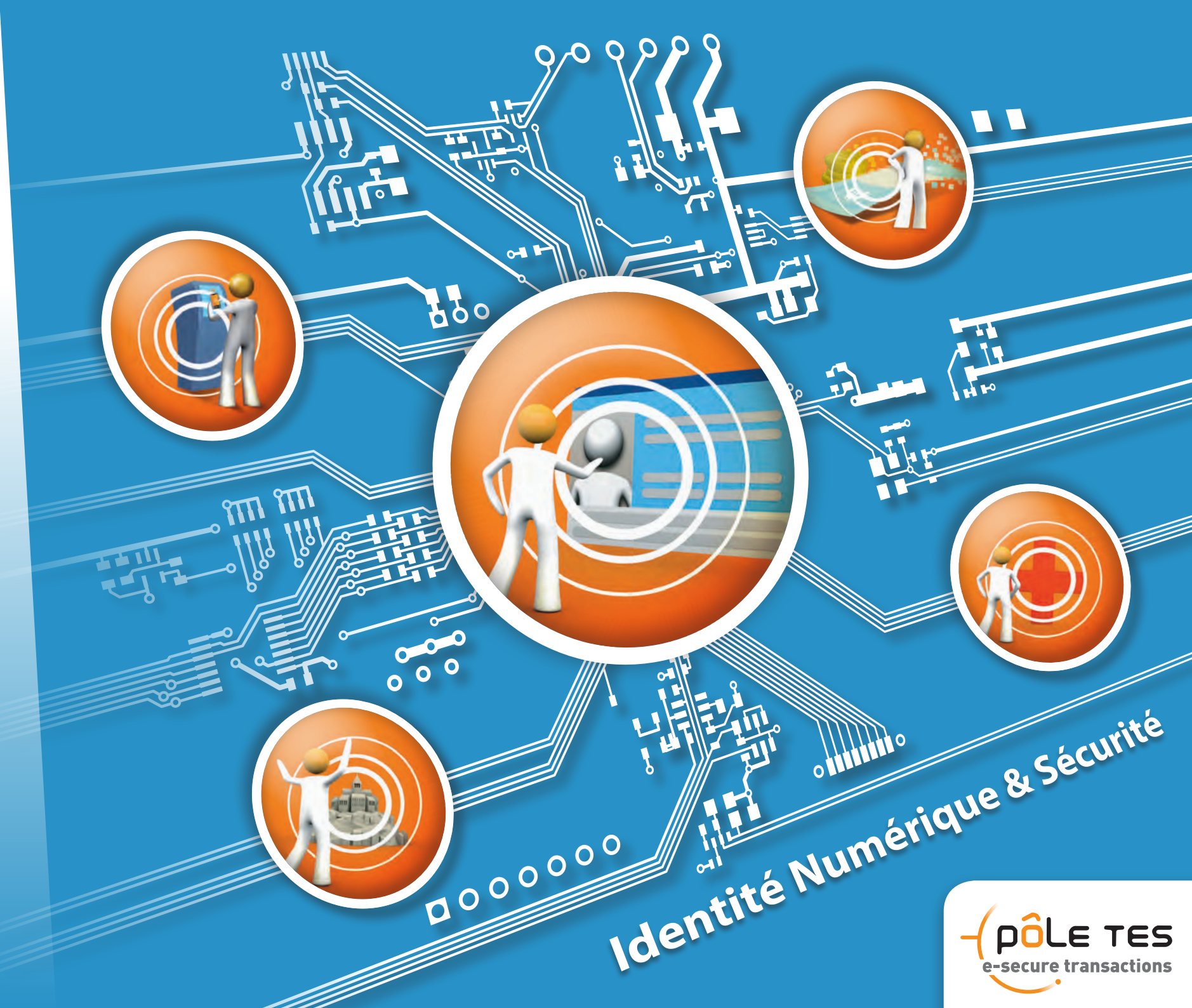
Pôle de compétitivité Transactions Electroniques Sécurisées

Position paper



Identité Numérique & Sécurité

pôle TES
e-secure transactions

Sommaire

Édito

Les usages quotidiens de services numériques et leur généralisation supposent, dans un nombre croissant de situations, la présentation par les citoyens de données d'identité numérique. Ces données prises au sens large peuvent être régaliennes ou privées, univoques ou simplement descriptives. Dans tous ces cas, l'identité numérique doit apporter la confiance nécessaire à la bonne exécution de transactions électroniques, dans laquelle chaque partie doit savoir si elle traite avec un interlocuteur fiable.

En même temps sur ces dernières années, les usages ont évolué grandement, avec la diversification des terminaux (tablettes, smartphones…) disposant de canaux de communications variés (NFC, réseaux fixes ou mobiles) et laissant envisager un potentiel immense de nouvelles applications. De plus en plus, on constate que l'utilisateur possède plusieurs de ces terminaux en plus des traditionnels PCs, notamment un smartphone. Alors que celui-ci se généralise il introduit une telle flexibilité d'usages et une telle ergonomie qu'il semble impossible de ne pas baser une partie importante des réflexions sur ce type de terminal personnel.

Ces dernières années ont également montré à quel point devenaient importantes les préoccupations des utilisateurs sur la maîtrise de leurs données personnelles et la sécurité. Les risques d'usurpation d'identité ainsi que les risques d'atteinte à la privacy de l'utilisateur ne sont pas des vues de l'esprit, alors qu'il aspire à une vie numérique sereine.

Enfin, il est admis avec juste raison que la maitrise de l'identité numérique est un facteur important dans l'économie numérique, et peut même être vu comme un enjeu de souveraineté nationale.

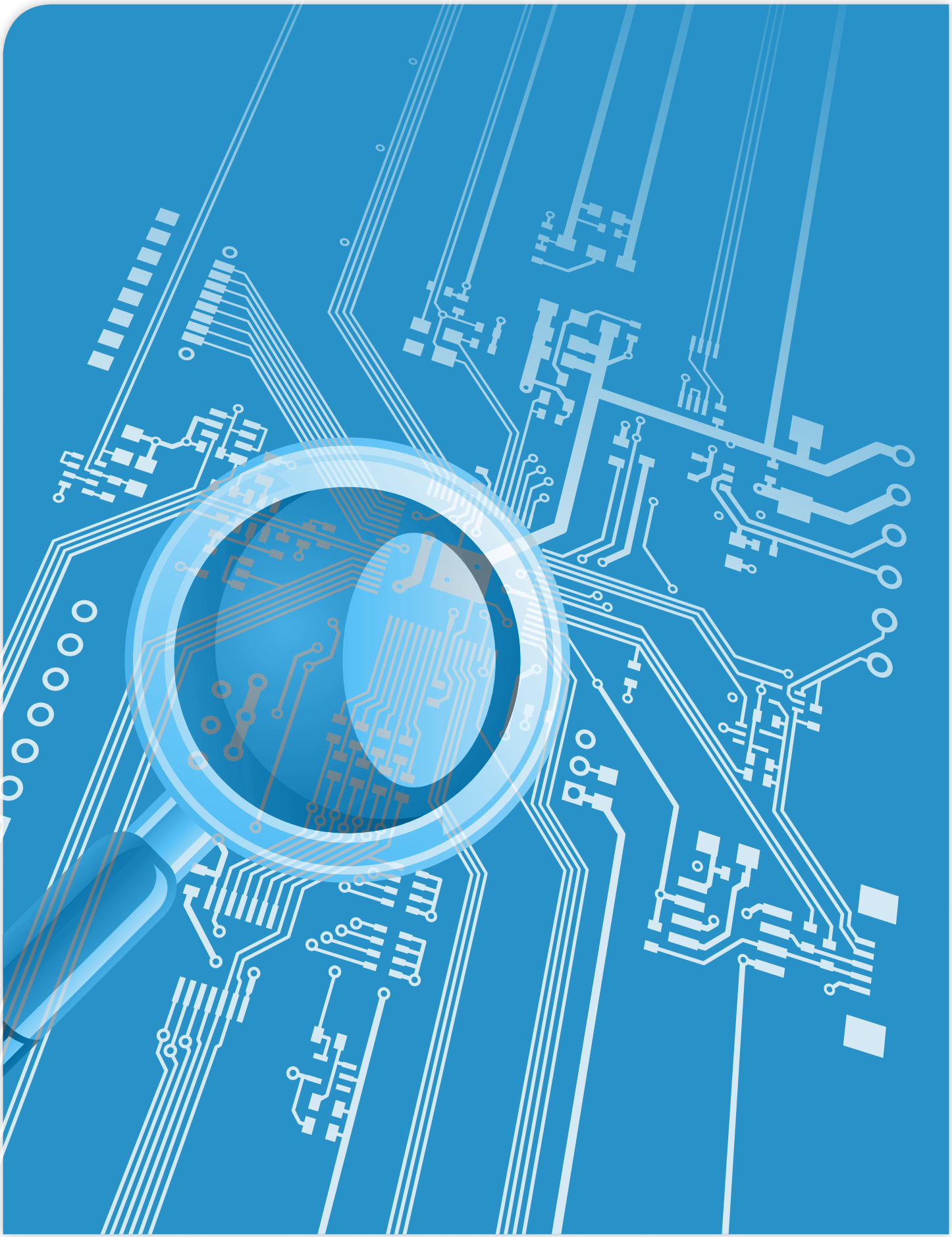
Dans ce contexte, le pôle TES, très impliqué dans le domaine des transactions électroniques sécurisées, s'est créé une entité interne dédiée à l'identité numérique. Une décision qui intervient au moment où un regain d'intérêt apparaît sur ce sujet au niveau national et européen. Cette contribution vise à apporter sa pierre à la compréhension des problématiques se rapportant à ce sujet et à définir une certaine vision en espérant qu'elle puisse contribuer à la créativité des acteurs du domaine, industriels, sociétés de services, prestataires de service et à l'éclosion de projets novateurs.

