorité qui a certifié l'âge

  ➡ Les signatures doivent être anonymes (signature de groupe / d'anneau)

Protection contre le vérifieur

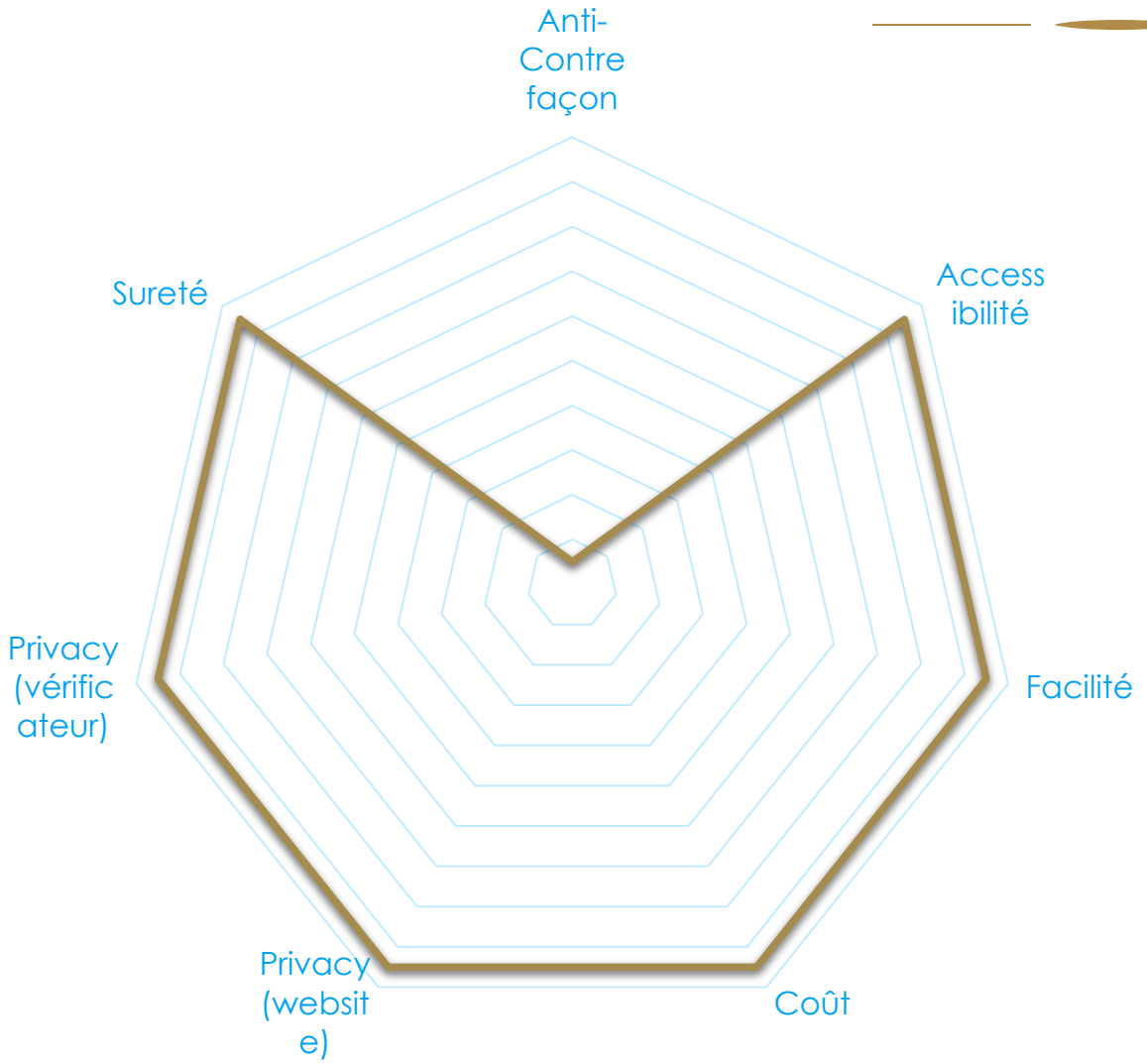
Le vérifieur ne doit pas apprendre :

- Quel âge est demandé (RS > 15 vs site X > 18)
  - ➡ Actuellement, il existe 3 seuils… autant répondre au 3

- Apprendre quel site fait la requête
  - ➡ Le challenge ne doit pas contenir d'info sur le site
  - ➡ Pas de communication directe entre le site et le vérifier (attention aux x-referral…)

Monde physique : Quand on génère votre carte d'identité, personne ne sait ce que vous allez en faire

