MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

EXAMEN PROFESSIONNEL D'INGENIEUR PRINCIPAL DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2023 -

Mardi 21 juin 2022

SUJET : 1

Etude de cas à partir de deux dossiers techniques de trente pages maximum, soumis au choix du candidat le jour de l'épreuve écrite, permettant de vérifier les capacités d'analyse et de synthèse du candidat ainsi que son aptitude à dégager des solutions appropriées.

(Durée : 4 heures – Coefficient 1)

Le dossier technique comporte 23 pages. (hors page d'énoncé du sujet).

Il vous est rappelé que votre identité ne doit figurer que dans l'en-tête de la copie (ou des copies) mise(s) à votre disposition. Toute mention d'identité ou tout signe distinctif porté sur toute autre partie de la copie ou des copies que vous remettez en fin d'épreuve entrainera l'annulation de votre épreuve.

Si la rédaction de votre devoir impose de mentionner des noms de personnes ou de villes et si ces noms ne sont pas précisés dans le sujet à traiter, vous utiliserez des lettres pour désigner ces personnes ou ces villes (A …, B…, Y…, Z…).

IMPORTANT

1. LES COPIES SERONT RENDUES EN L'ÉTAT AU SERVICE ORGANISATEUR. A L'ISSUE DE L'ÉPREUVE, CELUI-CI PROCÉDERA À L'ANONYMISATION DE LA COPIE.
2. NE PAS UTILISER DE CORRECTEUR OU D'EFFACEUR SUR LES COPIES.
3. ECRIRE EXCLUSIVEMENT EN NOIR OU EN BLEU – PAS D'AUTRE COULEUR.
4. IL EST RAPPELÉ AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE SUR LA COPIE.

SUJET

Le ministère auquel vous êtes rattaché(e) utilise aujourd'hui des identités numériques multiples pour délivrer ses services aux utilisateurs (agents, externes, ayant droits et citoyens).

L'identité numérique revêt de nombreux formats : adresse mail, login, carte agent, matricule, etc. Cette multitude génère des risques de sécurité, des charges de travail redondantes et représente un frein à la traçabilité des accès utilisateurs et administrateurs.

Afin de pallier ces contraintes, le ministère souhaite une convergence vers une identité numérique unique (INU) de ses agents. Ce projet doit permettre d'assurer, tout au long de la vie de l'INU, la gestion en dotation des agents et en consommation des SI. Celle-ci devra être une représentation informatique unique et invariante de l'identité réelle d'une personne physique. Le projet INU est ainsi une brique indispensable à la transformation numérique du ministère.

Dans ce contexte, en tant que chargé(e) de mission « identité numérique unique » auprès du secrétaire général du ministère, vous devez lui présenter une note permettant de lancer ce projet dans les meilleures conditions. Celle-ci devra s'appuyer sur les éléments proposés dans les documents annexés au sujet mais également sur vos connaissances en la matière.

Dans cette optique, il vous est demandé de présenter les enjeux et objectifs du projet, d'en dégager les avantages, les contraintes, les risques et les impacts forts au sein des directions métiers liés à sa mise en place.

Dossier technique :

Document 1	Identité numérique La Poste Source : https://www.docaposte.com/blog/securite/definition-identite-numerique/	Pages 1 et 2
Document 2	Identité numérique sécurisée Source :https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/identite/identite-numerique	Pages 3 à 10
Document 3	La fédération d'identités Source :https://orangecyberdefense.com/fr/insights/blog/iam/la-federation-didentite/	Pages 11 à 14
Document 4	Arrêté du 8 novembre 2018 relatif au téléservice « FranceConnect » Source : Legifrance	Pages 15 et 16
Document 5	Le règlement eIDAS Source :https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/	Pages 17 à 21
Document 6	SSO Source : https://www.oracle.com/fr/security/qu-est-ce-qu-un-sso.html	Pages 22 et 23

DOCUMENT 1

Source : https://www.docaposte.com/blog/securite/definition-identite-numerique/

Qu'est-ce qu'une identité numérique et comment fonctionne-t-elle ?

Technologie en plein essor, l'identité numérique permet de simplifier et de **sécuriser les démarches en ligne** pour les utilisateurs de vos services. Entre l'amélioration de la satisfaction client et la facilitation des interactions sur votre site web, votre site mobile ou votre application, nous revenons sur la définition et le principe de **fonctionnement des différentes identités numériques**.

La définition de l'identité numérique

Qu'est-ce que l'identité numérique d'une personne ?

Une identité numérique est une solution qui permet aux internautes de **se connecter simplement à différents services en ligne**, et ce, sans avoir besoin de créer plusieurs comptes ni mots de passe.

C'est notamment ce que proposent Facebook, Google, Mobile Connect et moi, ainsi que L'Identité Numérique La Poste. Avec de telles solutions, les utilisateurs peuvent se connecter via un **identifiant unique** à plusieurs sites internet et éviter ainsi de créer un compte supplémentaire, avec diverses informations et données personnelles, lors de chaque connexion.

Une identité numérique est donc une solution pratique pour les utilisateurs, tout en étant bénéfique pour votre entreprise : elle permet de vous **différencier de la concurrence** en réduisant la frustration lors de l'entrée en relation. C'est, par la même occasion, une opportunité pour obtenir de **meilleurs taux de transformation**...

Pour les secteurs à fort enjeu réglementaire – banques et assurances notamment – des solutions comme L'Identité Numérique La Poste permettent une authentification dite « forte » qui réponde aux différentes exigences légales.

➔ Identité personnelle et identité numérique : attention à la confusion !

La notion « d'identité numérique » peut aussi désigner **tout élément permettant d'identifier une personne sur Internet**. Autrement dit : son adresse IP, ses photos, ses vidéos et ses posts sur les réseaux sociaux, par exemple.

Ce concept intéressant d'identité personnelle ne doit pas être confondu avec l'identité numérique en tant que **solution technologique servant à sécuriser l'authentification**.

Par qui sont gérées les identités numériques ?

Les identités numériques sont proposées par des **fournisseurs d'identité** : les organisations auprès desquelles un utilisateur peut créer son identité numérique.
Ces fournisseurs peuvent être **publics** (c'est notamment le cas avec votre identifiant fiscal ou le compte Ameli lié à votre numéro de sécurité sociale) ou **privés** (Facebook Connect, Google, L'Identité Numérique La Poste...). Le portail FranceConnect propose une connexion via de nombreuses identités numériques publiques.

Les deux types de fournisseurs d'identité

- Les **fournisseurs d'identité faible** : l'internaute se connecte à l'aide d'un seul type de facteur d'authentification. Il s'agit souvent d'un mot de passe.

- Les **fournisseurs d'identité de niveau de garantie substantiel** : l'internaute doit utiliser au moins deux facteurs d'authentification différents pour se connecter. Pour cela, il existe :

- les facteurs de connaissance – mot de passe, réponse à une question secrète…
- les facteurs de possession – notification envoyée sur un smartphone via une application pour confirmer la connexion –,
- et les facteurs d'identité – empreinte digitale, reconnaissance faciale ou vocale...

Les composants de l'identité numérique d'une personne

Les éléments demandés à la création d'une identité numérique

L'identification réalisée lors de la création d'une identité numérique dépend avant tout du service utilisé.

Pour les plus simples, qualifiées d'identités numériques à niveau de sécurité faible, l'identité est déclarée par l'utilisateur sans être vérifiée. Il crée donc simplement son identifiant et son mot de passe. En fonction de l'identité numérique, il peut aussi être amené à déclarer son nom, sa date de naissance, etc.

À l'inverse, la solution L'Identité Numérique La Poste est la seule reconnue comme ayant un **niveau de sécurité substantiel** (vérification d'identité et authentification forte) par l'ANSSI (Agence nationale pour la sécurité des systèmes d'information). Sa création est simple et se fait en quelques étapes, avec :

- une **inscription en ligne**, via une application ou sur le web, puis la confirmation par une authentification (vérification de l'identité déclarée) ;
- le **scan de la pièce d'identité** ;
- la **vérification** de la pièce d'identité, en face-à-face dans un bureau de poste, avec un facteur à domicile ou 100 % en ligne par reconnaissance faciale au moyen d'une lettre recommandée électronique.

