Usages de l'identité numérique sécurisée

Rapport intégral de la mission DITP (mars-mai 2019)
Version définitive, 10 juillet 2019

modernisation.gouv.fr

Direction interministérielle de la transformation publique
libérer l'énergie publique

Objectifs de la mission et approche retenue

Lettre de mission : Identifier les usages locomotives (administratifs ou privés) pour le développement de l'identité numérique afin de tirer la demande :

- → Usages existants (de niveau de sécurité faible) à rendre compatibles
- → Usages à créer (de niveau de sécurité substantiel ou élevé)

Résultats :

- ✓ Alignement sur les concepts et enjeux
- ✓ Cartographie et groupement
- ✓ Qualification des locomotives
- ✓ Recommandations pour le déploiement
- ✓ Illustration des parcours et de la promesse d'usage « idéaux »
- ✓ Cahier « explorations »

Benchmark géographique

Retour d'expérience de programmes d'identité numérique dans 11 pays

Fournisseurs de services

~20 entretiens experts de services privés et publics, travaux existants

Revue et analyse des usages

55 usages publics et 25 usages privés recensés et qualifiés

Voix des usagers

Etude qualitative
Etude quantitative en ligne et par téléphone-
1250 répondants

Design de service

Modélisation des parcours + 1 atelier « agents/usagers »

Prospective

Explorations « experts/u

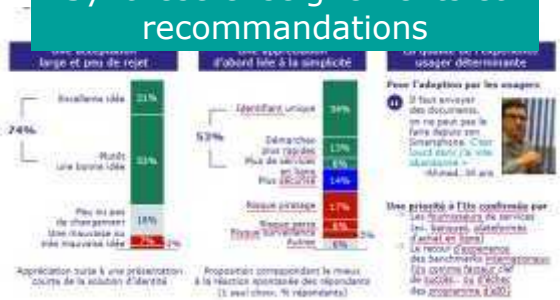
Présentation des principaux livrables

Benchmark international

Besoins fournisseurs de service

Résultats enquêtes usagers

Synthèse enseignements et recommandations

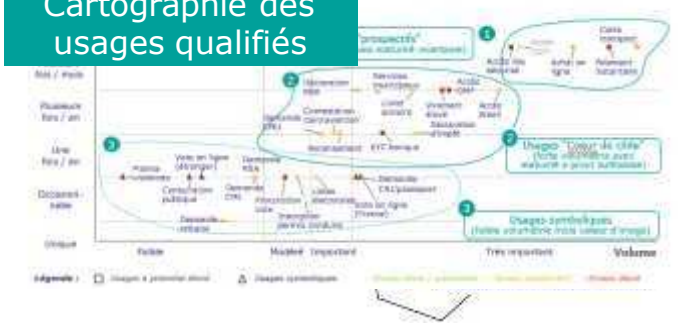


Videos « voix de l'usager »

Exploration Prospective

Illustration parcours e t usages « idéaux »

Cartographie des usages qualifiés



SYNTHESE DES TRAVAUX

Direction interministérielle de la transformation publique

libérer l'énergie publique

LES PRINCIPAUX ENSEIGNEMENTS (I)

Un attrait fort de la solution d'identité numérique, qui repose principalement sur ses bénéfices de simplification (solution universelle et simple pour s'identifier auprès du plus grand nombre de services, indépendamment du niveau de sécurité nécessaire)

> Les usages prioritaires (attentes, volume et fréquence) appartiennent aux univers de la santé, des prestations sociales, de la fiscalité, de la banque et de la vie citoyenne (vote, titres, …)
> D'autres usages à plus faible volumétrie mais à portée symbolique, renforcent la promesse et la valeur d'universalité

L'universalité de la solution doit s'appliquer en priorité et massivement à la sphère publique

> Un univers cohérent pour les usagers (complexité des démarches et sensibilité des données)
> L'opportunité de s'adosser aux grands programmes de transformation numériques (santé, justice)
> La valorisation de la CNIe au sein des fournisseurs d'identité FranceConnect (y compris sur faible et substantiel)
> Une extension de l'utilisation de la solution par des fournisseurs de services privés facilitée par l'adoption réussie dans la sphère publique (visibilité et familiarité)
> Une adjacence proche et naturelle vers le secteur bancaire

L'Ux et la fluidité des parcours sont fondamentales pour répondre aux attentes des usagers et des fournisseurs de services

> Des attentes élevées en matière de simplicité (ex. : identifiant simple, facile à retenir)
> Un levier de simplification des démarches administratives (ex. : partage de données d'identité)
> Un besoin important de modularité et de personnalisation (ex. : solution sur PC & Smartphone)

La stratégie de déploiement de la CNIe est clé pour la réussite du programme

> Un enjeu fort de communication en amont et auprès des leaders d'opinion (bénéfices, réassurances)
> La nécessité d'une procédure d'enrôlement simple, rapide et rassurante
> Un besoin d'accompagnement (modulaire et humain lorsque nécessaire) pour faciliter l'adoption
> Un déploiement rapide de la CNIe et la possibilité de l'obtenir par anticipation, sur demande

LES PRINCIPAUX ENSEIGNEMENTS (II)

La sécurité de l'identification, un critère important mais second

> Des attentes usagers limitées sur le renforcement de la sécurité des procédures existantes
> Une distinction entre les procédures d'identification de niveaux substantiel et élevé (réglementation eIDAS) peu reconnue et difficilement compréhensible
> Des bénéfices d'une identification élevée qui, globalement, ne suffisent pas à embarquer les fournisseurs de services privés (vs. craintes sur la fluidité des parcours et les coûts de mise en œuvre)
> Le fait que la CNIe permette de s'identifier avec un niveau de sécurité élevé (versus substantiel) ne peut pas être ce qui définit et ancre principalement le programme si l'on souhaite une adoption large

Les protections en cas d'usurpation d'identité et de fraudes, essentielles pour répondre aux craintes liées à la perte, au vol ou au piratage de son identité numérique / de sa CNIe

> Une conviction forte de la part des usagers : le risque zéro (sur internet) n'existe pas
> Les solutions de détection et de réaction en cas de problèmes (alertes SMS/email, opposition, mise en place d'une identité provisoire) plus rassurantes qu'une garantie d'inviolabilité
> La visée non commerciale d'une solution portée par l'Etat (pas de divulgation et de monétisation des données personnelles), un élément additionnel et distinctif de réassurance

La valeur perçue de la CNIe serait renforcée par la proposition de nouveaux services et de nouvelles fonctionnalités (ex. : vote en ligne, partage direct d'informations et documents)

> Une opportunité de valoriser le caractère innovant et créateur de valeur du programme

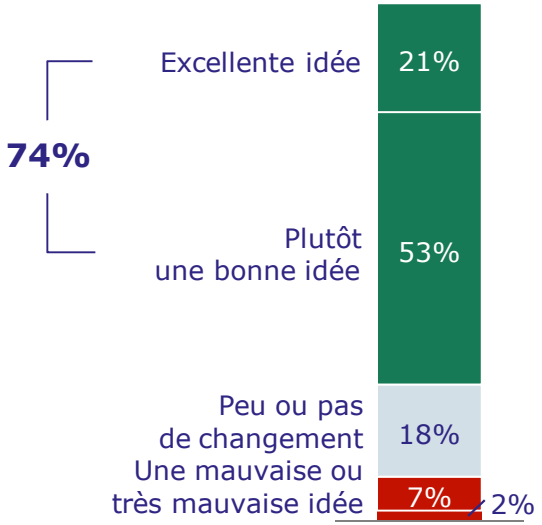
La CNIe peut être un vecteur d'inclusion numérique, à certaines conditions

> Une adhésion a priori moins forte et davantage d'inquiétudes exprimées
> Le nécessité de mettre en avant et d'assurer le bénéfice de la solution pour les "éloignés du numérique", à savoir la simplification des démarches administratives
> Le besoin d'un accompagnement humain important auprès de ces populations en capitalisant sur les structures et dispositifs existants (MSAP, EPN, etc.)

Dans un horizon plus lointain, un potentiel considérable d'usages et de services désirables au service des personnes, des collectifs et des politiques publiques … mais dont les risques doivent être connus, partagés et maîtrisés

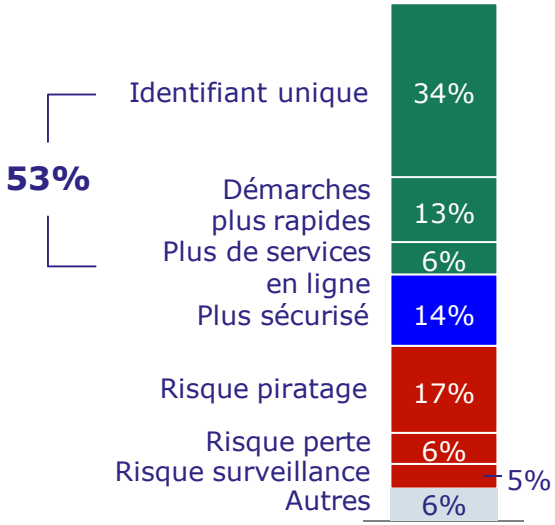
Un attrait fort de la solution d'identité numérique, lié aux bénéfices attendus de simplification

3/4 Une acceptation large et peu de rejet



Appréciation suite à une présentation courte de la solution d'identité*

Une appréciation d'abord liée à la simplicité



Proposition correspondant le mieux à la réaction spontanée des répondants (1 seul choix, % répondants)

La qualité de l'expérience usager déterminante

Pour l'adoption par les usagers

« Il faut envoyer des documents, on ne peut pas le faire depuis son Smartphone. C'est lourd donc j'ai vite abandonné »
-Ahmed, 34 ans

Une priorité à l'Ux confirmée par

- Les fournisseurs de services (ex. banques, plateformes d'achat en ligne)
- Le retour expérience des benchmarks internationaux (Ux comme facteur clef de succès… ou d'échec des programme d'eID)

(*) Voir annexe 3

Etude qualitative (4 focus group) et études quantitatives en ligne et par téléphone- 1250 répondants (mars-avril 2019)

Un bénéfice perçu d'universalité qui trouve tout son sens dans la sphère publique

Les services publics constituent un univers cohérent à fort potentiel

- Des données considérées sensibles
- Une forte attente de simplification
- Une généralisation attendue à l'ensemble des services publics (yc dans les services des collectivités)

« S'identifier sur les sites administratifs, **c'est vraiment une chaleur.**

« Ce qui serait merveilleux c'est que cela marche **aussi pour les services municipaux**

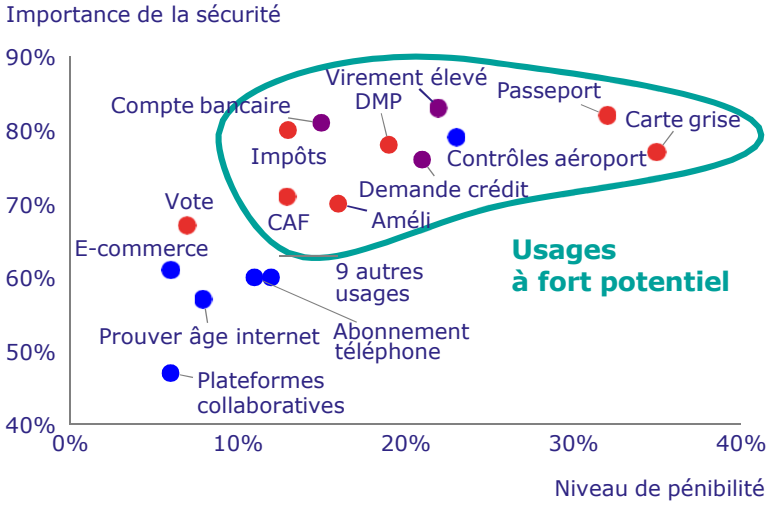
Les paiements et services bancaires une adjacence naturelle à fort potentiel

- Une proximité dans l'esprit des usagers, avec une forte attente de sécurité
- Un potentiel d'intérêt des acteurs sous réserve de visibilité sur les solutions techniques et l'UX

La généralisation de l'usage dans la sphère publique va favoriser l'adhésion des fournisseurs de services privés

- Notamment par la familiarité des clients/usagers avec la solution d'identité et les modes d'identification

Identification des cas d'usage à fort potentiel de création de valeur pour la solution d'identité



Des priorités en ligne avec l'analyse des usages par les volumes (# d'usagers et fréquence d'usages) et du niveau de sécurité requis par les fournisseurs de services

Le niveau de sécurité de l'identification est un critère important, mais second

- Retour d'expérience du benchmark international : le niveau de sécurité élevé (au sens eIDAS) n'est pas un point d'entrée pertinent dans les programmes les plus ambitieux d'identité numérique
- Les facteurs clef de succès tournent autour de l'ergonomie et de la densité de l'offre de services
- Une distinction entre les procédures d'identification de niveaux substantiel et élevé peu pertinente et difficilement compréhensible pour les usagers

- Les fournisseurs de services privés se positionnent peu en faveur de solutions d'identités numériques sécurisées couvrant le niveau de sécurité élevé (avec quelques exceptions près)
- Un attentisme lié aux craintes sur la fluidité des parcours ainsi qu'au manque de visibilité sur les coûts de mise en œuvre et les garanties de l'Etat sur la certification de l'identité, malgré des bénéfices bien identifiés autour de la lutte contre la fraude, l'amélioration de la qualité de service (notamment via des échanges plus faciles à distance), la réduction des coûts (ex. KYC) et la création de nouveaux services

- Des attentes limitées des usagers en termes de sécurité des procédures d'identification existantes
- Cependant, parmi les démarches pour lesquelles la sécurité est la plus importante :
  - Les services bancaires (virement d'un montant élevé pour 83% des répondants, ouverture d'un compte bancaire pour 81% des répondants)
  - Les démarches administratives (renouvellement de ses titres d'identité pour 82% des répondants, accès au site impots.gouv pour 80%, accès au DMP pour 79%)
- La particularité des univers publics et bancaires qui renvoient à un besoin de sécurité et de confidentialité des données

> “Pour tout ce qui est administratif et bancaire, la procédure d'identification doit être plus sécurisée qu'avec un mot de passe seulement.

> “Les données de santé, ce sont des informations intimes que l’on ne peut pas divulguer comme ça.

- Mais peu de demande de renforcement de la sécurité sur ces usages

Les réponses concrètes en cas de perte, de vol, etc. sont plus rassurantes que des promesses de fiabilité

Principales inquiétudes pour les usagers

#1- Usurpation d'identité en cas de perte ou vol (25% des répondants[1])

> “ L'usurpation d'identité, c'est vraiment le pire. Des gens font des achats ou des crédits à votre nom et vous endettent. C'est horrible !

#2- L’Etat une cible privilégiée des hackers (17% des répondants)

> “ Il y a plutôt intérêt à ce que les solutions techniques soient doublées car on ne dépend plus que d’un seul système. Si ça plante, je ne peux plus accéder à aucun site de l’administration.

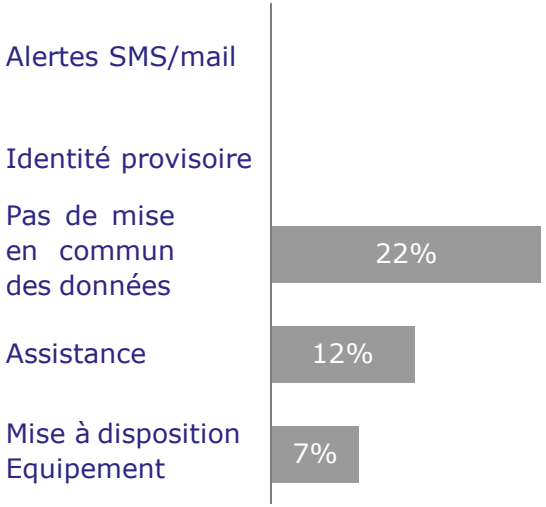
#3- La centralisation des données (16% des répondants)

> “ C'est inquiétant que toutes les données soient concentrées au même endroit. Si il y a un problème on perd tout

“ Le risque zéro n'existe pas !

Réassurances les plus fortes

% de répondants,
choix unique sur 5 options



L'Etat aussi source de confiance : gratuité, protection des citoyens, pas d’exploitation commerciale

1 - % de répondants, choix unique sur 8 options

La CNIe et l'identité numérique associée peuvent être des facteurs positifs d'innovation publique

Des fonctionnalités inédites à forte valeur pratique ou symbolique

Gagner du temps grâce au partage d'information pour faciliter les démarches – point positif pour 77% des répondants

Ne plus avoir à se déplacer avec plus de services en ligne - point positif pour 71% des répondants

Une seule carte plusieurs usages, >60% pour le permis de conduire et la carte vitale sur la CNIe

Voter, renouveler son passeport et déposer une plainte les trois nouveaux services en ligne les plus appréciés

De nouveaux usages à forte valeur symbolique
- → Exercice des droits citoyens
- → Accès universel aux services
- → Protection des plus faibles – dépôt de plainte facilité (ex violences conjugales)

Avec l'accompagnement nécessaire une opportunité d'inclusion numérique

Une attention particulière nécessaire pour les « éloignés du numérique »[1] moins positifs et plus inquiets
- → 48% approuvent (vs. 74%), 38% désapprouvent (vs. 9%)
- → 86% (vs. 70%) inquiets en cas de perte/vol, usurpation d'identité

En plus des éléments de réassurance généraux, proposer une assistance et la mise à disposition de matériels
- → Alertes et identité provisoire éléments les plus rassurants
- → 70% (vs. 47%) rassurés par une assistance disponible et 68% (vs. 39%) par la mise à disposition de matériels

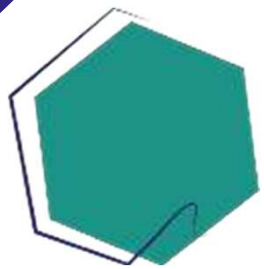
Mettre en avant le partage d'informations particulièrement apprécié par cette population pour simplifier les démarches
- → Fonctionnalité la plus appréciée (86%)

Exploiter l'introduction de la CNIe et ses fonctionnalités avec d'autres initiatives (Maisons France Services) pour favoriser l'inclusion et la digitalisation de publics éloignés du numérique

“ Mais pourquoi on n'a pas ça en France ?

1 – Personnes interrogées par téléphone et réalisant peu ou pas de démarches ou actes sur internet, comparaison avec l'échantillon de répondant à l'enquête online

Les recommandations pour une adoption large



RAPPORT INTEGRAL

Direction interministérielle de la transformation publique

libérer l'énergie publique

Sommaire

L'identité numérique recouvre trois concepts à distinguer

Concepts	Exemples
Supports d'identité électronique Solutions technologiques, immatérielles ou sur support physique, intégrant les données pivots qui leurs sont associées	→ Carte nationale d'identité électronique (CNIe) → Carte à puce telles que les cartes bancaires → Smartphone, PC → Solutions immatérielles → …
Différentes identités utilisées sur le numérique Représentation d'un utilisateur (personne physique ou morale) dans le monde numérique, construite sur la base de ses données personnelles et, le cas échéant, des traces qu'il y laisse	→ Profils, comptes et publications (réseaux sociaux, professionnels, etc.) → Avatars (Forum, jeux vidéos, etc.) → …
Moyens de preuve d'identité sur le numérique En référence ou non à une identité régalienne, sur la base d'un schéma d'identification qui repose sur 3 niveaux de sécurité au sein de l'UE	→ Identifiants et mots de passe → Boitiers générateurs de code → Logiciels de reconnaissance faciale → …

Mandat du projet : identifier les usages "locomotives" pour le développement de l'identité numérique (au sens de solution d'identification numérique en lien avec le déploiement de la future CNIe)

Source : Documentation Programme, DINSIC ; Analyses BCG & EY-Parthenon

La définition d'une solution d'identité numérique sécurisée peut être approchée au travers de 3 questions

À quoi sert-elle ?

Identifier les citoyens de manière numérique pour leur permettre de s'authentifier dans leurs démarches administratives en ligne

Offrir aux individus et aux organisations d'autres fonctionnalités :

- Echanges d'attributs d'identité et de données
- Autorisation et consentement
- Délivrance de prestations (numériques, physiques)

Pour quels bénéfices (directs et indirects) ?

Pour les usagers : des parcours plus simples et sécurisés, de nouveaux services et une maîtrise du partage de leurs données

Pour les Fournisseurs de Services : lutter contre la fraude, maîtriser ses coûts, une traçabilité renforcée et des opportunités d'innovation

Comment se concrétise-t-elle ?

Lors de la phase d'enrôlement, les citoyens récupèrent la carte et active l'identité numérique

Ils peuvent alors l'utiliser au quotidien

En cas de perte ou de vol, elle est sécurisée et peut être reconfigurée

Source : Documentation Programme, DINSIC ; Analyses BCG & EY-Parthenon

Définitions et notions clés

Etapes du parcours de l'usager

- **Enrôlement :** 1ère étape de la création d'une identité numérique, permettant de vérifier une identité déclarée vis-à-vis d'une source faisant autorité
- **Identification électronique :** Consiste à utiliser des données d'identification personnelle sous une forme électronique représentant une personne physique ou une personne morale (communiquer une identité préalablement enregistrée à l'aide d'un identifiant)
- **Authentification électronique :** Fait de produire la preuve de l'identité présentée a priori, en vue d'accéder à un service (apporter la preuve de cette identité : mot de passe, preuve biométrique, question secrète, etc.)
- **Moyen d'identification et d'authentification électronique :** Elément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service (physique ou numérique)
- **Ecosystème d'identités numériques :** Environnement organisé utilisant des systèmes numériques, éventuellement sous forme de plateforme, permettant de gérer un ou plusieurs schémas d'identités

Acteurs de l'identité numérique

- **Fournisseur d'identité :** Acteur chargé de mettre à disposition les moyens d'identification et garantir l'identité des utilisateurs
- **Fournisseur de services :** Acteur utilisant des identités numériques dans le cadre de la mise à disposition d'un service

Cadre de l'identité numérique

- **Architecture centralisée/décentralisée :** Paradigme informatique consistant soit à centraliser les données dans une même base, soit à distribuer les infrastructures et l'enregistrement des données dans plusieurs bases (en particulier pour en garantir la sécurité et améliorer la résilience du système)
- **Schéma d'identification électronique :** Système en vertu duquel les moyens d'identification électronique sont attribués. Ce document comporte des indications sur les niveaux de garantie, les autorités responsables, les schémas retenus et sur le régime de contrôle.
- **Règlement eIDAS :** Règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur définissant les 3 niveaux de garantie (faible, substantiel, élevé) pouvant être accordés à un moyen d'identification électronique. Il exige la reconnaissance mutuelle des moyens d'identification électronique notifiés par les Etats membres au niveau substantiel ou élevé, à compter du 29 septembre 2018 et vise à établir un cadre d'interopérabilité pour les différents systèmes.

Source : Documentation Programme, DINSIC ; Analyses BCG & EY-Parthenon

L'identité numérique sécurisée peut porter plusieurs fonctionnalités et services personnalisés (numériques ou physiques, privés ou publics)

À quoi sert-elle ?

Pour quels bénéfices (directs et indirects) ?

Comment se concrétise-t-elle ?

Identification	→ Communication d'une identité préalablement enregistrée à l'aide d'un identifiant (ex. un nom, un numéro de téléphone, une adresse mail, etc.)
Authentification	→ Apporter la preuve de cette identité (ex. : entrer un mot de passe, répondre à une question secrète, apporter une preuve biométrique, etc.)
Échanges d'attributs et de données	→ Transmission de données personnelles, de façon sélective, qu'il s'agisse des données pivots ou d'autres attributs d'identité (ex. données de santé, revenus, etc.)
Autorisation et consentement	→ Autorisations du détenteur de l'identité (ex. : signature électronique)
Délivrance de services de confiance (numériques et physiques)	→ Création de droits d'accès (ex. : en famille, en entreprise, etc.) et de processus de traçabilité (cachets électroniques, horodatages électroniques, recommandés électroniques, etc.) → Accès sécurisé traçable (ex. aéroports, prisons, sites sensibles)

☐ Fonctionnalités potentielles adossées à l'identité numérique

Source : Documentation Programme, DINSIC ; Analyses BCG & EY-Parthenon

L'identité numérique sécurisée peut bénéficier aux usagers ainsi qu'aux fournisseurs de services

Exemples – Non exhaustif

À quoi sert-elle ?

Pour quels bénéfices (directs et indirects) ?

Comment se concrétise-t-elle ?

Bénéfices usagers :

- Bénéficier de délais d'attentes plus courts et d'une réduction des déplacements requis
- Bénéficier de plus fortes garanties, être rassuré dans le cadre d'un recours à un service (ex. : économie collaborative, via l'authentification de l'identité des acteurs)
- Bénéficier d'un processus d'identification simplifié (ex. : réduction du nombre d'identifiants/mots de passe)
- Bénéficier de services personnalisés sur base de données mises à disposition avec consentement (bénéfice indirect)
- Contrôler la mise à disposition des données personnelles ainsi qu'obtenir une visibilité sur les acteurs les consultant (bénéfice indirect)

Bénéfices fournisseurs de services :

- Réduire / supprimer la fraude et les usurpations d'identité
- Optimiser ses coûts (ex. suppression des tâches, réduction des charges d'accueil)
- Retracer de façon certaine l'identité des usagers, renforcer les leviers de conformité
- Créer de nouveaux services et propositions de valeur, développer l'usage (ex. économie collaborative)

Bénéfices communs :

- Proposer / bénéficier d'un parcours client unifié (fluide et sécurisé) par le biais d'une centralisation des identifiants et comptes utilisateurs, ainsi que par la suppression des procédures de réassurance fastidieuses et une simplification des échanges de données

Source : Documentation Programme, DINSIC ; Analyses BCG & EY-Parthenon

Le paysage de l'identité numérique repose sur 3 types d'acteurs : les intégrateurs, les fournisseurs d'identité et les fournisseurs de services

	Types d'acteurs	Exemple en France
À quoi sert-elle ?	**Fournisseur d'identité** Autorité ou entité certifiant l'identité de l'usager en se positionnant en tant que tiers de confiance. Les solutions d'identification développées par les FI sont qualifiées de niveau faible, substantielles ou élevées (cf. infra – selon les définitions du règlement européen eIDAS)	**À date, 5 fournisseurs d'identité participent à France Connect**
Pour quels bénéfices (directs et indirects) ?	**Fédérateur d'identité** Dispositif permettant de faciliter l'accès aux services en ligne via un moyen d'identification et d'authentification unique	**FranceConnect, développé par la DINSIC, joue le rôle de fédérateur en France**
Comment se concrétise-t-elle ?	**Fournisseur de service** Tierce personne physique ou morale souhaitant vérifier la véracité d'une identité ou d'un document, dans le but de fournir un service en ligne, se positionnant ainsi en tant que tiers requérant	**+ de 460 fournisseurs de services[1]** actuellement accessibles via France Connect (ex. : Télépoints, Info-Retraite, etc.)

Note 1 : Au 28/01/2019
Source : Documentation Programme, DINSIC ; Analyses BCG & EY-Parthenon

Le parcours vu de l'usager comporte 3 temps : l'enrôlement, la récupération du moyen d'identification et son utilisation

À quoi sert-elle ?

Phase d'enrôlement

Je m'enregistre auprès d'un fournisseur d'identité, afin de créer mon « compte d'identification numérique », qui constitue l'étape clé me permettant d'utiliser le système d'identification pour m'identifier en vue d'avoir recours à des services (Ex. : création d'un compte Alicem à travers un processus impliquant que je valide la réception d'un code sur mobile ainsi que d'un e-mail, que je scanne un document d'identité via la technologie NFC, que je définisse mon code de sécurité et que j'effectue une reconnaissance faciale)

Pour quels bénéfices (directs et indirects) ?

Récupération du moyen d'identification

Je récupère mon moyen d'identification qui me permettra de m'authentifier au moment où je souhaiterai bénéficier d'un service qui nécessiterait de m'authentifier (Ex. : récupération d'un lecteur de carte ; réception d'un token générant des codes éphémères ; dans le cas d'Alicem, comme dans la majorité des schémas basés sur un moyen d'identification mobile, le moyen d'identification est représenté par l'application configurée durant la phase d'enrôlement)

Comment se concrétise-t-elle ?

Utilisation courante des moyens d'identification

J'utilise mon moyen d'identification pour accéder au service souhaité, en satisfaisant les différentes étapes requises par mon fournisseur d'identité (Ex. : lecture d'une carte d'identité numérique sur un boitier spécifique et introduction d'un code PIN)

Source : Documentation Programme, DINSIC ; Analyses BCG & EY-Parthenon

Exemples de solutions d'identification numérique (1/2)

	BankID	GOV.UK Verify	Aadhaar
Mode de reconnaissance	**Mot de passe & code en temps réel sur boitier**	**Mot de passe & code en temps réel sur mobile**	**Biométrie (empreintes digitales, iris)**
Supports nécessaires	**Boitier générateur de code**	**Fournisseurs d'identités et registres avec attributs d'identité**	**Base de données centrale**
Phase d'enrôlement	L'utilisateur se rend en physique à sa banque pour faire vérifier son identité (présentation d'un passeport	L'utilisateur choisit un fournisseur d'identité (ex. : Barclays), crée son mdp et lui fournit des données personnelles	L'utilisateur fournit ses données démographiques et biométriques aux autorités publiques
Mise à disposition du moyen d'identification	L'utilisateur reçoit un boitier générateur de code et son eID est créée	Le FI vérifie ces données en les comparant à divers registres (ex. : organismes de crédits) puis crée l'eID	Les données sont copiées dans une base centrale puis un n° d'identité unique est transmis à l'utilisateur
Utilisation du moyen	Pour utiliser cette eID, l'utilisateur doit renseigner son numéro d'identité norvégien, le code généré par le token et son mot de passe	Pour utiliser cette eID, l'utilisateur doit renseigner son mdp et un code envoyé sur son téléphone mobile	L'ID est vérifiée avec des scanners biométriques pour accéder à des services publics et privés

Source : Analyses BCG & EY-Parthenon

Exemples de solutions d'identification numérique (2/2)

Zoom sur les 3 étapes du parcours de l'utilisateur *d'Alicem*

Etapes	Description
Phase d'enrôlement	1. Je **télécharge l'application** sur mon smartphone (équipé de la technologie NFC) 2. Je saisis mon **numéro de mobile**. Un **code de confirmation** à copier dans l'application est envoyé par SMS. 3. Je saisis **mon adresse e-mail**, puis je la valide en répondant à la demande de **confirmation envoyée sur ma boîte mail** 4. Je **scanne avec mon smartphone la bande MRZ** de mon passeport ou de mon titre de séjour. 5. Je pose mon téléphone sur mon passeport ou mon titre de séjour pour **une lecture sans contact de la puce** 6. Je définis **mon code de sécurité** 7. J'effectue une **reconnaissance faciale en mode selfie**
Mise à disposition du moyen d'identification	→ L'authenticité et la validité des informations sont vérifiées auprès des services de l'Etat (DOCVERIF) → Le compte est **créé et activé**
Utilisation du moyen	→ Je saisis l'ID Alicem et reçois une **notification par SMS** me demandant de valider la demande → J'ouvre **l'application**, saisis le **code de sécurité** (voir scanne mon passeport dans le cas d'usage associé à un niveau élevé) → Ma demande est validée sur **l'application et j'accède au service**

Source : Analyses BCG & EY-Parthenon

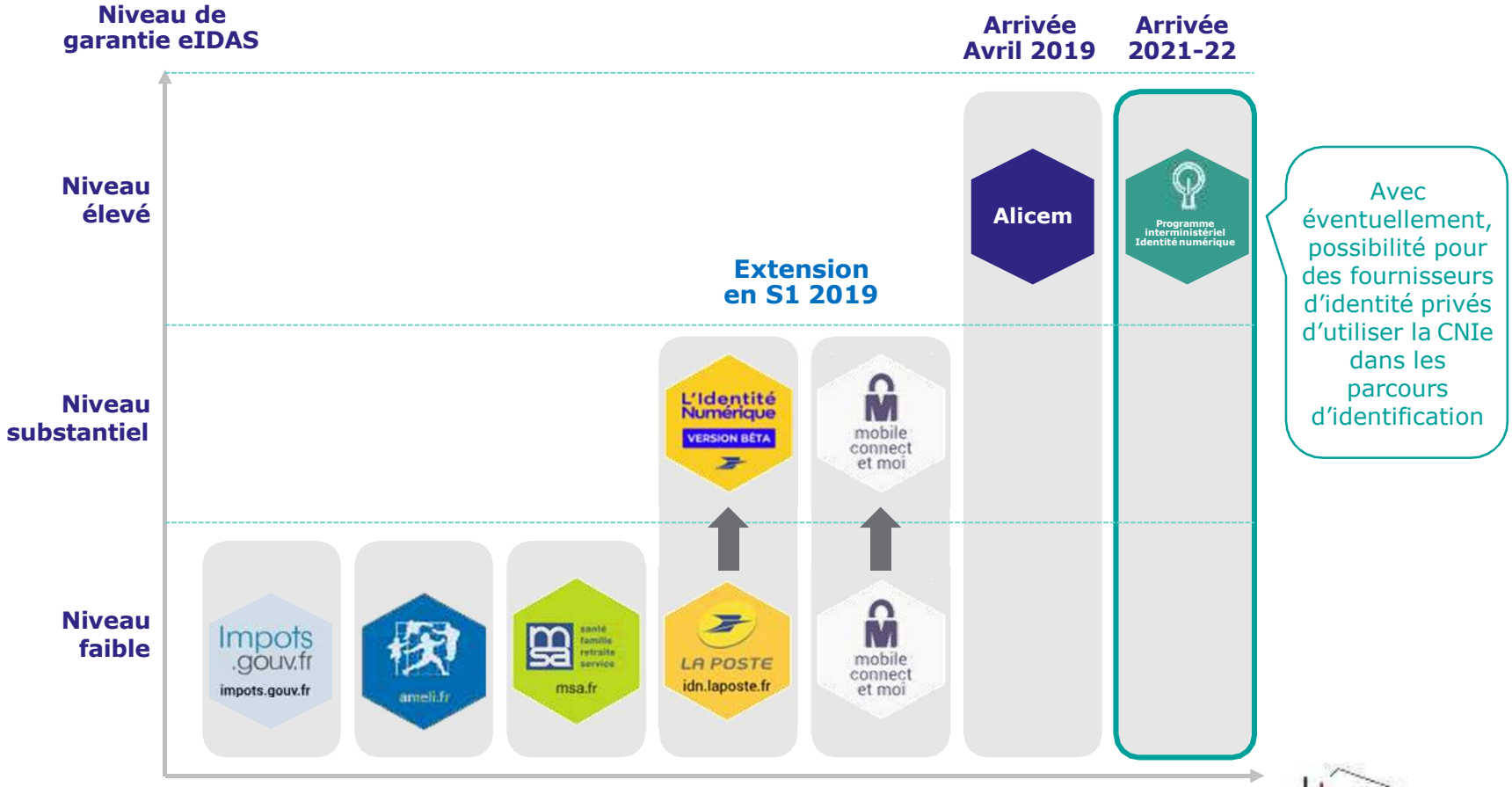
Pour mémoire : le règlement eIDAS définit 3 niveaux de garantie associés aux moyens d'identification

	Faible : Présumer	**Substantiel : Vérifier**	**Élevé : S'assurer**
Objectif à atteindre	Réduire le risque d'utilisation abusive ou d'altération d'identité	Réduire substantiellement le risque d'utilisation abusive de l'identité	Empêcher l'utilisation abusive ou l'altération de l'identité
Implications pour la phase d'enrôlement et de mise à disposition	**Vérification limitée de l'identité du demandeur et de sa validité** Ex. : scan de pièce d'identité avec vérification basique de l'authenticité et de la validité	**Vérification de la possession de la pièce d'identité, de son authenticité, de sa validité et risque maitrisé que la pièce se rapporte à une autre personne** Ex. : présentation pièce d'identité en ligne + comparaison photo avec selfie	**Identification évidente du demandeur via une ou plusieurs caractéristiques physiques** Ex. face à face pour la CNI Ex. pour le passeport, à distance possible via vérification dynamique de la puce et reconnaissance faciale
Implication pour la phase d'utilisation	1 facteur d'authentification « Ce que je sais » Ex. : Mot de passe ou code	2 facteurs d'authentification « Ce que je possède/je suis » Ex. : possession d'un smartphone + code PIN, si facteur matériel, remise en main propre ou en recommandé	2 facteurs d'authentification « Ce que je possède/je suis » Ex. : carte à puce avec PIN ou bio, solution sur smartphone utilisant un composant matériel qualifié (carte SIM, etc.)

Une distinction entre le niveau substantiel et élevé quasiment imperceptible du point de vue de l'usager en termes de parcours d'identification/authentification

Source : Agence Nationale de la Sécurité des Systèmes d'Information (ANNSI) ; Documentation Programme, DINSIC ; Analyses BCG & EY-Parthenon

L'écosystème de fournisseurs d'identité en France déploie des solutions permettant de couvrir les niveaux substantiels et élevés à terme



Sommaire

L'approche retenue pour recenser et qualifier les usages privés et publics combine plusieurs sources complémentaires

Usages privés

Conduite d'entretiens avec des experts sectoriels* et capitalisation sur les travaux existants (Programme, DINSIC), en vue de recenser les usages potentiels au sein des verticales sectorielles identifiées et de recueillir les besoins de sécurité associés (qui devront faire l'objet d'analyses complémentaires pour mesurer les bénéfices)

Exploitation de documents spécifiques (livres blancs, études de marché, recherche BCG EY, etc.) en vue de qualifier le potentiel de recours à l'usage

Benchmark international

Ex. de programmes d'eID de pays européens et/ou matures en termes numériques

Voix des usagers

Recherche qualitative

4 sessions de ~8 usagers avec des profils diversifiés

Etude quantitative

un questionnaire auprès de ~1200 répondants représentatifs de la population française

(internet et téléphone)

Usages publics

Capitalisation sur les travaux déjà existants et les ressources documentaires au sein de la DITP, du Programme et de la DINSIC, ainsi que sur les grands programmes en cours (ex. Simplification, Demat), en focalisant l'analyse sur les usages de niveau de sécurité élevé ou substantiel

Exploitation de documents spécifiques (rapports gouvernementaux, rapports de la cour des comptes, études BCG, etc.) en vue d'alimenter la qualification

~25 usages privés et ~55 usages publics recensés et qualifiés

(*) Voir liste détaillée en annexe 1

Plusieurs critères ont été utilisés pour identifier les usages à potentiel et caractérisés par un besoin élevé de sécurité (de façon non systématique)

Qualification du potentiel

Volumes

- **Volume de recours annuel à l'usage***
- **Fréquence de recours à l'usage**
- **Potentiel d'usagers concernés**
  (Appétence ; Degré d'irritation et de contrainte)

Usagers

- **Amélioration de la fluidité du parcours usager**
  (Délais d'attente, déplacements réduits, etc.)
- **Degré d'intérêt des usagers**
  (Enquête qualitative et quantitative)

Fournisseurs

- **Horizon de faisabilité**
- **Potentiel d'optimisation des coûts**
  (Qualitatif et/ou quantitatif)
- **Potentiel de création de valeur**
  (lutte contre la fraude, Ux, maîtrise des coûts)

Qualification du besoin de sécurité

Usagers

- **Besoin de protection exprimé vis-à-vis de l'usage**
  (Enquête qualitative et quantitative)
- **Sensibilité perçue des données impliquées, valeur symbolique**

Fournisseurs

- **Contraintes juridiques/ réglementaires existantes et projetées**
  (Y compris les enjeux régaliens)
- **Taux de fraude existant et projeté**
- **Risques liés aux fraudes**
  (Y compris le coût de la fraude)
- **Besoin de sécurisation exprimé, image**
  (Qualitatif**)

(*) Source : données publiques, analyse et estimations BCG & EY-Parthenon (notamment pour usages émergents)
(**) Source : entretiens experts sectoriels et données déclaratives recueillies par le programme ID NUM ; propositions BCG & EY-Parthenon lorsque déclaratif non disponible

Sommaire

2. Analyses des usages

- Benchmark géographique
- Enjeux des fournisseurs de services
  - Enjeux des fournisseurs de services privés
  - Enjeux des fournisseurs de services publics
- Analyse des besoins et usages des Français

Le benchmark géographique a permis de faire ressortir plusieurs enseignements tirés des différents dispositifs d'identité numérique étudiés

Une nécessité de centrer la réflexion sur l'usager et l'ergonomie
- Les pays ayant privilégié le développement de solutions technologiques à fort niveau de sécurité de manière antérieure à la réflexion des différents usages associés, ont connu un succès mitigé (Ex. : Allemagne, Belgique, Suisse)
- L'ergonomie de la solution représente un facteur majeur dans l'adoption du moyen déployé

Trois approches possibles identifiées qui renvoient à des contextes politiques et culturels très différents
- Une approche fondée sur un support physique régalien (Ex. : Allemagne, Belgique, etc.)
- Une approche fondée sur une identité numérique désolidarisée du support, pouvant être adossée à différents dispositifs tels que les cartes bancaires, SIM, de santé, smartphone, etc. (Ex. : Autriche, Finlande, etc.)
- Une approche fondée sur la biométrie et des bases de données / registres centralisés (ex. Inde)

Une nécessité de prioriser des usages massifs (population et fréquence d'usage) dès le lancement de l'identité numérique – certains, très populaires, pouvant être considérés comme des passages obligés (usages "évidents")
- La gestion des dossiers médicaux
- Les renouvellements de titres d'identité
- La gestion des permis de conduire
- L'accès aux comptes bancaires

Le niveau de sécurité élevé au sens eIDAS n'est pas un point d'entrée pertinent dans les programmes les plus ambitieux d'identité numérique
- La distinction des différents niveaux de sécurité associés aux usages n'a pas représenté un élément central dans les réflexions entourant le déploiement des dispositifs d'identité numérique dans les pays analysés

Des bonnes pratiques liées à la stratégie de déploiement, primordiales dans le succès de l'adoption
- Générer l'adoption autour de cas d'usage incontournables auprès de l'ensemble de la population (Ex. : banque)
- Adresser efficacement les enjeux d'interopérabilité et éviter la coexistence de multiples schémas
- Etablir rapidement et de manière proactive les règles régissant le schéma auprès des fournisseurs de services
- Construire la séquence de développement en fonction de l'ambition de dématérialisation (Ex. : adossement à une boîte aux lettres administrative électronique avec un abandon progressif des échanges de courriers papier ; facilitation de l'activation de la solution en privilégiant les clauses d'opt-out plutôt que les clauses d'opt-in)

Note : clause d'opt-out (l'identité numérique de l'usager est activée dès l'introduction de sa CNIe) vs clause d'opt-in (l'utilisateur doit demander à la faire activer)
Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Des facteurs de différentes natures ont influencé l'adoption de la solution déployée au sein des pays investigués

Pays et date de lancement	Adoption	Retours	Facteurs
Carte e-ID 2010 (Physique)	30%	Mitigés	Un lancement tardif, devancé par différents prestataires de services (ex. : banques) Une solution non-aboutie d'un point de vue technique (ex. : compatibilité limitée avec les systèmes d'exploitation) Une activation optionnelle, payante et un processus d'enrôlement et de recours aux services fastidieux Des difficultés éprouvées à convaincre les prestataires en raison d'une perception d'un nombre d'usagers trop faible
Digital iD 2016 (Démat.)		Mitigés	Une acceptabilité sociale limitée par une absence de législation spécifique au programme Une communication liée au déploiement limitée, notamment au sujet des bénéfices et des implications de la solution Un choix de technologie mal perçu par les citoyens et une coexistence de schémas d'identification qui prête à confusion
Mobile ID 2009 (Démat.)	10%*	Positifs	Un coût d'enrôlement à charge du citoyen inexistant et une absence de dispositif matériel spécifique Des campagnes de communication efficaces (à direction des fournisseurs de services et des citoyens)
Carte eID 2004 (Physique)	100%	Mitigés	Un déploiement jugé trop lent (5 années pour une population de 11,5 millions) Une communication sur les bénéfices et implications de l'eID insuffisante Une diffusion inefficace des lecteurs de cartes indispensables à l'utilisation de l'eID Une apparition d'une alternative privée entièrement dématérialisée présentant un meilleur confort d'utilisation
NemID 2010(Mixte)	90%	Positifs	Un nombre élevé de services publics et privés accessibles dès le lancement pour favoriser l'adoption
Carte CIE 2016 (Physique)		Positifs	Un lancement de dispositif accompagné d'une communication autour de l'accès unique fourni par le système à des initiatives, non essentielles, en vue de stimuler l'adoption (ex. : Pass culturel)
BankID 2004 (Mixte)	75%	Positifs	Une acceptation de l'ensemble des acteurs bancaires, limitant l'intérêt de démultiplier les solutions d'identification Un nombre important de services publics et privés accessibles dès le lancement
DigiID 2005 (Démat.)	70%	Positifs	Une capitalisation sur une population caractérisée par une maturité digitale et un pourcentage élevé de démarches administratives disponibles en ligne
BankID 2003(Mixte)	76%	Positifs	La multiplicité des supports d'identification proposés (mobile app, carte à puce physique ou PC)
e-ID 2020e	n.a	Mitigés	Un retard du déploiement engendré par une multiplication de débats autour du rôle de l'Etat dans le dispositif
Verify 2016 (Démat.)	~5%	Mitigés	Un nombre faible de services accessibles (19 vs. 46 ciblés) et Un système de vérification au fort taux d'échec (~50%) Une mise en place plus couteuse que prévue et des économies réalisées moins importantes que ciblées