Jean-Claude PAILLÈS, Coordinateur du Département Identité Numérique et Sécurité du Pôle TES

Tous les projets labellisés cités dans ce document sont présentés sur le site :
www.pole-tes.com

Contribution au débat sur l'identité numérique

Les constats



L'identité numérique est régalienne ou privée, univoque ou simplement descriptive, et se compose d'attributs préétablis ou dérivés

La multiplicité des identités numériques, résultat d'un développement protéiforme et non organisé des services dématérialisés, est un fait. Pour accéder à sa banque en ligne, à un site de e-commerce, au portail de téléservices de sa mairie, bénéficier d'e-coupons de réductions ou encore accéder au réseau de transports avec une carte à puce, nous utilisons des identités numériques distinctes.

L'identité numérique ne peut se réduire à une identité numérique régalienne

La diversité des identités numériques est durable car les besoins d'identification et d'authentification varient en fonction des services. Cette diversité est aussi un moyen de préserver les libertés individuelles et d'éviter la création d'un monde à la «big brother» reposant sur un système hypercentralisé. L'identification numérique ne peut donc passer par UNE seule solution qui viendrait de l'État et la coexistence des identités privées/régaliennes est nécessaire.

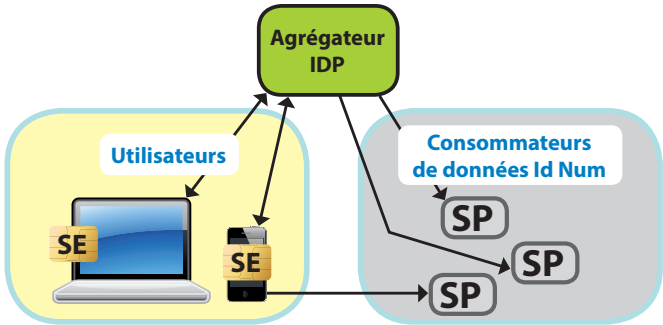
La multiplicité des identités numérique a cependant aujourd'hui atteint ses limites. Chacun d'entre nous doit mémoriser des dizaines d'identifiants et de mots de passe pour accéder à des services en ligne et notre portefeuille est encombré d'innombrables cartes de paiement, de fidélité ou de transport, que l'on garde dans sa poche. Cette multiplicité n'est pas gage de sécurité : souvent les mots de passe sont les mêmes ou peu sécurisés. Pour beaucoup de personnes, c'est un frein à l'utilisation du commerce en ligne ou des téléservices administratifs et plus généralement, une source de défiance à l'égard des services en ligne.
Face à cette situation, le pôle TES estime qu'il convient d'organiser cette diversité, de simplifier là où c'est possible - en particulier sur Internet - et de promouvoir des systèmes de fédération d'identité par sphères d'usages.

Dériver l'identité numérique d'une identité de confiance préexistante

La création d'une identité numérique de confiance est étroitement dépendante de la qualité et de la fiabilité des données qui ont permis de la créer. C'est la raison pour laquelle une identité numérique est souvent créée en utilisant un attribut dérivé d'une identité préexistante.

Dans ce schéma, la nouvelle identité est créée en utilisant un attribut, comme par exemple la date de naissance, qui servira à justifier que l'on est majeur et que l'on peut accéder à certains services réservés aux adultes ou une adresse, qui permettra de bénéficier d'une réduction à la piscine intercommunale, qui pratique un tarif spécifique pour les personnes résidant dans l'intercommunalité.

Ce mécanisme doit être associé à un niveau de confiance car si l'on dérive l'attribut (majeur) d'une identité de faible confiance - un compte Facebook par exemple - la nouvelle identité aura un niveau de confiance faible. Cette identité existante doit donc avoir été créée par une entité dotée d'un bon niveau de confiance comme une banque, un opérateur télécom ou un service public au moyen de justificatifs telle que la présentation d'un titre d'identité et/ou d'une facture pour justifier de son adresse.



voir zoom technique page 21 sur un modèle d'échange de données d'identité numérique.

IDP (Identity Provider)
SE (Elément de Sécurité)
SP (Service Providers)

2e constat

L'identité numérique est multiusages et multi-terminaux

Services publics, école, entreprise, consommation, accès aux locaux, santé, vie sociale… les besoins d'identité numérique sont le corollaire de la «numérisation» accélérée de la société. Ces services numériques sont partout, irriguent le quotidien de l'ensemble des français et dépassent nos frontières.

L'ordinateur n'est plus le support exclusif de l'identité numérique

L'identité numérique passe désormais par une multitude d'objets connectés : aujourd'hui les cartes à puce, les ordinateurs fixes ou portables, les téléphones mobiles et les tablettes, demain les lunettes, la voiture, le frigo… et toute sorte d'objets communicants associés à une personne physique.

Pour chacun de ces objets et terminaux, rarement mono-usage et souvent interconnectés, faudra-t-il que nous ayons à chaque fois un mode d'identification différent ? Ce n'est souhaitable ni pour l'utilisateur qui doit mémoriser des dizaines d'identifiants et mots de passe, ni pour le fournisseur qui souhaite faciliter l'accès au service en limitant les coûts liés à l'identification.

Pour le pôle TES, l'identité numérique doit passer par des serveurs d'identité alliant sécurité et simplicité d'usage. Ces serveurs peuvent être localisés dans un «nuage informatique» (cloud computing) sous maîtrise publique, ou, quand il n'y a pas de réseau ou que la transaction doit être très rapide (paiement NFC, validation NFC d'un titre de transport) utiliser un stockage sécurisé des données en local agissant comme une mémoire cache. Dans tous les cas de figure, une sécurité de bout en bout doit être assurée.

La pluralité des modes d'accès aux services doit être préservée

Le besoin de simplification de la gestion des identités numérique doit être concilié avec la nécessité de préserver différents modes d'accès aux services. En effet, la pluralité des supports de l'identité numérique est durable car liée au rythme de l'innovation, aux délais de renouvellement du parc (mobiles, ordinateur…) et aux aléas de la conjoncture économique.

Elle répond aussi à des questions pratiques. Par exemple, on peut réserver un ouvrage en ligne sur le site de la bibliothèque ou physiquement dans ses locaux : dans les deux cas le lecteur aura à justifier du fait qu'il est abonné mais selon un mode d'accès différent : par exemple identifiant/mot de passe en ligne, carte à puce ou mobile NFC dans les locaux de la bibliothèque.

Enfin la diversité des modes d'accès répond à un souci d'accessibilité des services. Une personne âgée préfèrera sans doute se rendre sur place et utiliser une carte, un adulte travaillant la journée préférera utiliser son ordinateur de bureau pour éviter un déplacement, l'adolescent optant pour le smartphone pour gérer son abonnement à la bibliothèque…

Le smartphone est particulièrement adapté pour l'accès aux services de proximité ou distants

Les atouts du smartphone

Aussi puissant qu'un ordinateur traditionnel, connecté à internet via la 3G/4G ou un réseau Wifi, doté d'un grand écran et d'un clavier, le smartphone nous accompagne partout dans nos déplacements et est en passe de devenir la «télécommande» de notre quotidien. Aux fonctions classiques du téléphone mobile (SMS, voix…) s'ajoutent l'accès à internet, la géolocalisation (GPS, triangulation…), l'appareil photo et l'hébergement d'applications pour des usages toujours plus nombreux. En outre, le système des magasins d'applications (app store) facilite la large diffusion des applications et leur mise à jour rapide à moindre coût, notamment en cas de faille de sécurité.

En matière d'identification numérique, le smartphone possède un avantage supplémentaire : il peut contenir des données confidentielles - et notamment des données d'identité - maintenues intègres et/ou confidentielles grâce à l'élément de sécurité (*secure element*) du mobile : la carte SIM de l'opérateur ou une carte additionnelle (carte SD…). Grâce à la technologie NFC, technologie de communication en champ proche qui équipe la grande majorité des nouveaux smartphones (hors Apple), le mobile peut dialoguer avec des objets comme le valideur d'un bus, un terminal électronique de paiement, la porte de sa voiture ou encore un serveur d'identité.

Toutes ces qualités font du smartphone un outil très intéressant pour gérer la sécurité et offrir des services nécessitant une vérification des droits d'accès.

Une adoption rapide de l'usage du smartphone

Apparu en 2007, le smartphone a rapidement séduit les utilisateurs. Selon Médiamétrie au troisième trimestre 2012, 23,8 millions de personnes, soit 46,6 % des Français, étaient équipés d'un smartphone ; ils étaient 17 millions au troisième trimestre 2011. Un taux qui dépasse même les 50 % chez les jeunes de moins de 25 ans. La tendance ne va que s'accentuer puisque plus d'un mobile sur deux vendu dans un magasin est un smartphone. Enfin, on soulignera que la plupart des smartphones commercialisés (à l'exception de ceux d'Apple) sont désormais équipés d'une puce NFC et selon les opérateurs, on comptait près de 2,6 millions de mobiles NFC en France (source : AFSCM) dans la poche des utilisateurs en février 2013.

Au-delà de ces statistiques, plusieurs éléments comportementaux sont intéressants au regard de son utilisation comme moyen d'identification : le téléphone mobile est un des seuls objets pour lequel on est prêt à faire demi-tour lorsqu'on l'a oublié, même après avoir fait plusieurs kilomètres ! C'est aussi un outil dont on se sépare difficilement et il faut moins d'une heure, en moyenne, pour que l'on se rende compte de sa perte.

