LE PORTEFEUILLE D'IDENTITÉS NUMÉRIQUES EUROPÉEN: EIDAS 2.0, ARCHITECTURE TECHNIQUE, ACTEURS, PROMESSES ET DÉFIS

MARYLINE LAURENT, PROFESSEUR, TÉLÉCOM SUDPARIS, INSTITUT POLYTECHNIQUE DE PARIS
COFONDATRICE DE LA CHAIRE DE L'IMT VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES

SÉMINAIRE ARISTOTE, ECOLE POLYTECHNIQUE, PALAISEAU, 29 JANVIER 2026

ACKNOWLEDGEMENTS

TRACIA project, funded under France 2030 programme, reference ANR-22-PESN-0006

MoreMedDiet project, as part of the PRIMA Programme, reference ANR-23-P012-0013

REMERCIEMENTS

Merci à Montassar Naghmouchi pour notre collaboration continue sur les identités numériques et les identités auto souveraines (SSI)

⇒ « Perspectives on National Digital Identity System », Journal Blockchain: Research and Applications, December 2025

=>

Merci aux membres de la Chaire IMT Valeurs et politiques des informations personnelles pour les nombreuses réflexions

Son fil Twitter : Twitter @CVPIP (toute l'actualité sur ce sujet)

REJOINDRE L'ACTION TRANSVERSE DU CNRS

"SÉCURITÉ INFORMATIQUE ET SCIENCES HUMAINES ET SOCIALES"

À la croisée entre le GDR Sécurité Informatique et le GDR Internet, IA et Société du CNRS

Plus d'informations et inscription ici :

AGENDA

Objectifs du portefeuille d'identités numériques européen

ARF v2 (le chantier technique de eIDAS v2) – version du 19/11/2025*

- l'architecture, les entités en présence pour la gouvernance et le bon fonctionnement
- les attestations, les services de confiance, la gouvernance
- des exigences (SHALL, SHOULD, MUST)

Le questionnement technique et plus largement

Quelques réflexions en conclusion

*https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#161-changed-formats-for-annex-2

OBJECTIFS DU PORTEFEUILLE D'IDENTITÉS NUMÉRIQUES EUROPÉEN (PEIN)

QU'APPORTE LE PEIN DE FAÇON SCHÉMATIQUE… ?

Dans la suite de eIDAS (v1) qui touche à l'identité numérique et aux services de confiance

Plus de confiance dans les interactions numériques en s'appuyant sur des identités numériques régaliennes => Contrecarrer les usurpations d'identités/fraudes (ex : ouverture de comptes bancaires)

A l'échelle de l'Europe => Transfrontalière (reconnaissance des identités numériques issues des autres EM)

Construire sur ce socle des services de confiance (signature numérique qualifiée, archivage…) => Moderniser les services (ex : signature de contrats) et des connexions plus sécurisées (ex : certificats d'accès)

S'appuyer sur l'ingéniosité des acteurs privés pour l'adoption massive par le grand public => Accès à des services administratifs, commerciaux…

