fntc

Fédération des Tiers de Confiance du numérique

Identité Numérique Professionnelle :

Cas d'usage dans les processus de la facturation électronique en France

Créée en 2001, la Fédération des Tiers de Confiance du Numérique (FnTC) est aujourd'hui l'une des organisations les plus transverses de l'écosystème numérique.

La Fédération regroupe plus de 160 adhérents qui prennent une part active dans la définition, la mise en œuvre et la promotion de la confiance dans l'économie numérique : des éditeurs de logiciels, des prestataires de services numériques, des experts, des professionnels réglementés, des start-up, des institutions et des utilisateurs des services de confiance.

Cette diversité offre à la Fédération un inestimable gisement de compétences pour favoriser une digitalisation fiable et sécurisée. Avec une attention constante à l'éthique, la FnTC œuvre depuis plus de vingt ans dans les domaines historiques de la dématérialisation (signature électronique, archivage électronique, facture électronique, vote électronique, e-finance). La Fédération agit aujourd'hui également dans les secteurs montants de la digitalisation : Blockchain, KYC, Cachet électronique visible (CEV), e-santé, identité numérique...

fntc

Fédération des Tiers de Confiance du Numérique

Notre objectif : une digitalisation fiable et sécurisée.

Notre méthode :

- Produire des expertises et des outils pour que les personnes et les organisations puissent au sein du monde numérique préserver leurs droits et limiter leurs risques.
- Elaborer de la doctrine, en produisant des guides, des référentiels et des labels.
- Participer à la normalisation et à la standardisation des bonnes pratiques numériques au niveau national (Afnor) et international (ISO)
- Assurer des formations universitaires, comme les Masters Droit du numérique des Universités de Corse, de La Rochelle et de Lyon, ainsi que de la formation continue

Cette fédération est aussi la vôtre : acteur de la confiance, rejoignez-nous dans un de ses quatre collèges ou au sein de la Pépinière des start up. Utilisateur d'outils de confiance, partagez vos expériences et agissez pour votre futur dans le collège 5 des utilisateurs !

Introduction :

La réglementation sur le futur dispositif de la facturation électronique en France contraint les assujettis à émettre et recevoir les factures en BtoB sous forme et par voie électronique. Cette obligation généralisée sera applicable à compter du 1er septembre 2026, voire au 1er septembre 2027 pour les microentreprises et petites et moyennes entreprises. Dans cette perspective, le niveau d'identification et d'authentification exigé pour certaines opérations dans le cadre de la dématérialisation des factures fait l'objet de dispositions spécifiques.
Ces obligations s'inscrivent dans une dynamique plus globale de l'identité numérique dans le contexte professionnel et des niveaux de sécurité permettant de répondre aux exigences posées par les textes selon les domaines concernés.

Cet avis d'experts ambitionne de fournir les clefs pour comprendre les différents concepts mis en jeu de façon générale lorsqu'il s'agit d'identité numérique professionnelle. Il propose un panorama des différentes solutions envisageables en faisant un focus sur le cas d'usage de la facture électronique dans le cadre des accès aux différentes plateformes (Annuaire de l'AIFE, Plateforme de dématérialisation partenaire et même Opérateur de dématérialisation). Cet avis n'adresse pas directement le régime applicable en matière de sécurisation des factures électroniques.

Il se positionne comme un premier avis d'experts sur les diverses applications de l'Identité Numérique Professionnelle

Le mot du président

L'identité d'une personne est nécessaire pour identifier un individu. Elle découle de l'état civil qui agrège les éléments indispensables à l'identification à savoir le nom, le(s) prénom(s), la date et lieu de naissance. Cette nécessité d'identification permet à chaque individu d'avoir des droits mais le soumet également à des règles. Le professeur Grégoire Loiseau définit ainsi « l'identité comme l'individu vu par le droit ».

Cette dimension individuelle est fondamentale pour les autres car elle permet de connaître l'individu à qui elle permet de s'incarner dans la société.

La digitalisation de la société nécessite de créer des identités numériques. De fait dans le cadre des activités de mandataire social il est crucial d'avoir une identité numérique professionnelle qui permette de soumissionner à des marchés publics et de conclure des contrats au nom de la personne morale.