Une fois l'authentification confirmée, l'identité numérique est activée : l'utilisateur n'a plus qu'à ouvrir l'**application mobile** dédiée et à choisir son propre code secret.

Les éléments permettant d'authentifier une personne en cours de relation

À chaque **connexion à un service en ligne** ou pour réaliser certaines opérations réglementées (demande de crédit, autorisation de découvert, entre autres), le fournisseur d'identité assure l'authentification de l'internaute.

Dans le cadre d'une identité numérique de niveau substantiel comme L'Identité Numérique La Poste, une notification est envoyée sur l'application de l'utilisateur et l'usage d'un code secret confirme qu'il est l'auteur de l'opération.

L'identité numérique est un gage de confiance et de sécurité… à condition qu'elle soit utilisée à bon escient et qu'elle réponde à certaines exigences incontournables. L'Identité Numérique La Poste, première en France à être **certifiée au niveau de sécurité substantiel**, est un moyen efficace d'apporter une valeur ajoutée à vos services en ligne !

Source : https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/identite/identite-numerique

Identité numérique sécurisée - Les 5 forces qui façonnent notre présent.

L'**identité numérique** s'impose comme l'une des tendances technologiques les plus répandues mondialement.

Pour un grand nombre d'acteurs publics et de citoyens, elle fait déjà partie de leur quotidien, et elle révolutionne la manière dont nous échangeons avec les institutions.

C'est maintenant au tour du secteur privé de se lancer dans l'aventure.

Dans cette étude, nous mettrons en évidence les cinq principales tendances qui vont façonner le paysage de **l'identité numérique** pour 2022 et au-delà.

Mais tout d'abord, examinons les faits marquants de la période 2016-2021 et commençons par une définition.

Qu'est-ce que l'identité numérique?

Une identité numérique est un ensemble d'attributs numériques (identifiants) et d'informations d'identification pour le monde digital, similaires à l'identité d'une personne pour le monde réel.

Habituellement émise ou réglementée par un système d'identification national, une identité numérique sert à identifier une personne en ligne ou hors ligne de manière formelle.

Elle peut inclure des **attributs** (identifiants) tels qu'un numéro, un nom, un lieu et une date de naissance, une citoyenneté, des données biométriques, etc., tels que définis par la législation nationale.

Avec des **informations d'identification spécifiques** (un numéro d'identification unique comme en Inde, un identifiant mobile comme en Finlande ou en Estonie, ou une carte eID comme en Allemagne, Belgique, Italie, Espagne ou Portugal), elle peut être utilisée pour **authentifier** son propriétaire et donc **garantir son identité**.

Ces informations d'identification peuvent également inclure un certificat électronique pour signer avec un code PIN par exemple (**donner son consentement**), sceller (**protéger l'intégrité** d'un message ou un contrat) et horodater (**associer une heure** à un acte).

On parle aussi d'identité numérique pour définir, plus largement, toutes les traces que nous laissons sur l'Internet et qui nous sont rattachées. Elles peuvent constituer un «portrait numérique» ou une représentation ou encore une identité sociale numérique qui nous caractériserait: nos intérêts, notre entourage, nos habitudes.
Notre dossier cible plus précisément l'**identité numérique régalienne**, pilotée ou supervisée par une structure nationale.

Identité numérique: les dynamiques sont enclenchées

Avant de se tourner vers le futur, repassons les années précédentes en revue. Nous aurons de bonnes pistes pour nous projeter sur 2022 - et au-delà.

1. Des programmes d'identité nationale électronique toujours plus nombreux

- Lors de la conférence **ID2020 Summit** en mai 2016 à New York, les Nations Unies lancent des discussions sur l'identité numérique, la technologie blockchain, les technologies de chiffrement et ses avantages pour les populations les plus démunies. 400 experts y partagent les meilleures pratiques et de nombreuses idées pour fournir une identité universelle à chacun.

- De nombreux **programmes nationaux d'identité électroniques** (basés sur des cartes et/ou des solutions mobiles) ont été lancés ou initiés. C'est, par exemple, déjà le cas en Algérie, en Belgique (Identité sur mobile istme), au Cameroun, en Ecuador, en Jordanie, en Italie, Philippines, Kyrgyzstan, Iran, Japon, Ukraine, au Sénégal, en Thaïlande, en Turquie et des annonces ont été faites dans ce sens aux Pays-Bas, en Bulgarie, en Norvège, au Liberia, en Pologne, en Jamaïque, au Sri Lanka.
- La plupart de ces programmes intègrent désormais la biométrie, majoritairement sous forme d'empreintes digitales.
- Des projets tels que l'initiative **Gov.UK Verify** a été introduit en 2016. En aout 2021, le gouvernement britannique a publié sa nouvelle version d'architecture de confiance.
- L'**Australie** a annoncé que la première phase de son programme d'identité numérique sera lancée d'ici le mois d'Août 2017. Plus de 6 millions d'australiens et un million d'entreprises utilisent myGovID à fin 2021.
- En **France**, tout début janvier 2020, Docaposte, filiale numérique du Groupe La Poste a annoncé l'Identité Numérique La Poste, la première identité électronique française conforme au règlement eIDAS. Le service public d'identité numérique, France identité numérique, sera lancé début 2022. Cette application sur smartphone sera disponible pour les possesseurs de la nouvelle carte d'identité française.
- L'**Allemagne** a dévoilé son plan d'identité numérique national durant l'été 2020. Tous les citoyens pourront avoir une identité électronique sur mobile dérivée de leurs cartes d'identité nationale dès septembre 2021. L'authentification se fera avec un code PIN.
- Le **Canada** progresse également avec son programme d'identité numérique fédéral appelé Cadre de la fiducie pan-canadienne piloté par le Conseil canadien de l'identification numérique et de l'authentification, un organisme à but non lucratif (DIACC). Un projet fédéral de validation de principe pour un service d'authentification unifiée par connexion appelé Sign In Canada doit démarrer à l'automne 2018.
- En **Inde**, lLe programme Aadhaar a franchi la barre du milliard d'utilisateurs en 2016. Au total, **1,3 milliard de résidents indiens** ont obtenu leur identifiant Aadhaar fin 2021. Cette identité numérique peut être obtenue sur la base des données biométriques et démographiques. L'appllication mobile mAadhaar est disponible en 13 langues.

2. Technologies et réglementations: la normalisation de l'identification numérique en marche

- Le programme d'identification pour le développement (ID4D) des Nations Unies et de la Banque mondiale a pour objectif d'offrir à chacun des habitants de la planète une **identité légale** d'ici 2030.
- Les projets de permis de conduire numérique (ou **permis de conduire sur mobile**) se multiplient dans des pays comme les États-Unis, le Royaume-Uni, l'Australie et les Pays-Bas.
- Des essais préliminaires de la **Blockchain**, une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans contrôle centralisé, se sont déroulés en Estonie, afin d'appuyer le développement d'un programme transnational novateur d'e-résidence, et au Royaume-Uni, afin d'étudier comment améliorer l'efficacité des versements des prestations sociales aux citoyens.
- Les passages aux **frontières et les aéroports intelligents** apparaissent à un rythme soutenu. Avec plus d'un milliard de passeports électroniques actuellement en circulation, et la poussée inexorable de la biométrie (notamment la reconnaissance faciale), ils offrent aux voyageurs sécurité, rapidité et transparence, lors de leurs déplacements à l'étranger.
- **L'industrie de la sécurité** a beaucoup travaillé pour améliorer les solutions IAM (Identity and Access Management) et de vérification d'identité. En particulier, les progrès de la reconnaissance faciale sont visiblement impressionnants. Grâce à l'intelligence artificielle, la précision des meilleurs algorithmes de reconnaissance faciale a été multipliée par 50 en moins de 6 ans.
- Le **règlement eIDAS**, sur l'identification et la signature électronique, est entré en vigueur en juillet 2016, et rend obligatoires l'interopérabilité des identités numériques des échanges électroniques depuis le 29 septembre 2018. Cela dit, il n'impose pas la mise en place d'un programme national d'identité numérique pour les 28 Etats membres.

