L’identité électronique s’impose

Joël Vanoverschelde
Partner
Technology & Enterprise
Application
Deloitte

Damien Ghielmini
Director
Technology & Enterprise
Application
Deloitte

Loic Saint Ghislain
Senior Manager
Technology & Enterprise
Application
Deloitte

Ismael Cisse
Manager
Governance, Risk
& Compliance
Deloitte

L'avènement et l'irrésistible montée en puissance de l'eID (« carte d'identité électronique ») est tout sauf une surprise. Les évolutions des technologies numériques, la mobilité, les facilités d'accès multi-canal aux services privés créent les conditions naturelles d'une demande similaire de la part des citoyens-clients vis-à-vis des services publics. Cette évolution a clairement été mise en évidence par Deloitte via son étude sur le devenir des services publics, et la dématérialisation (« digital ») à horizon 2020. Cette étude réalisée sur plus d'un an en consolidant les expertises de l'ensemble des acteurs actifs dans la sphère gouvernementale, et para publique, destinée à être régulièrement mise à jour, est disponible librement sur Internet, et l'évolution mentionnée se trouve par exemple sur http://government-2020.dupress.com

Plus les opérations, et enjeux, réalisables à distance, 24 heures sur 24 et 7 jours sur 7, à partir d'une authentification forte, sont nombreux et conséquents, plus l'intérêt de s'y impliquer est patent pour les organisations criminelles

Un besoin toujours accru d'identifier une personne …

Le besoin d'identifier de manière certaine un individu, qu'il s'agisse d'un citoyen, cas usuel, ou d'une personne en général (résident, ..) croit inévitablement avec la multiplication des opérations que l'on peut réaliser en ligne, sans contact direct. Lorsque l'individu est considéré comme faisant partie d'une organisation (cas typique: employé d'une société et habilité à la représenter avec un certain niveau d'autorité), la problématique est encore plus sensible. Dans un tel cas des éléments de complexité apparaissent naturellement: dimension temporelle plus forte, besoin accru de de contrôle et de traçabilité des opérations et mécanismes d'interruption en cas de cessation du lien de représentation pour gérer in fine une seule identité.

… et une menace qui croit en conséquence

En corollaire à la montée en puissance et en diversité de ces types de situation le niveau de menace qui caractérise notre société moderne croit exponentiellement car il se nourrit de l'explosion de la diffusion de ces opérations réalisées sans contact direct, qu'il y ait à l'origine un impact financier ou pas. Plus les opérations, et enjeux, réalisables à distance, 24 heures sur 24 et 7 jours sur 7, à partir d'une authentification forte, sont nombreux et conséquents, plus l'intérêt de s'y impliquer est patent pour les organisations criminelles. A ceci s'ajoute le fait que les gains sont souvent faciles, moins risqués (la législation peine à suivre et les moyens d'investigation sont dramatiquement lents), et les plaignants en position de faiblesse. L'usurpation d'identité, qui concerne chacun d'entre nous, et ce dans l'ensemble de ses dimensions sociales (citoyen, administré, employé, parent, simple acteur d'un réseau social, ..) est de facto un fléau de nos sociétés modernes alors que paradoxalement nous n'avons jamais eu autant de moyens de capturer, et échanger, des données sur chacun d'entre nous.

Une inexorable montée en puissance …

Si l'on revient au service élémentaire, dans lequel un document d'identité permet à un citoyen de déclencher une procédure administrative, ou à tout le moins de justifier de qui il est, on se rappelle qu'historiquement les besoins d'accès aux services eGovernment n'impliquaient pas forcément un document d'identité de sécurité, ni plus prosaïquement une démonstration de l'identité. Les premiers services étaient fréquemment relativement basiques, dans la forme, le niveau de contrôle et même l'enjeu et le gain opérationnel (réduit). Exemple type: accès à un formulaire, fréquemment téléchargé, plus rarement interactif, et envoi d'une demande, souvent par e-mail. Dans ces périodes finalement pas si anciennes, la notification d'un identifiant (ex. n° national) suffisait fréquemment, et le risque était ipso facto limité par les possibilités de contrôle et le traitement en différé.

