RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

DOUANES & DROITS INDIRECTS

BP1I22V1

CONCOURS INTERNE

POUR LE RECRUTEMENT DE CONTRÔLEURS DES DOUANES ET DROITS INDIRECTS

BRANCHE DU CONTRÔLE DES OPÉRATIONS COMMERCIALES ET D'ADMINISTRATION GÉNÉRALE

SPÉCIALITÉ « TRAITEMENT AUTOMATISÉ DE L'INFORMATION – PROGRAMMEUR »

SESSION 2022

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N° 1

(DURÉE : 3 HEURES – COEFFICIENT 2)

RÉPONSE À DES QUESTIONS ET/OU CAS PRATIQUE SUR UN SUJET A CARACTÈRE ADMINISTRATIF À PARTIR D'UN DOSSIER AFIN D'APPRÉCIER LES CAPACITÉS RÉDACTIONNELLES DES CANDIDATS

AVERTISSEMENTS IMPORTANTS

L'usage de tout document ou matériel autre que le matériel usuel d'écriture et de tout document autre que le support fourni **est interdit**.

Toute fraude ou tentative de fraude constatée par la commission de surveillance entraînera **l'exclusion du concours.**

Veillez à bien indiquer sur votre copie le nombre d'intercalaires utilisés (la copie double n'est pas décomptée).

Il est interdit de quitter définitivement la salle d'examen **avant le terme de la deuxième heure** (arrêté du 3 mars 1997 modifié fixant les conditions d'organisation des concours et examens professionnels de recrutement dans les services déconcentrés de la direction générale des douanes et droits indirects).

Le présent document comporte **16 pages** numérotées.

Tournez la page, SVP

Sujet

À partir des documents ci-joints, répondez, sur votre copie, à chacune des questions suivantes :

Question 1 :

Définissez le terme d'identité numérique, présentez son fonctionnement, puis dressez un état des lieux. (deux pages maximum)

Question 2 :

Décrivez les acteurs du domaine de l'identité numérique et leurs rôles. (une page maximum)

Question 3 :

Affecté(e) dans une DSI, votre responsable vous demande de rédiger une note synthétique présentant les motivations de la création d'un service public d'identité numérique. (deux pages maximum).

Liste des documents :

Document 1 : **Identités numériques – Clés de voûte de la citoyenneté numérique – Extraits**

Conseil national du numérique, juin 2020

Document 2 : **Mission d'information sur l'identité numérique – RAPPORT D'INFORMATION – Extraits**

Site assemblee-nationale.fr, 8 juillet 2020

Document 3 : **LE RÈGLEMENT EIDAS - Extraits**

ANSSI (Site ssi.gouv.fr/)

Document 4 : **30 millions d'utilisateurs conquis par FranceConnect !**

Site numerique.gouv.fr, 7 octobre 2021

Document 5 : **Découvrir le service – De quoi s'agit-il ? – Extraits**

Site france-identite.gouv.fr

Document 6 : **La future identité numérique en cinq questions – Extraits**

Les Echos : Publié le 10 juin 2021

DOCUMENT 1

Identités numériques – Clés de voûte de la citoyenneté numérique – Extraits

Conseil national du numérique, juin 2020

1. L'IDENTITÉ NUMÉRIQUE : UN SUJET COMPLEXE QUI FAIT RÉAGIR LES CITOYENS

1.1. De la citoyenneté numérique au service public de l'identité numérique

Un lien entre une nation et un citoyen se retrouve en partie dans la citoyenneté. Un citoyen est défini comme personne ayant la nationalité française et jouissant de ses droits civils et politiques (par exemple le droit de vote).

La citoyenneté peut prendre de multiples formes dans le quotidien des individus : au-delà de la gestion de la population et l'allocation des prestations sociales par l'État, un pan primordial de la citoyenneté s'inscrit dans la participation individuelle et collective à la vie sociétale, politique, associative, etc.

[...]

La dématérialisation croissante des services publics ainsi que certaines conditions particulières entraînent les citoyens à accorder une part de plus en plus grande au numérique dans leurs pratiques citoyennes.

