



L'identité biométrique, réponse à l'usurpation d'identité





Pourquoi une identité numérique ?

- Le constat sur la fraude à l'identité
- Le besoin de protection des citoyens
- => Lutte contre l'obtention induite de documents



Première réponse



- La dématérialisation de la transmission des actes d'état civil et du justificatif d'adresse
 - Évite la production de faux justificatifs et les identités fictives
 - N'évite pas la présentation d'une demande sous une fausse identité



Le schéma fonctionnel de la dématérialisation



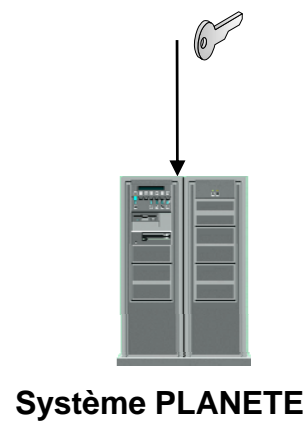
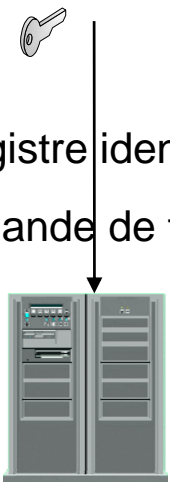
Mairie

Notaire

CNAF

Mairie de naissance
service Etat civil

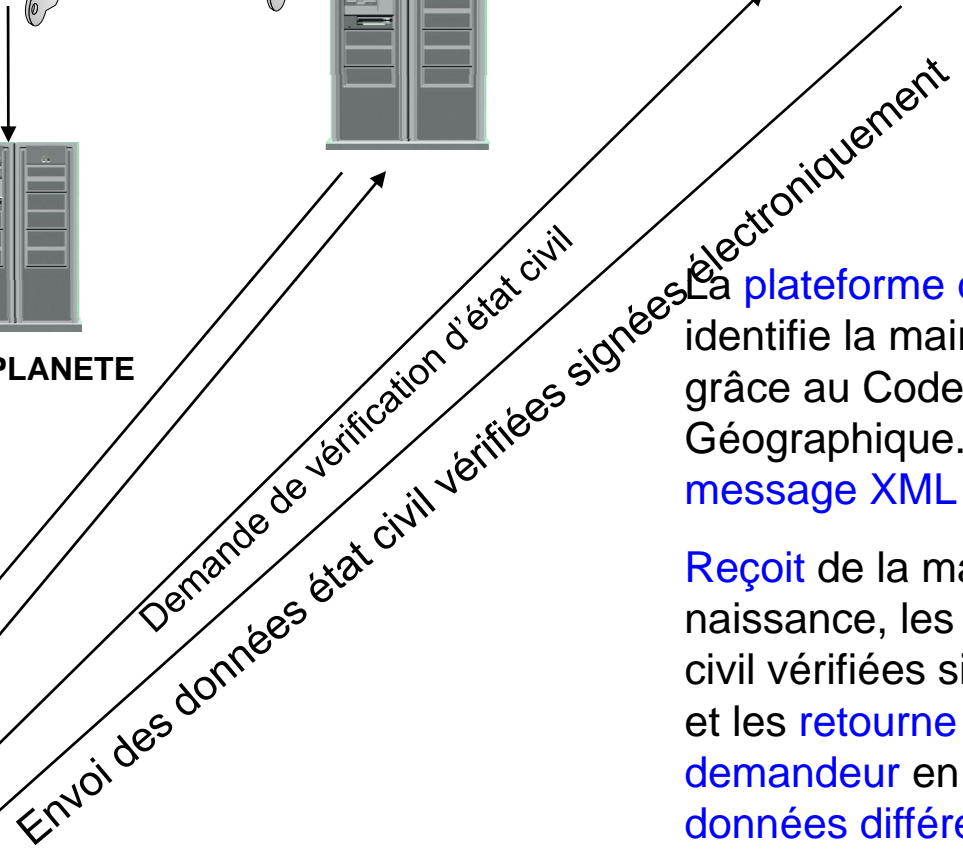
Enregistre identité
+demande de titre



Systeme TES



Plateforme de routage
Annuaire des mairies



La **plateforme de routage** identifie la mairie de naissance grâce au Code Officiel Géographique. Lui envoie un **message XML chiffré**

Reçoit de la mairie de naissance, les données d'état civil vérifiées signées, chiffrées et les **retourne au système demandeur** en lui **signalant les données différentes** entre identité objet de la demande et état civil



L'identification biométrique comme garante de l'unicité

En France, l'état civil est éclaté entre 36 000 communes.