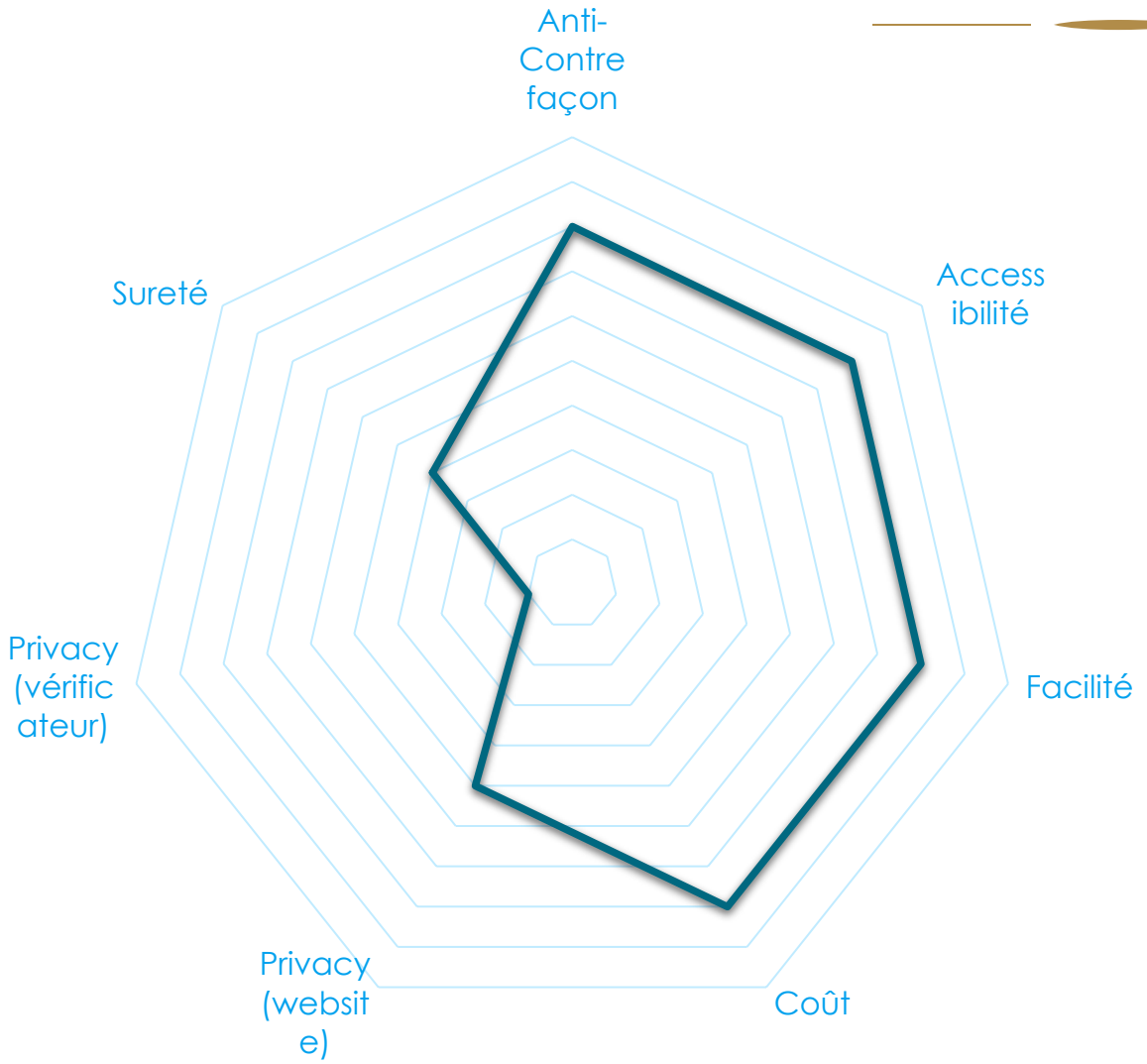
Vérification avec : Un disclaimer



Juste une boite oui/non

- **AC:** Tout le monde peut mentir, pas d'accès accidentel
- **Acc:** Pas de prérequis
- **Fac:** Un clic
- **Coût:** Marginal
- **Website:** Rien
- **Vérificateur:** Rien
- **Sureté:** Pas d'info donc pas de fuite