ARF V2 – ARCHITECTURE AND REFERENCE FRAMEWORK V2

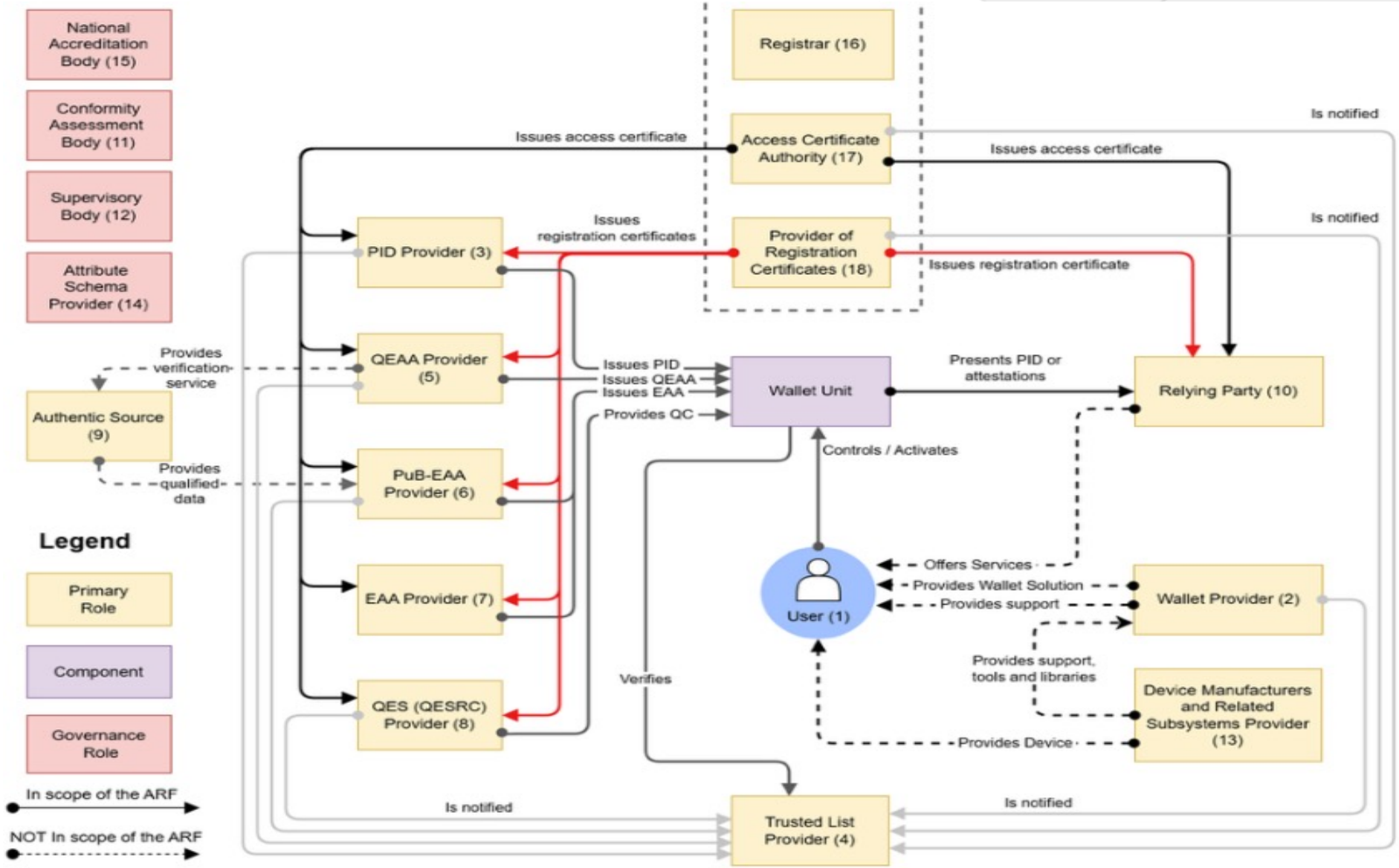
Recommandation 2021/946 de la Commission Européenne d'une action coordonnée européenne en vue de développer une boite à outils commune de l'Union

ARF – un ensemble de normes et de spécifications techniques communes ainsi qu'un ensemble de lignes directrices et de bonnes pratiques communes

La mise en œuvre technique et graduelle

	2023	2024	2025	2026	2027	2030
Europe	eIDAS 1.0 (from 2014) still effective	**April: eIDAS 2.0 regulation adopted**	Implementing regulation on trust services adopted	**States must propose at least one EUDIW**	**Private and public services must accept EUDIW as a means of authenticat./ identification**	**Objective of EU Comm.: 80% of europ. citizens equipped with an EUDIW**
Toolbox expert group	Architecture Reference Framework ARF v1		**ARF v2**	ARF updating		
Large Scale Pilots (LSP)	1st LSP – use case, Technical specification of the EUDIW (->2025)		2nd LSP (e.g. APTITUDE) - Testing & Feedback			

ARF V2 (ARCHITECTURE AND REFERENCE FRAMEWORK)



LES ATTESTATIONS

DES INFORMATIONS NUMÉRIQUES VÉRIFIÉES, POTENTIELLEMENT VÉRIFIABLES PAR UN TIERS

Les attestations : des informations numériques vérifiées, vérifiables par un tiers

Type d'attestation : carte d'identités, diplôme, permis de conduire, preuve d'âge…