Cette notion d'identité numérique professionnelle nécessite de se fonder sur des données authentiques, afin d'éviter la fraude. Aujourd'hui l'identité numérique professionnelle a été créée en France et dans quelques pays européens. Le nouveau règlement eIDAS a pris en compte le développement de la digitalisation des entreprises dans cet esprit afin de garantir la sécurité des transactions, d'optimiser et simplifier les processus B2B et B2G, et d'éviter la fraude ; il exige une qualification renforcée.
En parallèle il crée le EUDIW (European Digital Identity Wallet), portefeuille européen d'identité numérique dans lequel les citoyens pourront stocker leurs identités numériques, et les associer à des attributs comme des diplômes, des qualifications ou permis et utiliser des services comme la signature électronique qualifiée ou l'authentification forte au sens de la directive des services de paiement. Ces attributs pourront inclure également ceux liés à l'activité professionnelle du citoyen, évoqués dans le présent document.

Bernard Bailet, président de la Fédération des Tiers de Confiance du numérique

Sommaire

De l'identité personnelle à l'identité professionnelle

1

a) Identité numérique de la personne physique

L'identité d'une personne physique est un concept essentiel en droit mais aussi dans la vie en société. N'oublions pas la fameuse phrase de Cicéron : « Ubi jus, ubi societatis » : « Là où il y a une société, il y a du droit ». L'identité ne fait pourtant l'objet d'aucune définition officielle. Des juristes ont donc tenté de l'expliquer : « ce qui fait qu'une personne est elle-même et non une autre; par extension, ce qui permet de la reconnaître et de la distinguer des autres (...) » (Gérard Cornu. Vocabulaire juridique, Quadridge/PUF, 2000, v° Identité, p. 431.).

Dans le contexte électronique, l'identité numérique est étroitement liée à trois notions définies par le Règlement européen n° 910 /2014 du 23 juillet 2014 dit eIDAS, dont la version 2 a été publiée le 20 mai 2024 :

- les ***«données d'identification personnelle»***, qui sont « un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale » (article 3 (3) du Règlement eIDAS).
- l'***«identification électronique»***, qui est définie comme « le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale » (article 3 (1) du Règlement eIDAS).
- et les ***«moyens d'identification électronique»*** (MIE), qui sont des éléments matériels et/ ou immatériels « contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne » (article 3 (2) du Règlement eIDAS).

La confiance qui sera accordée à l'identité numérique de la personne physique dépendra du niveau de garantie exigé par la loi, voire par les parties (fournisseur de service et utilisateur du service). Les différents niveaux, simple/substantiel/élevé, sont précisés dans le Règlement d'exécution 2015/1502 de la Commission européenne du 8 septembre 2015.

Dans le cadre des factures électroniques, la réforme impose aux opérateurs de plateformes de dématérialisation d'assurer un niveau de garantie substantiel des moyens d'identification électronique de la personne utilisatrice (article 242 nonies F du CGI).

Concrètement, il s'agira, par exemple, de vérifier, en face à face l'identité de la personne sur des pièces/titres de sources officielles également dites authentiques (c'est-à-dire émis par les pouvoirs publics ou sur délégation de ceux-ci), de type CNI ou passeport. De plus, la personne physique sera identifiée numériquement de façon univoque, de telle sorte qu'il soit garanti qu'elle soit la seule à pouvoir utiliser le moyen d'identité électronique qui lui aura été délivré par l'Etat (moyen d'identité régalien), par un fournisseur d'identité certifié aux niveaux eIDAS substantiel ou élevé ou par un prestataire de service de confiance privé (comme les certificats électroniques qualifiés).

b) Notion de personne morale

Selon le considérant 68 du Règlement eIDAS, les termes « personne morale » désignent « toute entité constituée en vertu du droit d'un État membre quelle que soit sa forme juridique ».
Il appartient donc à chaque Etat membre de définir ce qu'est une personne morale.