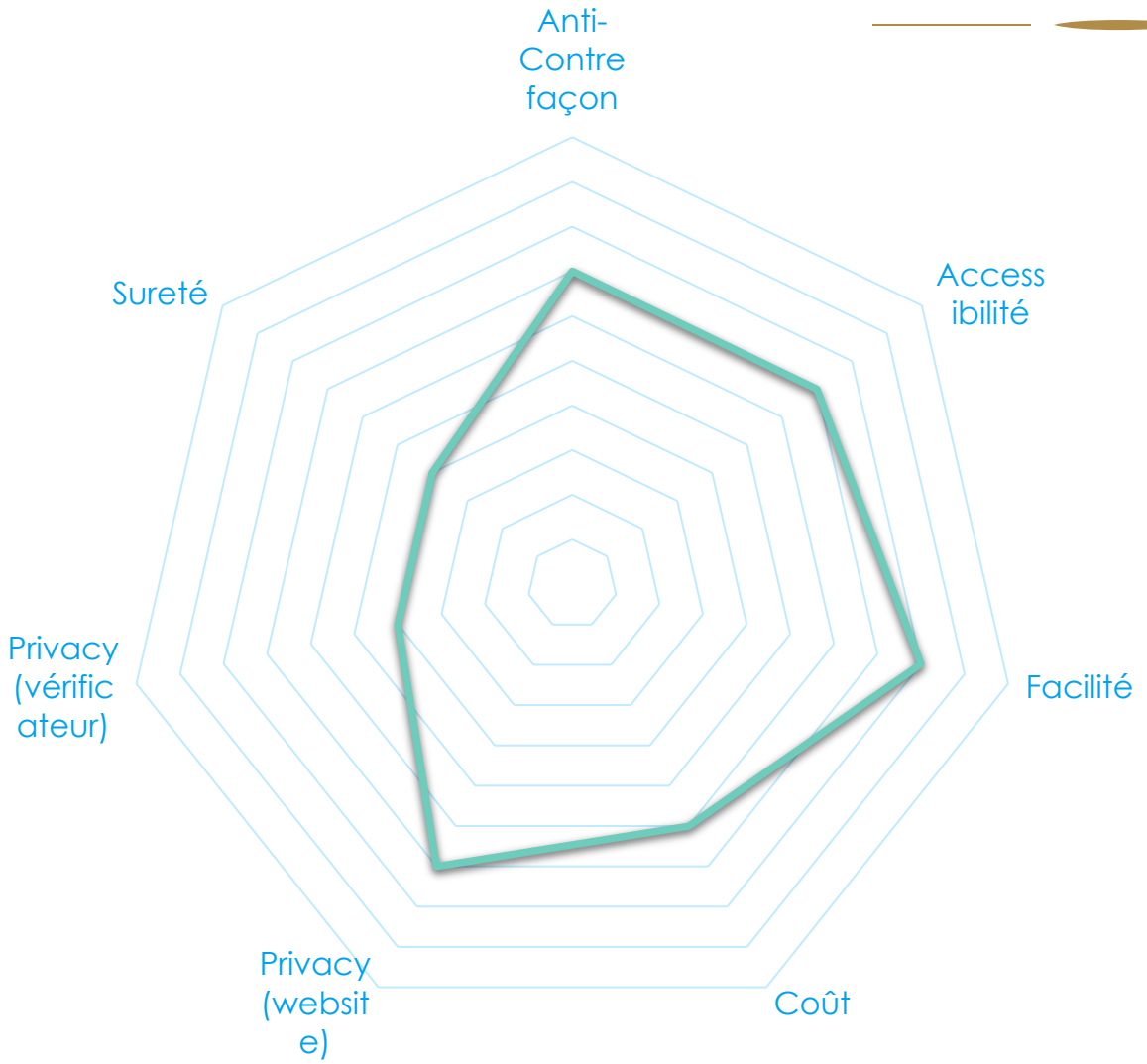
Vérification avec : Une Carte Bancaire



Un paiement de 0€

- **AC :** Système Bancaire, mais 16+
- **Acc:** Il faut un compte bancaire
- **Fac:** Très
- **Coût:** Faible (~0.10€)
- **Website:** Potentiellement rien
- **Vérificateur:** Apprend le compte et le site
- **Sureté:** Des méchants peuvent apprendre les details de CB, augmenté en cas de pub

