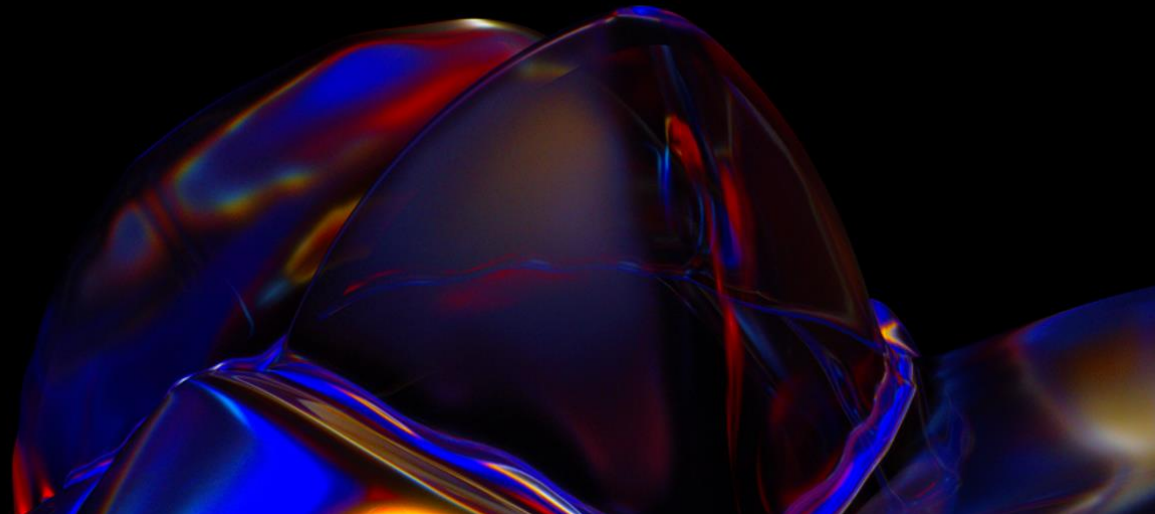

FIC
Forum International
de la Cybersécurité
du 5 au 7 avril 2023
à Lille Grand Palais

Portefeuille européen d'identité numérique

Principaux enjeux juridiques

FIC
Forum International de la Cybersécurité



Enseignante-chercheuse en droit

►Télécom Paris, département Sciences économiques et sociales
►Institut Interdisciplinaire de l'Innovation (I3), unité mixte du CNRS

Coordinatrice de la Chaire Valeurs et Politiques des Informations Personnelles (VP-IP) de l'IMT

Titulaire de la Chaire Économie des Communs de Données

Responsable du projet Living Lab 5 G en gare de Rennes

Membre

►Comité Pilote d'éthique du numérique rattaché au Comité Consultatif National d'Éthique pour les sciences de la vie et de la santé (CCNE)
►Comité d'éthique sur les données et l'IA d'Orange
►*Data Protection and Ethics Panel* d'Axa

Accompagner la transformation numérique à l'échelle européenne

- Disposer d'une identité numérique fiable afin d'accéder à des services de plus en plus dématérialisés
- Permettre la continuité d'activité pour les citoyens et les entreprises
  - Dans une multitude de contextes : e-santé, pass sanitaire, paiements et vote en ligne …

Rôle primordial de l'identité numérique dans le monde physique et virtuel

- Construction et détermination de nos interactions sociales, économiques ou politiques

Des identités numériques dispersées (sondage Chaire VP-IP 2019)

- 75% des répondants disposent de plusieurs adresses mails
- 60% utilisent des pseudonymes
- 31% recourent à une fausse identité, avec un faux nom et prénom

Sécurité	• Usurpation d'identité • Fraude : vote en ligne • Manipulation des opinions
Pouvoir de marché des plateformes	• Identité Google, Facebook Connect, Apple ID, Microsoft disponible à l'échelle mondiale • Identités privées, simples d'utilisation, et souvent déclaratives
Liberté de choix	• Respect de la vie privée • Transparence • Application du RGPD
Souveraineté	• Rôle des États • Rôle du secteur privé : banque, opérateur télécom … • Rôle de l'Union européenne

L'AMBITION POLITIQUE : LE PORTEFEUILLE EUROPÉEN D'IDENTITÉ NUMÉRIQUE (PEIN)

Garantir l'accès à une identité électronique

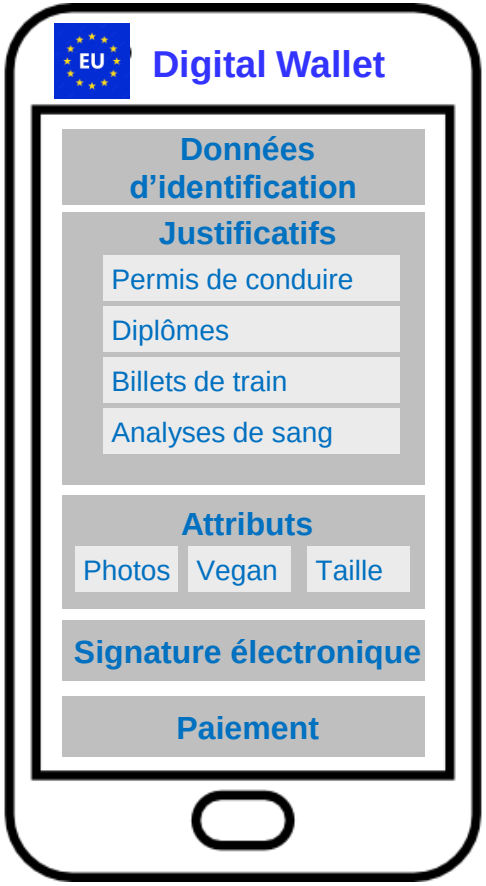
- ▶Hautement sécurisée et fiable
- ▶Utilisable partout dans l'Union européen
- ▶Sur des smartphones et d'autres terminaux

Au moins 80% des personnes

- ▶Physiques et morales

Sous le contrôle de l'utilisateur

En ligne et hors ligne



UNE CONSTRUCTION PAR ÉTAPES DANS LE CADRE DU MARCHÉ INTÉRIEUR NUMÉRIQUE

Signature électronique

1999

Directive n° 1999/93/CE

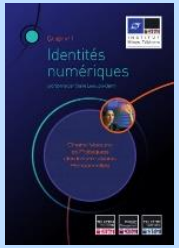
portant sur un cadre communautaire pour les signatures électroniques

eIDAS 1

2014

Règlement (UE) n° 901/2014

sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur



eIDAS 2

Juin 2021

Proposition de règlement

modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique

CALENDRIER

Législation : proposition de règlement eIDAS 2

Spécifications : Architecture and Reference Framework

Développement

Déploiement

Sélection d'un consortium pour développer les **briques du PEIN** et les mettre à disposition des États membres