En France, aucun texte ne donne une définition des personnes morales.
Les juristes les définissent notamment comme un « groupement », « sujet de droit fictif », qui est doté d'une personnalité juridique, est titulaire de droits et obligations variables, et est soumis à un régime juridique différent selon qu'il s'agisse d'une société, d'une association, de l'Etat...

En ce qui concerne l'identité numérique des personnes morales, les définitions de «données d'identification personnelle», d'«identification électronique», et de «moyens d'identification électronique» issues du Règlement européen n°910/2014 dit Règlement eIDAS se retrouvent à l'instar des personnes physiques.

Deux précisions méritent attention :

- D'une part, les personnes morales sont représentées, directement ou indirectement, par une ou des personnes physiques ;
- D'autre part, alors que la signature électronique est réservée aux personnes physiques (article 3 (9) du Règlement eIDAS), le cachet électronique est créé par une personne morale (article 3 (24) du Règlement eIDAS).

  De plus, l'identité numérique de la personne morale est constituée de données d'identification qui lui sont propres (comme sa dénomination sociale, son numéro SIREN...) et sont identification électronique repose sur des éléments d'identification autonomes par rapport aux données d'identification de la personne physique habilitée à la représenter. L'identité déclarée de la personne morale sera notamment vérifiée sur la base de pièces/titres de sources officielles (dites authentiques ou « faisant autorité »).

c) Notion d'Activités professionnelles : rôles et mandats

Dans le cadre de ses activités professionnelles, la personne morale agira via les mandataires sociaux, seules personnes physiques juridiquement compétentes pour la représenter, ou par délégation de ceux-ci.

Pour pouvoir engager la personne morale, les personnes physiques doivent disposer des pouvoirs juridiques nécessaires pour la représenter. Juridiquement, la remise de ces pouvoirs se fait de façon formelle dans les statuts de la personne morale ou dans le cadre d'un mandat, et subséquemment de délégations de signature ou de pouvoirs.

Au-delà de la représentation des personnes morales, une personne physique peut avoir une identité numérique à titre personnel (en tant qu'individu) mais aussi en tant que professionnel. Il en est ainsi par exemple des professions libérales exercées en nom propre (médecin, avocat, notaire…). Dans de tels cas, l'identité numérique professionnelle de la personne physique devra également pouvoir être établie.

d) Vers l'identité numérique professionnelle, quel cadre juridique en France et en Europe ?

En France, l'identité numérique professionnelle ne fait encore l'objet d'aucune disposition générale. Seul le 'Référentiel d'exigences de sécurité pour les moyens d'identification électronique' établi par l'ANSSI apporte certains éléments relatifs aux spécifications exigées afin que le lien entre la personne physique et la personne morale qu'elle représente soit établi (v1.2 du 11 août 2022). Les exigences varient selon le niveau de garantie concerné.

Proposition sur les exigences minimales liées à l'identité professionnelle

Niveaux	Objectifs	Moyen d'Authentification	Processus d'Identification Personne physique	Processus d'Identification Personne morale
Niveau Faible	Limiter le risque d'usurpation ou d'altération	Disposer d'un moyen d'authentification électronique mono-facteur comme un login/ mot de passe	Vérifier l'identité de la personne physique à partir de copie des documents de référence et un contrôle simple.	Vérifier l'identité de la personne morale à partir de copie des documents de référence et un contrôle simple.
Niveau Substantiel	Limiter substantiellement le risque d'usurpation ou d'altération par des procédures et moyens renforcés	Disposer d'un moyen d'authentification électronique à base de deux facteurs, sous le contrôle exclusif de son titulaire.	Vérifier l'identité de la personne physique mandataire à partir d'une pièce d'identité de source officielle et en cours de validité.	Vérifier l'identité de la personne morale et des attributs professionnels à partir de documents originaux ou des mandats de niveau substantiel ou qualifié. Les pièces doivent être vérifiées ou contrôlées auprès d'une source officielle, si celle-ci existe.
Niveau Elevé	Empêcher le risque d'usurpation ou d'altération en renforçant les procédures et les moyens techniques	Utiliser un moyen d'authentification électronique sur deux facteurs dont l'un reposant sur un composant cryptographique qualifié par l'ANSSI.	Vérifier l'identité de la personne physique mandataire à partir d'une pièce d'identité de source officielle et en cours de validité. Toutes les sécurités des pièces doivent être vérifiées (biométrie), auprès de listes d'opposition et de sources officielles, si elles existent.	Vérifier l'identité de la personne morale et des attributs professionnels à partir de documents originaux ou des mandats de niveau qualifié ou élevé. Les pièces doivent être vérifiées ou contrôlées auprès d'une source officielle, si celle-ci existe.