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

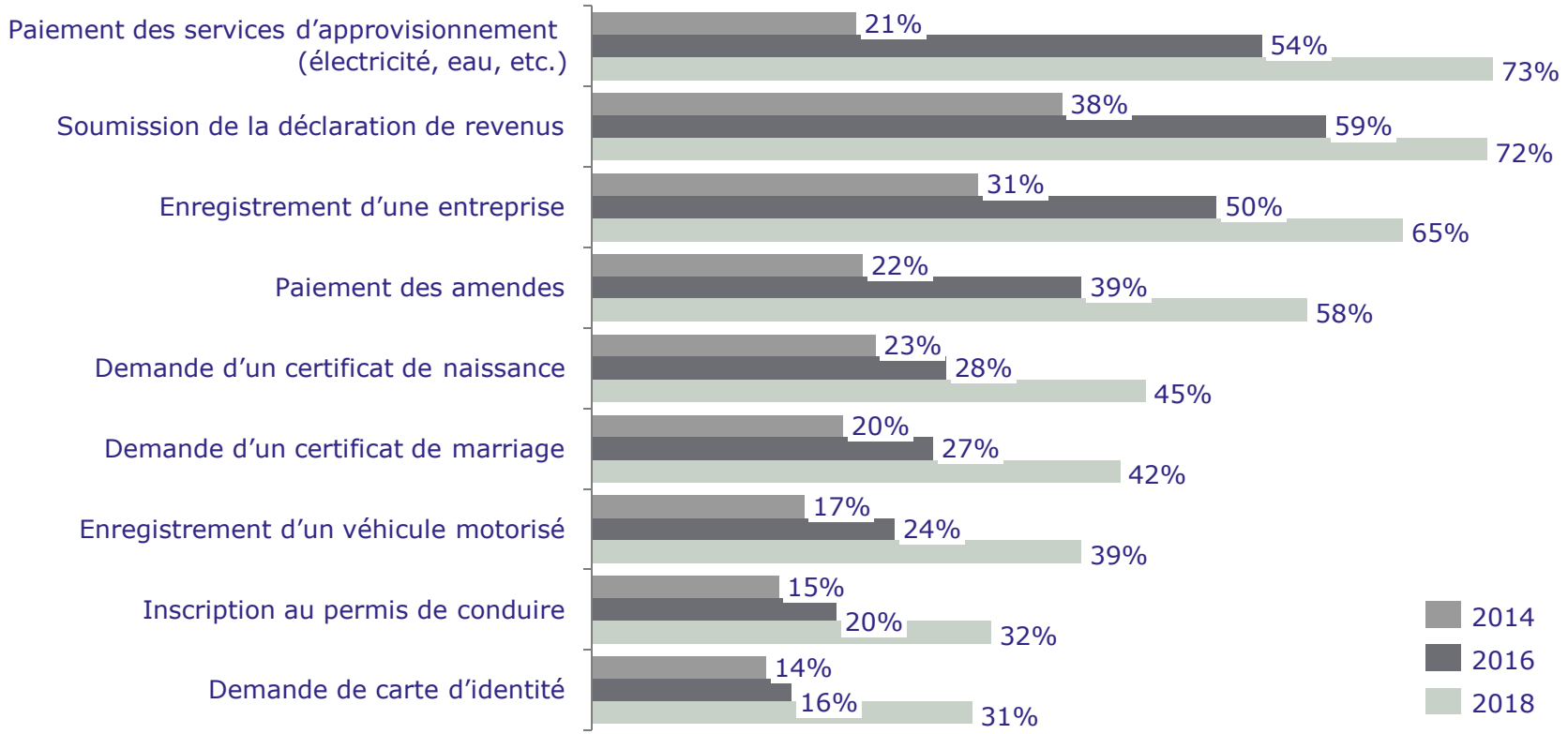
Certains usages de l'identité numériques apparaissent comme étant particulièrement populaires au sein des pays analysés

Pays et date de lancement	Facteurs
Carte e-ID 2010	→ Absence d'usages majeurs qui se distinguent → Usages privés pas adoptés en masse (notamment ceux en lien avec les services bancaires et l'e-commerce)
Digital iD 2016	→ Dossier de santé et remboursement de frais de santé → Gestion des impôts → Renouvellement du permis de conduire → Espace sécurisé de communication administrative
Mobile ID 2009	→ FinanzOnline : Portail en ligne de l'administration fiscale → ELGA : Système d'accès aux données de santé
Carte eID 2004	→ Déclaration en ligne d'impôts très largement désigné comme l'usage majeur (Tax-on-web), tandis que d'autres usages à volume bien plus faibles voient leur utilisation croître (dépôt de plainte, notification de naissance et suivi de dossier de pension)
NemID 2010	→ Digital Post : Canal de communication permettant aux autorités publiques de transmettre des communications électroniques → NemSMS : Service permettant aux autorités de contacter directement les citoyens par SMS (Ex. : rappel de RDV)
Carte CIE 2016	→ L'usage majeur mis en avant concerne le récipient électronique servant de canal de communication directe avec l'administration publique
BankID 2004	→ Recours aux services bancaires présenté comme le principal usage majeur du BankID, proposé par l'ensemble des banques → D'autres usages plébiscités : Signature électronique, achat en ligne, gestion patrimoniale et utilities
DigiID 2005	→ Gestion des impôts → Demande d'allocations → Gestion des pensions de retraite
BankID 2003	→ Transferts bancaires → Déclarations d'impôts → Achats en ligne
Verify 2016	→ Des usages majeurs difficilement identifiables compte tenu de l'état actuel du projet, avec une gestion du dispositif qui sera cédée à des partenaires privés en 2020

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

L'accès en ligne aux services publics transactionnels se généralise

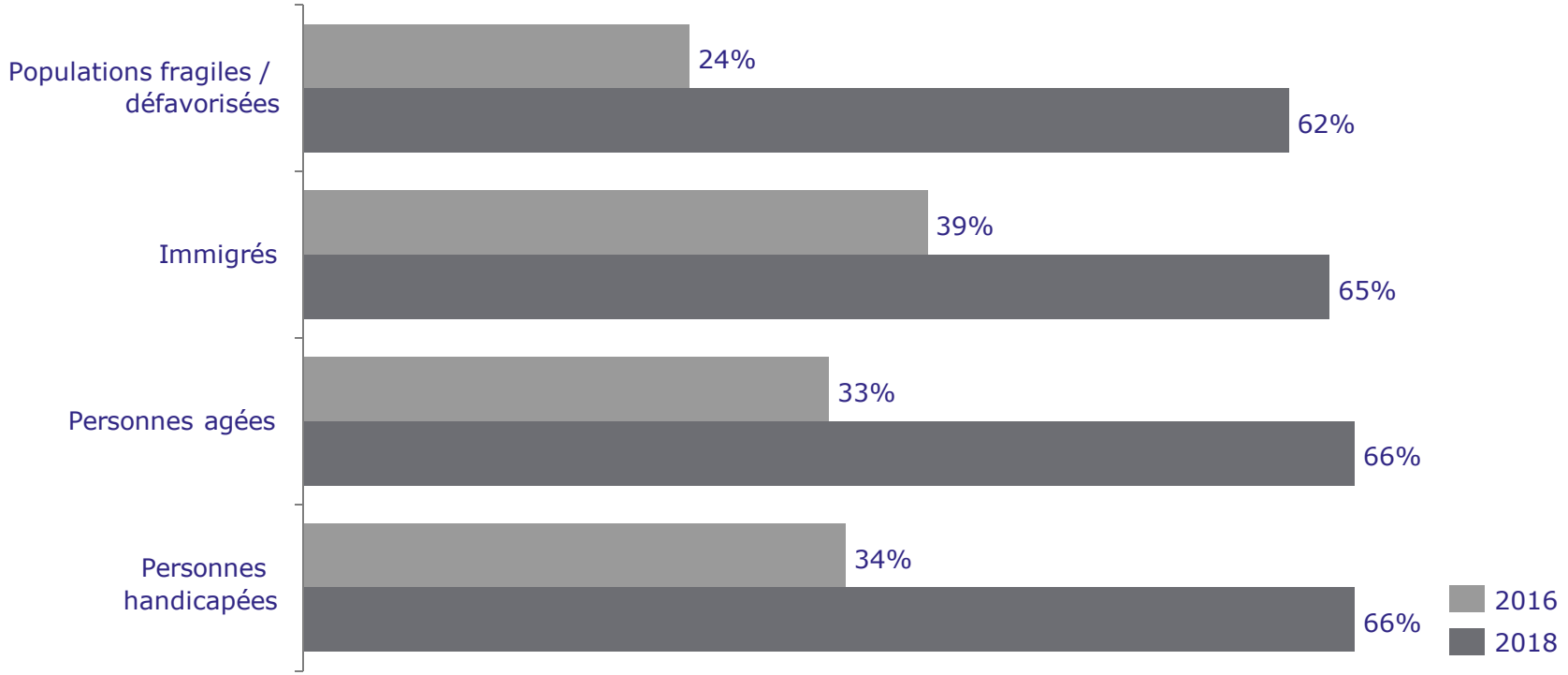
% de pays proposant les services ci-dessous en ligne (membres de l'ONU)



Note : 193 états membres de l'ONU
Source : Rapport de l'ONU "E-government survey 2018" ; Analyses BCG & EY-Parthenon

Les services publics en ligne à destination des populations les plus vulnérables se développent également

% de pays proposant des services publics en ligne aux catégories ci-dessous (membres de l'ONU)



Note : 193 états membres de l'ONU
Source : Rapport de l'ONU "E-government survey 2018« ; Analyses BCG & EY¨-Parthenon

L'UE a identifié des services publics en ligne accessibles grâce à une identité numérique qui sont particulièrement répandus en Europe

Activités professionnelles	→ Procédure de déclaration de TVA → Impôt sur les sociétés → Demande de remboursement de TVA → Transmission de données d'entreprises aux organismes de statistique → Cotisations sociales → Soumission des rapports financiers des entreprises → Signalement des maladies des employés
Déménagement	→ Communication de la nouvelle adresse (fiscalité, école, santé) → Désinscription de l'ancienne commune → Enregistrement de la nouvelle adresse dans le registre municipal
Transport	→ Paiement de l'impôt sur le véhicule / taxe de circulation → Immatriculation d'une voiture importée → Demande de certificat d'immatriculation pour véhicule de remplacement → Demande de carte / permis de stationnement → Traitement des amendes en lien avec la conduite
Justice	→ Récupération du jugement prononcé → Lancement de procédure pour petits litiges → Partage de preuves / documents d'appui par les citoyens → Appel contre la décision du tribunal

Source : Rapport "EU e-government benchmark 2018" ; analyse BCG
Note : Sélection parmi les services accessibles en ligne grâce à une eID de ceux qui sont proposés par le plus grand nombre de pays

Le benchmark géographique couvre principalement 11 pays, choisis en fonction de leur maturité digitale et avec un éclairage hors-UE

 **Allemagne**

 **Danemark**

 **Suède**

 **Australie**

 **Italie**

 **Suisse**

 **Autriche**

 **Norvège**

 **Grande-Bretagne**

 **Belgique**

 **Pays-Bas**

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Benchmark géographique - L'identité numérique en Allemagne

Allemagne

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
82,8 millions	Registre de population centralisé mais banques de données à l'architecture décentralisée	→ e-ID : Carte d'identité électronique à l'activation optionnelle (rendue systématique en 2017) déployée à partir de 2010 → Caractérisée par un niveau très élevé de sécurité, dicté par un contexte de création influencé par un cadre de sécurité des échanges et des données personnelles très rigoureux

Retours d'expérience sur la stratégie de déploiement

- → En 2017, l'eID permettait d'obtenir un accès à plus de 220 services fournis par plus de 110 prestataires (40% publics et 60% privés)
- → À mi-2017, estimation d'une activation d'uniquement 17 millions de cartes sur les 51 millions disponibles, notamment expliquée par :
  - > Un lancement perçu comme tardif, différents prestataires de services ayant développé leur propres solutions d'identification sécurisée (Ex. : banques) et accompagné par de nombreuses difficultés techniques (Ex : compatibilité limitée avec les OS et navigateurs, etc.)
  - > Une activation optionnelle et payante (~30 euros), rendue systématique uniquement depuis le milieu de l'année 2017
  - > Une activation bien supérieure dans les grandes agglomérations que dans les régions disposant d'une offre de service en ligne limitée
  - > Des difficultés éprouvées à convaincre les prestataires privés d'adopter l'eID, en raison d'un nombre d'usagers perçu comme trop faible
  - > Un processus d'enrôlement et un recours aux services décrits comme fastidieux, malgré des aménagements juridiques et un assouplissement du cadre sécuritaire engagés en 2012
- → Apparition en 2017 d'une solution concurrente, Verimi, développée par un consortium d'acteurs privés (dont Allianz, Daimler ou encore Axel Springer) entièrement basée sur mobile et plébiscitée pour sa simplicité d'utilisation

Usages majeurs

- → Absence d'usages majeurs
- → Les usages privés ne semblent pas avoir été adoptés en masse, notamment au niveau des usages bancaires et du e-commerce
- → Principal levier de développement de l'accès aux services publics online via une simplification des processus d'identification et d'authentification

« Il n'existe pas d'application en ligne phare qui justifie à elle seule un investissement, pas plus qu'il n'existe de services sur une autoroute reliant une région entière qui suffirait à justifier sa création et à garantir sa rentabilité dès le départ.

Efficacité, gain de temps, sécurité et proximité sont les moteurs initiaux. Les services viennent ensuite, lentement mais sûrement »

Gemalto

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Benchmark géographique - L'identité numérique en Australie

Australie

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
24,6 millions	Bases de données des documents d'identité délivrés par l'Etat (ex. : passeports, permis de conduire)	→ Plusieurs sources d'identités numériques : > Digital ID, service d'identification développé par Australia Post > myGovID, service d'identification en cours de développement par l'Etat (Digital Transformation Agency)

Retours d'expérience sur la stratégie de déploiement

- → MyGov a été d'abord un système d'identifiant unique permettant d'accéder à tous les services publics (accès aux services publics optionnel au début, puis obligatoire au bout de 3 ans, ce qui a permis de circonscrire les craintes liées à la protection des données personnelles), avec une stratégie inextricablement liée à la stratégie de numérisation des démarches administratives
- → Le dispositif myGovID rencontre néanmoins différentes difficultés :
  - > La version de lancement était très imparfaite en termes d'UX, ce qui a énormément pénalisé le déploiement de la solution (qui a été l'objet de railleries persistantes durant de longues années)
  - > Son acceptabilité sociale reste limitée car l'Etat n'a pas introduit de législation spécifique à ce programme et a peu communiqué sur ses bénéfices et ses implications (Ex. : protection des données)
  - > Le système de reconnaissance faciale utilisé est souvent confondu avec celui utilisé par la police australienne, générant des inquiétudes et des suspicions auprès des citoyens
  - > Le programme est en compétition directe et souvent confondu avec le service d'identification sécurisée développé par Australia Post, Digital ID
- → myGovID est en phase de test et s'ouvre progressivement à de nouveaux usages publics, tels que l'obtention d'un numéro fiscal, l'enregistrement d'une entreprise, la demande de subventions / bourses (notamment pour les jeunes et les personnes sans emploi), accès à My Health Record (résumé en ligne de données personnelles de santé) ou encore l'obtention d'un numéro d'identifiant étudiant, tandis qu'une ouverture aux fournisseurs privés est également engagée
- → Une gestion de la fracture digitale (~20% de la population) adressée à travers la possibilité de ce connecter au système via un aidant ou un tiers, ou encore, pour les 5% estimés de la population qui reste marginalisée, à travers une logique de centres d'accueil physiques pluridisciplinaires

Usages majeurs

- → Dossier de santé et remboursements des frais de santé (avec suppression progressive des remboursements cash, générant un palier d'adoption)
- → Impôts (de même, démarche en ligne progressivement rendue obligatoire)
- → Renouvellement des permis de conduire (il n'y a pas de CNI en Australie)
- → L'adresse mail administrative, qui s'est développée de façon contrainte suite à la suppression progressive des envois administratifs en format papier et se présente sous la forme d'un espace sécurisé

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Focus sur Digital iD, le programme concurrent de myGovID

Australie

Digital iD, une solution d'identité numérique sécurisée…

Objectif

Utilisation d'une identité numérique intégrée à une application mobile pour s'identifier et interagir avec les acteurs publics et privés

Création

Développé et lancé par Australia Post en 2017, pour un coût estimé de 30 à 50 millions de dollars

Lieu

Approuvé pour utilisation au sein du Territoire de la capitale australienne, du Territoire du Nord, du Queensland, de la Tasmanie et de l'Etat de Victoria

Partenaires

De nombreux partenaires notamment privés acceptent Digital iD comme moyen d'identification des usagers

… pour simplifier le processus d'identification des utilisateurs

1. Création de l'eID : l'utilisateur télécharge l'application, vérifie son numéro de portable et prend en photo un document d'identité
2. Vérification de l'eID : l'image est vérifiée en croisant des bases de données gouvernementales grâce à la blockchain et aux données biométriques
3. Utilisation de l'eID : l'utilisateur est en capacité de prouver son identité auprès de chaque partenaire Digital iD, sans vérification additionnelle

Benchmark géographique - L'identité numérique en Autriche

Autriche

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
8,8 millions	Un numéro unique rattaché à chaque citoyen, directement issu du registre de population et décliné de manière distincte dans chaque secteur (financier, social, fiscal, etc.)	→ Identité numérique multi-supports : > Carte de citoyen (BuergerKarte) > Cartes bancaire et de santé, cartes d'agents (notaires, avocats, etc.) et certaines cartes d'étudiant > Téléphone mobile (Mobile ID)

Retours d'expérience sur la stratégie de déploiement

- → Un succès du support carte particulièrement rencontré auprès des entreprises, tandis que les particuliers tendent à préférer le support mobile
  - > Un succès du mobile ID basé sur l'absence de dispositif matériel supplémentaire nécessaire (pas de nécessité de changer de SIM), une simplicité d'activation ainsi que des coûts d'enrôlement inexistants à charge du citoyen
  - > Décision d'orienter les nouveaux développements vers la gestion des données sur le cloud et la gestion de l'identité numérique sur les différents dispositifs mobiles
- → Une estimation de 700 000* utilisateurs utilisant activement le mobile ID (vs. 120 000* utilisateurs actifs de supports carte)
  - >Le mobile ID fournit l'accès à plus de 300* services en ligne, privés et publics
- → Une importance soulignée des campagnes de communication dans l'adoption
  - > À direction des fournisseurs de services, à travers des conférences et ateliers
  - > À direction des citoyens, à travers des campagnes de mail, des mentions sur l'ensemble des sites administratifs et des campagnes publicitaires

Usages majeurs

- → Deux usages majeurs plébiscités (voir slide suivante) :
  - > FinanzOnline : Portail en ligne de l'administration fiscale
  - > ELGA : Système d'accès aux données de santé

Note : Données d'Octobre 2016
Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Focus sur des exemples de cas d'usage

Autriche

	FINANZONLINE.AT	elga
Description	FinanzOnline est le portail en ligne de l'administration fiscale autrichienne pour les citoyens et les entreprises (déclarations de revenus, de TVA, etc.)	ELGA est le SI permettant un accès sécurisé aux données de santé personnelles (Ex. : résultats de laboratoire, résultats médicaux, etc.) pour les patients et les prestataires de soins
Identification numérique	Accès par le biais d'eID ou de mobile ID	Accès par le biais d'eID ou de mobile ID
Utilisateurs	FinanzOnline dispose de plus de 4,7 millions d'utilisateurs (~54% de la population)	La moitié des citoyens autrichiens ont recours à ELGA, qui collabore avec +160 établissements de santé

Source : Rapport "EU e-government benchmark 2018"

Benchmark géographique - L'identité numérique en Belgique

Belgique

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
11,4 millions	Enregistrement des données confié aux communes et à l'office des étrangers	→ eID : Carte d'identité électronique obligatoire déployée en 2004 > Versions spécifiques destinées aux -12 ans et aux étrangers > Munie d'une puce dotée d'un certificat d'authentification ainsi que d'un certificat d'apposition de signature électronique

Retours d'expérience sur la stratégie de déploiement

- Mise en place initiale d'une solution par le gouvernement dans l'optique de devancer les acteurs privés
- Généralisation de l'eID étalée sur une durée de 5 années, ayant permis d'atteindre 100% de la population cible en 2009, avec 2 années de retard sur l'objectif fixé, pour un coût estimé à 250 millions d'euros
- À date, parmi les 80 services de E-gouvernement accessibles en ligne, 22 sont accessibles par le biais de l'eID parmi lesquels un service d'impôt en ligne, Tax-on-web ou encore le portail de pension, mypension (cf. liste détaillée)
- Une utilisation des services en ligne en deçà des attentes, notamment expliquée par :
  - Un déploiement jugé trop lent, une communication sur les bénéfices et implications insuffisante et une diffusion inefficace des lecteurs de cartes indispensables à l'utilisation de l'eID
- Apparition en 2017 d'une l'alternative privée Itsme, application crée par le consortium Belgian Mobile ID regroupant 4 grandes banques et 3 opérateurs de réseaux mobiles, plébiscitée pour sa facilité d'utilisation qui passe exclusivement par mobile en liant son identité à sa carte sim
  - Une utilisation et une satisfaction en croissance (+114% d'utilisateurs entre mai 2018 et février 2019), stimulées par des mises à jour régulières élargissant l'éventail de partenaires
  - Un solution plébiscitée comme étant l'une des plus réussies en Europe, avec une moyenne de 6 transactions bancaires et 3 transactions e-gouvernementales par usager chaque mois

Usages majeurs

- L'usage majeur demeure de loin la déclaration d'impôts via Tax-on-Web, exploitée par près de 6 millions de citoyens en 2018
  - Police-on-Web : dépôt de plainte en ligne, prévoir un message d'absence et notifier vos systèmes d'alarme
- E-Birth : notification électronique d'une naissance par un prestataire de soins à l'état civil de la commune et envoi électronique des données statistiques aux Communautés
- MyPension : portail de suivi de dossier de pension

Source : Entretiens experts internationaux (voir annexe 1) ; Rapport de la cour des comptes ; Digital Belgium ; Recherche documentaire ; Analyses BCG & EY-Parthenon

22 services majeurs accessibles via l'eID belge (1/2)

Belgique

Thème	Intitulé / objet du service	Description
Economie	Finprof	Permet de transmettre à l'administration les déclarations au précompte professionnel
	My Enterprise	Permet aux entrepreneurs et indépendants d'accéder aux données de son entreprise dans la Banque-Carrefour des Entreprises et de centraliser la mise à jour des données
Famille	E-birth	Notification électronique d'une naissance par un prestataire de soins à l'état civil de la commune et envoi électronique des données statistiques aux Communautés
	E-Box	Boite aux lettres électronique accueillant les documents officiels émanant des administrations de la sécurité sociale
Impôts	Belcotax	Permet aux employeurs d'introduire et d'envoyer les fiches de rémunérations, attestations de libéralité, commissions, etc.
	Intervat	Permet de déposer différents types d'envois de TVA
	My Minfin	Application permettant au citoyen de gérer son dossier fiscal (intégrant également Tax-on-web)
	Tax-on-web	Permet aux personnes physiques de réaliser leur déclaration d'impôts
Justice	E-greffe	Permet le dépôt de dossier de création d'association / entreprise en ligne
	Police-on-web	Permet d'effectuer différentes déclarations auprès de la police ainsi que l'enregistrement d'un système d'alarme
Santé	E-health	Divers services aux entreprises, citoyens, institutions (hôpitaux, groupements d'infirmiers,…) et aux professionnels des soins de santé (Ex. : e-shop d'attestations de soins donnés)

Personne physique Personne morale

Source : Rapport de la cour des comptes ; Analyses BCG & EY-Parthenon

22 services majeurs accessibles via l'eID belge (2/2)

Belgique

Thème	Intitulé / objet du service	Description
Economie	SNCB ticket online	Permet d'acheter à distance les validations de Cartes Train et la plupart des billets
Famille	Pension	Permet d'effectuer une demande de pension ou de garantie de revenus aux personnes âgées
	Mypension	Portail de suivi de dossier de pension
	Chômage temporaire	Permet aux employeurs de satisfaire aux obligations de communication dans les situations de chômage temporaire
	Risques sociaux	Permet la déclaration de risques sociaux en ligne (licenciement, arrêt maladie de longue durée, etc.)
	Horeca@work	Permet au travailleur occasionnel du secteur de l'Horeca de consulter le nombre de jours où il bénéficie d'un calcul avantageux des cotisations de sécurité sociale
	Interruption de carrière	Permet de consulter son dossier d'interruption de carrière ou de crédit-temps
	Compte de vacances	Permet aux ouvriers, apprenti-ouvrier ou artistes de consulter ses propres données de vacances à travers le portail de sécurité sociale
	Mon Selor	Permet de postuler en ligne aux services publics fédéraux en vue de remplir les postes vacants contractuels
	Mycareer	Fourni un aperçu de l'historique de carrière: emplois précédents et actuel, salaire cumulé, nombre de jours prestés, périodes d'inactivités, etc.
	Student@work	Permet aux étudiants de vérifier le nombre de jours de travail qu'ils peuvent prester à un taux de cotisations sociales réduit

Personne physique Personne morale

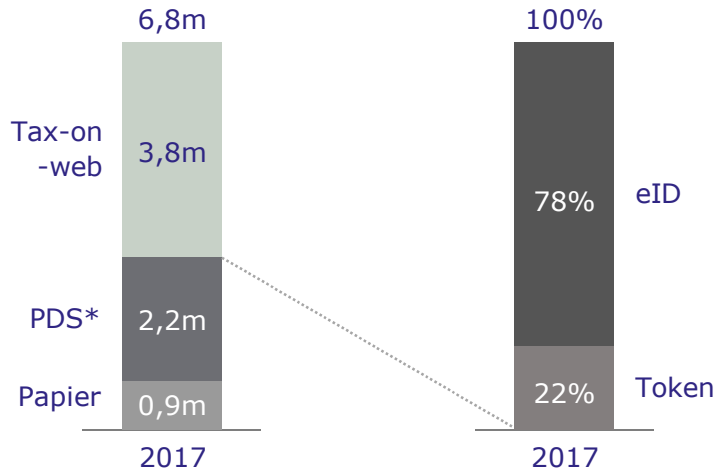
Source : Rapport de la cour des comptes ; Analyses BCG & EY-Parthenon

Focus sur Tax-on-web, service en ligne permettant aux personnes physiques de réaliser leur déclaration d'impôts

Belgique

Un recours au service passant majoritairement par le biais de l'eID

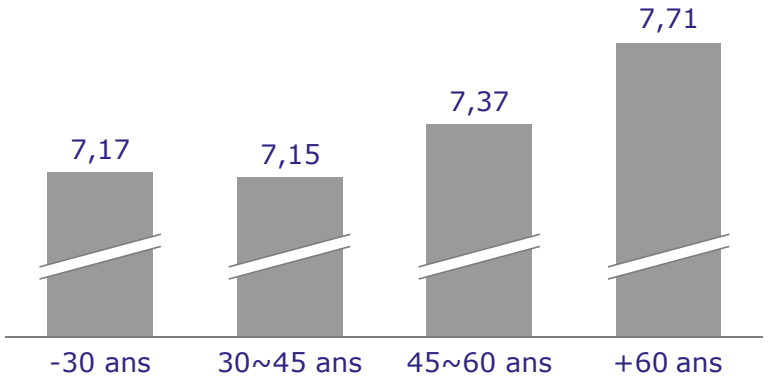
Répartition des déclarations et types de connexions
En millions de citoyens, 2017



L'alternative privée Itsme, basée sur une solution mobile, est acceptée par Tax-on-web depuis Mai 2018

Un service en ligne plébiscité

Enquête de satisfaction du service Tax-on-web (N=60k)
« Sur une échelle de 1 à 10, dans quelle mesure êtes-vous satisfait du contenu et des fonctions de Tax-on-web » ?



- Un Net Promoter Score (NPS) de 7,94
- Une facilité d'utilisation mise en avant
- Une capacité à pouvoir modifiée de manière instantanée un formulaire prérempli particulièrement appréciée

Note : PDS = Proposition de Déclaration Simplifiée
Source : Service Public Fédéral Finances ; Analyses BCG & EY-Parthenon

Benchmark géographique - L'identité numérique au Danemark

Danemark

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
5,75 millions	Registre central de population	→ NemID, déployé depuis 2010 sous 3 formes > La NemID card qui comprend un nombre limité de combinaisons de codes à rentrer au moment de l'identification/authentification > Le NemID Token générant des authentifiants éphémères > La NemID key, solution mobile lancée en Mai 2018 

Retours d'expérience sur la stratégie de déploiement

- → NemID utilisé régulièrement par près de 5 millions de citoyens Danois pour accéder à une panoplie de services publics et privés (~700)
  - > 55 millions de transactions mensuelles en moyenne
  - > Des transactions d'un montant de près de 775 millions de couronnes danoises (~103 millions d'euros), dont le tiers dans le cadre de services publics effectuées durant l'année 2018
  - > Une identité numérique utilisée par près de 280 000 compagnies et autorités
- → NemID actuellement en cours de révision, en vue d'être remplacé par le MitID à partir de 2020, principalement provoquée par la mise aux normes liée au règlement eIDAS, bien que les niveaux de sécurité n'aient pas été pour l'heure révélés
  - > MitID n'inclura qu'un seul eID, tandis que le NemID séparait l'accès entre les services publics et privés
  - > Les niveaux de sécurité attribués aux différents services sera flexible, afin de simplifier l'accès aux services pour lesquels un niveau plus faible serait suffisant, en vue de faciliter l'adoption par les fournisseurs de services et les citoyens

Usages majeurs

- → Digital Post –
  - > Canal de communication permettant aux autorités publiques de transmettre des communications de manière électronique
  - > ~91% des plus de 15 ans abonnés au service
  - > ~100 millions de communications transmises par an
  - > Taux de satisfaction de 84% à la mi-2018
- → NemSMS
  - > Service permettant aux autorités de contacter directement les citoyens par SMS (Ex. : rappel de RDV)
  - > 2.1 millions de citoyens ont recours à l'usage

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Benchmark géographique - L'identité numérique en Italie

Italie

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
60,9 millions	Registre unique (ANPR) permettant de regrouper les données citoyennes actuellement dispersées dans 8.000 registres	→ Carta d'identità elettronica (CIE 3.0) > Carte physique au format « carte de crédit » dotée d'une puce numérique avec un certificat d'authentification pour remplacer l'ancienne carte d'identité papier > Code PIN pour certaines utilisations

Retours d'expérience sur la stratégie de déploiement

- Une carte émise et gérée par l'Etat via les municipalités lancée en 2016 dont la démocratisation est lente (objectif 70% de la population en 2020)
  - A fin 2018, seulement 4,7M de cartes ont été distribuées vs un objectif de 10M fin 2017
  - Le coût d'obtention de cette carte a potentiellement représenté un frein à son déploiement (un coup moyen de 23€ pour les citoyens)
- Ce système à destination des citoyens et des entreprises doit faciliter les échanges avec l'Etat qui sont perçus comme complexes et fastidieux
  - Cette carte contient le nom, les informations de naissance, le numéro fiscal, la résidence et citoyenneté, le numéro et lieu de délivrance, un certificat d'identification, les empreinte digitales et une photo numérique ainsi qu'une option de consentement au don d'organe
  - Permet l'accès aux différents services en ligne : paiement des taxes, échanges avec les institutions, santé digitale, etc.
- SPID, un dispositif similaire à FranceConnect, regroupant 7 fournisseurs d'identité, dont Poste Italiane (80% des utilisations) permet l'accès en ligne à plus de 4000 services publics et privés à partir d'un PC, une tablette ou un smartphone en couvrant l'ensemble des niveaux de sécurité :
  - Le premier niveau permet l'accès aux services en ligne par un identifiant et un code PIN
  - Le second nécessite en plus l'utilisation d'un code d'accès temporaire à usage unique
  - Le troisième niveau ajoute à l'identifiant et au code PIN un support physique d'identification
- Une adoption du dispositif stimulée par 2 services culturels uniquement accessibles via la plateforme à destination des citoyens nouvellement majeurs et des enseignants

Usages majeurs

- L'usage majeur mis en avant concerne le récipient électronique servant de canal de communication directe avec l'administration publique

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Benchmark géographique - L'identité numérique en Norvège

Norvège

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
5,3 millions	Un numéro d'identité unique rattaché à chaque citoyen	→ La source d'identité numérique la plus utilisée est BankID : > Programme d'identités numériques mis en place par un consortium privé de banques et d'acteurs du paiement > L'eID est fournie par la banque de l'utilisateur

Retours d'expérience sur la stratégie de déploiement

- Depuis 2004, BankID connaît un fort succès en Norvège, il est utilisé par ~75% des Norvégiens notamment car :
  - BankID a été déployé pour de nombreux services publics et privés en ligne (plus de 350 acteurs privés sont partenaires de Bank ID)
- La version mobile de BankID (MobileID), disponible depuis 2009, se déploie rapidement avec un taux d'adoption d'environ 30% des Norvégiens
- Le parcours de l'usager d'une identité numérique BankID se décompose en 3 étapes :
  - L'utilisateur se rend en physique à sa banque pour faire vérifier son identité (passeport ou carte d'identité à montrer en physique)
  - L'utilisateur reçoit un boitier générateur de code en temps réel et son identité numérique est créée
  - Pour s'identifier en ligne auprès des entreprises partenaires de BankID, l'utilisateur doit renseigner son numéro d'identité, le code généré en temps réel sur son boitier et son mot de passe personnel

Usages majeurs

- L'usage majeur est indéniablement le recours aux services bancaires, BankID étant utilisé par l'ensemble des banques du pays
- D'autres usages plébiscités sont :
  - La signature électronique de documents ou de contrats (Ex dans l'immobilier avec les baux de location et les offres d'achat)
  - Les achats en ligne
  - La gestion des biens (actifs, patrimoine)
  - La souscription et le recours aux services des « utilities »

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Benchmark géographique - L'identité numérique aux Pays-Bas

Pays-Bas

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
17,08 millions	Numéro unique de citoyen	→ Actuellement le DigiD sous forme d'identifiant et de mot de passe en ligne, sa détention n'est pas obligatoire → Cette identité numérique est gérée par l'Etat et les municipalités → Version améliorée, élargie et plus sécurisée en cours de création avec l'eID Scheme → Applications mobiles

Retours d'expérience sur la stratégie de déploiement

- Une maturité digitale bien plus forte que ses voisins :
  - 75% des Néerlandais préfèrent utiliser les services en ligne vs 33% de moyenne en Europe, et 69% des formulaires administratifs sont disponibles en ligne vs seulement 29% en France
- Les Néerlandais ont accès depuis 2005 au DigiD, un système d'identification et d'authentification en ligne leur permettant d'échanger avec les administrations publiques (nationales et locales), utilisé par 12 millions de citoyens, soit 70% de la population
- Le gouvernement souhaite étendre le spectre de l'identité numérique en incluant les acteurs privés afin de créer un accès standard aux services en ligne
  - Ce système permettra aux citoyens d'échanger avec les acteurs privés en ligne (e-commerce majoritairement, banques, sites de voyages etc.), en plus des administrations publiques en ayant la main sur les informations qu'ils souhaitent partager
  - Ce système se veut plus sécurisé que le système actuel grâce à de nouveaux moyens d'authentification (face ID, empreinte digitale code PIN)
- Développement de ce système via un partenariat public – privé sous contrôle de l'Etat
- Réflexion en cours avec le Canada pour faciliter le contrôle aux frontières avec le projet « Know Traveller Digital Identity » prévu pour 2020

Usages majeurs

- Gestion des impôts
- Demande d'allocations
- Gestion de la pension

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Benchmark géographique - L'identité numérique en Suisse

Suisse

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
8,42 millions	Données des citoyens confirmées et stockées auprès de la police fédérale. Une seconde couche de données gérée par le secteur privé	→ Existence d'un écosystème de solution d'identification numérique par des entreprises et consortium privés : SuisseID, Mobile ID, Google ID, AppleID, OpenID … → L'introduction prochaine d'e-ID reconnus par l'Etat doit permettre de délivrer, sur la base des données d'identification personnelle disponibles auprès de la confédération, des moyens d'identification électronique officiels

Retours d'expérience sur la stratégie de déploiement

- Emergence d'un débat politique important sur la place de l'Etat dans le futur écosystème e-ID, ayant abouti au rejet d'une conception « tout-Etat », qui serait basée sur une carte d'identité numérique réservée aux Suisses, jugée trop chère et loin des réalités du marché
- Une répartition claire des rôles entre l'Etat et les acteurs du marché a été réalisée : l'Etat étant chargé de la mise en place d'un cadre légal et organisationnel fiable et les acteurs privés étant responsables de la mise à disposition des solutions d'eID
- La Suisse semble en retard sur ses voisins européens concernant la mise en place de ce système d'e-ID, prévue pour 2020
  - Fin 2018 les autorités suisses viennent seulement de fixer le cadre normatif reconnu par l'Etat et de définir les moyens techniques et les niveaux de sécurité obligatoires
  - En 2019, les autorités ont pour objectif de créer un modèle de référence d'e-ID à perfectionner, de lancer des actions de communication et marketing et de développer l'application de gestion des données d'identité
  - La création d'un cadre juridique respectant les normes européennes et internationales initialement prévu pour 2019 a été reporté à fin 2020
- L'Etat a pour objectif de redonner un souffle à l'identification numérique, SuisseID étant par exemple resté un produit de niche dû à :
  - Une utilisation malaisée, une durée de vie limitée à 3 ans des certificats, un manque d'applications et des frais d'acquisition importants
  - À l'inverse, les solutions mobile ID plus récentes ont été majoritairement mieux acceptés, bien que cela reste encore insuffisant

Usages majeurs

- Non-applicable compte tenu de l'avancement actuel du projet
- Voir slide suivante pour les usages évoqués par la confédération Suisse

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Différents usages à fort potentiel d'adoption ont été identifiés

Suisse

Domaines	Usages envisagés de l'e-ID en Suisse
Cyber-démocratie et cyber-participation	Votations populaires; Elections fédérales; Initiatives populaires et référendums fédéraux; Pétitions fédérales; Consultations et auditions
Cyber-administration	Formulaires en ligne auprès des autorités (déménagements, documents d'identité, etc.); Accès aux dossiers fiscaux et décomptes de TVA; Accès aux portails des services de contrôle des véhicules auto; Commande d'un extrait du casier judiciaire
Cybersanté	Accès au dossier électronique du patient; Enregistrement de données de santé par le patient; Cyberordonnance; Cyberconsultation
Cyber-éducation	Accès aux ressources scolaires; Accès aux informations scolaires par les parents; Confirmation de la prise de connaissance des résultats des enfants; Inscription pédagogique dans les branches supérieures
E-commerce	Preuve d'attributs d'identité lors de l'achat / souscription (Ex. : âge lors de l'achat d'alcool)
Signatures électroniques	Signature électronique en tant que service de confiance
Economie collaborative	Enregistrement des participants aux plateformes collaboratives (partage de voiture ou d'appartement, plateformes pour freelance, etc.)
Cloud	Protection des données stockées en cloud par combinaison à des méthodes cryptographiques
Réseaux sociaux	Identification pour les réseaux nécessitant de remplir des conditions d'adhésion

Source : Confédération suisse ; Rapport explicatif de la loi fédérale ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Benchmark géographique - L'identité numérique en Suède

Suède

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
10,1 millions	Bases de données des documents d'identité délivrés par l'Etat	→ 3 sources d'identité numérique approuvées par le gouvernement : > BankID, programme d'identité numérique mis en place par un consortium privé de 7 banques et le plus utilisé en Suède > AB Svenska Pass, une carte d'identité à puce fournie par l'administration fiscale > Freja eID+, solution d'identification privée disponible sur mobile uniquement

Retours d'expérience sur la stratégie de déploiement

→ BankID, lancé en 2003, est la solution d'identification numérique la plus utilisée en Suède avec un taux d'adoption d'environ 80% (8 millions d'utilisateurs)

→ Le succès de BankID (7,5 millions d'utilisateurs, soit 76% de la population) peut notamment ms'expliquer par :

> Le nombre important de services en ligne pour lesquels il est possible de s'identifier via BankID (plus de 300 acteurs publics et privés)

> La multiplicité des solutions techniques d'identification proposées : via un mobile (app à télécharger), via une carte à puce physique (lecteur de cartes nécessaire) ou via un PC (logiciel à télécharger)

> La double fonction que BankID peut assurer : identification et signature électronique de documents ou contrats

Usages majeurs

→ Transferts bancaires
→ Déclaration d'impôts
→ Achat en ligne

Source : Entretiens experts internationaux (voir annexe 1) ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Benchmark géographique - L'identité numérique au Royaume-Uni

UK

Caractéristiques du pays

Population	Type de registre de population	Support homologué d'identité numérique
66,04 millions	Numéro unique de citoyen	→ Système GOV.UK Verify via la création d'un compte en ligne, utilisable par la suite chez tous les partenaires utilisant ce système (similaire à FranceConnect) → Absence de support physique d'identité numérique

Retours d'expérience sur la stratégie de déploiement

- GOV.UK Verify, lancé officiellement en 2016 par le gouvernement après 5 années d'investigation, a été développé afin de fournir un point d'accès unique aux services de l'administration publique par le biais de 5 fournisseurs d'identités privés (provenant notamment de la Fintech)
- Le dispositif est perçu comme étant décevant, à plusieurs égards :
  - 3 années de retard au lancement à déplorer
  - Le nombre d'utilisateurs n'est estimé qu'à 3,6 millions et ne devrait atteindre que 5,4 millions d'ici 2020, bien loin des objectifs initialement fixés de 25 millions d'utilisateurs
  - Un nombre faible de 19 services accessibles via le dispositif à Février 2019, bien loin du nombre ciblé de 46 services disponibles pour 2018
  - Une mise en place plus couteuse et moins efficiente que prévu et des réductions de dépenses 4 fois inférieures au montant projeté (217 millions de pounds vs. 873 millions de pounds)
  - Un système de vérification inefficace, avec seulement ~40% de taux de réussite durant les 18 premiers mois du dispositif, bien loin des objectifs projetés de 90% (48% à Février 2019)
- Décision du gouvernement de céder la gestion du dispositif aux partenaires privés à partir de mars 2020

Usages majeurs

- Non-identifiables compte tenu de l'avancement actuel du projet
- Voir slide suivante pour les usages accessibles via Verify, ainsi que ceux qui le sont de manière exclusive

Source : Entretiens experts internationaux (voir annexe 1) ; National audit Office ; Recherche documentaire ; Analyses BCG & EY-Parthenon

8 services gouvernementaux parmi les 19 proposés par Verify sont uniquement accessibles via le dispositif

UK

Répartition des services proposés par Verify, par type d'accès

Mobilité	Ajouter un code de vérification du permis de conduire sur un appareil mobile	Service de gestion de voiture de fonction
	Renouveler l'autorisation médicale de conduite	Partager les informations relatives au permis de conduire
	Signaler des problèmes de santé affectant la conduite	Licence d'opérateur de véhicule motorisés
Emploi, Social et fiscalité	Obtenir sa pension d'Etat	Consulter sa pension d'Etat
	Signer sa dette hypothécaire	Mettre à jour ses paiements ruraux
	Service de divulgation et d'interdiction d'accès	Consulter ses impôts
	Obtenir un crédit universel	Compte de gestion des impôts
	Service d'aide à la protection cyber	Service de calcul d'imposition
		Obtenir une vision du relevé des revenus perçus
		Aider une tierce personne avec ses impôts (famille/amis)
		Demander un remboursement fiscal

Services uniquement accessibles via Verify Services également accessibles en dehors de Verify

Source : National Audit Office ; Investigation into Verify ; Analyses BCG & EY-Parthenon

Sommaire

Les fournisseurs de services privés manquent de visibilité pour pousser une solution d'identité numérique sécurisée malgré ses bénéfices potentiels

D'une manière générale, les fournisseurs de services privés se positionnent peu en faveur de solutions d'identités numériques sécurisées couvrant le niveau de sécurité élevé, en raison :

- Du manque de visibilité sur les solutions techniques retenues, des coûts de mise en œuvre et du calendrier de déploiement de la CNIe
- Des craintes / doutes autour de la préservation de parcours clients fluides et simples
- Du manque de clarté sur les obligations en matière de procédures d'identification de niveaux élevé / substantiel

Toutefois, plusieurs cas d'usage à fort potentiel identifiés[1] méritent de poursuivre les discussions entamées avec les fournisseurs de services pour mieux qualifier les bénéfices et lever les doutes (sécurité contre la fraude, parcours client, maîtrise des coûts)

- Pour les tiers de confiance : les actes authentiques et le consentement à distance
- Dans le secteur financier : KYC et les virements/transferts instantanés

Des sujets transversaux (intéressants plusieurs secteurs) peuvent également d'être approfondis, en raison de leur sensibilité, même s'ils ne suscitent qu'un intérêt modéré de la part des FS privés

- Les services "réservés", par exemple en fonction d'un critère d'âge (ex. jeux en ligne, …)
- La traçabilité et la certification des utilisateurs (ex. économie collaborative) et des échanges (LRE)

Recommandation : Au-delà des besoins exprimés par les fournisseurs de service, un levier réglementaire peut également être actionné par l'Etat

- Pour intégrer les demandes des usagers de plus de sécurité dans certains secteurs
- Pour lever des contraintes pouvant faire obstacle à l'utilisation de l'identité numérique

1. Eventuellement monétisables

Note : KYC correspond à "Know Your Customer", c'est-à-dire le processus permettant de vérifier l'identité des clients d'une entreprise

Source : Analyses BCG & EY-Parthenon

L'analyse par secteur d'activité souligne la faiblesse de traction spontanée des fournisseurs privés pour les usages de niveau élevé

Potentiel de niveau élevé

Synthèse par secteur de l'investigation des usages de niveau élevé

- **Tiers de confiance :** Un potentiel d'usages de niveau élevé existant, avec une profession notariale investiguant depuis de nombreuses années la problématique de l'identification / authentification en vue de réaliser des démarches à distance
- **Banque :** Un potentiel d'usages de niveau élevé réel, notamment dans une optique de facilitation / sécurisation du « Know Your Customer » (ex. avec un lien entre les données d'identité et fiscales), à condition de ne pas dégrader l'expérience client, même si la Fédération Bancaire Française privilégierait un maintien du niveau substantiel, arguant que FranceConnect couvre bien les besoins des banques. Un autre usage à potentiel porte sur la facilitation des paiements instantanés (pour générer la confiance)
- **Jeux :** Un potentiel d'usages de niveau élevé existant, malgré une possible réaction hostile des parties prenantes et des utilisateurs lors de la mise en œuvre, qui peut néanmoins être contenue par un apport de bénéfices immédiats en terme de fluidité de l'expérience (Ex. : délai d'attente) ou d'optimisation des coûts
- **Mobilité :** Un potentiel d'usages élevés identifié au sein des contrôles à l'embarquement de transports, notamment au niveau des aéroports qui investiguent différentes technologies d'identification / authentification
- **Plateformes collaboratives (ex. BlablaCar) :** Un potentiel limité d'usages élevé, les acteurs se positionnant eux-mêmes en tant que tiers de confiance vis-à-vis de leurs clients. S'ils prennent ce faisant le risque de se priver de certains clients, leur réservoir de croissance est assez dynamique encore pour que plus de sécurisation (ex. traçabilité, etc.) ne soit pas une priorité à court terme
- **Plateformes de services (ex. sites d'achats en ligne) :** Un potentiel limité d'usages élevé et une justification d'une éventuelle activation de leviers réglementaires peu évidente (axe possible : en fonction du montant des paiements)
- **Santé privée :** Un potentiel d'usages de niveau élevé davantage perceptible au sein de la santé publique, qu'au niveau des laboratoires privés
- **Assurance :** Des usages de niveau élevé limités, avec un éventuel potentiel dans le segment de l'assurance vie
- **Utilities :** Un potentiel d'usages de niveau élevé très limité (indépendamment de la question de leur positionnement en tant que fournisseur d'identité)

Source : Entretiens experts sectoriels (voir annexe 1) ; Analyses BCG & EY-Parthenon

Plusieurs verticales sectorielles (avec des enjeux de sécurité et de parcours client particulièrement sensibles) ont été investiguées

Assurance

Banque

Jeux

Mobilité

Plateformes de services et collaboratives

Santé privée

Tiers de confiance
(dont notaires, poste électronique, coffres forts, etc.)

