WISeKey

10 juin 2005

Contribution de l'Organisation Internationale pour la Sécurité des Transactions Electroniques (OISTE) et de la société WISeKey SA au meeting thématique sur la cybersécurité – ITU WSIS

VERS L'ETABLISSEMENT D'UNE SOUVERAINETE NATIONALE NUMERIQUE

De nombreux pays ont basé leur cadre législatif sur le code napoléonien élaboré au début du 19e siècle. A travers cette inspiration commune, il est possible d'ébaucher les contours de la notion de souveraineté nationale dont la pierre angulaire est l'indépendance nationale et l'autodétermination. Ce principe est, par exemple, très explicite en droit français, l'article 3 de la Constitution de 1958 posant comme principe fondamental que « *la souveraineté nationale appartient au peuple, qui l'exerce par ses représentants et par la voie du référendum ».*

Dans un monde physique tel que nous l'avons connu jusqu'à l'avènement de l'ère numérique initiée avec la création en 1946 du premier ordinateur – ENIAC –, les Etats avaient réussi à assurer leur souveraineté. La majorité des interactions avec des pays tiers étaient assujetties à des traités internationaux et les mouvements des individus contrôlés par des politiques d'immigrations. Mais avec la publication en 1981 de la norme « RFC 793 », standardisant le protocole de communication d'Internet – TCP –, puis l'invention des technologies hypertextes et du web au début des années 90 par Tim Berners-Lee et Robert Caillau au CERN à Genève, la notion de frontière nationale a été remise en cause. Cela a notamment eu pour corollaire un affaiblissement de la souveraineté de nombreux Etats soumis au dictat technologique des nations les plus avancées, voire de sociétés privées.

Les Etats n'ont pas su apporter une réponse adéquate à la protection de leur souveraineté dans un monde dématérialisé. La plupart se sont contentés de faire évoluer, de manière partielle et souvent inadéquate, leur cadre législatif. Les plus avancés ont lancés des projets de eGouvernement, ces derniers n'étant, pour la majorité, qu'un report vers un média électronique de processus administratifs existants. Ces démarches, bien qu'intéressantes et prometteuses, n'en restent pas moins principalement axés autour des administrations et non pas autour du citoyen.

Dans leur course, souvent désordonnée, pour entrer dans l'ère numérique, les gouvernements ont perdu de vue qu'étendre leur souveraineté dans la sphère digitale était à la fois une responsabilité principale et un défi majeur; l'un des éléments clés de la souveraineté d'un état étant, au-delà de son territoire, son peuple, ses citoyens.

L'un des liens les plus forts entre l'état souverain et le citoyen est assuré par la notion d'identité, l'état garantissant l'identité d'un individu et ce dernier reconnaissant son appartenance à une nation.

Dans le monde physique, ce lien est matérialisé par un document d'identité. Les premières références au concept de passeport remontent aux environs de l'an 450 avant Jésus-Christ alors que Néhémie, fonctionnaire auprès du roi Artaxerxès de la Perse ancienne, se rend en Judée. Le roi remet à Néhémie une lettre à l'intention « des gouverneurs de la province au-delà de la rivière », les sollicitant de lui assurer un sauf-conduit durant son passage sur leurs territoires. Depuis maintenant plusieurs dizaines d'années, les citoyens de la plupart des pays ont le moyen de prouver leur identité, que ce soit au travers d'une carte d'identité ou d'un passeport. Ces documents, qui au final ne sont que papier ou plastique, ne doivent leur légitimité que par le garant qui l'émet, à savoir l'Etat.

Dans le monde numérique, l'identité des acteurs n'est actuellement souvent pas garantie. Cette faiblesse est endémique à Internet et, déjà en 1993, un dessin satyrique de Peter Steiner paru dans le New Yorker et, devenu célèbre depuis, titrait « Sur Internet, personne ne sait que vous êtes un chien » :

[1]

Cela illustre l'incapacité qu'ont eu et, qu'ont toujours, les Etats à donner une identité numérique à leurs citoyens. Cette absence d'identification forte a comme corollaire la majorité des problèmes de cybersécurité actuels. Dans un monde où tout un chacun peut se cacher derrière une forme d'anonymat, toutes les dérives ont pu être observées.

C'est notamment le cas de la problématique liée aux courriers électroniques non sollicités aussi connu sous l'acronyme SPAM. Le principe du courrier anonyme existe depuis que les premiers services postaux ont été instaurés. Néanmoins, l'envoi, à large échelle, de courriers physiques se heurtait à des limitations physiques notamment liées aux coûts de l'affranchissement. Mais ces barrières naturelles ont disparu dans le monde électronique, la différence de coûts entre l'envoi d'un courrier électronique ou de plusieurs millions étant marginale. En outre, en l'absence d'un moyen d'identification fiable des expéditeurs, les systèmes et serveurs de gestion des courriers électroniques ont dû être conçus de manière à accepter tous les courriers même si l'auteur était anonyme ou si son identité ne pouvait pas être vérifiée.

De plus, l'adresse électronique est aujourd'hui utilisée, par défaut, comme l'un des vecteurs d'identification des utilisateurs. Cela revient à dire que des structures privées telles que des

[1] The above cartoon by Peter Steiner has been reproduced from page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20)only for discussion, evaluation, research and complies with the copyright law of the United States as defined and stipulated under Title 17 U. S. Code.

employeurs, des écoles ou encore des entreprises commerciales comme Yahoo ou Google se muent en entités souveraines garantes de l'identité des millions de personnes.

Il n'est pas concevable que des états souverains acceptent cette situation de fait où des nations subordonnent l'identité numérique de leurs citoyens à des entreprises privées.

Il convient donc de donner une nouvelle dimension à la gestion des identités électroniques. Internet, de par son essence même, réservera toujours une part importante à l'échange d'informations sous le couvert de l'anonymat ou de pseudonymes, notamment dans le cadre de constitutions de communautés à l'instar des développements open source ou des encyclopédies libres comme Wikipédia. Mais lorsqu'il s'agit d'interactions dématérialisées exigeant une dimension formelle ou contractuelle, il convient de doter le citoyen d'une identification numérique certifiée.

C'est la raison pour laquelle, OISTE et WISeKey SA formulent les propositions suivantes :

- Etablir et adopter, aux niveaux nationaux, régionaux et internationaux, des standards applicables aux identités digitales.

- Supporter le déploiement dans chaque pays d'infrastructure de gestion des identités numériques des citoyens.

- Elaborer, en collaboration avec des acteurs issus de l'économie privée, des modèles de partenariats publics-privés (PPP) visant à rendre économiquement accessibles ces solutions à une large part de la population mondiale.

- Instituer, au niveau international, une autorité d'approbation des politiques (Policy Approval Authority – PAA) liées aux identités digitales afin de permettre une interopérabilité administrative et légale des identités numériques nationales.

- Reconnaissance, d'un point de vue technique, d'une Clé Primaire Internationale unique permettant le déploiement technique de l'interopérabilité, régie par la PAA

Genève, 10 juin 2005

Contacts :

Carlos Moreira, Président
carlos@wisekey.ch

Juan Avellan, Chief Legal Officier and VP Corporate Development and Policy Chief
Juan@wisekey.ch

Marc Besson, Director Professional Services
mbesson@wisekey.ch

Benjamim Ferreira, VP e-gouvernement and Int'l Organizations Relations
benjamim@wisekey.ch