Au niveau européen, le lien entre le moyen d'identification électronique d'une personne physique et le moyen d'identification électronique d'une personne morale (dit « lien établi ») est traité par le Règlement d'exécution 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du Règlement eIDAS.

Actuellement, d'un point de vue juridique, les exigences relatives à l'identité numérique professionnelle ne couvrent pas l'ensemble des spécifications nécessaires à la mise en œuvre :

elles se limitent en effet à décrire les éléments relatifs au lien établi entre le moyen d'identification électronique d'une personne physique et le moyen d'identification électronique d'une personne morale. Ces exigences devraient dans un très proche avenir être plus encadrées et précises (voir sur ce point la partie dédiée aux évolutions à venir).

Parallèlement, les législations européennes comme nationales sont en train d'étendre et de renforcer les usages des identités numériques professionnelles. La réforme de la facturation électronique s'inscrit dans cette logique.

Les obligations d'identification au niveau substantiel dans le cadre de la facture électronique

2

Diverses obligations d'authentification de l'origine des flux ou des documents sont imposées dans le cadre de la facture électronique, de son émission jusqu'à la gestion de son archivage. Nous nous intéresserons ici à l'identification des utilisateurs de l'annuaire de l'AIFE et des plateformes de dématérialisation partenaires (PDP) certifiées par la DGFIP.

a) Quels textes ?

Le Décret n°2022-1299 du 7 octobre 2022 modifié par le Décret n° 2024-266 du 25 mars 2024 encadre la mise en œuvre « pratique » de la réforme de la facture électronique. Il vient compléter les spécifications externes et différents textes sur la sécurisation des documents.

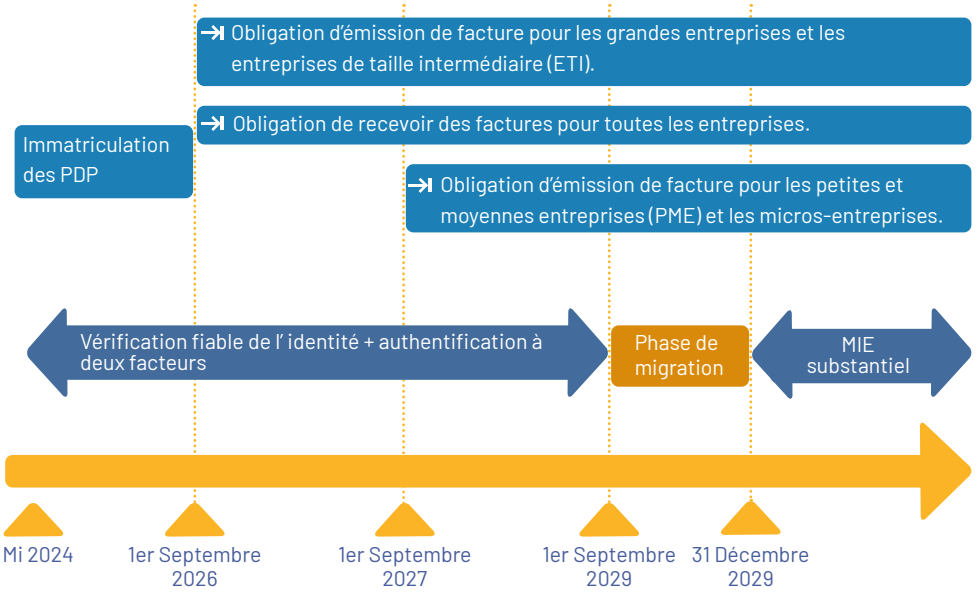
Il expose les obligations du PPF et des PDP et fixe les exigences minimales de ces obligations dans le calendrier de mise en œuvre de la réforme.

b) Quelles obligations pour quel calendrier ?