- De nouvelles solutions de **portefeuille d'identité** sont sur le point de donner une forte impulsion aux systèmes d'identification numérique dans le monde entier. Cette technologie récente définit une application mobile sécurisée pour stocker des versions numérisées et cryptées de documents d'identité (carte d'identité, permis de conduire, carte de santé, etc.).

  En d'autres termes, les citoyens peuvent avoir toutes leurs informations d'identification à portée de main. De tels portefeuilles permettent aux citoyens de prouver leur identité et leurs droits en ligne et en face à face. Surtout, le portefeuille permet au détenteur de partager ce qui est nécessaire pour vérifier une transaction et rien de plus. En effet, dans de nombreux cas d'utilisation, un attribut ou un droit particulier est juste nécessaire – l'âge, l'adresse, le droit de vote (citoyenneté) ou le bénéfice d'un programme d'aide sociale.

- A fin 2020, **19 schémas d'identité numérique** sont interopérables en Europe dans 15 pays: Allemagne, Belgique, Croatie, Danemark, Estonie, Italie, Espagne, Lettonie, Lithuanie, Luxembourg, Pays-Bas, Portugal, République Tchèque, Slovaquie, Royaume-Uni.
- En juin 2021, la Commission européenne a suggéré de créer un **portefeuille numérique personnel** (ID wallet) pouvant être utilisé dans toute l'UE par plus de 80 % de la population de l'UE d'ici 2030.

3. Émergence de nouvelles normes pour assurer compatibilité et interopérabilité

- Un nouveau groupe de travail de l'OACI sur les **certificats de voyage numériques** a été créé, piloté par l'Australie.
- Le sous-groupe Logical Data Structure 2 du Groupe de travail Nouvelles technologies de l'OACI a entamé la phase de conception de la norme LDS2, « l'avenir du passeport électronique ».
- Le comité technique n°14 de l'ISO SC17 WG10 a débuté ses travaux sur les normes de vérification pour le **permis de conduire mobile** et a défini le périmètre de la vérification hors ligne. Nous avons vu en 2018/2019 des ébauches de spécifications de vérification hors ligne et en ligne (ISO/IEC 18013-5).
- Les tests d'interopérabilité de cette norme ISO/IEC 18013-5 entre 2018 et 2021 ont permis de la **finaliser** en septembre 2021. Cette norme ISO devient une référence pour toutes les initiatives de modernisation des documents.
- Le groupe de travail sur **l'identité mobile** de l'IATA a été constitué en 2016 et a débuté ses travaux en 2017. En décembre 2020, l'IATA a lancé son Travel Pass.
- L'organisme américain de normalisation, le National Institute of Standards and Technology (NIST) a précisé ses recommandations (NIST SP 800-63-3) en aout 2021.
- En outre, des **alliances industrielles** ont défini et standardisé la cryptographie et les protocoles dans des cadres et des technologies tels que OpenID connect, l'authentification Web W3C (FIDO2) et les JWT. Ces briques techniques peuvent aider à initier des écosystèmes d'identité numérique robustes.

Identité numérique: les 5 tendances à suivre

Toujours dans la même dynamique de ces dernières années, les changements s'accélèrent grâce aux acteurs publics et leurs partenaires.

ABI research prévoit que 850 millions de citoyens disposeront d'une identité numérique mobile d'ici 2026.

Nous pensons que ces changements sont essentiels pour les autorités qui veulent faire de l'identité numérique (et des services en ligne de confiance - en particulier des services mobiles) une des clés de la transformation numérique.

Pour synthétiser, nous nous attendons à :

1. Davantage de **mobilité et d'accès à l'Internet**
2. Une **accélération de l'usage de l'identité numérique favorisée par l'explosion des services en ligne** due à la Covid19
3. Le besoin accru de **sécurité** et de confiance
4. Une demande croissante pour une gouvernance publique **des systèmes** d'**identification numérique**
5. Une augmentation des **programmes d'identité numérique régalienne**

Examinons ces cinq forces.

1. Première force: la mobilité prévaut en termes de communication

Les identités seront de plus en plus mobiles.

Inutile d'être un expert pour remarquer que nous sommes désormais passés à l'ère de la connectivité mobile.

Cette tendance n'est pas sur le point de fléchir.

Et les conséquences sur l'identité numérique sont considérables.

Voici quelques faits à retenir :

- Plus de 5 milliards de personnes ont accès à Internet en 2021.
- 50% du trafic internet est mobile à fin 2020 selon Statista.
- 65% de la population sub-saharienne aura un smartphone en 2025.
- Google, qui s'est toujours intéressé aux avancées technologiques, est en train de miser sur un **modèle entièrement mobile.**

La leçon à tirer pour l'ensemble des acteurs de l'identité numérique est claire: adoptez des solutions privilégiant le monde mobile.

2. Deuxième force: une accélération vers les services numériques

La pandémie a accéléré la tendance vers le numérique et booster l'usage de l'identité numérique en particulier.

Prenons deux exemples :

- **Italie**. En un an et demi, le nombre d'identités numériques délivrées par le dispositif national italien a explosé à 27 millions en décembre 2021 - contre 8 en juin 2020 - selon AGID (Agence pour le numérique en Italie.)
- **France**. Plus de 32 millions d'utilisateurs (contre 14 millions mi-2020) utilisent régulièrement FranceConnect pour s'authentifier et accéder à plus de 900 services en ligne en décembre 2021.

Non seulement de plus en plus de gouvernements peuvent délivrer à leurs citoyens un identifiant mobile de confiance, mais, ils peuvent aussi accélérer la dématérialisation des services publics.

Gartner prévoit d'ailleurs que, d'ici 2023, plus de 60 % des gouvernements auront triplé les services numériques aux citoyens.

- **Au Danemark**, NemID (bientôt appelé MitID), le système national d'identification numérique, atteint désormais 100 % d'adoption. Il est devenu obligatoire pour accéder aux services d'e-gouvernement du pays. Bien entendu, le dispositif a été conçu pour être inclusif en premier lieu et, à ce titre, offre des moyens d'authentification spécifiques aux personnes âgées, par exemple.

La pandémie offre donc une opportunité de changement systémique.

Dans son rapport de mars 2021, Gartner déclare que l'**identité numérique régalienne** est l'une des principales tendances qui peuvent transformer les services publics dans les mois à venir. Gartner prévoit que des normes émergeront d'ici 2024 et faciliteront l'exploitation de la technologie.

La pandémie mondiale a fait passer l'identité numérique de «pratique» à « indispensable » pour les gouvernements.

Conclusion: La pandémie est aussi une opportunité de transformation et de développement des identités numériques fortes.

3. Troisième force: la garantie de sécurité reste un impératif pour tous

L'identité est, par essence, le trait d'union qui réunit l'individu et le collectif.

Pour les pouvoirs publics, le principal défi à relever sera d'harmoniser les liens numériques qui sécurisent les relations entre les nouvelles identités régaliennes et la société au sens large.

La seule manière d'atteindre cet objectif est d'instaurer un **cadre de confiance**, garantissant la protection et la sécurité des données personnelles.

La période 2016-2021 a confirmé, une fois de plus, que les exigences de sécurité accrue et de lutte contre la fraude, la protection des données et de l'identité des citoyens, sont généralement bien acceptées par les citoyens.

Ce sont bien sûr des sujets régaliens par excellence.

Pour répondre à ces nouveaux besoins en matière de **confidentialité**, la prochaine génération d'identification mobile arrive sur le marché sous la forme d'un portefeuille d'identification numérique.

Soulignant l'importance de ce changement, Gartner a positionné les « Portefeuilles d'identité pour les citoyens » au sommet de sa vague de technologies pour l'eGouvernement en 2021.

Qu'est-ce qu'un portefeuille d'identité numérique exactement ?

Il s'agit tout simplement d'une solution mobile qui permet aux citoyens de stocker, gérer et divulguer de manière sélective des données liées à l'identité provenant de différentes sources et à d'autres fins.

Par exemple, la norme ISO 18013-5, qui définit les spécifications des documents mobiles, repose sur des principes de **confidentialité dès la conception** et donne aux citoyens le pouvoir de sélectionner l'attribut d'identité qu'ils souhaitent partager sans divulguer leur identité complète.

