Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie DFE
Secrétariat d'Etat à l'économie SECO
Communication

Documentation SuisseID destinée aux médias

Date 13 janvier 2011

Travaux en 2010 du groupe d'experts sur la sécurité

Contexte
Sous la direction du Secrétariat d'Etat à l'économie (SECO), les fournisseurs de services de certification reconnus légalement en Suisse ont élaboré avec des représentants de l'industrie des TI un standard pour la preuve d'identité électronique SuisseID. Ce standard permet aussi bien de réaliser une signature électronique reconnue sur le plan juridique que de procéder à une authentification sécurisée. Depuis mai 2010, la SuisseID est disponible sous la forme d'une carte à puce (*smartcard*) ou d'une clé USB équipée de certificats numériques d'authentification (IAC)[1] et de signature qualifiée (QC)[2].

Les travaux du groupe d'experts
Le 10 septembre 2010, le SECO a mis sur pied un groupe d'experts chargé d'étudier les moyens de réduire les risques liés à l'utilisation des cartes à puce. Un rapport d'experts a évalué la sécurité offerte par la SuisseID sur le plan technique en analysant la vulnérabilité de l'ensemble de sa chaîne de prestations (de l'utilisateur à l'application serveur, en passant par le certificat, l'appareil de lecture et l'ordinateur client). En complément, le SECO a mis sur pied un atelier en novembre 2010 pour aborder différentes questions de sécurité en lien avec la SuisseID, atelier auquel ont participé 35 experts des milieux de l'économie, de la recherche, de l'enseignement et de l'administration. Les précautions d'emploi présentées ci-dessous sont le fruit concret de ces travaux.

Précautions d'emploi
Compte tenu du fait qu'il n'existe pas de sécurité absolue dans des environnements électroniques en réseau, et donc dans des interactions en ligne dans lesquelles divers intermédiaires et parties peuvent être impliqués, il est important de comprendre que le degré de sécurité offert par la SuisseID dépend de nombreux facteurs, qu'il s'agisse, par exemple, du but de son utilisation ou du profit que pourrait tirer un pirate d'une cible donnée. Pour se faire une idée claire des mesures de protection nécessaires, il convient de considérer dans chaque cas les risques et effets liés à l'utilisation de la SuisseID. Etant donné que, le plus souvent, les risques sont fonction de l'application, des précautions d'emploi d'ordre général

---

[1] Identification and Authetication Certificate

[2] Qualified Certificate

ne peuvent constituer qu'un fil conducteur; dès lors, elles ne sauraient tenir lieu d'analyse et d'évaluation individuelles des risques, pas plus que de mesures de défense appropriées au cas particulier.

Les précautions d'emploi ci-dessous sont fondées sur le principe que l'ordinateur d'un utilisateur de la SuisseID peut comporter des failles de sécurité qui pourraient être exploitées par un logiciel malveillant (maliciel).

Précautions d'ordre général – Il convient d'employer les mêmes précautions avec la SuisseID qu'avec tout autre moyen d'accès électronique (p. ex. une carte bancaire). La SuisseID doit être constamment gardée en lieu sûr; il ne faut jamais la laisser traîner. Le code PIN secret ne sera jamais communiqué à un tiers. Il ne doit pas non plus être noté quelque part, et surtout pas sur la carte elle-même. En cas de doute quant à la sécurité offerte ou de disparition, la SuisseID doit être immédiatement révoquée. Les sites de ses fournisseurs et les documents remis avec elle expliquent la marche à suivre dans un tel cas.

Précautions concernant le lecteur de cartes – Dans de nombreux pays, des lecteurs de cartes nécessitant la saisie du code PIN à l'aide d'un clavier d'ordinateur (lecteurs de classe 1) sont utilisés pour la signature et l'authentification. Il ne fait aucun doute que des lecteurs de classe 1 sont plus vulnérables à des attaques techniques que des lecteurs de classes plus élevées fonctionnant par exemple à l'aide de PIN-pad ou d'un dispositif propre. Par contre, ces lecteurs de classe 1 sont plus faciles à utiliser. Les utilisateurs qui estiment nécessaire une sécurité plus élevée peuvent obtenir des appareils de lecture de classes plus élevées auprès de leur fournisseur de la SuisseID.