Utilities

Source : Entretiens experts sectoriels (voir annexe 1) ; Analyses BCG & EY-Parthenon

Recensement et analyse des besoins des fournisseurs de services privés (1/3)

Secteur	Usage recensé	Besoin de sécurité	Existence de l'usage	Bénéfices principaux du recours à une identité numérique	Commentaires
Banque	**Réaliser un paiement instantané**		Emergent	Optimisation potentielle des coûts très importante générée par une désintermédiation des opérateurs de carte bancaire	Voir slide de focus pour éléments complémentaires
	Ouvrir un compte bancaire		Existant	Optimisation des coûts d'ouverture de compte Amélioration de l'expérience client en se délestant de la présence physique	Volonté des banques d'investiguer le sujet, concurrencées par les banques en ligne
	Vérification des attributs d'identité du titulaire du compte (KYC)		Emergent	Optimisation de coûts majeure (ex. authentification, données fiscales, etc.) et réduction des risques de non-conformité (grâce à la responsabilité du FI)	Recherche des acteurs d'une solution de niveau élevé
	Changer de banque / coordonnées bancaires		Existant	Optimisation des coûts par le biais d'une actualisation complètement automatisée des coordonnées bancaires auprès des différents services payants contractés	Sous-couvert de la construction d'une fonctionnalité encore inexistante
	Demander un crédit (y compris crédit à la consommation)		Existant	Lutte contre la fraude (usurpation d'identité) Amélioration de l'expérience par le biais d'un partage des données nécessaires à la contraction d'un crédit	Investigation en vue d'aller au-delà de ce que permet le décret de novembre 2018
Jeux	**Ouvrir un compte de jeux en ligne**		Existant	Amélioration potentielle des délais de validation des inscriptions débloquant la possibilité de jouer avec de l'argent réel	Intérêt des acteurs dans le cas d'une amélioration du parcours d'inscription visible à CT

Note : Sur la base de l'expression de besoin des fournisseurs de services et des analyses BCG EY
Source : Entretiens experts sectoriels (voir annexe 1) ; Analyses BCG & EY-Parthenon

Focus Banque – Des enjeux économiques majeurs sont associés au développement de nouvelles méthodes de paiement

Banque

Un contexte réglementaire spécifique

→ **Une réflexion continue sur l'élaboration de nouveaux modes de paiements, récemment stimulée par la directive DSP2 qui sera déployée en septembre 2019**

→ **DSP2 exige d'avoir recours à une authentification forte du client lors des transactions électroniques, à travers au moins deux des trois facteurs suivants :**

- **Connaissance :** quelque chose que seul l'utilisateur connaît (par ex. un mot de passe, un code PIN, un numéro d'identification)
- **Possession :** quelque chose que seul l'utilisateur possède (par ex. un appareil mobile, un token, une carte à puce)
- **Caractéristique personnelle :** quelque chose qui caractérise l'utilisateur de manière unique (par ex. une empreinte digitale, la reconnaissance faciale ou vocale)

Un recours au paiement instantané encore limité par les solutions d'authentification actuelles

→ **Une révolution permettant de réaliser un virement bancaire en temps réel, avec un délai de seulement quelques secondes**

→ **Une désintermédiation des opérateurs de cartes bancaires, générant des économies potentiellement majeures pour les acteurs bancaires**

→ **Un obstacle principal à la démocratisation de cet usage résidant dans la crainte des usagers à l'égard du caractère instantané des transferts, notamment vis-à-vis des situations de fraudes qui pourrait être outrepassé par une solution d'identification/authentification fournissant des garanties de sécurité très élevées**

→ **Une estimation de 3.000.000 de transactions annuelles à horizon de 5 ans, avec une courbe d'adoption sensiblement similaire à celle du paiement sans contact en France**

Des initiatives disruptives déployées à l'international

Chine

→ **Recours à une solution de paiement entièrement basée sur la reconnaissance faciale via un terminal de paiement**

→ **Un déploiement actuel dans certains supermarchés et stations de métro du pays, à travers un système développé par Alipay d'une précision de 99,99%**

Espagne

→ **Caixabank est la première banque dans le monde à offrir la possibilité à ses clients d'avoir recours à la reconnaissance faciale pour retirer de l'argent aux distributeurs de billets**

Source : Entretiens experts sectoriels (voir annexe 1) ; Analyses BCG & EY-Parthenon

Recensement et analyse des besoins des fournisseurs de services privés (2/3)

Secteur	Usage recensé	Besoin de sécurité	Existence de l'usage	Bénéfices principaux du recours à une identité numérique	Commentaires
Mobilité	**Adossement de la carte de transport (Navigo et SNCF)**		Prospectif	Permettrait de fournir une alternative aux cartes de transports, et d'automatiser l'application des réductions sur base d'un partage des données associés	Mentionné à diverses reprises dans les travaux de la voix des usagers
	Accéder à un lieu sécurisé (travail, école, hôpital, etc.)		Existant	Permettrait d'adosser le badge d'accès de son lieu de travail directement sur sa CNIe afin de fournir par exemple une alternative en cas de perte / d'oubli	Pourrait être élargi à d'autres types de lieux sécurisés
	Contrôle à l'embarquement à l'aéroport		Emergent	Amélioration de la fluidité des contrôles générant d'importantes économies de coûts, sujet d'investigation majeur des acteurs du secteur	Voir slide de focus
Plateformes de services	**Faire un achat en ligne**		Existant	Permettrait de réduire la fraude liée à l'usurpation d'identité qui représente une part importante des activités illégales engagées par les usurpateurs	Potentiel perçu comme proportionnel au montant de l'achat
	Création de comptes auprès des sites de rencontre		Existant	Permettrait de relier son identité à son compte, sous contrainte réglementaire, afin d'assurer la traçabilité des membres et accroître la confiance des membres	Justification d'actionnement de leviers réglementaires peu évidente à date
Plate-formes collab.	**Création de comptes auprès des plateformes collaboratives en ligne**		Existant	Permettrait aux acteurs des plateformes collaboratives (ex. : conducteurs Blablacar ; hôtes AirBnb) de relier son identité à leur compte et accroître la confiance	Acteurs divisés entre le gain potentiel de confiance et la contradiction avec leur rôle de tiers de confiance
Santé	**Transmission des résultats d'analyse entre professionnels**		Emergent	Permettrait d'améliorer l'expérience du patient par le biais d'un partage entre professionnels des analyses réalisées	Recours hors DMP

Note : Sur la base de l'expression de besoin des fournisseurs de services et des analyses BCG EY
Source : Entretiens experts sectoriels (voir annexe 1) ; Analyses BCG & EY-Parthenon

Focus Mobilité : différentes initiatives d'identification digitale ont été mises en place autour de l'accès physique aux transports et aéroports

Mobilité

Contrôle aux frontières

- Depuis 2018, les aéroports de Paris et de Nice ont installé des **terminaux de reconnaissance faciale aux frontières**
  - Fonctionnent sur base du **recoupement du scan et de la photo du passeport**
  - Nécessitent néanmoins quelques amélioration de précision

Identification à l'embarquement

Schiphol Amsterdam Airport — CATHAY PACIFIC

- Partenariat de l'aéroport de Schiphol et de la compagnie Cathay Pacific pour le lancement d'un **système de reconnaissance faciale à l'embarquement**
- En plus des documents usuels, **un scan facial est réalisé à l'enregistrement** qui sera **comparé à celui effectué devant la porte d'embarquement**

Simplification du parcours voyageur

AIRFRANCE

- **Heathrow** : Lancement d'un projet de **reconnaissance faciale sur tout le parcours voyageur**
  - Utiliser un système de **reconnaissance faciale à chaque étape d'authentification du passager** (bornes d'enregistrement, dépose bagage, sécurité et embarquement)
  - **Objectif de réduction du temps de parcours voyageur**
- **Air France** : lancement d'une phase de test pour une **carte d'embarquement à reconnaissance faciale**
  - Suite à l'enregistrement (en ligne ou physique), du passag**la carte d'embarquement contiendra tous les informations d'authentificatione**r et sera la seule pièce à utiliser pour le reste du parcours

Un projet global : « Know Traveller Digital Identity »

- Un projet initié au World Economic Forum de Davos en 2018 par le Canada et les Pays-Bas qui vise à **faciliter les déplacements internationaux, améliorer les flux de passagers et renforcer la sécurité**
- Un principe de partage d'identité digitale basé sur les technologies de la biométrie, de la cryptographie et de la blockchain
- **Partage en amont des informations d'authentification et d'identité digitale** afin d'effectuer les contrôles nécessaires de manière anticipée pour prévenir les risques potentiels

Une initiative disruptive : la puce implantée dans la main

SJ TRAVEL GROUP

- En Suède, plusieurs milliers de personnes disposent d'un implant électronique inséré sous la peau dans le but de faire office de clés, cartes de visite, et plus récemment, de billet de train
- L'opérateur de transport Suédois SJ a été le premier au monde à accepter la puce implantée dans la paume du passager dans son processus de contrôle du billet

Source : Entretiens experts sectoriels (voir annexe 1) ; Analyses BCG & EY-Parthenon

ditp Direction interministérielle de la transformation publique — libérer l'énergie publique

Recensement et analyse des besoins des fournisseurs de services privés (3/3)

Secteur	Usage recensé	Besoin de sécurité	Existence de l'usage	Bénéfices principaux du recours à une identité numérique	Commentaires
Tiers de confiance	**Réaliser un acte authentique à distance**		Emergent	Potentiel d'amélioration des parcours (réduction des déplacements) Potentiel de réduction du coût (mutualisation des vérifications d'identité et cadastre) Nouveaux services (réflexion sur le pendant juridique du DMP)	La signature du premier acte authentique à distance a été réalisée en octobre 2018
	Réaliser un acte de vente à distance		Emergent		
Utilities	**Souscrire à un service de télécommunication**		Existant	Potentiel d'amélioration de la fluidité et de réduction de coûts à la souscription	Un secteur au taux d'attrition particulièrement élevé
	Souscrire à un service énergétique		Existant	Potentiel d'amélioration de la sécurité de souscription, actuellement perçue comme limitée	Pourrait également endiguer le rôle joué par la souscription dans les cas de squat
Transverse	**Envoyer une lettre recommandée électronique**		Emergent	Une nécessité de garantir l'identité du destinataire et de l'expéditeur pour attribuer une valeur juridique à la LRE	Emergence de start-up visant à démocratiser le recours à la LRE
	Passer un entretien par visioconférence		Emergent	Un recours à la visioconférence qui devrait croitre dans les années à venir, accentuant la nécessité de s'assurer de l'identité de l'interlocuteur	Existant, notamment dans l'embauche de cadres, mais à un niveau peu sécurisé
	Passer un examen en ligne / par visioconférence		Emergent		Davantage freiné par des problématiques technologiques que d'identification
	Démontrer la possession d'un diplôme		Prospectif	Permettrait de fiabiliser la vérification du diplôme supérieur au moment d'un recrutement	Sous couvert d'une constitution d'une base de diplômes

Note : Sur la base de l'expression de besoin des fournisseurs de services et des analyses BCG EY
Source : Entretiens experts sectoriels (voir annexe 1) ; Analyses BCG & EY-Parthenon

Sommaire

2. Analyses des usages

- Benchmark géographique
- Enjeux des fournisseurs de services
  - Enjeux des fournisseurs de services privés
  - Enjeux des fournisseurs de services publics
- Analyse des besoins et usages des Français

Synthèse des usages publics

Rappel de l'approche retenue :

- Capitalisation des travaux de recensement déjà effectués par le programme interministériel Identité numérique, en fonction du besoin de sécurité exprimé par les différents ministères
- Croisement avec des éléments de contexte issus des transformation ministériels et interministériels (100% dématérialisation, simplification, plans de transformation ministériels, etc.)
- Croisement avec d'autres bénéfices (amélioration et simplification des parcours client, lutte contre la fraude, levier de dématérialisation via la fourniture d'une solution sécurisée d'identification et/ou d'authentification, maîtrise des coûts)

Résultat : une première sélection d'usage publics susceptibles de justifier une niveau de sécurité substantiel ou élevé

- Des besoins de sécurité élevé en soutien aux enjeux stratégique et de transformation numérique dans le domaine de la citoyenneté, de la justice et de la santé
- Des réductions de couts permises par la solution d'identité numérique dans de nombreux domaines, associées à la facilitation de la lutte contre la fraude (ex : prestations, autorisations diverses, pièces identités) et au développement de la dématérialisation
- Un potentiel d'amélioration des parcours usagers

Source : Documentation interne Programme, DINSIC, DITP ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Recensement détaillé des usages publics (1/5)

Ministère/ Entité	Usage recensé	Besoin de sécurité exprimé	Autre bénéfice	Commentaires
Affaires étrangères	Voter de manière électronique en tant que Français de l'étranger	Elevé	Parcours usager amélioré Participation plus forte	Usages peu volumiques mais à valeur symbolique forte
	S'inscrire auprès du registre des Français établis hors de France	Substantiel	Parcours usager amélioré Recensement plus exhaustif	
Affaires sociales	Couverture maladie universelle- complémentaire	Substantiel	Lutte contre la fraude Maîtrise des coûts	
	Demande de carte européenne d'assurance maladie (Ceam)	Substantiel	Lutte contre la fraude Levier de dématérialisation	
	Déclaration de loyer pour l'aide au logement	Substantiel	Lutte contre la fraude Levier de dématérialisation	
	Avis de changement de situation pour les prestations familiales	Substantiel	Lutte contre la fraude Levier de dématérialisation	
	Attestations fiscales retraités régime général	Substantiel	Parcours usager amélioré Levier de dématérialisation	
Education	Consulter le livret scolaire des enfants	Substantiel	Parcours usager amélioré Levier de dématérialisation	*Autres usages à investiguer autour de ParcourSup et de l'accompagnement personnalisé*
INSEE	Recensement de la population (OMER)	Substantiel	Parcours usager amélioré Levier de dématérialisation	

Source : Documentation Programme, DINSIC, DITP ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Recensement détaillé des usages publics (2/5)

Ministère/ Entité	Usage recensé	Besoin de sécurité exprimé	Autre bénéfice	Commentaires
Intérieur (1/2)	Inscription sur les listes électorales	Elevé	Parcours usager amélioré Participation plus forte	Lien avec l'objectif gouvernemental de développement du vote en ligne à horizon 2020
	Voter de manière électronique en France dans le cadre des élections (Présidentielle, législative, européenne)	Elevé	Parcours usager amélioré Participation plus forte	
	Obtenir une procuration de vote	Elevé	Parcours usager amélioré Participation plus forte	
	Participer à une consultation publique	Elevé	Parcours usager amélioré Participation plus forte	
	Participer à un référendum d'initiative partagée	Elevé	Parcours usager amélioré Participation plus forte	
	Déclarer son rattachement à un parti	Elevé	Parcours usager amélioré Levier de dématérialisation	
	Demande de passeport (mineurs, majeurs et mineurs émancipés)	Elevé	Parcours usager amélioré Levier de dématérialisation	
	Obtenir une autorisation de détention d'arme	Elevé	Lutte contre la fraude (traçabilité)	

Source : Documentation Programme, DINSIC, DITP ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Recensement détaillé des usages publics (3/5)

Ministère/ Entité	Usage recensé	Besoin de sécurité exprimé	Autre bénéfice	Commentaires
Intérieur (2/2)	Consulter et suivre son dossier d'infraction routière	Substantiel	Parcours usager amélioré Levier de dématérialisation	
	Demande de carte nationale d'identité (mineurs, majeurs et mineurs émancipés)	Elevé	Parcours usager amélioré Levier de dématérialisation	
	Demande de Visa Schengen court séjour (séjour de 3 mois maximum)	Substantiel	Parcours usager amélioré Lutte contre la fraude	
	Autorisation de sortie du territoire (AST) d'un mineur non accompagné par un titulaire de l'autorité parentale	Substantiel	Parcours usager amélioré Levier de dématérialisation	
	Déclaration de perte de carte nationale d'identité et de passeport	Substantiel	Parcours usager amélioré Lutte contre la fraude	
	Inscription au permis de conduire (primata + extension + perte de droits)	Elevé	Parcours usager amélioré Levier de dématérialisation	
	Permis de conduire : demande de titre après réussite à l'examen	Substantiel	Parcours usager amélioré Levier de dématérialisation	
	Demande de certificat d'immatriculation d'un véhicule neuf (carte grise)	Substantiel	Parcours usager amélioré Lutte contre la fraude	
	Déclaration de cession d'un véhicule	Substantiel	Parcours usager amélioré Levier de dématérialisation	

Source : Documentation Programme, DINSIC, DITP ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Recensement détaillé des usages publics (4/5)

Ministère/ Entité	Usage recensé	Besoin de sécurité exprimé	Autre bénéfice	Commentaires
Justice	Demande d'aide juridictionnelle	Substantiel	Lutte contre la fraude Lutte contre le non recours Levier de dématérialisation	Axe stratégique : cf. loi de programmation 2018-2022 et de réforme pour la justice
	Dépôt de plainte (pour violences sexuelles)	Elevé	Levier de dématérialisation Parcours usager amélioré (éviter un contact visuel/ jugement d'autrui)	
	Suivi des affaires judiciaires en ligne	Substantiel	Parcours usager amélioré Levier de dématérialisation	
	Suivi des affaires civiles en ligne	Substantiel	Parcours usager amélioré Levier de dématérialisation	
	Visiter un proche en prison	Elevé	Maîtrise des coûts (libération de capacité d'accueil "physique")	
	Demander un extrait de son casier judiciaire	Substantiel	Parcours usager amélioré Levier de dématérialisation	
Solidarité et Santé (1/2)	Consulter un médecin en ligne	Elevé	Levier de dématérialisation (confiance dans l'authenticité et la sécurité des données)	Axe stratégique : volet numérique de la STSS, notamment espace numérique de santé individuel, généralisation de la e-prescription et déploiement de la télémédecine (.../...)
	Connexion au compte Ameli	Substantiel	Parcours usager amélioré	
	Accéder au Dossier Médical Partagé	Substantiel/ élevé	Parcours usager amélioré Lutte contre la fraude	

Source : Documentation Programme, DINSIC, DITP ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Recensement détaillé des usages publics (5/5)

Ministère/ Entité	Usage recensé	Besoin de sécurité exprimé	Autre bénéfice	Commentaires
Solidarité et Santé (2/2)	Changement d'adresse Ameli	Substantiel/ élevé	Parcours usager amélioré Levier de dématérialisation	(…/…) avec des objectifs de réalisation avant 2022 -> cf. Ma santé 2022
	Demande de carte vitale	Substantiel/ élevé	Parcours usager amélioré Lutte contre la fraude	
	Consulter et gérer son compte CAF	Substantiel	Parcours usager amélioré Lutte contre la fraude	
	Introduire une demande de retraite en ligne	Substantiel	Parcours usager amélioré Levier de dématérialisation	
	Demande de carte mobilité inclusion (CMI)	Substantiel	Levier de dématérialisation Lutte contre la fraude	
	Introduire une demande de RSA	Substantiel	Levier de dématérialisation Lutte contre la fraude	
	Réaliser sa déclaration trimestrielle RSA	Substantiel	Lutte contre la fraude Maîtrise des coûts	
Travail	Inscription/réinscription à pôle emploi	Substantiel/ faible	Lutte contre la fraude Maîtrise des coûts	
	Déclaration de ressources CAF – Année N-1	Substantiel	Parcours usager amélioré Lutte contre la fraude	
	Ouverture ou accès au compte personnel de formation (CPF)	Substantiel	Parcours usager amélioré Lutte contre la fraude	Priorité gouvernementale

Source : Documentation Programme, DINSIC, DITP ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Sommaire

2. Analyses des usages

- Benchmark géographique
- Enjeux des fournisseurs de services
  - Enjeux des fournisseurs de services privés
  - Enjeux des fournisseurs de services publics
- Analyse des besoins et usages des Français

Analyse des besoins et usages des français

Synthèse et méthodologie

Direction interministérielle de la transformation publique
libérer l'énergie publique

Rappel de la méthode de l'étude "voix des usagers"

Etude qualitative : 4 ateliers MindDiscovery® organisés

Format de "focus groups" avec utilisation de techniques de stimulation et d'animation créatives

2 ateliers à Paris et 2 ateliers à Tours (27 au 29/03/19)

Dans chaque ville, un atelier avec des usagers de -40 ans et un avec des +40 ans

8 personnes par atelier avec des profils diversifiés : genre, revenus, situation familiale, aisance pour utiliser internet, attitude quant à la protection des données personnelles sur internet et les nouvelles technologies, etc

Etude quantitative : 2 questionnaires administrés auprès de ~1200 personnes

Un questionnaire administré en ligne (8 au 14/04/19)
- 1033 répondants
- Echantillon représentatif de la population française sur les critères : genre, âge, zone d'habitation, CSP

En complément, un questionnaire administré au téléphone (16 au 21/04/19)
- 156 répondants
- Echantillon de personnes "éloignées du numérique" , i.e. faisant peu ou pas de démarches par internet

Analyse des données et segmentation en fonction de l'âge, de la zone d'habitation, de la CSP et de l'aisance numérique

Voir annexe 3 pour compléments sur éléments de méthode et annexe 4 pour vidéo focus group (si video disponibles)

L'étude "voix des usagers" fait apparaître une opportunité majeure pour répondre à un besoin clair de simplification des démarches administratives

Une opportunité majeure de création de satisfaction pour les usagers, de simplification des démarches administratives et d'accélération de la dématérialisation via de nouveaux usages

Une solution qui répond aux principaux irritants liés à l'identification, notamment auprès des services publics et pour combler une forte attente d'universalité et de facilité

> Parmi les principaux irritants, l'impératif de se déplacer, la fourniture de documents, la multiplicité des identifiants et mots de passe et la complexité croissante de certains

Un univers d'usages "secteur public" naturellement défini et cohérent pour les usagers

> Combinant un impératif reconnu de sécurité et une forte attente de simplification

> Avec une adjacence naturelle vers le domaine des services bancaires

En conséquence, une acceptation très large, suscitant très peu de rejet

> ~75% des répondants considèrent que c'est une très ou plutôt bonne idée et moins de 10% une très ou plutôt mauvaise idée

> Une appréciation spontanée d'abord liée à la facilité d'une solution « unique et universelle » (53% en spontané), la demande de sécurité est forte mais ni spontanée ni première

> Une gestion par l'Etat pertinente, levant le risque d'exploitation commerciale des données (2/3 des répondants), avec une promesse de gratuité et de protection des citoyens ainsi qu'une légitimité naturelle sur l'univers des démarches administratives et publiques

> Le vote et le renouvellement des papiers priorisés comme nouveaux usages "à distance" (50% des répondants les placent dans leurs 3 priorités)

Source : Enquête auprès des usagers et focus spécifique sur des usagers éloignés du numérique ; analyses BCG & EY-Parthenon

Plusieurs leviers ont été identifiés pour répondre aux craintes exprimées

Différentes craintes exprimées essentiellement autour de la perte et du vol, de la centralisation des données et du piratage (deux tiers des répondants) avec une conviction de la part des usagers : le risque zéro n'existe pas

> Une projection dans les situations de perte d'identifiant et de ses conséquences immédiates et concrètes : « on ne pourra plus rien faire », « on pourrait avoir accès à toutes mes données »
> La capacité de l'Etat à gérer les éventuels problèmes peut être source d'inquiétudes, notamment en termes de réactivité

Les réassurances les plus puissantes tournent autour de la détection des fraudes, de la résolution ou du contournement rapides en cas de problèmes

> La possibilité de désactiver son identité numérique immédiatement et les alertes / notifications en cas d'utilisations suspectes parmi les caractéristiques les plus appréciées
> La maîtrise du dispositif par l'usager, par la possibilité de choisir et tracer les utilisations possibles de son identité (par ex. pour le partage d'informations)

Les solutions de reconnaissance biométrique et faciale préférées pour leur sécurité et ergonomie

Une demande de personnalisation et de modularité de la solution et de ses modalités d'usages

> En fonction des différences d'équipement, de sensibilité à la sécurité entre les usagers d'une part et de besoin de sécurité et d'ergonomie entre les usages d'autre part

Focus : Les "éloignés du numérique" présentent des réticences et inquiétudes plus fortes

> Un taux de rejet de la solution plus élevé (~40% trouvent que c'est une mauvaise idée vs ~10%)
> Des inquiétudes similaires (usurpation d'identité, risques de perte / vol), mais plus marquées
> L'attrait de la solution principalement tiré par la simplification des démarches

Source : Enquête auprès des usagers et focus spécifique sur des usagers éloignés du numérique ; analyses BCG & EY-Parthenon

Au final : l'ergonomie et l'expérience usager, premiers facteurs d'adoption

Visuels choisis par les usagers participant aux sessions MindDiscovery pour représenter leur solution « idéale »

Une solution simple & rapide à utiliser

Simplicité
et convivialité

Plus besoin
de se déplacer

Un équilibre entre innovation & maîtrise

Être zen
et rassuré

Précis
et fiable

Une solution universelle & accessible à tous

Utilisable
par tous

Même les
plus âgés

Une solution modulaire & personnelle

Une solution
à la carte

Un système
souple

Note : dans le cadre de l'analyse qualitative, il est demandé aux usagers de choisir la photo qui caractérise le mieux leur identité numérique idéale (parmi 200 propositions de photos)
Source : Analyses BCG & EY-Parthenon

Analyse des besoins et usages des français

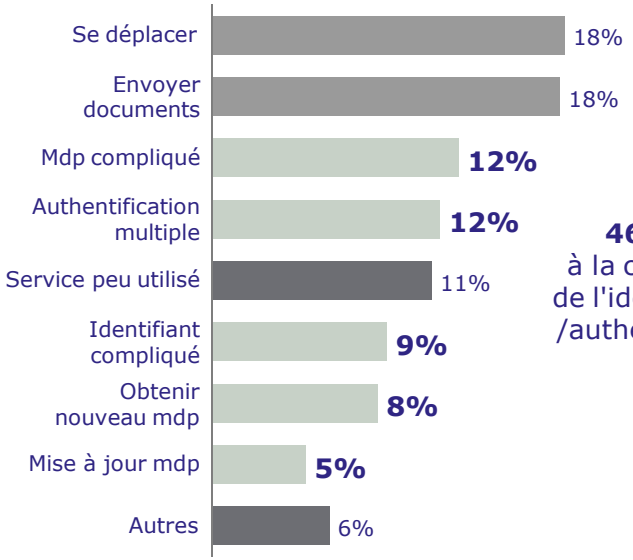
Focus groups et questionnaire en ligne : Réactions des usagers du panel (questionnaire internet)

Direction interministérielle de la transformation publique
libérer l'énergie publique

Deux grandes sources d'insatisfaction lors des procédures d'identification et d'authentification ressortent de l'écoute des usagers

Une perte de temps pour se déplacer ou fournir des documents

% d'occurrences à la question "qu'est-ce qui fait que vous trouvez la manière de vous identifier particulièrement pénible ?"



46% liés à la complexité de l'identification /authentification

La gestion d'un ensemble complexe d'identifiants et de mots de passe

Une multitude d'identifiants et de mots de passe à retenir

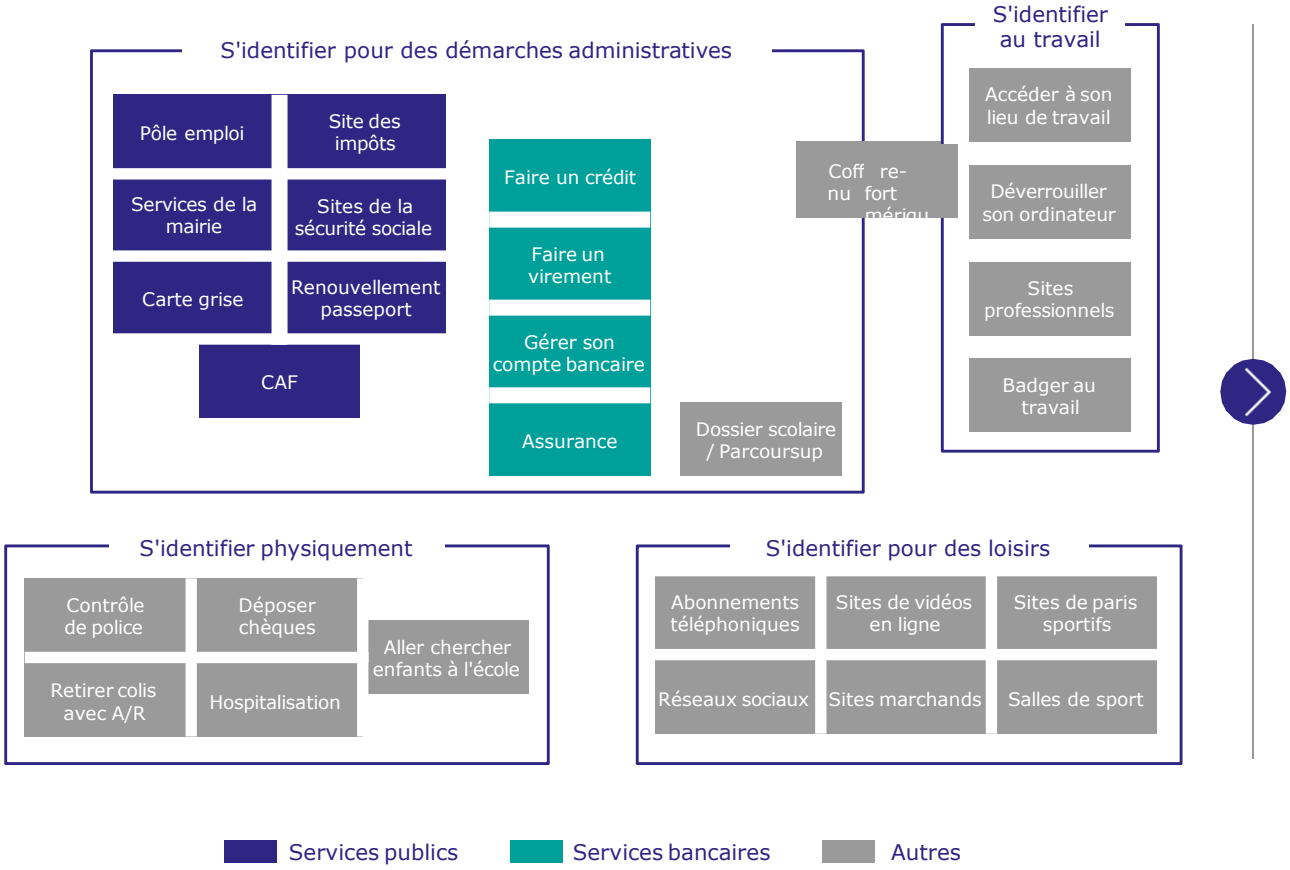
> *C'est compliqué car il faut se souvenir de plein de mots de passe : j'en ai au travail, j'en ai à la maison, c'est une vraie galère.*

Des identifiants et des mots de passe complexes, difficiles à retenir

> *Il faut des caractères spéciaux, des chiffres, des majuscules, etc. C'est un vrai casse-tête.*

Note 1 : la colonne de gauche correspond à l'étude quantitative en ligne (question posée "qu'est-ce qui fait que vous trouvez la manière de s'identifier particulièrement pénible ?") et la colonne de droite à celle qualitative
Note 2 : la ligne "Autres" concerne principalement la longueur et le manque de clarté des procédures d'identification, les bugs informatiques qui rendent l'identification impossible et le nombre élevé de renseignements à fournir pour s'identifier

Les usagers catégorisent spontanément les services publics comme un univers à part (et proche de celui du secteur bancaire)



Les services publics, un univers spécifique, clairement identifié et défini

La banque, un univers spontanément proche de celui des services publics

2 univers qui sont associés à des **démarches administratives**

Note : dans le cadre de l'étude qualitative, les usagers ont dû citer toutes les situations d'identification auxquelles ils pensent spontanément puis ont dû les catégoriser (ils ont dû placer les post-it correspondants à chacune des situations citées sur une matrice dont les axes n'étaient pas définis)

L'accès aux services publics présente trois éléments différenciant majeurs

Des procédures d'identification particulièrement compliquées

- Les identifiants sont souvent imposés et compliqués à retenir
- La structure demandée pour le mot de passe est souvent complexe
- Obtenir un nouveau mot de passe est souvent long voire pénible

Des données sensibles et confidentielles

> *« **Les sites de l'administration c'est plus sensible**. Pour les impôts, c'est toutes nos données financières. Pour Améli, c'est toutes nos données de santé.*

> *« Les données fournies à l'administration, **c'est vraiment des données personnelles**.*

De multiples procédures d'identification peu homogènes entre les différents services (impôts, sécurité sociale, services municipaux,…)

Les services publics, des procédures d'identification compliquées

Des situations spontanément citées comme compliquées et pénibles

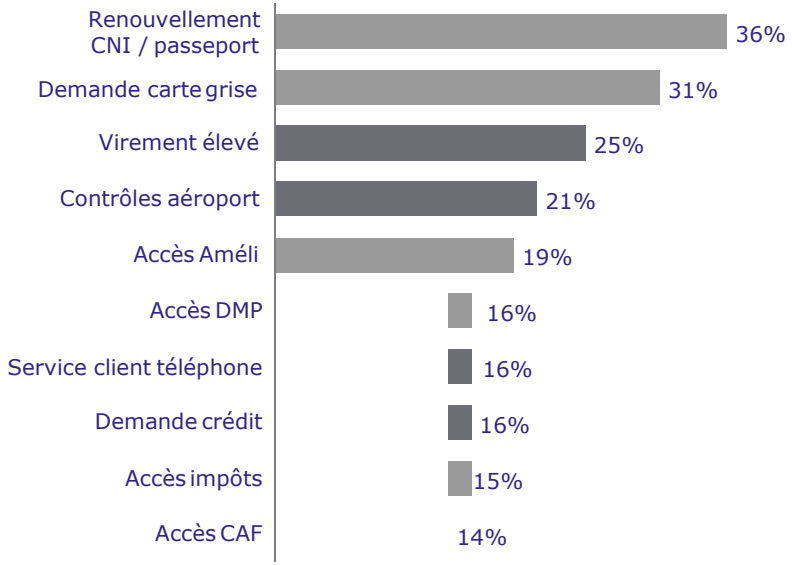
> *S'identifier sur les sites administratifs, **c'est vraiment une chaleur.***

> *Aller sur le site de la sécu c'est pénible. Le mot de passe est compliqué et si on ne s'en souvient pas, **il faut attendre 7/10 jours** pour en recevoir un nouveau par courrier.*

> *C'est pénible de se connecter au site de la CAF car notre identifiant n'a rien à voir avec nous, **on ne s'en souvient jamais.***

6 des 10 situations considérées comme les plus pénibles

Quelles sont les 3 situations pour lesquelles s'identifier est le plus compliqué et pénible parmi les 25 ci-dessous ? (% d'occurrences)



Note : la colonne de gauche correspond à l'étude qualitative et la colonne de droite à celle quantitative en ligne

La banque et la santé, des univers souvent associés aux services publics

Des procédures d'identification particulièrement complexes

Des identifiants et codes compliqués

*« Sur le site de ma banque, c'est énervant de **devoir retrouver mon identifiant à chaque fois**. Ce n'est pas une adresse mail dont on peut se rappeler facilement.*

Nécessité d'envoyer des documents d'identité pour prouver qui l'on est

- Hospitalisation
- Ouverture de compte bancaire en ligne
- Demande de crédit en ligne

Obligation de se déplacer pour prouver son identité dans certaines situations

- Virement d'un montant élevé
- Consultation avec un médecin

Des données sensibles car personnelles et confidentielles

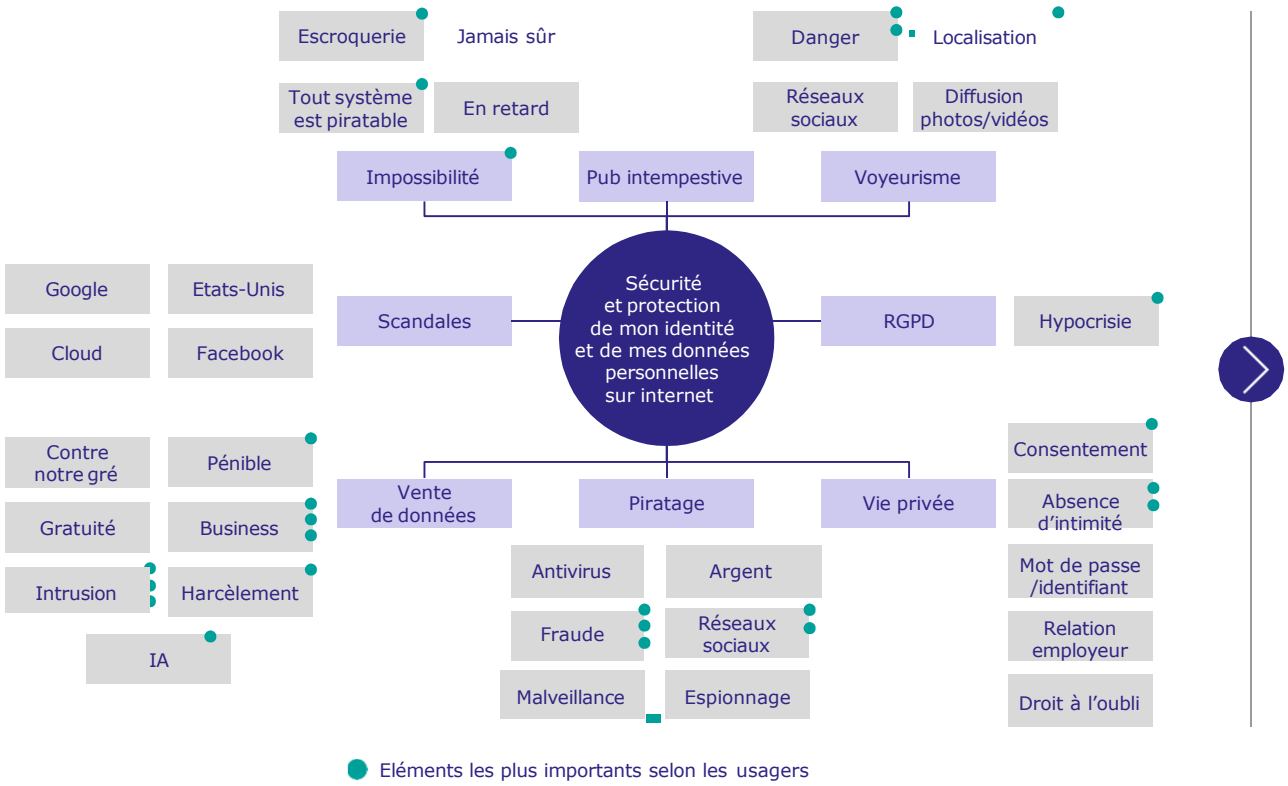
*« Pour tout ce qui est administratif et bancaire, **la procédure d'identification doit être plus sécurisée** qu'avec un mot de passe seulement.*

*« Les données de santé, ce sont des **informations intimes** que l'on ne peut pas divulguer comme ça.*

Note : les citations sont issues de l'étude qualitative

La sécurité et la protection de son identité et de ses données sur internet, un enjeu connoté très négativement, à l'origine d'inquiétudes fortes

Activité « Mindmap » d'associations spontanées par les participants des sessions MindDiscovery



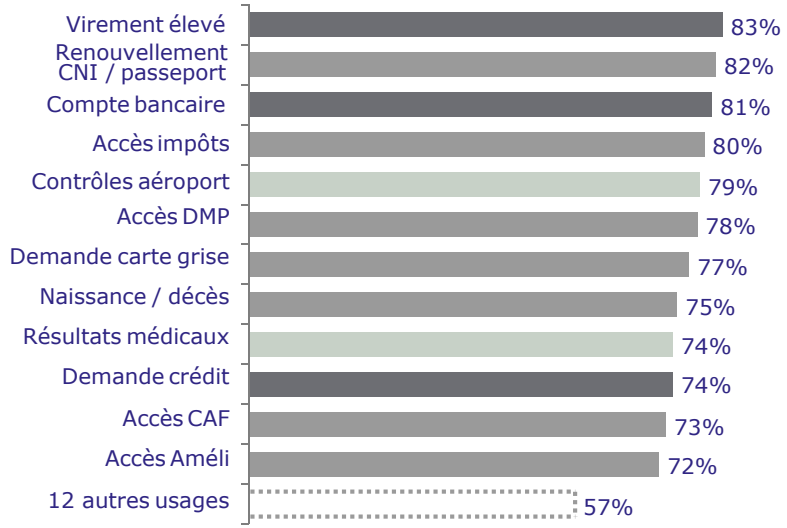
La vente des données personnelles et l'exploitation commerciale et intrusive qui en découle sont les principales craintes liées à la sécurité des données sur internet

Note : dans le cadre de l'étude qualitative, les usagers ont dû dire ce qu'ils associent spontanément à l'expression "sécurité et protection de mon identité et de mes données personnelles sur internet" (encadrés bleus). puis ils ont recommencé cet exercice d'association d'idées à partir des thématiques figurant dans les encadrés bleus (encadrés gris)

La banque et les services publics, des situations d'identification pour lesquelles la sécurité est primordiale mais suffisamment élevée aujourd'hui

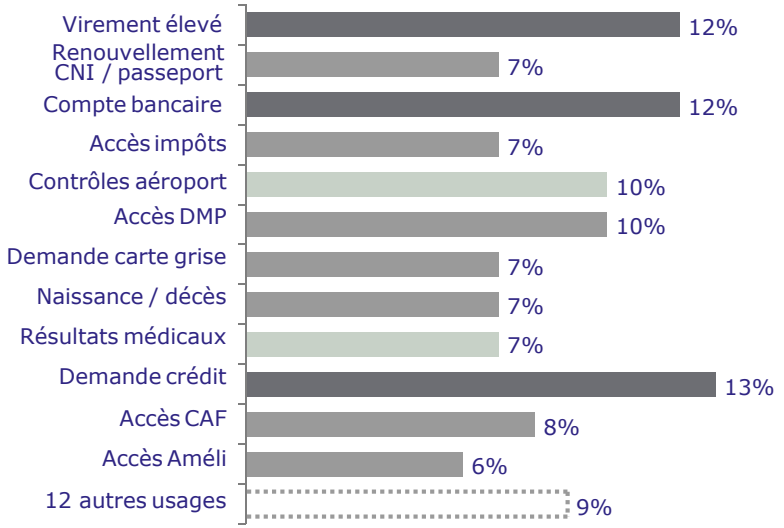
Banque et services publics, les usages pour lesquels la sécurité est cruciale

→ Usages pour lesquels la sécurité de la procédure d'identification est très ou extrêmement importante (% répondants)



Mais une impression limitée de manque de sécurité pour ces usages

→ Usages pour lesquels la sécurité de la procédure d'identification devrait être renforcée (% répondants)