Sélection de 4 consortiums pour tester les **spécifications techniques du PEIN** et implémenter les **cas d'usage** interopérables

Commission européenne

Proposition

ARF

Architectural and Reference Framework

Version intermédiaire

Objectifs, nécessités fonctionnelles et composantes

Conseil de l'UE

Orientation générale

ARF

Architectural and Reference Framework

Parlement européen

Rapport (2 mars 2023)

Mandat de négociation (16 mars 2023)

1. L'APPROCHE FONCTIONNELLE

1.1. L'AUTHENTIFICATION DE L'UTILISATEUR

1.2. LES SERVICES DE CONFIANCE

Institut Mines-Télécom

1. L'APPROCHE FONCTIONNELLE

1.1. L'AUTHENTIFICATION DE L'UTILISATEUR

Institut Mines-Télécom

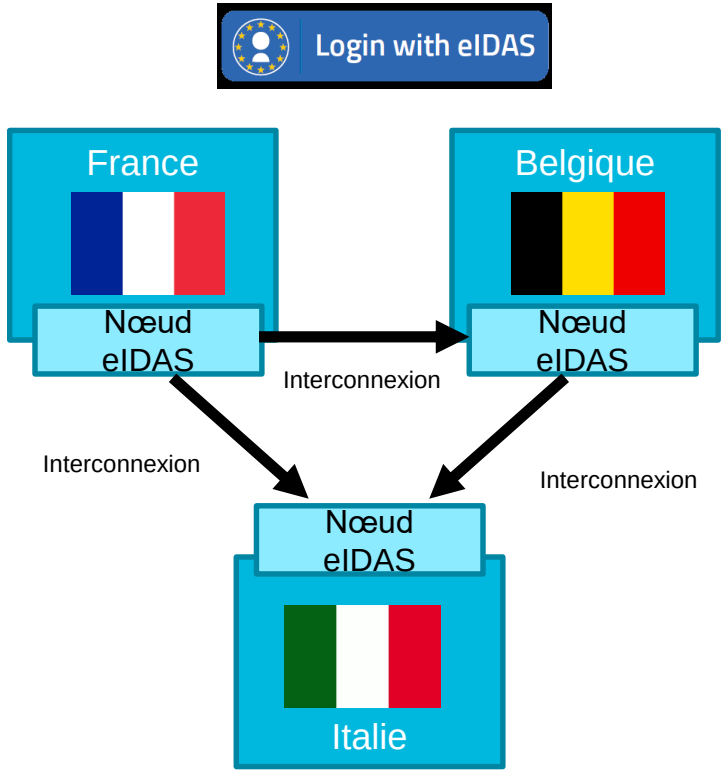
Identité numérique : une compétence nationale

►L'Union européenne ne peut pas obliger les États à mettre en place des systèmes nationaux d'identification électronique

- Par exemple en créant une carte d'identité européenne électronique
- Ou en établissant un système européen de gestion de l'identité numérique

Marché intérieur : une compétence de l'UE

►L'UE peut intervenir afin que les systèmes d'identification électronique nationaux prennent une dimension européenne en les interconnectant



Pour s'interconnecter, les systèmes nationaux d'identification électronique doivent présenter des caractéristiques communes

►4 actes d'exécution dont un règlement d'exécution qui définit le cadre d'interopération basé sur des spécifications techniques communes et des normes

Une procédure permet de s'assurer qu'un schéma d'identification électronique respecte les spécifications techniques communes

►Notification par l'État à la Commission européenne du **schéma d'identification électronique**
►**Revue par les « pairs »**
►Publication au journal officiel de l'UE de la liste des schémas nationaux notifiés

Reconnaissance mutuelle

►**Un État A ne peut pas refuser l'utilisation du moyen d'identification électronique notifié par un État B *dans certains cas***

SCHÉMAS NATIONAUX D'IDENTIFICATION ÉLECTRONIQUE : VUE D'ENSEMBLE

Carte physique, inscription
Ordinateur, smartphone

Émetteur
public ou privé

3 niveaux
de garantie

Title	Member State	Title of the scheme	eID means under the scheme	Level of assurance	Status	Date	OJEU
Liechtenstein	Liechtenstein	eID.li	eID.li, Class A eID.li, Class B	Substantial, High	NOTIFIED		
Slovenia	Slovenia	Slovenian eID card scheme	SI eID card	High	PRE-NOTIFIED		
Czech Republic	Czech Republic	National identification scheme of the Czech Republic	CZ eID card	High	NOTIFIED	13 Sep 2019	2019/C 309/09
Estonia	Republic of Estonia	Estonian eID scheme: ID card Estonian eID scheme: RP card Estonian eID scheme: Digi-ID Estonian eID scheme: e-Residency Digi-ID Estonian eID scheme: Mobiil-ID Estonian eID scheme: diplomatic identity card	— ID card — RP card — Digi-ID — e-Residency Digi-ID — Mobiil-ID — Diplomatic identity card	High	NOTIFIED	07 Nov 2018	2018/C 401/08
France	French Republic	French eID scheme "FranceConnect+ / The Digital Identity La Poste"		Substantial	NOTIFIED	02 Feb 2021	2021/C 522/03
Italy - eID	Republic of Italy	Italian eID based on National ID card (CIE)	Italian eID card (Carta di Identità elettronica)	High	NOTIFIED	13 Sep 2019	2019/C 309/09
The Netherlands (DigiD)	The Kingdom of the Netherlands	DigiD	DigiD Substantieel DigiD Hoog	Substantial, High	NOTIFIED	21 Aug 2020	2020/C 276/02
Sweden	The Kingdom of Sweden	Swedish eID (Svensk elegitimation)	BankID Freja eID (Notified) EFOS	Substantial and High	NOTIFIED	14 Dec 2020	2022/C 78 I/02
Portugal - Sistema de Certificação de Atributos Profissionais	The Portuguese Republic	Sistema de Certificação de Atributos Profissionais	Professional Attributes Certification System		PRE-NOTIFIED	30 May 2018	
Spain	The Kingdom of Spain	Documento Nacional de Identidad electrónico (DNIe)	Spanish ID card (DNIe)	High	NOTIFIED	07 Nov 2018	2018/C 401/08
Malta	Malta	Identity Malta	Maltese eID card and e-residence documents	High	NOTIFIED	04 Mar 2021	2021/C 522/03
Poland	Poland	Public Electronic Identification System	Trusted profile, personal profile	Substantial, High	NOTIFIED		
Latvia	Latvia	Latvian eID scheme (eID)	eID karte	Substantial, High	NOTIFIED	18 Dec 2019	2019/C 425/06

UNE NOTIFICATION FRANÇAISE

Please find below information about the pre-notified and notified eID schemes under eIDAS:

Titre	Member State	Title of the scheme	eID means under the scheme	Level of assurance	Status	Date
Liechtenstein	Liechtenstein	eID.li	eID.li, Class A eID.li, Class B	Substantial, High	NOTIFIED	
Slovenia	Slovenia	Slovenian eID card scheme	SI eID card	High	PRE-NOTIFIED	
Czech Republic	Czech Republic	National identification scheme of the Czech Republic	CZ eID card	High	NOTIFIED	13 Sep 2019
			— ID card — RP card — Digi-ID — e-Residency Digi-ID — Mobiil-ID — Diplomatic identity card	High	NOTIFIED	07 Nov 2018
France	French Republic	French eID scheme "FranceConnect+ / The Digital Identity La Poste"		Substantial	NOTIFIED	02 Feb 2021
Italy - eID	Republic of Italy	Italian eID based on National ID card (CIE)	Italian eID card (Carta di Identità elettronica)	High	NOTIFIED	13 Sep 2019
The Netherlands (DigiD)	The Kingdom of the Netherlands	DigiD	DigiD Substantieel DigiD Hoog	Substantial, High	NOTIFIED	21 Aug 2020
Sweden	The Kingdom of Sweden	Swedish eID (Svensk elegitimation)	BankID Freja eID (Notified) EFOS	Substantial and High	NOTIFIED	14 Dec 2020
Portugal - Sistema de Certificação de Atributos Profissionais	The Portuguese Republic	Sistema de Certificação de Atributos Profissionais	Professional Attributes Certification System		PRE-NOTIFIED	30 May 2018
Spain	The Kingdom of Spain	Documento Nacional de Identidad electrónico (DNIe)	Spanish ID card (DNIe)	High	NOTIFIED	07 Nov 2018
Malta	Malta	Identity Malta	Maltese eID card and e-residence documents	High	NOTIFIED	04 Mar 2021
Poland	Poland	Public Electronic Identification System	Trusted profile, personal profile	Substantial, High	NOTIFIED	
Latvia	Latvia	Latvian eID scheme (eID)	eID karte eParaksts karte	Substantial, High	NOTIFIED	18 Dec 2019

SCHÉMAS NATIONAUX D'IDENTIFICATION ÉLECTRONIQUE : 3 NIVEAUX DE GARANTIE

Belgium - eID	The Kingdom of Belgium	Belgian eID Scheme FAS / eCards	Belgian Citizen eCard Foreigner eCard	High	NOTIFIED	27 Dec 2018
Italy - SPID	Republic of Italy	SPID – Public System of Digital Identity	SPID eID means provided by: • Aruba PEC	Low, Substantial, High	NOTIFIED	10 Sep 2018

Niveau	Objectif	L'exemple des facteurs d'authentification
Garantie Faible	Réduire le risque d'utilisation abusive ou d'altération de l'identité	1 facteur : Ex. : un mot de passe
Garantie Substantielle	Réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité	2 facteurs : Ex. : mot de passe + code temporaire envoyé par SMS
Garantie Élevée	Empêcher l'utilisation abusive ou l'altération de l'identité	Subtantielle + protéger des attaquants à potentiel d'attaque élevé Ex : utilisation du titre d'identité électronique

eIDAS 2

- PEIN de garantie élevée mais discussion
- Revue par les pairs et/ou certification

1. L'APPROCHE FONCTIONNELLE

1.2. LES SERVICES DE CONFIANCE

Institut Mines-Télécom

1. S'identifier/authentifier auprès d'une « partie utilisatrice »

► « Une personne physique ou morale qui se fie à un moyen d'identification électronique, y compris les portefeuilles européens d'identité numérique, ou à un service de confiance »

2. Obtenir et partager des attestations électroniques d'attributs

►En recourant à un prestataire de services de confiance délivrant des attestations électroniques d'attributs

►L'attestation va permettre l'authentification d'attributs

3. Signer au moyen de signatures électroniques

►En recourant à un prestataire de services de confiance de signatures électroniques de niveau qualifiée

Le prestataire de confiance

- Respecte les exigences de sécurité définies par le règlement eIDAS
- Prend les mesures adéquates pour gérer les risques liés à la sécurité
  - En particulier : obligation de notification de toute atteinte à la sécurité ou de perte d'intégrité « ayant une incidence importante sur le service de confiance fourni ou sur les données personnelles qui y sont conservées» dans les 24 h (ANSSI)

Le prestataire de confiance qualifié

- Fournit les services de confiance non qualifiés et qualifiés
- Car il respecte des exigences de sécurité renforcée
  - Prendre des mesures appropriées concernant les preuves à produire en justice
  - Tient à jour une base de données relative aux certificats
  - Bénéficie d'un système d'assurance responsabilité
  - Assure la continuité du service

Statut attribué par l'organe de contrôle (ANSSI)

- Figure sur une liste de confiance

5 SERVICES DE CONFIANCE EN 2014

Services	Niveaux de confiance		
			Délivré par un prestataire de services de confiance qualifié
Signature électronique Création, vérification, validation, conservation des signatures et certificats	**Simple**	**Avancé**	**Qualifié** Reconnue et acceptée dans tous les États Effet juridique équivalent à celui d'une signature manuscrite
Cachet électronique Pour les personnes morales			
Horodatage électronique Création, vérification, validation des certificats	**Simple**		**Qualifié** : signé au moyen d'une signature ou d'un cachet électronique avancée Reconnu et accepté dans tous les États Présomption d'exactitude de la date, de l'heure et de l'intégrité des données Effet juridique identique au même service ramené au papier
Service d'envoi recommandé électronique Création, vérification, validation des certificats	**Simple**		**Qualifié**
Authentification de site web Création, vérification, validation des certificats	**Simple**		**Qualifié**

4 NOUVEAUX SERVICES DE CONFIANCE

Services	Niveaux de confiance		
		Délivré par un prestataire de services de confiance qualifié	
Archivage électronique	**Simple**	**Qualifié** Étend la fiabilité du document électronique au-delà de la période de validité technologique Présomption concernant l'intégrité des données et documents archivés, leur disponibilité, traçabilité, exactitude et origine ainsi que l'identification des utilisateurs	
Création de signature et de cachet électronique à distance Gestion	**Simple**	**Qualifié**	
Registre électronique Enregistrement	**Simple**	**Qualifié** Présomption quant au caractère univoque et à l'authenticité des données qu'il contient, à l'exactitude de la date et de l'heure de ces données et à leur classement chronologique séquentiel dans le registre	Supprimé par le Parlement européen
Attestation électronique d'attributs Création, validation, vérification = authentification d'attributs	**Simple**	**Qualifié** Reconnue et acceptée dans tous les États Même effet juridique qu'une une attestation délivrée légalement sur papier	