Dans ce contexte les identités numériques sont des outils essentiels pour la faire valoir en faisant perdurer le lien entre la nation et ses citoyens.

Les identités numériques peuvent bousculer les différents pans de la citoyenneté numérique tant en facilitant les formes d'expression des uns qu'en réduisant les accès à la citoyenneté des autres. De fait, l'identité numérique, qui donne accès aux droits civils et politiques, doit être en partie appréhendée, gérée et pensée comme un bien public qui doit être inclusif et accessible à tous.

1.2. L'identité numérique : une notion sibylline

L'identité est une notion complexe puisqu'il s'agit d'une notion évolutive, dépendante de l'acteur qui l'attribue ainsi que du champ dans lequel cette attribution est faite. Liée avec le terme numérique, elle fait référence en premier lieu à l'identifiant (par exemple nom d'utilisateur), choisi pour ou par le détenteur et permettant – souvent associé à un mot de passe – d'accéder à des services (publics, privés ou professionnel, locaux, nationaux ou internationaux). L'identité numérique peut être déclarative (comme sur Twitter où le pseudo est choisi) ou imposée par le service (comme sur le site de l'assurance maladie où l'identité se fait par l'état civil), en rapport avec l'état civil ou non. Il existe alors une multiplicité d'identités numériques propres aux pratiques numériques de chaque individu.

En second lieu, l'identité numérique peut aussi être perçue comme le reflet des comportements en ligne des individus : soit l'ensemble des traces (données, métadonnées) qu'un individu peut laisser en surfant sur internet, et qui permettront de définir une cartographie de ces comportements et de faire entrer celui-ci dans une typologie.

C'est selon le premier niveau, une identité attribuée, que l'identité numérique sera abordée dans ce rapport. Celle-ci intervient lorsqu'une relation a besoin d'un certain niveau de confiance, de certitude concernant les caractéristiques des interlocuteurs, pour perdurer. L'État est un acteur historique pour identifier les parties prenantes, de par sa prérogative régalienne de tenue à jour des actes de naissance et de décès des citoyens à travers l'état civil. [...]

DOCUMENT 2

Mission d'information sur l'identité numérique – RAPPORT D'INFORMATION – Extraits

Site assemblee-nationale.fr, 8 juillet 2020

B. LE FONCTIONNEMENT DE L'IDENTITÉ NUMÉRIQUE [...]

1. Le trinôme « utilisateur – fournisseur de services – tiers de confiance »

L'identité numérique, comprend une phase d'identification puis d'authentification faisant intervenir trois figures clefs : l'utilisateur, le fournisseur de services et enfin le tiers de confiance, ce dernier étant amené à jouer plusieurs rôles. Il convient de toujours bien distinguer l'identification, qui consiste à établir l'identité de l'utilisateur (via un identifiant unique) de l'authentification, qui permet à l'utilisateur d'apporter la preuve de son identité, selon différentes modalités en fonction du niveau de sécurité exigé. Une solution d'identité numérique permet donc à un utilisateur identifié de prouver son identité numérique, avec la solution d'authentification de son choix, qu'elle soit publique ou privée.

a. L'utilisateur

L'utilisateur est la personne physique souhaitant accéder à un ensemble de services aussi bien publics (effectuer une déclaration de revenus en ligne, par exemple), que privés (achats de biens et services). Il recherche en général la facilité d'accès au service et la protection de ses données personnelles, afin de se prémunir de toute tentative d'usurpation d'identité.

b. Le fournisseur de services

Le fournisseur de services est l'opérateur public ou privé qui met à la disposition de l'utilisateur un ensemble de services en ligne. L'accès à ces derniers est en général conditionné à une authentification de l'utilisateur. Cette phase passe, le plus souvent, par la création d'un compte utilisateur unique, propre à ce service et à ce fournisseur, ce qui a pour conséquence de multiplier les identités numériques des utilisateurs.

