LA GESTION DES IDENTITÉS NUMÉRIQUES EVOLUTION ET PERSPECTIVES

MARYLINE LAURENT, DIRECTRICE DU DÉPARTEMENT RST
COFONDATRICE DE LA CHAIRE VP-IP DE L'IMT
SAMOVAR, TÉLÉCOM SUDPARIS, INSTITUT POLYTECHNIQUE DE PARIS

JOURNÉES NATIONALES 2022 DU GDR SÉCURITÉ INFORMATIQUE

- **UNE CHAIRE DE L'IMT DEPUIS 2013**

CHAIRE VP-IP

VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES

DONNÉES, IDENTITÉS ET CONFIANCE À L'ÈRE NUMÉRIQUE

IN GROUPE

orange™

CNIL
Commission Nationale de l'Informatique et des Libertés

DASSAULT SYSTEMES

BNP PARIBAS

• L'ÉQUIPE PLURI-DISCIPLINAIRE

Claire Levallois-Barth

Maître de conférences
en Droit
Coordinatrice et
co-fondatrice de la Chaire

Ivan Meseguer

EU Affairs, Head of Brussels Office,
représentant de l'IMT à Bruxelles – DG IMT
Co-fondateur de la Chaire

Mark Hunyadi

Professeur de Philosophie morale et politique

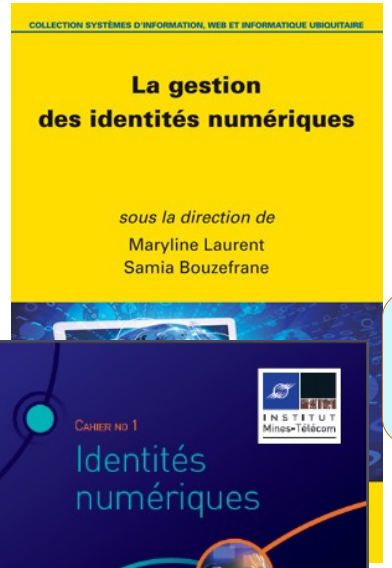
Patrick Waelbroeck

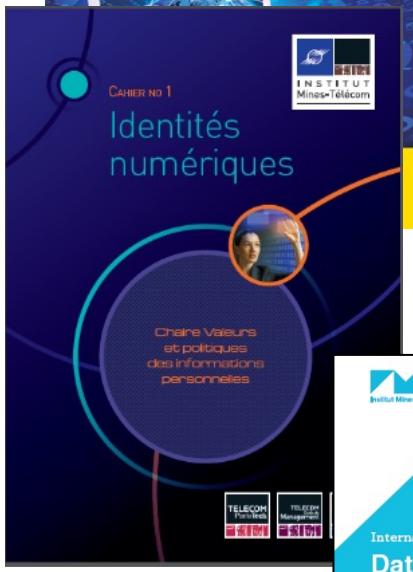
Professeur d'Economie
Co-fondateur de la
Chaire

Maryline Laurent

Professeure en Sciences
Informatiques
Co-fondatrice de la
Chaire

- **LES 5 AXES DE RECHERCHE**





Axe 1. Identités numériques

Axe 2. Gestion des informations personnelles

Axe 3. Contributions et traces

Axe 4. Informations personnelles dans l'Internet des objets

Axe 5 . Politiques des informations personnelles

cvpip.wp.mines-telecom.fr

Twitter @CVPIP

CONTENU

Architecture type de gestion d'identités

Analyse des architectures classiques de gestion des identités sous certains critères (principes de la chaire VP-IP)