Les schémas d'identité décentralisés et les normes d'informations d'identification vérifiables du W3C tentent également d'atteindre le même objectif, en donnant plus de contrôle aux citoyens sur leurs données.

Les derniers mois ont vu une avalanche de nouvelles réglementations concernant la protection de la vie privée dans le monde entier.

Puisque la confiance en l'autre est au centre de la construction sociale, peut-on vraiment s'étonner que la modernisation de l'identité et de l'identification soient des thèmes majeurs?

C'est à la lumière de ces attentes qu'il faut aussi comprendre la force du RGPD (Règlement Général de Protection des Données), le texte de référence en matière de protection des données de l'Union européenne.

Oui, une seule loi protège près de 500 millions de personnes depuis mai 2018.

Et cette tendance est confirmée de part le monde.

- En Inde, la Cour suprême a confirmé en août 2017, que la protection des données est un droit fondamental.
- Le Brésil a, depuis août 2020, une loi cadre regroupant plus de 40 textes, la LGPD (pour « Lei Geral de Proteção de Dados »)
- La Californie vient de se doter d'un cadre juridique proche du RGPD avec deux lois (CCPA et CPRA) : l'une en vigueur depuis le 1 janvier 2020 et l'autre à partir de Juillet 2023. Ces textes serviront sans doute de modèles pour une loi fédérale (2021). Ils ont potentiellement une importance aussi grande que le RGPD européen.
- La Chine a validé son nouveau cadre de protection des données personnelles. Largement inspiré du RGPD, selon Le Monde, il est entré en application le 1er novembre 2021.

Pour en savoir plus, voir notre dossier sur la protection des données (en anglais).

Nous assistons depuis 2018 à l'émergence d'un consensus global.

Son principe est simple: la mauvaise gestion des informations personnelles ne sera pas tolérée. Les entreprises ou organisations privées et publiques qui ne protègent pas correctement les données pourront se voir infliger de lourdes amendes.

Points importants à retenir :

- Les citoyens sont non seulement prêts à accepter, mais souhaitent et exigent une sécurité accrue.
- La période actuelle offre une **occasion unique aux pouvoirs publics** de revitaliser le lien fondamental qui les unit aux citoyens. Ils prouveront ainsi que la **confiance collective** n'est pas une relique du passé, mais un symbole identitaire puissant.

4. Quatrième force: la gouvernance publique est essentielle pour soutenir la croissance de l'économie numérique

Confrontés à une situation économique et sociale parfois tendue, les gouvernements sont inévitablement à la recherche de nouvelles opportunités pour une croissance harmonieuse et durable.

Avec la mise en place d'un environnement réglementé, une collaboration étroite entre le monde de la finance, les pouvoirs publics, à l'échelle nationale et locale, et les opérateurs de communication numérique permettra la création de solutions efficaces et la mise en œuvre des meilleures pratiques.

Bien entendu, ces nouveaux débouchés ne sont pas une conséquence directe de l'identité numérique, mais de la multitude d'applications qui en découleront.

C'est une des conclusions du rapport d'information sur l'identité numérique en France présenté en juillet 2020 à l'Assemblée Nationale.

Il préconise aussi : *"Une identité numérique gratuite pour les citoyens et les fournisseurs de services publics mais payante pour les acteurs privés."*

En d'autres termes, ce n'est pas la vente d'identités numériques mais bien les services de confiance et leurs nouvelles opportunités qui en assureront le modèle économique.

C'est là où les banques, les assurances, et autres opérateurs pourront constater un **retour sur investissement.**

Comme nous l'avons déjà souligné, l'identité numérique sécurisée est désormais une réalité technique.

L'accent sera donc mis sur l'adoption de nouvelles structures et réglementations indispensables pour régir les services et transactions associés.

Qu'est-ce que cela signifie en pratique ?

Le rôle des pouvoirs publics consistera à :

1. Créer une dynamique nationale
2. Soutenir et coordonner les investissements publics, sans lesquels les transformations des collectivités locales ne pourraient opérer efficacement
3. S'assurer que ces multiples **initiatives locales** déboucheront sur une large palette de solutions cohérentes et interopérables: où qu'ils se trouvent, les citoyens mobiles auront besoin de se référer à des modes de services similaires.

5. Cinquième force: Plus d'initiatives nationales et de lancements

Au cours de ces années, le marché suivra ces initiatives.

Comment pouvons-nous en avoir la certitude ?

En raison des preuves de plus en plus nombreuses de l'adhésion à l'identité numérique forte et aux services associés.

Elles nous signalent clairement, depuis l'introduction de ce concept il y a une quinzaine d'années, que nous sommes arrivés à une étape charnière.

Une identité numérique pour tous les Européens

Dans sa proposition de juin 2021, la Commission européenne a spécifiquement suggéré de créer un **portefeuille d'identité numérique**, en anglais « digital id wallet ».

Selon ce rapport, les identités numériques basées sur des portefeuilles numériques stockées en toute sécurité sur des appareils mobiles sont clairement identifiées comme un élément majeur pour une solution pérenne.

Cette nouvelle pièce d'identité permettrait aux 450 millions d'habitants de l'UE d'accéder aux services publics et privés.

Pourquoi une nouvelle proposition ?

Le règlement eIDAS actuel « ne répond pas » aux nouvelles demandes du marché, selon la Commission.

Il y a plus.

L'ancienne réglementation était limitée au secteur public, complexe pour les tiers et manquait de flexibilité.

En d'autres termes, eIDAS n'a pas atteint son potentiel. Seuls 60% des résidents de l'UE ont accès à des systèmes d'identification de confiance et seulement sept systèmes d’identité sont entièrement mobiles.

En revanche, avec ce nouveau système d'identité numérique, **au moins 80% devraient utiliser des identifiants numériques d'ici 2030.**

Le portefeuille d'identité de l'UE pourrait fonctionner dans toute l'UE et inclure des attestations électroniques d'attributs tels que des pièces d'identité, des permis de conduire, des diplômes ou des certificats de santé et accéder à un large éventail de services. Ce portefeuille ne sera pas obligatoire pour les résidents.

Les portefeuilles harmonisés émis par les États membres se présenteraient sous la forme d'une application pour smartphone.

Les plateformes privées comme Facebook ou Google seraient « obligées » d'accepter le portefeuille européen d'identité numérique.

Les citoyens utiliseraient alors leur portefeuille d'identité de l'UE à la place, comme le dit Margrethe Vestager, la commissaire européenne à l'Europe numérique.

La suite?

Le projet devra être discuté avec les membres de l'UE.

Un accord sur les détails techniques est attendu d'ici l'automne 2022. Pour devenir une loi, le plan proposé devra être validé par les législateurs européens du Parlement européen.

Les États-Unis et l'identité numérique

Comme le souligne le parlementaire Bill Foster en juin 2021 : « Il est temps que les États-Unis rattrapent le reste du monde en matière d'identité numérique ».

La stratégie nationale (américaine) pour les identités de confiance dans le cyber-espace avait pourtant exploré un système plus global de fournisseurs de services d'identité interopérables (publics et privés).

Les directives normatives d'identité numérique du NIST (Institut national des normes et de la technologie), connues sous le nom de NIST SP 800-63-3 ont même été publiées dès juin 2017 avec une édition étendue en 2020 et une nouvelle version est en cours de finalisation pour 2022.

Mais l'initiative lancée par l'administration Obama a fait long feu car aucun fournisseur de services n'a adopté ce système.

Le pays manque clairement d'une stratégie globale d'identification numérique, comme l'a déclaré CSO Online (17 septembre 2020.)

Selon le site POLITICO, la loi sur l'identité numérique de 2020 revient en 2022 (Loi sur l'amélioration de l'identité numérique.)

En résumé, la conception d'un système d'identification américain cohérent devra s'attaquer aux aspects uniques de l'organisation fédérale, au rôle du secteur privé et aux problèmes de confidentialité et de sécurité.

Pour le moment, plusieurs États américains ont pris les devants et ont lancé ou envisagent de lancer des permis de conduire numériques (alias permis de conduire mobiles) avec la possibilité d'utiliser les identifiants en ligne.

DOCUMENT 3

Source : https://orangecyberdefense.com/fr/insights/blog/iam/la-federation-didentite/

La fédération d'identité

Qu'est-ce que la fédération d'identités ?