Cette authentification voit son niveau de sécurité varier en fonction de la nature du service proposé. Elle reste néanmoins, à l'heure actuelle, une authentification faiblement sécurisée pour la plupart des sites internet des fournisseurs de services. Le fournisseur de services dispose assez rarement des moyens de vérifier la véracité des attributs présentés par l'utilisateur dans sa phase de création d'accès et de connexion à distance au service proposé.

c. Le fournisseur d'identité – tiers de confiance

Le fournisseur d'identité, qui est un tiers de confiance, va permettre de faire le lien entre le fournisseur de services et l'utilisateur. Sa fonction est de s'assurer de la correspondance entre les attributs présentés par l'utilisateur et leur véracité.

Il existe en France des acteurs économiques spécialisés dans le domaine de la vérification de l'identité électronique. Ces derniers appartiennent au secteur économique dit « de la confiance numérique », et sont représentés au sein de l'Alliance pour la confiance numérique.

Le tiers de confiance peut assurer les trois fonctions différentes, distinctes ou cumulées suivantes :

– autorité de délivrance (ou fournisseur d'identité originelle) : le tiers de confiance fait alors le lien initial entre la personne physique ou morale et son identité numérique. Il attribue l'identité numérique originelle. À titre d'exemple, l'autorité de délivrance de la carte nationale d'identité électronique (CNIe) est l'État, et plus spécifiquement l'Agence nationale des titres sécurisés (ANTS), placée sous la tutelle du ministère de l'Intérieur. La délivrance en mairie, qui intervient après la validation du dossier au niveau de la préfecture (centre d'expertise et de ressources titres) permet ainsi de faire le lien initial entre l'identité physique de la personne et son identité numérique ;

– fournisseur d'identité authentifiée : le tiers de confiance assure alors la gestion au quotidien de cette identité et procède à sa confirmation auprès du fournisseur de services. Le fournisseur d'identité confirme donc auprès du fournisseur de services, les attributs « de base » que prétend détenir l'utilisateur du service. L'identité donnée au fournisseur de services dérive nécessairement d'une identité originelle ;

– fournisseur(s) d'attributs : le tiers de confiance fournit alors des attributs supplémentaires concernant l'utilisateur, afin de garantir un niveau d'authentification plus fortement sécurisé. Ce peut être, par exemple, l'exercice d'une profession, ou la valeur d'un revenu fiscal. [...]

2. Les trois phases de la vie d'une identité numérique : enrôlement – authentification – utilisation

a. L'enrôlement

L'utilisation d'une solution d'identité numérique passe par une première phase dite d'enrôlement (de l'anglicisme *enrolment*) qui correspond de facto à l'inscription. C'est le moment où l'autorité de délivrance, qui peut également être le fournisseur d'identité, établit de façon certaine le lien entre l'utilisateur et son identité numérique (c'est-à-dire la somme de ses attributs).

Le niveau de sécurité requis fait logiquement varier les conditions encadrant cette phase d'inscription (voir infra). L'enrôlement peut ainsi simplement comprendre la fourniture d'un identifiant, d'un mot de passe, d'un numéro de téléphone et d'une adresse mail (Facebook), ou comporter des éléments plus complets pour assurer un niveau de sécurité plus élevé, tels que l'usage d'un titre d'identité, certifié par exemple (Alicem).

La phase d'enrôlement est donc une étape essentielle pour garantir la sécurité de l'identité numérique délivrée, mais aussi son déploiement à grande échelle. Le processus d'enregistrement doit en effet être suffisamment fluide et robuste pour que l'utilisateur souhaite aller jusqu'à son terme. [...]

b. L'authentification

Une fois enregistrée, la personne est en capacité de s'authentifier et donc d'accéder aux services via l'usage de son identité numérique. L'authentification désigne le fait de produire la preuve de l'identité présentée a priori, en vue d'accéder à un service. Elle est donc un processus qui permet de confirmer l'identité d'une personne, qui ne doit pas être confondu avec l'identification, qui permet de déterminer l'identité de quelqu'un à partir d'un ensemble d'attributs.