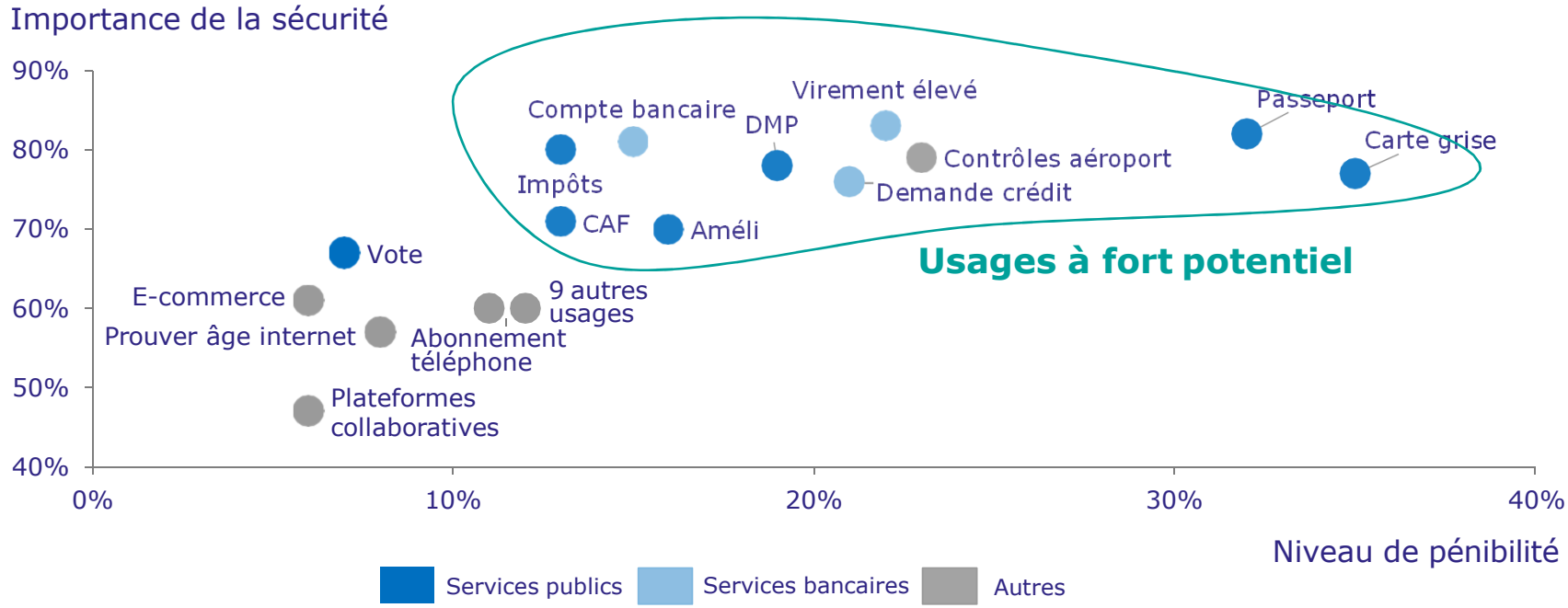


Services publics | Services bancaires | Autres

Note 1 : résultats issus de l'étude quantitative en ligne, questions posées "lorsque vous vous identifiez pour réaliser les actions suivantes, la sécurité de la procédure d'identification est-elle particulièrement importante ?" et "dans quelle mesure trouvez-vous que la manière de s'identifier aujourd'hui est suffisamment sécurisée ou que la sécurité devrait être renforcée ?"
Note 2 : réponses "je ne sais pas" exclues, les % des "13 autres usages" correspondent à une moyenne

Les cas d'usage à fort potentiel pour répondre aux attentes de facilité et de sécurité se concentrent dans les services publics et bancaires

Comparaison des cas d'usage en fonction de la pénibilité des procédures d'identification et du niveau de sécurité souhaité pour s'identifier

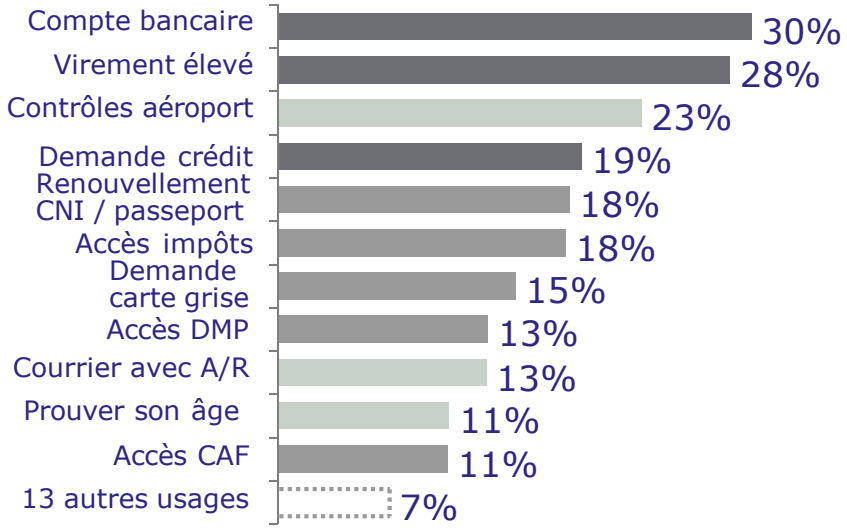


Note 1 : résultats issus de l'étude quantitative en ligne, questions posées "lorsque vous vous identifiez pour réaliser les actions suivantes, la sécurité de la procédure d'identification est-elle particulièrement importante ?" et "pour chacune des actions suivantes, dans quelle mesure trouvez-vous que la manière de s'identifier est simple ou compliquée ?"
Note 2 : importance de la sécurité inclut "extrêmement important" & "très important", niveau de pénibilité inclut "plutôt compliqué et pénible" & "très compliqué et pénible", "je ne sais pas" exclus
Note 3 : les 9 autres usages incluent "service client au téléphone", "courrier avec A/R", "résultats médicaux", "services municipaux", "sites de jeux d'argent", "déclaration naissance / décès", "assurance", "sites de rencontre" et "accès au travail"

La banque et les services publics, les situations d'identification à améliorer en priorité selon les usagers

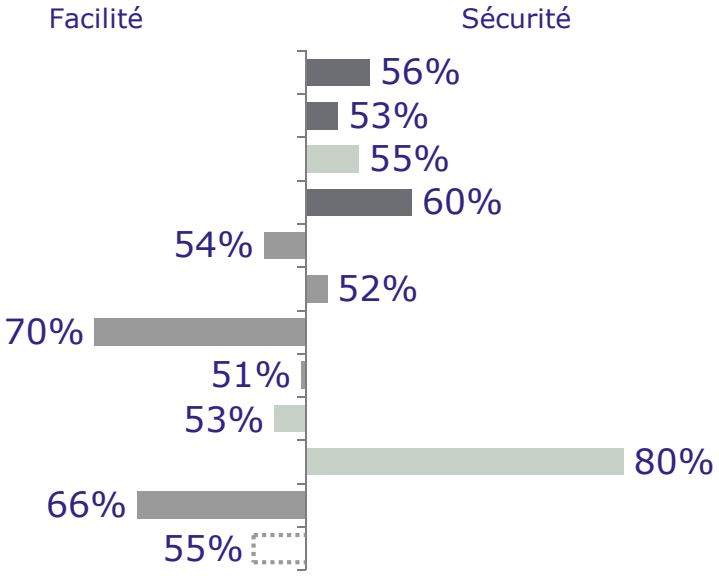
Banque et services publics, les cas d'usage à améliorer en priorité

% répondants qui considèrent la situation d'identification concernée comme une des 3 à améliorer en priorité



Améliorer en priorité l'UX pour les services publics et la sécurité pour ceux bancaires

% répondants en faveur de la facilité ou de la sécurité



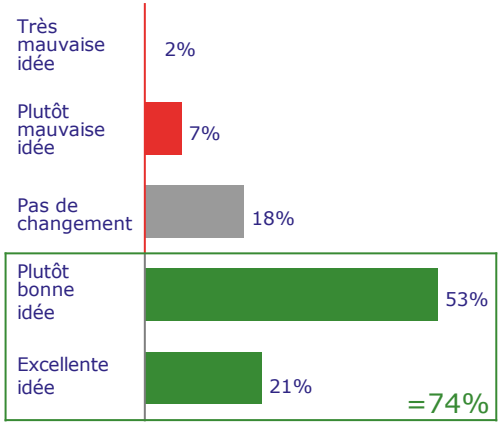
Services publics | Services bancaires | Autres

Note : chiffres issus de l'étude quantitative en ligne, questions posées "si vous aviez la possibilité d'améliorer la manière de s'identifier dans 3 situations, lesquelles choisiriez-vous ?" et "pour les 3 situations que vous avez choisies, qu'aimeriez-vous améliorer en priorité ?"

Le concept d'identité numérique sécurisée bénéficie d'une forte acceptation et ne suscite que très peu de rejet de la part des usagers

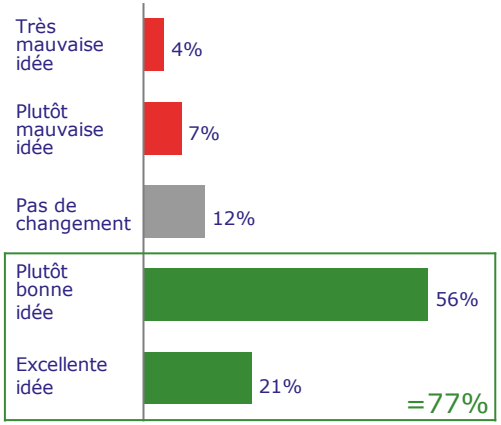
74% d'acceptation après présentation générale du concept

% de répondants qui trouvent que c'est une...



77% d'acceptation après présentation des fonctionnalités

% de répondants qui trouvent que c'est une...



Un taux de **rejet** de la solution **très faible**

Un **fort taux d'adhésion, qui augmente (un peu) après présentation détaillée** de la solution

Une solution et des fonctionnalités **accueillies très favorablement par les usagers**

« Ce serait le rêve. Pourquoi est-ce qu'on n'a pas ça en France ?

« C'est génial, ça Simplifierait la vie !

« Facilité, sécurité, simplicité. Je trouve que ça va être bien.

Note 1 : chiffres issus de l'étude quantitative en ligne, questions posées "sur la base de cette idée générale, vous diriez que cette idée est… ?" et "au regard des différentes possibilités offertes et des nouveaux usages rendus possibles, pensez-vous qu'une telle solution d'identité numérique est… ?"
Note 2 : détail de la présentation du concept fournie aux répondants en annexe

Cette identité numérique sécurisée est spontanément associée à une simplification des procédures d'identification

Réactions spontanées

Que pensez-vous de cette solution ?

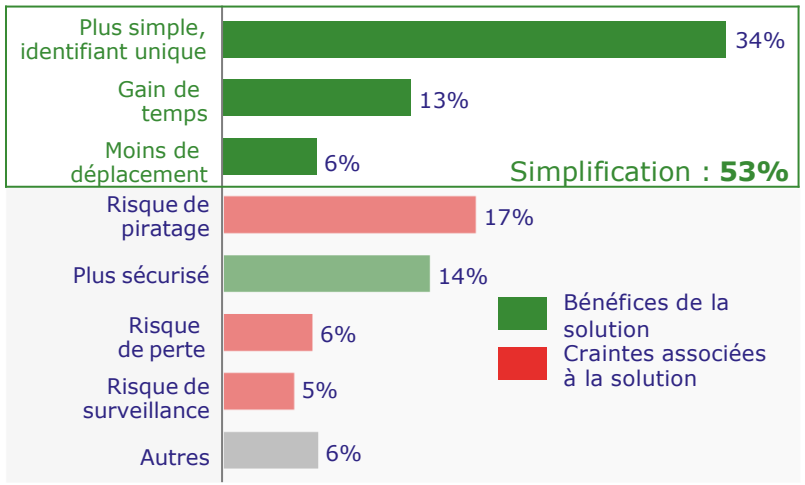
> *Ca **simplifierait** la vie !*

> ***Ce serait pratique** déjà, on n'aurait pas besoin d'utiliser différents codes pour se connecter à différents sites.*

> *Je l'utiliserais quasiment pour tout, **s'il me fait gagner du temps** et qu'il me change la vie, je dis oui !*

Réactions guidées

Quelle proposition correspond le plus à ce à quoi vous avez spontanément pensé ? (1 seule réponse, % d'occurrences)



De manière spontanée, la valeur apportée par une sécurité renforcée est secondaire par rapport à la simplification des procédures

Note : la colonne de gauche correspond à l'étude qualitative et la colonne de droite à celle quantitative en ligne

Sans dominer dans les premières réactions spontanées, les risques associés à cette identité numérique sont bien identifiés par les usagers

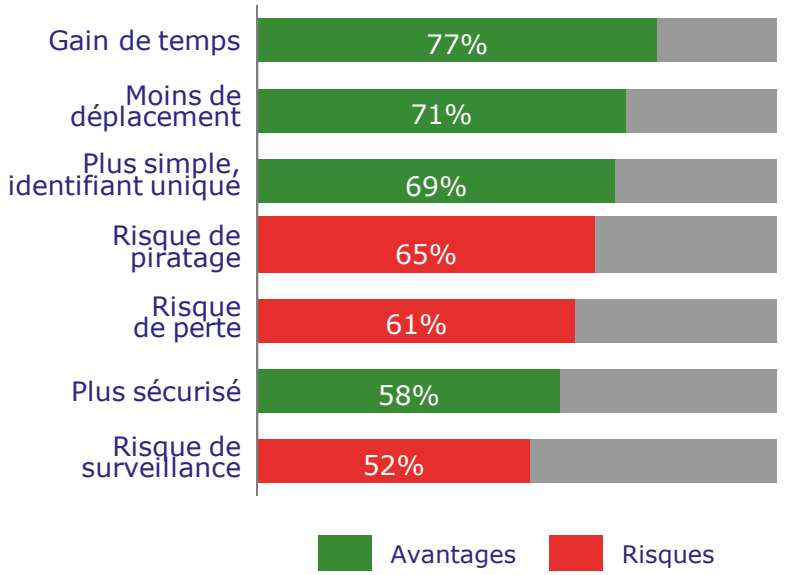
Quels sont les risques associés à cette solution ?

> *C'est bien, c'est facile, c'est pratique mais cela n'exclut pas le danger.* ***Si vous vous faites hacker cette identité****, c'est pour tous les sites concernés.*

> *C'est pratique mais c'est* ***risqué si on la perd****. On ne peut plus accéder à de nombreux sites.*

> *Le gouvernement pourrait aussi nous suivre et* ***nous surveiller.***

% de répondants qui sont d'accord avec les avantages ou les risques ci-dessous



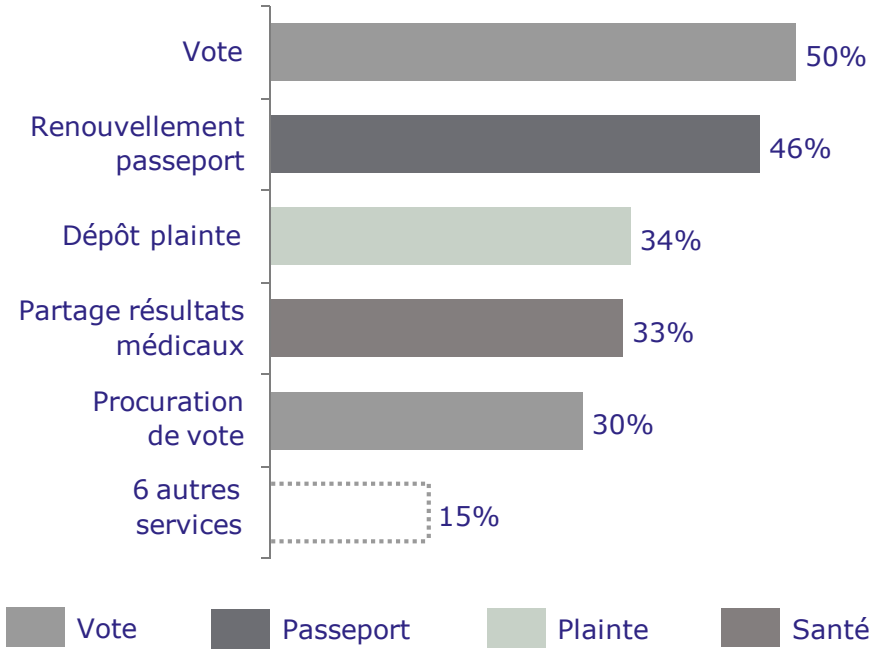
Une perception des avantages et des risques liés à la solution plus équilibrée que lors des réactions spontanées

Note 1 : la colonne de gauche correspond à l'étude qualitative et la colonne de droite à celle quantitative en ligne, question posée "dans quelle mesure êtes-vous personnellement d'accord avec les propositions suivantes ?"
Note 2 : être d'accord inclut les réponses "tout à fait d'accord" et "plutôt d'accord'

Voter et renouveler ses documents d'identité : les deux usages les plus prospectifs plébiscités pour être dématérialisés

Quels seraient les nouveaux services en ligne rendus possibles qui auraient le plus d'intérêt ?

% d'occurrences dans le top 3



> *Je ne comprends pas qu'on ne puisse pas voter en ligne. Il faut encore se déplacer dans un bureau de vote.*

> *Déposer une plainte et suivre son avancement en ligne éviterait d'attendre trois heures au commissariat et permettrait d'avoir un vrai suivi.*

Note : la colonne de gauche correspond à l'étude quantitative en ligne (question posée "parmi ces 11 possibilités, quelles sont les 3 qui vous intéresseraient le plus ?") et la colonne de droite à celle qualitative

L'Etat apparaît comme légitime pour porter cette solution car c'est un acteur à but non lucratif peu enclin à monétiser les données personnelles

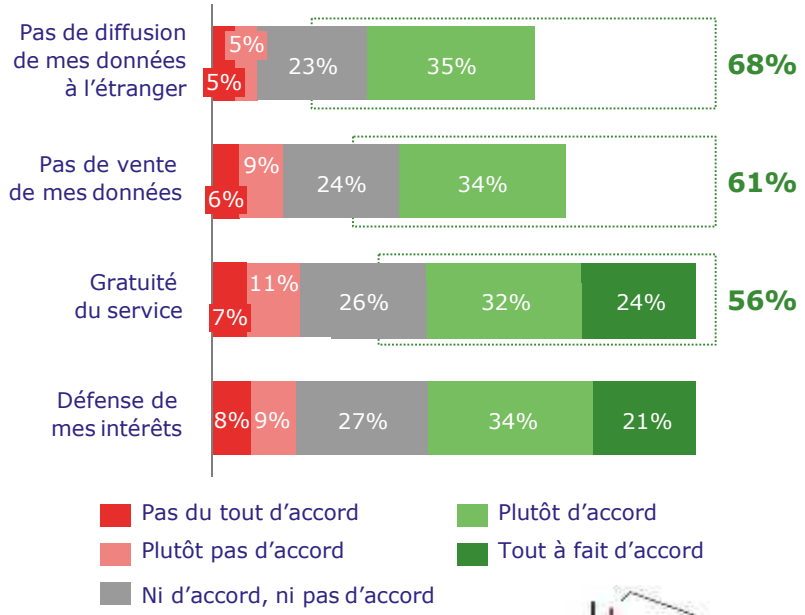
Réactions spontanées

« *L'Etat est là pour nous protéger, il a un **devoir vis-à-vis de nous.** Avec les entreprises, c'est tout de suite du business, tout pour le pognon.*

« *Je sais que **Facebook** voit tout ce que je fais et c'est géré aux Etats-Unis. Je ne l'utilise donc **jamais pour m'identifier.***

Réactions guidées

Dans quelle mesure êtes-vous d'accord avec les avantages suivants dus au fait que la solution soit gérée / garantie par l'Etat ?



Note : la colonne de gauche correspond à l'étude qualitative et la colonne de droite à celle quantitative en ligne

L'identité numérique sécurisée soulève cependant plusieurs inquiétudes

La crainte de se faire usurper son identité numérique et d'être victime de fraudes
(crainte alimentée par les expériences fréquentes de vol de données bancaires et de divulgation non contrôlée de données personnelles)

La dépendance envers un seul système d'identification
(aggrave les conséquences en cas de perte/vol du fait du nombre d'usages empêchés et d'accès à des données personnelles)

Les risques associés à la centralisation des données personnelles fournies à différents services (confusion entre stockage et accès aux données par un identifiant unique)

D'autres inquiétudes citées de manière plus ponctuelle

- Manque de réactivité de l'Etat en cas de problème
- Risque de surveillance étatique
- Risque que l'Etat soit une cible privilégiée par les hackeurs

Trois grandes inquiétudes : l'usurpation d'identité, la centralisation des données et la dépendance envers un seul système d'identification

Réactions spontanées

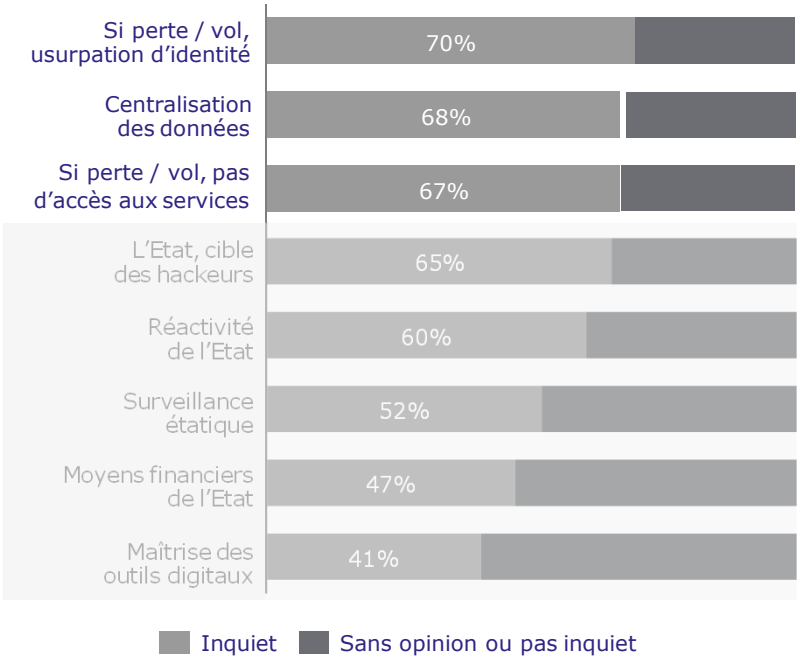
> *L'usurpation d'identité, c'est vraiment le pire. Des gens font des achats ou des crédits à votre nom et vous endettent.* ***C'est horrible !***

> *C'est inquiétant que* ***toutes les données soient concentrées*** *au même endroit.*

> *Il y a plutôt intérêt à ce que les solutions techniques soient doublées car on ne dépend plus que d'un seul système.* ***Si ça plante, je ne peux plus accéder à aucun site*** *de l'administration.*

Réactions guidées

% de répondants inquiets par les propositions suivantes

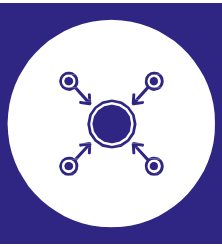


Note 1 : la colonne de gauche correspond à l'étude qualitative et la colonne de droite à celle quantitative en ligne, question posée "voici différentes inquiétudes que d'autres personnes ont exprimées, dans quelle mesure ressentez-vous les mêmes inquiétudes ?"
Note 2 : être inquiet(e) inclut les réponses "très inquiet(e)" et "un peu inquiet(e)"

Des éléments de réassurance à communiquer et mettre en place pour répondre aux inquiétudes et accélérer l'adoption de la solution

Usurpations d'identité et fraudes

- Système d'alertes par mail / sms en cas d'utilisation suspecte de son identité
- Possibilité de désactiver instantanément son identité numérique en cas de perte / vol
- Réactivité de l'Etat en cas de problème



Dépendance envers un seul système

- Système provisoire pour accéder à certains services en attendant le renouvellement de son identité numérique perdue / volée
- Rapidité de la procédure de renouvellement

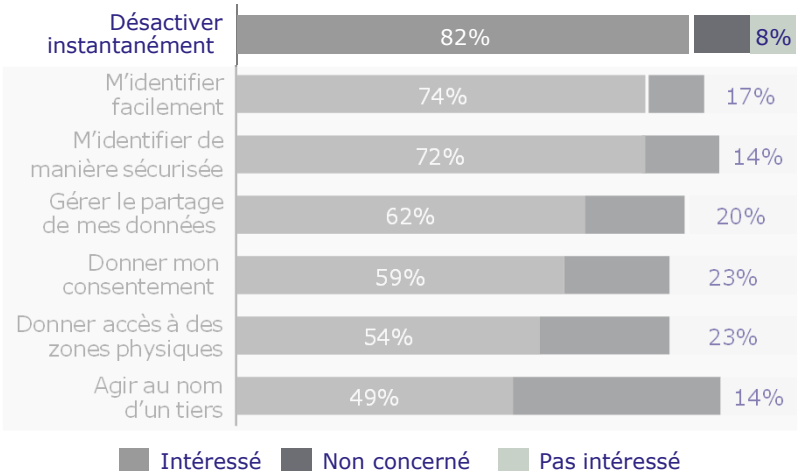
Centralisation des données personnelles

- Communication sur le fait que les données des différents services restent cloisonnées (l'identité numérique n'est qu'une clé d'accès) et que le partage de données doit rester à la main de chacun
- Pas de perte de contrôle sur la gestion de ses données personnelles

Une demande forte de garanties contre les usurpations d'identité & fraudes

"Pouvoir désactiver son eID" est la fonctionnalité la plus appréciée (82%)

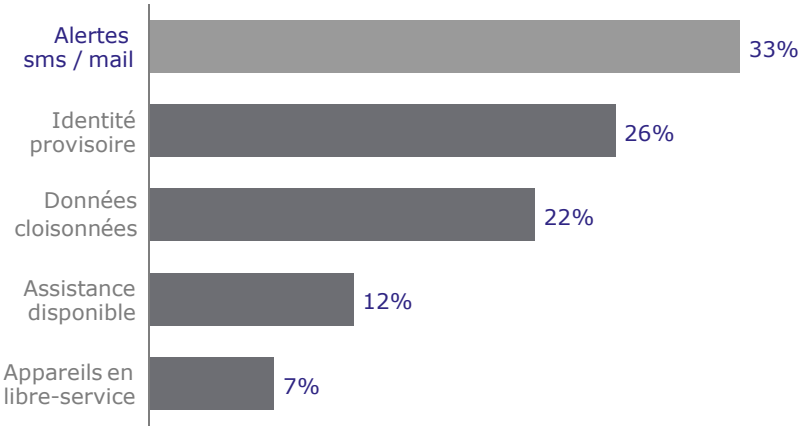
Seriez-vous intéressé(e) par ces fonctionnalités ?



« En cas de perte ou de vol de mon identité numérique, il ne faut pas que ça traine, il faut qu'il y ait tout de suite une action.

Les alertes en cas d'utilisation suspecte : caractéristique la plus rassurante

Parmi les propositions suivantes, quelle serait la plus rassurante pour vous ? (% d'occurrences)



« Ce serait bien d'avoir un système d'alertes comme sur Google. En cas d'utilisation suspecte de mon identité numérique, je reçois un mail pour me prévenir.

Note 1 : résultats issus de l'analyse quantitative en ligne
Note 2 : être intéressé(e) inclut les réponses "Absolument, ce serait un vrai progrès" et "Plutôt oui, ce serait mieux"

Les usagers apprécient les solutions modulaires et personnalisables qui leur donne la liberté d'utiliser leur identité numérique selon leurs préférences

Pouvoir choisir les cas d'usage où ils ont recours à leur eID pour s'identifier

Certains souhaiteraient utiliser la solution pour les services administratifs seulement

> *Je pourrais avoir un système pour tout ce qui est étatique, un autre système pour tout ce qui est achats sur internet, etc. Je ne me vois pas utiliser le système fourni par l'Etat pour m'identifier partout. Cela me mettrait mal à l'aise.*

D'autres souhaiteraient l'utiliser pour toutes les situations pour des raisons pratiques

> *Si le système de l'Etat me fait gagner du temps et qu'il me change la vie, je l'utiliserais pratiquement pour tout.*

Pouvoir choisir l'appareil qu'ils utilisent pour s'identifier avec leur eID

Certains souhaiteraient utiliser la solution uniquement sur leur Smartphone

> *Dès que je me connecte sur internet, j'utilise mon téléphone jamais un PC.*

> *Je n'allume plus mon ordinateur. Depuis que j'ai mon smartphone, je m'en sers très peu.*

D'autres préfèreraient pouvoir s'identifier avec leur eID sur leur PC, notamment pour les démarches administratives

> *Je fais quasiment tout sur PC. Ce n'est pas pratique d'utiliser mon Smartphone.*

> *Les choses importantes, les impôts par exemple, je vais les faire sur PC.*

Note : résultats issus de l'analyse qualitative

La biométrie et la reconnaissance faciale, des moyens d'identification et d'authentification considérés comme pratiques, simples et sécurisés

Des modes d'identification rapides et simples à utiliser

> *La reconnaissance faciale c'est bien parce qu'il n'y a **pas besoin de retenir le code**. Vous n'avez qu'à montrer votre visage et le code ressort directement. **C'est génial !***

> *L'empreinte digitale c'est **très pratique** : j'ai juste à placer mon doigt sur le téléphone. **Je n'ai pas à fournir de chiffres, de codes,** etc.*

Des technologies considérées comme les plus sécurisés

> *Je trouve qu'avec les empreintes digitales ou la reconnaissance faciale on sait à qui on a affaire, c'est la vraie personne. **C'est une valeur sûre.***

> *Le seul moyen de **s'identifier de manière certaine** c'est avec les empreintes digitales ou avec l'iris de l'œil.*

Note : résultats issus de l'analyse qualitative

Analyse des besoins et usages des français

Questionnaire en ligne : Segmentation des répondants selon leur profil et leur maturité digitale

Direction interministérielle de la transformation publique
libérer l'énergie publique

Les réactions des usagers varient principalement selon leur maturité digitale (et peu selon les critères socio-démographiques classiques)

Critères socio-démographiques

=

Pas de différence significative dans l'acceptation de la solution d'identité numérique, les craintes et réassurances par tranche d'âge, zone d'habitation ou catégorie socio-professionnelle

Maturité digitale

≠

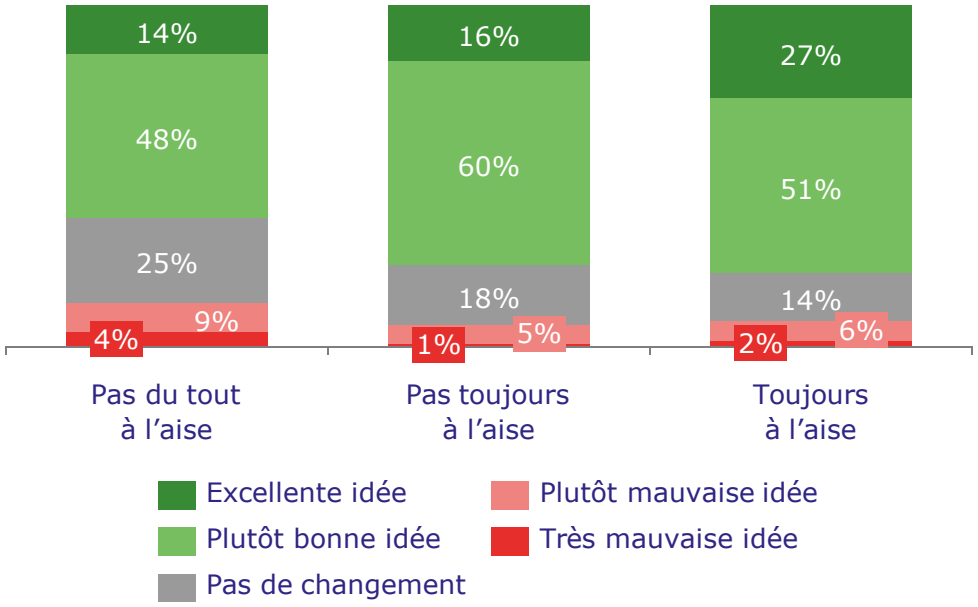
Des différences en revanche suivant le degré d'aisance[1] avec l'utilisation des outils numériques (smartphones)

- → Une acceptation moins générale de la solution par le segment des usagers les moins à l'aise avec les outils numériques (25% des usagers) que par les autres usagers (62% d'acceptation vs. 78%)
- → Des inquiétudes plus fortes sur ce segment d'usagers, qui sont aussi plus difficiles à rassurer. Les éléments de réassurance les plus efficaces auprès d'eux restent cependant les mêmes que pour l'ensemble des usagers
- → Pas de différence non plus dans la priorisation des usages à fort potentiel entre les plus et les moins à l'aise

1 – 3 catégories de répondants: 1) A l'aise pour utiliser son smartphone pour 4 usages classiques, 2) Pas du tout à l'aise pour les 4 usages, 3) Pas toujours à l'aise pour les 4 usages testés
Note : résultats issus de l'analyse quantitative en ligne

Plus les répondants sont à l'aise avec le digital et plus ils adhèrent à la solution d'identité numérique sécurisée

Sur la base de cette idée générale, vous diriez que cette idée est… ? (% de répondants)



78% des répondants "toujours à l'aise avec le digital" adhèrent à la solution d'identité numérique (vs. moyenne à 74%)

Seulement 62% y adhèrent parmi les répondants "pas du tout à l'aise avec le digital"

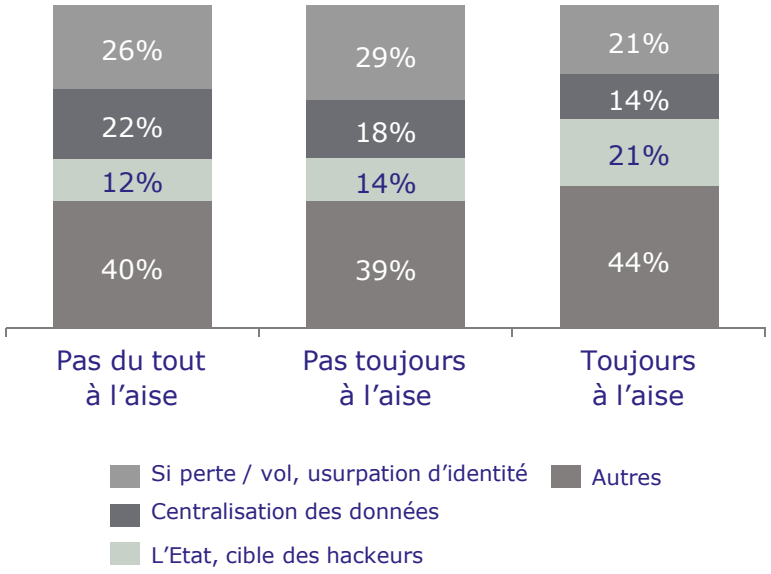
Un taux de rejet plus élevé parmi les répondants "pas du tout à l'aise" (13%) vs. moyenne à 9%

Note : résultats issus de l'analyse quantitative en ligne

Les répondants les moins à l'aise avec le digital sont aussi les plus inquiets par rapport à cette identité numérique…

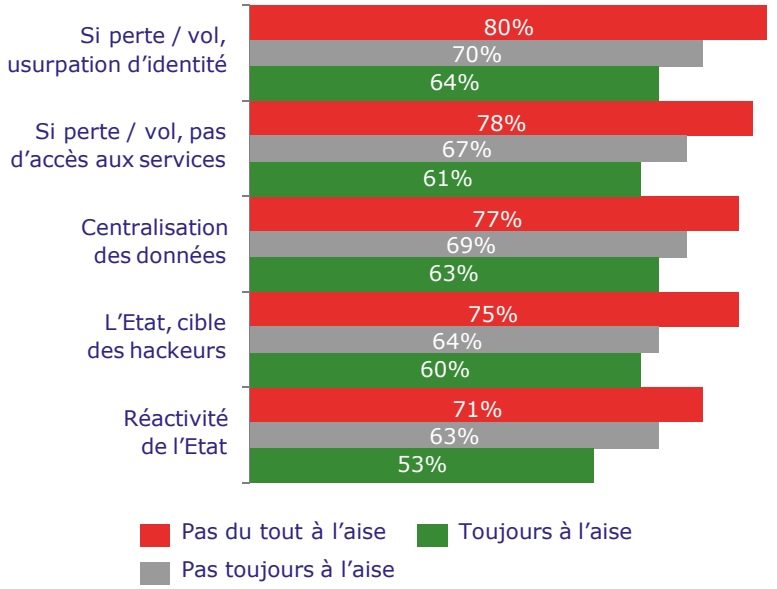
Les inquiétudes les plus fortes sont similaires entre les répondants

Parmi les propositions suivantes, quelle serait la plus inquiétante pour vous ? (% d'occurrences)



Mais le niveau d'inquiétudes est plus élevé pour ceux qui sont peu à l'aise avec le digital

Dans quelle mesure ressentez-vous les inquiétudes suivantes ? (% de répondants inquiets)

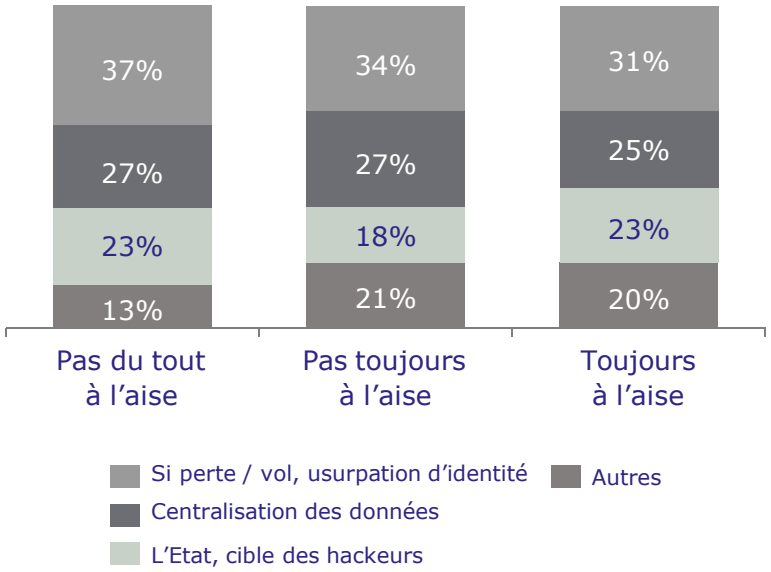


Note 1 : résultats issus de l'analyse quantitative en ligne
Note 2 : être inquiet(e) inclut les réponses "très inquiet(e)" et "un peu inquiet(e)"

… Et ceux qui seront les plus difficiles à rassurer

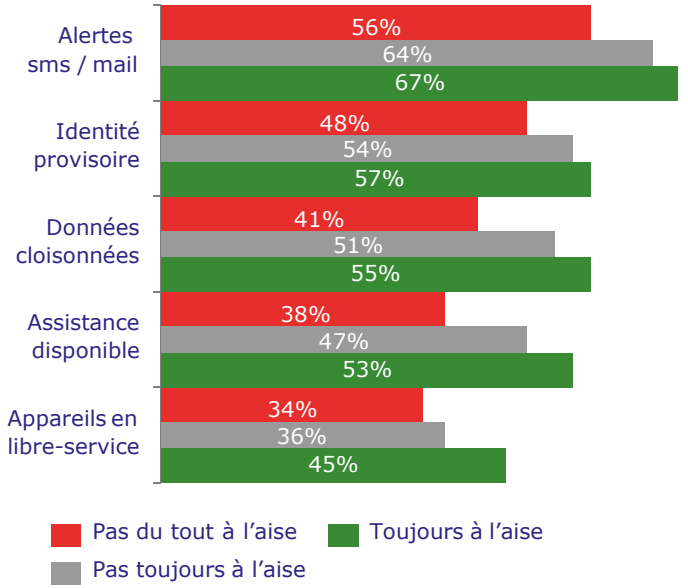
Les propositions les plus rassurantes sont similaires entre les répondants

Parmi les propositions suivantes, quelle serait la plus rassurante pour vous ? (% d'occurrences)



Mais moins ils sont à l'aise avec le digital et moins les éléments de réassurance sont efficaces

Dans quelle mesure seriez-vous rassuré(e) par les propositions suivantes ? (% de répondants rassurés)



Note 1 : résultats issus de l'analyse quantitative en ligne
Note 2 : être rassuré(e) inclut les réponses "très rassuré(e)" et "plutôt rassuré(e)"

Analyse des besoins et usages des français

Questionnaire au téléphone : Réactions des populations "éloignées du numérique"

Direction interministérielle de la transformation publique
libérer l'énergie publique

Enseignements clés de l'étude réalisée auprès des "éloignés du numérique"

- Les "éloignés du numérique" interrogés utilisent peu ou pas internet par manque de confiance (56%) et de maîtrise de la technologie (31%)
- Pour faire des démarches ou des achats, leurs alternatives à internet sont de se déplacer, de téléphoner voire d'abandonner (environ 2/3) — plutôt que de demander assistance (amis, famille, etc., environ 1/3)

- Moins de la moitié (43%) des "éloignés du numérique" adhèrent à la solution d'identité numérique sécurisée, contre 74% pour les autres répondants
- Un taux de rejet plus élevé (38%) de la part de cette population (versus 9% pour les répondants)

- L'attrait de la solution pour les "éloignés du numérique" est d'abord tiré par la simplification des démarches, permise notamment par le partage direct d'informations et de documents

- Les "éloignés du numérique" partagent les mêmes inquiétudes majeures que les autres répondants : le risque d'usurpation d'identité et la dépendance envers un seul système d'identification
- Ces deux inquiétudes sont encore plus fortes pour cette population (~85% inquiets vs ~70%)

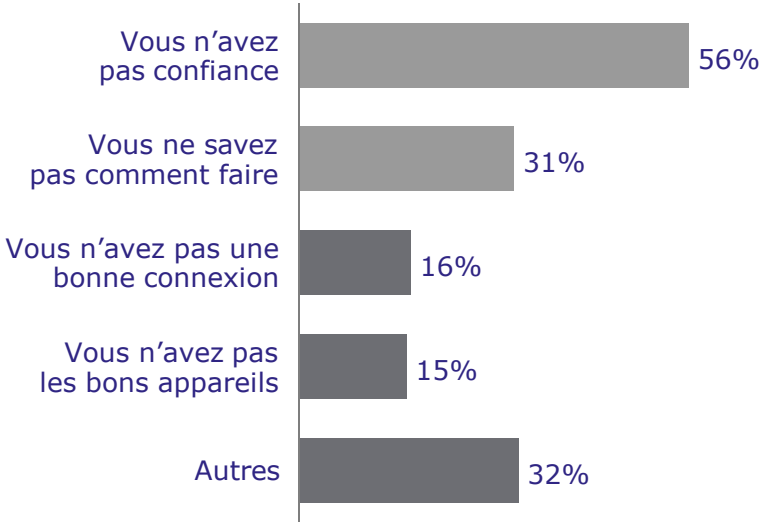
- Comme pour les autres répondants, les alertes en cas d'utilisation suspecte et la mise à disposition d'une identité provisoire en cas de perte / vol sont les éléments les plus rassurants
- La mise en place d'une assistance et la mise à disposition d'appareils nécessaires à l'utilisation de la solution dans des sites publics sont également des éléments de réassurance importants

Note : résultats issus de l'analyse quantitative au téléphone

Ils utilisent peu internet par manque de confiance et de compétences et préfèrent se déplacer, téléphoner voire abandonner la démarche

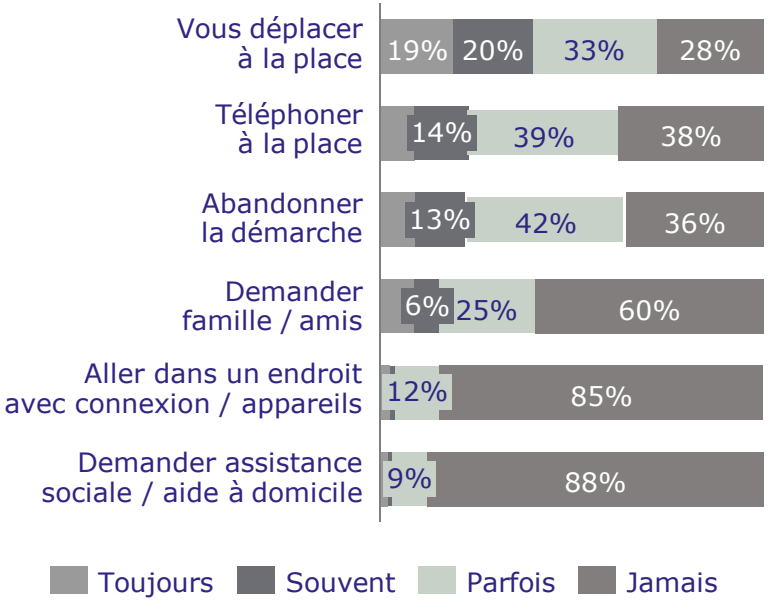
Une faible utilisation due à un manque de confiance et de maîtrise de la technologie

Pour quelles raisons n'utilisez-vous pas ou peu internet ? (% de répondants)



3 alternatives principales aux démarches sur internet : se déplacer, téléphoner & abandonner

Pour faire des démarches / achats sur internet, vous arrive-t-il de… ? (% de répondants)

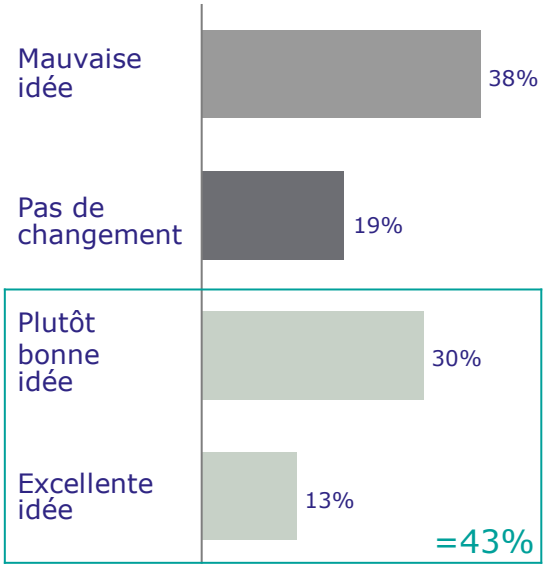


Note : résultats issus de l'analyse quantitative au téléphone

Une adhésion de la solution d'identité numérique garantie par l'Etat plus limitée de la part des "éloignés du numérique"