Autant d'éléments qui font du smartphone, un outil particulièrement adapté pour gérer l'identité numérique.

NFC en quelques mots :

La near field communication (NFC) ou communication en champ proche est une technologie de communication sans-fil à courte portée permettant l'échange d'informations entre deux terminaux. Utilisée depuis plusieurs années pour les cartes d'accès aux transports (Pass Navigo) NFC équipe désormais beaucoup de mobiles. Les usages possibles sont très divers : billettique, paiement, accès à un véhicule ou à un lieu sécurisé…

En chiffres

23.8 millions

c'est le nombre de Français dotés d'un smartphone, parmi lesquels 2,6 millions de mobiles NFC. (Source : AFSCM).

4e constat

Les craintes des utilisateurs portent désormais sur la protection de la vie privée

La problématique de l'identité numérique est indissociable de celle de la protection de la vie privée. Protéger la vie privée, c'est lutter contre le risque de vol ou d'usurpation d'identité mais aussi garantir un usage adéquat de données personnelles très convoitées.

L'usurpation d'identité numérique, une pratique en hausse

En France, le coût de la fraude à l'identité était estimé en 2010 par un rapport parlementaire à plus de 20 milliards d'euros de dommages pour les seules administrations sociales. Une fraude qui concerne tous les domaines et connaît une expansion constante avec le développement du commerce et des services en ligne. Pour la seule carte bancaire, la fraude a par exemple fait une progression spectaculaire avec un préjudice chiffré par les banques à 74 M€ en 2010 pour atteindre 104 millions d'euros en 2011*.

Si les techniques utilisées par les pirates ne cessent de se diversifier - faux sites ou faux mails simulant celui de votre banque (le phishing), intrusions via le navigateur internet, captage distant des mots de passe saisis sur le clavier… - l'objectif des pirates est généralement le même : subtiliser des données personnelles pour les utiliser frauduleusement. Si ces attaques ont essentiellement des finalités pécuniaires (achats, virements frauduleux), elles peuvent aussi avoir pour objectifs de nuire à la réputation en ligne, «l'e-réputation» de la victime.

L'augmentation de la fraude à l'identité numérique appelle des réponses adaptées. On soulignera cependant que priorité doit être donnée à la sécurisation des données régaliennes servant à établir les autres identités (numériques ou pas).

(* Source : GIE cartes bancaires)

La crainte du traçage

A l'heure des moteurs de recherche et des réseaux sociaux, le vol de données d'identité n'est cependant plus la seule crainte des internautes et mobinautes.

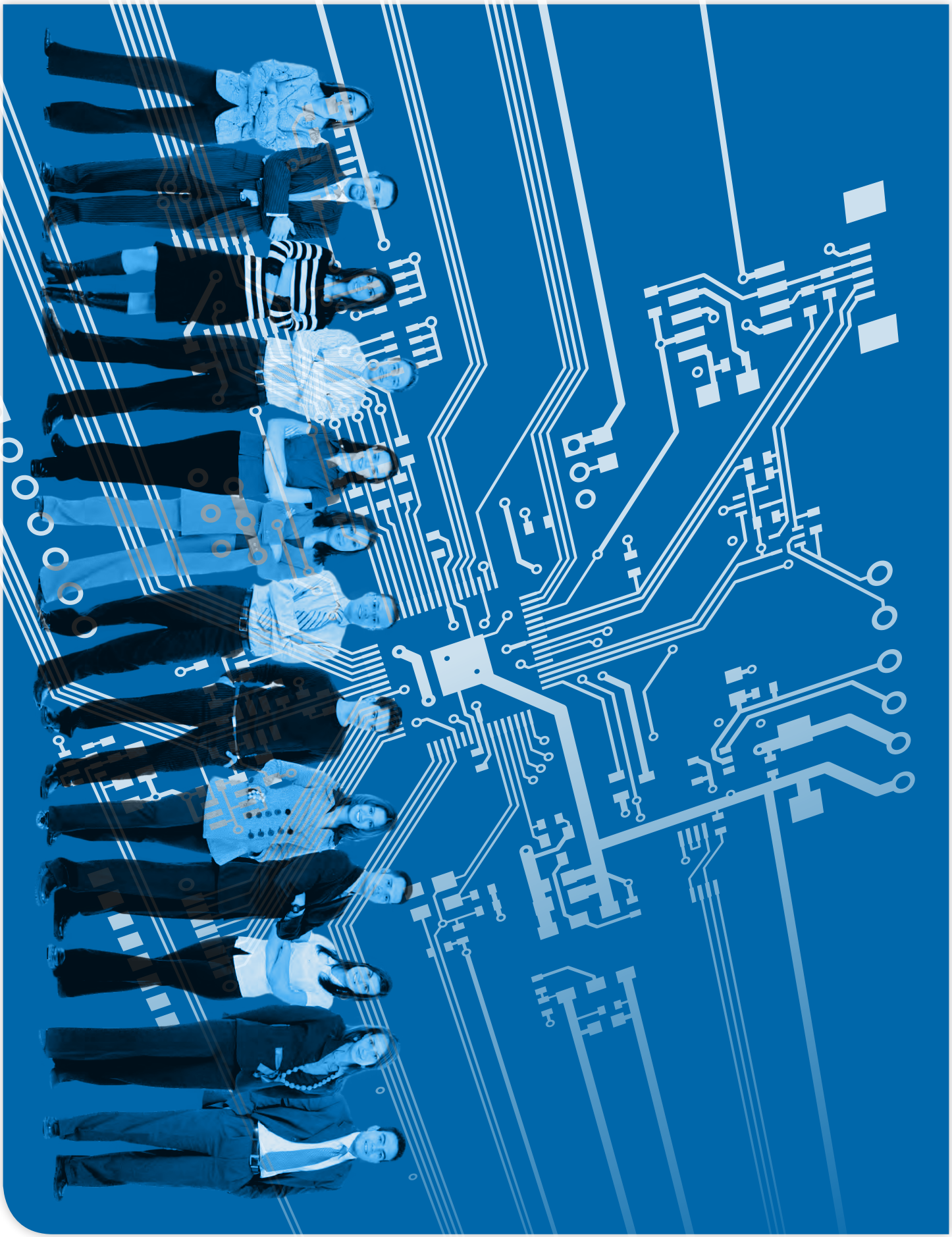
A partir des sites et pages fréquentées par l'utilisateur, il est possible de reconstituer ses habitudes, ses goûts de consommation, les personnes qu'il fréquente… la généralisation du GPS sur les mobiles et tablettes ne fait qu'accentuer ce risque de «traçage» en permettant de connaître heure par heure les lieux fréquentés par leurs possesseurs. Du point de vue des services utilisant ces données personnelles, l'objectif est de mieux connaitre les attentes des utilisateurs (personnalisation, contextualisation…) mais ces derniers ont le sentiment - à juste raison - d'être espionnés ou, pour le moins, mal informés sur les objectifs poursuivis et, surtout, sur le devenir de leurs données.

Aussi, enquête après enquête, les craintes sur les données personnelles figurent en tête des préoccupations des français. Selon l'enquête annuelle sur les TIC de l'Arcep (juin 2012), pour un tiers des Français, les données personnelles ne sont pas assez protégées, chiffre qui ne cesse de s'élever depuis 10 ans (+ 10 points depuis 2006). On notera cependant que la crainte est loin d'être uniforme selon les catégories de population : les jeunes sont plus enclin à se dévoiler sur internet, surtout s'ils bénéficient de services suplémentaires, et les personnes les plus éloignées du numérique sont aussi celles qui se révèlent être les plus méfiantes.

Partant de ce constat, il est impératif que les dispositifs d'identification numérique offrent des garanties sur la protection de la vie privée. Un équilibre doit cependant être trouvé entre ces exigences et l'innovation dans les services, car l'innovation passe de plus en plus par une connaissance des comportements des utilisateurs. L'important est donc de donner à l'utilisateur les moyens pour maitriser l'usage de ses données personnelles.

Contribution au débat sur l'identité numérique

Les 8 propositions du Pôle TES



1ère proposition

Passer d'une approche sécuritaire et centralisée à une vision plus pragmatique de l'identité numérique

Identifié depuis les débuts d'internet comme un frein au développement des usages, l'identité numérique a fait l'objet de plusieurs projets nationaux qui ont du mal à déboucher sur des réalisations concrètes.

La CNIe en stand by

Issue du projet INES (identité numérique électronique sécurisée), projet visant à sécuriser les titres régaliens (carte d'identité, passeport, permis de conduire…), la carte nationale d'identité électronique (CNIe) a fait l'objet de deux projets de loi en 2006 et 2009. Son principal objet est de lutter contre les faux titres d'identité qui se sont multipliés ces dernières années.

Le dernier projet de loi en date a été adopté en 2012 par le parlement mais en étant amputé de plusieurs dispositions par le Conseil constitutionnel. Initialement, la CNIe devait en effet comporter deux compartiments dans la puce : l'un pour gérer l'identité du porteur *stricto sensu*, l'autre pour permettre au détenteur de s'identifier sur internet et de signer des documents électroniques. Ce volet «e-services», comme la création d'une base nationale de données biométriques a été censuré par le Conseil constitutionnel. A l'heure actuelle, un audit de l'inspection générale de l'administration est en cours pour déterminer la suite à donner à ce projet qui ne fait l'objet d'aucune ligne budgétaire dans la loi de finances pour 2013.