Depuis le début de ce siècle notamment, les gouvernements, sous l'impulsion de la Commission Européenne, se sont engouffrés dans cette voie consistant à multiplier l'offre de services numériques. Ceci se justifiait autrefois pour des raisons d'image de marque interne et/ou de facilitation de la vie du citoyen avec des plages d'accès plus larges: qui n'a jamais pesté contre un guichet fermé alors qu'a contrario notre temps disponible pour s'y rendre ne cessait de s'amoindrir et que les besoins de documents administratifs ne baissaient pas réellement ?

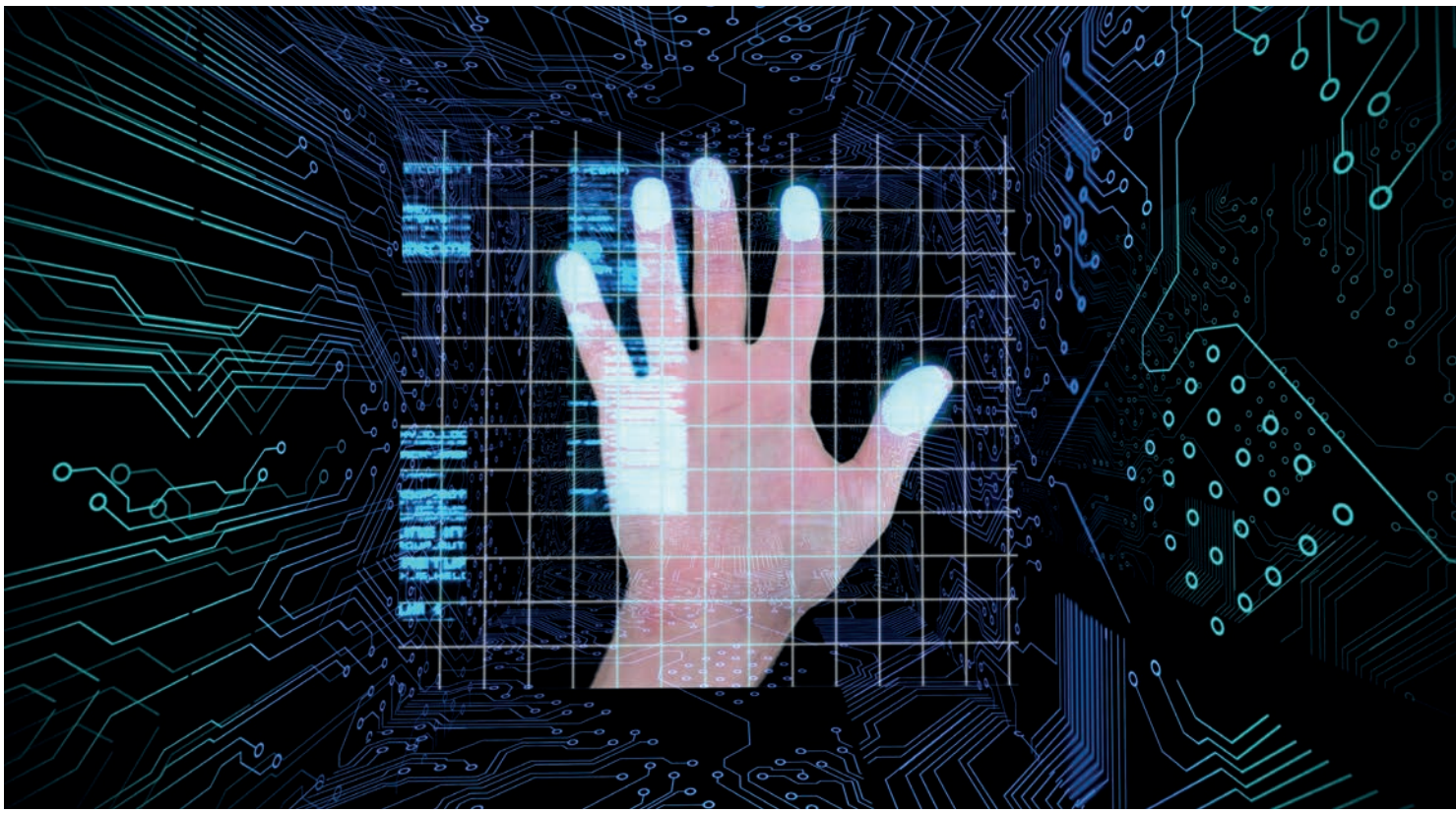
Dans une époque que l'on peut qualifier d'intermédiaire des objectifs visant à optimiser les moyens (humains), la réactivité dans la mise en place de réponses adaptées, ou la recherche d'efficacité opérationnelle ont pris le relais et sont durablement inscrits dans les réflexes des gouvernements et administrations.