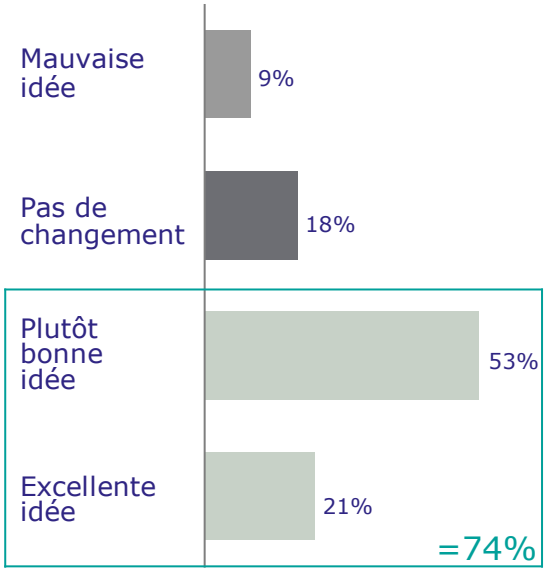
43% d'adhésion parmi les "éloignés du numérique"

% de répondants trouvant que la solution est une…



Contre 74% pour les autres répondants

% de répondants trouvant que la solution est une…



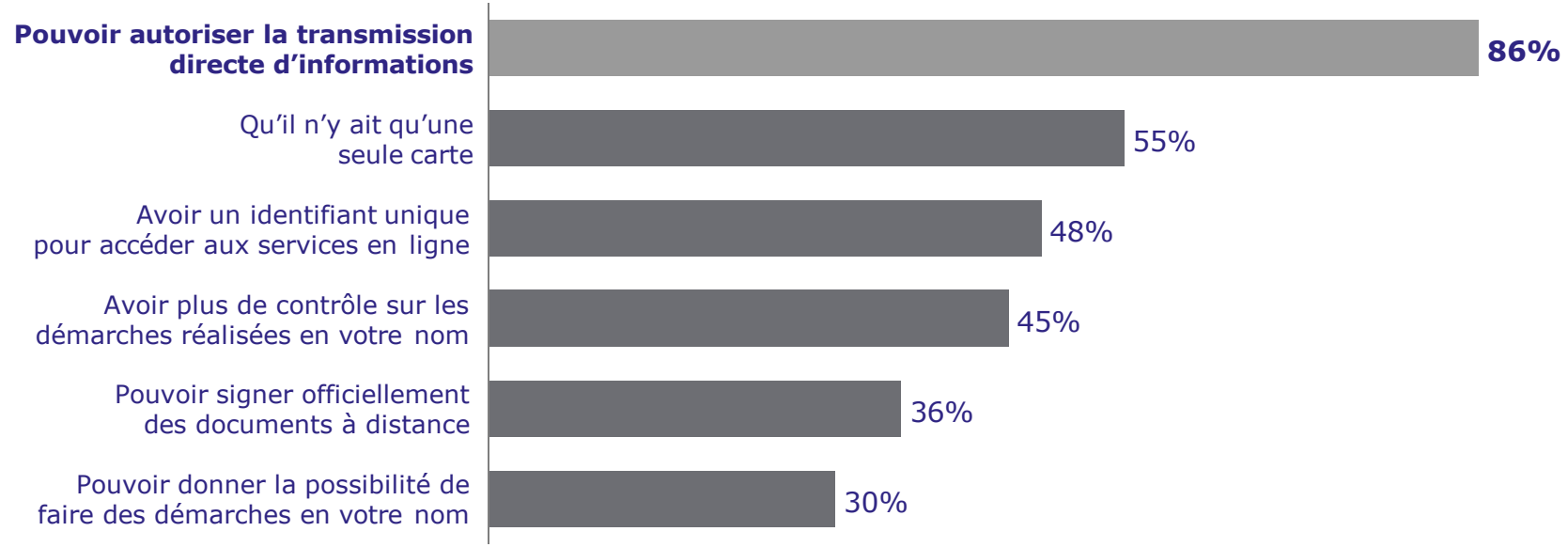
Un taux de rejet élevé de la part des "éloignés du numérique" (38% vs 9% pour les autres)

Moins de la moitié des "éloignés du numérique" **adhèrent à la solution**

Note : pour la colonne de gauche, résultats issus de l'analyse quantitative au téléphone et pour la colonne de droite, résultats issus de celle en ligne

Pour les "éloignés du numérique", l'intérêt principal de la solution est la simplification des démarches notamment par le partage direct d'informations

Quelles sont les 3 possibilités offertes par la solution que vous trouvez les plus intéressantes ? (% d'occurrences dans le top 3)

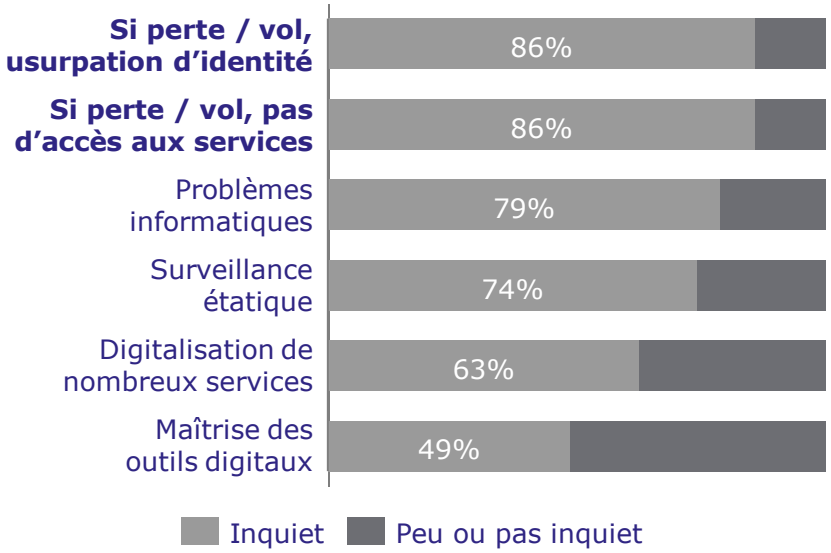


La simplification des démarches (notamment administratives) permise par la solution est un **élément clé à communiquer** pour favoriser l'adhésion des "éloignés du numérique"

Note : résultats issus de l'analyse quantitative au téléphone

Les "éloignés du numérique" partagent les mêmes inquiétudes majeures : risques d'usurpation d'identité et dépendance envers un seul système

Êtes-vous inquiet(e) ou non par rapport aux éventualités suivantes ? (% de répondants)



L'usurpation d'identification et la dépendance envers un seul système sont les inquiétudes majeures des "éloignés du numérique"

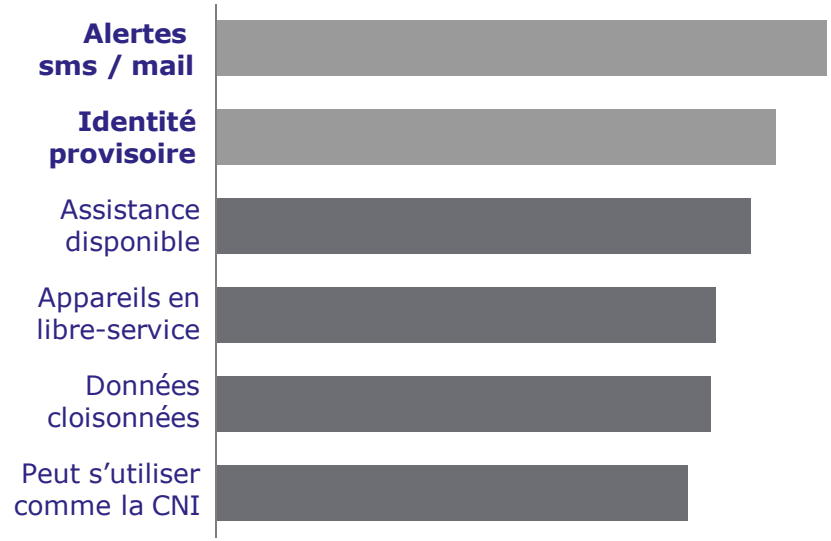
Ces 2 inquiétudes sont plus fortes parmi cette population (86% vs ~70% pour les autres répondants)

Le risque de surveillance par l'Etat est également une inquiétude importante pour les "éloignés du numérique"

Note 1 : résultats issus de l'analyse quantitative au téléphone
Note 2 : être inquiet(e) inclut les réponses "Très inquiet(e)" et "Plutôt inquiet(e)"

Les systèmes d'alertes et d'identités provisoires sont aussi les éléments qui rassurent le plus les "éloignés du numérique"

Trouvez-vous les précisions suivantes rassurantes ou non ? (% de répondants rassurés)



Les 2 éléments de réassurance majeurs répondent aux inquiétudes fortes des "éloignés du numérique" :

- Système d'alertes en cas d'utilisation suspecte de la solution
- Possibilité de recevoir une identité provisoire en cas de perte ou de vol

Le service d'assistance et les appareils mis en libre-service sont également des éléments de réassurance importants pour les "éloignés du numérique"

Note 1 : résultats issus de l'analyse quantitative au téléphone
Note 2 : être rassuré(e) inclut les réponses "Tout à faire rassuré(e)" et "Plutôt rassuré(e)"

Sommaire

Synthèse : qualification des usages porteurs

Les usages à plus forte volumétrie ne sont pas toujours les plus compatibles avec l'intégration d'une solution d'identification numérique sécurisée

> Usages pour lesquels les fournisseurs de services privés privilégient l'Ux (ex. achats en ligne)

> Accès à des lieux physiques qui présentent des risques de surveillance / géolocalisation, dont la mise en œuvre relève d'autres solutions (ex. lieu de travail, école, EHPAD, transports, etc.)

Les usages prioritaires pour intégrer la solution d'identité numérique sécurisée combinent plusieurs caractéristiques : une volumétrie importante, un niveau de pénibilité élevé pour les usagers, une exigence de sécurité importante

Ces usages prioritaires s'inscrivent dans 4 univers de besoins principaux :

> La santé et les prestations sociales

> La banque et les paiements

> La fiscalité

> Le vote et les devoirs du citoyen (y compris le renouvellement des titres d'identité)

D'autres usages méritent aussi de figurer au rang des priorités

> Avec moins de volumes mais à forte portée symbolique, comme par ex. l'accès à certains services publics "réservés" (prestations pour des publics fragiles, démarches pouvant nécessiter une mise à distance avec les agents publics comme pour certains types de plaintes)

> Et/ou des usages nouveaux qui facilitent l'accès à certains droits / services (ex. échanges sécurisés à distance comme la consultation d'un médecin ou un acte notarié, vérification d'un statut comme celui de chômeur ou d'étudiant)

Source : Documentation interne Programme, DINSIC, DITP ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Plusieurs critères ont été utilisés pour identifier les usages à potentiel et caractérisés par un besoin élevé de sécurité (de façon non systématique)

Qualification du potentiel

Volumes

- **Volume de recours annuel à l'usage***
- **Fréquence de recours à l'usage**
- **Potentiel d'usagers concernés**
  (Appétence ; Degré d'irritation et de contrainte)

Usagers

- **Amélioration de la fluidité du parcours usager**
  (Délais d'attente, déplacements réduits, etc.)
- **Degré d'intérêt des usagers**
  (Enquête qualitative et quantitative)

Fournisseurs

- **Horizon de faisabilité**
- **Potentiel d'optimisation des coûts**
  (Qualitatif et/ou quantitatif)
- **Potentiel de création de valeur**
  (lutte contre la fraude, Ux, maîtrise des coûts)

Qualification du besoin de sécurité

Usagers

- **Besoin de protection exprimé vis-à-vis de l'usage**
  (Enquête qualitative et quantitative)
- **Sensibilité perçue des données impliquées, valeur symbolique**

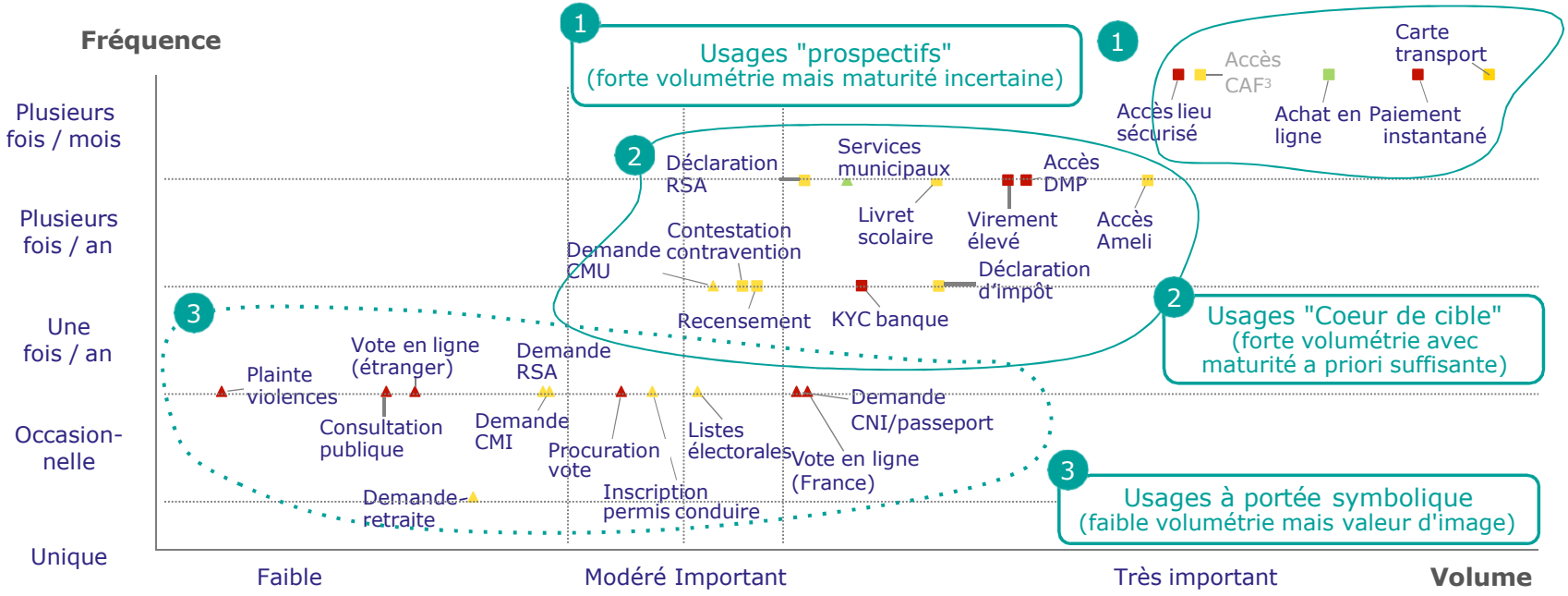
Fournisseurs

- **Contraintes juridiques/ réglementaires existantes et projetées**
  (Y compris les enjeux régaliens)
- **Taux de fraude existant et projeté**
- **Risques liés aux fraudes**
  (Y compris le coût de la fraude)
- **Besoin de sécurisation exprimé, image**
  (Qualitatif**)

(*) Source : données publiques, analyse et estimations BCG & EY-Parthenon (notamment pour usages émergents)
(**) Source : entretiens experts sectoriels et données déclaratives recueillies par le programme ID NUM ; propositions BCG & EY-Parthenon lorsque déclaratif non disponible

Des usages à très forte volumétrie qui ne sont pas forcément matures pour une identité forte, des usages "cœurs de cible" et des usages symboliques, à forte visibilité

Cartographie – Fréquence x volume



Légende : ☐ *Usages à potentiel élevé* △ *Usages symboliques* *- Niveau faible / substantiel - Niveau substantiel - Niveau élevé*

Note 1 : Les paliers de volumes sont définis par une segmentation en quartiles, sur base de l'ensemble de l'estimation des volumes des usages analysés (volumes actuels ou potentiels pour les usages émergents) ; source : données publiques, analyse et estimations BCG & EY-Parthenon
Note 2 : Les critères retenus pour les usages à fort potentiel sont la fréquence = une fois par an ou plus fréquent et le volume = important ou très important
Note 3 : L'accès à son compte CAF est une exception, c'est un usage "cœur de cible«
Note 4 : Les niveaux de sécurité se basent sur les entretiens experts sectoriels (voir annexe 1) et les données déclaratives recueillies par le programme ID NUM (services publics) + propositions BCG & EY-Parthenon lorsque le déclaratif n'était pas disponible
Source : Analyses BCG & EY-Parthenon

Clef de lecture : trois catégories d'usages identifiées en fonction des volumes tirés par ces usages et de leur fréquence d'utilisation

1 **Les usages qui tirent des volumes très importants mais qui ne sont pas encore prêts à bénéficier d'une procédure d'identification très sécurisée**

> Un potentiel très élevé en termes de volume et de fréquence d'utilisation

> Mais des usages qui sont insuffisamment matures pour y intégrer une procédure d'identification très sécurisée ou pour être adossés à la CNIe (fournisseurs de services privilégiant l'UX, usages prospectifs liés notamment à l'accès à des lieux physique, etc.)

> Accéder à son compte CAF est une exception : usage à fort potentiel pour la CNIe, mais bénéfice
d'un niveau de sécurité élevé à approfondir

2 **Les usages qui tirent des volumes importants et qui sont d'excellents candidats cœur de cible à la mise en place d'une procédure d'identification très sécurisée**

> Santé : accéder à son compte Améli, à son dossier médical partagé, …

> Administrations : se connecter à impôts.gouv, faire sa déclaration trimestrielle RSA, …

> Banque : faire un virement d'un montant élevé, ouvrir un compte bancaire (KYC), …

3 **Les usages symboliques qui tirent de plus faibles volumes mais à forte visibilité pour le programme CNIe du fait de leur dimension symbolique**

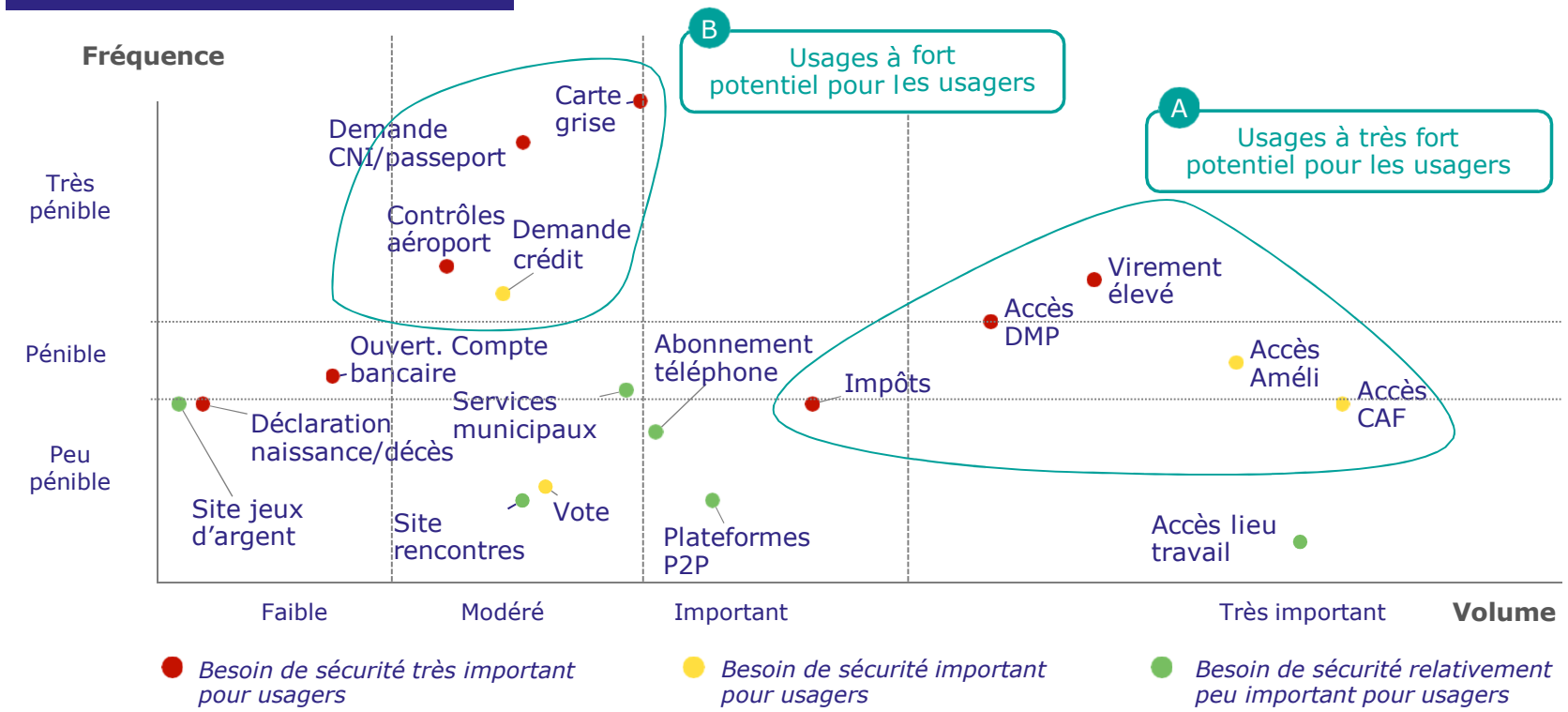
> Vie citoyenne : vote en ligne, demande de procuration en ligne, …

> Droits sociaux : demande de RSA, demande de CMI, …

> Justice : signalement de violences conjugales, d'agressions sexuelles, …

Les usages à fort potentiel appartiennent aux univers de la santé, des prestations sociales, de la fiscalité et de la banque

Cartographie – **Pénibilité x volume**



Note 1 : Les paliers de volumes sont définis par une segmentation en quartiles, sur base de l'ensemble de l'estimation des volumes des usages analysés (volumes actuels ou potentiels pour les usages émergents) ; source : données publiques, analyse et estimations BCG & EY-Parthenon
Note 2 : Les taux de pénibilité sont issus du questionnaire "voix des usagers" en ligne (% de répondants qui trouvent la situation d'identification pénible)
Note 3 : Les paliers de pénibilité sont définis par une segmentation en tertiles
Source : Analyses BCG & EY-Parthenon

Clef de lecture : deux catégories d'usages identifiées en combinant les potentiels de volumes et la "voix des usagers"

	Catégorie A	Catégorie B
Volumes tirés	**Très importants**	Modérés ou importants
Niveau de pénibilité pour les usagers	Elevé	**Très élevé**
Besoin de sécurité pour les usagers	**Elevé ou très élevé**	**Elevé ou très élevé**
Exemples d'usages	> Accéder à son compte CAF > Accéder à son compte Améli > Faire un virement d'un montant élevé	> Demander une carte grise > Renouveler ses papiers d'identité > Demander un crédit
	Très fort potentiel	**Fort potentiel**

Méthodologie pour cartographier les usages

Identification d'une **liste détaillée d'usages**, issue des différents besoins exprimés par les fournisseurs de services publics et privés

Premier élément de qualification de chacun de ces usages : leur **volumétrie** et de leur **fréquence** d'utilisation

Deuxième élément de qualification : le niveau de **sécurité** attendu par les **fournisseurs de services** et par les **usagers**

Troisième élément de qualification : le niveau de **pénibilité** de chaque usage pour s'identifier du point de vue des usagers

En **croisant ces 3 critères** (volumétrie, sécurité et pénibilité), les **usages à très fort potentiel** ont été identifiés

Source : Analyses BCG & EY-Parthenon

Les usages privés et publics recensés sont tous intrinsèquement reliés à des moments de vie de l'usager

« Je gère mon identité numérique »
Diffusion d'attributs d'identité de façon sélective, suivi de l'historique de consultation de mes données, etc.

« Je me forme et je travaille »
S'inscrire à l'école, se connecter aux portails scolaires (Parcoursup, universités), passer des examens / concours, etc

« Je me soigne »
S'inscrire à la sécurité sociale, souscrire une mutuelle, accéder aux portails Ameli, se faire hospitaliser, consulter un médecin, etc.

« Je m'acquitte de mes devoirs de citoyen »
Déclarer impôts, payer taxe d'habitation, renouveler titres d'identité, etc.

« Je gère mes services du quotidien »
Ouvrir un compte bancaire, EDF ou d'abonnement téléphonique, gérer mon épargne, déclarer un sinistre, etc.

« Je suis impacté par un évènement »
Se marier, changer d'adresse, acheter ou louer un bien immobilier, déclarer la naissance d'un enfant, déclarer un décès, etc.

Moments de vie

« Je fais valoir mes droit sociaux »
S'inscrire à Pôle emploi et à la CAF, consulter mon relevé de carrière (retraite), etc.

« J'achète un produit ou un service »
Se connecter à des sites marchands, payer sur un terminal ou en ligne, recevoir un colis, s'inscrire à un programme de fidélité, etc.

« Je participe à la vie citoyenne »
Voter aux élections et aux référendums, participer aux consultations citoyennes, etc.

« Je profite de mon temps libre »
Accéder à la salle de sport, visiter un musée, se connecter aux réseaux sociaux, jouer aux jeux vidéos en live, etc.

« Je me déplace, je voyage »
Prendre l'avion, franchir des frontières, obtenir un visa, j'accède à des lieux sécurisés, etc.

Source : Analyses BCG & EY-Parthenon

Parmi la liste détaillée d'usages recensés, 14 sont caractérisés par une forte volumétrie et un besoin élevé de sécurité

	Qualification du potentiel	Qualification du besoin de sécurité
Priorités	Accès au dossier médical partagé (DMP) ★	Accès au dossier médical partagé (DMP) ★
	Réaliser un paiement instantané d'un montant élevé ★	Réaliser un paiement instantané d'un montant élevé ★
	Accéder à un lieu sécurisé (travail, école, EHPAD, etc.) ★	Accéder à un lieu sécurisé (travail, école, EHPAP, etc.) ★
	Ouvrir un compte bancaire (KYC)	Ouvrir un compte bancaire (KYC)
	Se connecter à son compte Ameli	Consulter et gérer son compte CAF
	Couverture maladie universelle – complémentaire	Demande de carte vitale
	Consulter et gérer son compte CAF	Consulter un médecin en ligne ★
	Consulter le livret scolaire de ses enfants, gérer la vie scolaire	Envoi de lettre recommandée électronique (LRE)
	Réaliser sa déclaration trimestrielle de RSA	Voter de manière électronique en France
	Participer au recensement de la population (OMER)	Voter de manière électronique en tant que Français de l'étranger
	Utiliser la CNIe comme titre de transport ★	Obtenir une procuration de vote
	Faire un achat en ligne	Participer à une consultation publique ★
	Réaliser sa déclaration d'impôt	Participer à un référendum d'initiative partagée ★
	Contester une contravention	Passer les contrôles à l'embarquement à l'aéroport ★
		Demander et renouveler sa carte d'identité nationale en ligne
		Demander et renouveler son passeport en ligne
		Suivre une affaire judiciaire ou civile en ligne
		Visiter un proche en prison
		Etablir un acte authentique à distance (y compris de vente)

★ Usage émergent

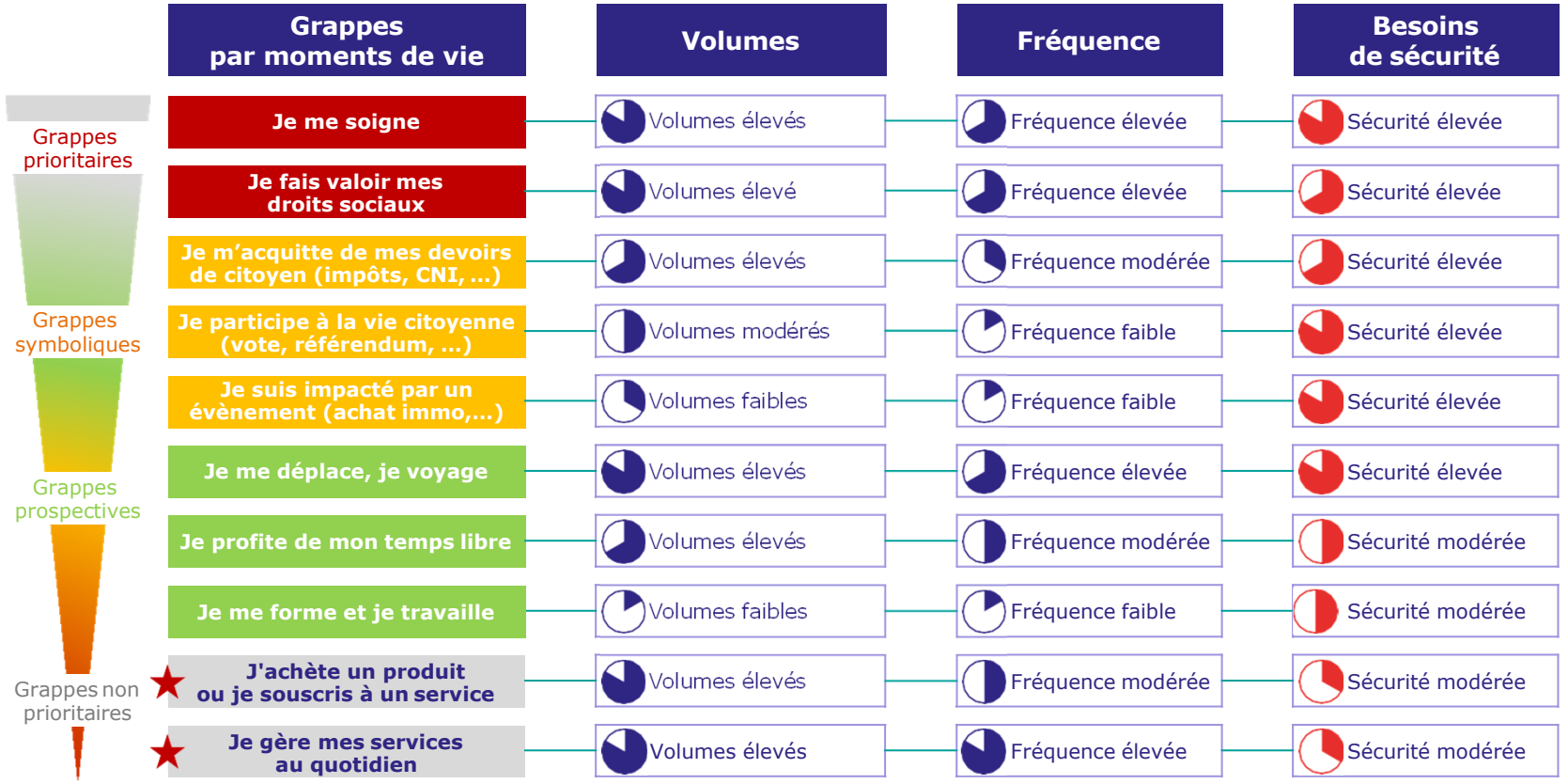
Note 1 : Critères retenus pour les usages à fort potentiel : Fréquence = Une fois par an ou plus fréquent ; Volume = Important ou très important
Note 2 : Volumes sur base de l'ensemble de l'estimation des volumes des usages analysés (volumes actuels ou potentiels pour les usages émergents) ; source : données publiques, analyse et estimations BCG & EY-Parthenon
Note 3 : Les niveaux de sécurité se basent sur les entretiens experts sectoriels (voir annexe 1) et les données déclaratives recueillies par le programme ID NUM (services publics) + propositions BCG & EY-Parthenon lorsque le déclaratif n'était pas disponible
Source : Analyses BCG & EY-Parthenon

Au-delà de la volumétrie et du besoin de sécurité, il est essentiel d'intégrer à la démarche des usages à dimension symbolique et à forte visibilité

	Exemples d'usages à portée symbolique, recensés
Potentiel d'amélioration dans l'exercice de ses droits	Voter de manière électronique en France
	Inscription sur les listes électorales
	Voter de manière électronique depuis l'étranger
	Participer à un référendum d'initiative partagée
	Obtenir une procuration de vote
	Participer à une consultation publique
Potentiel d'amélioration de l'accès et du parcours sur des démarches sensibles	Prouver un droit à réduction (handicap, chômage, etc.)
	Dépôt de plainte pour violences sexuelles
	Demande de carte mobilité inclusion (CMI)
	Demande de CMU
Image de l'Etat (garant de la modernisation des services publics, de la lutte contre la fraude, de la protection des citoyens, etc.)	Prouver son âge en ligne
	Demande/renouvellement de Carte nationale d'identité
	Inscription au permis de conduire
	Faire une démarche auprès de sa mairie
	Demande de RSA / de prestations sociales / chômage

Source : Analyses BCG & EY-Parthenon

Une séquence de déploiement des usages qui peut être pensée par grappes, sur des parcours cohérents, priorisés par volume et besoins de sécurité



★ Sauf pour le secteur bancaire qui est une priorité

Note : cf. pages détaillées pour la liste des usages par moments de vie

Pour mémoire : liste des usages étudiés et qualifiés (1/7)

▲ *Usage symbolique*

Moment de vie	Usages qualifié	Type	Sécurité (besoin FS)	Fréquence	Volume (# recours/an)	Pénibilité (usagers)	Sécurité (besoin usagers)
Je me soigne	Consulter un médecin en ligne	Public	Elevé	Plusieurs fois par an	Faible (~900 000)	Usage prospectif plutôt apprécié par les usagers (28% d'occurrences dans top 3)	
	Connexion au compte Améli	Public	Substantiel	Plusieurs fois par an	Très important (~201 000 000)	Pénible	Importante
	Changement d'adresse Améli	Public	Elevé	Occasionnelle	Important (~3 100 000)		
	Demande de carte vitale	Public	Substantiel	Unique	Faible (~710 000)		
	Accéder au Dossier Médical Partagé (DMP)	Public	Substantiel	Plusieurs fois par an	Très important (~60 000 000)	Très pénible	Très importante
	▲ Demande de la CMU – complémentaire	Public	Substantiel	Une fois par an	Important (~2 630 000)	*Usages qui ne sont pas ressortis dans l'étude "voix des usagers"*	
	Demande de carte européenne d'assurance maladie (Ceam)	Public	Elevé	Unique	Important (~3 800 000)		
	Transmission de résultats médicaux entre professionnels	Privé	Substantiel	Non qualifié	Non qualifié	Usage prospectif très apprécié par les usagers (34% d'occurrences dans top 3)	
Je gère mes services quotidiens (1/2)	Envoyer une lettre recommandée électronique qualifiée (LRE)	Privé	Elevé	Occasionnelle	Modéré (~1 000 000)	*Usages qui ne sont pas ressortis dans l'étude "voix des usagers"*	
	Réaliser un paiement instantané	Privé	Elevé	Plusieurs fois par mois	Très important (~3 000 000 000)		
	Effectuer un virement d'un montant élevé	Privé	Elevé	Plusieurs fois par an	Très important (~100 000 000)	Très pénible	Très importante

Note 1 : Qualification de la fréquence selon 5 paliers (Plusieurs fois par mois / Plusieurs fois par an / Une fois par an / Occasionnelle / Unique).
Note 2 : Qualification du volume sur la base de quartiles des usages analysés (Très important / Important / Modéré / Faible) – source : données volumes actuels ou potentiels pour les usages émergents ; source : données publiques, analyse et estimations BCG & EY-Parthenon .
Note 3 : Qualifications de la pénibilité et du besoin de sécurité (usagers) selon 3 paliers (Peu pénible / Pénible / Très pénible et Relativement peu important / Important / Très important) .
Note 4 : niveaux de sécurité sur la base des entretiens experts sectoriels (voir annexe 1) et des données déclaratives recueillies par le programme ID NUM (services publics) + propositions BCG & EY-Parthenon lorsque le déclaratif n'était pas disponible.

Pour mémoire : liste des usages étudiés et qualifiés (2/7)

▲ *Usage symbolique*

Moment de vie	Usages qualifié	Type	Sécurité (besoin FS)	Fréquence	Volume (# recours/an)	Pénibilité (usagers)	Sécurité (besoin usagers)
Je gère mes services quotidiens (2/2)	▲ S'inscrire aux services proposés par sa mairie	Public	Faible / Substantiel	Plusieurs fois par an	Très important (~10 000 000)	Pénible	Relativement peu importante
	Consulter le livret scolaire des enfants	Public	Substantiel	Plusieurs fois par an	Très important (~24 450 000)	Usage prospectif plutôt apprécié par les usagers (21% d'occurrences dans le top 3)	
Je fais valoir mes droits sociaux	▲ Introduire une demande de retraite en ligne	Public	Substantiel	Unique	Faible (~238 000)	Usages qui ne sont pas ressortis dans l'étude "voix des usagers"	
	▲ Demande de carte mobilité inclusion (CMI)	Public	Substantiel	Occasionnelle	Faible (~510 000)		
	▲ Inscription / réinscription à Pôle emploi	Public	Substantiel	Occasionnelle	Important (~6 500 000)		
	Consulter et gérer son compte CAF	Public	Substantiel	Plusieurs fois par mois	Très important (~340 200 000)	Pénible	Importante
	Faire une demande de RSA	Public	Substantiel	Occasionnelle	Faible (~479 000)		
	▲ Réaliser sa déclaration trimestrielle RSA	Public	Substantiel	Plusieurs fois par an	Très important (~6 530 000)		
	Déclaration de loyer pour l'aide au logement	Public	Substantiel	Une fois par an	Modéré (~2 500 000)		
	Avis de changement de situation pour les prestations familiales	Public	Substantiel	Occasionnelle	Important (~2 700 000)		
	Déclaration de ressources CAF (année N-1)	Public	Substantiel	Occasionnelle	Modéré (~1 900 000)		

Note 1 : Qualification de la fréquence selon 5 paliers (Plusieurs fois par mois / Plusieurs fois par an / Une fois par an / Occasionnelle / Unique).
Note 2 : Qualification du volume sur la base de quartiles des usages analysés (Très important / Important / Modéré / Faible) – source : données volumes actuels ou potentiels pour les usages émergents ; source : données publiques, analyse et estimations BCG & EY-Parthenon .
Note 3 : Qualifications de la pénibilité et du besoin de sécurité (usagers) selon 3 paliers (Peu pénible / Pénible / Très pénible et Relativement peu important / Important / Très important) .
Note 4 : niveaux de sécurité sur la base des entretiens experts sectoriels (voir annexe 1) et des données déclaratives recueillies par le programme ID NUM (services publics) + propositions BCG & EY-Parthenon lorsque le déclaratif n'était pas disponible.

Pour mémoire : liste des usages étudiés et qualifiés (3/7)

▲ *Usage symbolique*

Moment de vie	Usages qualifié	Type	Sécurité (besoin FS)	Fréquence	Volume (# recours/an)	Pénibilité (usagers)	Sécurité (besoin usagers)
Je participe à la vie citoyenne	▲ Inscription sur les listes électorales	Public	Substantiel	Occasionnelle	Modéré (~2 245 000)	Usage qui n'est pas ressorti dans l'étude "voix des usagers"	
	Voter électroniquement en France pour des élections	Public	Elevé	Occasionnelle	Très important (~6 720 000)	Peu Pénible	Importante
	Voter électroniquement (Français de l'étranger)	Public	Elevé	Occasionnelle	Faible (~133 000)		
	Obtenir une procuration de vote	Public	Elevé	Occasionnelle	Modéré (~1 050 000)	Usage prospectif plutôt apprécié par les usagers (30% d'occurrences dans le top 3)	
	Participer à une consultation publique	Public	Elevé	Occasionnelle	Faible (~100 000)	Usages qui ne sont pas ressortis dans l'étude "voix des usagers"	
	Participer à un référendum d'initiative partagée	Public	Elevé	Occasionnelle	Non qualifié		
	Déclarer son rattachement à un parti	Public	Substantiel	Occasionnelle	Faible (~400 000)		
	Recensement de la population (OMER)	Public	Substantiel	Une fois par an	Important (~4 050 000)		
Je me déplace, je voyage (1/2	Adossement de la carte de transport (Navigo et SNCF)	Privé	Substantiel	Plusieurs fois par mois	Très important (~6 114 000 000)		
	Accéder à son lieu de travail sécurisé	Privé	Elevé	Plusieurs fois par mois	Très important (~275 000 000)	Peu pénible	Relativement peu importante

Note 1 : Qualification de la fréquence selon 5 paliers (Plusieurs fois par mois / Plusieurs fois par an / Une fois par an / Occasionnelle / Unique).
Note 2 : Qualification du volume sur la base de quartiles des usages analysés (Très important / Important / Modéré / Faible) – source : données volumes actuels ou potentiels pour les usages émergents ; source : données publiques, analyse et estimations BCG & EY-Parthenon .
Note 3 : Qualifications de la pénibilité et du besoin de sécurité (usagers) selon 3 paliers (Peu pénible / Pénible / Très pénible et Relativement peu important / Important / Très important) .
Note 4 : niveaux de sécurité sur la base des entretiens experts sectoriels (voir annexe 1) et des données déclaratives recueillies par le programme ID NUM (services publics) + propositions BCG & EY-Parthenon lorsque le déclaratif n'était pas disponible.

Pour mémoire : liste des usages étudiés et qualifiés (4/7)

▲ *Usage symbolique*

Moment de vie	Usages qualifié	Type	Sécurité (besoin FS)	Fréquence	Volume (# recours/an)	Pénibilité (usagers)	Sécurité (besoin usagers)
Je me déplace, je voyage (2/2)	▲ Demande de passeport	Public	Elevé	Occasionnelle	Important (~2 765 000)	Très pénible	Très importante
	Contrôle à l'embarquement à l'aéroport	Privé	Elevé	Occasionnelle	Important (~ 4 131 000)	Très pénible	Très importante
Je profite de mon temps libre	Ouvrir un compte de jeux en ligne	Privé	Substantiel	Occasionnelle	Modéré (~1 110 000)	Pénible	Relativement peu importante
	S'authentifier auprès des sites de rencontre	Privé	Substantiel	Unique	Important (~6 000 000)	Peu pénible	Relativement peu importante
	Création de comptes auprès des plateformes P2P en ligne	Privé	Substantiel	Unique	Très important (~15 300 000)	Peu pénible	Relativement peu importante
	Prouver son âge sur internet	Privé	Substantiel	Plusieurs fois par mois	Non qualifié	Peu pénible	Importante
J'achète un produit ou je souscris à un service (1/2	▲ Souscrire à un service de télécommunication (internet, téléphone et télévision)	Privé	Substantiel	Occasionnelle	Très important (~11 600 000)	Peu pénible	Relativement peu importante
	Souscrire à un service énergétique	Privé	Substantiel	Occasionnelle	Modéré (~2 300 000)	Usage qui n'est pas ressorti dans l'étude "voix des usagers"	
	Ouvrir un compte Bancaire en ligne	Privé	Substantiel	Occasionnelle	Modéré (~2 365 000)	Pénible	Très importante
	Changer de banque / coordonnées bancaires	Privé	Substantiel	Occasionnelle	Modéré (~1 190 000)		
	Ouvrir un compte bancaire (KYC)	Privé	Elevé	Une fois par an	Très important (~11 600 000)	Usage qui n'est pas ressorti dans l'étude "voix des usagers"	

Note 1 : Qualification de la fréquence selon 5 paliers (Plusieurs fois par mois / Plusieurs fois par an / Une fois par an / Occasionnelle / Unique).
Note 2 : Qualification du volume sur la base de quartiles des usages analysés (Très important / Important / Modéré / Faible) – source : données volumes actuels ou potentiels pour les usages émergents ; source : données publiques, analyse et estimations BCG & EY-Parthenon .
Note 3 : Qualifications de la pénibilité et du besoin de sécurité (usagers) selon 3 paliers (Peu pénible / Pénible / Très pénible et Relativement peu important / Important / Très important) .
Note 4 : niveaux de sécurité sur la base des entretiens experts sectoriels (voir annexe 1) et des données déclaratives recueillies par le programme ID NUM (services publics) + propositions BCG & EY-Parthenon lorsque le déclaratif n'était pas disponible.

Pour mémoire : liste des usages étudiés et qualifiés (5/7)

▲ *Usage symbolique*

Moment de vie	Usages qualifié	Type	Sécurité (besoin FS)	Fréquence	Volume (# recours/an)	Pénibilité (usagers)	Sécurité (besoin usagers)
J'achète un produit ou je souscris à un service (2/2)	Demander un crédit en ligne	Privé	Substantiel	Occasionnelle	Important (~5 450 000)	Très pénible	Importante
	Faire un achat en ligne	Privé	Faible / Substantiel	Plusieurs fois par mois	Très important (~1 234 200 000)	Peu pénible	Relativement peu importante
	Obtenir une autorisation de détention d'arme	Public	Substantiel	Occasionnelle	Faible (~93 000)	Usage qui n'est pas ressorti dans l'étude "voix des usagers"	
Je suis impacté par un évènement	▲ Dépôt de plainte pour violences sexuelles	Public	Elevé	Occasionnelle	Faible (~19 000)	Usage prospectif très apprécié par les usagers (34% d'occurrences dans le top 3)	
	Suivi des affaires judiciaires	Public	Elevé	Occasionnelle	Faible (~655 000)		
	Suivi des affaires civiles	Public	Elevé	Occasionnelle	Modéré (~1 116 000)		
	Demande d'aide juridictionnelle	Public	Substantiel	Occasionnelle	Faible (~743 000)	Usages qui ne sont pas ressortis dans l'étude "voix des usagers"	
	Visiter un proche en prison	Public	Elevé	Plusieurs fois par mois	Modéré (~1 992 000)		
	Demander un extrait ou une copie d'actes d'Etat civil (naissance, mariage, décès, etc.)	Public	Substantiel	Occasionnelle	Modéré (~1 247 000)	Pénible	Très importante
Je m'acquitte de mes devoirs (1/3)	S'inscrire auprès du registre des Français établis hors de France	Public	Substantiel	Occasionnelle	Faible (~276 000)	Usage qui n'est pas ressorti dans l'étude "voix des usagers"	

Note 1 : Qualification de la fréquence selon 5 paliers (Plusieurs fois par mois / Plusieurs fois par an / Une fois par an / Occasionnelle / Unique).
Note 2 : Qualification du volume sur la base de quartiles des usages analysés (Très important / Important / Modéré / Faible) – source : données volumes actuels ou potentiels pour les usages émergents ; source : données publiques, analyse et estimations BCG & EY-Parthenon .
Note 3 : Qualifications de la pénibilité et du besoin de sécurité (usagers) selon 3 paliers (Peu pénible / Pénible / Très pénible et Relativement peu important / Important / Très important) .
Note 4 : niveaux de sécurité sur la base des entretiens experts sectoriels (voir annexe 1) et des données déclaratives recueillies par le programme ID NUM (services publics) + propositions BCG & EY-Parthenon lorsque le déclaratif n'était pas disponible.