Les ID auto-souveraines : évolution sociétale, réglementaire et technologique

Quelques réflexions sur le programme européen

ARCHITECTURE TYPE DE GESTION D'IDENTITÉS

Fournisseur d'identités

IDP

1

2

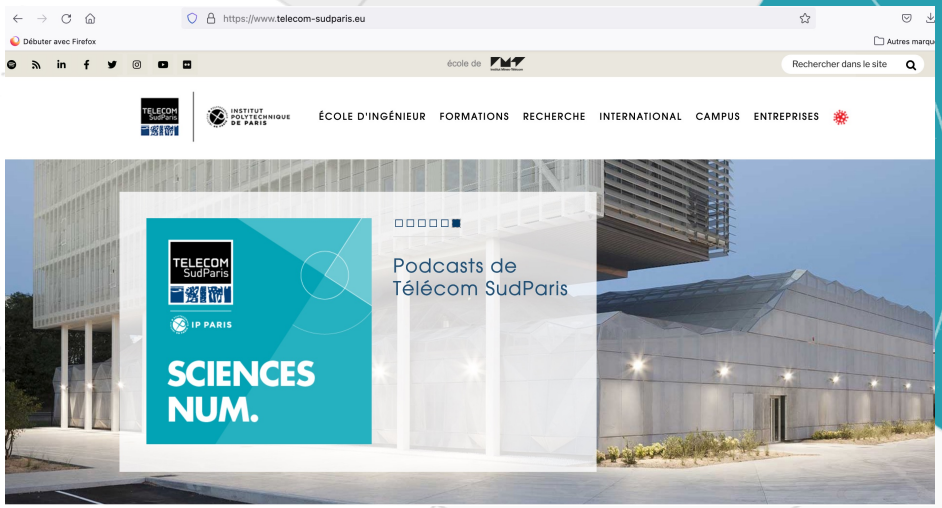
Utilisateur

(ID, Att)

Ex - ID Citoyenne

ID : No fiscal

Att : Nom, prénom, nationalité, date et lieu de naissance, statut marital, adresse postale



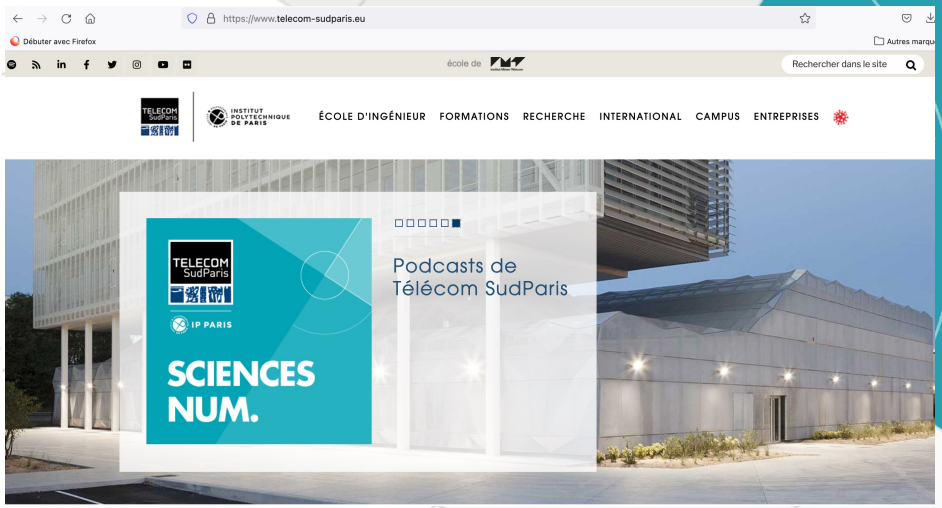
Fournisseur de services

SP

ARCHITECTURE TYPE DE GESTION D'IDENTITÉS

DES IDENTITÉS MULTIPLES - UNE PAR CONTEXTE

IDP1 IDP2 IDP3



SP

Utilisateur

(citoyenne, patiente, consommatrice, mère de famille, chercheuse, joueuse en ligne, membre forum…)