Cette phase d'authentification, moins lourde que celle d'enrôlement, varie elle aussi en fonction de la nature du service demandé et donc de l'utilisation de l'identité numérique. Dans le cadre envisagé de la dérivation d'une identité numérique à partir de la carte nationale d'identité électronique (CNIe), l'utilisation de ce titre d'identité serait par exemple nécessaire uniquement pour des usages d'un niveau de sécurité élevé. Pour les usages d'un niveau faible ou substantiel, le smartphone seul suffirait.

c. L'utilisation

L'utilisation de l'identité numérique consiste à s'appuyer sur son identité numérique pour accéder à un ensemble de services, une fois l'authentification réussie. L'avantage d'une identité régalienne réside dans la robustesse des données utilisées pour créer l'identité numérique (l'État faisant office en l'espèce d'autorité de délivrance et de fournisseur d'identité) et dans la confiance que peuvent lui accorder les citoyens au regard de son rôle de garant de l'intérêt général.

L'utilisation d'une identité numérique régalienne passerait par l'utilisation du fédérateur d'identité FranceConnect. On désigne, par le terme de fédérateur d'identité, un environnement organisé utilisant des systèmes d'identités numériques, sous forme de plateforme, permettant de gérer un ou plusieurs schémas d'identités.

Très concrètement, utiliser son identité numérique régalienne nécessitera, dans le cadre d'une dérivation de la CNIe, de recourir soit au smartphone et à ce titre d'identité (authentification de niveau élevé), soit au seul terminal de l'utilisateur, pour des usages ne requérant qu'un niveau de sécurité simple ou substantiel.

Il peut être mis fin à cette utilisation par simple déconnexion du service concerné. En cas de perte ou de vol du smartphone, l'utilisateur doit se créer une nouvelle identité numérique afin de faire expirer son identité numérique précédente. [...]

DOCUMENT 3

LE RÈGLEMENT EIDAS – Extraits

ANSSI (Site ssi.gouv.fr/)

Le Règlement « eIDAS » n°910/2014 du 23 juillet 2014 a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur. Il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

Le règlement eIDAS concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne. Il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il couvre notamment le sujet de la signature électronique, et abroge la directive 1999/93/CE. L'ANSSI est l'un des organismes nationaux chargés de la mise en œuvre de ce règlement. [...]

CHAMP D'APPLICATION ET DESTINATAIRES

Le règlement eIDAS s'applique à l'identification électronique, aux services de confiance et aux documents électroniques. Il vise à établir un cadre d'interopérabilité pour les différents systèmes mis en place au sein des États membres afin de promouvoir le développement d'un marché de la confiance numérique.

Le règlement formule des exigences relatives à la reconnaissance mutuelle des moyens d'identification électronique ainsi qu'à celle des signatures électroniques, pour les échanges entre les organismes du secteur public et les usagers. Il exclut les échanges internes des administrations sans impact direct sur les tiers ainsi que les actes sous-seing privé.

PRINCIPALES MESURES DU RÈGLEMENT

Le règlement eIDAS est essentiellement consacré à l'identification électronique et aux services de confiance. Il traite également, dans une moindre mesure, des documents électroniques en leur accordant un effet juridique.

L'ANSSI intervient à double titre dans l'application du règlement : en tant que garante de la sécurité pour le volet « identification électronique » et en tant qu'organe de contrôle pour le volet « services de confiance ».

Identification électronique

Objectifs et principes du chapitre « identification électronique » du règlement

Le règlement eIDAS vise à instaurer un mécanisme de reconnaissance mutuelle des moyens d'identification électronique des États membres sur l'ensemble des services en ligne des autres États membres.

[...]

Les exigences applicables aux différents niveaux de garantie qui sont prévus par le règlement sont détaillées dans le règlement d'exécution n°2015/1502 du 8 septembre 2015. Ces niveaux sont accordés en fonction du respect de spécifications, normes et procédures minimales. Trois niveaux de garantie sont prévus par le règlement :

- Faible : à ce niveau, l'objectif est simplement de réduire le risque d'utilisation abusive ou d'altération de l'identité ;

- Substantiel : à ce niveau, l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité ;
- Élevé : à ce niveau, l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

La reconnaissance mutuelle des moyens d'identification électronique est devenue obligatoire le 29 septembre 2018.