… et logiquement l'émergence de nouveaux équilibres

Désormais la compétition entre pays a pris place (amélioration de l'image de marque du pays cette fois, génération de revenus tirés de la propriété intellectuelle, attraction des talents auprès des jeunes générations internationales avides de dynamisme et élevées dans un monde ou Facebook et Wikipedia ont remplacé l'encyclopédie papier d'antan) avec des produits de plus en plus modernes, des séquences d'écrans et prises de décision élaborées et un niveau de complexité qui n'a plus grand-chose à envier au privé. La sophistication des services administratifs, gouvernementaux en particulier, est en fait logique. Elle se nourrit de la conjonction du foisonnement des réglementations, dont notre époque, particulièrement craintive, est friande, et de mouvements tectoniques majeurs (transferts de service au privé, délocalisation, coopération entre états, ..) auxquels les gouvernements sont soumis. Elle répond également à un besoin de prise en compte d'un degré d'exigence accru du citoyen consommateur qui de plus en plus veut comprendre chaque élément de décision (texte de loi, jurisprudence, options).

Si l'on se réfère à des tendances révélées par l'étude GOV2020, relative au futur des services gouvernementaux, menée par Deloitte, le transfert de certaines opérations au privé, que l'on connait traditionnellement via les PPP (partenariats public privé), qui s'inscrivent dans des opérations lourdes, de longue durée, va s'étendre à des cas plus nombreux ou les gouvernements s'appuieront sur des sociétés franchisées pour réaliser certaines opérations simples. Ce type de situation existe déjà pour les opérations lointaines, telles que les recensements de demandes de visas, dans des pays du bout du monde. Quoi qu'il en soit cette ubiquité de la présence publique contribue également à augmenter le degré d'exigence lié à l'authentification, et au traçage, pour le demandeur et pour le professionnel, et ce de manière homogénéisée.

De plus en plus une authentification forte de la personne connectée est donc requise car c'est à partir de ce niveau de garantie que des opérations à forte complexité, et donc valeur ajoutée, sont envisageables. Cette tendance structurelle s'accompagne d'un besoin de simplicité dans la détermination de cette authentification forte. Une partie du challenge se trouve dans la combinaison de ces dimensions: infaillibilité, fréquence et simplicité.



La carte d'identité électronique d'aujourd'hui …

La multiplication des tokens, petits, pratiques, peu onéreux, mais relativement spécifiques, reste laborieuse. Certes des acteurs majeurs émergent, tels que LuxTrust au Grand-Duché permettant d'accéder aux systèmes d'une série de grandes banques, mais des barrières demeurent conduisant de facto à la possession fréquente de plusieurs tokens. En parallèle la relative lenteur d'introduction de cartes d'identité électronique à puce, avec certificat, qu'elles soient avec ou sans contact, et peut-être aussi le besoin d'imaginer un espace de stockage personnel proche et transportable (type coffre-fort personnel) ont contribué à rendre crédible l'hypothèse d'une "clé universelle", d'origine étatique, apte à des usages mixtes, tant publics que privés.

Cette clé peut aussi être perçue comme un premier pas vers une "clé des clés", sachant qu'aujourd'hui chaque individu dispose, et se remémore (ou essaie …) d'une multitude de mots de passe, pour des usages professionnels ou privés, avec la contrainte d'avoir à les changer régulièrement. De là l'imagination saute très vite le pas vers une clé de référence, dont l'accès pourrait être plus sophistiqué et intégrant le plus haut degré de protection, y compris demain avec des moyens biométriques. Cette clé serait le sésame pour accéder à une boite des autres clés, ce que des acteurs privés tentent, ou ont déjà tenté de réaliser mais qui nécessite à nos yeux une garantie de niveau national, voire supranational, pour se développer.