Attribut

- « Une particularité, une caractéristique ou une qualité d'une personne physique ou morale ou d'une entité, sous forme électronique »

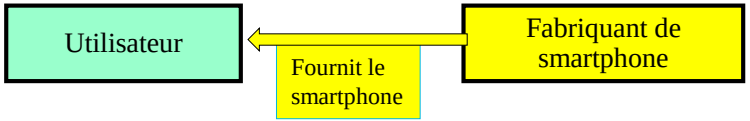
Vérification auprès de sources authentiques

- Le prestataire de confiance qualifié qui délivre une attestation électronique d'attributs qualifiée doit pouvoir vérifier auprès d'un « répertoire ou d'un système, administré sous la responsabilité d'un organisme du secteur public ou d'une entité privée »
- À la demande de l'utilisateur
- L'authenticité **a minima de 9 types d'attributs**

Adresse, 2. Age, 3. Sexe, 4. État civil, 5. Composition de la famille,
6. Nationalité
7. Diplômes, titres, certificats du système éducatif
8. Permis et licences détenues par l'utilisateur
9. Fourniture des informations financières et des données d'entreprises

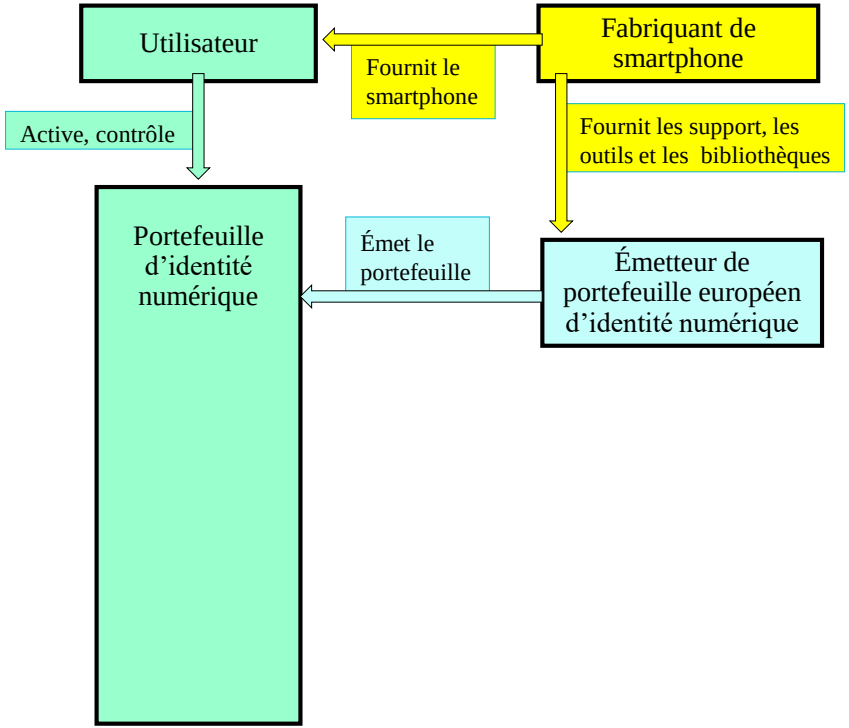
En France

2. 3. 4. Répertoire national d'identification des personnes physiques
8. Fichier National des Permis de Conduire