Organismes nationaux compétents

En France :

- la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC)[1] assure le rôle de point de contact unique en matière d'identification électronique ;
- l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est responsable de l'établissement du référentiel des exigences applicables à chaque niveau ainsi que de l'évaluation du niveau de garantie des moyens d'identification électronique.

[...]

1 Remplacée depuis le 25 octobre 2019 par la direction interministérielle du numérique (DINUM).

DOCUMENT 4

30 millions d'utilisateurs conquis par FranceConnect !

Site numerique.gouv.fr, 7 octobre 2021

FranceConnect facilite désormais l'accès aux démarches en ligne de plus de 30 millions de Français. Services numériques de l'État, de collectivités ou du secteur privé : le fédérateur d'identités mis en place par l'État est la clé d'entrée vers plus de 1000 démarches du quotidien, et poursuit son accélération.

FranceConnect est le service d'identification en ligne proposé par l'État, créé et opéré par la direction interministérielle du numérique (DINUM), sous l'autorité de la ministre de la Transformation et de la Fonction publiques.

5 ans seulement après son lancement, il a atteint et même dépassé avec plus d'un an d'avance l'objectif de 30 millions d'utilisateurs fixé par le Gouvernement pour fin 2022.

Raison principale de cette nouvelle accélération ? FranceConnect est le sésame pour récupérer son attestation de vaccination anti-Covid, sur le site officiel de l'Assurance maladie attestation-vaccin.ameli.fr. Les Français y faisant appel massivement, cette nouvelle démarche FranceConnectée a permis de conquérir plus de 3 millions de nouveaux utilisateurs sur 3 mois, entre juin et août 2021.

Le nombre de connexions mensuelles moyen a quasiment doublé en un an : de 10 millions en 2020, il est passé à plus de 18 millions de connexions mensuelles à fin septembre 2021.

Et c'est là la deuxième bonne nouvelle : non seulement les Français sont de plus en plus nombreux à utiliser FranceConnect, mais ils y ont aussi recours de plus en plus souvent. Ils étaient 8 millions fin 2020 à l'utiliser plus de 4 fois par an, ils sont maintenant 12 millions, à fin septembre 2021.

« *FranceConnect s'est vraiment installé dans le paysage de l'identité numérique française.* » conclut Christine Balian, cheffe de la mission IDNUM au sein de la DINUM

Une simplicité d'utilisation plébiscitée

Si FranceConnect se taille une place de choix dans les habitudes numériques des Français, c'est principalement pour la simplicité que leur offre le service : il leur permet de se connecter à plus de 1000 services en ligne en utilisant toujours les mêmes identifiant et mot de passe, parmi ceux proposés (Ameli, impots.gouv.fr, l'Identité Numérique La Poste, MobileConnect et moi ou msa.fr), sans avoir à créer chaque fois de nouveau compte. Il leur simplifie aussi les démarches : en se connectant via FranceConnect, certaines données sont préremplies, avec leur autorisation.

Une enquête Ifop réalisée en avril 2021 auprès de 1000 personnes a montré que 83 % des utilisateurs sont convaincus par la facilité d'utilisation du service.

FranceConnect est également reconnu comme un vecteur de réassurance pour les usagers, qui sont 65 % à lui faire confiance selon le baromètre 2021 de l'Acsel[2].

2 L'Association pour l'économie numérique, préalablement nommé Association pour le commerce et les services en ligne.

1000 services FranceConnectés, publics et privés

Le nombre de services en ligne FranceConnectés continue lui aussi de progresser, et compte à la fois des services publics mais aussi privés depuis fin 2018. Des banques, des assurances, des mutuelles, des fournisseurs d'énergie, à l'instar de Boursorama ou Enedis, proposent le bouton FranceConnect depuis quelques années et continuent à rejoindre l'écosystème. Un gage de sécurité pour les services qui s'assurent ainsi de l'identité de leurs utilisateurs, mais aussi une façon d'innover et de faciliter la vie de leurs clients. [...]