(De maintenant à 2027, puis au-delà !)

Le nouveau calendrier de la réforme a été publié au Journal Officiel le 29 décembre 2023.

Nouveau planning des PDP et niveaux d'identification / authentification (Décret n° 2024-266 du 25 mars 2024 relatif à la généralisation de la facture électronique)



« Les opérateurs de plateformes de dématérialisation partenaires assurent un niveau de garantie substantiel des moyens d'identification électronique de la personne utilisatrice au sens des dispositions du règlement d'exécution 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3 du règlement (UE) no 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 »

Mais une période de transition est instaurée jusqu'au 1er septembre 2029. Ainsi, au plus tard jusqu'au 31 décembre 2029, les PDP peuvent recourir à un autre niveau de garantie à la double condition que le dispositif mis en œuvre repose sur :

«a) Une vérification fiable de l'identité de la personne utilisatrice et de sa qualité de représentant légal, mandataire ou délégataire de l'assujetti, au moment de la création d'un compte sur la plateforme ou de l'adhésion aux services proposés par celle-ci;

«b) Un mécanisme d'authentification à deux facteurs, dont l'un dynamique .»

c) Décryptage des notions

La notion de garantie de niveau substantiel correspond aux exigences du règlement eIDAS (n°910/2014) et ces moyens peuvent être certifiés selon le « Référentiel d'exigences de sécurité pour les moyens d'identification électronique v 1.2 du 11 août 2022 » de l'ANSSI.

Le niveau substantiel se caractérise par l'équilibre entre les deux « jambes » de l'identité numérique :

- La « jambe » identification qui consiste à s'assurer de l'identité de la personne physique et, dans le cadre d'une action professionnelle au bénéfice d'une entreprise, de la réalité des droits de la personne physique à agir pour la personne morale. Dans le cas d'espèce, il faut vérifier que la personne peut réaliser des opérations, et lesquelles, liées à la facturation électronique.

Cela suppose de vérifier l'identité mais aussi les droits revendiqués comme être représentant légal ou mandaté pour agir dans ce cadre.

- La « jambe » moyen technique d'authentification permettant de garantir que c'est la personne dûment identifiée qui agit.

Cela nécessite un moyen non reproductible et une détention exclusive sous le contrôle de la personne physique agissante.

Qu'est-ce qu'un moyen d'identification électronique substantiel ?

Il se caractérise par :

- Le niveau de sécurité lors de la création de l'identité : face à face ou équivalent face à face, au cours duquel de nombreux contrôles sont réalisés (automatiques et humains) de véracité de la pièce d'identité et de concordance entre le visage du détenteur et la photo présente sur le titre

- La méthode d'authentification qui devra être effectuée à chaque usage de l'identité : elle devra faire intervenir 2 des 3 facteurs, ce que je sais, ce que je suis et ce que je possède. Actuellement, ce sont les facteurs « ce que je suis » via une App mobile ou un support cryptographique certifié et « ce que je possède» via un code personnel, qui sont les plus répandus.

La liste des moyens d'identification électronique certifiés se retrouve sur le site de l'ANSSI.

d) Comment s'assurer qu'une personne a le droit d'agir au nom d'une entité ?

Dans un premier temps, il faut toujours demander un Kbis ou un document INPI de moins de trois mois.

Si la personne physique apparaît comme représentant légal sur le Kbis, alors elle a le droit de faire toutes les opérations.

Si elle n'apparaît pas sur le Kbis, une délégation de pouvoir ou de signature, selon le cas, doit être signée par une personne juridiquement habilitée (représentant légal notamment) et vérifiée, ainsi que l'identité du délégant et du délégataire. Si la délégation est signée électroniquement, la signature électronique doit être au moins de niveau avancé avec certificat qualifié.

e) Peut-on prévoir des autorisations limitées ?