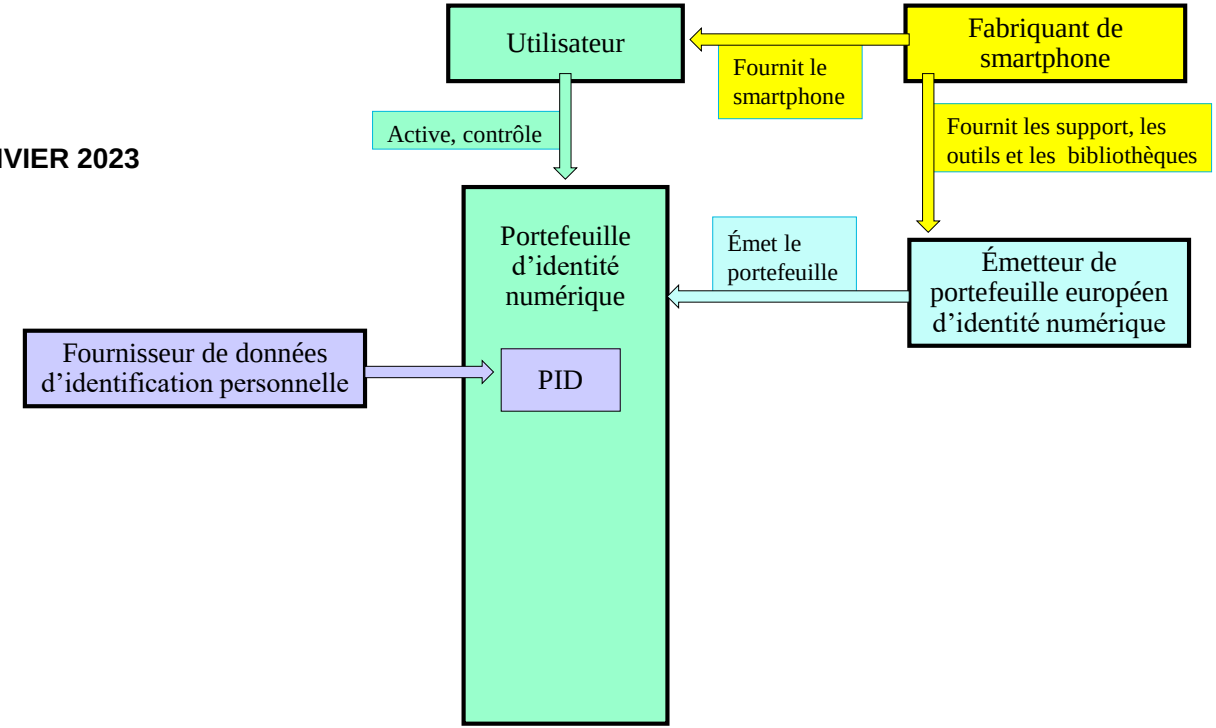


SOURCE : ARF JANVIER 2023

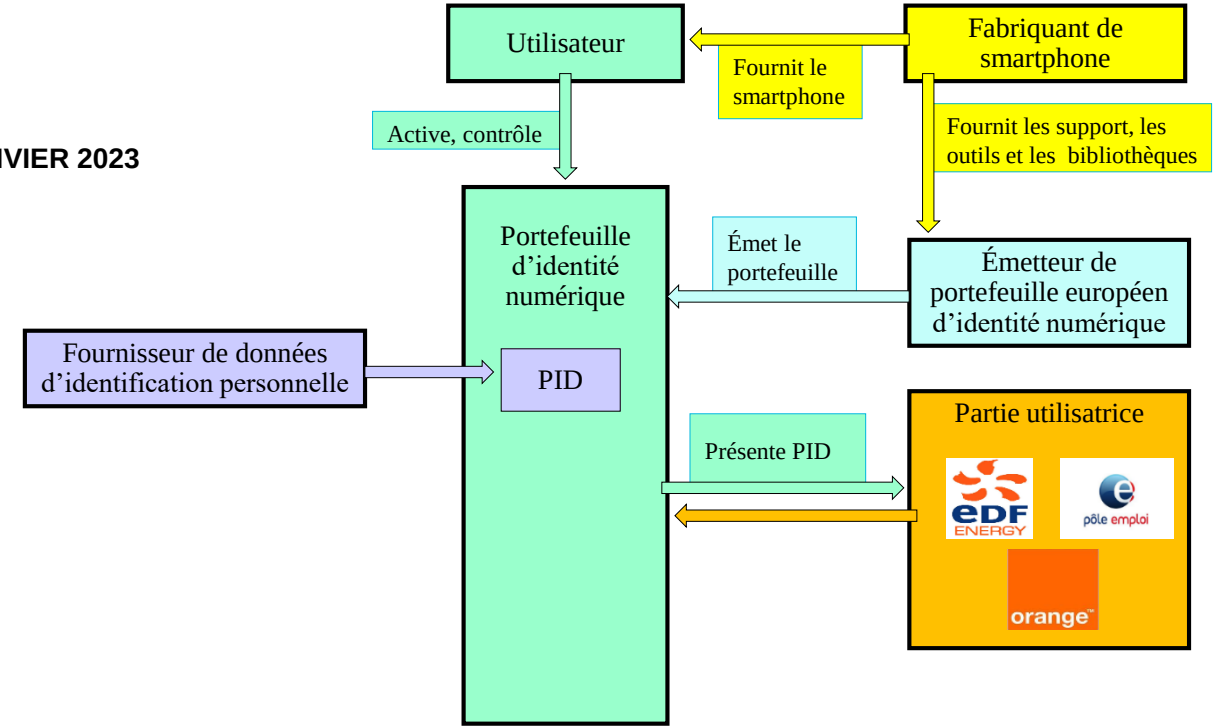
SOURCE : ARF JANVIER 2023



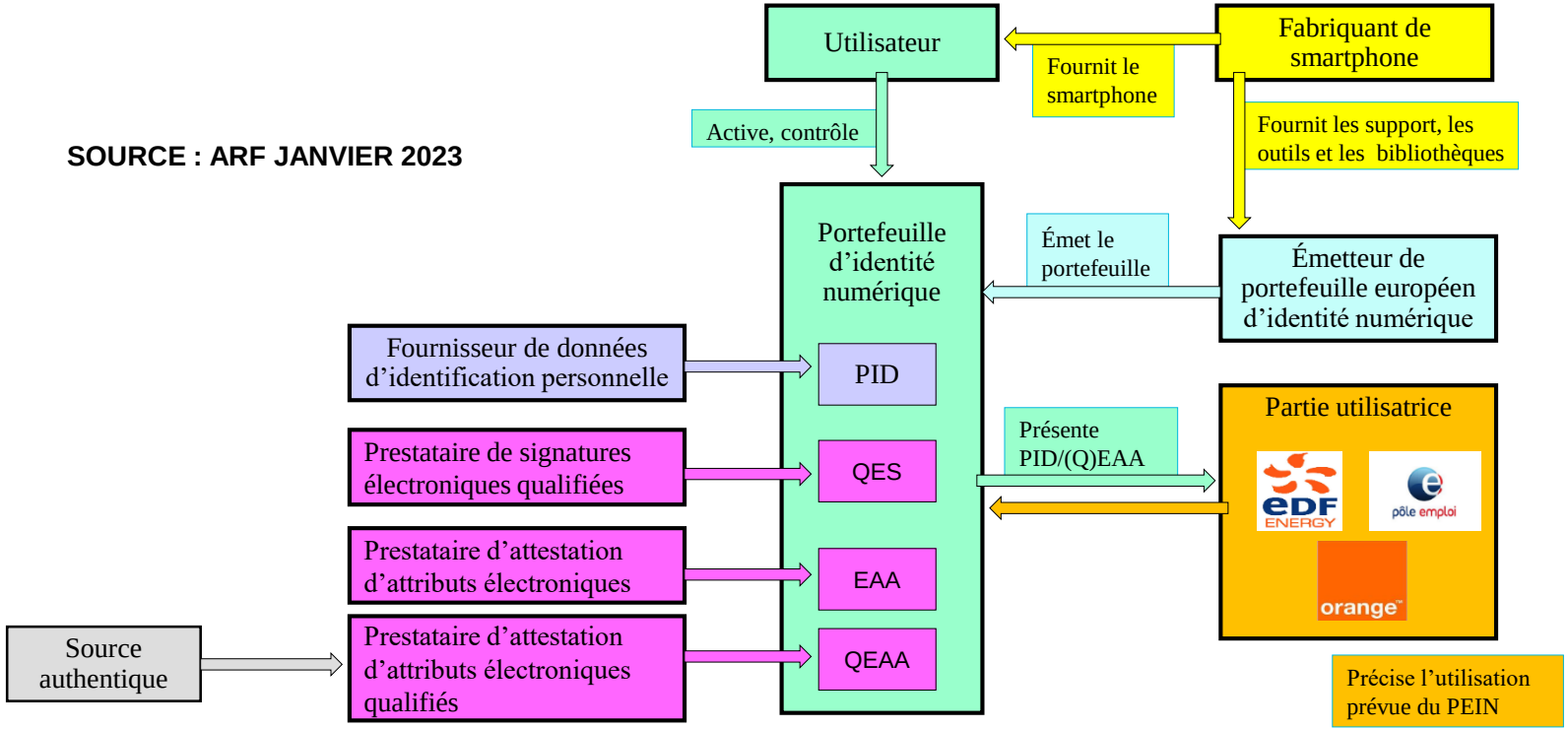
SOURCE : ARF JANVIER 2023



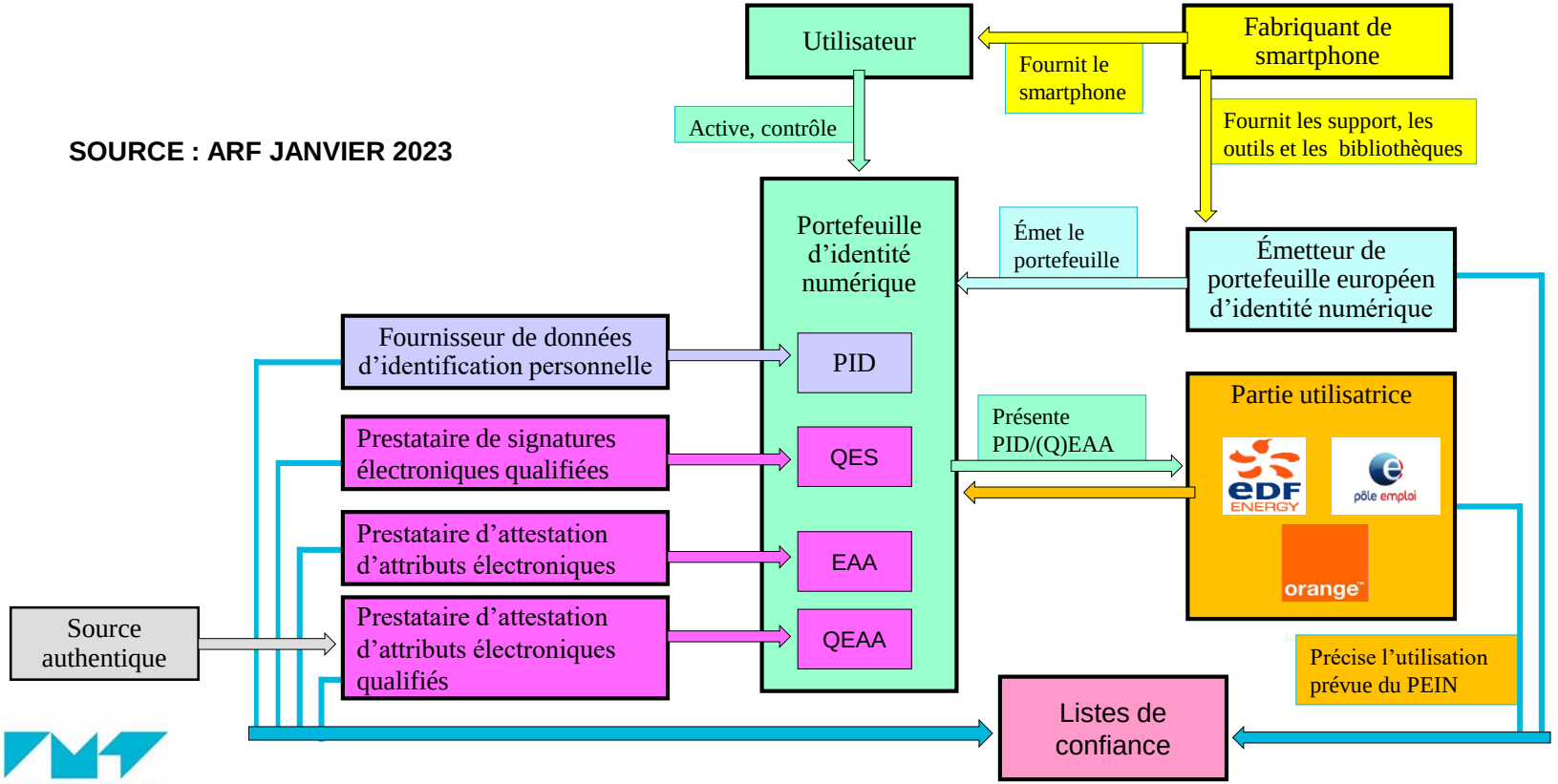
SOURCE : ARF JANVIER 2023



SOURCE : ARF JANVIER 2023



SOURCE : ARF JANVIER 2023



2. L'APPROCHE CRITIQUE

2.1. LA LIBERTÉ DE L'UTILISATEUR

2.2. LA MISE EN ŒUVRE DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES

2.3. LE RECOURS À LA CERTIFICATION

2.4. LA QUESTION DE LA SOUVERAINETÉ

Institut Mines-Télécom

2. L'APPROCHE CRITIQUE

2.1. LA LIBERTÉ DE L'UTILISATEUR

Institut Mines-Télécom

Cristian Terheş, député européen, Commission LIBE, 18 mai 2021

- « Telle que cette proposition [de règlement eIDAS 2 de la Commission européenne] est envisagée, elle **conduirait à la chinifisation/sinisation de l'Europe, permettant la création d'un système de crédit social similaire** qui déterminerait la surveillance et le contrôle de masse de tous les européens, ce qui ne doit pas être accepté ».

- « As this proposal is envisioned, it would lead to the Chinafication of Europe, allowing for the creation of a like social-credit system that would determine the mass surveillance and control of all Europeans, which must not be accepted. EU was envisioned as an “area of freedom” and efforts must be continued to keep it as such ».
- DRAFT OPINION of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on Industry, Research and Energy on the proposal for a regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, (COM(2021)0281 – C9 0200/2021 – 2021/0136(COD)), Rapporteur for opinion: Cristian Terheş, 2021/0136(COD), 18.5.2022, https://www.europarl.europa.eu/doceo/document/LIBE-PA-732601_EN.pdf.

Est tenu(e) d'accepter l'utilisation du PEIN

- ►Un **organisme public** qui fournit un service en ligne est tenu d'accepter l'utilisation d'un PEIN
- ►Une **très grande plateforme** qui exige que ses utilisateurs s'authentifient est tenue d'accepter l'utilisation du PEIN
  - ■ Cf. Règlement sur les marchés numériques (Digital Market Act - DMA)

N'est pas tenue d'accepter l'utilisation du PEIN