FranceConnect+, pour des usages encore plus sécurisés

De nouveaux usages de FranceConnect peuvent également se développer. Grâce à une qualification obtenue auprès de l'ANSSI début 2021, FranceConnect est désormais habilité à intégrer des identités de niveau substantiel ou élevé au sens du règlement européen eIDAS, c'est-à-dire des identités encore plus sécurisées, pour des démarches plus sensibles.

« Avec FranceConnect+, l'idée est de pouvoir intégrer des services en ligne qui éviteront au citoyen d'avoir à se déplacer pour effectuer une démarche, pour prouver son identité, explique Christine Balian. Il permet aussi de donner accès à des services qui traitent des données sensibles, de santé par exemple. »

La DINUM travaille ainsi actuellement à l'intégration de FranceConnect+ pour les services de l'AP-HP ou encore pour l'espace numérique de santé. À suivre !

DOCUMENT 5

Découvrir le service – De quoi s'agit-il ? – Extraits

Site france-identite.gouv.fr

Le service public d'identité numérique est :

- facultatif
- gratuit
- accessible à tous
- activable et révocable en ligne

Une application pour prouver votre identité en ligne

Les démarches dématérialisées font aujourd'hui l'objet d'un usage massif, encore accentué avec la crise sanitaire. Dans ce contexte, le besoin d'identification et d'authentification numériques devient quotidien.

C'est pour cela que le gouvernement français a lancé en 2018 le programme interministériel « France identité numérique », sous l'impulsion des ministères de l'Intérieur, de la justice, et du secrétariat d'État au numérique chargé de concevoir et de mettre en œuvre une solution d'identification numérique pour l'ensemble des citoyens.

Pourquoi une nouvelle solution numérique ?

- Pour augmenter la sécurité sur internet
- Pour protéger les données des usagers
- Pour donner le contrôle aux citoyens
- Pour simplifier l'accès aux services en ligne
- Pour plus de services en ligne
- Pour répondre à une exigence européenne d'interopérabilité
- Pour correspondre aux acteurs institutionnels et privés

Accroître confiance et sécurité

Pseudonymes et anonymats sont monnaie courante sur le web. Cependant, pour nombre de démarches publiques et privées (demande de prestation, exercice d'un droit, mise en œuvre d'un engagement juridique ou à fort impact financier, accès ou mise à disposition de données sensibles), il est indispensable prouver son identité en ligne, ou à l'inverse, de s'assurer de celle de son interlocuteur.

Alors que les dispositifs actuels (identifiant + mot de passe) permettent l'accès à de nombreux services et données, leur sécurité reste fragile. Dans un contexte de piratages croissants, les fraudes à l'identité et les fuites de données constituent de réels risques.

L'usurpation d'identité en ligne : un risque bien réel

Selon un sondage IPSOS effectué en octobre 2020 pour le programme France identité numérique, plus d'un Français sur quatre (28 %) a fait l'objet d'une ou plusieurs tentatives de vol de son identité en ligne, au

cours des deux dernières années. Et près d'un sur cinq (18 %) a été effectivement victime d'une usurpation d'identité. Les conséquences sont multiples : d'un point de vue moral (perte de temps pour 65 %, stress important pour 46 %...), et d'un point de vue financier (751 € de préjudice moyen).

Empêcher la commercialisation de l'identité

Par ailleurs, l'identité numérique est devenue aussi un enjeu économique majeur, notamment pour les grands acteurs mondiaux du web : la commercialisation de ces précieuses données et le quasi-monopole de quelques plate-formes en matière d'authentification tendent à faire perdre au citoyen la maîtrise de ses attributs d'identité, qui conditionnent souvent l'accès à l'ensemble de ses données personnelles.

L'objectif du programme FIN est par conséquent d'offrir aux citoyens qui le souhaitent, une solution publique souveraine qui lui permette de s'authentifier en ligne et garantisse la non-commercialisation de ses données d'identité...

[...]

Un service qui s'adresse à tous

La solution en cours de développement par le programme a vocation à s'adresser à l'ensemble des citoyens et des étrangers en situation régulière. Pour ce faire, le projet prend en compte les référentiels les plus récents en matière d'accessibilité et intègre nativement une attention prioritaire à l'expérience utilisateur.