Dans le cadre particulier du dispositif français de la facture électronique, il peut être opportun de prévoir des droits spécifiques à certains utilisateurs. Ces droits seront pris en compte au niveau des PDP. La gestion de ces droits peut être intégrée aux systèmes des opérateurs ou déléguée aux opérateurs d'identités numériques professionnelles sous forme d'attributs spécifiques.

21

Plusieurs solutions possibles pour répondre aux exigences de la réglementation sur la dématérialisation des factures

3

Les différentes solutions exposées sont mises en œuvre selon la stratégie de chaque PDP, sans aucune obligation.

a) Pendant la phase intermédiaire, jusqu'au 31 décembre 2029

Associer une solution de vérification d'identité personne physique non rejouable lors de l'ouverture du compte sur la PDP et la preuve du lien avec la personne morale par un Mandat ou une Délégation à une méthode d'authentification à double facteurs qui sera utilisée à chaque accès, par la personne physique identifiée.

- Utiliser d'ores et déjà des identités personne physique de niveau eIDAS substantiel ou élevé (cf. la liste des MIE certifiés de l'ANSSI) associées à la preuve du lien avec la personne morale par un Mandat ou une Délégation.
- Utiliser des identités de niveau faible de personne physique associées à la preuve du lien avec la personne morale par un Mandat ou une Délégation, intégrant une authentification double facteur.
- Utiliser des certificats professionnels d'authentification de niveau RGS** ou des certificats qualifiés eIDAS double usage (signature et authentification).

b) Deux options, à partir du 1er janvier 2030 :

Option 1 : Utiliser des identités personne physique de niveau eIDAS substantiel ou élevé (cf. la liste des MIE certifiés de l'Anssi) associées à la preuve du lien avec la personne morale par un Mandat ou une Délégation.

Option 2 : Utiliser des identités personne morale de niveau eIDAS substantiel ou élevé. La personne morale est identifiée de façon univoque par son SIREN et éventuellement son SIRET pour plus de précision. Dans un cadre européen, le numéro de TVA intracommunautaire peut être utilisé. Dans le futur, ce sera également le cas pour le référentiel LEI (Legal Entity Identifier).

Option 1 : **L'association à la volée**

L'authentification au moyen d'un moyen d'identification électronique substantiel (MIES) ou d'un moyen d'identification électronique élevé (MIEE) de l'utilisateur sur le portail de la plateforme de dématérialisation partenaire (PDP) sera possible dès lors qu'un compte utilisateur aura été créé en amont.

La création du compte utilisateur comportera la fourniture d'un KBIS de moins de trois mois et la preuve du lien avec la personne morale par un Mandat ou une Délégation. L'utilisateur n'ayant pas de compte sera redirigé vers une procédure de demande en ligne lui permettant de déposer les pièces justificatives nécessaires.

L'utilisateur n'ayant pas de MIES ou MIEE, sera redirigé vers un portail de demande. L'obtention d'un MIES ou MIEE est totalement gratuite.

Une fois en possession de son MIES ou MIEE, et d'un compte utilisateur sur le portail de la PDP, l'utilisateur pourra l'utiliser pour s'authentifier, soit via les services de France connect +, soit en direct sur le portail de la PDP.

Option 2 : **Les Droits associés**

Le principe de « l'option 2 » est la délivrance préalable d'une identité numérique professionnelle associant une personne physique et la personne morale pour laquelle elle agit avec une codification technique des droits associés à ce lien entre la personne physique et la personne morale. Ce lien peut être issu, comme expliqué en première partie de cet avis, du rôle de Représentant Légal de la Personne physique pour la personne morale ou la conséquence d'une délégation délivrée par une personne autorisée vis-à-vis de la personne morale et accepté par la personne physique mandatée.

Pour délivrer cette identité professionnelle, l'autorité de certification (ou toute autre entité habilitée à cet effet) va s'assurer au moyen des procédures adaptées et auditées et en recourant à des sources officielles de l'authenticité des informations. L'utilisation de cette identité se fera au moyen d'un M.I.E. de niveau substantiel sous le contrôle de son titulaire ou d'un certificat numérique qualifié intégrant cette identité.