►Une partie utilisatrice privée

Sauf si elle

►**Relève de certains secteurs** : transport, énergie, services bancaires et financiers, sécurité sociale, santé, eau potable, services postaux, infrastructures numériques, éducation, télécommunications

►**Et que le droit national, le droit de l'UE ou une obligation contractuelle exige une authentification forte**

- ■ Utilisation d'au moins 2 éléments indépendants appartenant aux catégories 'connaissance de l'utilisateur', 'possession' et 'inhérence'

Le cout du format numérique

►Commission européenne

- L'utilisation du PEIN est gratuite pour les personnes physiques

►Conseil de l'UE

- L'utilisation du PEIN est gratuite **pour l'authentification par les personnes physiques**
- Les services reposant sur l'utilisation du portefeuille peuvent entraîner des coûts, par exemple la délivrance des attestations électroniques d'attributs au portefeuille

►Parlement européen

- La délivrance et l'utilisation du PEIN est **gratuite pour toutes les personnes physiques et morales**
- Les utilisateurs doivent obtenir la **signature électronique qualifiée, gratuitement et par défaut**
- Le prestataire qualifié d'attestations électroniques d'attributs doit pouvoir vérifier gratuitement l'authenticité de l'attribut auprès d'une source authentique dans le secteur public

La liberté d'utiliser des documents physiques

►Commission européen

- Ne précise pas que les portefeuilles ne peuvent être qu'un complément aux documents physiques
- Discrimination : difficulté pour certaines personnes à utiliser un dispositif numérique

►Parlement européen

- Précise que l'utilisation du PEIN est volontaire.
- Sa non utilisation ne doit pas constituer un désavantage

Importance de disposer d'identités multiples selon les contextes

- Permet notamment d'assurer la liberté d'expression ou la non-discrimination
  - Cf politique des noms réels

Non reconnaissance par la Commission européenne

- Article 5. « Sans préjudice de l'effet juridique donné aux pseudonymes en droit national, **l'utilisation de pseudonymes dans les transactions électroniques n'est pas interdite** ».