Si l'on se réfère à nouveau à l'étude sur les services gouvernementaux à horizon 2020 (http://government-2020.dupress.com) rien n'interdit d'imaginer à l'extrême des moyens de reconnaissance faciale pour ouvrir l'accès à une carte qui, in fine, contiendrait alors l'ensemble des données utiles à un individu, soit directement au niveau de la carte (i.e dans la puce), soit dans des endroits hyper-sécurisés ou seule une combinaison de clés permet alors d'entrer. La limite de ce genre d'approche peut se trouver au niveau des agences chargées de la protection des données, telle la CNPD à Luxembourg, qui fort logiquement demanderont à avoir des preuves indiscutables, et sans doute des périodes d'observation, avant de telles avancées. Le consentement, même éclairé, du citoyen sera probablement un passage incontournable mais sauf à imaginer des usages, publics/ privés, novateurs et susceptibles de déclencher une adhésion massive, et une pression sur les agences, ce type de situation ne se dessinera que sur le long terme.

Puisque l'on parle d'usages, il est logique de se poser la question du degré d'utilisation, en fréquence et en variété, pressenti pour des cartes d'identité électroniques puisqu'il est clair que la seule justification de contrôle de l'identité à des fins régaliennes (Police, Douanes, ..) n'est qu'un objectif très élémentaire. Disposer d'un document d'identité au top de la technologie et de la sécurité ne suffit donc pas forcément. Pour qu'un cercle vertueux s'engage, et l'univers de l'informatique et de la téléphonie le démontre chaque jour, il faut qu'un standard se mette en place et que les usages réalisables à partir de ce standard, ou de cet éco-système (on parle d'usage "IN"), soient visiblement plus nombreux que les usages qui nécessitent un moyen alternatif (usages "OUT"). Une telle dynamique ne pourra se créer que si des interconnexions fortes sont possibles entre les documents des différents pays, autrement dit que si une eID Luxembourgeoise par exemple est reconnue de manière globale par une série de sites gouvernementaux européens.

Fort opportunément une telle interopérabilité est en marche, toujours sous l'impulsion de la Commission Européenne. Son nom … eIDAS (règlement (EU) No 910/2014). Plus qu'une interopérabilité eIDAS est en fait une approche visant à une reconnaissance mutuelle des schémas d'identification électronique nationaux (par exemple les documents d'identité électroniques nationaux) entre les pays membres. Ceci implique mécaniquement des moyens de contrôles permettant à chaque pays de s'assurer de la validité de documents d'autres pays, et donc notamment niveaux de sécurité et des protocoles d'échanges harmonisés. Pour les citoyens des pays qui adhéreront à cette approche, ouverte à tous, des simplifications majeures se dessineront, que ce soit au niveau de la reconnaissance mutuelle des documents d'identité électroniques, mais surtout de l'accès aux sites web, gouvernementaux ou non, et à la signature électronique qui sera reconnue à un niveau transfrontalier.

Les avancées au niveau des déplacements intra-européens des personnes peuvent sembler de prime abord modestes, avec potentiellement le risque d'avoir plusieurs groupes de pays à plusieurs vitesses (Schengen ? eIDAS ?) mais en pratique c'est bien l'utilisation native de son document d'identité électronique national partout qui se dessine, que ce soit pour s'inscrire auprès d'une université étrangère, ou pour attester globalement de son identité dans un autre pays auprès d'un acteur quelconque.

Pour les pays eux-mêmes, nul n'est en mesure de dire aujourd'hui si ceux qui seront prêts les premiers, pour les sites gouvernementaux, mais surtout pour les sites marchands, vont bénéficier d'un afflux supplémentaire de demandes, ou plus raisonnablement jouir par la suite d'une position privilégiée. Notre analyse est que les avancées et initiatives gouvernementales, comme par exemple celle de l'Estonie, vont de facto crédibiliser les propositions d'acteurs privés, à forte identité nationale et issus des mêmes pays. C'est indirectement une manière de diversifier l'économie et c'est une thématique majeure au niveau du Grand-Duché.

