

**Final conclusions of Working Group 3
at Workshop Münchenwiler 20-21 of May 2010
on «Digital Identity, Trust & Confidence»**

Moderator : Alain Sandoz

Rapporteurs : Wolf Ludwig, Olivier Glassey, Sylvain Maret and Théo Bondolfi

WG members :

Alain Sandoz, Wolf Ludwig, Franco Furger, Olivier Glassey, Sylvain Maret, Théo Bondolfi, Stéphane Koch, , Andreas Schweizer, Raymond Morel and Raphael Rousseau

Reference authors : Alain Sandoz, Raymond Morel, Wolf Ludwig

WG-3-v4-22052010-12h30

General Observations:

There is a lack of systems architecting in the pursuit of digital identity concepts and managements in Switzerland.

The position of prevailing market standards versus open standards in public administration projects is not explicitly defined.

Projects seem to be driven under pressure and urgency and not correspond to effective “windows of opportunity”.

There is a lack of available resources and competencies in domains that are getting increasingly complex and evolving fast.

There is a lack of user awareness, education in technologies and user / citizen empowerment for a wide range of potential users from digital natives to digital migrants and seniors.

There is a lack of regulation and control on actors in possession of data on individuals.

There is a need for clarification of post-mortem regulations (what happens with the data once the owner of the digital ID disappears or dies?).

Observations specific to SwissID project:

There is a lack of coherence and symmetry in the SwissID project which is perceived as a commercial approach and not transparent for potential users and citizens.

There is a need for clarification of official data retention rules and practices with regards to login information in SwissID.

The SwissID model doesn't cover the variety of diverse digital identities – digital signature is only one aspect.

Recommandation 1: approche concertée & fédérée des sphères d'intérêt

Considérant que:

There are new Gatekeepers – extremely powerful like Google etc. – controlling and supervising access and information search habits of users and citizens.

Self-determination on personal information and data becomes more and more difficult.

There is a co-existence of different cultures, desires and needs for privacy, leading to yet unanswered questions:

- how much privacy is really needed?
- should we force those who have/see no problem exposing/exhibiting themselves with their private sphere and data not to do this?
- is governmental paternalism judicious?
- should we concentrate on and support those who really want / need to protect their privacy?
- may our kids benefit from the same freedoms and rights in about 20 years as we do today?"
- what are the opportunities and limits of nowadays Connectivity?
- where are we going to?

There are different e-ID management models, basically there are (at least) three spheres:

- the Government and its administration (SECO)
- Business and Commerce? (Property products)
- Individual users, consumers and citizens / civil society?

Nous recommandons

Une approche fédérée et concertée des différentes sphères d'intérêt

Actions :

- Une plateforme est créée et issue des trois grandes sphères et de leur approche respective: SwissID, Liberty Alliance et OpenID.
- Chaque projet fournit à cette plateforme un représentant appuyé par une équipe de cinq membres.
- La plateforme élabore un projet unique et pérenne d'identité numérique couvrant les besoins de tous les domaines d'activité de la société suisse pour les 10 prochaines années et visant à bâtir une infrastructure nationale pour y répondre.
- La plateforme est financée par un partenariat privé-public liant la Confédération, les cantons et le secteur privé.

Recommandation 2: cohérence, symétrie et transparence dans le développement de l'identité numérique en Suisse

Considérant

- L'importance de la sphère privée à l'ère numérique.
- La nature intimement liée à la personne, et donc aux droits fondamentaux de la personne, de l'identité et donc de la signature électronique.
- Le manque d'homogénéité des solutions proposées et l'absence de pérennité due à leur évolution rapide.
- Que la lisibilité des processus liés à l'e-identity constitue un facteur fondamental pour construire les conditions nécessaires à l'établissement de la confiance.

Nous recommandons de :

- promouvoir la cohérence des solutions d'identité numérique en les fondant à partir d'une architecture garantissant des principes de symétrie et de transparence pour l'ensemble des acteurs impliqués ;
- développer des modèles d'e-identity dans lesquels les moyens sont adaptés aux besoins et qui préservent les droits des citoyens ;
- instaurer un principe de symétrie entre les informations demandées et celles reçues ;
- informer l'utilisateur de l'usage et des conditions de traçabilité des informations qui lui sont demandées ;
- rappeler que la signature électronique, qui fait partie de notre identité à part entière, ne soit pas seulement considérée sous un aspect économique (produit) mais aussi dans ses aspects citoyens.

Action :

Définir un projet de démocratie participative ouvert à tous, basé sur l'identité numérique des acteurs, et visant à fonder sur un modèle collaboratif les processus de communication, d'appropriation et de déploiement de l'identité numérique en Suisse.

Recommandation 3: standards ouverts

Considérant que :

- la pérennité, la généralisation et en même temps la nécessité de l'évolution comme des éléments incontournables des solutions adoptées à l'échelle de la Confédération ;
- l'administration se doit de rester indépendante des constructeurs et des éditeurs de solutions propriétaires ;
- les enjeux se situent au-delà des frontières politiques et géographiques ;
- les choix en matière de technologies passent par une participation aux communautés œuvrant dans ces domaines spécifiques.