Pour mémoire : liste des usages étudiés et qualifiés (6/7)

▲ *Usage symbolique*

Moment de vie	Usages qualifié	Type	Sécurité (besoin FS)	Fréquence	Volume (# recours/an)	Pénibilité (usagers)	Sécurité (besoin usagers)
Je m'acquitte de mes devoirs (2/3)	Réaliser un acte authentique à distance	Privé	Elevé	Occasionnelle	Important (~2 626 000)	Usage prospectif moins apprécié par les usagers (14% d'occurrences dans le top 3)	
	Réaliser un acte de vente à distance	Privé	Elevé	Occasionnelle	Faible (~460 000)		
	Réaliser sa déclaration d'impôt en ligne	Public	Substantiel	Une fois par an	Très important (~24 950 000)	Pénible	Très importante
	Demander un extrait de son casier judiciaire	Public	Substantiel	Occasionnelle	Faible (~836 000)	Usages qui ne sont pas ressortis dans l'étude "voix des usagers"	
	Attestations fiscales retraités régime général	Public	Substantiel	Occasionnelle	Important (~3 700 000)		
	▲ Demande de carte nationale d'identité	Public	Elevé	Occasionnelle	Important (~3 267 000)	Très pénible	Très importante
	Demande de Visa Schengen court séjour (3 mois maximum)	Public	Substantiel	Occasionnelle	Important (~2 641 000)	Usages qui ne sont pas ressortis dans l'étude "voix des usagers"	
	Consulter et suivre son dossier d'infraction routière	Public	Substantiel	Occasionnelle	Important (~2 835 000)		
	Contestation d'avis de contravention	Public	Substantiel	Une fois par an	Important (~3 508 000)		
	Autorisation de sortie du territoire (AST) d'un mineur	Public	Substantiel	Occasionnelle	Modéré (~1 537 000)		
	Déclaration de perte de CNI ou de passeport	Public	Substantiel	Occasionnelle	Faibles (~654 000)		

Note 1 : Qualification de la fréquence selon 5 paliers (Plusieurs fois par mois / Plusieurs fois par an / Une fois par an / Occasionnelle / Unique).
Note 2 : Qualification du volume sur la base de quartiles des usages analysés (Très important / Important / Modéré / Faible) – source : données volumes actuels ou potentiels pour les usages émergents ; source : données publiques, analyse et estimations BCG & EY-Parthenon .
Note 3 : Qualifications de la pénibilité et du besoin de sécurité (usagers) selon 3 paliers (Peu pénible / Pénible / Très pénible et Relativement peu important / Important / Très important) .
Note 4 : niveaux de sécurité sur la base des entretiens experts sectoriels (voir annexe 1) et des données déclaratives recueillies par le programme ID NUM (services publics) + propositions BCG & EY-Parthenon lorsque le déclaratif n'était pas disponible.

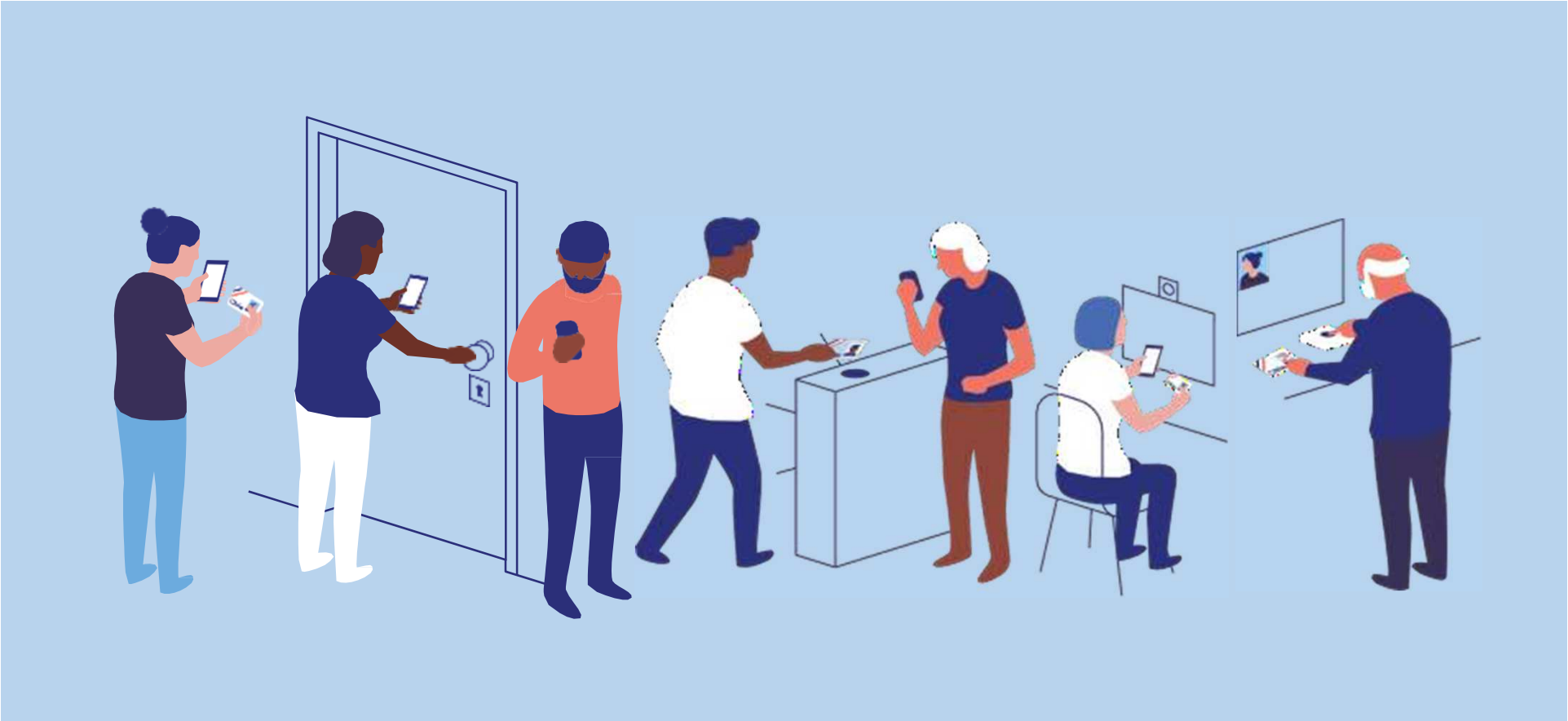
Pour mémoire : liste des usages étudiés et qualifiés (7/7)

▲ *Usage symbolique*

Moment de vie	Usages qualifié	Type	Sécurité (besoin FS)	Fréquence	Volume (# recours/an)	Pénibilité (usagers)	Sécurité (besoin usagers)
Je m'acquitte de mes devoirs (3/3)	Inscription au permis de conduire	Public	Substantiel	Occasionnelle	Modéré (~1 430 000)	Usages qui ne sont pas ressortis dans l'étude "voix des usagers"	
	Permis de conduire : demande de titre après réussite à l'examen	Public	Substantiel	Unique	Modéré (~1 191 000)		
	Demande de carte grise pour un véhicule neuf	Public	Substantiel	Unique	Modéré (~1 840 000)	Très pénible	Très importante
	Déclaration de cession d'un véhicule	Public	Substantiel	Unique	Très important (~7 630 000)		
	Demande de changement de titulaire sur la carte grise	Public	Substantiel	Unique	Très important (~10 725 000)		
	Demande de certificat de situation administrative simple	Public	Substantiel	Unique	Très important (~8 204 000)	Usages qui ne sont pas ressortis dans l'étude "voix des usagers"	
	Demander son certificat de situation administrative détaillé	Public	Substantiel	Unique	Important (~5 069 000)		
Je me forme et je travaille	Passer un entretien par visioconférence	Transverse	Substantiel	Occasionnelle	Faible (~482 000)	Usage prospectif moins apprécié par les usagers (14% d'occurrences dans le top 3)	
	Passer un examen en ligne/par visioconférence	Transverse	Substantiel	Plusieurs fois par an	Faible (~730 000)	Usage prospectif moins apprécié par les usagers (10% d'occurrences dans le top 3)	
	Démontrer sa possession d'un diplôme de l'éducation supérieure	Transverse	Substantiel	Occasionnelle	Modéré (~1 577 000)	Usages qui ne sont pas ressortis dans l'étude "voix des usagers"	
	Ouverture ou accès au compte personnel de formation (CPF)	Public	Substantiel	Occasionnelle	Modéré (~1 778 000)		

Note 1 : Qualification de la fréquence selon 5 paliers (Plusieurs fois par mois / Plusieurs fois par an / Une fois par an / Occasionnelle / Unique).
Note 2 : Qualification du volume sur la base de quartiles des usages analysés (Très important / Important / Modéré / Faible) – source : données volumes actuels ou potentiels pour les usages émergents ; source : données publiques, analyse et estimations BCG & EY-Parthenon .
Note 3 : Qualifications de la pénibilité et du besoin de sécurité (usagers) selon 3 paliers (Peu pénible / Pénible / Très pénible et Relativement peu important / Important / Très important) .
Note 4 : niveaux de sécurité sur la base des entretiens experts sectoriels (voir annexe 1) et des données déclaratives recueillies par le programme ID NUM (services publics) + propositions BCG & EY-Parthenon lorsque le déclaratif n'était pas disponible.

Sommaire



Usages de l’Identité numérique

Illustrations des parcours souhaitables et des scenarii d’usages désirables

Vraiment Vraiment
Design d’intérêtgénéral

D'OÙ VIENT CE DOCUMENT ? QUELLE EST SA VOCATION ?

Ce document, réalisé par la DITP pour le compte du programme « Identité Numérique », a pour ambition de présenter les usages potentiels de la future Carte Nationale d'Identité électronique et d'une solution d'identité numérique associée.

Il traduit, dans un format pédagogique et facile d'appropriation, les attentes des usagers auxquelles il serait possible de répondre ainsi que les préoccupations et freins à lever pour favoriser l'adoption large de cette identité numérique. Il incarne les usages et fonctionnalités potentiels, désirables, supportés ou rendus possibles. De ce fait, les scénarios d'usages ainsi que les principes mentionnés n'ont pas nécessairement vocation à se réaliser mais tracent des perspectives « idéales » et les conditions de succès.

Les éléments qui ont servi de base à l'élaboration de ces illustrations ont été recueillis et co-construits avec des citoyens / usagers, entre mars et mai 2019[1].

QUEL EST SON CONTENU ?

Après avoir présenté les concepts et principes de la CNIe et de l'Identité Numérique, le document illustre les scénarios de gestion de l'Identité Numérique ainsi que les utilisations possibles de l'Identité Numérique au quotidien ou dans des moments de vie importants.

Il est constitué de plusieurs parties :

- Présentation des promesses d'usages et fonctionnalités
- Présentation des modalités de fonctionnement
- Illustrations des scénarios d'usages souhaitables / désirables
- Annexe

(1) 4 focus group d'une 10aine de participants chacun, enquête représentative réalisée auprès de 1250 personnes (par voie électronique et téléphonique), atelier de co-conception associant agents publics et usagers.

Promesses d'usages et fonctionnalités

Une identité numérique adossée à la future CNIe, qui simplifie la viequotidiennedes citoyens / usagers, **fabrique de la confiance dans les usages en ligne et favorise le développement de nouveaux services en ligne.**

PROMESSES D'USAGE

- Solution d'Identification universelle et hautement sécurisée, garantie par l'Etat
- Meilleure protection contre les risques d'usurpation d'identité
- Simplification des accès aux services en ligne publics et privés
- Accès à de nouveaux services en ligne rendus possibles par une identification certaine del'usager
- Certification de l'identité des interlocuteursnumériques
- Maitrise de son identité numérique par le citoyen / usager (traçabilité, personnalisation, liberté de choix,…)

FONCTIONNALITÉS PRINCIPALES

	Scénario(s)
Identification universelle aux services en ligne publics ou privés	5,6,7 et 8
Identification hautement sécurisée pour gérer des données sensibles ou faire des actes engageants en ligne (ex: virements élevés, signature de documents, vote en ligne)	5,6 et 8

FONCTIONNALITÉS ADDITIONNELLES POSSIBLES

	Scénario(s)
Gestion de mandats et procurations	6 et 8
Archivage de données et documents personnels	6 et 7
Transmission de données ou documents à des acteurs tiers, de manière sécurisée	6 et 8
Accès à des espaces restreints (aéroports, frontières) ou àdes lieux sécurisés (lieux de travail, université, Ministères, etc.)	6 et 8
Signature authentifiée de documents (bail de location, procuration, acte de vente etc.)	6
Certification de l'identité des participants à des vidéo-conférences	7
Transmission partielle d'attributs d'identité (âge, statut d'étudiant ou de chômeur, …)	7 et 8

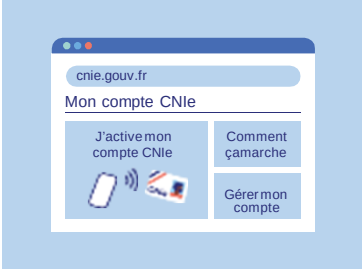
Principes de fonctionnement

DEUX SUPPORTS :

Une carte

La carte national d'identité électronique (ici appelée CNIe) permet de s'identifier de deux manières :

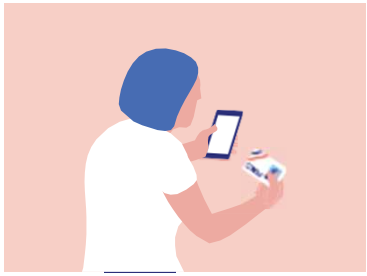
- de manière traditionnelle devant un agent public ou un agent de sécurité via un contrôle visuel de la photo et des données d'identité
- par lecture des données contenues dans la puce, en sans contact par exemple



Une solution numérique

La solution numérique (ici appelée « compte CNIe »), supporte l'identité numérique associée à la CNIe. Elle permet de s'identifier en ligne via un identifiant et mot de passe, a minima, et de gérer son identité numérique en ligne et les fonctionnalités associées.

DEUX NIVEAUX DE SÉCURITÉ :



Niveau substantiel :

L'identification à un niveau de sécurité substantiel permet de vérifier l'identité d'un usager.
Elle peut se faire de plusieurs manières distincte :

- Demande d'un code PIN et vérification envoyéesur smartphone
- Présentation d'une pièced'identité en ligne
- Comparaison avec un selfie (on le met celui là ou pas ?)

Niveau élevé :

L'identification à un niveau de sécurité élevé permet de s'assurer de l'identité d'un usager de manière certaine.
Elle passe par plusieurs étapes (facteurs de réassurance) :

- **Lecture sans contact** de la pièce d'identité physique (**CNIe**) puis **renseignement d'un identifiant avec mot de passe**, ou **contrôle par reconnaissance biométrique**
- **Solution sur smartphone utilisant un matériel authentifié puis renseignement d'un identifiant avec mot de passe**

Scénarios d'usages

Vue d'ensemble

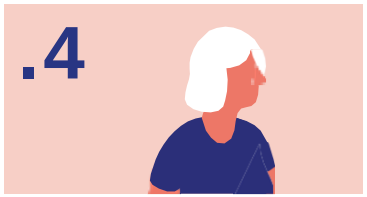
GÉRER SON IDENTITÉNUMÉRIQUE

Illustration des parcours « idéaux » de gestion de l'Identité Numérique, souhaitables, pour en favoriser l'adoption et l'usage (inclusion, réassurance, assistance et traitement des incidents).

Première délivrance de la CNIe, en autonomie

Première délivrance inclusive de la CNIe, en assisté

Alerte de sécurité



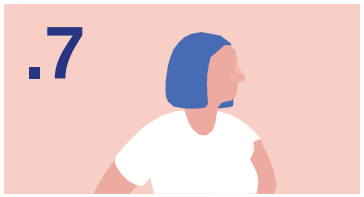
Perte de la carte CNIe

UTILISER SON IDENTITÉ NUMÉRIQUE

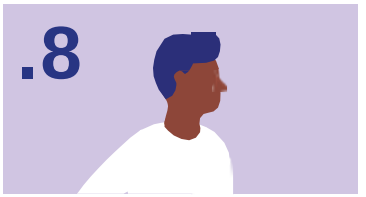
Illustration des utilisations potentielles, désirables, de l'Identité Numérique au quotidien ou dans des moments de vie importants (usages facilités, nouveaux services et fonctionnalités) .

Connexion universelle aux services en ligne

Achat d'appartement



Reconversion professionnelle



Séjour Erasmus

1. Première délivrance de la CNIe et activation de l'identité numérique

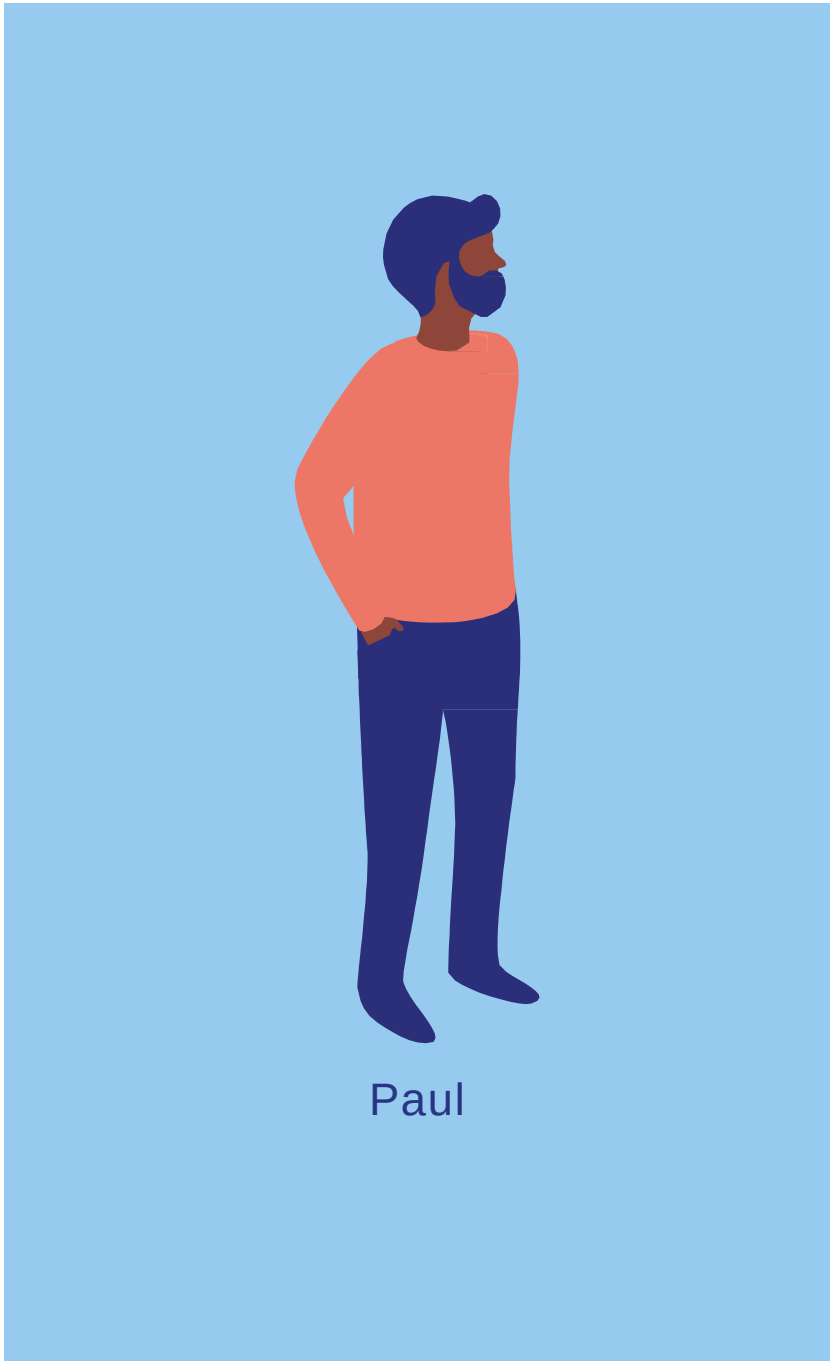
(e n toute autonomie)

Attentes des usagers (facteurs d'adoption)

- Une prise en main de la CNIe et de l'identité numérique facile et intuitive pouvant être faite en totale autonomie, via son smartphone.
- La liberté de choisir et de personnaliser : les modalités de délivrance, d'interaction avec l'administration, d'assistance et d'usage de l'identité numérique

Craintes des usagers (freins potentiel à l'adoption)

- Un parcours de renouvellement / délivrance de la carte nationale d'identité rendu plus complexe avec le nouveau format à puce et l'arrivée de la solution d'identité numérique.
- Une promotion des usages de la CNIe et de l'identité numérique excessive etintrusive



Paul, 34 ans

Paul, 34 ans, a vu un panneau devant sa mairie qui l'informe qu'il peut voter depuis l'étranger grâce à la Carte Nationale d'Identité électronique (CNIe) et l'identité numérique associée.

Demande derendez-vous

Il anticipe le fait qu'il sera à l'étranger lors du prochain référendum et fait une demande de CNIe afin de pouvoir voter en ligne.
Il se rend sur le site cnie.gouv.fr pour constituer son dossier en ligne et prendre rendez-vous dans le lieu de son choix (mairie ou en maison France service, par exemple).

Confirmation du rendez-vous

Quelques jours avantla date, un sms informe Paul que son dossier est complet etlui rappelle l'horaire et le lieu du rendez-vous.

Préparation de la CNIe

Lors du rendez-vous, l'agent invite Paul à :

- -authentifier son identité et prendre ses empreintes
- -faire la demande d'un lecteur de CNIe s'il le souhaite (ce lecteur permet de se connecter plus facilement, notamment s'il ne possède pas de smartphone)
- -choisir l'endroit où il souhaite récupérer sa CNIe
- -donner son accord pour disposer de la « fonction électronique» de sa carte.
- -consulter les rubriques du site cnie.gouv.fr où il trouvera davantage d'informations.

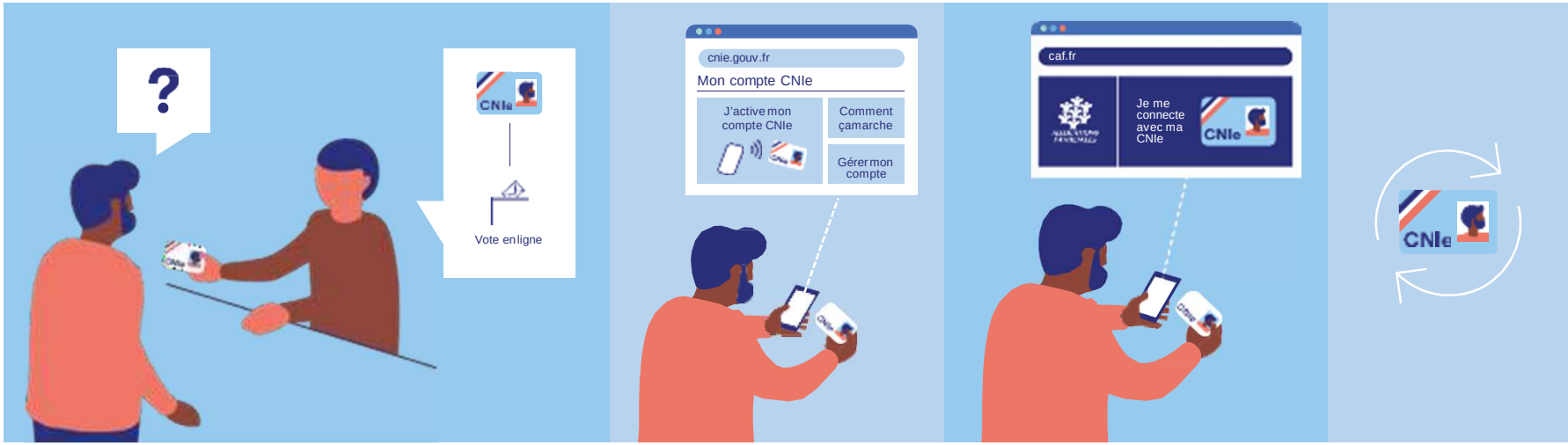
Les + pour l'usager

Paul peut demander la création de sa CNIe par anticipation de l'expiration de sa CNI afin de profiter de la fonctionnalité « Vote en ligne » uniquement permise par une identité numérique sécurisée.

Paul a le choix : du mode de prise de rdv, du lieu de rdv, des modalités de constitution de son dossier, de la date du rdv, du type de rdv (rdv simple ou rdv+, s'il souhaite un accompagnement)

Paul est informé du suivi de son dossier et son rendez-vous lui est rappelé. Il peut ainsi anticiper ses démarches et modifier son rendez-vous si nécessaire.

Paul peut s'informer sur le fonctionnement de sa future CNIe et les usages possibles, en toute autonomie grâce aux informations pédagogiques accessibles depuis le site cnie,gouv.fr (FAQ, tutoriels, chatbot, ...)et déclinées pour les différents publics (avertis, éloignés du numériques, en situation de handicap, ...)



Délivrance de la CNIe

Paul reçoit un sms l'informant que sa CNIe est prête et qu'il peut la récupérer dès qu'il le souhaite à l'endroit choisi.

Il passe donc à la mairie récupérer sa carte CNIe. L'agent lui présente de manière succincte les modalités d'utilisation de la CNIe dans le cadre du référendum. Il lui remet toute la documentation nécessaire.

Paul confirme son accord pour disposer de la « fonction électronique » de sa carte.

Activation de l'identité numérique

De retour chez lui, grâce au code qu'il a reçu par sms, il active son Identité Numérique via l'application « mon compte CNIe».
Il paramètre son compte : il personnalise les questions de sécurité, et autorise les notifications par SMS.

Accès universel aux services

Paul a maintenant accès à tous les services publics en ligne avec un même couple identifiant/mot de passe. Il peut aussi accéder à de nouveaux services nécessitant une identification élevée.

Renouvellement

Lors du prochain renouvellement de sa CNIe, Paul n'aura pas à passer par toutes ses étapes et aura accès à un parcours simplifié

Paul peut récupérer sa CNIe en quelques minutes.
S'il souhaite des informations complémentaires, il pourra consulter à tout moment les informations disponibles en ligne et solliciter une assistance à distance.

Paul dispose d'un compte pour gérer son identité numérique et personnaliser ses préférences.
Il peut consulter un catalogue de démarches personnalisées, une FAQ en cas de questions, etc.

Lors du prochain renouvellement de sa CNIe, Paul n'aura pas à passer par toutes ses étapes et aura accès à un parcours simplifié

2. Première délivrance de la CNIe et activation de l'identité numérique

(avec accompagnement)

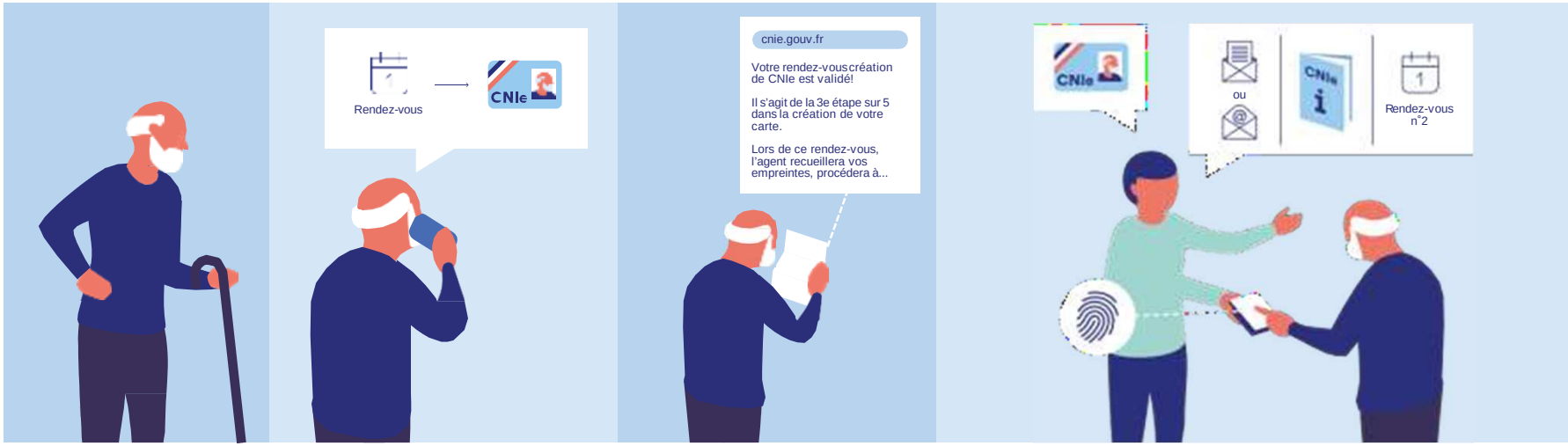
Attentes des usagers (facteurs d'adoption)

- Une prise en main de la CNIe et de l'identité numérique inclusive, pouvant être faite avec l'assistance d'un agent public et via un ordinateur.
- Un accompagnement renforcé, à la carte, pour l'usager et ses aidants éventuels
- La liberté de choisir et de personnaliser : les modalités de délivrance, d'interaction avec l'administration d'assistance et d'usage de l'identité numérique

Craintes des usagers (freins potentiel à l'adoption)

- Un parcours de renouvellement / délivrance de la carte nationale d'identité rendu plus complexe avec le nouveau format à puce et l'arrivée de la solution d'identité numérique et générant de nouvelles formes d'exclusion
- Une promotion des usages de la CNIe et de l'identité numérique peu adaptée aux publics les plus éloignés du numérique

Anselme



Anselme, 80 ans

Anselme, 80 ans, est retraité dans une commune rurale du Gers. Il n'a pas de smartphone mais possède un ordinateur et utilise parfois internet.

Il doit renouveler sa Carte Nationale d'Identité (CNI) qui arrive bientôt à expiration.

Demande de rendez-vous

Il prend rendez-vous par téléphone et est informé du nouveau format de la carte d'identité : la CNIe.
Ayant des difficultés à se déplacer, il demande à ce qu'un agent public se rende chez lui et il accepte et choisit sa date de rdv.

Confirmation du rendez-vous

Anselme reçoit un mail lui confirmant le rendez-vous et les pièces à préparer pour constituer son dossier.
Ce mail l'informe du niveau d'avancement dans le processus de la demande. Il est informé des nouvelles possibilités offertes par la CNIe et apprend qu'il a la possibilité de participer à une réunion d'information collective de la CNIe, s'il le souhaite.

Préparation de la CNIe

Le jour du rendez-vous, un agent public se déplace à son domicile. Lors du rendez-vous, l'agent invite Anselme à :

- -authentifier son identité et prendre ses empreintes.
- -faire la demande d'un lecteur de CNIe qui permet d'utiliser la CNIe depuis un ordinateur
- -lui indiquer les rubriques du site cnie.gouv.fr où il trouvera davantage d'informations
- -donner son accord pour disposer de la « fonction électronique » de sa carte.
- -choisir l'endroit où il souhaite récupérer sa CNIe et la possibilité qui lui est offerte qu'un agent public se déplacera à nouveau chez lui, pour lui remettre sa CNIe et l'aider à activer son identité numérique
- -participer à une réunion d'information collective de la CNIe, avec un aidant, s'il le souhaite.

Les + pour l'usager

Anselme a le choix : du mode de prise de rdv, du lieu de rdv, des modalités de constitution de son dossier, de la date du rdv, du type de rdv (rdv simple ou rdv+, s'il souhaite un accompagnement).
Anselme n'est pas obligé de se déplacer.

Anselme est informé du suivi de son dossier et son rdv lui est rappelé. Il peut ainsi anticiper ses démarches et modifier son rdv si nécessaire.

Anselme peut s'informer sur le fonctionnement de sa future CNIe et les usages possibles, grâce aux informations pédagogiques accessibles depuis le site cnie,gouv.fr (FAQ, tutoriels, chatbot, ...)et déclinées pour les différents publics (avertis, éloignés du numériques, en situation de handicap, ...). Il peut également bénéficier d'un accompagnement personnalisé, à domicile et pourra compléter ses connaissances lors de séance collectives.

Délivrance de la CNIe et activation de l'identité numérique

Lorsque sa CNIe est prête, reçoit un mail l'invitant à prendre rdv.
A la date convenue, un agent public se déplace chez Anselme afin de lui remettre sa carte CNIe et sonlecteur.
Anselme confirme son accord pour activer la fonction «électronique» de sa carte.

Cette visite est également l'occasion pour Anselme d'être aidé pour activer son identité numérique et paramétrer son compte CNIe (personnalisation des questions de sécurité, autorisation des notifications par SMS ou mail, ...).
L'agent public répond à toutes les questions d'Anselme sur le fonctionnement de sa CNIe et de son identité numérique.

Accès universel aux services

Dans les semaines qui suivent, Anselme et son aidant participent à un atelier collectif « ma nouvelle CNIe et ses usages ».
Anselme peut désormais, seul ou avec son aidant, utiliser son compte CNIe via son PC, son lecteur et ses codes et identifiants pour simplifier ses démarches et accéder à de nouveaux services..

Anselme pourra par exemple donner à distancesa procuration à son petit-fils pour allervoter.

Anselme n'est pas obligé de se déplacer

Il est accompagné par un agent qui dispose du temps nécessaire pour l'aider à prendre un main sa CNIe et son identité numérique.
Anselme ne se sent pas exclu des avancées technologiques proposées par l'administration

Anselme dispose d'un compte pour gérer son identité numérique et personnaliser ses préférences.
il peut consulter un catalogue de démarches personnalisées, une FAQ en cas de questions, etc.

Il continue à pouvoir bénéficier d'un accompagnement.

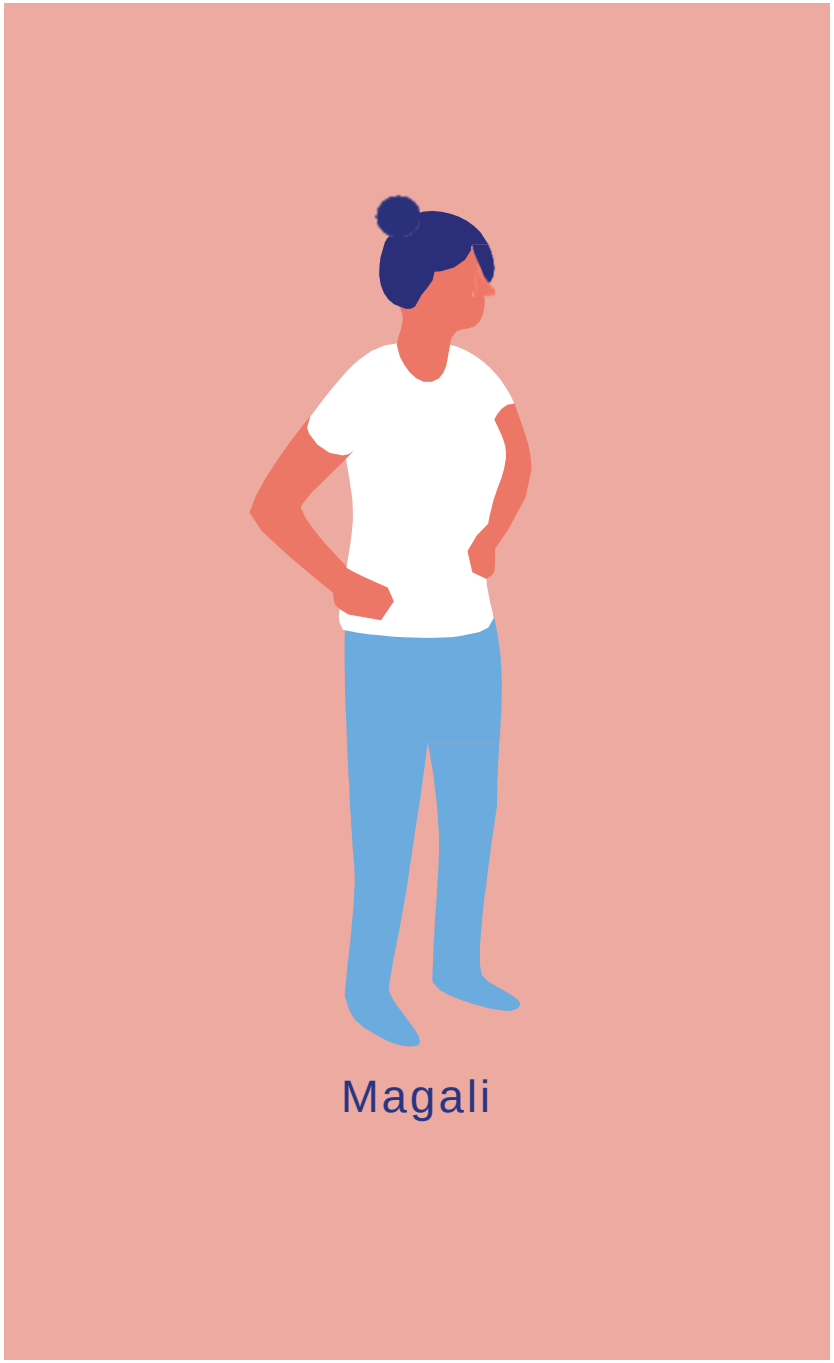
3. Alerte de sécurité

Attentes des usagers (facteurs d'adoption)

- Des alertes et des recommandations en cas de problèmes identifiés avec l'assurance que l'emetteur est bien l'administration en charge
- Le maintien d'un accès au compte et à certains usages de son identité numérique pendant le traitement de l'alerte de sécurité
- La liberté de choisir et de personnaliser : les modalités de sécurisation, de limitation de l'usage, …
- L'utilisation de procédures de référence, rassurantes, auxquelles on est déjà familiers (ex : opposition CB, alerte utilisation compte Google, …)

Craintes des usagers (freins potentiel à l'adoption)

- Des incidences trop fortes en cas de problème de sécurité (perte de tous les accès, risque de divulgation des données personnelles, …)
- Une assistance en cas de problème peu efficace et réactive de la part de l'administration (délai de réponse, durée de blocage, …)



Magali, 42 ans

Magali, 42 ans, est libraire àAngers.

Elle utilise régulièrement son identité numérique pour accéder de manière simple et sécurisée à de nombreux services en ligne, via son smartphone

Réception d'une alerte de sécurité

Magali reçoit la notification qu'une tentative de connexion infructueuse a eu lieu avec son identifiant depuis un nouvel appareil. Elle est invitée à se connecter à son compte CNIe pour gérer vérifier cette alerte et prendre les mesures nécessaires.

Gestion de l'alerte de sécurité

Magali peut voir que la tentative de connexion avait eu lieu depuis l'étranger.

Elle confirme la tentative d'usurpation d'identité et indique être toujours en possession desa CNIe

Par mesure de précaution, elle demande à modifier son code et ses questions desécurité.

Les + pour l'usager

Magali est alertée dès qu'une anomalie est constatée, par le mode de contact qu'elle a choisi (sms, mail, ...)

Magali est à l'initiative du renouvellement de son code et questions de sécurité. Elle peut choisir de ne pas les renouveler si elle estime qu'il ne s'agit pas d'une tentative d'usurpation.

Phase transitoire

Son identité numérique reste utilisable sur des fonctions restreintes avec un niveau d'identification hautement sécurisé.

Modification du code d'accès

Magali choisit un moment de la semaine pour confirmer la modification de son code d'accès et questions de sécurité grâce au code qu'elle a reçu par sms. Par sécurité, elle doit procéder à la lecture de sa CNIe. Elle retrouve ainsi l'usage de l'ensemble des fonctionnalités de son compte CNIe et redescend à un niveau de sécurité normal.

Magali peut de nouveau accéder normalement à tous les sites qu'elle a l'habitude d'utiliser avec son identité numérique, en utilisant son nouveau code.

La demande de renouvellement du code ne bloque pas l'utilisation de l'identité numérique et permet de conserver l'usage des fonctions restreintes.

Le niveau d'identification hautement sécurisé déclenché suite à l'alerte permet à Magali de choisir le meilleur moment pour modifier son code.

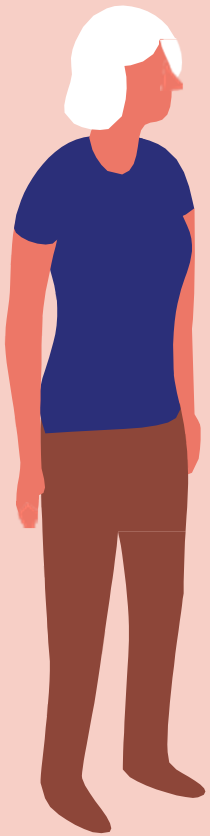
4. Perte de la CNIe

Attentes des usagers (facteurs d'adoption)

- Le maintien d'un accès au compte et à certains usages de son identité numérique en attendant le renouvellement de sa CNIe
- La liberté de choisir et de personnaliser : les modalités de sécurisation, de limitation de l'usage, …
- L'utilisation de procédures de référence, rassurantes, auxquelles on est déjà familiers (ex : opposition CB, alerte utilisation compte Google, …)
- Un parcours de renouvellement « d'urgence » de sa CNIe facile et rapide (déclenchement automatique, délais racourcis, …)

Craintes des usagers (freins potentiel à l'adoption)

- Des incidences trop fortes en cas de problème de sécurité (perte de tous les accès, risque de divulgation des données personnelles, …)
- Une assistance en cas de problème peu efficace et réactive de la part de l'administration (délai de réponse, durée de blocage, mise à disposition d'une nouvelle CNIe …)



Anne

ANne, 29 ans

Anne, 29 ans, est professeure des écoles à Paris.

Perte de la carte CNIe

Elle réalise qu'elle a perdu sa carte CNIe.

Déclaration de perte

Elle se connecte à son compte et déclare la perte de sa carte.
Elle est informée qu'une demande de renouvellement de sa carte va être déclenchée et est invitée à indiquer le lieu où elle souhaite la récupérer.

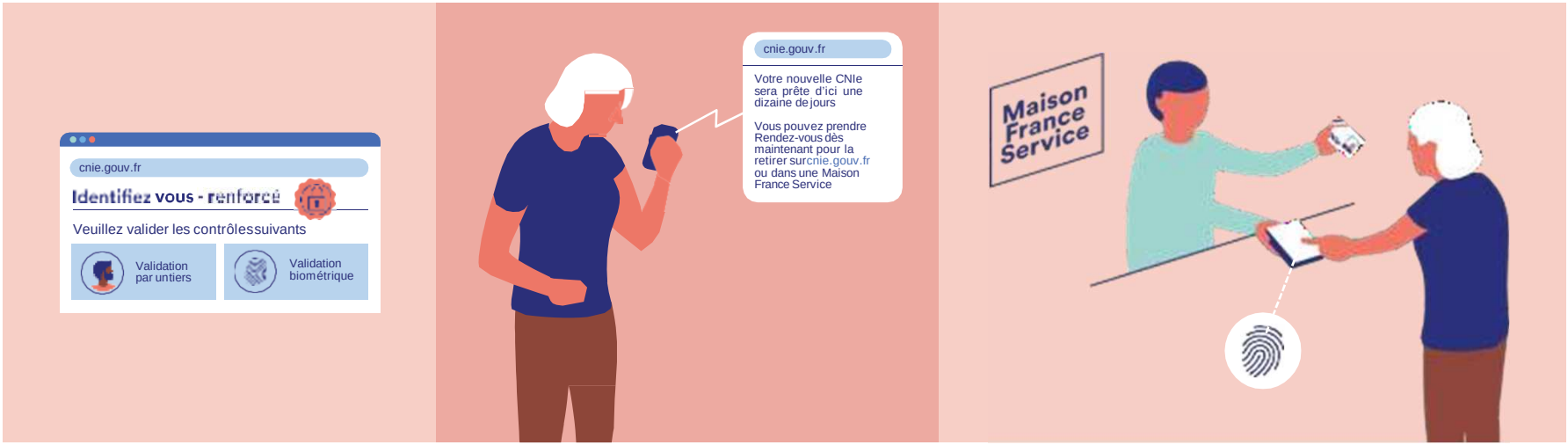
Opposition

Anne est invitée à faire opposition à son identité numérique si elle l'estime nécessaire.
Ne sachant pas où elle a pu perdre sa carte, Anne choisit de faire opposition.

Les + pour l'usager

Anne peut déclarer la perte de sa CNIe depuis son compte CNIe. Le processus de renouvellement de sa carte est totalement automatisée.

Anne est à l'initiative de l'opposition.
Elle peut décider de ne pas faire opposition si elle estime que cela n'est pas nécessaire.



Phase transitoire

Son identité numérique reste utilisable sur des fonctions restreintes avec un niveau d'identification hautement sécurisé.

Notification de la disponibilité de sa carte CNIe

Anne reçoit une notification pour lui indiquer que sa nouvelle carte CNIe est disponible.

Délivrance de la nouvelle carte CNIe

Anne se rend à en maison France service pour récupérer sa nouvelle carte et les éléments de connexion. Elle atteste de son identité en vérifiant ses empreintes au moment du retrait de la carte. De retour chez elle, Magali met à jour son compte CNIe, grâce au sms qu'elle a reçu.

L'opposition ne bloque pas l'utilisation de l'identité numérique et permet de conserver l'usage des fonctions restreintes.

Le renouvellement de la CNIe est automatisée et, sauf exception, ne nécessite pas de rdv pour préparer son dossier.