(ID1, Att1) **(No fiscal, {nom, prénom, adresse, date de naissance… })**

(ID2, Att2) **(Pseudo joueuse, {langue, niveau, pouvoirs, ses amis})**

(ID3, Att3) **(ID parent d'élève, {enfant, classe})**

H. Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life, 2010

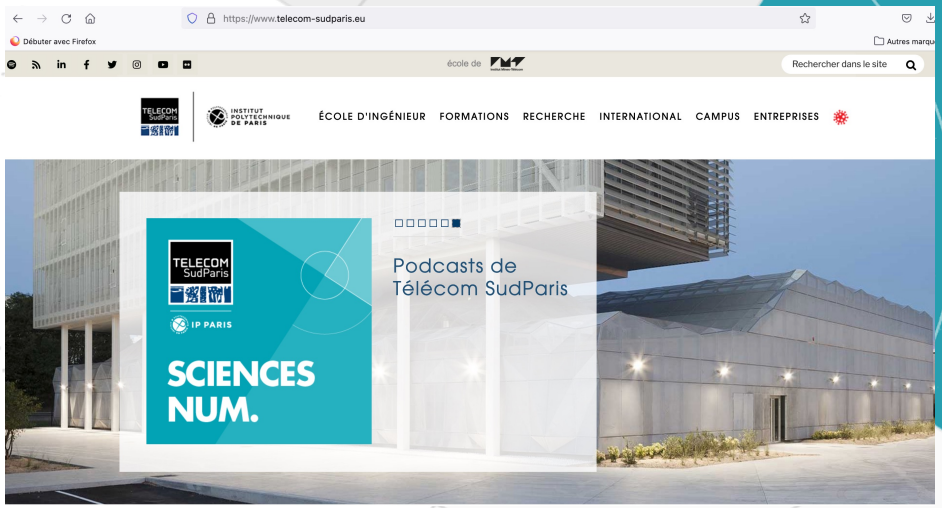
ARCHITECTURE TYPE DE GESTION D'IDENTITÉS

RISQUES À NE PAS CLOISONNER LES IDENTITÉS

IDP1

IDP2

IDP3



SP

Utilisateur

(citoyenne, patiente, consommatrice, mère de famille, chercheuse, joueuse en ligne, membre forum…)

(ID1, Att1) **(No fiscal, {nom, prénom, adresse, date de naissance… })**

(ID2, Att2) **(Pseudo joueuse, {niveau, pouvoirs, ses amis})**

(ID3, Att3) **(ID parent d'élève, {enfant, classe})**

H. Nissenbaum, Privacy in Context: Technology, Policy and the Integrity of Social Life, 2010

PRINCIPES / CRITÈRES D'ANALYSE

1 - Identités multiples par cloisonnement — Défendu par chaire

2 - Pseudonymat — Défendu par chaire

3 - Preuves d'attributs — Besoin des SP

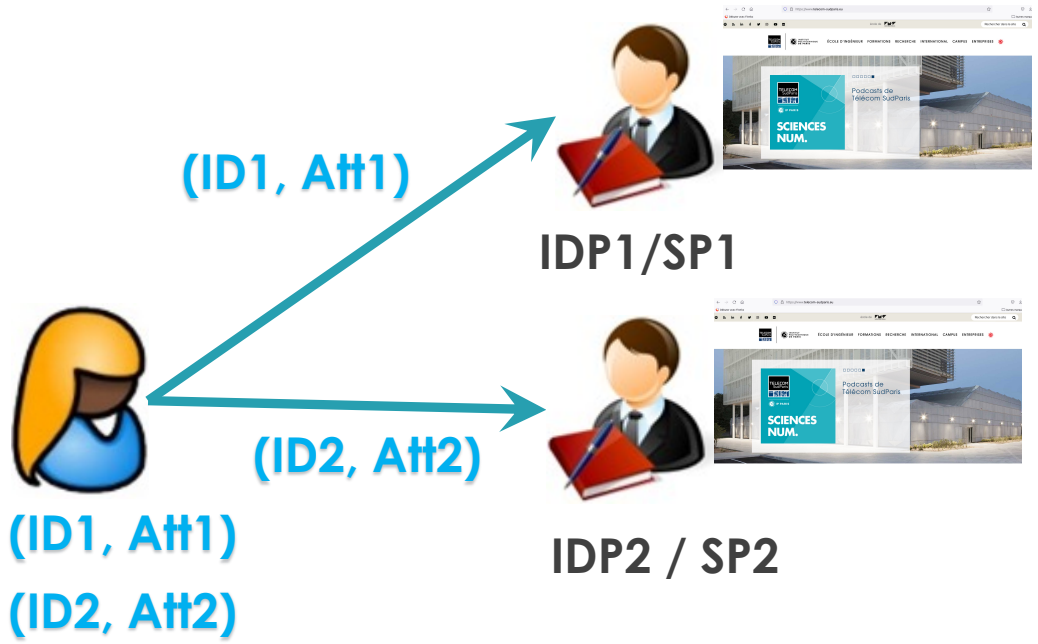
4 - Minimisation de données — Défendu par chaire et le RGPD