Reconnaissance par le Parlement européen

- **Article 5, §2**. : Sans préjudice de l'effet juridique accordé aux pseudonymes en vertu du droit national et à moins que des règles spécifiques de l'Union ou du droit national n'imposent aux utilisateurs de s'identifier à des fins juridiques, **l'utilisation de pseudonymes dans les transactions électroniques, librement choisis par l'utilisateur, est toujours autorisée** et n'est pas interdite ou restreinte par un contrat ou les conditions générales applicables à l'utilisation du service.
- **Article 6a. :** Les PEIN permettent à l'utilisateur de générer des pseudonymes et de les stocker de manière cryptée et locale en son sein

2. L'APPROCHE CRITIQUE

2.2. LA MISE EN ŒUVRE DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES

Institut Mines-Télécom

Principe de minimisation des données

- Les portefeuilles doivent permettre la **divulgation sélective des attributs aux parties utilisatrices**
  - Cette fonctionnalité doit devenir un élément de conception de base
- L'utilisateur doit pouvoir **contrôler la quantité de données transmises**
  - Ex. : si un service exige la preuve de l'âge, divulguer uniquement l'année de naissance
- Rien sur l'utilisation des métadonnées : Ex. : au lieu de communiquer une année de naissance pour acter sa majorité, communiquer la métadonnée : « Plus de 18 ans »

Principe de nécessité

- Les émetteurs de moyens d'identification électronique et d'attestations électroniques d'attributs ne doivent pas croiser des données personnelles provenant d'autres services

Garanties techniques et organisationnelles

- Les données personnelles relatives à la fourniture des portefeuilles ou de services d'attestation électronique d'attributs doivent être maintenues séparées
- Le **prestataire d'attestation d'attributs qualifiée** doit fournir ses services dans le cadre d'une entité juridique distincte

Les mineurs, personnes sous tutelle, curatelle, décédées

Le principe de transparence, droit d'accès aux données, droit d'information

►Pourtant l'information sur les attributs exigés conditionne la validité du consentement

La durée de conservation des données

Les données sensibles de santé, origine raciale ou ethnique

►Les données biométriques doivent simplement faire l'objet de mesures « proportionnées au risque »

►Ces données représentent une caractéristique univoque d'une personne et sont utilisées dans de nombreuses applications à des fins d'authentification

Les technologies renforçant la protection de la vie privée (PETs)

- Pourtant un élément important dans la recherche d'un équilibre entre la fourniture d'identités numériques fiables et la protection des données personnelles

Un tableau de bord activé par défaut

Pour « garantir un niveau plus élevé de transparence

- Vue d'ensemble de toutes les parties utilisatrices avec lesquelles l'utilisateur a établi une connexion
- Vue des types de données partagées avec chaque partie utilisatrice
- Suivi toutes les transactions exécutées avec le PEIN

Et de contrôle par l'utilisateur de ses données qui doit pouvoir

- Demander à une partie prenante de supprimer des données personnelles
- Signaler facilement depuis le PEIN à l'autorité nationale de contrôle où est établie une partie utilisatrice en cas de demande de donnée illégale ou inappropriée
- Révoquer toute attestation électronique d'attributs délivrée par l'utilisateur

- Demande une **interface pour informer les utilisateurs sans délai d'une violation de sécurité** qui peut compromettre le PEIN

Le règlement eIDAS 1 définit un « ensemble minimal de données d'identification personnelle représentant de manière univoque une personne physique ou morale »

Représentation d'une personne physique

► 4 attributs obligatoires pour établir une identité exacte

1. Nom(s) de famille actuel
2. Prénoms actuels
3. Date de naissance
4. Identifiant unique « qui soit aussi persistant que possible dans le temps »

La Commission envisage d'inclure un identifiant **univoque et constant** dans l'ensemble minimal des PID

- Pour réduire les risques d'abus ou d'erreurs et faciliter l'utilisation des portefeuilles
- « En conformité avec le droit de l'Union dans les cas où il est nécessaire d'identifier juridiquement l'utilisateur à sa demande d'une manière univoque et persistante »

Une dangerosité pourtant reconnue

- **Allemagne** : les identifiants uniques sont inconstitutionnels (violation de la dignité humaine)
- **France** : adoption de la Loi Informatique et libertés en 1978 suite au projet SAFARI
  - L'utilisation du NIR (n° de sécurité sociale) est strictement encadré
- **Contrôleur européen à la protection des données** : recommande d'explorer des moyens alternatifs à la création d'un « identifiant univoque et constant » pour renforcer la sécurité du rapprochement entre une personne et des données

Le cadre d'interopérabilité est composé d'un ensemble minimal de PID nécessaires pour **représenter sans équivoque une personne**

Pour les personnes physique

- Pour l'accès à des services publics transfrontaliers **nécessitant l'identification de l'utilisateur en vertu du droit de l'Union ou du droit national**
  - À la demande de la personne
  - Les États membres qui disposent d'au moins un identifiant unique délivrent des identifiants univoques et constants pour une utilisation transfrontalière
- **Ces identifiants peuvent être spécifiques à des secteurs ou à des parties utilisatrices**
  - Ils sont émis par les États membres ou générés par le PEIN

Pour les personnes morales : identifiant univoque et constant

2. L'APPROCHE CRITIQUE

2.3. LE RECOURS À LA CERTIFICATION

Institut Mines-Télécom

S'appuie sur des schémas européen de certification de cybersécurité, ou parties de ces schémas

►**Cibles non précisées**

- Conseil de l'UE – Orientation générale : le stockage sécurisé du contenu cryptographique devrait également faire l'objet d'une certification de cybersécurité

►**Niveau de sécurité non précisé**

- Alors que le PEIN contient des données critiques et peut être utilisé pour l'authentification forte