En quoi centraliser les données est essentiel pour les entreprises ? Décryptage avec notre expert cybersécurité.

Principe de base

La fédération d'identités est un concept qui vise à mettre en place une centralisation des données, et notamment des données d'identité, au sein d'un domaine informatique. Ainsi un utilisateur ne se connectera qu'une unique fois par session auprès d'une structure reconnue qui lui fournira la preuve de son identité (sous forme de jeton). L'utilisateur le présentera aux autres ressources qui souhaitent s'assurer de son identité, sans qu'il n'ait à dérouler une nouvelle procédure d'authentification. Qui dit une seule authentification (dite primaire), dit un seul mot de passe. Il est alors plus facile d'appliquer une politique de renouvellement et complexité sans se confronter aux utilisateurs récalcitrants. La fédération d'identités permet également de centraliser les données d'un utilisateur (comme son adresse mail de contact, un nom, une langue). Ces données sont appelées "attributs" et leur centralisation permet, entre autres, de les modifier plus facilement.

Les acteurs

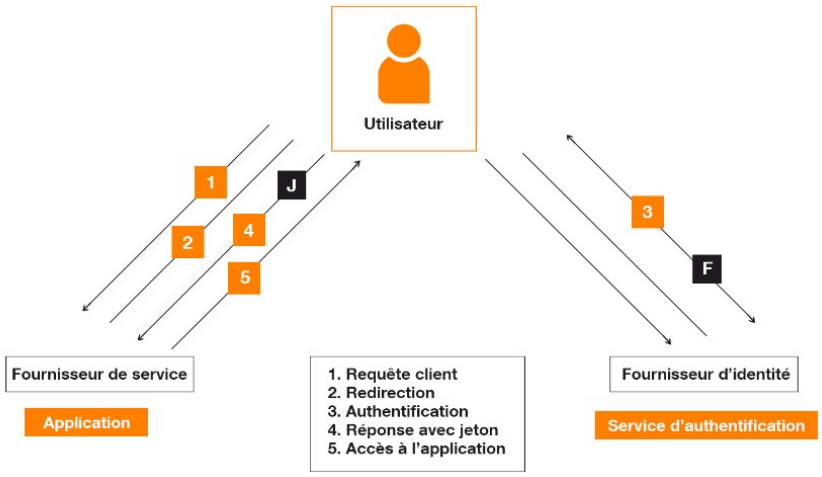
Dans un schéma en fédération d'identités, il est nécessaire de reconnaître trois acteurs et d'identifier les différents flux entre eux :

- L'utilisateur : il s'agît de la personne qui interagit via son navigateur web. Il a une unique identité numérique associée à plusieurs attributs et souhaite accéder à une application protégée.
- Le fournisseur d'identité : il est l'élément central de l'architecture. Il est chargé d'authentifier les utilisateurs. Il vérifie les facteurs d'authentification de l'utilisateur et fournit la preuve de son identité. Il est aussi en charge des autorisations d'accès aux attributs. On parle également d'Identity Provider – IdP.
- Le fournisseur de service : il s'assure de l'identité de l'utilisateur et peut avoir besoin des attributs de l'utilisateur. On parle également de Service Provider – SP.

Les flux

Ces différents acteurs interagissent entre eux pour, in fine, autoriser l'accès à l'utilisateur. Requête client, réponse avec jeton… Voici les étapes clés :

1. Requête client : l'utilisateur demande l'accès à un service protégé par une authentification ;
2. Redirection : le fournisseur de service redirige l'utilisateur vers le fournisseur d'identité pour qu'il puisse s'authentifier ;
3. Authentification : l'utilisateur s'authentifie (il justifie de son identité) à l'aide des facteurs d'authentification compatibles avec la méthode en place (login/mot de passe, clé, OTP …) ;
4. Réponse avec jeton : le fournisseur d'identité redirige l'utilisateur vers le fournisseur de service accompagné du jeton attestant de son identité ;
5. Accès à l'application : le fournisseur de service évalue le jeton et autorise l'accès de l'utilisateur.



Focus sur la vulnérabilité “CovertRedirect”

Présentation

Ces redirections rendent les flux transparents pour l’utilisateur. Or une redirection mal gérée peut être exploitée par un attaquant pour lui permettre de rediriger l’utilisateur vers un site malveillant (phishing ou téléchargement de malware). CovertRedirect n’est pas une vulnérabilité protocolaire mais bien une vulnérabilité touchant l’implémentation des protocoles qui est faite sur certains services.

L’exploitation de redirection est un problème bien connu : OpenRedirect1, vulnérabilité des redirections est classé dans le top 10 OWASP depuis 2010.

Cette faille vise les sites qui comportent des liens de cette forme :

siteWeb.com/Other/Path?redirectionVers=UneAutrePageOuUnAutreSite

Ces liens permettent aux applications d’effectuer un traitement (côté serveur) avant de rediriger l’utilisateur vers la ressource souhaitée définie en tant que paramètre dans l’URL (comme une destruction de session avant une redirection vers la page d’accueil sur un bouton « log off » par exemple).

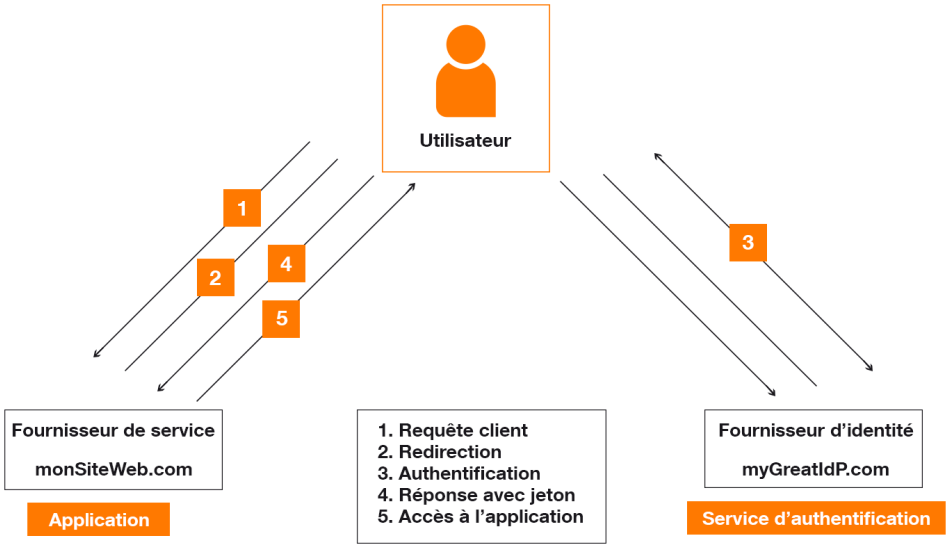
Dans la majorité des cas, ces liens proviennent d’une mauvaise conception, et leur implémentation est fortement déconseillée. SiteWeb.com peut alors servir de relais pour un phishing. par exemple, un attaquant peut forger un lien de type :

siteWeb.com/Other/Path?redirectionVers=UnSiteCorrompu.com

CoverRedirect : historique

CovertRedirect est apparu au printemps 2014, mise en évidence par Wang Jing, doctorant à l’université de nouvelles technologies de Nanyang à Singapour. L’impact de cette vulnérabilité est d’abord estimé comme important car une grande partie des géants du web seraient impliqués (GAFA, LinkedIn, Yahoo, Live, GitHub). Puis dans un second temps les spécialistes se rétractent pour finalement minimiser son impact [2].