5 - Non traçabilité des utilisateurs entre 2 SP — Propriété d'indistingabilité

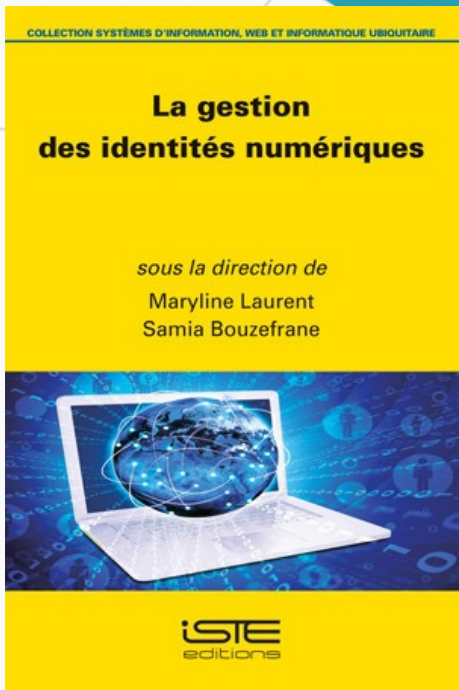
6 - Non traçabilité des activités d'un utilisateur par un IDP — Propriété d'indistingabilité

GESTION DES IDENTITÉS EN SILO

SP EST ÉGALEMENT IDP – 1 CREDENTIEL PAR SP

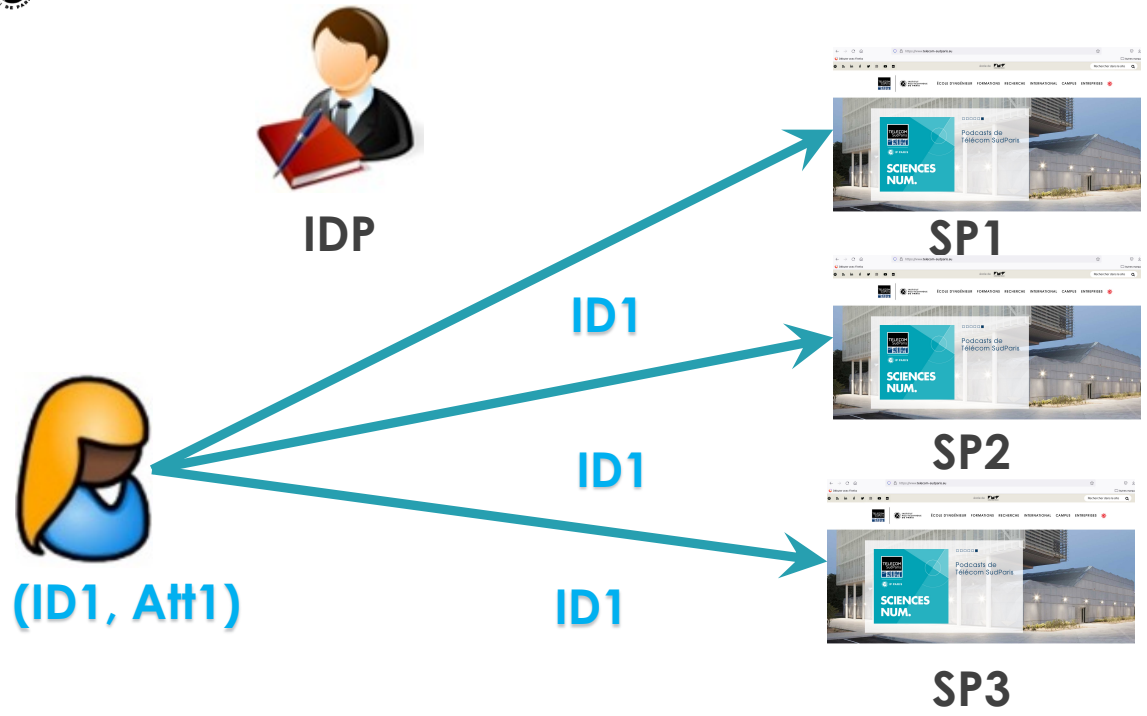


ID multiples	✓
Pseudonymat	✓
Preuves d'attributs	NA
Minimisation de données	NA
Non traçabilité par les SP	✓
Non traçabilité par les IDP	✓