Attestations d'attributs électroniques qualifiées et non qualifiées (QEAA et EAA)

Fournisseur de PID (Person Identification Data) et d'attestations : attestations délivrées par des entités de confiance (ex : gouvernement, banque, université)

Suit des modèles de données et des règles d'attestation

Attestations obtenues *(issuance)* d'un fournisseur d'attributs faisant ou pas appel à une source authentique et stockées dans EUDIW

Attestations présentées *(presentation)* par PEIN au fournisseur de service *(relying party)* avec la nécessité de démontrer que l'attestation a été émise par une entité de confiance *(Trusted List)* et que l'utilisateur du PEIN en est bien le propriétaire

Présentation de proximité ou en ligne

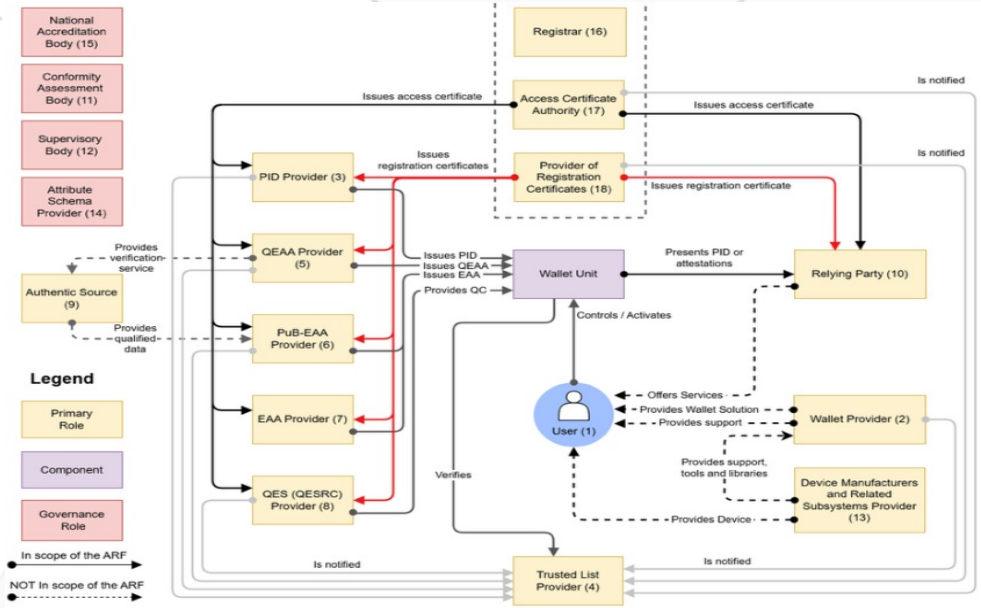
La problématique de : la minimisation de données, du pseudonymat, de la révocation et du respect de la vie privée (non traçabilité, non réidentification)

LES SERVICES DE CONFIANCE

Plusieurs services concernés : signature électronique qualifiée ou non, cachet électronique qualifié ou non, horodatage qualifié ou non, envoi recommandé qualifié ou non, attestation d'attributs qualifiée ou non

Qualifié = même effet juridique qu'un document légal sur papier

Les prestataires « qualifiés » sont soumis à des exigences et des obligations de sécurité renforcées et doivent obtenir le statut « qualifié » d'un organe de contrôle



LA GOUVERNANCE

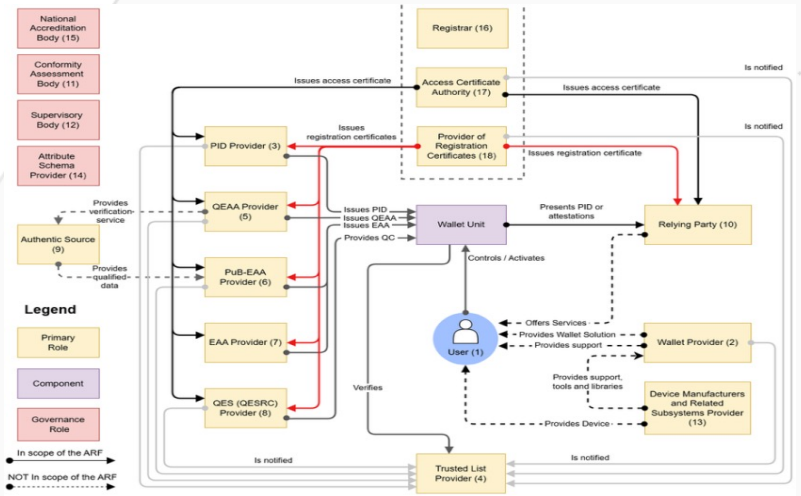
LES ENTITÉS EN RESPONSABILITÉ

Organisme national d'accréditation (NAB) : organisme désigné par un EM pour accréditer des organismes CAB