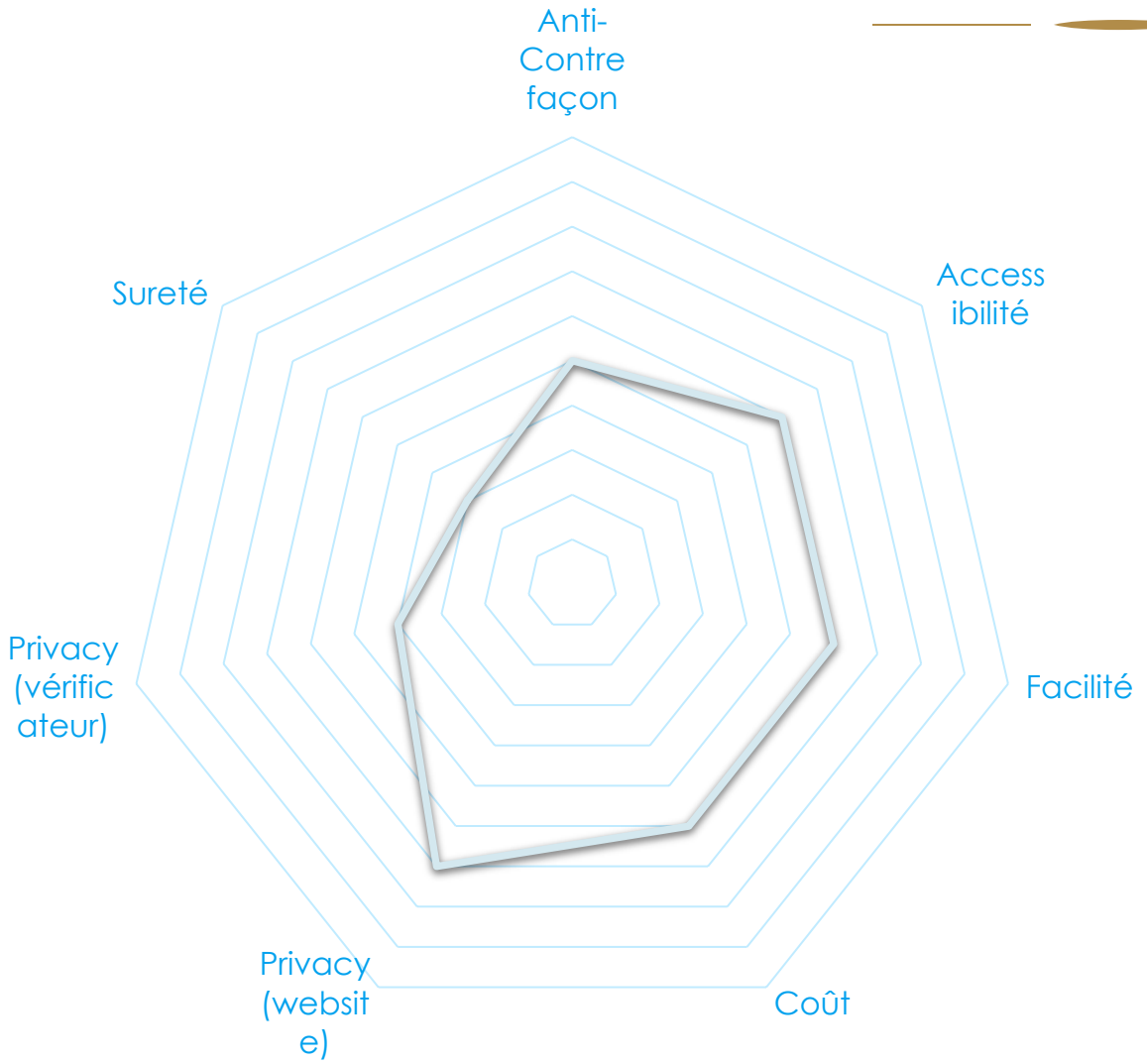
Vérification avec : l'Analyse Faciale



Utiliser la webcam pour estimer l'âge de l'utilisateur

- **AC:** Bonne pour les personnes loin de la limite
- **Acc:** Une webcam
- **Facilité:** Très… modulo biais
- **Coût:** ~0.30€
- **Website:** Peut ne rien apprendre
- **Vérificateur:** Apprend le site
- **Sûreté:** Ouvrir une webcam peut augmenter l'efficacité du phishing