GESTION CENTRALISÉE DES IDENTITÉS

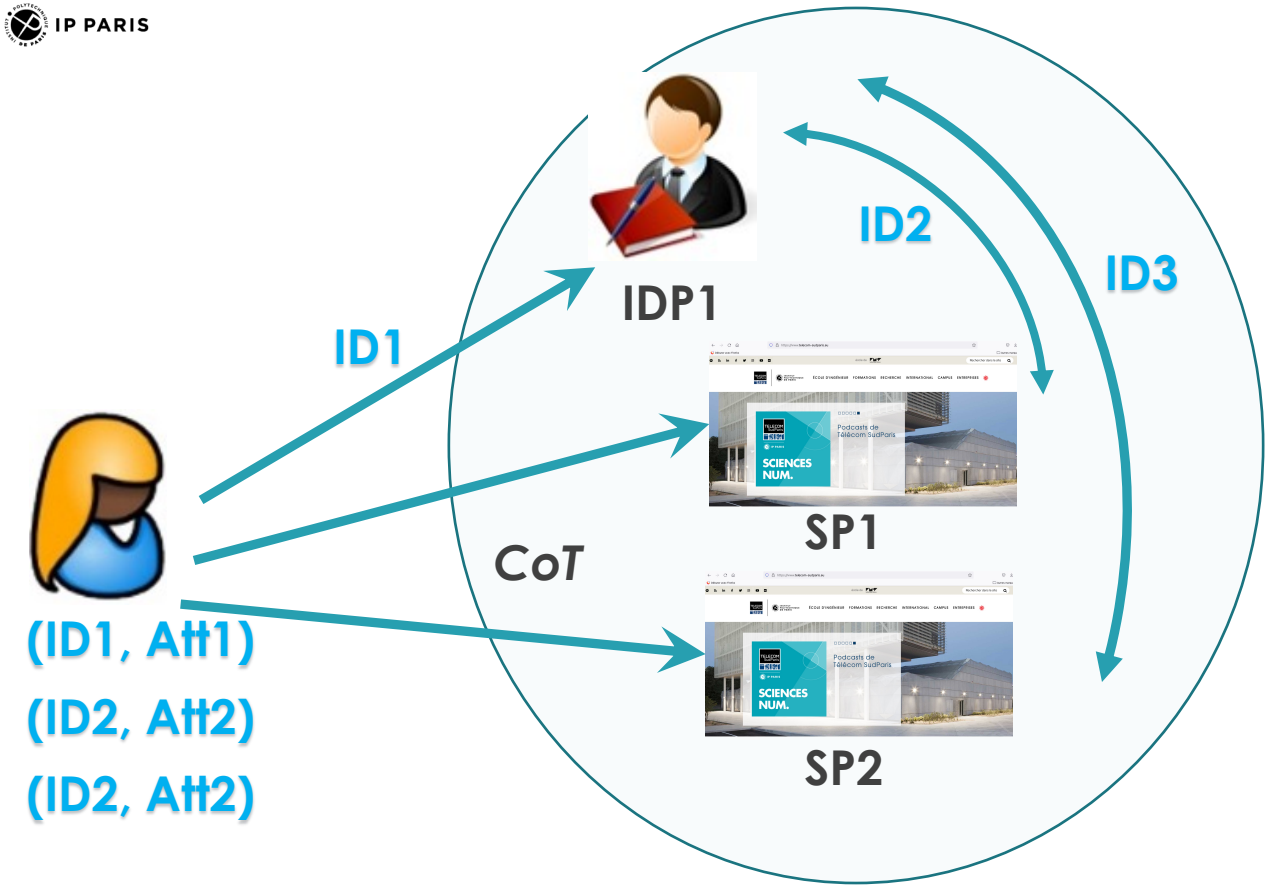
UNE IDENTITÉ POUR ACCÉDER À DE MULTIPLES SERVICES



ID multiples	**X**
Pseudonymat	NA
Preuves d'attributs	NA
Minimisation de données	NA
Non traçabilité par les SP	**X**
Non traçabilité par les IDP	**X**