IDénum remis en selle

Face aux retards pris par la CNIe, le précédent gouvernement avait engagé le projet «IDénum», visant à promouvoir des solutions d'identification en ligne conçues par des entités privées sur des bases techniques garanties par l'Etat via l'ANSSI. Un dispositif dont la vocation est de faciliter la vie des internautes et de lutter contre la fraude à l'identité. Fin janvier, le gouvernement a annoncé qu'IDénum prendrait la forme d'une société, financée par le programme investissements d'avenir, à laquelle participent la Caisse des dépôts, le Groupe La Poste, Euro-Information (Groupe Crédit Mutuel/CIC), Pages Jaunes et SFR. IDénum proposera une solution d'identification multisupports (clés USB, carte bancaire, téléphone mobile) avec pour objectif de fédérer «le plus grand nombre d'acteurs du Web».

Parallèlement, le gouvernement a annoncé l'élaboration d'une stratégie de l'État d'ici juin 2013 en matière d'identification/authentification des utilisateurs et de sécurisation des transactions. Le présent document du pôle TES s'inscrit pleinement dans cette démarche et a vocation à alimenter la réflexion des pouvoirs publics.

Promouvoir une approche complémentaire

Au-delà des vicissitudes du projet français, on soulignera la nécessité d'un portage politique pour garantir l'adoption d'un système national de gestion de l'identité numérique par une large fraction de la population. En Estonie, pays parmi les plus avancés en ce domaine, l'utilisation de la CNIe (baptisée ID Card) au delà de la sphère administrative a fait l'objet d'un vaste plan de communication auprès de la population. Actions facilitées par la taille du pays qui équivaut à celle d'une grande ville avec seulement 1,3 million d'habitants et qui «bénéficie» d'une culture, liée au passé soviétique, propice à l'émergence d'un système hyper centralisé. Même si l'ID card est un succès dans son pays, le modèle nous parait peu transposable.

Si un projet de CNIe est remis en selle, il faudra donc veiller à intégrer un volet communication sans lequel cette carte ne sera pas optimisée. Dans tous les cas, il s'agit d'un projet à moyen terme (minimum deux ans). Sauf à passer par la voie réglementaire - ce qui est peu probable - un projet de loi nécessite quatre lectures au parlement sans compter l'avis du conseil d'État, de la CNIL et une probable saisine du Conseil constitutionnel en fin de parcours… En outre, l'audit en cours porte essentiellement sur le volet sécuritaire du projet - création d'une base de données biométriques nationale - et il n'est pas certain que le volet e-services soit relancé.

Face à cette situation, des systèmes d'identification alternatifs apparaissent indispensables car ils contribueront à créer une valeur d'usage et une acculturation de l'identité numérique sécurisée susceptible de favoriser l'adoption de la CNIe.

Intérêts et limites du modèle Estonien

Initiée par le gouvernement, l'ID card estonienne est opérationnelle depuis 2002. Souvent citée comme modèle, l'ID card parait difficilement transposable. L'ID card ne concerne en effet «que» 1,92 millions d'estoniens, soit la taille d'une métropole française et est assise sur un registre national de la population, interdit en France. On notera aussi que c'est l'adjonction de services privés (transports, banques…) associée à la possibilité d'exporter une partie des fonctions de l'ID card sur d'autres supports (mobile, clef USB) qui a permis le décollage des usages. Fin 2013 elle a généré plus de 100 millions d'e-signatures et 171 millions d'authentifications. voir http://id.ee

Utiliser l'identité numérique comme le socle commun d'un écosystème d'applications de confiance

L'usage d'abord

La problématique de la sécurité et de l'identification a été trop souvent pensée en tant que telle, en décalage avec l'usage et les risques associés.

A cet égard, on citera l'exemple de la déclaration de revenus sur internet. Initiée par l'État dans les années 2000, la procédure de télédéclaration imposait à l'origine d'utiliser un certificat offert gratuitement par l'État. Ce système s'est révélé compliqué à gérer pour les utilisateurs (installation, problèmes de compatibilité, diversité des équipements…) comme pour le ministère des Finances (hotline, maintenance…). Le ministère a finalement décidé d'abandonner l'obligation d'utiliser un certificat, pour choisir un système alternatif de mots de passe envoyés par des courriers postaux différents. Elle a aussi conduit l'État à privilégier la création d'un bouquet d'e-services administratifs avec le projet mon.service-public.fr. Ce portail repose sur un système de fédération d'identité qui permet d'accéder à sa déclaration de revenu mais aussi de réaliser d'autres démarches (Pôle emploi, sécurité sociale…) avec une authentification unique.

Le choix du dispositif technique d'identification doit donc être précédé d'une réflexion sur l'usage et les risques associés pour déterminer le bon niveau de sécurité. A l'heure du tout numérique et des restrictions budgétaires, il est également essentiel de réfléchir à des moyens de mutualiser les investissements tout en simplifiant l'usage des dispositifs.

Promouvoir des portefeuilles de services fondés sur un moyen d'identification mutualisé

La nécessité de mutualiser les coûts tout en concevant des systèmes dotés de niveaux de sécurité adaptés conduit le pole TES à préconiser une réflexion sur l'identité numérique par grandes sphères d'usage.

L'e-santé apparaît ainsi comme le secteur le plus sensible et le plus exigeant en matière de sécurité. Non seulement les données de santé touchent à notre intimité mais elles sont aussi dotées d'une valeur économique : elles intéressent par exemple notre employeur ou notre assureur et leur vol peut avoir de lourdes conséquences sur notre vie quotidienne. L'e-administration - accès aux services publics locaux et formalités administratives - constitue une seconde sphère d'usages avec plusieurs caractéristiques : une grande diversité des services, une dissémination géographique des lieux d'acceptation, des capacités d'investissement des administrations limitées. Le tourisme, enfin, exige des solutions souples pour s'adapter au public étranger et à la grande hétérogénéité des acteurs (publics, privés…) et services cibles (transports, accès, paiement…).

Pour répondre à ces besoins, le pôle TES promeut le concept de portefeuille de services (*wallet* en anglais). Ce concept vise à réunir plusieurs applications dans un «portefeuille virtuel». A l'image de son équivalent physique, il réunit en un seul endroit les moyens de paiement, cartes d'accès, billettique transport et cartes de fidélité qui encombrent nos poches. Ce portefeuille est stocké dans le compartiment étanche de la carte SIM du téléphone mobile ou de la tablette, une clé USB ou un espace sécurisé sur le disque dur du PC.

Le portefeuille de services simplifie la vie du client-usager en lui évitant d'avoir à gérer de multiples cartes. Il offre une ergonomie commune aux différentes applications et facilite leur utilisation. Il ouvre aussi la voie à de nouveaux services : personnalisation, alertes et offres spéciales, historique des transactions, réduction du nombre d'interlocuteurs en cas de problème technique... Pour le fournisseur de services, il simplifie l'enrôlement des utilisateurs, principale source de coûts et facilite la mutualisation des infrastructures de sécurité (serveur d'identité, terminaux d'acceptation).

3e proposition

Promouvoir des principes nationaux garantissant l'interopérabilité et la sécurité des systèmes de gestion d'identité

Il convient de trouver un équilibre entre une approche trop centralisée et une multiplication des dispositifs d'identification dans un contexte mondialisé.

Un enjeu mondial

L'identité numérique est un enjeu qui dépasse largement nos frontières sur lequel se positionnent tous les grands acteurs du numérique : opérateurs, équipementiers, moteurs de recherche, réseaux sociaux...

A cet égard, la réflexion du pôle TES s'inscrit dans la perspective de la nouvelle réglementation européenne sur les transactions électroniques. Si, à la différence des passeports, l'Union Européenne n'est pas compétente pour réglementer l'émission de cartes nationales d'identité, numériques ou non, elle intervient depuis 1999 sur le développement des échanges dématérialisés, perçus par Bruxelles comme un moyen de fluidifier le marché intérieur. La Commission vient ainsi de publier un projet de règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur qui prévoit que les États membres devront reconnaître les identités électroniques émises par d'autres pays membres de l'UE et les accepter pour leurs services d'administration électronique. Ce règlement, discuté en 2013, fait ressortir un certain retard en matière d'identité numérique de la France par rapport à ses partenaires européens. Néanmoins, il n'est sans doute pas trop tard pour la France de concevoir un système interopérable à même de séduire les pays membres qui ne se sont pas encore dotés de dispositifs d'identité numérique.

Des prescriptions à bien calibrer

Au niveau national, sans préjuger du devenir des projets CNIe/IDénum, les acteurs français de la sécurité ont besoin d'un cadre clair portant sur l'interopérabilité des systèmes, la simplification des mécanismes d'enrôlement et la création de larges réseaux d'acceptation.

Dans l'idéal, la création d'un serveur d'identité numérique national - qui implique la création d'un fichier des populations comme il en existe en Belgique ou en Estonie - serait la solution optimale. Cette architecture est cependant aujourd'hui refusée par la CNIL et il convient donc de se tourner vers des systèmes alternatifs en valorisant l'existant. On soulignera l'exemple de mon.service-public.fr, avec ses 4 millions de comptes créés à l'initiative des français. Ce service, qui reste sous-utilisé faute d'un bouquet de services attractif, pourrait peut-être se transformer en serveur d'identité. Dans ce schéma, l'usager pourrait autoriser un service tiers à vérifier, par exemple, son adresse ou son âge auprès de mon-service-public.fr, sans pouvoir collecter d'autres informations personnelles.