5. Connexion universelle

Fonctionnalités mobilisées

- Solution d'Identification universelle et hautement sécurisée, garantie par l'Etat
- Meilleure protectioncontre les risques d'usurpation d'identité
- Simplification des accès aux services en ligne publics et privés
- Accès à de nouveaux services en ligne rendus possibles par une identification certaine de l'usager
- Certification de l'identitédes interlocuteurs numériques

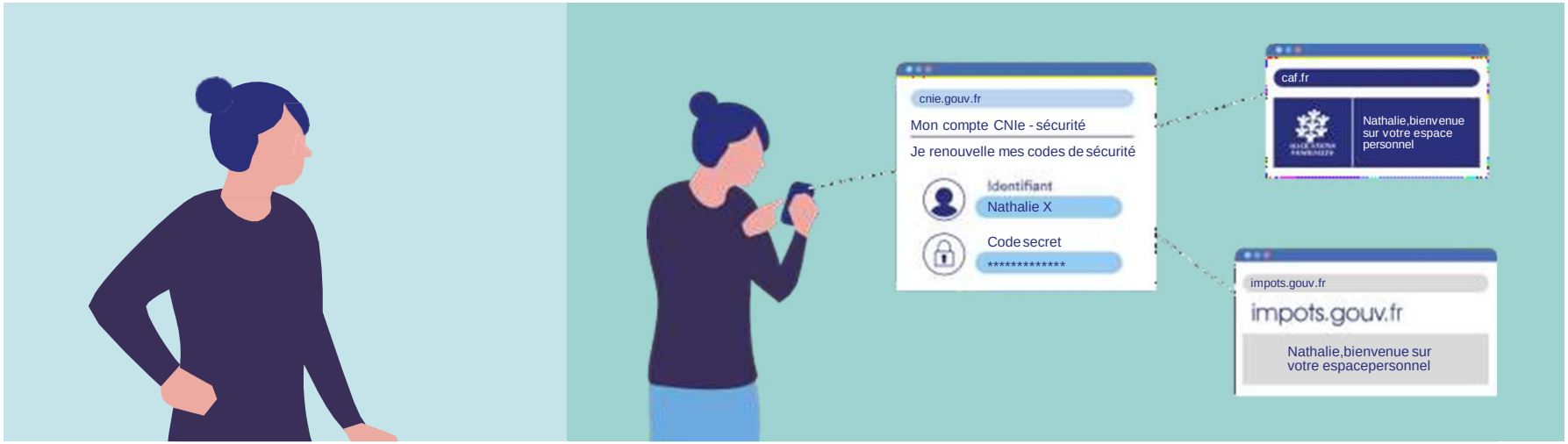
Attentes des usagers

- **Un Identifiant simple**, facile à mémoriser et incarnant vraiment son identité
- **Un couple identifiant/mot de passe universel**, vecteur de simplification administrative
- **De nouveaux services en ligne** / à distance hautement sécurisés (vote en ligne, signature d'un baillocatif)

Bénéfices des fournisseurs de services

- **La possibilité de dématérialiser plus de démarches ;** notamment, celles nécessitant actuellement un acte en accueil physique
- **Une opportunité de dialogue facilité entre administrations**, notamment pour la mise en place de mesures de simplification du type « dites le nous une fois ».

Nathalie



Nathalie, 53 ans

Nathalie exerce une profession qui l'amène à souventse déplacer.

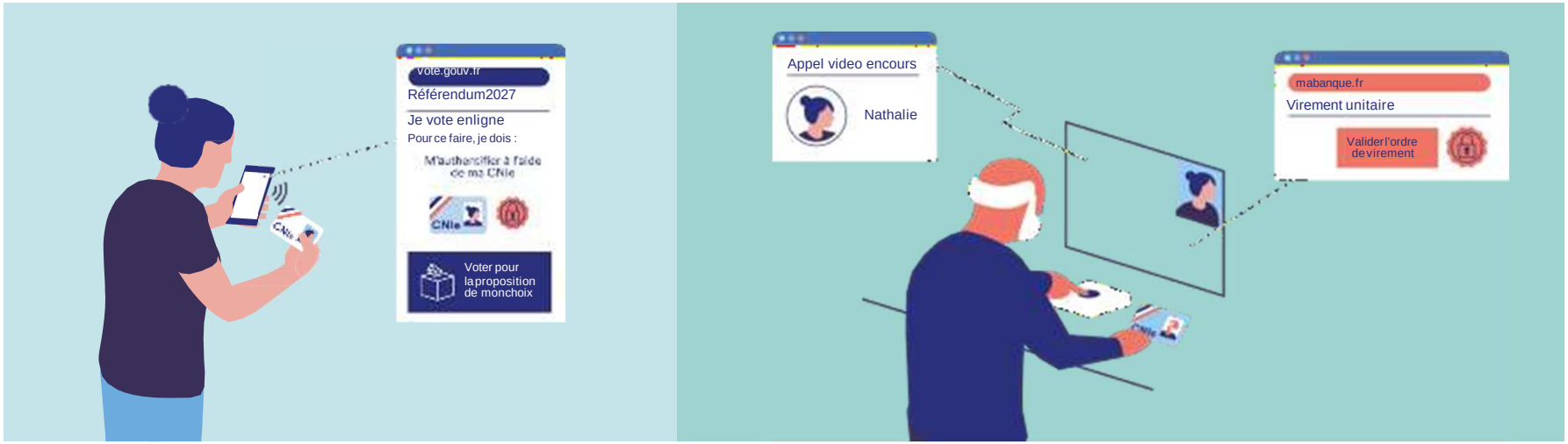
Elle souhaite pouvoir effectuer ses démarches en ligne de manière simple et sécurisée, partout où ellese trouve.

Connexion à tous les services avec un même identifiant et mot de passe

Nathalie utilise son identité numérique (identifiant et mot de passe) pour accéder à tous ses servicespublics : suivre l'évolution de ses allocations familiales, déclarer ses impôtsou demander une autorisation de stationnement auprès de sa mairie, etc.

Les + pour l'usager

L'identité numérique permet de se connecter à différents services sur son téléphone au moyen de son identifiant CNIe (simple et mémorisable) et de son mot de passe.
L'identité numérique, certifiée par l'Etat est universelle, elle permet de n'avoir qu'un seul identifiant et un seul mot de passe pour accéder , en toute sécurité à tous les services publics numériques et même plus.



Accès à des nouveaux services en ligne hautement sécurisés

Nathalie participe à un référendum en ligne en utilisant son identité numérique (identifiant et mot de passe), puis elle confirme son identité par lecture de la puce de sa carte via sonsmartphone.

Accès inclusif pour les personnes éloignées du numérique

Nathalie aide son père Charles à réaliser un virement élevé sur le site de sa banque. Pour cela elle lui montre comment se connecter à son compte bancaire depuis son ordinateur au moyen de son lecteur de carte.

Charles utilise son identifiant et mot de passe CNIe, puis confirme son identité par lecture de la puce de sa carte via le lecteur.

La CNIe permet de profiter de nouveaux usages numériques en prouvant de manière certaine son identité pour des démarches en ligne officielles ou à forte sensibilité, sans avoir à se déplacer. Ex : actes notariés, vote en ligne, renouvellement ses papiers etc

L'identité numérique permet d'accéder à des services privés, même très sécurisés, si ceux-ci ont fait le choix de proposer ce mode de connexion et ce, sans plus avoir à se déplacer.

Le lecteur de carte permet de bénéficier des usages et fonctionnalités permis par l'identitié numérique même si l'on n'est pas équipé d'un smartphone, tout en conservant un fort niveau de sécurité, même en cas de médiation.

6. Achat d'appartement

Fonctionnalités mobilisées

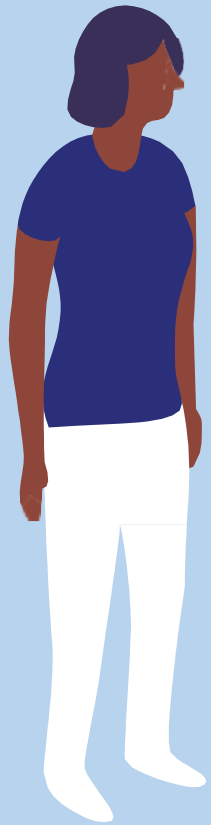
- Solution d'Identification universelle et hautement sécurisée, garantie par l'Etat
- Meilleure protection contre les risques d'usurpation d'identité
- Simplification des accès aux services en ligne publics et privés
- Accès à de nouveaux services en ligne rendus possibles par une identification certaine de l'usager
- Certification de l'identité des interlocuteurs numériques

Attentes des usagers

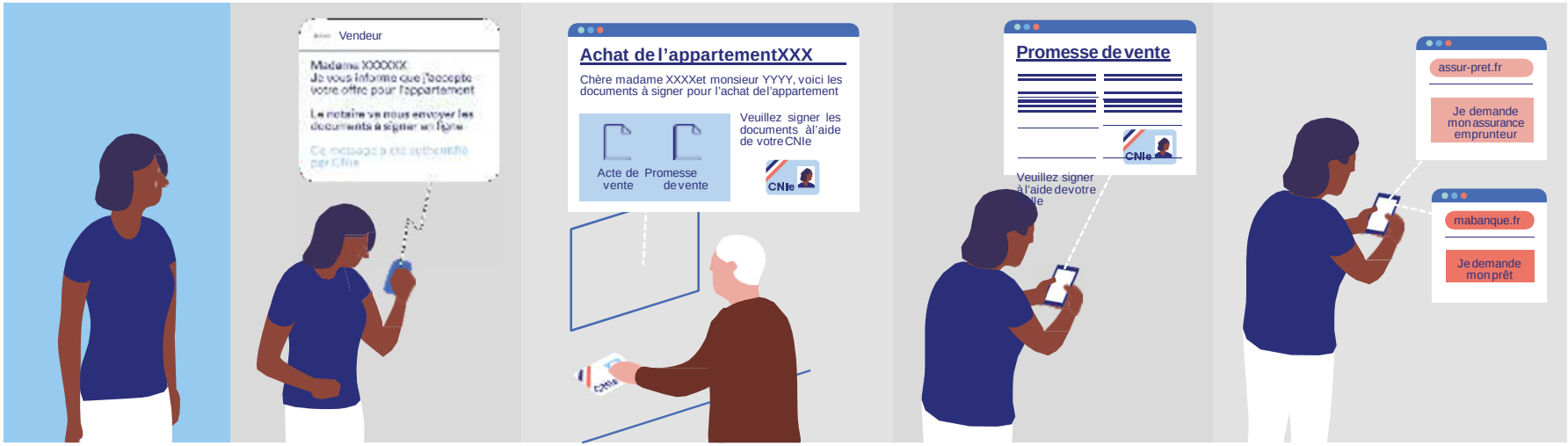
- **La simplification** des démarches administratives (ex : effectuer des démarches à deux, éviter des déplacements importants, limiter le nombre d'étapes ou d'envoi de documents dans les démarches en ligne)
- **De nouveaux services en ligne** / à distance hautement sécurisés (ex : signature d'actes notariés, virement élevé)
- **Une confiance renforcée dans les transactions en ligne** (ex : garantie de l'identité de l'interlocuteur, maitrise et sécurité dans la transmission de données personnelles, limitation des risques d'usurpation)

Bénéfices des fournisseurs de services

- **La possibilité de dématérialiser plus de démarches** ; notamment, celles nécessitant actuellement un acte en accueil physique
- **La réduction du risque sur des activités sensibles ou règlementées**, en utilisant un service d'identification hautement sécurisé, garanti par l'état
- **Une meilleure régulation des activités professionnelles en ligne** avec la possibilité d'attester de manière certaine de son statut professionnel



Jamila



Jamila, 32 ans

Jamila, 32 ans, vit à Paris et a déposéune offre pour acheter un appartement à Aix-en-Provence.

Acceptation de l'offre

Jamila est informée que son offre vient d'être acceptée par le vendeur. Sur Le document qu'elle reçoit l'identité du vendeur et la sienne sont authentifiées par leur CNIe.

Envoi des documents par le notaire

Via son espace professionnel en ligne, le notaire transmet à Jamila et au vendeur les documents à signer . Son identité professionnelle est attestée par CNIe et permet de valider l'authenticité des documents transmis aux deux parties.

Signature de la promesse de vente

Jamila choisit d'un commun accord avec son compagnon et le vendeur designer électroniquement sesdocuments notariaux (promesse de vente, projet de contrat, etc.)

Demande de prêt bancaire/assurance en ligne

Jamila effectue une demande de prêt et d'assurance à distance en son nom et en celui de soncompagnon.

Les + pour l'usager

L'usager est rassuré quant à l'identité des interlocuteurs avec lesquels il interagit à distance, lors d'opérations présentant un risque (financier, usurpation identité, divulgation de données personnelles sensibles)

L'identité numérique peut permettre de certifier l'identité professionnelle.

L'identité numérique permet de limiter les déplacements, y compris pour des actes officiels.

L'usager a toujours le choix : numérique ou rencontre physique.

Les démarches sont simplifiée via grâce à la transmission de données maitrisée et sécurisée.

L'usager peut utiliser son identité numérique auprès de fournisseurs de services privés. Il n'a plus à retenir qu'un seul couple « identifiant / mot de passe ».

Transmission de données par Jamila

A l'aide de son compte sa CNIe elle transmet ses données et les justificatifs requises à la constitution du dossier.
Elle active également une demande de transmission auprès de son compagnon.

Transmission de données par son compagnon

Son compagnon reçoit une notification et valide à son tour la demande de transmission des données nécessaires à la constitution du dossier.

Signature de l'acte de vente

La demande de prêt ayant été acceptée, Jamila et le vendeur conviennent de signer l'acte de vente à distance.
Le notaire transmet les documents via une étude notariale virtuelle, Jamila et le vendeur signent l'acte de vente à distance avec une procédure d'identification hautement sécurisée (identifiant + mot de passe + lecteur de la puce de la CNIe via smartphone ou lecteur).

Versement du solde du prix d'achat

Sur le site de sa banque, Jamila verse le solde du prix d'achat en s'authentifiant avec sa CNIe.

Grâce aux différentes fonctionnalités du compte CNIe (gestion des données d'identité, coffre-fort électronique), Jamila peut transmettre des données et documents personnels de manière ciblée et sécurisée.

La solution d'identité numérique adossée à la CNIe permet de réaliser à distance des actes règlementés qui nécessitaient une présence physique jusqu'à présent.

Grâce à l'identification hautement sécurisée, il est possible de réaliser des versements élevés, en ligne, simplement, sans avoir à se déplacer ou à suivre une démarche complexe.

7. Reconversion professionnelle

Fonctionnalités mobilisées

- Solution d'Identification universelle et hautement sécurisée, garantie par l'Etat
- Meilleure protection contre les risques d'usurpation d'identité
- Simplification des accès aux services en ligne publics et privés
- Accès à de nouveaux services en ligne rendus possibles par une identification certaine de l'usager
- Certification de l'identité des interlocuteurs numériques

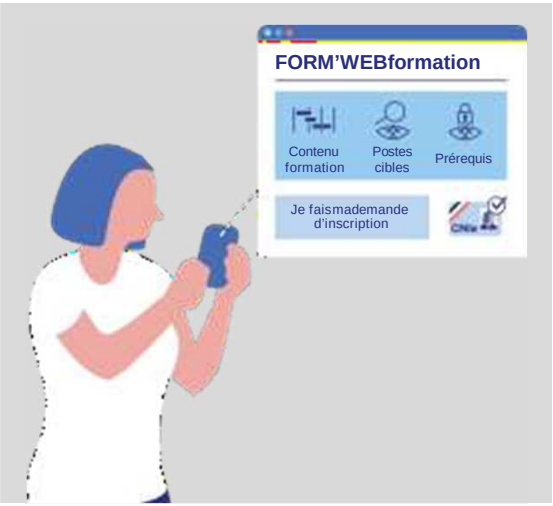
Attentes des usagers

- **La Simplification des démarches administratives** (ex limiter le nombre d'étapes ou d'envoi de documents dans les démarches en ligne)
- **De Nouveaux services en ligne** / à distance hautement sécurisés (ex : examen video en ligne)
- La possibilité d'**attester de ses droits sans être stigmatisé** (ex : justification du statut de chomeur)
- **Une gestion personnalisée de son identité numérique** (ex : ajout de compétence certifiée suite à sa formation, archivage de son diplôme dans un coffre-fort numérique intégré à la solution)

Bénéfices des fournisseurs de services

- **Le renforcement de la relation de confiance entre partenaires :** (ex : entre Pôle emploi et les prestataires de formation, meilleure lutte contre la fraude via le pointage automatisé).
- **La possibilité de proposer de nouveaux services en ligne innovant** à ses usagers / clients (ex : video-conférence avec identité certifiée)

Sonia



Sonia, 38 ans

Après un licenciement, elle décide de sereconvertir.

Inscription à Pôle emploi

Sonia s'inscrit à Pôle emploi, en ligne, à l'aide de son identité numérique. Elle transmet l'attestation d'employeur via le coffre-fort numérique de son compte CNIe, ses autres données d'identitésont transmises automatiquement.
Elle décide d'intégrer son statut de demandeur d'emploià ses données d'identité numérique.

Accès à tarifs réduits dans les lieux culturels

Sonia bénéficie d'un tarif réduit au musée en s'identifiant avec son identité numérique. Elle n'a cependant pasbesoin de mentionner qu'elle est en recherche d'emploi pour enbénéficier.

Inscription à une formation en ligne

Stéphanie souhaite participer à une formation en e-learning pour sereconvertir.

Elle ouvre un compte sur le site d'un l'organisme de formation et transmet les informations requises à son inscription en formation via son compte CNIe.

Tout au long de la formation, son identité numérique lui permettra d'accéder à la plateforme d'elearning et complètera automatiquement la feuille de présence.

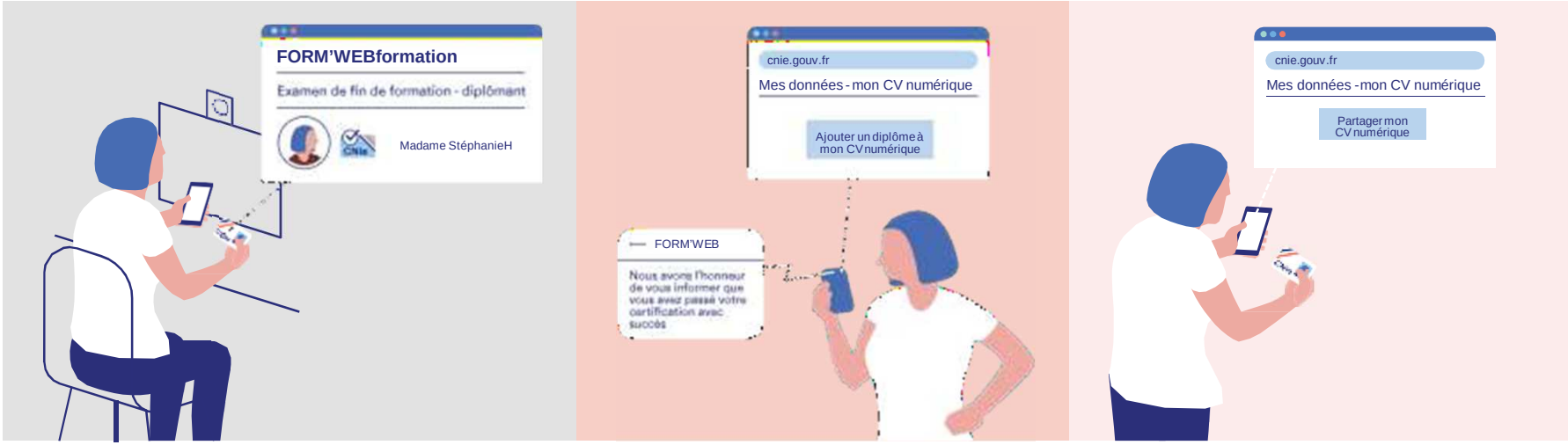
Les + pour l'usager

La compte CNIe permet de transmettre simplement et immédiatement toutes les informations requises et des documents justificatifs.

L'usager peut décider d'ajouter des données d'identité complémentaires à son identité numérique «officielle»

L'identité numérique contribue à éviter la stigmatisation en permettant de bénéficier de tarifs réduits sans en donner la raison.

L'identité numérique permet à l'usager d'ouvrir des comptes sur des sites privés volontaires sans créer de nouveaux identifiants, et de transmettre des données de manière simple et sécurisée à des acteurs tiers, facilitant ainsi de nombreux traitements (ex : attestation de présence en formation, rémunération des formations de Pôle Emploi).



Examen de certification par vidéo

Au terme de sa formation, Stéphanie passe un examen oral en ligne, par vidéo certifiée.
Un système de reconnaissance faciale permet de comparer son visage à la photo de sa CNIe pour certifier que c'est bien elle qui passe l'examen.

Réussite de l'examen

Sonia est informéequ'elle a réussi l'examen.

Elle décide d'enrichir ses données d'identité numérique avec la certification qu'elle vient d'obtenir (données de compétence, diplôme).

Transmission d'un dossier d'embauche

Après un entretien d'embaucheréussi, Stéphanie transmet les pièces administratives requises à la constitution de son dossier d'embauche via son compte CNIe.

L'identité numérique favorise le développement de nouveaux services, comme la vidéo certifiée par biométrie

L'usager peut choisir d'enrichir ses données et son coffre fort numérique au fil de ses activités.

L'usager peut valoriser de manière simplifiée des certifications acquises en formation.

8. Séjour ERASMUS

Fonctionnalités mobilisées

- Solution d'Identification universelle et hautement sécurisée, garantie par l'Etat
- Meilleure protectioncontre les risques d'usurpation d'identité
- Simplification des accès aux services en ligne publics et privés
- Accès à de nouveaux services en ligne rendus possibles par une identification certaine de l'usager
- Certification de l'identitédes interlocuteurs numériques

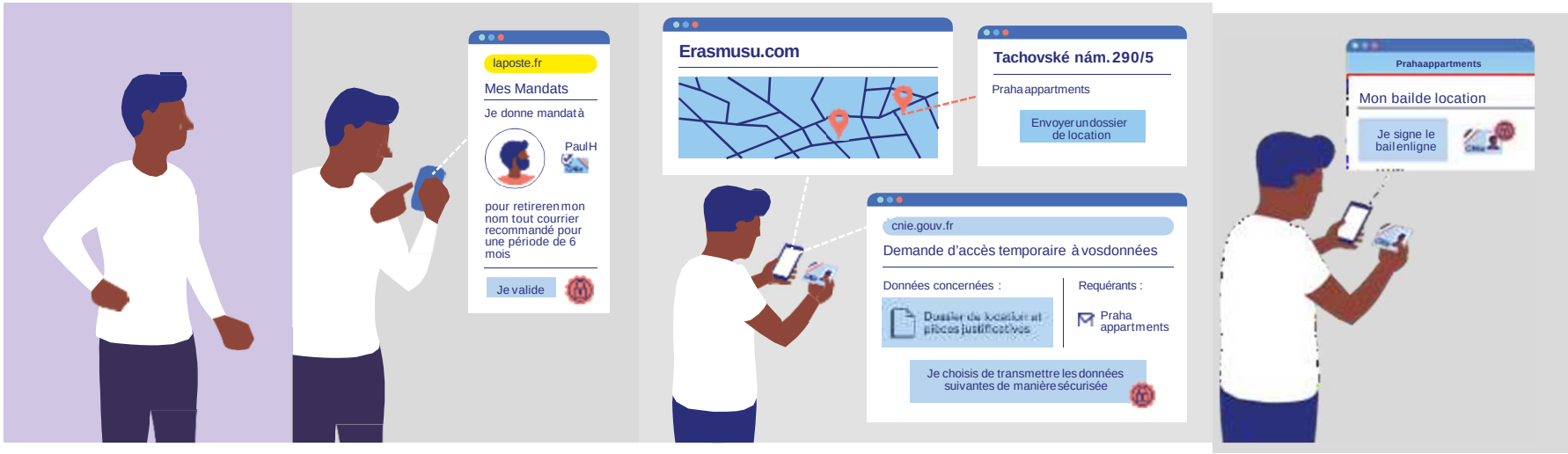
Attentes des usagers

- **Un accompagnement de l'Etat dans la gestion de son Identité Numérique** (ex : notification de fin de mandats)
- **De Nouveaux services en ligne et en physique** (vote en ligne, signature d'un bail locatif, accès à des lieux sécurisés, contrôles aéroport)
- **La facilité, en cas d'expatriation**, à effectuer des démarches et à maintenir le lien avec la France (ex : gestion de mandats etprocuration, reconnaissance de l'identité numérique en europe)

Bénéfices des fournisseurs de services

- L'opportunité de **renforcer l'image d'un service public innovant facilitant la vie des citoyens / usagers** (ex : français à l'étranger)
- La possibilité de **développer la citoyenneté et le sentiment d'appartenance** (ex : participation électorale via l'ouverture du vote en ligne, lien d'affiliation national avec les expatriés)

Kevin



Kevin, 20 ans

Kevin, 20 ans, est étudiant en école d'architecture. Il part en échange universitaire à Prague pendant un an, grâce au programme Erasmus.

Procuration

Avant de partir, Kevin donne procuration à son meilleur ami, via leurs comptes CNIe, pour récupérer ses recommandés et courriers.

Recherche d'appartement

Kevin recherche un appartement dans son pays d'accueil. Il dépose plusieurs dossiers de location en ligne en transmettant via son compte CNIe les données et justificatifs requis pour la constitution de dossiers locatifs.

Signature du bail à distance

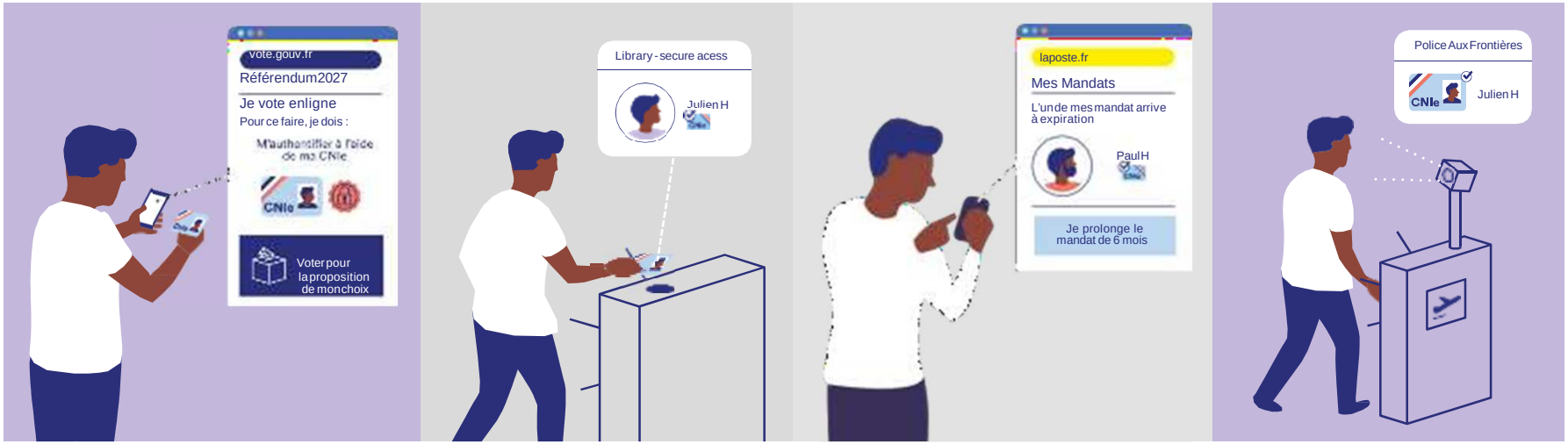
Grâce à son identité numérique garantie par l'état et reconnue en République Tchèque, il signe son bail depuis la France pour un appartement à Prague.

Les + pour l'usager

L'usager peut donner divers types de procurations à différentes personnes. Il peut gérer ses mandats via son tableau de bord sur son compte CNIe en ligne.

Le compte CNIe ouvre la possibilité de transmettre des documents facilement.

L'identité numérique adossé à la CNIe est un dispositif reconnu et interopérable au sein de l'union européenne.



Vote en ligne

Un référendum a lieu lors de son année à l'étranger. Pour voter en ligne depuis Prague, il s'identifie à l'aide de son identité numérique par procédure hautement sécurisée (identifiant + mot de passe + lecture de la puce de sa CNIe en sans contact avec son smartphone).

L'identité numérique sécurisée permet de réaliser à distance des actes officiels qui nécessitaient une présence physique jusqu'à présent

Elle facilite les « actes citoyens » sans avoir à anticiper et à suivre des démarches lourdes de procuration.

Accès à la bibliothèque

La bibliothèque de l'université est sécurisée suite à plusieurs incidents.

Kevin peut y accèder via une lecture sans contact de sa carte CNIe àl'entrée.

L'identité numérique favorise le développement de nouveaux services, comme les autorisations d'accès à des lieux sécurisés.

Préparation du retour en France

15 jours avant son retour en France, Kevin reçoit une notification l'informant que la procuration qu'il a donnée à son meilleur ami arrive bientôt à expiration.

Il décide de ne pas laprolonger.

Son compte CNIe l'aide à gérer ses mandats et procurations.

Passage des contrôles à l'aéroport

A l'aéroport, Il passe les différents contrôles rapidement à l'aide de sa CNIe.

La CNIe permet de passer rapidement les différents contrôles, comme le passeport biométrique.

Sommaire

ANNEXES

Direction interministérielle de la transformation publique

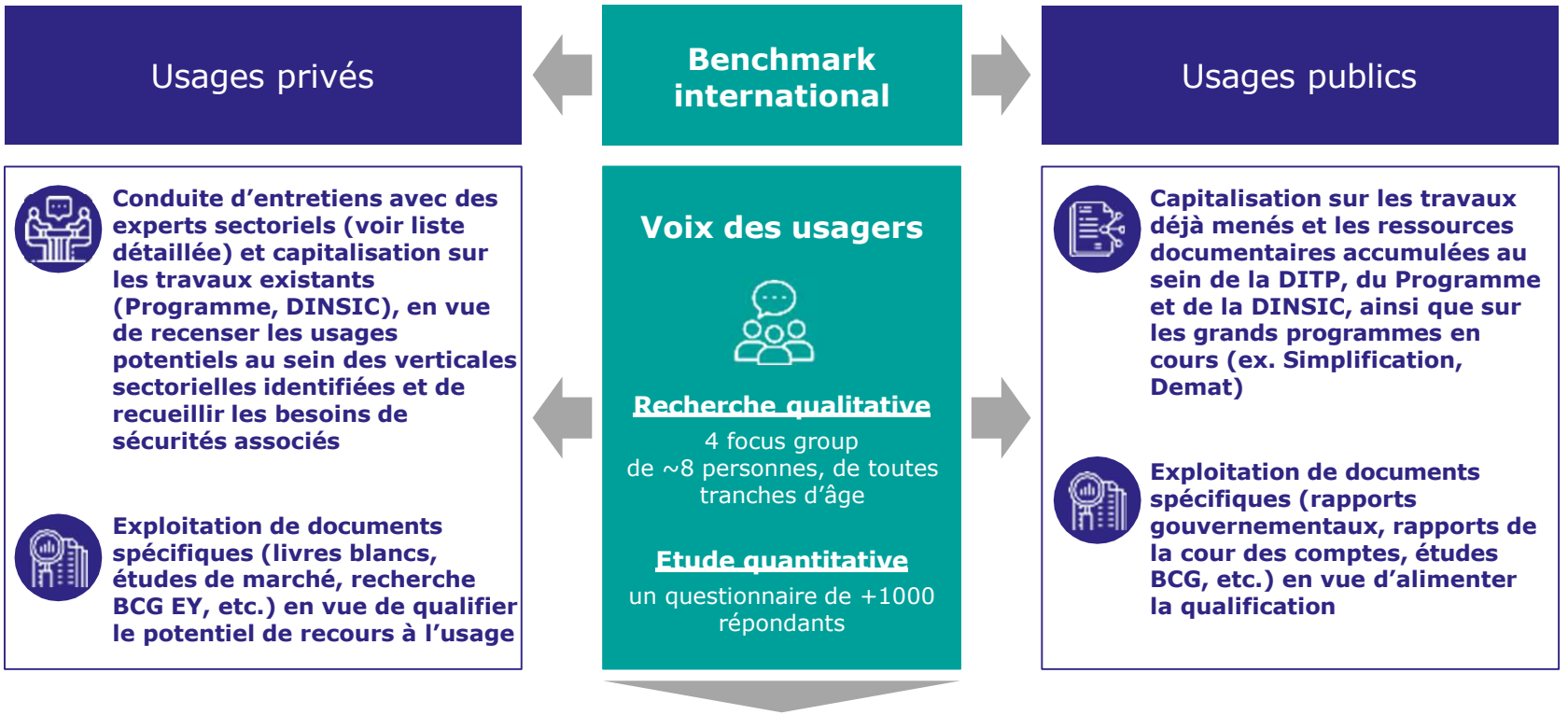
libérer l'énergie publique

Annexe 1

Approche retenue et méthode pour la cartographie et la qualification des usages porteurs de l'identité numérique

Direction interministérielle de la transformation publique
libérer l'énergie publique

L'approche retenue pour recenser et qualifier les usages privés et publics combine plusieurs sources complémentaires



~25 usages privés et ~55 usages publics recensés et qualifiés

Le benchmark géographique couvre principalement 11 pays, choisis en fonction de leur maturité digitale et avec quelques éclairages hors-UE

 **Allemagne**

 **Danemark**

 **Suède**

 **Australie**

 **Italie**

 **Suisse**

 **Autriche**

 **Norvège**

 **Grande-Bretagne**

 **Belgique**

 **Pays-Bas**

Source : Entretiens experts internationaux ; Recherche documentaire ; Analyses BCG & EY-Parthenon

Pour information : liste des entretiens menés dans le cadre du benchmark géographique (1/2)

Pays concerné	Contact	Poste du contact
Allemagne	Patrick Bauer	Partner BCG
Autriche	Elfriede Baumann	Partner EY
Belgique	Jeroen Magnus	Partner BCG
Italie	Arturas Piliponis	Partner EY
	Diego Pavoni	Partner EY
Pays Bas	Peter Geluk	Senior Partner BCG
Suède	Olof Sundstorm	Partner EY

Pour information : liste des entretiens menés dans le cadre du benchmark géographique (2/2)

Pays concerné	Contact	Poste du contact
Suède	Linda Andersson	Partner EY
Australie	Brendan Whiting	Partner EY
	Miguel Carrasco	Partner BCG
Grande-Bretagne	Dean Frankle	Partner BCG
	Radhika Chadwick	Partner EY
Inde	Thampy Koshy	Partner EY
Suède	Florian Frey	Partner BCG

Plusieurs verticales sectorielles (avec des enjeux de sécurité et de parcours client particulièrement sensibles) ont été investiguées

Assurance

Banque

Jeux

Mobilité

Plateformes de services et collaboratives

Santé privée

Tiers de confiance
(dont notaires, poste électronique, coffres forts, etc.)

Utilities

Source : Entretiens experts sectoriels ; Analyses BCG & EY-Parthenon

Pour information : liste des entretiens menés dans le cadre du recensement et de la qualification des usages privés et publics (1/2)

Sphère du domaine d'expertise	Domaine d'expertise	Contact	Fonction
Public	Social publique	Déborah Autheman	Délégué transformation pilotage modernisation – Région Nouvelle-Aquitaine
Public	Santé publique	Loïc Chabannier	Partner EY en charge de l'activité Santé publique
Public	Santé publique	Daniel Benamouzig	Spécialiste Santé au CSO / Sciences Po
Privé	Assurances	Charles-Antoine Wallaert	Partner BCG
Privé	Assurances	Thomas Ollivier	MAIF – Responsable du développement des partenariat (orienté économie collaborative)
Privé	Assurances	Laurent Borella	Malakoff Médéric – Directeur du pôle santé
Privé	Banque	Yann Senant	Partner BCG

Pour information : liste des entretiens menés dans le cadre du recensement et de la qualification des usages privés et publics (2/2)

Sphère du domaine d'expertise	Domaine d'expertise	Contact	Fonction
Privé	Télécoms	Jean Baptiste Bearez	Partner BCG en charge de l'activité Télécoms
Privé	Banque	Jérémie Borot	Natixis Payments - Directeur
Privé	Banque	Valérie Villafranca + Equipe KYC / Compliance	Société Générale – Global head KYC transformation
Privé	Energie	Emmanuel Austruy	Partner BCG
Privé	Jeux	Cyril Duport	FDJ – Chef de projet parcours d'inscription & d'identification
Privé	Santé privée	Arnaud Laferte	Partner EY en charge de l'activité Santé privée
Privé	Télécoms	Etienne Costes	Partner EY en charge de l'activité Télécoms

Annexe 2

Règlement eIDAS

Direction interministérielle de la transformation publique

libérer l'énergie publique

Le règlement européen eIDAS définit de manière exhaustive les spécifications techniques et procédures associées au parcours usager (1/2)

Phase d'enrôlement

Faible

1. La personne peut être **présumée en possession d'un élément d'identification** reconnu par l'État membre
2. L'élément d'identification peut être **présumé authentique**
3. L'existence de l'identité alléguée est connue d'une source faisant autorité et on peut **présumer que la personne est celle qu'elle prétend être**

Substantiel : Niveau faible, plus l'une des options énumérées aux points 1 à 4 ci-après

1. La possession d'un élément d'identification, authentique, est vérifiée ou des mesures ont été prises pour minimiser le risque qu'il ne s'agisse pas de l'identité alléguée (Ex. : Perte, vol, suspension, révocation, expiration, etc.)
2. Une pièce d'identité est présentée au cours d'un processus d'enregistrement et la pièce d'identité semble se rapporter à la personne et des mesures ont été prises pour minimiser le risque qu'il ne s'agisse pas de l'identité alléguée
3. Lorsque les procédures précédemment utilisées par une entité publique ou privée dans le même État membre (en dehors de la délivrance) assurent une garantie équivalente au point précédent, l'entité responsable de l'enregistrement n'est pas tenue de répéter ces précédentes procédures, sous condition de confirmation par un organisme d'évaluation de la conformité
4. Lorsque des moyens d'identification électronique sont délivrés sur la base d'un moyen d'identification électronique notifié valide ayant le niveau de garantie élevé ou substantiel et tenant compte des risques d'une modification des données d'identification personnelle, il n'est pas nécessaire de répéter les processus de preuve et de vérification d'identité (doit être confirmé par un organisme d'évaluation en cas d'absence de notification)

Élevé : Niveau substantiel, plus l'une des options énumérées aux points 1 à 3 ci-après

1. Lorsque la **possession d'un élément d'identification biométrique ou photographique a été vérifiée** et que cet élément **correspond à l'identité** alléguée, l'élément fait l'objet d'une **vérification de validité** par comparaison de caractéristiques physiques de la personne
2. Lorsque les **procédures précédemment utilisées par une entité publique** ou privée dans le même État membre (en dehors de la délivrance) assurent une garantie équivalente à un niveau de garantie élevé, l'entité responsable de l'enregistrement **n'est pas tenue de répéter** ces précédentes procédures, sous réserve que cette garantie équivalente soit confirmée par un organisme de conformité
3. Lorsque des moyens d'identification électronique sont délivrés sur la base d'un **moyen d'identification électronique notifié valide ayant le niveau de garantie élevé**, et en tenant compte des risques d'une modification des données d'identification personnelle, il n'est **pas nécessaire de répéter les processus de preuve et de vérification d'identité** (ou doit être confirmé par un organisme d'évaluation en cas d'absence de notification).

Le règlement européen eIDAS définit de manière exhaustive les spécifications techniques et procédures associées au parcours usager (2/2)

Mise à disposition du moyen d'identification

Faible :
Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il ne sera reçu que par le destinataire prévu

Substantiel :
Après la délivrance, le moyen d'identification électronique est mis à disposition par un mécanisme permettant de présumer qu'il sera exclusivement remis en la possession de la personne à laquelle il appartient

Élevé :
Le processus d'activation vérifie que le moyen d'identification électronique a été remis exclusivement en la possession de la personne à laquelle il appartient

Utilisation du moyen d'identification

Faible :
La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité. Lorsque des données d'identification personnelle sont mémorisées dans le cadre du mécanisme d'authentification, ces informations sont sécurisées afin d'assurer leur protection contre toute perte ou compromission, y compris une analyse hors ligne.
Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque de base renforcé puissent nuire aux mécanismes d'authentification.

Substantiel : Niveau faible, plus les options ci-après
La diffusion de données d'identification personnelle est précédée par la vérification fiable du moyen d'identification électronique et de sa validité par une authentification dynamique. Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque modéré puissent nuire à l'authentification.

Élevé : Niveau substantiel, plus l'option ci-après
Le mécanisme d'authentification met en œuvre des contrôles de sécurité pour la vérification du moyen d'identification électronique, de sorte qu'il est hautement improbable que des activités telles que les tentatives de décryptage, l'écoute, l'attaque par rejeu ou la manipulation d'une communication par un attaquant ayant un potentiel d'attaque élevé puissent nuire aux mécanismes d'authentification

Annexe 3

Chantier "voix des usagers"
Eléments de méthode

Direction interministérielle de la transformation publique
libérer l'énergie publique

Rappel de la méthode de l'étude "voix des usagers"

Etude qualitative : 4 ateliers MindDiscovery® organisés

Format de "focus groups" avec utilisation de techniques de stimulation et d'animation créatives

2 ateliers à Paris et 2 ateliers à Tours (27 au 29/03/19)

Dans chaque ville, un atelier avec des usagers de -40 ans et un avec des +40 ans

8 personnes par atelier avec des profils diversifiés : genre, revenus, situation familiale, aisance pour utiliser internet, attitude quant à la protection des données personnelles sur internet et les nouvelles technologies, etc

Etude quantitative : 2 questionnaires administrés auprès de ~1200 personnes

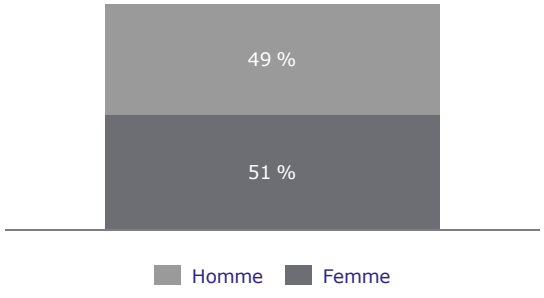
Un questionnaire administré en ligne (8 au 14/04/19)
- 1033 répondants
- Echantillon représentatif de la population française sur les critères : genre, âge, zone d'habitation, CSP

En complément, un questionnaire administré au téléphone (16 au 21/04/19)
- 156 répondants
- Echantillon de personnes "éloignées du numérique" , i.e. faisant peu ou pas de démarches par internet

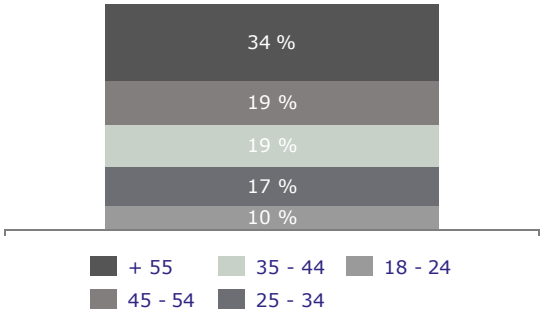
Analyse des données et segmentation en fonction de l'âge, de la zone d'habitation, de la CSP et de l'aisance numérique

Un échantillon représentatif de la population française

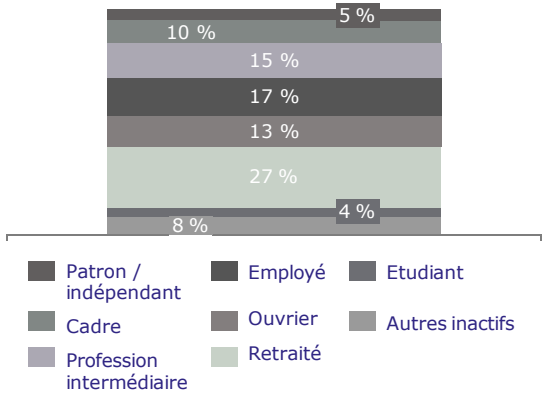
Sexe



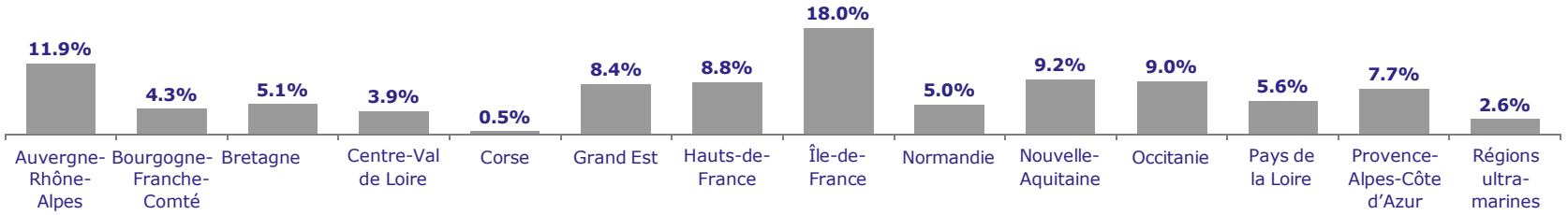
Âge



CSP



Régions



Les cas d'usage testés dans le questionnaire en ligne

Considérés comme "E-commerce" dans l'analyse	1	Créer un compte sur un site de vente en ligne
	2	Se connecter à son compte sur un site de vente en ligne
	3	Ouvrir un compte bancaire en ligne
	4	Souscrire une assurance (auto, habitation) en ligne
	5	Faire une demande de crédit en ligne
	6	Faire un virement d'un montant élevé
	7	Gérer son abonnement téléphonique en ligne
	8	S'identifier auprès du service client d'une entreprise au téléphone
	9	Accéder à son lieu de travail (avec un badge d'entreprise par exemple)
	10	Réceptionner un courrier ou un colis avec accusé de réception
	11	Prendre l'avion (contrôles d'identité à l'aéroport)
	12	Se connecter sur le site impots.gouv pour déclarer et payer ses impôts sur internet
	13	Créer et gérer son dossier médical partagé en ligne
	14	Faire une demande de carte grise en ligne
	15	Se connecter sur le site de la CAF, par exemple pour gérer ses droits sociaux
	16	S'inscrire sur des plateformes collaboratives (comme Airbnb ou BlaBlaCar)
	17	Déclarer une naissance ou un décès à la mairie
	18	Prouver son âge sur internet (par exemple pour accéder à des contenus réservés aux personnes majeures)
	19	S'inscrire sur des sites de jeux d'argent en ligne (les sites de paris sportifs par exemple)
	20	S'inscrire sur des sites de rencontres
	21	Voter aux élections (présidentielles, législatives ou municipales par exemple)
	22	S'inscrire aux services proposés par sa mairie (cantine, crèche, loisirs par exemple)
	23	Obtenir des résultats d'examens médicaux
Considérés comme "Accès Améli" dans l'analyse	24	Se connecter sur le site de la sécurité sociale (Ameli)
	25	Faire une demande de nouveau mot de passe pour le site de la sécurité sociale (Ameli)
	26	Faire une demande de renouvellement de pièces d'identité (cartes d'identité, passeports)

Présentation du concept d'identité numérique sécurisée dans le questionnaire en ligne

Nous allons vous présenter une idée de nouvelle solution pour vous identifier et prouver qui vous êtes.