Ex : solutions WebSSO

GESTION FÉDÉRÉE DES IDENTITÉS

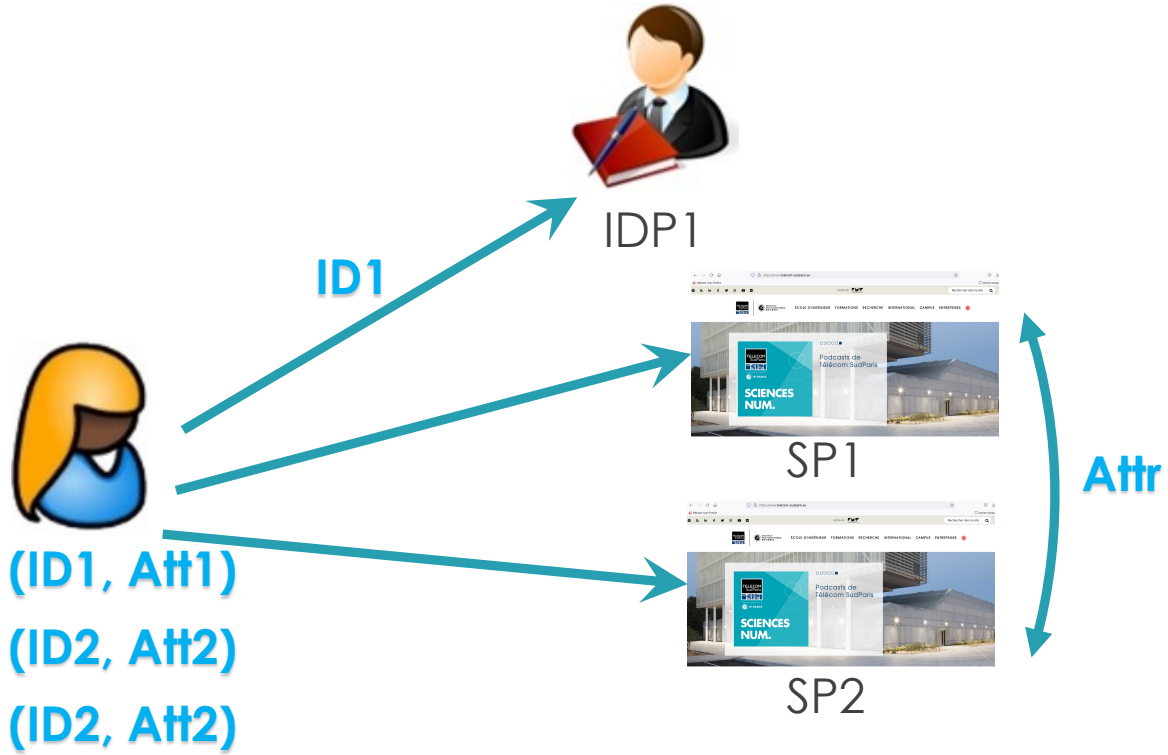


ID multiples	✓
Pseudonymat (sur les SP)	✓
Preuves d'attributs	NA
Minimisation de données	X
Non traçabilité par les SP	✓
Non traçabilité par les IDP	**X**