Parallèlement, le régulateur pourrait encourager les systèmes d'identification fondés sur une base hiérarchique ou des accords multilatéraux. Un tiers gestionnaire d'identité, reconnu par l'État à partir d'un cahier des charges précis, pourrait ainsi obliger deux parties à accepter les attributs d'une autre partie. On peut également imaginer des accords bi ou multilatéraux, permettant, par exemple, à une personne s'étant enregistrée dans la chaîne d'hôtel A de bénéficier d'un accès aux installations sportives d'un partenaire B sans avoir à s'enregistrer à nouveau.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

mon.Service-Public.fr
Le compte personnel des démarches en ligne

Penser les systèmes d'identification en privilégiant l'ergonomie et l'utilisabilité des services

Ergonomie et utilisabilité

Allier sécurité et facilité d'utilisation - utilisabilité diront les ergonomes - tel est le défi des concepteurs de systèmes d'identification numérique. Cette réflexion approfondie sur l'ergonomie des systèmes est le gage de leur appropriation et de leur utilisation effective par le client-usager qui gagne du temps pour une procédure jugée fastidieuse. Pour le fournisseur de services, l'utilisabilité est synonyme de davantage de trafic, de fluidification des files d'attentes, de coûts d'exploitation moindre voire de revenus supplémentaires. A l'heure du multi-équipement et de la mobilité, l'ergonomie des systèmes d'identification passe aussi de plus en plus par les terminaux mobiles que l'on emporte partout avec soi.

A cet égard, on soulignera les atouts des technologies «sans contact» fondées sur la «near field communication» (NFC) et utilisées avec succès depuis de nombreuses années pour les cartes de transport. Cette technologie, qui équipe désormais la plupart des nouveaux smartphones, allie la sécurité des cartes à puces à une grande facilité d'utilisation : le simple geste d'approcher son téléphone mobile à proximité d'une borne d'accès ou d'un terminal de paiement suffit pour accéder au service. Un dispositif dont la sécurité peut être renforcée par l'adjonction d'une authentification par code PIN (cas des paiements supérieurs à 20 euros en France) ou par biométrie.

Renverser la logique en partant du local

Face à la difficile émergence d'un grand projet national autour de l'identité numérique, il convient aujourd'hui de renverser la logique en privilégiant une approche locale fondée sur les besoins des utilisateurs et à même de s'étendre progressivement à l'ensemble du territoire.

Les leviers publics et privés sont incontournables dans ce projet. Tout d'abord les collectivités territoriales qui ont d'importants besoins en matière d'identification numérique pour le développement de la mobilité (transports publics, autopartage…), de la e-administration (formalités, démarches…) et des services de proximité (accès aux équipements, billettique culturelle, tourisme…). Les collectivités ont aussi pour caractéristique d'avoir des besoins similaires partout en France, ce qui favorise la dissémination des avancées technologiques. En complément de ce réseau d'acceptation publique, les projets en matière d'identité numérique doivent pouvoir s'appuyer sur des réseaux privés comme ceux des banques, de la Poste, les grandes chaînes hôtelières, les loueurs de voiture, la grande distribution… qui au travers de réalisations exemplaires en matière de paiement, de fidélité ou d'accès au service peuvent avoir un effet de levier important.

Cette approche par le local est en parfaite adéquation avec la logique des pôles de compétitivité et des «investissements d'avenir». Les projets initiés par le pôle TES - Easymove (voir ci-contre), Clefs de la ville (présenté page 18 «La parole aux adhérents») - après avoir été testés et validés localement ont vocation à être utilisés partout en France.

Easymove :

Dans le contexte du développement de services locaux (collectivités, services divers), Easymove apporte des solutions techniques (plateformes interconnectées) afin :

- d'éviter les enrôlements multiples et garantir la cohérence d'accès aux services,
- d'apporter une continuité et/ou une compatibilité de services entre collectivités (à plus forte raison si elles sont limitrophes).

5e proposition

Prendre en compte les exigences de la CNIL en amont des projets

La France a une grande antériorité dans le domaine de la protection des données personnelles et sa législation fait aujourd'hui école dans de nombreux pays. Bien conçue, l'identité numérique peut contribuer à minimiser la communication de données personnelles.

Identité numérique et protection des données personnelles

Les grands principes des loi de 1978 et 2004 sur la protection des données personnelles - consentement préalable, proportionnalité des traitements par rapport aux services cibles, durée de conservation des données adaptée, droit d'opposition… - sont au cœur de l'approche française en matière de gestion de l'identité numérique.

L'utilisation de moyens cryptographiques peut contribuer à sécuriser les échanges de données via la mise en place de protocoles de contrôle d'accès aux données et à la création d'un canal sécurisé de bout en bout pour le transfert de documents et d'e-signatures. Il est aussi possible de minimiser la transmission de données personnelles par une gestion intelligente des attributs associés à l'identité. Ainsi, pour savoir si un individu est majeur, il suffira à un serveur d'identité de confirmer par un oui/non le prédicat «est majeur» relatif à un individu sans autre communication de données personnelles. La fédération d'identités, alliant authentification unique et compartimentage des données personnelles propres à chaque service, est également une solution intéressante. Elle a fait l'objet d'une documentation complète dans le cadre du projet FC² labellisé par le pôle TES.

On notera cependant que l'utilisation d'un système d'identification numérique respectueux de la vie privée ne garantit pas contre les risques de profilage/traçage du service en ligne sur lequel il est utilisé. Une stratégie en matière d'identité numérique respectueuse de la vie privée a donc pour corollaire la définition d'un «droit à l'oubli» qui s'impose aux services numériques. Ce droit à l'oubli reste pour l'essentiel à construire mais on soulignera ici qu'un cadre trop rigide risquerait de porter un coup fatal au développement de services innovants, basés en grande partie sur l'analyse des comportements des utilisateurs.

Promouvoir la «privacy by design»

Actuellement, les mesures de protection de la vie privée sont largement «réactives» : on attend qu'une atteinte à la vie privée ait lieu pour agir, ou bien on établit des règlementations complexes et difficiles à faire respecter concernant ce que font les consommateurs d'identité numérique (prestataires de services) des informations privées récoltées. En conséquence, on intervient en aval du projet au lieu d'agir en amont pour prévenir l'atteinte, en utilisant des méthodes techniques spécifiques (cryptographie). La spécification Européenne IAS-ECC, d'origine Française, adresse cette problématique. La carte d'identité allemande dispose de tels mécanismes techniques*, qui par ailleurs sont bien connus et font l'objet de nombreux projets de recherche notamment Européens. C'est aussi une préoccupation du pôle TES qui a initié des projets spécifiques sur ces sujets à l'image de Lyrics.

On signalera que la «privacy by design» a largement inspiré la nouvelle réglementation européenne sur les données personnelles qui entrera en vigueur entre 2014 et 2016. Elle prévoit que la protection des données personnelles soit intégrée en amont de la conception des services et non au moment de leur mise sur le marché, voire a posteriori comme actuellement.

La «privacy by design» est particulièrement adaptée aux services d'identification utilisant le mobile NFC où la plupart des services sont en cours de mise en place. La protection des données personnelles peut être prise en amont des projets en limitant par exemple les risques de traçage et de croisements d'information. Avec ce système, par exemple, il sera impossible de savoir que tel usager d'un réseau social professionnel aura payé pour accéder à un service de recrutement et se sera exprimé dans des discussions sur tel ou tel sujet de société posté sur le net.

*Domain-specific pseudonymous signatures for the german identity card (BSI/Darmstadt University)

Privacy by design

La privacy by design vise à intégrer le respect de la vie privée directement dans la conception des services (au niveau par exemple des procédures «d'enrôlement», des protocoles et de la cryptographie) au lieu de l'ajouter postérieurement, sous forme de règles et de contraintes de fonctionnement et d'exploitation concernant les systèmes support des services considérés.

Donner pleinement la maîtrise de leurs données personnelles aux usagers des applications

En chiffres

10 % C'est le nombre d'européens ayant mené des actions pour maitriser leurs données personnelles (profil de réseau social, paramètres navigateur…).

Source BCG - enquête aout 2012

Le traçage, face cachée de certains systèmes d'identification

Les systèmes d'identification promus par Google, Apple, Facebook ou Amazon (GAFA) connaissent un grand succès auprès du public car ils sont simples d'usage et bénéficient d'un réseau d'acceptation croissant. La contrepartie de leur utilisation est le traçage des individus dont il est possible de reconstituer les comportements de consommation, les opinions, les achats ou encore les lieux par lesquels ils sont passés… De plus, ces données sont stockées quelque part sur un serveur (situé hors de France) sans véritable garantie sur leur devenir. Si en théorie, face aux critiques, ces services ont amélioré la maîtrise des données personnelles (paramétrage du profil, possibilité de destruction de compte…), une enquête menée par le Boston Consulting Group (BCG)* a montré que ces fonctions étaient rarement utilisées.

Une maîtrise des données personnelles multiformes

En pratique, la maîtrise des données personnelles peut prendre des formes très variées. Classiquement, l'utilisateur peut, avant d'accéder au service, cocher des cases pour valider les données personnelles qu'il souhaite communiquer ou rendre accessible à des tiers. Cette approche est limitée car rapidement fastidieuse et réalisée dans un contexte où l'utilisateur n'est pas informé des avantages et inconvénients de cocher ou ne pas cocher les cases. De fait, ce type de système est adapté à une minorité, plus consciente que les autres de l'enjeu du service sur la vie privée. Il doit en outre être assorti d'un «droit à l'oubli» garantissant à l'utilisateur que les données publiées seront intégralement détruites passé un certain délai.

