



PREMIER MINISTRE  
SECRÉTARIAT D'ÉTAT CHARGÉ DE LA PROSPECTIVE  
ET DU DÉVELOPPEMENT DE L'ÉCONOMIE NUMÉRIQUE

## ANNEXE IDéNum - Foire aux questions

### Le label et les certificats labellisés

#### A quoi le label IDéNum est-il destiné ?

- Le label IDéNum sert à remplacer les mots de passe et autres moyens utilisés par l'internaute pour accéder à ses comptes en ligne, sur les sites web publics et privés. Il apporte plus de simplicité, plus de sécurité, et permet le développement de nouveaux usages.

#### Qu'est-ce qu'un certificat ?

- Un certificat permet d'associer une identité à un support physique et à un code secret. Le nom et le prénom de son titulaire sont les seules données personnelles divulguées.
- Le certificat permet, après avoir composé son code d'activation, de prouver l'identité de son titulaire et de se connecter au service en ligne qui l'accepte.
- Différents supports physiques peuvent être associés au certificat. Il peut notamment s'agir d'une clef USB à module cryptographique, d'une carte à puce associée à un lecteur, lui-même connecté en USB à l'ordinateur, ou de la carte SIM associée à un téléphone portable.
- Pour être labellisés, les certificats doivent répondre aux exigences de sécurité et d'interopérabilité des référentiels mis en place pour l'administration électronique.

#### Quelles données personnelles le certificat contient-il ?

- Un certificat contient le nom et le prénom de son titulaire.

#### Un certificat labellisé IDéNum est-il nécessairement sur un support et si oui de quel type ?

- Un certificat labellisé IDéNum est nécessairement lié à un support. L'accès aux services en ligne nécessite ainsi la possession du support et la connaissance du code associé.

#### Quelles sont les conditions d'obtention du label IDéNum ?

- Pour obtenir le label IDéNum, les organismes émetteurs devront se conformer à un cahier des charges portant notamment sur la sécurité du système et sur sa compatibilité technique.

#### Les référentiels sur lesquels est basé le label IDéNum imposent-ils aux certificats de comporter des données biométriques ?

- Les référentiels n'imposent aucun enregistrement de donnée biométrique.
- L'objectif étant de permettre d'accéder à des sites web, seuls les nom et prénoms suffiront.

### Un certificat labellisé IDéNum peut-il être associé à un pseudonyme ?

- Les certificats labellisés IDéNum ont pour objectif de communiquer l'identité officielle afin d'accéder à un service en ligne qui a besoin d'authentifier l'internaute de manière certaine et en toute confiance. L'usage d'un pseudonyme n'entre donc pas dans le champ du label.

### Quel est le lien avec le site mon.service-public.fr ?

- Mon.service-public est un site proposant un accès plus simple de l'utilisateur vers les services administratifs qu'il utilise. Ce site propose notamment d'accéder à tous les services en prouvant son identité une seule fois. Actuellement, cet accès se fait par login/mot de passe. Il pourra également se faire avec un certificat IDéNum. Le label vient ainsi en complément de mon.service-public.

### Quelle est la différence entre le label IDéNum et le projet de Carte Nationale d'Identité Electronique (CNIE)?

- La carte d'identité, qu'elle soit électronique ou pas, est d'abord un document d'identité qui a pour fonction la preuve d'identité dans les démarches « réelles » ou lors de passages de frontières. Dans certains pays, la carte d'identité électronique sert également à prouver son identité dans les services en ligne. Elle remplit alors la même fonction que celle qui fait l'objet d'IDéNum, en utilisant les mêmes technologies de certificat.
- Le label IDéNum et une CNIE sont des projets complémentaires.

### Comment peut-on utiliser un certificat sur téléphone mobile pour accéder à un service web sur son ordinateur fixe ?

- Le mobile doit être connecté à l'ordinateur via le câble USB de synchronisation. L'internaute entre son code secret sur le mobile comme il le ferait sur un terminal de paiement de carte bancaire.