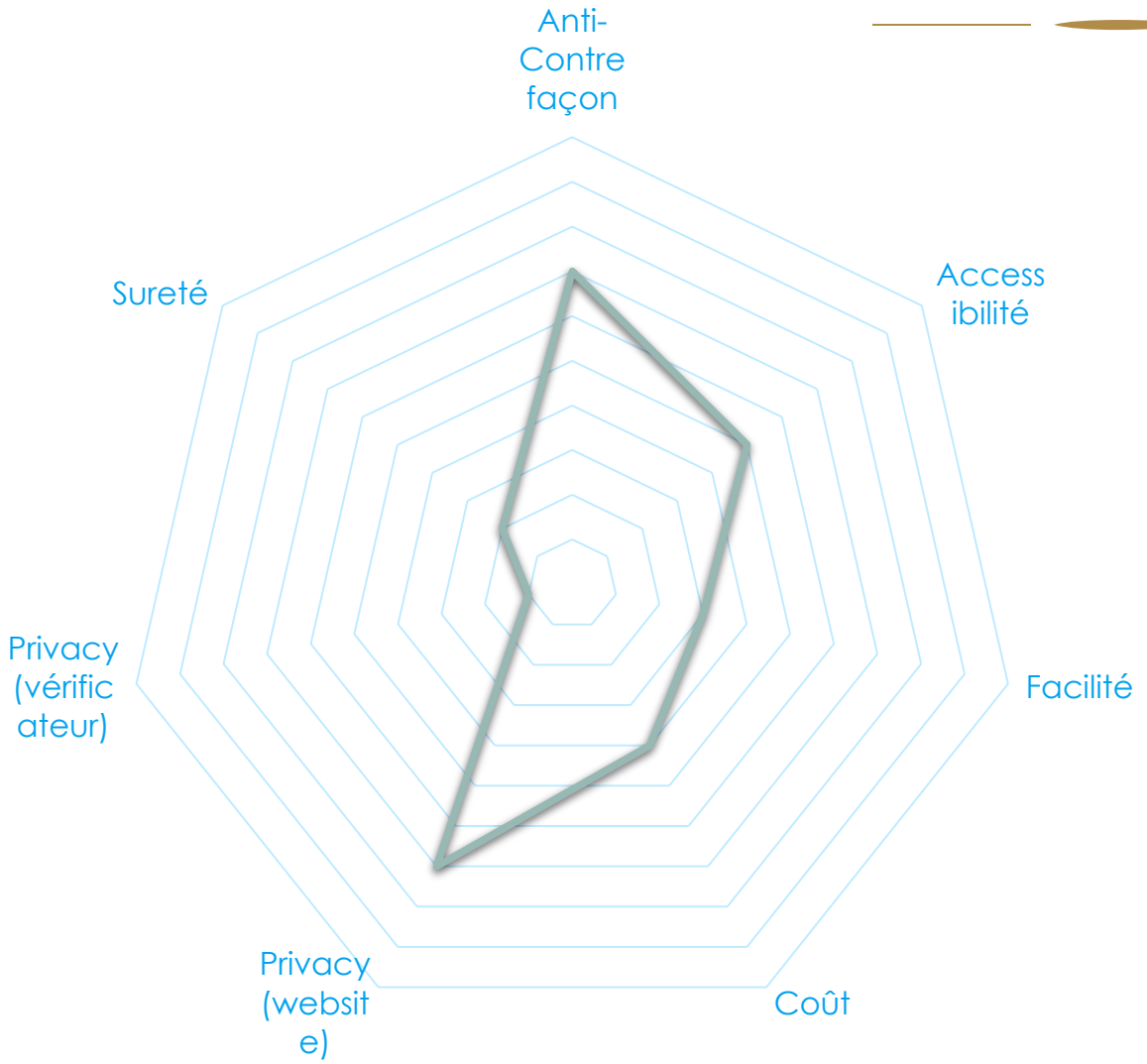
Vérification avec: une carte d'ID (local)



Analyse locale d'une carte d'ID

- **AC:** Les cartes d'ID sont dures à contrefaire, mais plein de scans sont dispo
- **Acc:** Il faut une carte *locale*
- **Fac:** Il faut pouvoir la scan
- **Coût:** Marginal
- **Website:** Peut ne rien apprendre
- **Verificateur:** Apprend le site web
- **Sureté:** Ok si l'analyse est bien locale

