Identités numériques

Document de position de l'association faîtière ICTswitzerland

1. Situation initiale dans le monde «analogique»

D'ordinaire, les citoyens/-ennes, habitants/-es de notre pays justifient leur identité auprès des administrations, des représentants administratifs, ou si nécessaire auprès de partenaires commerciaux (par exemple banques en nouant une relation d'affaires) en présentant au service ou à la personne concerné un document authentifié par un notaire ou une pièce d'identité officielle (passeport, carte d'identité).

Cet état de faits se déroule ainsi lorsque nous évoluons dans des «réseaux» traditionnels (tels que ferroviaire ou routier) et que nous devons justifier notre identité. Personne ne se formalise du fait que nous donnons régulièrement notre identité lors de contrôles, à moins d'avoir quelque raison inavouable.

Ces documents servent de preuve concernant l'identité de leur propriétaire et donnent également des renseignements sur les données et informations relatives à l'individu. De telles données sont stockées et actualisées dans les registres de la Confédération, des cantons et des communes concernés. Il en va également ainsi pour les extraits du registre du commerce et les sociétés qui y sont inscrites (personnes morales), pour les autorisations d'exercer et les procurations faites aux mandataires commerciaux.

2. Données du problème dans le monde «numérique»

Avec la diffusion du Vidéotex (Minitel), de l'Internet (particulièrement le World Wide Web), des appareils de téléphonie mobile, et avec l'utilisation d'informations et services basés sur un réseau, la question de l'identification sécurisée et sans défaut des différents acteurs (fournisseurs, intermédiaires, utilisateurs) lors des transactions en ligne s'est alors posée avec une importance croissante. Dans les faits, l'identification en ligne de nouveaux clients ne se trouve pas au premier plan. C'est l'autorisation de clients déjà enregistrés et identifiés de manière analogique traditionnelle qui est au centre des préoccupations.

Ces domaines d'utilisation, étant donnée la nature des affaires posant des exigences élevées en matière de sécurité et de possibilités de contrôle (p. ex. telebanking avec les banques suisses) sont réglés par des processus qui ont été clairement définis dès le début. Les moyens et procédés utilisés, qui n'ont pas toujours entièrement correspondu aux exigences des clients, ont été constamment améliorés. A l'heure actuelle, les solutions proposées par les grands instituts sont considérées comme sûres, fiables et résistantes aux attaques.

De telles constatations ne sont pas valables pour les acteurs qui se rencontrent pour la première fois par voie électronique et lors de transactions en ligne, et qui n'ont pas été préalablement identifiés de manière traditionnelle par une pièce d'identité. Afin d'assurer une identification sûre et sans équivoque dans de telles conditions, notamment en cas d'exigence légale, des moyens techniques doivent être mis à disposition et des bases légales créées rapidement.

Etant donné que de nombreux acteurs considèrent ce monde virtuel comme un nouvel espace d'action largement dépourvu de droits et de lois, ils se trouvent gênés lorsqu'il s'agit, à la demande légitime du partenaire de la transaction, de décliner leur identité sur le réseau électronique, alors même qu'ils le feraient sans autre dans le monde réel, que ce soit dans le train ou sur la route. L'envie d'anonymat, le besoin de se cacher derrière un pseudonyme dans le réseau en ligne connaît un essor sans précédent, pour des raisons qui restent encore à éclaircir.

3. Identités numériques lors de transactions en ligne

Afin d'identifier les acteurs (ou toute entité interagissante) de manière sûre et sans équivoque dans le monde virtuel et lors de transactions en ligne (en cas de nécessité ou lorsque la loi l'exige), il s'agit de *clarifier les questions fondamentales* et de *prendre les mesures qui s'imposent*.

3.1 Qu'est-ce/qui interagit avec qui/quoi?

- Personnes physiques, c'est-à-dire citoyens/-ennes, habitants/-es
- Sociétés, personnes morales, entreprises et entrepreneurs, administrations publiques et juridiques, institutions, et personnes physiques agissant en leur propre nom (employés, fondés de pouvoir, cf. point 3.4 *Trust Directory*)
- Animaux domestiques identifiés et contrôlés au moyen du système ANIS (Animal Identity Service)
- Objets, p. ex. biens identifiés par des lecteurs à l'aide de puces RFID actives ou passives, lors d'opérations de transport/logistique
- Services électroniques, p. ex. service Web interagissant au cours de processus numériques entre diverses organisations lors de flux de données

Il est communément accepté que, dans les environnements interconnectés des sociétés de l'information modernes, l'identification numérique deviendra sous peu la clé de toutes les interactions.

3.2 De quelle manière les entités interagissantes sont-elles identifiées?

- A l'aide de caractéristiques et d'informations indéniables et sans équivoque, p. ex. des échantillons d'ADN, des données biométriques ou des propriétés spécifiques. En cas de doute, cette certitude peut être remise en question par des experts, notamment lors de mutations génétiques, de changement de sexe ou de contexte social, de double nationalité.
- A l'aide d'enregistrements de données et d'informations décrivant ces caractéristiques d'identification. De tels enregistrements peuvent être redondants, du moins sur le plan théorique, et cependant distincts, notamment en cas de double nationalité.
- A l'aide d'inscriptions dans des registres officiels (bases de données) contenant ces enregistrements d'informations et de données d'identité, qui peuvent si nécessaire être vérifiés.
- A l'aide de support de données (p. ex. SmartCards, clés USB, etc.), contenant de manière partielle, exhaustive ou complétée, les données d'identité (p. ex. carte de citoyen).
- A l'aide d'interfaces (p. ex. appareils de lecture ou d'entrée de PC) capables de lire de tels supports de données, pour autant que les droits d'accès soient respectés.
- A l'aide d'autres services et procédés (p. ex. PKI/ICP (infrastructure à clé publique), certificat ou signature numérique), qui assurent et vérifient la transaction en ligne identifiée (p. ex. transmission sécurisée et signée de données par courrier électronique), selon la loi et les prescriptions (p. ex. ZertES).