La maîtrise des données personnelles peut aussi être liée à la technologie utilisée dans la droite ligne de la «privacy by design». On peut, par exemple, concevoir des identités numériques aléatoires et «jetables», utilisées pour un usage unique, aucune donnée n'étant conservée après usage du service. Le lieu de stockage des données sensibles peut également être optimisé. Dans le cas de la biométrie, par exemple, la CNIL privilégie les systèmes où la donnée biométrique est stockée dans la puce de la carte de son titulaire, et non dans une base de données centralisée, plus facilement piratable. La carte SIM du mobile est un autre lieu possible pour stocker de matière fiable les données personnelles, sans nécessité de connexion réseau.

La compatibilité d'un service avec la protection de la vie privée peut enfin être garantie aux nouveaux clients par les anciens utilisateurs et/ou certifiée par une autorité indépendante délivrant un label.

*Note : The Value of Digital Identity, BCG 2012
https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity

7e proposition

Valoriser le savoir-faire français dans le domaine de la carte à puce et du NFC pour gérer l'identité numérique sur mobile

Pour gérer l'identité numérique, la France dispose aujourd'hui d'un atout incontestable avec son savoir-faire en matière de cartes à puce et sa maitrise des technologies sans contact.

Les avantages du NFC pour gérer les services de proximité

Utilisée avec succès pour sécuriser les cartes bancaires et les transactions financières, la puce s'est imposée pour stocker dans les téléphones mobiles les droits d'accès des abonnés des opérateurs télécoms. Associée à la technologie de communication sans fil NFC, cette carte SIM peut aujourd'hui gérer l'accès à de nombreux services comme le paiement, l'accès aux transports ou encore la gestion d'avantages (réductions, droits sociaux…). On notera que la SIM, qui appartient à l'opérateur, n'est pas le seul «secure element» possible pour héberger des services NFC (carte de stockage SD notamment).

La technologie carte SIM/NFC a reçu la certification d'autorités régulatrices françaises comme le GIE cartes bancaires ou l'ANSSI. Reposant sur des standards internationaux, la technologie NFC a été adoptée par la GSMA, association qui réunit les grands opérateurs de télécommunication mondiaux. De leur côté, l'ensemble des équipementiers, à l'exception d'Apple, propose désormais des terminaux compatibles NFC. Dotés d'un haut niveau de sécurité et d'une forte interopérabilité, particulièrement adaptés aux applications en mobilité, les services NFC ont aussi pour avantage d'associer l'accès au service à un geste (approche du mobile du valideur) exprimant le consentement de l'utilisateur.

C'est aujourd'hui une technologie qui est déployée à grande échelle dans des pays comme la Corée, le Japon ou encore la Chine pour des services toujours plus nombreux.

Le décollage des services NFC en France en 2013

La technologie NFC a été industrialisée à Caen en 2002 par le fabricant de puces NXP qui s'appelait à l'époque Philips Semiconductors. Les premiers tests en matière de paiement (projet Pegasus) et billettique sur mobile (projet Ulysse) ont eu lieu à partir de 2006 à Caen puis dans d'autres villes (Bordeaux, Strasbourg, Rennes…). Les acteurs du NFC - banques, opérateurs mobiles, grande distribution - se sont ensuite organisés pour élaborer des spécifications visant à favoriser l'interopérabilité des applications et définir un parcours client. Le pôle TES a activement participé à ces groupes de travail techniques.

Ces avancées ont permis d'envisager un pré-déploiement commercial des services à Nice en 2010 avec quatre opérateurs mobiles, un opérateur de transports et plusieurs banques. Le gouvernement a décidé en 2012 de soutenir une quinzaine de projets NFC via le programme des «investissements d'avenir». L'agglomération de Caen-la-mer est chef de file d'un projet bas-normand ambitieux «Smart Normandy» qui vise à déployer à partir de 2013 un bouquet de services dans le domaine de la mobilité, du tourisme et de l'e-administration.

Les PME et industriels du pôle TES ont de fortes attentes à l'égard des projets NFC des collectivités locales et en particulier du projet caennais. L'émergence de services sans contact à l'échelle de territoires d'envergure va en effet contribuer à créer une dynamique nationale et fournir aux acteurs français de la confiance numérique une vitrine internationale.

2007 : Premiers tests de paiement sans contact à Caen. «Payez Mobile» issu du projet Pegasus labellisé par le Pôle TES.

Considérer le secteur de l'identité numérique comme un facteur de croissance et un enjeu de souveraineté nationale

L'identité numérique, prochain terrain de jeu de GAFA ?

Comme l'a rappelé un rapport récent qui vise à lier la collecte de données par les entreprises à la fiscalité, «les données personnelles sont la ressource essentielle de l'économie numérique. Elles permettent aux entreprises qui les collectent de mesurer et d'améliorer les performances d'une application, de personnaliser le service rendu, de recommander des achats à leurs clients, de soutenir des efforts d'innovation donnant naissance à d'autres applications, de prendre de décisions stratégiques».

Au delà des données comportementales liées à l'utilisation de leurs services ou des données de «profil», les géants du Net - et en particulier Google, Apple, Facebook ou Amazon (GAFA) - investissent aujourd'hui massivement le marché de l'identité numérique pour fiabiliser et compléter leurs bases de données personnelles. Google a ainsi lancé en 2011 un porte-monnaie électronique sur mobile, la *Google wallet*. Cette application va permettre à l'acteur californien d'affiner sa connaissance des comportements des internautes en lui donnant accès aux pratiques d'achat dans les commerces de proximité. Facebook promeut pour sa part *Facebook connect*, moyen d'identification sur le Net qui lui permet d'affiner le profilage de ses utilisateurs en connaissant leurs pratiques sur internet. Avec *Passbook*, application de gestion de tickets, billets d'avions et autres coupons de réduction, Apple va pour sa part améliorer sa connaissance des goûts et comportements de consommation des voyageurs pour proposer de nouveaux produits via son apps store iTunes. Loin de s'arrêter aux services marchands, les géants américains proposent aussi leurs services aux gouvernements. Récemment PayPal a ainsi signé avec le gouvernement britannique un accord pour gérer le système d'identification aux sites publics.

Face à une offensive tous azimuts, il est urgent que la France se positionne sur le marché de la protection des données personnelles dont fait partie d'identité numérique. Car le risque est non seulement que des térabits de données personnelles échappent à leurs utilisateurs mais aussi que le savoir-faire des PME françaises soit racheté par les géants du Net. Ces «GAFA» pourraient également imposer leurs solutions à l'ensemble du monde via leur main mise sur les organismes normatifs internationaux comme l'ETSI.

L'importance des GAFA dans les problématiques d'identité numérique pourrait générer des dépendances commerciales dangereuses pour les fournisseurs de services locaux, comme les mairies ou prestataires privés qui devraient alors se plier à la politique commerciale de ces acteurs mondiaux.

Consolider la filière de la confiance numérique

Étendant la notion d'identité digitale ou numérique à l'ensemble des données disponibles sur les individus, le cabinet de consultant Boston Consulting Group qualifie les données personnelles de «nouvelle monnaie d'échange». La valeur créée par l'identité digitale (au sens large) croîtrait en Europe de 22 % chaque année avec un bénéfice de 330 milliards d'euros… Une source de croissance qui, insiste BCG, ne va pas profiter qu'aux entreprises du web 2.0 mais à l'ensemble de l'économie.

Dans ce marché, la France a une carte à jouer en consolidant le secteur de la confiance numérique. Il s'agit de proposer des solutions offrant un équilibre entre la protection des données personnelles, le souhait des utilisateurs de partager certaines données pour obtenir des services supplémentaires et le droit à «l'oubli» et / ou à la restitution de leurs données. La mission Colin/Collin enjoint les pouvoirs publics à utiliser la fiscalité pour obliger les entreprises à «*renforcer la protection des libertés individuelles, favoriser l'innovation sur le marché de confiance numérique et à encourager l'émergence de nouveaux services au bénéfice des utilisateurs*».