►**Difficulté à établir les normes**

Modalités de certification

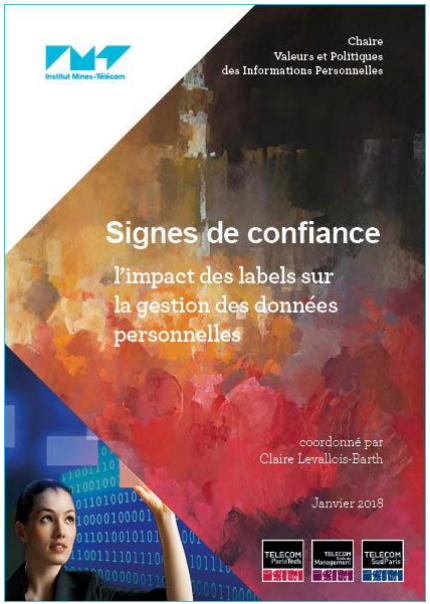
►La Commission européenne dresse une liste des normes de certification (au plus tard 6 mois après l'entrée en vigueur du règlement eIDAS 2)

►Les organismes publics et privés accrédités désignés par les États membres

- Évaluent la conformité aux normes
- Certifient le PEIN

►Les États membres informent la Commission européenne des PEIN délivrés et certifiés

►La Commission publie une liste des PEIN certifiés qui bénéficient d'une présomption de conformité aux exigences de fonctionnalité et d'interopérabilité



Les opérations de traitement de données personnelles liées au PEIN sont certifiées selon les modalités prévues par le RGPD

►Les « cibles » ne sont pas précisées

►Une certification RGPD n'est pas imposée aux fournisseurs d'attestations d'attributs qualifiées

►Pas de calendrier de publication des référentiels

2. L’APPROCHE CRITIQUE

4. LA QUESTION DE LA SOUVERAINETÉ

Institut Mines-Télécom

Recours très important aux normes

►Portefeuilles européens d'identités numériques, attestations électroniques qualifiées d'attributs, services de confiance …

►Objectif : répondre à un rythme d'innovation de plus en plus rapide

Faiblesse du mode d'élaboration des normes et spécifications techniques

►Cf Communication de la Commission, Une stratégie de l'UE en matière de normalisation, 22 fév. 2022

►Au sein des instances européennes (ETSI, CEN/CENELEC)

- Sous-représentation des États, PME et de la société civile qui favorise certains intérêts industriels

►Au sein des instances internationales (ISO, W3C,NIST …)

- Des acteurs publics et privés non européens ont étendu leur influence
- Ces acteurs préconisent des solutions technologiques qui « sont souvent incompatibles avec les valeurs […] et le cadre réglementaire de l'UE »

Améliorer la gouvernance du système européen de normalisation

- ► Renforcer la participation des PME et ONG
- ► Les mandats à la demande de la Commission européenne auprès des organisations européennes de normalisation doivent être traités par les délégués des organismes nationaux des États membres de l'UE et de l'EEE

Soutenir l'innovation, notamment

- ►En renforçant les liens entre la recherche et la normalisation
  - ■ Recommandation (UE) 2023/498 de la Commission européenne du 1er mars 2023 sur un code de bonnes pratiques en matière de normalisation dans l'espace européen de la recherche

Développer une nouvelle génération d'experts

…

Délivrance des portefeuilles

1. Par un État membre (qui est tenu de notifier au moins un schéma et un portefeuille)
2. Sur mandat d'un État membre
3. Indépendamment d'un État mais reconnu par l'État

► Un État peut laisser la fourniture et la gestion du PEIN à toute entreprise intéressée

Avantage concurrentiel des GAFAM/MAMA

►Susceptible d'impacter les conditions de concurrence équitable

- Identité Google, Facebook, Apple, Microsoft déjà commercialisés
- Qui peuvent facilement être rendues conforme à la règlementation

►A termes, pourrait réduire drastiquement le choix des citoyens et des entreprises

Suisse 7 mars 2021 : rejet du projet de loi

►64,4% des votants s'opposent au fait que l'e-ID suisse soit gérée par des banques, assureurs … et non l'État

- Un risque d'utilisation abusive des données
- L'e-ID soit bien plus qu'un identifiant de commerce électronique, il est « **un pilier de la démocratie numérique** »
- Notamment « appliqué pour l'exercice des droits populaires »

CALENDRIER PRÉVISIONNEL

Législation : proposition de règlement eIDAS 2

Spécifications : Architecture and Reference Framework

Développement

Déploiement

Consortium pour développer les **briques du PEIN** et les mettre à disposition des États membres

4 consortiums pour tester les **spécifications techniques du PEIN** et implémenter les **cas d'usage** interopérables

POTENTIAL
European Consortium for Digital Identity

CHAIRE VP-IP
VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES
DONNÉES, IDENTITÉS ET CONFIANCE À L'ÈRE NUMÉRIQUE

Mars 2023 | Juillet 2023 | Sept. 2023 | Janv. 2024 | Mars 2025 | 2026

Parlement européen
Mandat de négociation

Trilogue

Parlement européen
Session plénière

Parlement européen
Début de campagne électorale

1ers actes d'exécution

ARF
Schémas européen de **certification de cybersécurité**

?

Institut Mines-Télécom

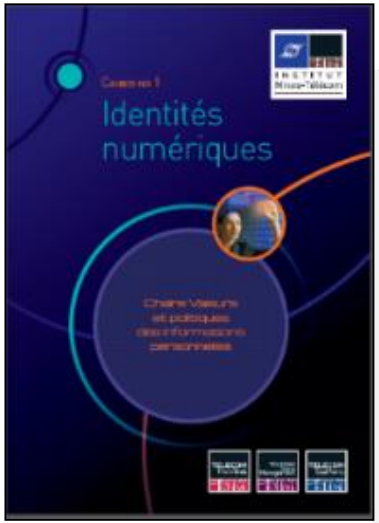
CHAIRE VP-IP

VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES

DONNÉES, IDENTITÉS ET CONFIANCE À L'ÈRE NUMÉRIQUE

www.informations-personnelles.org

@CVPIP



- Les enjeux de la révision du règlement eIDAS : quelle stratégie pour instaurer des identités numériques respectueuses de nos valeurs démocratiques ?, C. Levallois-Barth, in L'Europe et les nouvelles technologies, ed. Bruylant, 2023
- Les acteurs de l'écosystème des identités numériques, C. Levallois-Barth, M. Laurent, 2023
- Pourquoi un portefeuille numérique européen à marche forcée ?, 30 avril 2022, Tribune de M. Hunyadi, C. Levallois-Barth, I. Meseguer, M. Laurent et P. Waelbroeck, Le Club de Médiapart
- Pour la reconnaissance d'un droit à des identités numériques multiples, 2020, C. Levallois-Barth

YouTube

11mars 2021
21e Rencontre

Institut Mines-Télécom

IN GROUPE

orange

altrnativ

CNIL

FIC

Contact

Claire Levallois-Barth
E-mail : @forum-fic.com
Tél. : +33 6 00 00 00 00