L'absence de fichier de population nécessite une donnée identifiante : seule la biométrie répond à ce défi.

Des données biométriques sont recueillies pour les documents de voyage et d'identité, mais pour quels usages ?



Les usages déterminent le mode de stockage des données biométriques

- Pour la délivrance des documents d'identité, le contrôle d'unicité biométrique (1: n) s'impose pour chaque demande nouvelle.
 - L'absence de base de données biométriques de référence permettrait à un faussaire de coupler des données biométriques à une fausse identité, le repérage de la fraude étant impossible par le simple contrôle carte contre empreinte.
 - La base de données biométriques permet aussi de lutter contre le vide documentaire (Si le composant électronique de la carte est altéré, le seul contrôle avec les données de la carte est impossible)
 - Par construction, l'identification requiert une base de données de la population de référence.



Typologie des données bio à enregistrer pour l'identité



- Les paramètres à prendre en considération :
 - Taille de la population de référence
 - Efficacité de la recherche
 - Niveau de précision
- La saisie d'un nombre élevé de données limite les refus à l'enregistrement et améliore la précision. En France, le choix a été fait d'enregistrer huit empreintes digitales pour les documents d'identité.



Comment construire l'identité numérique

- Contexte français et européen de protection des données personnelles (CNIL, Comité article 29)
- Référence : modèle « Citizen Centric »
- Les principes à respecter :
 - finalité,
 - proportionnalité,
 - sécurité,
 - information des personnes concernées



Comment construire l'identité numérique

- Modalités de conception d'une BDD biométrique centrale pour l'émission des documents :
 - Le titre doit être sûr,
 - Le processus d'usage doit être sûr,
 - Le processus de délivrance doit être sûr
 - Les données collectées pour les tests d'unicité garantissent le processus de délivrance, mais d'autres usages sont possibles...



Comment construire l'identité numérique

- Les usages autres que la recherche d'unicité :
 - Sélection de l'identité pour obtenir la biométrie (utile lors du renouvellement du titre)
 - Sélection de la biométrie pour obtenir l'identité (cette fonction sert à gérer l'identification des « interdits »)
- Le contrôle des usages consiste à répartir en bases distinctes l'identité et la biométrie.
 - Les bases sont reliées par des liens chiffrés sous contrôle d'une autorité indépendante
 - Il existe plusieurs modèles de lien chiffré.



Trois modèles de lien proposés

- Le lien bi directionnel (permet d'aller de la biométrie à l'identité et réciproquement)
- Le lien identité vers la biométrie
- Le lien biométrie vers l'identité

- Pour mémoire, il existe aussi des modèles à lien faible dont l'objet est de découpler les bases pour limiter les recherches



Fonctionnalités des modèles



	Modèle 1 Lien bidirectionnel	Modèle 2 Lien unidirectionnel ID vers BIO	Modèle 3 Lien unidirectionnel BIO vers ID
association ID-Bio	Oui dans les 2sens	ID vers BIO	BIO vers ID
Gestion de l'association	Fonction cryptographique sous contrôle	Fonction cryptographique à sens unique	Fonction de cryptographique à sens unique
Entrée = ID Sortie = Bio	Oui	Oui	Non
Entrée = Bio Sortie = ID	Oui	Non	Oui



Fonctionnalités des modèles



	Modèle 1 Lien bidirectionnel	Modèle 2 Lien unidirectionnel ID vers BIO	Modèle 3 Lien unidirectionnel BIO vers ID
Renouvellement	Facile	Facile par authentification	Plus lourde par identification
Suppression (Décès)	Oui	Facile par l'identité	Plus lourde par identification
Authentification sur carte illisible	Oui	Oui	Peu réaliste, par identification sur la totalité de la base
Identification (victimes, amnésiques, criminels)	Oui	Non	Oui
Destruction des liens	Oui, par destruction des fonctions crypto	Oui, par destruction des fonctions crypto	Oui, par destruction des fonctions crypto
Contrôle possible par une Autorité	Oui	Oui	Oui
Possibilité de rétablir les liens en clair	Oui	Oui	Oui
Maturité industrielle	Prouvée	Prouvée	Prouvée



Authentification et « e-services »



- Les 3 modèles de lien chiffré sont égaux pour le test d'unicité, qui est le seul usage indispensable de la sphère de confiance requise par les e-services.
- A la différence de la sphère publique qui focalise sur l'identification pour authentifier un demandeur de titre, la sphère privée des « e-services » est plutôt motivée par l'unicité à des fins de non répudiation de la carte ou du moyen de paiement.



Merci pour votre attention