### Ce type de label existe-t-il déjà dans d'autres pays ?

- Le label IDéNum s'inspire de l'expérience de nos voisins européens (Autriche, Norvège, Finlande, Estonie, Suède, Italie, Turquie, Slovénie..). Ceux-ci proposent à leurs citoyens des certificats sur plusieurs supports – cartes à puce, clés USB, téléphones mobiles – , éventuellement émis par des entités non-étatiques – régions, chambres de commerce, employeurs, banques, postes, opérateurs télécom -

#### Quelques liens utiles :

Autriche : [www.buergerkarte.at](http://www.buergerkarte.at)

Norvège : [www.bankid.no](http://www.bankid.no)

Finlande : [www.fineid.fi](http://www.fineid.fi)

Estonie : [www.id.ee](http://www.id.ee)

Italie : [www.crs.lombardia.it](http://www.crs.lombardia.it); [www.regione.sicilia.it/crs](http://www.regione.sicilia.it/crs)

Turquie : [www.turkcell.com.tr/en/services/Information/turkcellmobilimza](http://www.turkcell.com.tr/en/services/Information/turkcellmobilimza)

## Les fournisseurs de certificats labellisés IDéNum

### Qui va fournir de tels certificats aux internautes ?

- Pourra fournir des certificats IDéNum tout organisme susceptible de vérifier en face à face l'identité des demandeurs et proposant un support et une organisation répondant au cahier des charges de sécurité et de compatibilité technique.
- La procédure de labellisation constitue une démarche volontaire de l'émetteur.
- Sont susceptibles de proposer des certificats IDéNum des organismes comme les banques, les opérateurs de téléphonie ou La Poste, mais également des institutions sectorielles comme des ordres professionnels.

### Qui doit financer les certificats ?

- Plusieurs modèles économiques sont envisageables pour l'émetteur de certificats. Certains organismes ont déjà prévu des projets de fourniture d'outils d'identification forte à certaines populations d'internautes, pour des raisons de contrainte réglementaire ou parce que la dématérialisation des procédures génère suffisamment de gains de productivité en interne pour justifier l'investissement. D'autres proposeront les certificats à leurs clients comme une commodité ou comme un service. Chaque organisme sera libre de définir sa politique commerciale.

## Les internautes

### Comment l'internaute peut-il obtenir un certificat labellisé IDéNum ?

- L'internaute peut se procurer un certificat IDéNum auprès du fournisseur de son choix. Il peut se procurer des certificats auprès de plusieurs fournisseurs s'il le souhaite.
- Il devra effectuer personnellement la demande dans un des points d'accueil du fournisseur, muni d'un titre d'identité.

### Combien le certificat coûte-t-il à l'internaute ?

- Chaque organisme émetteur est libre de sa politique commerciale.

### Combien de temps le certificat IDéNum est-il valable ?

- Pour des raisons de sécurité et d'usure du support, un certificat est en général valable 3 à 5 ans.

### Si l'internaute perd le support du certificat ou se le fait voler, que doit-il faire ?

- Il peut joindre par téléphone un centre de révocation pour faire mettre son certificat en opposition (sur le modèle de la carte bancaire).

### Sur quels services en ligne l'internaute peut-il utiliser le certificat IDéNum ?

- L'internaute peut utiliser le certificat labellisé IDéNum sur tous les services web publics et privés qui l'acceptent comme moyen d'accès. Ces derniers pourront facilement le montrer en présentant sur leur site le logo du label.

- Le label IDéNum est conçu pour être utilisable sur tous les sites de l'administration électronique compatibles avec son niveau de sécurité.

#### Quels avantages l'internaute a-t-il d'utiliser les certificats labellisés ?

- Les avantages pour l'internaute : plus de sécurité grâce au support physique, plus de simplicité (un même code et un même certificat pour tous les services les acceptant), et de nouveaux services (notamment ceux qui nécessitaient jusqu'à présent l'envoi par la poste de justificatifs d'identité ou de formulaires papier signés).

### **Les services en lignes**

#### Quels services en ligne peuvent accepter des certificats labellisés IDéNum pour authentifier leurs usagers ?

- Il est parfaitement possible de naviguer sur Internet de manière anonyme ou avec des pseudonymes. Toutefois, l'internaute a également de plus en plus souvent besoin de prouver son identité, ne serait-ce que pour accéder à son compte bancaire et effectuer des virements ou encore pour procéder à des démarches administratives en ligne.
- Tous les services qui fonctionnent aujourd'hui avec des login/mots de passe, des accès par OTP, par SMS, par CD sécurisé... pourront remplacer ces dispositifs par un moyen simple et fiable : le certificat IDéNum.
- En outre, de nouveaux services en ligne, nécessitant une signature de l'internaute, pourront également utiliser ce certificat.

