Identités numériques

Dr Michel DUBOIS
Chef du Pôle Expertise
Direction de la cybersécurité - Groupe La Poste

Du latin " identitas " signifiant " le même ", l'identité présente de multiples définitions en fonction du domaine d'étude. Ainsi, le psychologue allemand Erik Erikson, dans son ouvrage " Enfance et société ", définit l'identité comme " le sentiment subjectif et tonique d'une unité personnelle et d'une continuité temporelle ". Pour la philosophe Anne-Marie Drouin-Hans, l'identité sépare le soi du non-soi. Le sociologue Erving Goffman explique, dans son ouvrage " Stigmate ", que l'identité d'un individu s'élabore par le jeu de l'interaction et résulte de l'opposition entre une identité définie par autrui et une identité pour soi. Dans le domaine juridique, l'identité correspond à " la personnalité civile d'un individu, légalement reconnue ou constatée, établie par différents éléments d'état civil et par son signalement ".

Comme nous pouvons le voir, définir la notion d'identité, est un problème difficile, dépendant du domaine d'étude et évolutif dans le temps. Malgré tout, il nous faut définir la notion d'identité dans le domaine du numérique.

Dans son rapport " Identités numériques - Clés de voûte de la citoyenneté numérique ", le Conseil national du numérique définit l'identité numérique sous deux angles :

- l'identité numérique peut faire référence à l'identifiant d'accès à un service, choisi pour ou par le détenteur. Dans ce cas, l'identité numérique peut être déclarative ou imposée par le service, en rapport avec l'état civil ou non. Il existe alors une multiplicité d'identités numériques propres aux pratiques numériques de chaque individu ;
- l'identité numérique peut aussi être perçue comme le reflet des comportements en ligne des individus, c'est à dire l'ensemble des traces qu'un individu peut laisser en surfant sur Internet, et qui permettront de définir une cartographie de ces comportements et de faire entrer celui-ci dans une typologie.

Le deuxième angle est celui utilisé dans le marketing. Il permet de catégoriser un internaute en fonction de son comportement sur les sites Web qu'il visite. Nous allons nous focaliser sur le premier angle de définition de l'identité numérique : celui basé sur un identifiant que nous appelons couramment login, adresse email ou pseudo en fonction du contexte.

La problématique de l'identité numérique réside dans la conception d'Internet. En effet, Internet a été construit sans qu'il soit possible de savoir à qui et à quoi on se connecte. Comme cette capacité essentielle fait défaut, des solutions de rechange ont dû être trouvées afin d'identifier qui accède à quoi. La conséquence directe de cet état de fait est qu'Internet, en l'absence d'une couche d'identité native, est basé sur un patchwork d'identités ponctuelles et multiples.

C'est ainsi que l'internaute moderne s'est habitué à saisir ses identifiants sans avoir la certitude de l'authenticité des sites Web qu'il visite, ou si des informations privées sont divulguées à des parties illégitimes à son insu. Les cybercriminels ont bien compris cette situation et ont développé des attaques spécifiques comme le phishing, le spear phishing, la fraude 4-1-9, l'arnaque au président, le pharming et le credential stuffing. Cette dernière attaque étant directement liée à la multiplicité des identités numériques ce qui entraîne une réutilisation des éléments d'authentification.

Avec le temps, des protocoles spécifiques ont été élaborés comme "Transport Layer Security" (TLS). TLS est un protocole de sécurisation des échanges sur un réseau informatique et donc sur Internet. Ce standard permet d'authentifier le serveur et l'utilisateur ainsi que de garantir l'intégrité et la confidentialité des échanges. Concrètement, TLS est le "S" de HTTPS dans les adresses des sites Web. Sur le plan technique, des réponses ont été apportées, cependant elles ne sont pas universellement déployées. En outre, elles ne concernent que le monde des réseaux informatiques et ne résolvent pas le problème des identités multiples.

Il est donc primordial de disposer d'une plateforme permettant d'agréger les différentes identités numériques d'un individu.

Pour être adoptée massivement par les utilisateurs, une telle plateforme devrait répondre à un certain nombre de principes :

- Contrôle et consentement de l'utilisateur. L'utilisateur doit pouvoir faire confiance à la plateforme de gestion de son identité. Pour gagner cette confiance, la plateforme doit être conçue de manière à ce que l'utilisateur puisse contrôler les identités numériques utilisées et les informations divulguées. La plateforme doit également protéger l'utilisateur contre la fraude, en vérifiant l'identité de toute partie qui demande des informations. Enfin, la plateforme doit permettre à l'utilisateur de connaître les raisons pour lesquelles les informations sont recueillies ;
- Collecte restreinte du nombre d'identifiants. La plateforme doit être conçue en tenant compte du risque de compromission de son annuaire interne. À ce titre, elle ne doit collecter que le minimum d'éléments d'identification pour chaque individu ;
- Ségrégation des identités. La plateforme garantit la ségrégation des identifiants destinés aux entités publiques, administratives, professionnelles ou privées. L'utilisateur doit pouvoir faire en sorte que l'identité numérique utilisée à titre privée ne soit pas connue de son employeur ou de l'administration ;
- Centralisation sur l'humain. Dans un processus d'identification on distingue le consommateur, qui offre un service, et les contextes de données d'identification. En fonction du consommateur, l'individu doit pouvoir choisir quel contexte de données d'identification utiliser. Ainsi, l'utilisateur pourra s'identifier sur un service médical avec des éléments identifiants différents de ceux utilisés pour un service assurantiel ;
- Compatibilité multi protocole. La plateforme doit permettre l'interfaçage avec les différentes technologies et normes de gestion des identités et d'authentification ;
- Expérience utilisateur. La plateforme doit garantir à ses utilisateurs une expérience simple et cohérente tout en permettant la séparation des contextes. Indépendamment du contexte, les procédures d'identification et d'authentification doivent être identiques et simples à utiliser.

Il existe de multiples plateformes d'agrégation d'identité permettant, au travers d'une identité pivot, d'accéder à des services divers et variés. Cependant, ces plateformes sont opérées par les grands noms d'Internet : Google, Apple, Facebook, Amazon et Microsoft. De ce fait, elles ne répondent pas aux critères précédemment énoncés.

En 2014, la France s'est dotée d'un dispositif répondant aux principes que nous avons détaillés. Mise en œuvre par la Direction interministérielle du numérique, la plateforme "FranceConnect" est la

solution proposée par l'État pour sécuriser et simplifier la connexion à plus de 700 services en ligne.

Reposant sur le protocole OpenID connect, son objectif est de mettre en relation des fournisseurs d'identité et des fournisseurs de service. Ainsi, lorsqu'un utilisateur souhaite effectuer une démarche en ligne, il lui suffit de cliquer sur le bouton " FranceConnect " et de choisir un compte sur l'un des fournisseurs d'identité référencés. La plateforme FranceConnect le redirige alors sur la page d'authentification. Une fois les opérations d'identification et d'authentification réalisées, l'utilisateur peut accéder au service désiré.

La plateforme FranceConnect est cependant limitée au seul usage de la relation entre un citoyen et l'administration. Il manque donc un équivalent de FranceConnect regroupant l'ensemble des besoins de support de l'identité du citoyen : vis-à-vis de l'administration, mais aussi, dans le cadre de sa vie privée et professionnelle.

L'idéal serait que notre pays dispose d'une plateforme sur laquelle chaque citoyen puisse gérer, en fonction du contexte, une identité pivot regroupant ses différentes identités numériques. En attendant ce jour, il reste d'autres difficultés, liées à l'identité numérique, à prendre en compte comme, par exemple, la suppression des mots de passe.