CovertRedirect qui exploite la présence d’OpenRedirect sur des sites impliqués dans la fédération d’identités. Comment opère-t-elle ? Pour mieux la comprendre, mettons nous en situation. Un utilisateur souhaite s’authentifier sur un site monSiteWeb.com à l’aide de son identité gérée par le site myGreatIdP.com



L'utilisateur se connecte au client monSiteWeb.com [1] qui va envoyer l'utilisateur faire la demande d'authentification sur le serveur cible. Pour cela il redirige l'utilisateur [2] sur une URL de type :

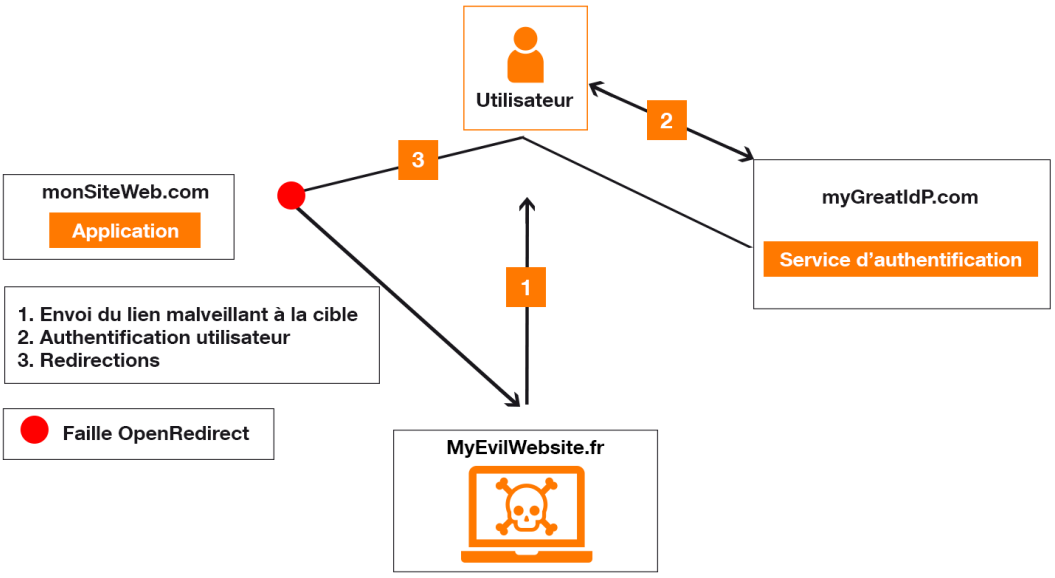
myGreatIdP.com/dialog/authen?redirect=monSiteWeb.com/UserProfile?
scope=DroitsDuJeton&client_id=11

monSiteWeb.com/UserProfile est l'adresse sur laquelle le serveur attend la réponse d'authentification.

L'utilisateur s'authentifie sur myGreatIdP.com [3] qui le redirige [4] vers :
monSiteWeb.com/UserProfile?token=ValeurDuJeton

monSiteWeb.com peut maintenant utiliser ce jeton pour identifier l'utilisateur et lui fournir l'accès demandé [5].

Maintenant dans le cas où monSiteWeb.com contient une redirection sur
monSiteWeb.com/LogOff?GoTo=HomePage.html



Un attaquant peut exploiter CovertRedirect en faisant cliquer un utilisateur sur un lien de ce type :

myGreatIdP.com/dialog/authen?redirect=monSiteWeb.com/LogOff?GoTo=MyEvilWebsite.fr/Input/
CovertRedirect&response_type=token?scope= DroitsDuJeton&client_id=11

On y retrouve :

- l'application,
- le fournisseur d'identité,
- un serveur malveillant.

C'est l'étape 1 de l'attaque.

L'utilisateur se retrouve alors sur myGreatIdP.com qui lui demande de s'authentifier pour le site monSiteWeb.com [2].
Il est alors redirigé par l'IdP vers la page de redirection monSiteWeb.com [3]

monSiteWeb.com/LogOff?GoTo=MyEvilWebsite.fr/Input/CovertRedirect?token=ValeurDuJeton

Le site fera les traitements de LogOff (destruction de session par exemple) et rédigera l'utilisateur (à cause de sa vulnérabilité OpenRedirect) vers
MyEvilWebsite.fr/Input/CovertRedirect?token=ValeurDuJeton

L'attaquant aura alors dans les logs du serveur la valeur du jeton. Il peut sous certaines conditions réutiliser ce jeton pour accéder en lecture (ou écriture parfois) aux données de l'utilisateur.

La fédération d'identités : un facteur multiplicateur d'impact ?

Dans un schéma en fédération d'identités, les murs internes au SI peuvent être vus comme plus fins, et le poids porté par l'authentification plus lourd. Ainsi, la fédération d'identités peut être vue comme un facteur multipliant les impacts d'une possible attaque. Si l'identité d'un des utilisateurs est compromise, ses accès à l'ensemble des applications du périmètre seront affectés. Si un incident intervient sur la brique d'authentification, l'ensemble de mes utilisateurs seront concernés. Il est donc essentiel de pouvoir gérer ces potentiels incidents en intégrant des mécanismes de hautes disponibilités et en renforçant la sécurité de l'authentification.

En réalité, la fédération d'identités doit plutôt être vue comme un simplificateur du SI, et les vulnérabilités structurelles ou protocolaires y sont plutôt rares. Les identités et habilitations seront administrées centralement, et les utilisateurs ne seront plus obligés de manipuler une multitude d'identifiants et de mots de passe (parfois auto-synchronisés). Ces projets nécessitent une grande implication de l'ensemble des métiers de l'entreprise, mais simplifiera l'expérience utilisateurs et pourra permettre de faire appliquer certaines contraintes de sécurité propres aux secteurs et métiers.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Légifrance
Le service public de la diffusion du droit

Arrêté du 8 novembre 2018 relatif au téléservice dénommé « FranceConnect » créé par la direction interministérielle du numérique et du système d'information et de communication de l'Etat

Dernière mise à jour des données de ce texte : 16 novembre 2018

NOR : PRMJ1819224A
JORF n°0264 du 15 novembre 2018

Version en vigueur au 21 février 2022

Le Premier ministre,
Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
Vu le règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;
Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;
Vu le code des relations entre le public et l'administration et notamment ses articles L. 112-9, L. 113-12 et L. 114-8 ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
Vu l'ordonnance n° 2005-395 du 28 avril 2005 relative au service public du changement d'adresse ;
Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
Vu les délibérations n° 2015-254 et n° 2018-164 de la Commission nationale de l'informatique et des libertés en date du 16 juillet 2015 et du 24 mai 2018,
Arrête :

Article 1

Il est créé, par la direction interministérielle du numérique et du système d'information et de communication de l'Etat (DINSIC), un téléservice dénommé « FranceConnect ».

Article 2

Le téléservice a pour finalité de proposer au public de s'identifier et de s'authentifier, auprès de partenaires, fournisseurs de téléservices et de services en ligne, au moyen de dispositifs mis en œuvre par des fournisseurs d'identité partenaires de « FranceConnect ».
« FranceConnect » repose sur une fédération d'identités et permet :
1° De simplifier des démarches et formalités administratives effectuées par le public et d'en assurer la traçabilité et le suivi ;
2° De sécuriser le mécanisme d'échange d'informations entre autorités administratives prévu par les articles L. 113-12 et L. 114-8 du code des relations entre le public et l'administration susvisés. Le téléservice assure uniquement une fonction de mise en relation des autorités administratives, sans traiter des données susceptibles d'être échangées dans ce cadre ;
3° De simplifier l'accès du public aux services en ligne proposés par les entités partenaires ;
4° Au public, d'accéder à des téléservices d'autres Etats membres en respectant les dispositions prévues par le règlement du 23 juillet 2014 susvisé, notamment les exigences relatives au niveau de garantie requis par le téléservice concerné.
L'adhésion au téléservice « FranceConnect » est facultative.

Article 3

Les catégories de données à caractère personnel enregistrées sont les suivantes :
1° Pour la gestion de l'identification de l'utilisateur :
a) De façon obligatoire :

- le sexe ;
- le nom de famille ;
- le(s) prénom(s) ;
- la date et le lieu de naissance complet ;
- l'adresse de courrier électronique ;
- le cas échéant, le numéro d'inscription de l'entreprise ou de son établissement au répertoire des entreprises et de leurs établissements (SIREN ou SIRET) vérifié et utilisé dans les conditions fixées par les articles R. 123-220 et suivants du code de commerce ;
- les clés de fédération ou « alias » générés par le système à la connexion de l'utilisateur ;
- un alias technique unique propre au système obtenu par le hachage irréversible de tout ou partie des données à caractère personnel mentionnées au présent 1°. Cet alias technique est utilisé pour les seuls besoins du téléservice. Il n'est ni diffusé ni divulgué aux tiers ;

b) De façon facultative :

- le nom d'usage ;
- le numéro de téléphone fixe ;
- le numéro de téléphone portable ;
- l'adresse de courrier électronique ;
- l'adresse postale.