#### L'usage du certificat respectera-t-il la vie privée de l'internaute ?

- Le système respecte la liberté de l'internaute : acquisition du certificat sur une base volontaire et libre choix du fournisseur.
- L'internaute est libre, pour chaque service, d'utiliser un certificat IDéNum (il peut même en avoir plusieurs) ou un autre moyen.
- Aucun organisme central ne conserve de trace de tous les usages d'un certificat réalisés par un internaute.
- Naturellement, chaque service auquel l'internaute accède en utilisant le certificat IDéNum conserve les données de connexion de ses clients, selon les dispositions légales en vigueur.

#### Combien les services en ligne doivent-ils payer pour pouvoir accepter les certificats labellisés ?

- Techniquement, n'importe quel service peut librement accepter un accès par certificat IDéNum. Il peut avoir recours à des prestations complémentaires proposées par les émetteurs, comme la consultation de la liste des certificats mis en opposition.
- Le modèle économique reste à déterminer en concertation avec tous les partenaires du projet.

#### Quels sont les avantages, pour les services en ligne, d'accepter les certificats labellisés ?

- Accepter les certificats labellisés permet de remplacer les différents dispositifs de contrôle d'accès existants, soit pas assez sécurisés (mot de passe), soit trop disparates (CD sécurisé, OTP, SMS...) par un système simple, efficace, fiable, et mutualisé.
- Le service en ligne n'a plus à gérer les dispositifs d'accès de ses clients.
- Le site web peut proposer de nouveaux services, impossibles à dématérialiser jusque là car nécessitant une signature.

N'y a-t-il pas un risque d'interconnexion de fichiers si trop de sites obligent leurs membres à utiliser des certificats labellisés pour accéder à leur service, l'internaute n'ayant alors plus d'autre choix que de s'identifier ainsi sur chaque site ?

- L'utilisation d'un certificat n'a de sens que pour des services en ligne gérant des données personnelles ou pour signer des engagements. Pour les autres sites web, une navigation anonyme ou avec un pseudonyme reste la règle.
- L'internaute peut décider lors de chaque connexion à ces services d'utiliser ou non son certificat IDéNum ; il peut s'il le souhaite détenir plusieurs certificats différents qu'il utilise à son gré.

Quels seront les nouveaux services proposés ?

- Aujourd'hui, de nombreuses démarches administratives ou privées peuvent être initiées en ligne, mais ne peuvent être conclues que par l'envoi, par la poste ou par scan, de pièces justificatives de l'identité, ou par l'envoi d'un formulaire papier signé. Le certificat IDéNum permettra de mener ces démarches en ligne jusqu'au bout.
- On peut citer parmi les démarches qui pourront être menées jusqu'au bout en ligne grâce à l'emploi d'un certificat IDéNum :

Applications gouvernementales ou publiques :

- Inscription sur les listes électorales (en test actuellement par le ministère de l'intérieur, mais nécessite l'envoi des pièces justificatives de l'identité)
- Gestion du personnel dans la fonction publique : signature des demandes de mutation, de mise en congé parental, de gestion du compte-épargne-temps...
- Demande d'allocation CAF ou sociale
- Demande de congé parental
- Demande de pension de retraite
- Demande d'allocation chômage
- Signature des bulletins scolaires dans l'Espace numérique de travail (ENT) de l'Education nationale

Applications privées :

- Ouverture en ligne d'un compte bancaire supplémentaire (livret d'épargne, compte pour les enfants...)
- Instructions à son conseiller bancaire
- Souscription d'emprunt
- Souscription de contrat d'assurance
- Signature d'un contrat de location ou d'abonnement
- Signature d'avenants à un contrat

Applications mixtes :

- Réception de mails avec accusé de réception électronique
- Signature d'e-mails (anti-spam)
- Signature de documents électroniques, de fichiers, etc...
- Sécurisation de l'accès distant au système informatique de l'employeur

## **La compatibilité**

Que signifie la compatibilité des certificats IDéNum ?

- Tous les certificats labellisés IDéNum, quel que soit leur fournisseur, sont utilisables indifféremment sur tous les services en ligne qui ont décidé de les accepter.

Sont-ils utilisables sur les sites web qui conservent un système à mot de passe ?

- Un service en ligne reste libre quant au choix de son système d'authentification de l'internaute. Il peut proposer plusieurs solutions : accès avec un couple identifiant/mot-de-passe, et de façon complémentaire à partir d'un certificat labellisé.