Organismes d'évaluation de la conformité (CAB) : organismes publics ou privés accrédités pour certifier les solutions de portefeuille et pour auditer périodiquement les prestataires de services de confiance qualifiés – permettent aux EM de délivrer une solution PEIN et d'attribuer le statut « qualifié » à un prestataire de services de confiance

Autorités de surveillance : autorités créées et désignées par les EM pour contrôler le bon fonctionnement des fournisseurs de PEIN et des acteurs de l'écosystème PEIN

Fournisseur de schéma d'attestation : définit le règlement d'attestation (QEAA, EAA…) lisible par une machine et par un humain.



LES EXIGENCES (SHALL, SHOULD, MUST)

PLUS DE 100 PAGES D'EXIGENCES

Fournisseurs légitimes (fournisseurs de PEIN, certificat d'enregistrement, QEAA…)

Services légitimes rendus par des fournisseurs (attributs, signatures, partie utilisatrice)

Authenticité des entités en interaction (PEIN, partie utilisatrice, fournisseur de QEAA…)

Impossibilité de falsifier la présentation des attributs par l'utilisateur

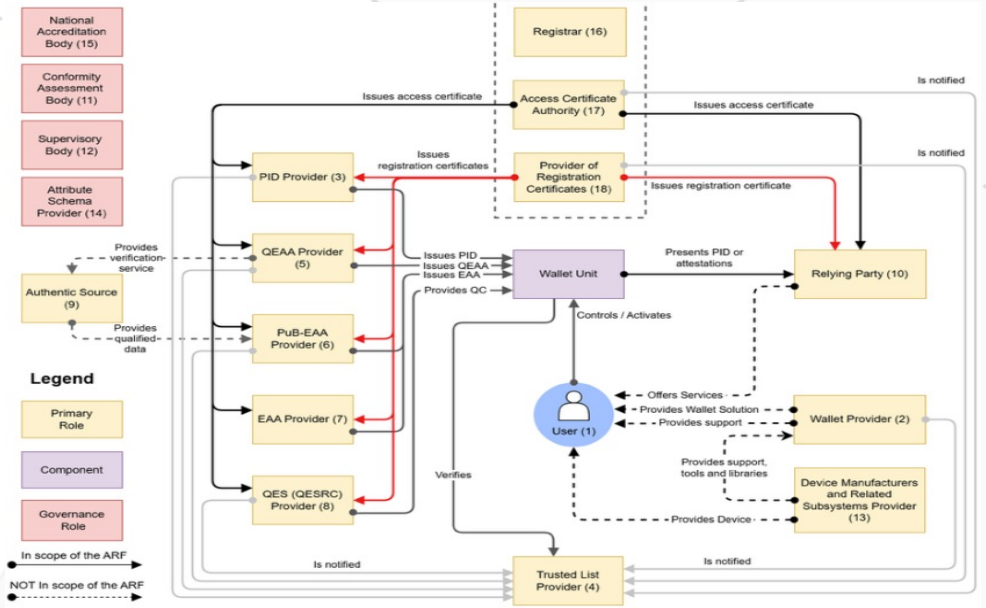
Présentation à proximité et à distance des attestations PID/attributs

Révocation des PID/attributs

Minimisation de données

Niveau d'assurance élevé pour la mise en œuvre du PEIN

Cf. https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md#161-changed-formats-for-annex-2