Une fois cette délivrance réalisée, le schéma de fonctionnement est le suivant :

1 -Demande d'authentification sur un PDP

2 -Interrogation du site du fournisseur d'identité

3 -Interrogation du MIE du porteur

4 -Réponse du MIE au portail d'authentification

5 -Réponse, identité et/ou attributs, du Portail d'Authentification vers la PDP

c) Proposition de format électronique de l'identité

Les acteurs de l'Identité Numérique Professionnelle travaillent sur un référentiel sémantique commun et un protocole unique pour l'ensemble des acteurs. Le principe est que ces travaux soient sous licence Open Source pour assurer l'ouverture et le développement du marché.

C'est un échange sous forme d'un jeton OpenID sécurisé qui est mis en œuvre avec une extension des spécifications OpenID Connet pour prendre en compte les besoins de la partie professionnelle.

Dans ces échanges les informations sont codifiées et sont décrites dans le référentiel sémantique. Voici un extrait des travaux réalisés au sein du Club PSCO :

Pour codifier une entreprise (actuellement au statut de document de travail) :

Attribut	Champ OIDC	Type	Obligatoire	Description
Nom de l'organisation	organization_name	String	OUI	Nom complet de l'organisation
Identifiant d'enregistrement unique de l'organisation	organization_ identifier	String	OUI	Référence d'enregistrement de l'organisation en s'appuyant sur les règles de structuration du CABForum - Exemple : NTRFR-123456789
Nom de l'établissement (OPTION)	organization_ unit_name	String	NON	Nom complet d'un établissement de l'organisation identifiée dans «organizationName»
Identifiant d'enregistrement unique de l'établissement (OPTION)	organization_ unit_identifier	String	NON	Référence d'enregistrement de l'établissement en s'appuyant sur les règles de structuration du CABForum - Exemple : NTRFR-12345678900023

Comment envisager la délégation (actuellement au statut de document de travail) :

Champs	Obligatoire	Description
delegation_sector	OUI	Secteur de référence de la délégation
delegation_nature	OUI	Nature de la délégation dans le secteur
delegation_ termination_date	NON	Date de fin de délégation
delegation_limitation_ amount	NON	Limitation en valeur financière d'engagement par acte (codifié comme : id-etsi-qcs-QcLimitValue pour un certificat qualifié)
delegation_limitation_ domain	NON	Limitation par domaine de l'engagement (définition selon le secteur)
delegation_sub_ delegation	NON	Sous délégation autorisée, un niveau, multi-niveaux
delegation_validation_ level	OUI	Niveau de validation de la délégation : Déclaratif - Certifié

Ce référentiel sémantique est indépendant de la forme des échanges et sera donc extrêmement important dans la mise en œuvre des eWallet professionnels pour inventorier et structurer les données et relations échangées.

Quelles évolutions avec eIDAS v2 ?

4

Le Règlement eIDAS n°910/2014 a été modifié par l'adoption du Règlement eIDAS 2 (n° 2024/1183). L'application des modifications ne deviendra effective qu'une fois les textes d'application prévus adoptés et selon les délais déterminés.

En attendant son application effective, deux évolutions sont à noter :

→| **Le service de confiance spécifique « certificats d'attributs »**

Compte tenu du développement des usages professionnels et des moyens d'identification électronique, le Règlement eIDAS 2 fait des « attributs » un nouveau service de confiance. L'article 3 donne les définitions suivantes :

> *(43) «attribut», une caractéristique, une qualité, un droit ou une autorisation d'une personne physique ou morale ou d'un objet;*
>
> *(44) «attestation électronique d'attributs», une attestation sous forme électronique qui permet l'authentification d'attributs;*

Il est également précisé :

> *46. «attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou pour son compte», une attestation électronique d'attributs délivrée par un organisme du secteur public qui est responsable d'une source authentique ou par un organisme du secteur public qui est désigné par l'État membre pour délivrer de telles attestations d'attributs pour le compte des organismes du secteur public responsables de sources authentiques conformément à l'article 45 septies et à l'annexe VII;*
>
> *47. «source authentique», un répertoire ou un système, administré sous la responsabilité d'un organisme du secteur public ou d'une entité privée, qui contient et fournit les attributs concernant une personne physique ou morale ou un objet et qui est considéré comme étant une source première de ces informations ou est reconnu comme authentique conformément au droit de l'Union ou au droit national, y compris les pratiques administratives.*