Nous recommandons que les administrations publiques privilégient les standards ouverts lors de la conception et la mise en œuvre des composants technologiques.

Parmi ces standards : OpenID, OAuth, OATH, OWASP et SAML

Les avantages d'une telle approche sont :

- la mutualisation des efforts pour ne pas faire reposer la conception, la mise en œuvre et la maintenance de ces systèmes sur les seuls contribuables suisses ;
- la transparence qui favorise la confiance des citoyens et est garante d'une réduction des risques propres à la sécurité ;
- une agilité permettant une réactivité adaptée aux évolutions rapides des technologies de l'information.

Actions :

- Procéder à une étude d'appropriation par TA-Swiss.
- Mettre en place un processus évolutif permettant de maîtriser le problème, la montée en puissance et le nécessaire échelonnement de l'identité numérique en Suisse à long terme en se basant sur les standards ouverts.

Recommandation 4: authentification forte

Considérant que :

- les technologies d'authentification évoluent rapidement ;
- l'administration se doit de prendre en compte des comportements et les sensibilités des citoyens ;
- l'utilisation du couple identifiant/mot de passe est une approche obsolète et inadaptée aux nouvelles menaces.

Nous recommandons que les administrations publiques privilégient les solutions d'authentification forte agnostiques face aux technologies et laissant le choix aux utilisateurs.

Les avantages d'une telle approche sont :

- de meilleures pratiques d'adoptions des technologies par les citoyens ;
- une réduction des pratiques à risques liée à la complexité des solutions actuellement mise en œuvre ;
- une simplification amenant un meilleur confort d'utilisation des technologies d'authentification forte ;
- la pierre angulaire pour amener plus de confiance et offrir une meilleure protection des données et des droits d'accès.

Action:

Définir pour les administrations suisses, d'une part les différents niveaux de sensibilité correspondant aux besoins réels de la population et, d'autre part, leurs niveaux d'authentification avec les technologies ouvertes adaptées à leur mise en œuvre.

Recommandation 5: Vers des Etats généraux de l'e-Société suisse

Considérant que :

- l'argent public doit être utilisé avec prudence et en respect des standards et les bonnes pratiques existantes, particulièrement dans le domaine sensible de la gestion des données personnelles ;
- malgré d'immenses investissements par les Etats dans des projets basés sur des intérêts privés, seuls les projets numériques "endogènes" (conçus sur une base populaire de type "bottom->up", et non pas imposés par une démarche "top-down", tels le W3C & HTML, TCP/IP, Mozilla (navigateur le plus utilisé en 2010), Debian (distribution GNU/Linux utilisée sur plus de 50% des serveurs web), Wikipedia sont aujourd'hui des standards de confiance largement adoptés ;
- comme présentés au Forum Economique de Davos en 1997 dans la "déclaration d'indépendance du cyberspace", les environnements numériques sont régis par des règles qui échappent aux territoires physiques et ne peuvent donc tout simplement pas être colonisés sur mandat gouvernemental ;
- la signature électronique est un sous-ensemble et non pas un synonyme d'identité numérique ;
- de nombreuses études scientifiques démontrent que la sécurité avec transparence répond mieux aux besoins de la majorité des utilisateurs d'informations numériques ;
- une économie durable dans un contexte d'échanges numériques, avec des initiatives innovantes et nombreuses, dépend d'une part de la "net-neutralité" définie par le consortium W3C, d'autre part, dépend de la démarche des "contrats sociaux" tels ceux proposés par les développeurs DEBIAN et aussi des 4 libertés fondamentales telles qu'adoptées au Sommet Mondial de la Société de l'Information (Genève 2003). Les projets citoyens Wikipedia, Mozilla (tous leaders dans leur domaine) sont les socles sur lesquels construire des initiatives privées ;
- 14 préposés à la protection des données des pays occidentaux (Canada, France, Allemagne, Espagne, Israel,...) ont, en avril 2010, envoyé un courrier à la direction d'une multinationale de l'information pour l'interpeller sur les dérives de la privatisation des données des citoyens.

Recommandations :

les politiques publiques, sur la base du serment fait par les élus au moment de leur intronisation, garantissent aux citoyens que :

- seuls les outils et méthodes respectant la culture numérique durable soient soutenus par les budgets publics ;
- la construction et la gestion courante de l'identité personnelle, notamment chez les jeunes générations, soient facilitées par l'usage d'un langage approprié ;
- le principe de la clé USB vendue au public suisse pour la gestion soit revu afin qu'il s'agisse d'un service reconnu d'utilité publique sans but lucratif et non pas servir des intérêts privés ;
- l'acquis de la liberté de choix soit totalement préservé, tel que le prévoient le chapitre 1 de la constitution fédérale (Droits fondamentaux, 18 avril 1999) de la constitution, quand aux systèmes de gestion des codes d'accès aux services de l'administration publique.

Action :

organiser, en écho à la stratégie du Conseil fédéral, des Etats généraux de l'e-Société suisse avec tous ses acteurs.