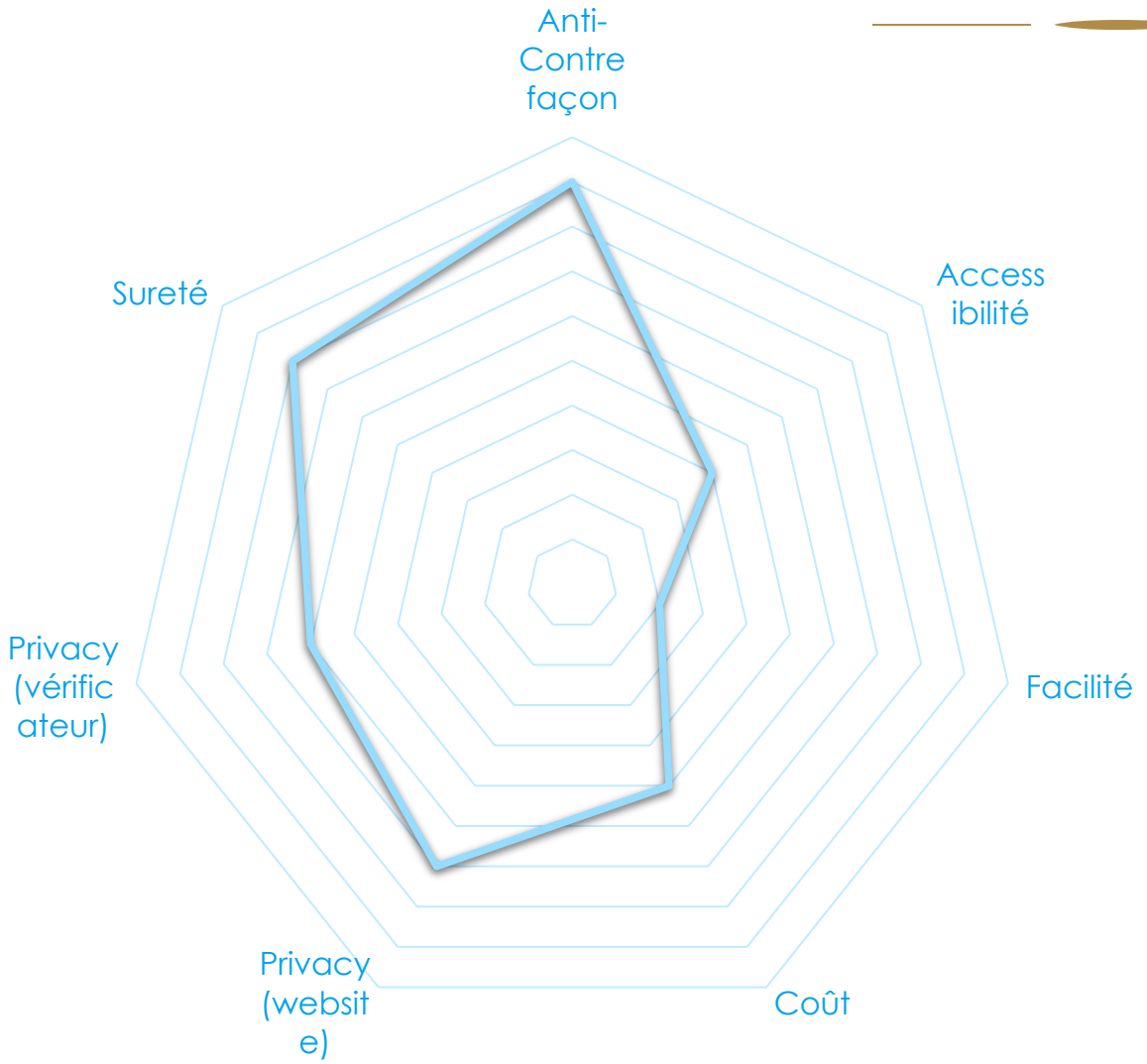
Vérification avec: Une carte d'ID à distance



Envoyer une photo à distance

- **AC:** Dur à contrefaire
- **Acc:** Carte + ID
- **Fac:** Long (10-15 min)
- **Coût:** 1-2€
- **Website:** Apprend le vérif
- **Vérificateur:** A l'ID et le site
- **Sureté:** Des méchants ont vos documents d'identité

Vérification avec: E-ID



Si on a une carte compatible eIDAS.

- **AC:** Aussi sûr qu'une CB
- **Acc:** Il faut un lecteur
- **Fac:** Sans contact
- **Coût:** Marginal
- **Website:** Rien
- **Verificateur:** Execution locale
- **Sûreté:** Des méchants pourraient distribuer de fausses apps. Mais la portée serait restreinte

Double-Anonymat à la rescousse

Preuve de concept faite avec la CNIL et le PEReN

- Permet une approche **standardisée** protégeant la vie privée
  - Surcoût marginal :
    - Une certification annuelle par des régulateurs
    - Une communication à peine plus lourde

- **Ne change pas** la nature de la vérification
  - Pas d'interférence avec le business model
  - Pas besoin d'app dédiée

Les PETs pour l'authentication: Signatures de groupe

Les signatures sont une primitive bien connue : Une entité authentifie un message de telle façon que n'importe qui puisse verifier que le message a été approuvé par la dite identité.

Problème : Si une banque authentifie une ID? Alors le site web apprend que ID est client de la banque…

Les Signatures de groupe permettent de signer "anonymement" au nom d'un groupe. Ainsi tout le monde sait que ID a été authentifié par une entité agréée sans apprendre laquelle.

Une authorité spéciale (Opener) peut révoquer cet anonymat en cas de comportement à risque.

Group Signatures: Securité

Experiment $\mathsf{Exp}^{\mathsf{anon}-b}_{\mathsf{GS},\mathcal{A}}(\mathfrak{K})$

1. $(\mathsf{pk}, \mathsf{msk}, \mathsf{skO}) \leftarrow \mathsf{Setup}(1^{\mathfrak{K}})$
2. $(m, i_0, i_1) \leftarrow \mathcal{A}(\texttt{FIND}, \mathsf{pk}, \mathsf{msk} : \mathsf{joinP}, \mathsf{corrupt}, \mathsf{sign})$
3. $\sigma \leftarrow \mathsf{Sign}(\mathsf{pk}, i_b, m, \mathsf{sk}[i])$
4. $b' \leftarrow \mathcal{A}(\texttt{GUESS}, \sigma : \mathsf{joinP}, \mathsf{corrupt}, \mathsf{sign})$
5. $\texttt{IF}\ \ i_0 \notin \mathsf{HU}\ \texttt{OR}\ \ i_1 \notin \mathsf{HU}\ \texttt{RETURN}\ 0$
6. $\texttt{RETURN}\ \ b'$

Expérience:

1) Génère les clés
2) L'adversaire est l'autorité (msk) et peut corrompre des utilisateurs. Après un moment, elle choisit 2 utilisateurs (honnêtes) et un message cible..