LE QUESTIONNEMENT

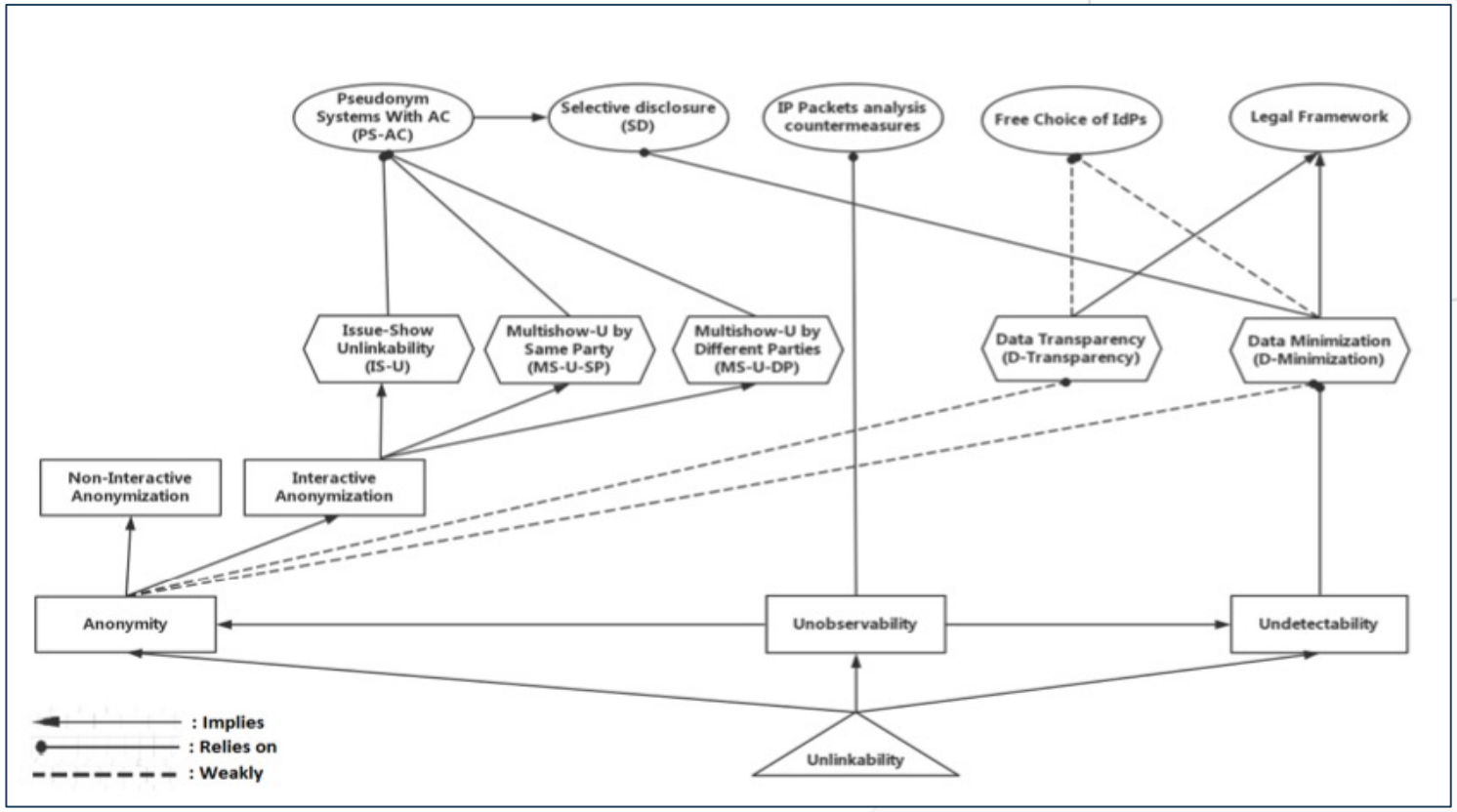
LA SÉCURITÉ DES PORTEFEUILLES N'EST PAS FIABLE À 100%

- Une multitude d'acteurs privés impliqués (composants technologiques, déploiement/administration des portefeuilles NDI) -> risque de failles de sécurité et de fuites de données (cf. PEGASUS 2021 sur les smartphones, RSA Security 2013 sur les puces cryptographiques)
- Des enjeux de souveraineté avec une implication quasi inexistante des entreprises de l'UE sur les technologies du smartphone : matériel (Apple, Google, Samsung), système d'exploitation (Google ou Apple)
- Les normes et les certifications ne sont pas une garantie (ex : une puce Infineon certifiée, mais avec un générateur de clés défectueux - rappel de 750 000 cartes d'identité citoyennes par le gouvernement estonien en 2017)
- Des usages parfois sensibles (pour voter aux élections présidentielles)
- L'objet PEIN très attractif pour les pirates informatiques (attaques massives possibles à l'échelle nationale, qualité des données – non déclaratives - hébergées sur PEIN)
- PEIN comme vecteur de divulgation de données personnelles et comme moyen d'usurpation d'identité