Ex : solutions Liberty Alliance, Shibboleth

MONTÉE EN FORCE DES GAFAM/BATX

GRÂCE AUX PROTOCOLES OAUTH ET OPENID CONNECT

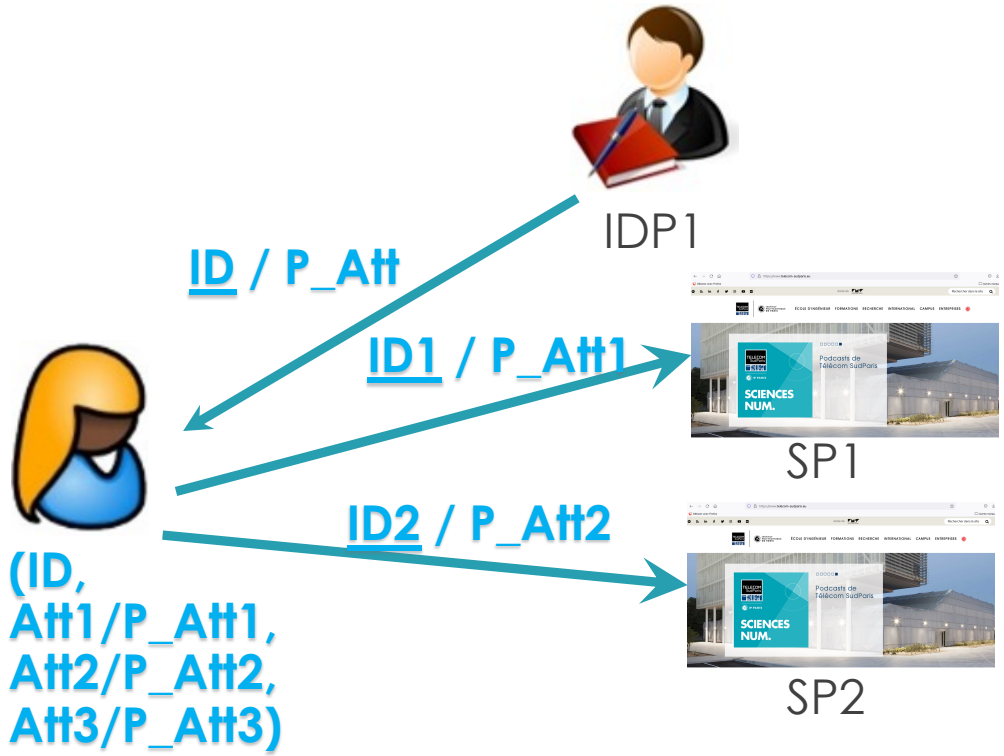


ID multiples	✓
Pseudonymat (sur les SP)	✓
Preuves d'attributs	NA
Minimisation de données	✓
Non traçabilité par les SP	✓
Non traçabilité par les IDP	**X**

oAuth 2.0 redonne le pouvoir de décision de collecte de données à l'utilisateur, mais c'est sans compter sur d'autres procédés d'identification des terminaux, ex : fingerprinting

LES IDENTITÉS AUTO-SOUVERAINES

PAR DES SOLUTIONS CRYPTOGRAPHIQUES DE CERTIFICATION



ID multiples	✓
Pseudonymat (sur les SP)	✓
Preuves d'attributs	✓
Minimisation de données	✓
Non traçabilité par les SP	✓
Non traçabilité par les IDP	✓

Certification d'attributs :

- **anonyme (UPROVE, IDEMIX)**
- **sous pseudonymat (solution de TSP : PIMA)**

LES IDENTITÉS AUTO-SOUVERAINES

EVOLUTIONS SOCIÉTALES

Une défiance qui monte :

Enquête réalisée par la chaire VP-IP – Médiamétrie 2017 et 2019

(téléchargement libre)

88% **Des Internautes se sentent surveillés sur Internet**

60%

Des Internautes sont plus vigilants sur Internet par rapport à il y a quelques années

VS 54% en 2017

+6pts

Question : Par quel acteur vous sentez-vous le plus surveillé sur Internet ?