Dès 2014, date de l'introduction de cette nouvelle régulation, 2015, de la reconnaissance des schémas d'identification électronique sur base volontaire entre états membres, et jusque 2018, date de la reconnaissance mutuelle obligatoire des schémas d'identification électronique notifiés à la Commission Européenne pour l'accès aux services publics en ligne, des sites publics et des marchands vont progressivement valoriser les facilités induites par la reconnaissance des documents d'identité électroniques. A minima cela contribuera à dynamiser l'image de marque du pays, voire drainera certains types de procédures ou facilitera l'accès à certains services aujourd'hui peu concurrentiels. On pense par exemple aux services de soins, et donc pas uniquement certains types de chirurgie (ex. dentaire), pour lesquels certaines barrières, largement psychologiques, pourraient tomber, et donc générer une concurrence plus globale, ou à tout le moins une redistribution des réflexes et "parts de marchés". L'intégration Européenne est de facto déjà largement en route avec la carte de sécurité sociale standardisée Européenne, traditionnelle (sans puce), et l'intégration de facilités au niveau de l'eID aurait pour corollaire immédiat de réduire l'encombrement dans les portefeuilles (moins de cartes ...), avancée pas forcément aussi anodine qu'il n'y parait.

… et des perspectives de déploiement prometteuses, si les conditions sont réunies

Toutes ces projections s'inscrivent dans un futur relativement proche, et dans une dynamique pan-européenne. De là à imaginer que les cartes d'identité électroniques remplacent un jour les passeports, voire d'autres documents d'identité et/ou de voyage il y a un pas que nous ne franchirons pas. Plus proche de nous, sur le territoire Luxembourgeois, et certainement, espérons-le, plus rapidement, des avancées sont envisageables au niveau des services publics, dans le domaine de la santé, qui est un débouché naturel, mais pas exclusif, voire dans le domaine privé (exemple avec les pharmacies, effectivement toujours dans le domaine de la santé). Pour que ces avancées significatives trouvent un terrain fertile et se réalisent pratiquement il faut au préalable créer les conditions de la confiance par rapport aux cartes actuelles, et au certificat qu'elles contiennent, sachant qu'aujourd'hui les demandeurs de cartes d'identité Luxembourgeoise ne choisissent pas tous l'option du certificat.

Les motivations d'une telle situation sont sans doute autant dans la perplexité vis-à-vis des usages futurs, non ou mal connus ou imaginés, ou une méfiance de principe devant une telle technologie. Ce n'est en tout cas pas le coût, identique avec ou sans certificat, qui influe. Il serait aussi probablement possible, comme cela a été le cas en Belgique, de dépasser le cadre purement national de la carte d'identité Luxembourgeoise pour servir également les résidents, voire plus largement encore. Ce décalage entre la population initiale (nationaux) et une population beaucoup plus large en volume est une caractéristique structurelle du Grand-Duché et pourrait aussi contribuer à faciliter les conditions d'une plus grande cohésion, qui se traduirait par des facilités identiques offertes au plus grand nombre, sans distinction. Ce serait à tout le moins sans nul doute un signal dans la bonne direction.

Conclusion

Très concrètement, au niveau e-santé, rappelons que 300.000 cartes d'identité Luxembourgeoises sont la cible ultime, nouveaux-nés et séniors compris, alors qu'environ 2.000.000 de personnes sont concernées, au niveau de la Grande Région, par l'offre de soins du Grand-Duché. Cela situe clairement l'écart qu'il faut, potentiellement, combler, et les différences d'échelle pour passer d'une carte d'identité électronique stricto sensu, à vocation de simple identification et titre de transport intra UE, à une carte avec une combinatoire d'usages, et d'usagers, d'une toute autre ampleur. Au-delà de l'interopérabilité du monde public, l'extension corollaire et coordonnée des usages privés (connexion aux sites des banques), ou mixtes (accès à des données de base par les pharmaciens) est la condition évidente à une monté en puissance, gage d'améliorations patentes pour les citoyens ; une fois cet objectif atteint, avec une eID devenue le "couteau suisse" des accès, seule l'imagination sera un frein au développement des usages.