2° Pour la gestion de la traçabilité des accès de l'utilisateur :

- l'adresse IP ;
- les dates et heures de connexion au service « FranceConnect » ;
- les jetons issus du mécanisme d'échange d'informations permettant de vérifier la bonne information de l'utilisateur et, le cas échéant, le recueil de son consentement.

Article 4

Les destinataires ou catégories de destinataires des informations enregistrées par le traitement sont :

- les autorités administratives partenaires habilitées à traiter les démarches et formalités des usagers en vertu d'un texte législatif ou réglementaire ;
- les personnes morales mentionnées au II et au III de l'article 1er de l'ordonnance du 28 avril 2005 susvisée qui proposent des services en ligne liés à la démarche de changement d'adresse et uniquement pour ces services ;
- les personnes morales de droit privé qui proposent des services en ligne dont l'usage nécessite, conformément à des dispositions législatives ou règlementaires, la vérification de l'identité de leurs utilisateurs ou de celle de certains de leurs attributs et uniquement pour les services qui nécessitent cette vérification.

En outre, les données enregistrées de façon obligatoire mentionnées au 1° du I de l'article 3 sont adressées à l'INSEE pour consultation du répertoire national d'identification des personnes physiques, à seule fin de certification dans le cas où l'autorité partenaire n'est pas en mesure de réaliser cette certification elle-même.

Article 5

Les données à caractère personnel relatives à la gestion de l'identification sont conservées pendant la durée de la session de l'utilisateur. Au-delà de cette durée, elles sont détruites sans délai.
Les données relatives à la gestion de la traçabilité des accès sont supprimées, en l'absence de connexion de l'utilisateur pendant une durée de six mois.
Les clés de fédération et l'alias technique unique propre au système sont supprimés, en l'absence de connexion de l'utilisateur pendant une durée de trente-six mois. Pour ce qui concerne la finalité mentionnée au dernier alinéa de l'article 2, cette durée est fixée à six mois.
Pour les autres données, la durée de conservation est corrélative à la finalité propre de chaque service en ligne partenaire.

Article 6

Le droit d'accès, de rectification et de suppression prévu par les articles 39 et suivants de la loi du 6 janvier 1978 susvisée s'exerce auprès de la direction interministérielle du numérique et du système d'information et de communication de l'Etat située au 20, avenue de Ségur, 75007 Paris, par voie postale ou par voie électronique, dans les conditions fixées dans les modalités d'utilisation du téléservice.

Source : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

Le règlement eIDAS

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.

Contexte et historique

Le Parlement européen et le Conseil de l'Union européenne ont adopté, le 23 juillet 2014, le règlement n° 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS ».

L'adoption de ce règlement fait suite à un relatif constat d'échec de la directive 1999/93/CE sur la signature électronique. Des différences dans la transposition de cette directive ainsi que dans les choix techniques effectués par les États membres n'ont pas permis l'émergence d'un socle commun d'interopérabilité nécessaire au développement des échanges transfrontaliers. Cet état de fait avait été relevé par la Commission à deux reprises en 2010, amenant le Conseil européen à demander en 2011 la création d'un marché unique numérique à échéance de l'année 2015.

En juin 2012, la Commission a initié des travaux destinés à favoriser le commerce électronique au sein de l'Union avec pour objectif l'adoption d'un règlement qui s'appliquerait directement aux Etats membres, sans transposition dans leur droit national. Plus de deux ans de discussions ont été nécessaires pour parvenir au texte définitif du règlement eIDAS.

Le règlement eIDAS a été publié au Journal officiel de l'Union européenne (JOUE) le 28 août 2014 et est entré en vigueur le 17 septembre 2014.

Le règlement eIDAS est applicable depuis le 1er juillet 2016 pour la majeure partie de ses dispositions. La reconnaissance mutuelle des moyens d'identification électronique est obligatoire depuis le 29 septembre 2018.

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.

Afin de pouvoir bénéficier de cette reconnaissance mutuelle, un moyen d'identification électronique doit :

1. Avoir été délivré conformément à un schéma d'identification électronique notifié par l'Etat membre concerné et figurant sur la liste publiée par la Commission.
   Selon le règlement, un schéma d'identification électronique est un système pour l'identification électronique en vertu duquel des moyens d'identification électronique peuvent être délivrés à des personnes physiques ou morales. Les États membres peuvent notifier des schémas d'identification électronique depuis le 29 septembre 2015.
2. Avoir un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public concerné pour accéder à ce service en ligne, à condition que ce niveau soit substantiel ou élevé.
   Cette reconnaissance mutuelle ne concerne ainsi que les organismes du secteur public qui exigent, pour accéder à l'un de leurs services en ligne, une identification électronique répondant au moins aux exigences du niveau substantiel.

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) 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.

De plus, un réseau de coopération eIDAS a été instauré par la décision d'exécution 2015/296 et rend des avis sur les différents schémas d'identification électronique notifiés par les Etats membres. Ces avis sont publics et sont disponibles via ce lien
https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Opinions+of+the+Cooperation+Network

Services de confiance

Objectifs et principes du chapitre « services de confiance » du règlement

Le règlement eIDAS a également pour objectif d'instaurer un cadre juridique pour l'utilisation des services de confiance. Il prévoit des exigences pour les services de confiance relatifs à la signature électronique, au cachet électronique, à l'horodatage électronique, à l'envoi recommandé électronique et à l'authentification de sites internet.

Le règlement établit une distinction entre les services de confiance qualifiés et les services de confiance non qualifiés. Les services de confiance qualifiés satisfont à des exigences particulières et peuvent bénéficier d'effets juridiques spécifiques. Les services de confiance qualifiés sont assurés par des prestataires de services de confiance qualifiés.

Les prestataires de services de confiance qualifiés font l'objet d'audits réguliers effectués par des organismes d'évaluation de la conformité, accrédités conformément au règlement n°765/2008 du 9 juillet 2008. Le règlement eIDAS est applicable depuis le 1er juillet 2016 pour les services de confiance.

Services de confiance qualifiés prévus par le règlement

Les services de confiance qualifiés prévus par le règlement eIDAS sont les suivants :

- Délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet ;
    - Les certificats qualifiés de signature électronique permettent d'attester de l'identité des personnes physiques auxquelles ils ont été délivrés. L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.
    - Les certificats qualifiés de cachet électronique permettent d'attester de l'identité des personnes morales auxquelles ils ont été délivrés. Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles il est lié.
    - Les certificats qualifiés d'authentification de site internet permettent d'attester de l'identité des personnes physiques ou morales auxquelles ils ont été délivrés, ainsi que du nom des sites internet correspondants.
- Validation qualifiée des signatures électroniques qualifiées et des cachets électroniques qualifiés ;
    - Un service de validation qualifié des signatures électroniques qualifiées ou cachets électroniques qualifiés permet de garantir la sécurité juridique d'une signature ou d'un cachet qualifié en fournissant une preuve de validation par un tiers qualifié.
- Conservation qualifiée des signatures électroniques qualifiées et des cachets électroniques qualifiés ;
    - Un service de conservation qualifié des signatures électroniques qualifiées ou cachets électroniques qualifiés permet d'étendre la fiabilité de ceux-ci au-delà de leur période de validité technologique.
- Horodatage électronique qualifié ;
    - L'horodatage électronique qualifié permet d'attester que des données sous forme électronique existaient à un instant donné. Un tel procédé peut être utilisé pour apposer une date d'expédition ou de réception d'un courrier mais aussi plus largement pour attester de l'existence d'une donnée à un instant, ou de la date d'un acte réalisé par voie électronique.
- Envoi recommandé électronique qualifié.
    - L'envoi recommandé électronique qualifié permet de transmettre des données entre tiers par voie électronique en fournissant des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et en protégeant ces données contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.

La création de signature électronique qualifiée « à distance » (ou « *server signing* »), lorsque le signataire ou le créateur du cachet conserve sa clé dans un équipement cryptographique mis en œuvre dans l'environnement d'un tiers, n'est pas un service de confiance qualifié au sens du règlement.