Imaginez une solution d'identification numérique gérée et garantie par l'Etat et particulièrement sécurisée. Elle vous permet de vous identifier avec le même identifiant pour toutes vos démarches avec tous les services publics (santé, impôts, services municipaux, …) que ce soit sur internet ou pour prouver votre identité lors de visites en personne auprès de ces services.

Vous pouvez aussi utiliser cette identité numérique garantie par l'Etat pour certifier officiellement diverses démarches à distance (contrats de vente, actes notariés, ...).
Enfin, vous pouvez l'utiliser pour vous identifier en ligne auprès de services privés qui le proposeraient, par exemple pour s'inscrire plus vite à des services ou pour des transactions demandant une plus grande sécurité.

Cette solution d'identité numérique garantie par l'Etat aurait pour supports une carte à puce et, si vous le souhaitez, une application sur smartphone. Nous appellerons cette solution d'identification sécurisée ID Num (pour « Identité Numérique ») dans le reste du questionnaire pour des raisons de facilité.

Réactions au concept d'identité numérique sécurisée testées dans le questionnaire en ligne

1. « C'est une bonne idée, cela me simplifierait la vie d'avoir un seul identifiant pour de nombreux services, notamment pour tous les services publics. »
2. « C'est une bonne idée, cela me ferait gagner du temps en m'évitant de scanner et d'envoyer divers documents d'identité par courrier ou par mail. »
3. « C'est une bonne idée, cela permettrait de limiter les risques de fraudes et d'usurpations d'identité, en particulier sur internet. »
4. « C'est une bonne idée, cela permettrait d'accéder à davantage de services en ligne et m'éviterait ainsi de me déplacer physiquement. »
5. « Cela me paraît risqué car si je perds mon identité numérique je ne peux plus accéder à de nombreux services, notamment en ligne (ceux qui utilisent ID Num comme moyen d'identification). »
6. « Cela me paraît risqué car si l'on me vole mon identité numérique, le hacker a accès à plusieurs de mes comptes en ligne et peut usurper mon identité sur de nombreux sites (ceux qui utilisent ID Num comme moyen d'identification). »
7. « Cela me paraît risqué car l'Etat pourrait être capable de surveiller quand et pour quoi faire je m'identifie avec la solution ID Num. »
8. Aucune de ces réactions n'est proche de ce que je me suis dit.

Les fonctionnalités testées dans le questionnaire en ligne (1/2)

1. M'identifier et m'authentifier facilement et rapidement

Avec ID Num, je peux utiliser le même identifiant et mode de validation (code, code SMS,…) pour me connecter plus facilement à tous les services publics (administrations, services municipaux, etc).

Je peux aussi utiliser mon identifiant ID Num pour me connecter rapidement à d'autres sites ou services sur internet même privés qui le proposent sans avoir à créer un nouvel identifiant et mot de passe et en évitant d'utiliser un identifiant de réseau social ou service internet commercial et les possibles échanges de données que cela peut permettre.

2. M'identifier et m'authentifier de manière sécurisée

Je veux accéder à un service en ligne pour lequel je dois m'identifier et prouver qui je suis de manière certaine (faire un virement d'un montant élevé par exemple). ID Num me permet de m'identifier de manière sécurisée sur le site internet en question (celui de ma banque par exemple) depuis mon PC ou mon smartphone (avec un code envoyé par sms en temps réel ou par lecture de mon empreinte digitale par exemple) et donc de limiter les risques d'usurpations d'identité et de fraudes.

3. Donner mon consentement à distance de manière légale et officielle

Je dois prouver que je suis d'accord avec un engagement que je prends (un acte de vente d'un bien immobilier par exemple). ID Num me permet de prouver qui je suis depuis mon PC ou mon smartphone et de faire une signature électronique qui a une valeur légale et officielle (contrairement aux signatures électroniques actuelles), me permettant ainsi de ne pas avoir à me déplacer physiquement pour signer divers documents (chez mon notaire par exemple).

4. Me donner accès à des zones physiques

Je dois prouver qui je suis pour accéder à une zone contrôlée ou sécurisée (l'aéroport, mon lieu de travail, ma salle de sport par exemple). ID Num me donne la possibilité d'utiliser mon support d'identité numérique (une carte à puce ou mon smartphone par exemple) pour accéder à ces zones. Je peux choisir d'utiliser mon support d'identité ID Num comme mon seul moyen d'accès à plusieurs endroits (au lieu d'avoir une multitude de badges comme celui fourni par mon employeur pour accéder à mon lieu de travail) ou je peux l'utiliser quand je n'ai pas le badge classique sur moi (si je l'ai oublié par exemple)

Les fonctionnalités testées dans le questionnaire en ligne (2/2)

5. Agir au nom d'un tiers

Si je suis le représentant permanent ou temporaire de quelqu'un (d'une personne âgée sous tutelle ou d'une personne expatriée par exemple), je dois agir en son nom (par exemple pour gérer ses dépenses et ses démarches administratives). ID Num me permet de prouver mon mandat ou ma procuration grâce à mon support d'identité numérique (carte à puces, PC, smartphone) à chaque fois qu'on me les demande, au lieu de montrer en physique ou d'envoyer par mail la preuve d'un tel mandat ou d'une telle procuration.

6. Gérer le partage de mes données personnelles

Pour effectuer une démarche (faire une demande de crédit, inscrire un enfant à la cantine par exemple), je dois transmettre diverses informations (revenus, justificatif de domicile…). ID Num me donne la possibilité de partager avec un acteur public ou privé (ma banque par exemple) certaines de mes données (je choisis ce que je veux partager). Les éléments sont envoyés directement à cet acteur, je n'ai plus besoin de fournir les documents en devant me déplacer physiquement ou les envoyer par mail.

7. Protéger mon identité

Si je perds ou si je me fais voler le support de mon identité numérique (une carte à puce ou mon smartphone par exemple), ID Num me permet de faire opposition à mon identité numérique instantanément. Il est alors impossible que quelqu'un utilise mon identité numérique pour usurper mon identité (un peu comme faire opposition sur une carte). Un nouvel identifiant m'est envoyé pour pouvoir continuer à utiliser les services les plus courants qui utilisent ID Num.

Les usages prospectifs testés dans le questionnaire en ligne

1. Voter en ligne pour les élections sans se déplacer au bureau de vote
2. Passer un entretien en ligne sans se déplacer (chez le recruteur ou dans une agence Pôle emploi)
3. Faire une procuration de vote (pour des élections) en ligne sans se déplacer au commissariat
4. Consulter un médecin à distance sans se déplacer au cabinet médical
5. Partager ses données personnelles de santé et ses résultats médicaux à un médecin sans se déplacer à son cabinet médical pour un suivi à distance régulier
6. Déposer une plainte en ligne et suivre son avancement en ligne sans se déplacer au commissariat ou au tribunal
7. Communiquer à distance avec les établissements scolaires (école primaire, collège, …) grâce à un carnet de correspondance numérique (pour signaler l'absence de son enfant par exemple)
8. Signer un acte de vente d'un bien immobilier en ligne sans se déplacer chez le notaire
9. Faire son testament en ligne sans se déplacer chez le notaire
10. Renouveler son passeport en ligne sans se déplacer à la préfecture
11. Passer un examen (études, formation) en ligne par vidéo sans se déplacer au centre d'examen

Les inquiétudes testées dans le questionnaire en ligne

1. Je pourrais ne pas avoir accès, ne pas posséder ou ne pas maîtriser les outils digitaux nécessaires à l'utilisation d'une telle identité numérique (smartphone, ordinateur connecté à internet).

2. L'administration publique pourrait être peu réactive en cas de problème lié à mon identité numérique (perte, vol, problème informatique).

3. L'Etat pourrait ne pas avoir les moyens financiers pour mettre en place un système informatique suffisamment sécurisé (comparé aux acteurs privés).

4. L'Etat pourrait être une cible privilégiée par les hackeurs (comparé aux acteurs privés).

5. En cas de perte ou de vol de mon identité numérique, je pourrais être victime d'usurpation d'identité sur un nombre important de sites internet.

6. L'Etat pourrait être capable de surveiller quand et pour quoi faire je m'identifie avec la solution.

7. En cas de perte ou de vol de mon identité numérique, je pourrais perdre accès à un nombre important de services, en particulier sur internet.

8. J'ai peur que toutes mes données soient concentrées au même endroit, ce qui me rendrait très vulnérable en cas de problème ou de piratage informatiques.

Les éléments de réassurance testés dans le questionnaire en ligne

1. Des personnes sont disponibles pour vous aider à maîtriser les outils digitaux nécessaires au téléphone ou en physique (dans votre mairie par exemple).

2. Les appareils nécessaires à l'identification en ligne (smartphone, PC) sont mis à disposition des citoyens en libre-service dans des sites publics (mairies, bureaux de poste par exemple).

3. Des alertes (sms ou mail) vous sont envoyées en cas d'utilisation inhabituelle de votre identité numérique (nouvel appareil, nouvelle localisation) pour réduire les risques de fraudes ou d'usurpations d'identité.

4. En cas de perte ou de vol de votre identité numérique, un identifiant et un mot de passe provisoires vous sont envoyés pour pouvoir accéder à la plupart des services (pas les plus sensibles) en attendant le renouvellement de votre identité numérique.

5. Il n'y a aucune mise en commun des données des différents services concernés (seulement l'identifiant et la manière par laquelle vous vous identifiez seront communs).

Source : Analyses BCG & EY-Parthenon

Annexe 4

Chantier "voix des usagers »

Synthèse vidéo des focus group

Focus Groups : Extraits vidéo

Format de "focus groups" avec utilisation de techniques de stimulation et d'animation créatives
2 ateliers à Paris et 2 ateliers à Tours, du 27 au 29/03/19
Dans chaque ville, un atelier avec des usagers de -40 ans et un avec des +40 ans
8 personnes par atelier avec des profils diversifiés : genre, revenus, situation familiale, aisance pour utiliser internet, attitude quant à la protection des données personnelles sur internet et les nouvelles technologies, etc

Annexe 5

Chantier "voix des usagers »

Eléments d'analyse complémentaires

Des technologies plus sécurisées pour s'identifier auprès des services publics, des banques et des professionnels de santé

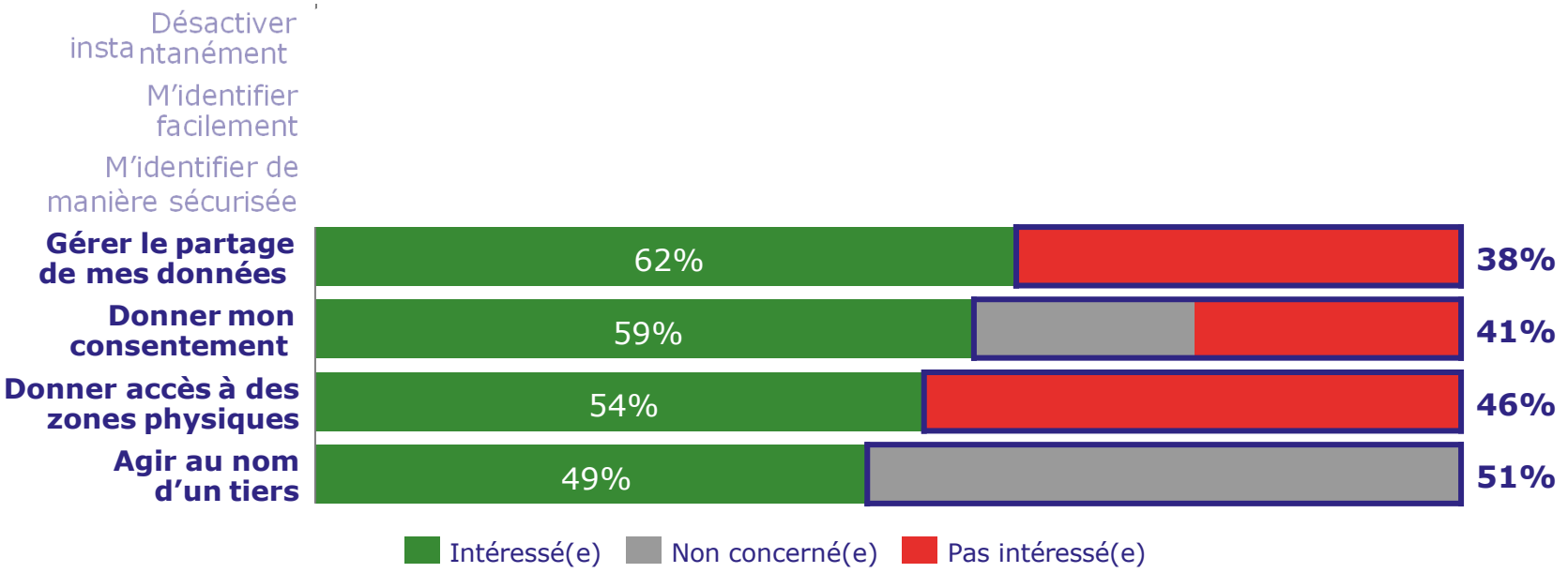
		- sécurisé → + sécurisé		
		Mot de passe	**Mot de passe & code SMS**	**Mot de passe & biométrie**
Services publics	Renouveler son passeport en ligne	0	2	22
	Voter en ligne	1	6	17
	Déposer une plainte en ligne	8	4	12
Banque	Ouvrir un compte en banque en ligne	2	7	22
	Demander un crédit en ligne	1	5	9
Santé	Consulter son médecin à distance	2	1	19
Secteurs privés	Faire un achat en ligne	2	**18**	8
	Gérer son abonnement téléphonique	2	**6**	3
	S'inscrire sur une plateforme collaborative	**7**	**7**	0

Les usagers n'ont pas spontanément souhaité des niveaux de sécurité différents en fonction des situations d'identification

Source : Analyses BCG & EY-Parthenon

Les fonctionnalités les plus innovantes ne bénéficient pas d'une adhésion spontanée forte

Seriez-vous intéressé(e) par ces fonctionnalités ?



Les 4 fonctionnalités les plus innovantes sont celles qui convainquent le moins les répondants

2 usages symboliques identifiés : prouver son âge sur internet et signaler des violences conjugales

Prouver son âge sur internet

18%
répondants

Trouvent que la procédure pour prouver son âge sur internet est **insuffisamment sécurisée**

1ère situation pour laquelle la sécurité est insuffisante selon les répondants

> Ce serait bien que les enfants puissent prouver leur âge sur internet avec cette identité numérique. Sur certains sites, il suffit de cocher une case **pour prouver qu'on est majeur, ce n'est pas assez sécurisé.** Karine, 46 ans

Signaler des violences conjugales

34%
répondants

Pensent que déposer une plainte en ligne est un des 3 usages à rendre **accessibles en ligne en priorité**

3ème usage prospectif le plus intéressant selon les répondants

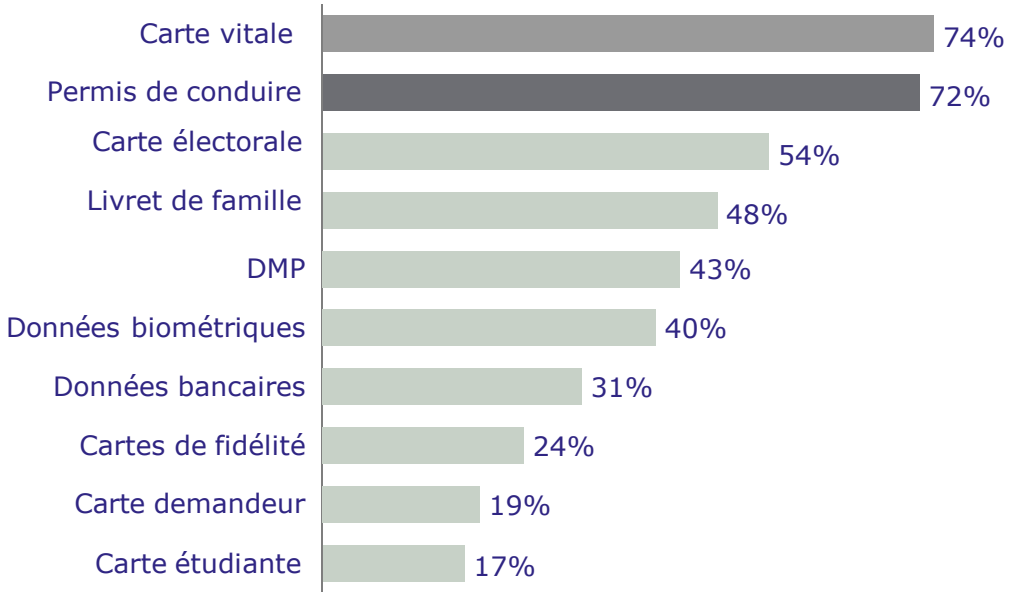
> Les gens **oseraient plus facilement** dénoncer des violences conjugales **en ligne** car ils ont **peur d'aller au commissariat.** Ce n'est pas facile d'aller raconter ce genre de choses à un inconnu. Sylvie, 63 ans

Note : pourcentages issus de l'analyse quantitative et citations issues de l'analyse qualitative
Source : Analyses BCG & EY-Parthenon

Les informations relatives à la carte vitale et au permis de conduire, les données à associer en priorité à la future CNIe

Quelles informations souhaiteriez-vous associer à cette carte personnelle et officielle d'identification, au-delà de vos données d'identité classiques ?

(% de répondants favorables)



Les 18-34 ans souhaitent davantage intégrer les données liées à leur carte étudiante, leur carte de demandeur d'emploi et leurs cartes de fidélité

Les +55 ans souhaitent davantage intégrer les données liées à leur carte vitale et leur dossier médical partagé

Note 1 : résultats issus de l'analyse quantitative (question posée " quelles informations souhaiteriez-vous associer à cette carte personnelle et officielle d'identification, au-delà de vos données d'identité classiques ?")
Note 2 : réponses "je ne me prononce pas" et "autres" exclues
Source : Analyses BCG & EY-Parthenon

Les réactions des usagers varient principalement selon leur maturité digitale (et peu selon les critères de segmentation classiques)

Les réactions des répondants par rapport aux situations d'identification actuelles et à la solution d'identité numérique (appréciation générale, inquiétudes, éléments de réassurance, …) dépendent peu de leur âge, de leur zone d'habitation ou de leur catégorie socio-professionnelle

La maturité digitale des répondants en revanche est un critère de segmentation important :
78% des répondants qui sont "toujours à l'aise avec le digital" adhèrent à la solution d'identité numérique contre 62% pour ceux qui ne sont "pas du tout à l'aise"

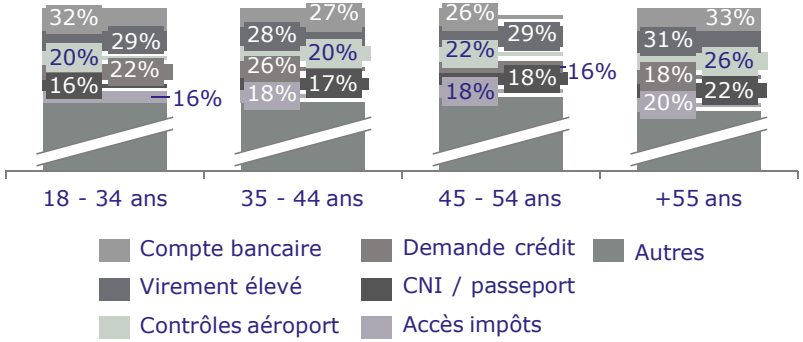
Mais les situations d'identification à fort potentiel du point de vue des usagers sont communes aux différents segments de maturité digitale :
- Les plus pénibles : renouveler sa CNI / son passeport, accéder à son compte Améli, demander une carte grise, faire un virement d'un montant élevé & passer les contrôles à l'aéroport
- Celles avec le besoin de sécurité le plus fort : renouveler sa CNI / son passeport, faire un virement d'un montant élevé, accéder à son compte impôts. Gouv & passer les contrôles à l'aéroport

Les répondants les moins à l'aise avec le digital sont aussi les plus inquiets par rapport à cette identité numérique et ceux qui seront les plus difficiles à rassurer

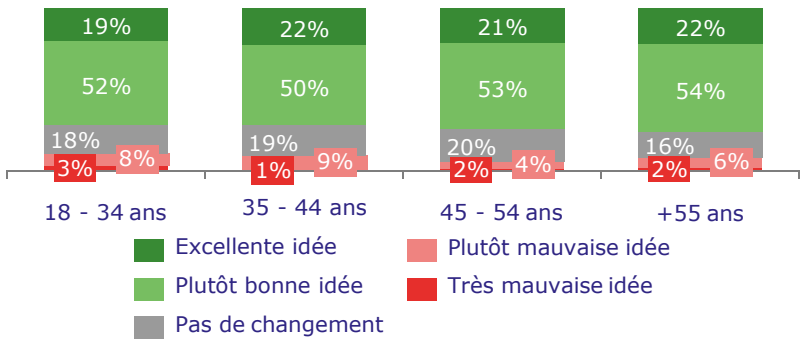
Source : Analyses BCG & EY-Parthenon

Les réactions des usagers dépendent peu de leur âge

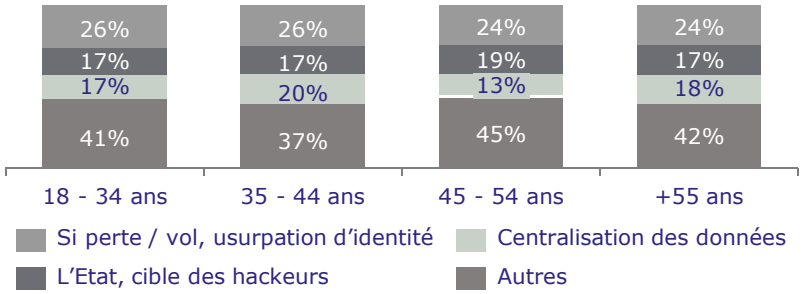
Top 3 des situations d'identification à améliorer (% occurrences)



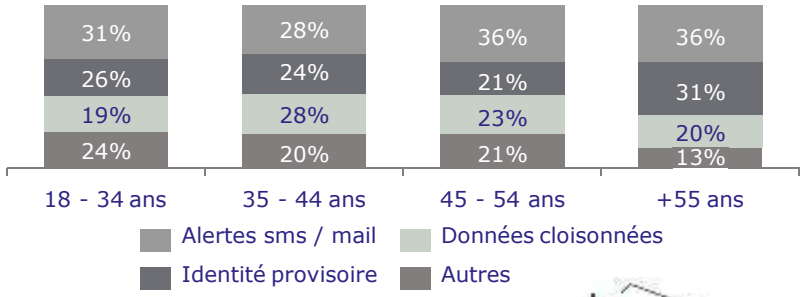
Réaction spontanée au concept d'identité numérique (% répondants)



Top 1 des inquiétudes (% répondants)



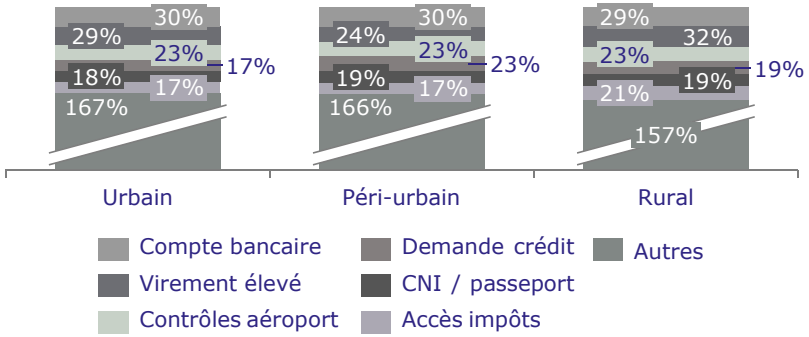
Top 1 des éléments de réassurance (% répondants)



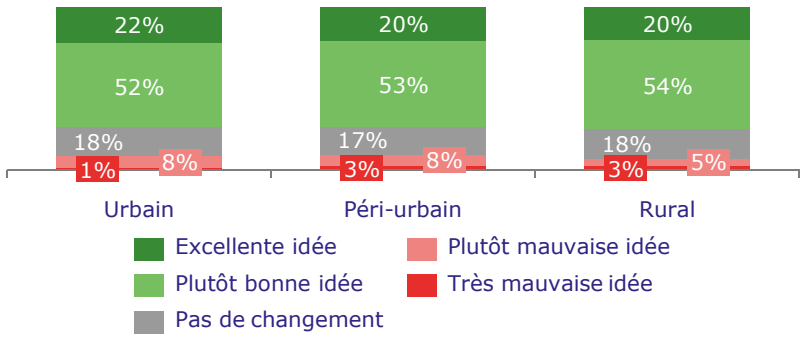
Source : Analyses BCG & EY-Parthenon

Les réactions des usagers dépendent peu de leur zone d'habitation

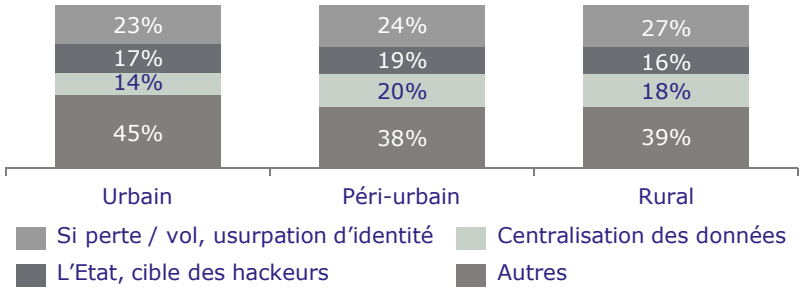
Top 3 des situations d'identification à améliorer (% occurrences)



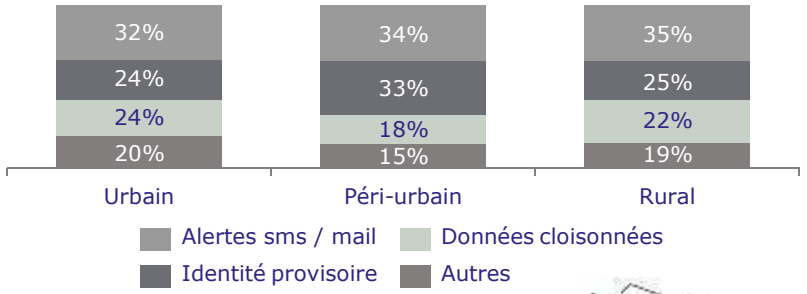
Réaction spontanée au concept d'identité numérique (% répondants)



Top 1 des inquiétudes (% répondants)



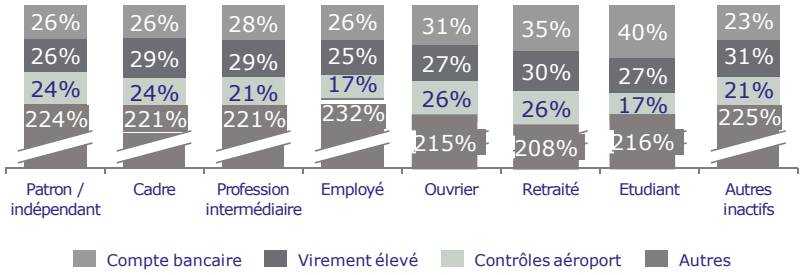
Top 1 des éléments de réassurance (% répondants)



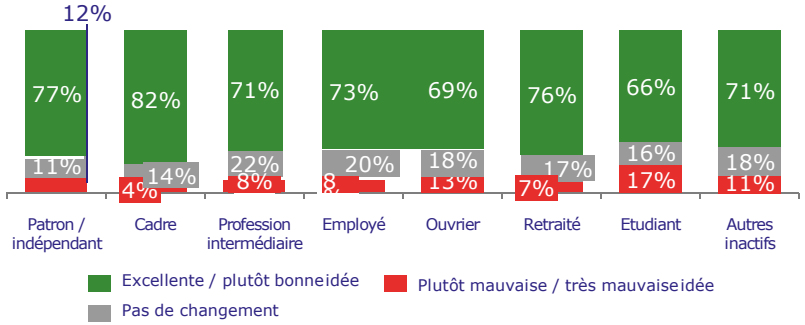
Source : Analyses BCG & EY-Parthenon

Les réactions des usagers dépendent peu de leur CSP

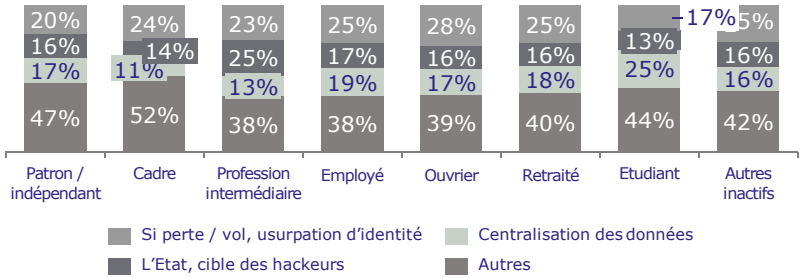
Top 3 des situations d'identification à améliorer (% occurrences)



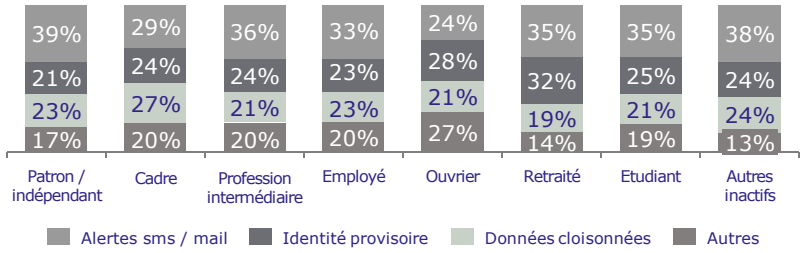
Réaction spontanée au concept d'identité numérique (% répondants)



Top 1 des inquiétudes (% répondants)



Top 1 des éléments de réassurance (% répondants)



Note : résultats issus de l'analyse quantitative
Source : Analyses BCG & EY-Parthenon

Méthode utilisée pour segmenter les répondants selon leur maturité digitale

Segmentation fondée sur les réponses à une question

Dans quelle mesure êtes-vous à l'aise pour réaliser les actions suivantes ?

- Faire des achats en ligne avec votre Smartphone
- Faire des démarches administratives avec votre Smartphone
- Faire des achats en ligne avec votre PC ou tablette
- Faire des démarches administratives en ligne avec votre PC ou tablette

3 profils définis pour segmenter les répondants du questionnaire

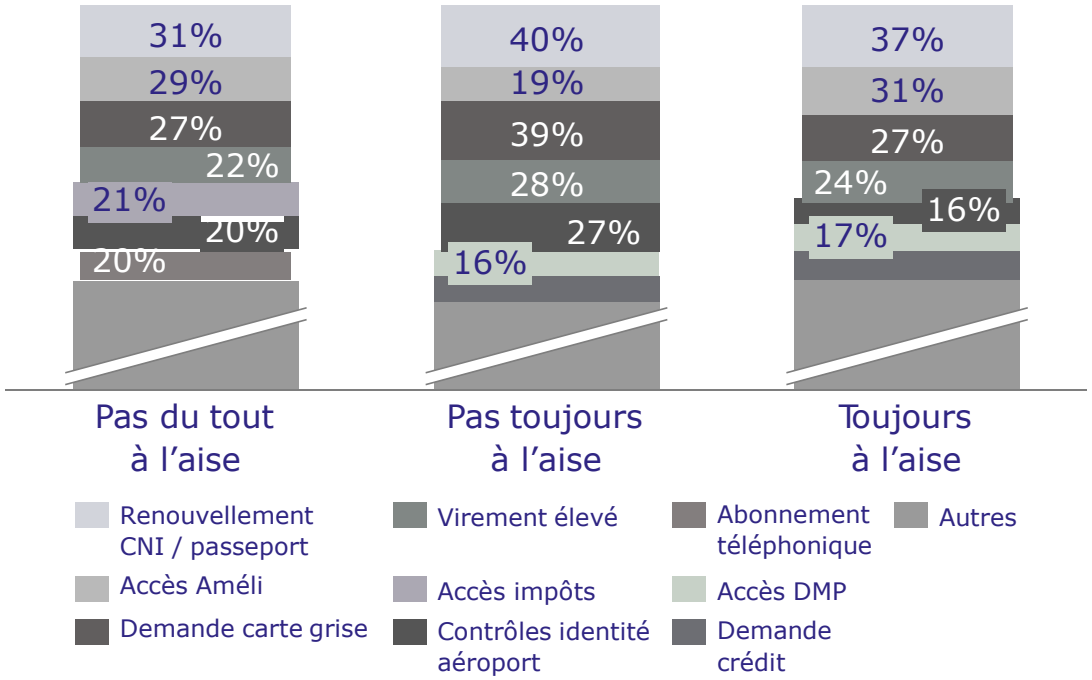
1. Les répondants "pas du tout à l'aise" avec le digital
   Les répondants qui ont choisi "pas du tout à l'aise" pour au moins un des 4 items

2. Les répondants "toujours à l'aise" avec le digital
   Les répondants qui ont choisi "plutôt à l'aise" ou "très à l'aise" pour les 4 items

3. Les répondants "pas toujours à l'aise" avec le digital
   Le reste des répondants

Les situations dans lesquelles s'identifier est le plus pénible sont globalement les mêmes entre répondants de maturités digitales différentes

Quelles sont les 3 situations dans lesquelles s'identifier est le plus compliqué et pénible parmi les 25 ci-dessous ?
(top 7 des situations les plus fréquemment citées)



5 des 7 situations les plus pénibles sont communes :

- Renouveler CNI / passeport
- Accéder à son compte Améli
- Demander une carte grise
- Faire un virement élevé
- Passer les contrôles à l'aéroport

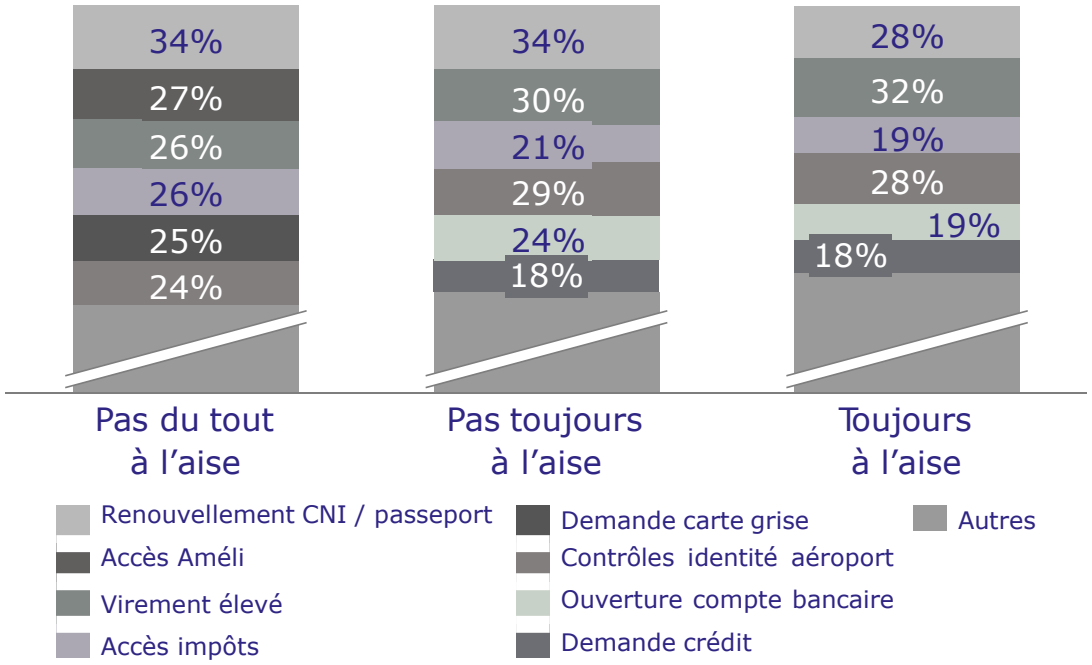
Quelques différences :

- Demander un crédit en ligne et accéder à son DMP pour "les plus à l'aise avec le digital"
- Accéder à son compte impôts.gouv et gérer son abonnement téléphone en ligne pour "les moins à l'aise"

Note : résultats issus de l'analyse quantitative
Source : Analyses BCG & EY-Parthenon

Les situations pour lesquelles la sécurité de la procédure d'identification est la plus importante sont également globalement les mêmes

Quelles sont les 3 situations pour lesquelles la sécurité de la procédure d'identification est la plus importante parmi les 25 ci-dessous ?
(top 6 des situations les plus fréquemment citées)



4 des 6 situations où la sécurité est la plus importante sont communes :

- Renouveler CNI / passeport
- Faire un virement élevé
- Accéder à son compte impôts.gouv
- Passer les contrôles à l'aéroport

Quelques différences :

- Ouvrir un compte bancaire et demander un crédit en ligne pour "les plus à l'aise avec le digital"
- Accéder à son compte Améli et demander une carte grise pour "les moins à l'aise"

Note : résultats issus de l'analyse quantitative
Source : Analyses BCG & EY-Parthenon

FranceConnect est connu par la moitié des répondants, avec une intention qui répond bien aux irritants mis en avant mais reste mal comprise

48% répondants ont déjà entendu parler de FranceConnect

> "J'ai entendu parler de FranceConnect mais **je n'ai pas bien compris de quoi il s'agit**. Ca rassemble tous les sites administratifs ?
>
> Sandrine, 43 ans

> "L'objectif est de rapprocher différents services de l'Etat et de **les mettre sur une même plateforme**.
>
> Nahed, 33 ans

> "Ca vous permet de vous connecter sur plusieurs sites institutionnels **en liant vos comptes impôts.gouv et Améli** par exemple.
>
> Fabien, 31 ans

Constat : l'intention et les fonctionnalités de FC répondent aux irritants identifiés (unicité de l'identifiant, possibilité de partage d'informations personnelles)

Mais tous les usagers n'ont pas **compris la promesse de FranceConnect :** faciliter l'accès aux services publics

Certains usagers **confondent l'accès à différents services et la mise en commun** de ceux-ci (et des données associées)

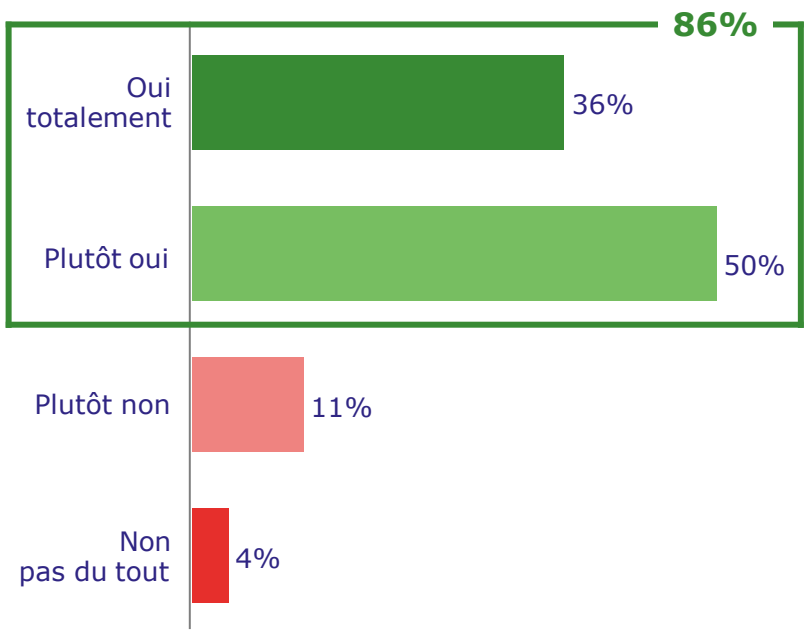
36% répondants ont déjà utilisé FranceConnect

Note : pourcentage issu de l'analyse quantitative et citations issues de l'analyse qualitative
Source : Analyses BCG & EY-Parthenon

FranceConnect, un service apprécié par 86% des répondants qui l'utilisent mais un enrôlement vu comme complexe qui freine l'inscription

Un taux de satisfaction élevé parmi les utilisateurs de FranceConnect

→ Un taux de satisfaction élevé parmi les utilisateurs de FranceConnect



Un taux de satisfaction élevé parmi les utilisateurs de FranceConnect

“ J'avais essayé de m'inscrire **mais j'ai vite lâché l'affaire.** Ils demandaient trop de choses, c'était trop compliqué.

Nahed, 33 ans

“ Il faut avoir un ordinateur pour scanner et envoyer des documents, on ne peut pas le faire depuis son Smartphone. **C'est lourd comme procédure donc j'ai vite abandonné.**

Ahmed, 34 ans

Note : pourcentages issus de l'analyse quantitative et citations issues de l'analyse qualitative
Source : Analyses BCG & EY-Parthenon

Annexe 6

Illustration de la promesse de valeur

Promesse de valeur pour les usagers (1/2)

Principes

La valeur de la promesse est dans :

- L'universalité en termes d'accès, à la fois côté secteur public et côté secteur privé
- La simplicité d'usage et des parcours plus fluides (identification, fournitures de documents, etc.)

Les deux valeurs génératrices de confiance vont être la maîtrise et la personnalisation, ce qui renvoie à la liberté de :

- Choisir les usages pour lesquels l'identification passe par la solution d'identité numérique sécurisée
- Voire de choisir le niveau de sécurité préféré pour chaque usage (que ce soit sur PC ou via un smartphone)

La capacité de l'Etat à rassurer sur la question de la gestion de la perte / du vol du support et/ou de l'usurpation de l'identité numérique va être fondamentale

Cette promesse peut se décliner sur plusieurs dimensions pour renforcer la confiance dans les technologies numériques et simplifier les démarches administratives

Source : Enquête auprès des usagers et focus spécifique sur des usagers éloignés du numérique ; analyses BCG & EY-Parthenon

Promesse de valeur pour les usagers (2/2)

Projections (non-exhaustif)

Mieux se protéger contre
les risques d'usurpation d'identité

Prouver son identité ou certains attributs, de manière certaine,
sans avoir à montrer / envoyer ses papiers (ex : ouverture de compte bancaire, sites réservés aux majeurs, …)

Faciliter l'accès
à ses droits de citoyen
(ex : vote en ligne, suivi plainte en ligne)

S'assurer de l'identité d'un interlocuteur numérique
(ex. plateformes collaboratives, télémédecine)

Bénéficier de nouveaux services en ligne
(ex. : partage direct de données, LRE, examen à distance)

Eviter un face-à-face difficile
(ex. dépôt de plainte, justification d'une réduction « chômeur »)

Eviter de se déplacer pour **gagner du temps**
(ex. : virement élevé, entretien, renouvellement papiers)

Promesse de valeur pour les fournisseurs de services

La promesse doit s'articuler autour des blocs suivants

- Un outil de lutte contre la fraude (cf. authentification d'attributs d'identité) et l'usurpation d'identité (cf. crédits à la consommation, achats en ligne) et de baisse des coûts associés (préventif ou curatif)
- Un levier de dématérialisation des démarches et de maîtrise des coûts (cf. éviter des déplacements en agences, optimiser les coûts de mise en œuvre des exigences de vérification d'identité)
- Un levier de protection des clients (et de communication sur la capacité à les protéger)
- En fonction du design et des fonctionnalités, un levier d'amélioration de l'Ux et de développement de l'usage (cf. possibilité de donner directement accès à des données ou documents personnels)
- En fonction du design et des fonctionnalités, un levier de construction de nouveaux services (ex. traçabilité des interlocuteurs sur des plateformes collaboratives)

Source : Enquête auprès des usagers et focus spécifique sur des usagers éloignés du numérique ; analyses BCG & EY-Parthenon

Promesse de valeur pour les fournisseurs de services

Deux parcours transversaux

- L'enrôlement et la mise à disposition de la CNIe (y compris pour les publics de la fracture numérique)
- La gestion d'une situation de perte ou d'usurpation d'identité

Quelques moments de vie (assez larges pour croiser des usages privés et publics et une large palette de fonctionnalités)

- Je déménage / j'achète un appartement (notaire, prêt, assurance, etc.)
- J'ai un problème de santé (gestion du DMP, admission dans un centre hospitalier, accès aux résultats d'analyse, télémédecine post-opératoire, etc.)
- Je change d'emploi / je me forme (certification des diplômes et des acquis professionnels, entretien, accès à l'entreprise, entretiens / examens à distance, etc.)

Des fonctionnalités

- Je donne accès à mes données personnelles de façon sélective à certaines administrations ou à certains fournisseurs de service privés
- Je gère en ligne des démarches importantes pour un de mes proches

Source : Enquête auprès des usagers et focus spécifique sur des usagers éloignés du numérique ; analyses BCG & EY-Parthenon