3) On en choisit un, et signe en son nom
4) L'adversaire devine lequel des deux
5) Si les 2 utilisateurs sont encore honnêtes on considère la réponse de l'adversaire.

Vue d'ensemble du PoC X/CNIL/PEReN

Une meta-autorité certifie les vérificateurs (ERGA?)

→ Permet aux vérificateurs qu'ils sont dans un cadre légal

Quand un utilisateur accède à un site, il reçoit un challenge

→ Séparation + Unicité

Il envoie ce challenge au vérificateur de son choix

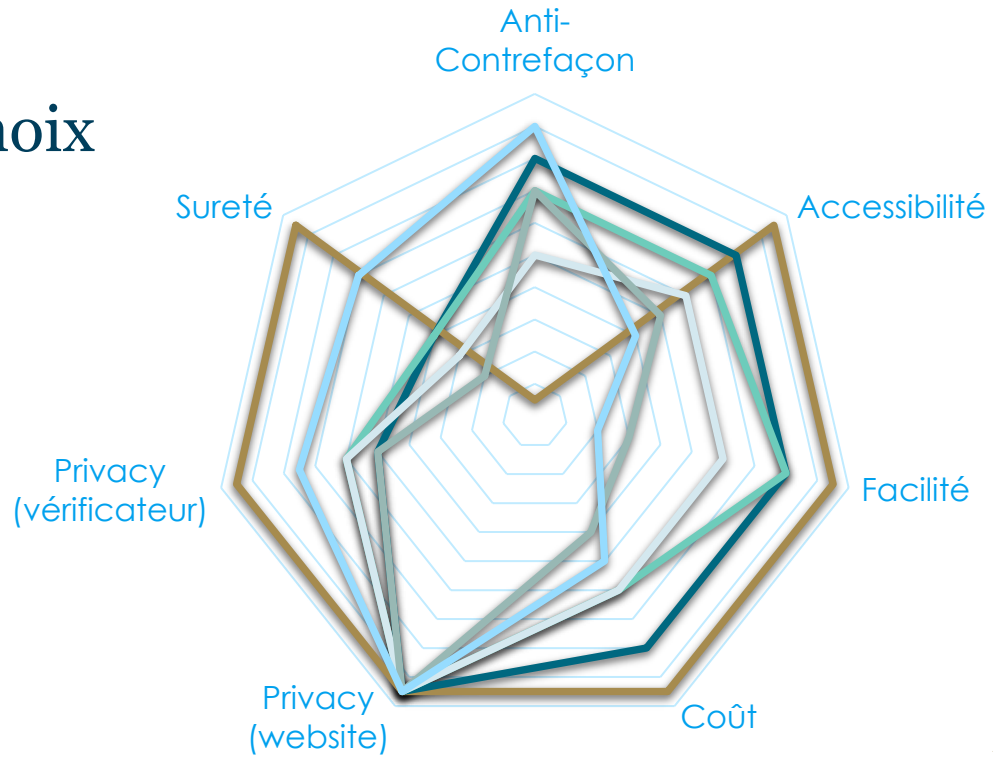
→ Séparation + Choix

Le vérificateur signe (…) le challenge

→ Anonymat du vérificateur + Anti Contrefaçon

L'utilisateur envoir la signature

→ Séparation + Anonymat



D’un point de vue technique

De la cryptographie éprouvée

- Preuve à divulgation nulle de connaissance
- Signature de groupe

Tout est publiquement auditable

- Aucune étape ne repose sur un calcul non vérifiable par les extérieurs
- L’utilisateur peut ajouter de l’entropie à ce qu’il reçoit

Le site n’a aucun privilège

- Il est donc parfaitement masquable
- Un site malicieux n’est pas plus avancé qu’un adversaire hors du système

Caractéristiques générales

L'API est **compatible** avec tous les systèmes de verif d'âge

- Pas de limitation technique, le législateur ne doit pas s'enfermer dans une solution

Le code est ouvert, libre, disponible depuis plus d'un an

- Les audits publics sont importants…
- Un commun digital est une approche importante dans le numérique…