3.3 Qui assure l'infrastructure et l'exploitation?

- La détermination «ab-initio» de l'identité de personnes physiques (citoyens/-ennes, habitants/-es) et de sociétés (personnes morales, entreprises et entrepreneurs, institutions, etc.), domiciliées sur le territoire suisse, est une tâche de l'Etat que celui-ci ne peut déléguer.
- Cela concerne également la saisie, le suivi et l'administration des enregistrements de données et informations stockés et actualisés dans les registres de la Confédération, des cantons et des communes. L'harmonisation de ces registres, l'unification des procédés et l'intégration des services

dans des réseaux dépassant le niveau des entreprises et sociétés est une tâche urgente et prioritaire dans le cadre de la réalisation de la nouvelle stratégie suisse de e-government.

- L'Etat doit également veiller à produire ces données et informations décrivant l'identité sous forme de documents adéquats (p. ex. passeport, carte d'identité, extrait de registre du commerce), qui peuvent alors être utilisés dans l'environnement électronique. Dans le cadre de la réalisation de la nouvelle stratégie suisse de e-government, nous estimons urgent et nécessaire de remplacer automatiquement toutes les cartes d'identité arrivant à échéance par de nouveaux documents «intelligents», à l'exemple des SmartCards (p. ex. cartes de citoyen autrichien).
- La production et la distribution de telles SmartCards dans les milieux économiques peut être assurée par des entreprises spécialisées, selon les consignes et sous le contrôle des offices fédéraux correspondants, et ce au tarif usuel. Il en va de même pour les appareils d'entrée et de lecture, dans la mesure où ils répondent aux spécificités et aux standards officiellement reconnus.
- L'emploi factuel et l'utilisation d'identités numériques (ou de caractéristiques d'identification dans les registres et supports de données) ne se mesurent pas par des lois ou des ordonnances, ni par la présence de SmartCards et d'interfaces, mais par la disponibilité des services correspondants, simples d'utilisation, dans les programmes de e-government, e-democracy, e-health, e-learning, ainsi que dans d'autres contextes de négociations importants d'une société moderne d'information et de transmission de savoir. Mettre sur pied de tels services, ou du moins créer des attraits indéniables pour susciter leur mise à disposition, est la tâche prioritaire et urgente de l'Etat, dans le cadre de la réalisation de la stratégie du Conseil fédéral pour une société de l'information dans notre pays.
- L'utilisation de solutions PKI/ICP et par la même des services, procédés et processus liés, doit être laissée à des sociétés qualifiées et certifiées dans le domaine. En revanche, la *gouvernance*, c'est-à-dire la surveillance du respect des conditions cadre définies pour des transactions en ligne sécurisées et fiables, est une tâche que les autorités ne peuvent déléguer (cf. Sarbanes-Oxley Act et réglementations comparables).

3.4 Quelles décisions concrètes doivent être prises lors de la session d'hiver 06/07?

- Détermination des compétences, tâches et responsabilités (si cela n'a pas déjà été réalisé) pour la mise en place de la stratégie du Conseil fédéral promouvant une société de l'information en Suisse (sept dossiers thématiques respectant les sept principes) ainsi que pour la réalisation de la nouvelle stratégie suisse de e-government de la part des instances prévues (gouvernement national, départements, offices fédéraux, organe dirigeant, responsable, secrétariat, etc.).
- Saisie du nouveau numéro d'assurance sociale pour personnes physiques dès 2007 dans les registres et sortie automatique dès 2007/2008, identités numériques sans équivoque et sous forme appropriée pour les cartes d'identité électroniques (SmartCards), comme sus-mentionné.
- Détermination de l'identité électronique d'entreprise (UID) pour les organisations (personnes morales, entreprises et entrepreneurs, institutions, etc.) en tant que numéros CH dans le registre du commerce (RC) électronique (zefix); saisie continue des entités ne figurant actuellement pas dans le RC (p. ex. indépendants, médecins, agriculteurs) selon le n° BUR (registre des exploitations et entreprises de l'OFS) dans le RC électronique, sous forme de chiffres CH.
- Libération, mise à disposition et conduite opératoire (p. ex. via Swisscom Directories, Orell Füssli/ Teledata, etc.) d'un *Trust Directory* pour les sociétés et leurs mandataires (le concept détaillé est disponible depuis 2005).
- Information et communication dans le cadre de la réalisation de la stratégie suisse de e-government, en particulier via eCH (standards, aides, Best Practices), eVanti.
- Formation et *Change Management* des cadres et employés de l'administration, afin qu'ils soutiennent ces mesures en les acceptant comme un défi, permettant ainsi leur réalisation rapide et compétitive, garante de succès.

Nous restons volontiers à votre disposition pour de plus amples informations et des présentations.

Adresse de contact:

Markus Fischer, MF Consulting, 1789 Lugnorre FR
markus-fischer@bluewin.ch, +41 79 600 0412

Membre du comité ICTswitzerland
Membre du comité d'experts eCH
Conseiller scientifique SATW