S'inscrire dans un cadre européen

En 2014, l'Union européenne a mis en place un cadre d'interopérabilité des identités numériques sécurisées, le règlement eIDAS. Son objectif est d'accroître la confiance dans les transactions électroniques au sein du marché intérieur. Il établit ainsi un socle commun et définit trois niveaux de garantie : faible, substantiel et élevé. Nombre de nos partenaires européens disposent désormais d'un dispositif d'identité numérique sécurisé : Allemagne, Belgique, Danemark, Espagne, Estonie, Italie, Pays-Bas, Portugal...

Le programme FIN, est conçu pour s'intégrer à ce cadre européen tout en respectant nos particularités administratives et juridiques (absence de registre de population, absence de numéro d'identification unique, carte d'identité facultative...) et notre forte et légitime volonté de la préservation des données personnelles.

DOCUMENT 6

La future identité numérique en cinq questions – Extraits

Les Echos : Publié le 10 juin 2021

Conçue comme un moyen de sécuriser et de faciliter les démarches en ligne, l'identité numérique pourrait devenir un outil clé au cours des prochaines années. À tel point que la Commission européenne appelle à développer une solution harmonisée à l'échelle de l'Union.

Un seul mot de passe pour effectuer toutes ses démarches en ligne. Cette phrase pourrait passer pour une belle utopie, compte tenu du nombre d'identifiants et de codes d'accès qu'il faut retenir aujourd'hui.

Mais cela pourrait devenir rapidement une réalité. Les initiatives se multiplient pour mettre en place des systèmes d'identité numérique, qui doivent permettre de s'identifier sur un grand nombre de sites. La Commission européenne s'est emparée récemment du sujet, appelant à une « identité numérique » unifiée à l'échelle de l'UE.

1. Qu'est-ce que l'identité numérique ?

Au sens large, l'identité numérique d'une personne est l'ensemble des éléments la concernant publiés sur Internet. Cela peut être des contenus postés sur les réseaux sociaux, un pseudonyme, un avatar, des commentaires, etc. Mais ce terme prend désormais une autre signification, plus institutionnelle, plus servicielle.

Dans cette optique, l'identité numérique devient une sorte de jumeau en ligne. Elle peut être directement liée à la carte nationale d'identité, qui dispose, dans certains pays, d'un volet numérique, ou reposer sur une solution développée par un organisme ou une entreprise.

Elle permettra d'obtenir un accès uniformisé et sécurisé à un maximum de services sur Internet, du paiement de ses impôts ou de ses factures d'énergie à la gestion de ses droits de formation, par exemple. En d'autres termes, il devient possible d'utiliser un même dispositif d'identification pour effectuer la majorité de ses démarches en ligne. Et celui-ci se suffit à lui-même pour prouver l'identité de l'utilisateur, qui aura donc moins de justificatifs à fournir.

2. Que veut faire la Commission européenne ?

Au cours d'un point presse, le 3 juin, la Commission européenne a proposé la mise en place d'un cadre européen portant sur l'identité numérique, avec l'idée que celle-ci soit « accessible à tous les citoyens, résidents et entreprises de l'UE ».

« Les citoyens pourront accéder à des services en ligne grâce à leur identification numérique nationale, qui sera reconnue dans toute l'Europe », ambitionne ainsi l'instance.

« L'identité numérique européenne nous permettra d'agir dans n'importe quel État membre comme nous le ferions chez nous, sans frais supplémentaires et plus facilement, que ce soit pour louer un appartement ou pour ouvrir un compte bancaire en dehors de notre pays d'origine, a déclaré la vice-présidente de la Commission, Margraethe Vestager. [...] Nous aurons ainsi une occasion unique d'approfondir ce que cela signifie de vivre en Europe et d'être européen. »

Dans les faits, cette volonté implique de rendre compatibles et de faire communiquer entre eux les systèmes d'identité numérique nationaux. « Afin que cette initiative se concrétise dans les meilleurs délais, [...] la Commission invite les États membres à mettre en place une boîte à outils commune d'ici à septembre 2022 et à entamer immédiatement les travaux préparatoires nécessaires », précise l'exécutif européen.