Un outil **modulaire**

- Possibilité d'intégrer un mécanisme de facturation
- Plusieurs niveaux de confiance peuvent être gérés

PETs pour de la facturation anonyme: Batch Threshold Opening

Les vérificateurs d'âge veulent facturer leurs services aux sites de contenus. Comme une facturation directe n'est pas acceptable, il faut ruser…

Un service de taxe pourrait récupérer le token auprès du site web tous les x mois, et faire une ouverture de masse à seuil. Sans voir les tokens individuels, il récupèrerait à la fin que N tokens viennent de A, M de B, L de C…

Des tokens Canari permettraient de s'assurer qu'un site web n'oublie pas de transmettre des tokens pour moins payer…

PETs pour de la facturation anonyme: Batch Threshold Opening

Usage dans le monde reel :

- Présent dans des solutions de vote électronique (Fr, Su, No, …)
  - Permet de dépouiller sans regarder les bulletins un par un
- Utilisé dans certaine cryptomonnaie (Zcash)
  - La verification en batch coûte moins chère (en temps/resource) que celle individuelle.

PETs pour un meilleur Anonymat : Blind (Group) Signature

En l'état, l'autorité apprend le nonce qu'elle signe

Problème: Bien que le nonce ne contienne pas d'identification, il peut servir d'identifiant si une autorité et un site web s'allient

Les Blind Signatures apermettent à une entité de signer un message sans en apprendre son contenu. Il faudrait alors que le client fassent un (petit) calcul en local pour transformer la blind signature en vraie signature avant de la presenter au site web.

Attention : En l'absence de VPN, l'IP sera toujours un "lien" possible...

PETs pour un meilleur Anonymat : Blind (Group) Signature

- E-voting:
- Permettent d'avoir un bulletin certifié sans en révéler sa valeur…
- E-Cash:
- Permet de retirer de l'argent d'un compte sans qu'il soit ensuite liable à une dépense spécifique

PETs contre les Sous-Groupes : Steppable Group Signature

En l'état, un utilisateur ne peut pas verifier qu'un token a été généré 100% honnêtement

Problème: Si une autorité malicieuse a 2 clés certifiées, elle pourrait en réserver une pour un utilisateur spécifique… Et donc lors de la facturation savoir quell site Alice a consulté…

Les Steppable Signatures permettent à une autorité de générer une signature de groupe et de prouver volontairement que c'est bien avec la bonne clé secrete, augmentant ainsi la confiance pour un coût négligeable.

A posteriori Group Signature: Cette primitive permet de générer une signature non anonyme verifiable par l'utilisateur et qu'ensuite, il la transforme en signature de groupe (anonyme) classique

Compromis: La première solution demande juste à l'utilisateur une verification, là où la seconde est plus coûteuse en terme de calcul… Cependant, des incidents récentes montrent que les verifications sont généralement omises…

Soucis ?

La fracture numérique ?

- Les personnes accédant un site web ont nécessairement de la tech sous la main
- Attention aux touristes, ils n'ont pas forcément d'identité locale…

Et les VPN?

- Indépendant de notre solution… Si le site web ne sait pas qu'il doit appliquer la législation française…
- Une solution globale…

Anonymat ?

- En termes de RGPD, c'est du pseudonymat. L'IP n'est pas masquée.
- Mais l'API n'affaiblit pas plus la protection de la vie privée que la communication de base

Approche adverserielle

La vérification d'âge pour **restreindre** l'accès est **très mal** perçue

- Les gens vont vite la contourner (VPN …)
- Ou juste **partager** les tokens d'accès

Des informations critiques sont gérées

- Des méchants peuvent les emmagasiner -> Besoin d' **accréditations**
- Des risques de piratage, d'où un besoin de **minimisation**

Pour une **meilleure** perception, aussi s'en server pour des **bonus**

- Réduction / avantage senior
- Création de groupe / reduction pour les enfants

En conclusion

La vérification d'âge est multiple, il faut trouver le **juste** équilibre

- **La Facilitié d'utilization** est très importante.
  - 5 min de délais -> seuls 1.7% des volontaires sont allés au bout du processus
  - 13% pour les CB / Analyse Faciale
- Une app dédiée est un soucis…
- **Une Balance** est à trouver entre un test à la creation et à chaque connexion

Il est **possible** de faire une solution respectant le RGPD

- Une ID numérique (**eIDAS** … en mieux) aiderait énormément

Une approche **globale** à l'echelle de l'EU, avec des spécificités **locales** est possible

Attention à l'inclusion de tous…

Merci

Olivier.blazy@polytechnique.edu

https://github.com/LINCnil/SigGroup

ÉCOLE POLYTECHNIQUE

INSTITUT POLYTECHNIQUE DE PARIS