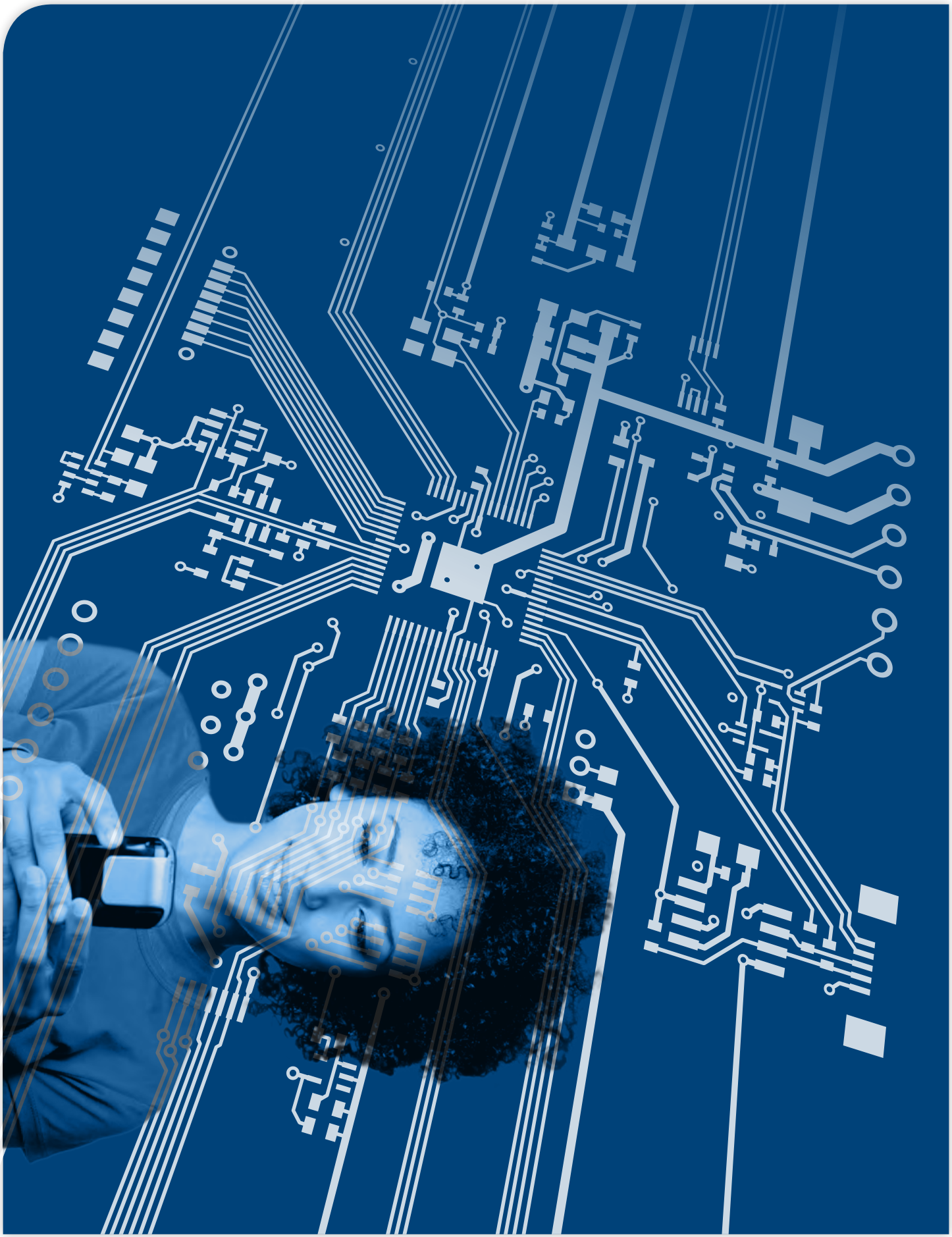
S'il n'appartient pas au pôle TES de se prononcer sur les moyens à mettre en œuvre, il ne peut qu'adhérer à ces objectifs très généraux qui doivent être complétés par des décisions à court terme sur des enjeux spécifiques au secteur de l'identité numérique.

Il s'agit notamment :

- de définir un cadre clair donnant éventuellement la possibilité de dériver des identités numériques à partir d'une identité régalienne avec la création de serveurs d'identités placés sous le contrôle de l'État ;
- d'accélérer la simplification de la réglementation sur les données personnelles visant notamment à simplifier les conditions d'enrôlement des utilisateurs et à faciliter la création de bouquets de services homogènes utilisant un identifiant unique ;
- de confirmer et d'accentuer la dynamique créée autour des services sans contact NFC. Sur ce dernier point, on soulignera l'importance de projets nationaux en matière de transports, d'accès aux services publics et de tourisme.

Contribution au débat sur l'identité numérique

En savoir plus



Contributions :

Ce document est l'aboutissement des échanges d'un groupe de travail associant les membres du Pôle TES intéressés par cette démarche. Les témoignages qui suivent reflètent l'approche de ces entreprises et collectivités en matière d'identité numérique.

La parole aux adhérents

«CEV Group a conçu les Clés de la Ville, une plateforme de gestion d'identité locale qui s'interface avec les applications métiers des collectivités territoriales. Dans le prolongement de ce projet mis en œuvre à Saint-Lô, CEV a participé au projet FC[2], centré sur la fédération d'identités entre cercles de confiance (bancaire, télécom et collectivités) où CEV était en charge du cercle Collectivités. Ce projet, aux dimensions technique et juridique, a permis d'aborder la gestion d'identité pour les inscriptions aux services des collectivités, dématérialisées sur le Web, en concevant des mécanismes d'échange d'attributs entre les cercles de confiance. Le défi de la gestion d'identité est de bien adapter les mécanismes technologiques pour aller vers des solutions ergonomiques, compréhensibles par un utilisateur qui doit rester maître de ses données personnelles».

Hervé JEAN Directeur Technique de CEV

«Les applications mobiles aujourd'hui déployées sur des millions de Smartphones capturent, transmettent et traitent des données relatives aux utilisateurs. Elles permettent un dialogue permanent entre un système central et une multitude d'entités applicatives individuelles, représentant des individus anonymes mais néanmoins caractérisés. En ce sens, elles constituent autant de «petits morceaux d'identité» de leurs utilisateurs à qui elles proposent des services personnalisés. Dejamobile met à disposition de ses clients entreprises et collectivités la puissance de cette relation-usager «one-to-one» au travers de ses solutions NFC de mobilité interactive, tout en respectant le droit à la vie privée et à l'anonymat».

Houssem ASSADI - Déjàmobile

«La gestion de l'identité numérique n'est pas un sujet futur, il est au contraire au cœur de l'actualité et des préoccupations quotidiennes des citoyens comme des entreprises. En réunissant institutions, collectivités locales, industriels et PME, le Pôle TES a une légitimité particulière pour le traiter.
Il est aujourd'hui indispensable que les acteurs français et européens de l'identité numérique apportent une réponse raisonnée sur ce sujet stratégique. Ne rien faire serait risquer de voir s'échapper la valeur que constituent les services liés à l'identité numérique et risquer que d'autres acteurs prennent place sur ce marché en imposant des solutions inadaptées».

Franck LEFEVRE - Digital Airways

«Venue de la monétique et des transactions électroniques sécurisées, Galitt intervient dans divers domaines liés à l'identité numérique. Galitt a ainsi fourni à l'armée américaine dès 2002 les outils de test pour la mise au point d'une carte d'identification fondée sur des standards désormais adoptés pour gérer la cohabitation d'applications sensibles dans le mobile. Une décennie plus tard, le sujet continue à mûrir et à stimuler l'innovation : nous sommes aujourd'hui partenaire technique de Natural Security, qui démontre que sécurité, facilité d'utilisation et respect de la vie privée sont parfaitement compatibles. Natural Security propose en effet une authentification biométrique pour les transactions de paiement ou le contrôle d'accès sans recourir à une base de données centralisée. Les applications et données d'authentification du porteur sont stockées sur un support individuel, qui peut être un smartphone, placé sous maitrise du porteur. Le support individuel est sécurisé et l'authentification repose sur une technologie sans contact, évitant toute manipulation du support que le porteur peut conserver sur lui».

Diane WALCH, Directeur Business Development de Galitt

«Territoire leader du mobile sans contact» en 2011 et retenu dans l'appel à projet Ville numérique en 2012, la communauté d'agglomération de Caen la Mer entend déployer des services mobiles intelligents sur son territoire. La gestion de l'identité numérique étant une condition sine qua non d'une telle volonté, Caen la Mer est aujourd'hui positionnée comme animateur du groupe de travail national «Identité» avec la DGCIS, la Caisse des dépôts et les collectivités retenues dans le cadre de «Villes numériques». Nos travaux ont d'ores et déjà permis d'accompagner la CNIL et le SGMAP dans la rédaction d'un arrêté concernant la gestion des «Télé-services», texte fondamental pour l'utilisation des données personnelles et la possibilité de concevoir des portails de gestion de l'identité. Pour les années à venir, Caen la Mer envisage de déployer une carte de vie quotidienne à ses 240 000 habitants. Que ce soit pour les écoles, les piscines, les déchetteries, les salles de spectacle ou les bibliothèques, ce type de carte aura plus encore d'intérêt si elle est liée à un compte usager permettant un enrôlement unique aux services proposés. Les travaux du pôle TES sont déterminants afin d'aider le territoire à faire les bons choix stratégiques et techniques.

Pierre-André Martin, Directeur de la DOSIIN - Communauté d'agglomération de Caen la Mer et ville de Caen

La vie de Julie, étudiante à Caen, simplifiée grâce à l'utilisation de son Smartphone et d'applications d'Identité Numérique

Lors de son inscription à l'université, Julie s'est rendue au service «accueil des nouveaux étudiants». Avec son smartphone elle a décliné son identité en le plaçant devant un lecteur situé à coté de l'agent d'accueil. Celui-ci, habilité à se connecter au service IDnum départemental, a pu vérifier l'état civil et la photo de Julie et récupérer deux attributs nécessaires à son inscription : sa situation de famille et sa nationalité. Il n'a pas eu accès à la filiation de Julie car celle-ci est inutile pour l'inscription. Via la plateforme en ligne nationale réservée aux universités, l'agent a aussi pu vérifier qu'elle avait bien le baccalauréat nécessaire à son inscription.

Cette formalité effectuée, le secure element intégré au smartphone de Julie a été mis à jour : elle est désormais étudiante en 1ère année d'économie à Caen. Dès lors, en se connectant avec son smartphone à l'application «accueil étudiant» de l'université - elle aurait pu aussi le faire depuis un ordinateur, mais aurait eu de toute façon à s'authentifier avec son smartphone - elle a pu compléter son inscription à plusieurs services du campus. La rubrique cantine lui a permis de définir ses préférences alimentaires, et elle a coché qu'elle était végétarienne. Elle a aussi pu réserver une chambre étudiante sur le campus. Désormais, elle accède à la cantine sur présentation de son mobile où elle sait qu'elle pourra choisir un plateau végétarien. Elle peut aussi ouvrir sa chambre avec son mobile, accéder physiquement à la bibliothèque tout comme à la salle informatique, et via internet, vérifier la disponibilité d'ouvrages dans la bibliothèque, et les réserver.

Le statut étudiant que Julie a dans son smartphone lui permet de bénéficier d'une réduction sur son abonnement aux transports en commun, mais aussi aux nombreux avantages proposés par les commerçants.