**La simplicité**

En quoi le label simplifie-t-il les démarches d'identification en ligne des internautes ?

- Les certificats labellisés sont compatibles avec tous les services qui les acceptent.
- L'internaute peut ainsi faire usage d'un même certificat pour accéder à différents services en ligne.
- A un certificat correspond un unique code PIN. L'internaute n'a plus qu'un seul code à mémoriser.

N'est-ce pas plus compliqué de devoir porter avec soi de tels outils plutôt que d'utiliser des mots de passe ?

- Les supports ne sont pas encombrants.
- Ils sont pour la plupart d'entre eux (carte à puce, clé USB, téléphone mobile) déjà quotidiennement dans la poche de bon nombre d'internautes.

**La sécurité**

En quoi IDéNum renforce-t-il la sécurité ?

- L'accès au service en ligne nécessite la possession du support (clé USB, carte à puce, téléphone mobile) et la connaissance du code associé.
- Il n'y a plus de base de données de mots de passe, gérée par les fournisseurs de services en ligne, et surtout vulnérable au piratage.
- Les services en ligne n'ont pas à connaître le code secret pour permettre l'accès. Le code secret n'est utilisé que pour l'activation du support. Il n'est pas transmis au fournisseur de service en ligne.

Pour un même certificat, le code secret est le même pour tous les services en ligne. Un service ne peut-il pas le détourner pour accéder aux comptes d'autres services ?

- L'accès à un service en ligne nécessite la possession du support (clé USB, carte à puce, téléphone mobile) et la connaissance du code associé.
- Le code secret n'est utilisé que pour l'activation du support. Il n'est pas transmis au fournisseur de service en ligne.

Les pirates en informatique sont toujours en avance sur les nouveaux usages. Qu'est-ce qui donne confiance dans cette technologie ?

- C'est justement pour renforcer et harmoniser la sécurité de l'identification qu'une telle technologie à base de certificats et de supports physiques est mise en avant. Les certificats

IDéNum répondront à un cahier des charges avec des exigences de sécurité rigoureuses, validé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il n'y a pas d'exemple connu de cassage de ces niveaux de sécurité.

Quels sont les moyens d'évolution des référentiels pour s'adapter aux nouvelles cyber-menaces et comment répercuter ces évolutions sur les outils s'ils sont déjà labellisés ?

- Les exigences du cahier des charges seront mises à jour régulièrement.
- Les fournisseurs labellisés seront soumis à des audits réguliers.
- Les certificats seront renouvelés régulièrement pour suivre l'évolution des technologies.

La création de ce label permet-elle de lutter contre le phishing ?

- Le phishing consiste à attirer l'internaute sur un site contrefaisant celui d'une institution, afin de l'amener à dévoiler son mot de passe.
- Avec un certificat, la preuve d'identité est générée sur le support physique (clé USB, carte à puce, téléphone mobile) activé par le code secret. Cette preuve est à usage unique et liée au contexte de la connexion. Elle ne peut pas être réexploitée par le pirate ultérieurement.
- La possession du support physique est indispensable pour ouvrir l'accès au service. Le code secret n'est jamais transmis en ligne. Il permet uniquement d'activer le support.

**La signature électronique**

Qu'est-ce qu'une signature électronique ?

- Une signature électronique n'est pas l'image scannée de la signature manuscrite !
- Une signature électronique est un fichier codé qui permet d'établir un lien entre un contenu (le texte à signer), un support physique et un code secret (ceux du certificat IDéNum) et l'identité du titulaire du certificat.
- La validité juridique de la signature électronique est définie par l'article 1316-4 du Code civil.

Comment peut-on signer électroniquement un document ?

- La signature électronique a lieu en deux étapes majeures : 1/ l'internaute sélectionne le document numérique à signer. 2/ il crée une signature grâce au support du certificat en composant son code secret.

Une signature électronique est-elle copiable ?

- La signature électronique étant générée à partir du fichier qu'elle signe, à deux documents différents correspondront deux signatures différentes.
- Il n'est pas possible de réutiliser une signature pour signer frauduleusement un autre document, pas plus qu'on ne peut modifier le document initial après signature.
- La signature électronique à partir des certificats labellisés nécessite de composer le code secret, ce qui apporte la preuve de la volonté du signataire.