LES IDENTITÉS AUTO-SOUVERAINES

EVOLUTIONS SOCIÉTALES

60%

Des Internautes sont plus vigilants sur Internet par rapport à il y a quelques années

VS 54% en 2017

+6pts

Parmi lesquels :

Veulent garder le contrôle sur leurs informations en ligne
vs. 94% pour l'ensemble

96%
Contre 94% en 2017

Utilisent une fausse identité ou un pseudonyme sur Internet
vs. 69% pour l'ensemble

70%
Contre 65% en 2017

Un besoin pour 94% des internautes de garder le contrôle sur ce que les entreprises et acteurs du numérique peuvent apprendre en ligne

LES IDENTITÉS AUTO-SOUVERAINES

EVOLUTIONS RÉGLEMENTAIRES ET TECHNOLOGIQUES

Des évolutions réglementaires en faveur d'un meilleur contrôle des individus sur leurs données et leurs identités :

- **RGPD sur la protection des données mis en application en 2018**
- **eIDAS en cours de révision**
- **ePrivacy toujours en projet**

Des solutions technologiques qui permettent :

- **Plus de sécurité dans la gestion des identités et de l'authentification : ex de la certification FIDO2 (FIDO Alliance)**
- **Plus de contrôle par les utilisateurs sur leurs identités et leurs données (user centric) : certification anonyme**
- **Plus de distribution du pouvoir – éviter la concentration de pouvoir : blockchain (*La blockchain est-elle une technologie de confiance ?, Signes de confiance, 2018 ; Distributed access control solution for the IoT based on multi-endorsed attributes and smart contracts, IWCMC2019*)**
- **Une perte de précisions des profils utilisateurs par les SP : *A Validated Privacy-Utility Preserving Recommendation System with Local Differential Privacy », TrustCom/BigDataSE 2021*,**

LES PORTE-FEUILLES D'IDENTITÉS NUMÉRIQUES

PROGRAMME DE LA COMMISSION EUROPÉENNE – RÉVISION DE EIDAS

- **80% des citoyens européens équipés d'une identité européenne numérique d'ici 2030**
- **Usages ouverts auprès des administrations et des acteurs privés -> risque de décloisonnement des ID si des usages non identifiés**
- **Des porte-feuilles d'identités sur smartphones déployées par des Etats ou des acteurs privés -> risques de perte de souveraineté**
- **Une multitude d'acteurs privés - depuis les briques technologiques jusqu'au déploiement/administration -> risques sur la sécurité du porte-feuille et de fuite des données**
- **Un calendrier précipité : 3 juin 2021 (proposition de règlement par la CE), 3 juin 2021 (recommandation par la CE d'une coopération avec les EM et le secteur privé pour publier une boîte à outils pour octobre 2022), 15 février 2022 (appel d'offre pour des projets pilotes par la CE), octobre 2022 (première discussion au Parlement européen) -> *cf. Tribune – Médiapart Union européenne : pourquoi un portefeuille numérique à marche forcée ? Mark Hunyadi***

CONCLUSIONS

En tant que chercheurs, ingénieurs, juristes, sociologues, économistes, philosophes, encore un gros travail reste à faire :

- **Sensibilisation des différents acteurs (publics,**
- **Réflexion/projection sur « quel numérique pour demain ? »**
- **Outils de préservation pour assurer le cloisonnement des ID multiples – complexité (toute la pile protocolaire touchée)**
- **Poursuivre l'effort sur l'utilisation de la technologie (PETs) pour renforcer en deuxième ligne les mesures de cybersécurité éventuellement défaillantes**

MERCI AUX ORGANISATEURS

Maryline.Laurent_at_telecom-sudparis.eu