Aujourd'hui, elle achète une robe chez un commerçant où elle bénéficie d'une réduction de 10 % réservée aux étudiants. Lors de la transaction, avant le paiement, s'est affiché sur son smartphone un écran lui demandant son accord pour transmettre son statut d'étudiante, son nom et son email. Ne voulant pas être importunée par des mailings, elle a accepté de révéler son statut d'étudiante (conditionnant le rabais) mais a refusé de donner son nom et son mail en décochant ces données sur l'écran.

L'histoire de Julie :

Le groupe de travail à l'origine du présent document a souhaité illustrer les principales recommandations du Pôle TES sur l'identité numérique par la «vie de Julie». Ce cas d'usage n'a pas prétention à refléter fidèlement la réalité, nécessairement plus complexe, mais constitue une hypothèse de travail.

Service IDnum : placé sous la responsabilité de l'Etat, en mesure de faire le lien avec les autres services départements : alimenté par exemple par les données d'état civil des mairies.

Pas d'accès à la filiation : aucune donnée n'est transmise : la photo fait partie des informations d'identité numérique stockées de façon sécurisée dans son smartphone.

Utilisation de différents terminaux, suivant la situation (chez soi, ou en mobilité) et les préférences de l'utilisateur. Cependant le smartphone et sa puce sécurisée sert de référence sécuritaire.

Utilisation de différents canaux de communication, adaptés au local (NFC) ou au distant (NET).

Le principe de contrôle et de minimisation des données personnelles fournies permet à Julie de montrer qu'elle est étudiante, sans donner plus d'information.

L'intérêt primordial du smartphone pour l'utilisateur, comme moyen de dialogue et de filtrage des requêtes (lorsque des données personnelles sont demandées par un prestataire, préalablement à l'obtention d'un droit pour un service de ce prestataire).

Un peu plus tard, Julie désire s'abonner au journal «Les Echos» qui propose une offre gratuite réservée aux étudiants en économie. Le site peut recevoir de manière sécurisée le statut d'étudiante de Julie qui se trouve stocké dans la puce sécurisée de son smartphone. Après avoir fourni son mail elle obtient une carte «Les Echos» qui apparaît dans le porte-carte de son smartphone la même «carte» apparaitra dans son PC. Elle n'aura désormais plus à fournir à chaque connexion les id/pw qu'elle conservait jusqu'alors dans son PC, dans un fichier Excel, lui-même protégé par un mot de passe soit disant confidentiel (sa date de naissance).

L'aspect multi-terminal apparaît ici aussi, avec l'obtention de droits d'accès utilisables sur différents terminaux, grâce à l'interposition d'un serveur d'identité et de droit.

Pour faire face à ses dépenses, Julie a besoin de contracter un prêt étudiant et se rend dans une banque. Elle présente son mobile pour prouver son statut d'étudiant et déclare que son père se portera caution. La banque a également accès au service IDnum national et est habilitée à récupérer des informations sur sa filiation. La banque peut dès lors élaborer le projet de contrat de prêt et envoyer de manière sécurisée le dossier sur le mail de Julie et la demande de caution à son père. Avant de partir, la conseillère bancaire propose à Julie des réductions comme cadeau de bienvenue. Après avoir donné son accord le wallet de son mobile s'enrichit d'un onglet «réductions» réservées aux clients de la banque. Julie en profitera plus tard, en réservant une chambre dans une chaîne hôtelière partenaire de la banque à l'occasion d'un séjour à Strasbourg.

IDnum est un serveur racine auquel peuvent se connecter des entités privées habilitées par l'Etat comme des banques ou des opérateurs télécoms… pour vérifier les données d'identité nécessaires à la réalisation de certaines prestations.

Pour se rendre à Paris le week-end suivant, Julie a chargé l'application billettique RATP sur son smartphone et a profité de l'offre «WE à Paris» avec une réduction pour les étudiants. Elle peut ainsi prendre le train, le métro, le RER et un vélib en présentant à chaque fois son mobile pour valider son trajet, grâce au NFC. En lisant la description de ce service sur le site RATP, elle a vu que les mots anonymat et intraçabilité apparaissaient souvent, et que d'autre part, ce titre est personnel, et susceptible d'être contrôlé, et que dans ce cas elle aura à prouver son identité avec sa photo affichée sur l'écran de son smartphone.

Ici, est fait un parallèle entre l'obtention d'un droit tel que l'accès au journal «les echos» et l'accès au métro parisien durant un week-end. Il est évident que la complexité du cas RATP est bien plus grande, mais il semble utile de cacher cette complexité à l'utilisateur par une approche harmonisée. Par ailleurs, il est clair que le cas RATP nécessite l'anonymat et l'intraçabilité des accès au métro, pour respecter les règles déjà en vigueur pour le pass NAVIGO anonyme.

La photo fait partie des informations d'identité numérique stockées de façon sécurisée dans son smartphone.

Un modèle des échanges de données d'identité numérique

La figure ci-dessous synthétise un certain nombre de points apparaissant dans le document, notamment ce qui concerne les aspects «multi-terminaux» et «multiusages» qui nous apparaissent fondamentaux.

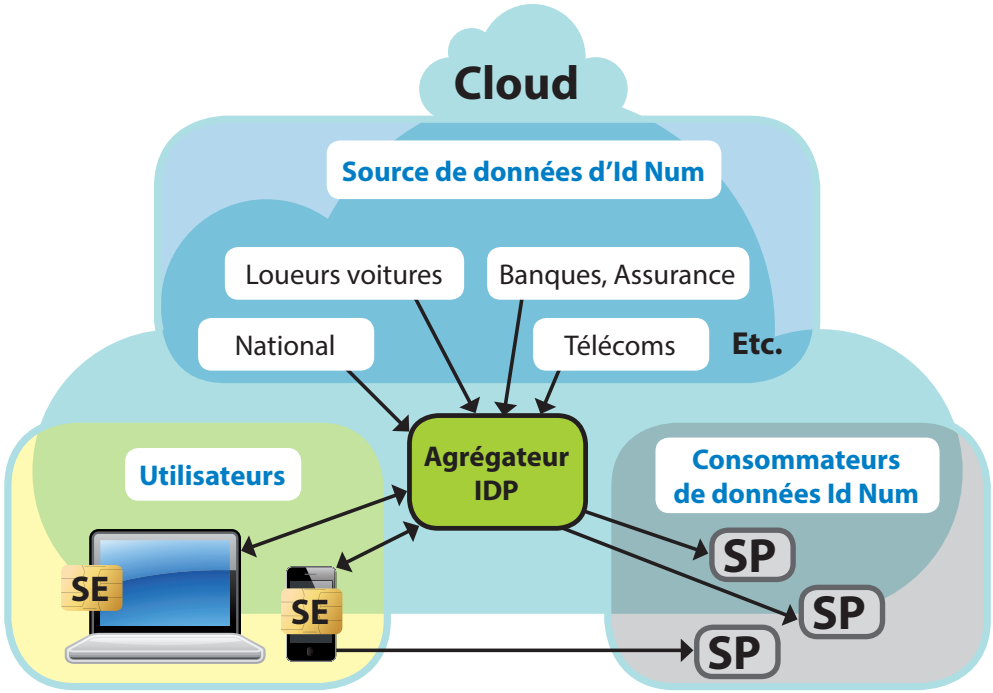
Les sources de données d'identité numérique sont diverses et agrégées dans le cloud par une (ou plusieurs) entités «agrégateur» appelées aussi IDP (Identity Provider). Les consommateurs de données d'identité numérique sont des prestataires de services SP (Service Providers). Il reçoivent ces données d'utilisateurs ayant divers types de terminaux, dotés d'un SE (Elément de Sécurité).

Les consommateurs de données peuvent également être des sources de données. La création d'une identité numérique de confiance est étroitement dépendante de la qualité et de la fiabilité des données qui ont permis de la créer. Le niveau de confiance d'une identité dépend bien-sûr du minimum des niveaux dans la chaîne qui a permis de l'établir.

Le SE doit contenir de façon sécurisée un sous-ensemble plus ou moins grand des données numériques de l'utilisateur. Il est vu ici comme un genre de mémoire cache des données de l'utilisateur connu par le ou les IDP. Cette mémoire cache doit être mise à jour automatiquement (synchronisation) pour que son contenu soit cohérent par rapport aux évolutions des identités numériques de l'utilisateur. Ces évolutions seront fréquentes si l'on se conforme à l'acception large de l'identité numérique proposée par ce document.

Plusieurs modes de consommation de l'identité numérique sont possibles :

- **Direct :** c'est le cas par exemple du NFC entre un smartphone et un terminal appartenant à un SP. Le SE garantit l'intégrité et l'authenticité des informations communiquées au SP,
- **Indirect via l'IDP :** c'est le choix classique de nombreux systèmes d'identité numérique (OpenID par exemple) où l'attribut désiré par le SP est donné par l'IDP au SP sous contrôle de l'utilisateur. Le SE sert plutôt dans ce cas à authentifier l'utilisateur par l'IDP.



Pôle de compétitivité Transactions Electroniques Sécurisées
Campus EffiScience - 8 rue Sédar Senghor -14460 Colombelles
02 31 53 63 30 - contact@pole-tes.com

En complément, un glossaire très complet de tous les termes de l'identité numérique est en ligne sur le site du Pôle TES :
www.pole-tes.com

Le Pôle TES est soutenu par :

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA RÉGION BASSE-NORMANDIE

RÉGION BASSE NORMANDIE

Conseil Général Calvados

CAEN Normandie

communauté de communes de l'agglomération saint-loise

LES PÔLES DE COMPÉTITIVITÉ
MOTEURS DE CROISSANCE ET D'EMPLOI