Précautions relatives à la signature électronique – Des signatures électroniques telles que celles permises par la SuisseID sont déjà utilisées dans de nombreux pays. Une fois signé, un document électronique ne peut plus être manipulé; la signature ne peut pas non plus être trafiquée sans que la manipulation n'apparaisse. Il ne faudrait recourir à la signature électronique que si le logiciel de signature employé provient d'une source fiable et que le signataire connaît l'ensemble du contenu auquel il appose sa signature. Par conséquent, le logiciel de signature doit montrer tous les contenus sans exception. Il ne devra donc pas accepter de contenus dynamiques. La sécurité du logiciel de signature dépend aussi de celle de l'ordinateur sur lequel il est installé et utilisé. En cas de doute quant au degré de sécurité offert par l'ordinateur, on renoncera à la SuisseID tant pour la signature que pour l'authentification (log-in).

Précautions relatives aux formats de données pour la signature – En principe, n'importe quel document électronique peut être signé de manière valable juridiquement avec la SuisseID. La loi sur la signature électronique ne prévoit pas de restrictions à ce propos. Le format PDF/A est largement répandu. Il est adapté à cette fin et c'est le seul, en ce qui concerne les données électroniques, que les autorités sont tenues d'accepter. Il existe de nombreux outils permettant la signature et l'examen de la signature de documents PDF. Etant donné que la sécurité de ces instruments dépend elle aussi de celle de l'ordinateur, on appliquera le même principe de précaution que ci-dessus: en cas de doute quant au degré de sécurité offert par l'ordinateur, on renoncera à la SuisseID tant pour la signature que pour l'authentification (log-in).

Précautions en matière de protection contre les virus – La sécurité offerte par la SuisseID ne peut pas être compromise par un logiciel malveillant (maliciel), contrairement à celle de son environnement. Dès lors, il appartient à l'utilisateur de faire preuve de la vigilance nécessaire et de protéger son ordinateur à l'aide de mesures connues et usuelles telles que des programmes antivirus ou anti-spyware, des mises à jour régulières de la sécurité du système d'exploitation, des logiciels et des données. Ces mesures offrent une protection efficace contre de nombreuses attaques connues.

Précautions concernant la procédure d'accès via des sites internet (log-in) – Un accès au moyen de la SuisseID est considéré comme étant très sûr et représente une amélioration notable par rapport à un accès au moyen d'un nom d'utilisateur et d'un mot de passe. S'il y a un danger, il provient du site internet choisi. Par conséquent, la SuisseID ne devrait être utilisée que sur des sites fiables. Il n'existe pas, pour l'heure, de label de qualité pour les sites internet qui acceptent la SuisseID (le logo «SuisseID LOGIN» est très répandu mais n'est qu'un moyen de reconnaissance uniforme). Les sites internet qui ont des certificats serveurs de valeur élevée, reconnaissables dans de nombreux outils de navigation à leur adresse en vert, sont considérés comme étant sérieux et fiables, en particulier parce que l'identité du responsable est connue et a été vérifiée. Ici aussi: en cas de doute quant au degré de sécurité offert par l'ordinateur, on renoncera à la SuisseID tant pour la signature que pour l'authentification (log-in).

Perspectives d'avenir
Le SECO poursuivra le dialogue avec les experts en matière de sécurité. Il s'engage activement pour la diminution des risques lors de l'utilisation de technologies de l'information et a fait de la sécurité un des thèmes principaux de ses activités en matière de cyberéconomie.

De plus, un groupe de travail sur la sécurité a été formé au sein de l'association responsable de la SuisseID. Il analysera les résultats de l'enquête réalisée en 2010 et orientera son activité en fonction de ceux-ci.

Vous trouverez de plus amples informations concernant la SuisseID sur le site http://www.SuisseID.ch/.