Produits qualifiés pour la signature électronique et le cachet électronique

Le règlement précise que les signatures électroniques qualifiées et cachets électroniques qualifiés sont réalisés respectivement au moyen de :

- Dispositifs de création de signature électronique qualifiés ;
- Dispositifs de création de cachet électronique qualifiés.

Au sein de chaque Etat membre, la certification de conformité de ces produits aux exigences du règlement est attestée par un organisme certificateur désigné à la Commission européenne.

Le règlement prévoit que, dans certains cas, la création de signature ou de cachet puisse être déléguée à un prestataire de services de confiance qui assure, pour le signataire ou le créateur de cachet légitime, la génération ou la gestion des données de création de signature ou de cachet. Dans ce cas, ce prestataire doit être un prestataire de services de confiance qualifié au titre de l'un des services de confiance qualifiés précités.

Organisme national compétent

En France, le rôle d'organe de contrôle pour les services de confiance est assuré par l'ANSSI. A ce titre, elle prend notamment en charge :

- la définition des modalités techniques permettant le respect des exigences du règlement ;
- la qualification des prestataires de confiance établis sur le territoire français.

En complément, l'ANSSI assure deux autres rôles prévus par le règlement :

- elle élabore et maintient à jour de listes de confiance répertoriant les prestataires de service de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent;
- elle assure la certification de conformité des dispositifs de création de signature ou de cachet électronique qualifiés.

Déclinaisons techniques du règlement

Pour ses aspects techniques le règlement eIDAS renvoie à des actes d'exécution (listés dans la partie « Référentiel documentaire lié au règlement eIDAS »).

Dans le cadre du Mandat M/460, qui est une initiative de la Commission européenne ayant pour objectif de fournir une réponse coordonnée sur le sujet du déploiement d'un marché européen digital unique, l'ETSI (European Telecommunications Standards Institute) et le CEN (Comité Européen de Normalisation) se sont vu confier la mission d'élaborer des normes relatives aux services de confiance prévus par eIDAS.

Certaines de ces normes ont déjà été publiées, d'autres sont encore en cours d'élaboration. Le cas échéant, les actes d'exécution renvoient directement à certaines normes déjà existantes.

Par ailleurs, les organismes compétents au sein des Etats membres peuvent préciser les modalités techniques permettant d'assurer le respect des exigences du règlement, pour les moyens d'identification électronique et pour les services de confiance qualifiés.

Les documents réalisés par l'ANSSI, précisant ces modalités techniques pour les moyens d'identification électronique notifiés par la France ainsi que pour les prestataires de services de confiance qualifiés en France, sont disponibles dans la rubrique dédiée.

Impacts sur le référentiel général de sécurité (RGS)

Le RGS continue à s'appliquer pleinement aux échanges entre autorités administratives.

Le RGS s'applique également aux échanges entre autorités administratives et usagers, avec une exception relative à l'obligation de reconnaissance mutuelle des moyens d'identification électronique et des signatures et cachets électroniques prévue par le règlement eIDAS.

Source : https://www.oracle.com/fr/security/qu-est-ce-qu-un-sso.html

Qu’est-ce que le Single Sign-On (SSO) ?

Le Single Sign-on (SSO) est un service d'authentification de session et d'utilisateur qui permet à un utilisateur d'utiliser un ensemble d'informations d'identification (par exemple, nom et mot de passe) pour accéder à plusieurs applications. SSO peut être utilisé par les entreprises, les petites organisations et les particuliers pour atténuer la gestion de divers noms d'utilisateur et mots de passe.

Concrètement, comment fonctionne un SSO ?

Dans un service SSO Web de base, un module agent sur le serveur d'application récupère les informations d'authentification spécifiques d'un utilisateur individuel à partir d'un serveur de politiques SSO dédié, tout en authentifiant l'utilisateur par rapport à un référentiel utilisateur tel qu'un répertoire LDAP (Lightweight Directory Access Protocol). Le service authentifie l'utilisateur final pour toutes les applications auxquelles l'utilisateur a reçu des droits et élimine les demandes de mot de passe futures pour des applications individuelles au cours de la même session.

Comment fonctionne l'authentification unique

L'authentification unique est un arrangement de gestion d'identité fédérée (FIM) et l'utilisation d'un tel système est parfois appelé fédération d'identité. OAuth, qui se prononce "oh-auth", est le cadre qui permet à l'utilisateur final d'utiliser les informations de son compte par des services tiers, tels que Facebook, sans exposer son mot de passe.

Le processus SSO

Une visualisation du fonctionnement de l'authentification unique

OAuth agit à titre d'intermédiaire au nom de l'utilisateur final en fournissant au service un jeton d'accès qui autorise le partage de certains renseignements sur le compte. Lorsqu'un utilisateur tente d'accéder à une application du fournisseur de services, ce dernier envoie une demande d'authentification au fournisseur d'identité. Le fournisseur de services vérifiera ensuite l'authentification et connectera l'utilisateur.

Risques de sécurité et SSO

Bien que l'ouverture de session unique soit pratique pour les utilisateurs, elle présente des risques pour la sécurité de l'entreprise. Un attaquant qui prend le contrôle des informations d'identification SSO d'un utilisateur se verra accorder l'accès à chaque application sur laquelle l'utilisateur a des droits, augmentant ainsi le montant des dommages potentiels. Afin d'éviter les accès malveillants, il est essentiel que tous les aspects de l'implémentation du SSO soient couplés à la gouvernance de l'identité. Les entreprises peuvent également utiliser l'authentification à deux facteurs (2FA) ou l'authentification multifactorielle (MFA) avec SSO pour améliorer la sécurité.

Social SSO

Google, LinkedIn, Twitter et Facebook offrent tous des services de SSO populaires qui permettent à un utilisateur final de se connecter à une application tierce avec ses identifiants d'authentification des médias sociaux. Bien que le Single Sign-on social soit une commodité pour les utilisateurs, il peut présenter des risques de sécurité car il crée un point d'échec unique qui peut être exploité par les pirates. De nombreux professionnels de la sécurité recommandent aux utilisateurs finaux de s'abstenir complètement d'utiliser les services SSO sociaux, car une fois qu'un attaquant a pris le contrôle des identifiants SSO d'un utilisateur, il pourra accéder à toutes les autres applications qui utilisent les mêmes identifiants.

Single Sign-on social

Apple a récemment dévoilé son propre service d'authentification unique et le positionne comme une alternative plus privée aux options SSO fournies par Google, Facebook, LinkedIn et Twitter. La nouvelle offre, qui s'appellera Sign In with Apple, devrait limiter l'accès des services de données tiers aux données. Le Single Sign-on (SSO) d'Apple améliorera également la sécurité en exigeant que les utilisateurs utilisent une authentification à deux facteurs sur tous les comptes Apple ID pour prendre en charge l'intégration avec Face ID et Touch ID sur les appareils iOS.

SSO d'entreprise

Les produits et services logiciels d'authentification unique d'entreprise (eSSO) sont des gestionnaires de mots de passe avec des composants client et serveur qui connectent l'utilisateur à des applications cibles en rejouant les identifiants utilisateur. Ces identifiants sont presque toujours le nom d'utilisateur et le mot de passe, et les applications cibles n'ont pas besoin d'être modifiées pour fonctionner avec le système eSSO.

Avantages et inconvénients du SSO

Les avantages du SSO incluent :

- Permet aux utilisateurs de se rappeler et de gérer moins de mots de passe et de noms d'utilisateur pour chaque application.
- Simplifie le processus d'ouverture de session et d'utilisation des applications - plus besoin de saisir à nouveau les mots de passe.
- Réduit les risques d'hameçonnage
- Moins de plaintes ou de problèmes concernant les mots de passe pour les services d'assistance informatique.

Les inconvénients du SSO incluent :

- Il ne traite pas de certains niveaux de sécurité dont chaque ouverture de session d'application peut avoir besoin.
- En cas de perte de disponibilité, les utilisateurs sont bloqués sur les multiples systèmes connectés au SSO.
- Si un utilisateur non autorisé obtient l'accès, alors l'accès pourrait avoir accès à plus d'une application.