3. Où en est la France ?

[...]

A l'heure actuelle, il n'existe qu'une seule alternative validée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Proposée par La Poste, elle s'appuie sur France Connect, qui offrait déjà une compatibilité entre les systèmes d'identification de plusieurs plateformes institutionnelles, comme l'Assurance maladie ou Impôts.gouv.fr.

La solution proposée par le groupe public, qui comptabilise à ce jour 300 000 inscriptions, repose sur une double authentification. « À chaque fois que vous allez vous connecter sur un site, votre application Identité numérique La Poste va s'ouvrir sur votre smartphone et vous demander de confirmer l'accès via un code à quatre chiffres, ou de le bloquer si vous n'êtes pas à l'origine de cette connexion », explique-t-on du côté de l'entreprise publique.

Celle-ci revendique une compatibilité avec « 900 services publics et privés ». On retrouve notamment dans la liste l'Agence nationale des titres sécurisés (ANTS), qui sert au renouvellement des titres d'identités ou des cartes grises de véhicules, les impôts et l'Assurance maladie, donc, mais aussi l'Assurance retraite, le Compte personnel de formation, mais aussi des banques, des mutuelles, ou des fournisseurs d'énergie comme Engie ou Enedis.

4. Comment créer son identité numérique ?

La Poste propose trois méthodes différentes pour obtenir son identité numérique. La première consiste à se préinscrire en ligne, en fournissant les scans de sa carte nationale d'identité, son passeport ou son titre de séjour, puis de se déplacer en bureau de poste ou de prendre rendez-vous avec son facteur pour obtenir la certification.

La seconde se fait à 100 % en ligne. Après la préinscription, l'utilisateur reçoit par e-mail une lettre recommandée numérique, contenant le code d'activation du service. Pour l'ouvrir, il doit compléter un processus de reconnaissance faciale, qui va comparer l'image capturée par la caméra du smartphone ou de l'ordinateur à celle de la pièce d'identité. Dans ces deux premiers cas, le délai maximal entre la préinscription en ligne et la finalisation de la procédure ne doit pas excéder 15 jours.

La troisième méthode, donne quant à elle la possibilité de se rendre dans un bureau de poste sans préinscription préalable pour réaliser l'ensemble de ces opérations avec l'aide d'un chargé de clientèle.

Dans tous les cas de figure, il est impératif de disposer d'un smartphone permettant l'installation de l'application dédiée. La Poste précise par ailleurs que « les Français habitant à l'étranger pourront créer leur Identité Numérique avec un numéro portable portant un indicatif autre que celui de la France à partir de la fin juillet ».

5. Où en sont les autres pays européens ?

Selon la Commission européenne, il existe aujourd'hui 19 systèmes d'eID, utilisés au sein de 14 États membres, offrant une couverture théorique de 60 % de la population de l'UE. « Mais le décollage est lent et leur utilisation est fastidieuse », souligne l'instance.

Certains pays sont particulièrement avancés. C'est notamment le cas de l'Allemagne, qui opère déjà la liaison entre la carte nationale identité et l'identité numérique. Depuis mars, une compatibilité est d'ailleurs assurée entre les eID allemande, autrichienne et néerlandaise. L'Estonie fait également partie des États membres les plus en pointe sur le sujet.

L'UE elle-même ne va d'ailleurs pas partir de zéro pour son projet d'uniformiser les eID de ses pays membres. Depuis 2014, elle dispose d'un cadre juridique dénommé eIDAS, conçu pour sécuriser et faciliter l'identification électronique aux frontières et la certification numérique au sein de l'UE. Mais celui-ci n'a aucun

caractère contraignant pour les États membres et ne permet pas une utilisation pour des services privés ou via des appareils mobiles. Autant de points que devra régler le cadre de la future eID européenne.

IMPRIMERIE NATIONALE – 21 1527 – D'après documents fournis