L'annexe VI du Règlement eIDAS 2 précise au titre de la liste minimale d'attributs pouvant être vérifiés par rapport à des sources authentiques, que les Etats membres doivent permettre aux prestataires de services de confiance qualifiés chargés de la fourniture d'attestations électroniques d'attributs de vérifier par des moyens électroniques, à la demande de l'utilisateur, l'authenticité des attributs suivants par rapport à la source officielle pertinente :

> *« 9. les pouvoirs et les mandats pour la représentation de personnes physiques ou morales; ».*

→| **Le portefeuille européen d'identité numérique (Wallet)**

Il s'agit d'un moyen d'identification électronique permettant notamment de stocker, de gérer, de valider et de fournir des données d'identification personnelle et des attestations électroniques d'attributs. Ces informations sont issues d'acteurs de confiance (État ou acteurs privés tiers de confiance). C'est un droit pour tous les citoyens, résidents et personnes morales de l'UE. Son utilisation est placée sous le contrôle de la personne titulaire du portefeuille. Cette thématique sera développée dans une prochaine publication de la FnTC.

CONCLUSION

Ce premier guide de la FnTC sur l'Identité Numérique Professionnelle vous a présenté les concepts fondateurs de l'authentification des acteurs des échanges entre personnes dans un contexte professionnel. Les principes de garantie de l'identité de la personne, de l'origine du document, et d'imputabilité, exigés dans le cadre de la facturation électronique, pourront être associés aux principes fondamentaux du droit sur le pouvoir d'agir au nom d'une personne morale. Si les moyens techniques de mise en œuvre existent depuis longtemps avec les certificats, nous avons proposé des évolutions qui constituent les prémices de la Génération eWALLET portée par le Règlement eIDAS v2.

Glossaire

- **AIFE :** Agence informatique financière de l'Etat
- **ANSSI:** Agence nationale de la sécurité des systèmes d'information
- **CGI :** Code général des impôts
- **DGFIP :** Direction générale des Finances Publiques
- **JORF :** Journal officiel de la République française
- **JOUE :** Journal officiel de l'Union européenne
- **KYC :** Know Your Customer
- **MIE :** Moyen d'identification électronique
- **PDP :** Plateforme de dématérialisation partenaire
- **PM :** Personne morale
- **PP :** Personne physique
- **PPF :** Portail public de facturation
- **PVID :** Prestataire de vérification d'identité à distance
- **OD :** Opérateur de dématérialisation
- **OpenID :** Protocole technique permettant la fédération sécurisée d'identité

Sources

- JORF – Décret n° 2022-1299 du 7 octobre 2022 et Décret n°2024-266 du 25 mars 2024
- Référentiel d'exigences de sécurité pour les moyens d'identification électronique v 1.2 du 11 août 2022
- Règlement (UE) n°910/2014 du parlement 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, JOUE L 257/73 du 28 août 2014, dit Règlement eIDAS
- Règlement d'exécution 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
- Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique
- Guide FnTC : KYC - Comment maîtriser et optimiser votre connaissance client, août 2021

Comité de rédaction:

Bernard Bailet (Conseil national des greffiers de tribunaux de commerce)

Anne Cantero (Société d'avocats Caprioli & Associés)

Stéphane Gasch (Chambersign)

Hong Girault (Cegedim Business Services)

Elise Lenoir (Darva)

Yves Le Querrec (AIGCEV)

Stéphane Mavel (IDnow)

Cyril Murie (Chambre Nationale des Commissaires de Justice)

Dorian Napoli (CMCIC)

Hélène Roizin (Consultante)

Frédéric Tran Du Phuoc (Société Générale)

Allaa Siam (SRCI)

Morgan Violeau (LuxTrust)

Fédération des Tiers de Confiance du numérique
wwww.fntc-numérique.com
5 impasse Gomboust 75001 Paris
infos@fntc-numerique.com

DÉCEMBRE 2024