LE QUESTIONNEMENT

LE RESPECT DE LA VIE PRIVÉE

- La propriété centrale est la « non-liabilité » *(unlinkability)* : ne pas pouvoir relier deux items entre eux (l'identité d'une personne et une transaction, son identité et un attribut, deux transactions…)



Source: LP Sondeck (2016)

LE QUESTIONNEMENT

LE CAS DU PSEUDONYMAT

- 3 formes de pseudonymat dans ARF v2 : vérifiable, attesté, « scope rate »
  - Pseudonyme vérifiable : l'utilisateur prouve qu'il est détenteur de ce pseudo et s'authentifie
  - Pseudonyme attesté : vérifiable + un tiers atteste le lien que le pseudo appartient à l'utilisateur
- Difficulté - la validité d'une attestation d'attributs liée à l'identité principale :
  - Apporter une garantie à la partie utilisatrice (PU) que l'utilisateur est détenteur de l'attestation
  - Eviter que le lien soit fait entre le pseudonyme et la véritable identité de l'utilisateur (PID)
  - L'utilisateur se présente au PU avec son pseudonyme vérifiable, et il veut prouver qu'il est détenteur d'une attestation EAA/QEAA établie pour son identité principale, sans dévoiler cette dernière => pas d'assurance qu'il y ait un lien entre l'attestation et le pseudo, risque que l'attestation ne soit pas celle de l'utilisateur, risque que des attributs soient assignés à un utilisateur de façon illégitime
- Alternative - demander que l'attestation d'attributs soit liée au pseudonyme :
  - Lourdeur : besoin de demander au fournisseur d'attributs une attestation pour chaque pseudo
  - Risque sur la vie privée : le fournisseur d'attributs connait les pseudos de l'utilisateur
- Plus généralement :
  - Pas de vie privée si le PEIN transmet un numéro unique à chaque interaction
  - La moindre fuite à n'importe quel niveau du PEIN (ex : application, système, constructeur du smartphone, opérateur) a une incidence sur la vie privée

LE QUESTIONNEMENT

LA GOUVERNANCE

- Besoin critique que l'Europe maitrise les technologies au vu des usages prévus (ex : passage aux frontières, sécurité sociale et d'autres à venir) et de l'aspect pratique du portefeuille dans les interactions numériques
- Les GAFAM sont sur les rangs pour proposer un PEIN (technologies de smartphones et de présentation d'attestations sophistiquées)
- => Risque de perte de souveraineté technologique (ingérence, déni de service…)

- Risque que certains Etats marchandent la citoyenneté européenne (c'est déjà le cas)

RÉFLEXION

TOUT EST DANS L'IMPLÉMENTATION ET LA GOUVERNANCE

- La transparence du code pour plus de confiance en mettant le code source à disposition de la communauté scientifique
- Mieux : encourager la communauté scientifique et universitaire à proposer un portefeuille en open source, susceptible d'être reconnu par certains EM et utilisé par les citoyens et résidents de l'UE
- Un suivi très strict de la mise en œuvre : des audits par des entités indépendantes
- Un suivi encore plus strict du respect de la vie privée (ex. : la mise en œuvre du pseudonymat) dans une société où la marchandisation des données personnelles est monnaie courante
- Des sanctions fortes qui soient appliquées
- De la souveraineté dans le choix des solutions PEIN retenues
- Et il faudrait toujours avoir en tête… un plan B

MERCI

Pour plus d'informations et rejoindre l'action transverse du CNRS "Sécurité Informatique et Sciences Humaines et Sociales"

=>

À la croisée entre le GDR Sécurité Informatique et le GDR Internet, IA et Société du CNRS