Position de l'ACN sur la sécurité de l'identité numérique

L'Alliance pour la Confiance Numérique (ACN) réunit les principaux acteurs en France de l'identité numérique et de la cybersécurité. Ses membres sont force de propositions ; ils ont notamment développé et publié la Feuille de route Nationale de l'Identité Numérique et formulé des propositions au Secrétariat Général pour la Modernisation de l'Action Publique (SGMAP), dans le cadre de sa consultation de mai 2013 sur les « Identité(s) numérique(s), Quelle stratégie pour l'Etat ? ».

Pour l'ACN, l'identité numérique doit naturellement porter l'objectif de protection des données personnelles et de la vie privée, et apporter, en fonction des enjeux des services utilisant cette identité, un niveau d'assurance de l'identité qui sera corrélé à la sécurité intrinsèque de la solution. Elle travaille actuellement ces sujets et apportera des contributions dès cette année. **Le présent document constitue la position de l'ACN, pour la sécurité de l'identité numérique dans le cadre du futur règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.**

L'ISO et le projet européen STORK2 ont défini 4 niveaux d'assurance de l'identité numérique (minimal, faible, substantiel et élevé). **Pour l'ACN, le niveau élevé d'assurance d'une identité numérique doit :**

- **garantir qu'à l'identité numérique présentée correspond une identité avérée de l'individu connecté ;**
- **Minimiser la communication des données personnelles et permettre l'authentification et la signature électronique sous pseudonyme ;**
- **reposer sur des solutions sécurisées, évaluées et certifiées selon une méthodologie éprouvée.**

Ces trois objectifs sont en fait mêlés : une identité prouvable nécessite une solution de confiance.

Evaluation, certification de la sécurité de l'identité numérique :

L'ISO a publié l'ensemble de normes « Critères Communs » pour une évaluation impartiale de la sécurité des systèmes et logiciels informatiques. Des accords de reconnaissance mutuelle garantissent l'acceptation des certificats de sécurité émis par les pays signataires.

Les Critères Communs sont un guide de référence pour le développement et le contrôle de produits et systèmes de l'information manipulant des données personnelles. Ils constituent un support méthodologique pour le développeur de la solution et l'évaluateur. Les exigences fonctionnelles de sécurité et les exigences d'assurance de sécurité y sont décrites. Le certificat émis par une autorité en charge de la certification, suite au rapport d'évaluation garantit que le produit ou la technologie évaluée respecte un niveau d'assurance, soit une note allant de EAL1 à EAL7[1]. A chaque niveau correspond un paquet minimum d'exigences d'assurance.

Des profils de protection définissent l'ensemble d'exigences de sécurité pour une catégorie de produits, en tenant compte de leur utilisation (par exemple document de voyage, signature électronique,…) et non de leur implémentation.

[1] EAL : Evaluation Assurance Level

Les critères communs permettent donc :

- Aux utilisateurs finaux, de définir leur politique de sécurité et de déterminer si un produit répond à leur besoin de sécurité,
- Aux développeurs, d'identifier les exigences de sécurité que le produit doit assurer,
- Aux évaluateurs, de vérifier qu'un produit est conforme à sa cible d'évaluation selon une méthodologie et des critères standardisés.

Un point important des critères communs est l'étude de la résistance aux attaques en vue de compromettre la sécurité et notamment d'accéder aux données. Une analyse de vulnérabilité donne une note de AVA_VAN.1 à AVA_VAN.5[2]. Une étude plus poussée peut être indiquée par l'ajout du signe + après la mention EAL attribuée, mais il convient de vérifier dans le certificat que ce + concerne bien la résistance aux vulnérabilités. Les laboratoires d'évaluation sont tenus de disposer d'experts, de mener une veille technologique, de connaître l'état de l'art des attaques et de procéder sur les produits à des attaques, à l'aide de moyens techniques adaptés aux niveaux d'analyse de vulnérabilité visé par le produit. Ceci afin de garantir un haut niveau de résistance des produits face à des attaques à fort potentiel. Ces attaques de haut niveaux sont menées en parfaite connaissance de la conception des produits, puisque les laboratoires disposent des dossiers de conception, source du logiciel comprise.

Deux accords de reconnaissance mutuelle des certificats critères communs, qui garantissent l'acceptation des certificats de sécurité émis par les pays signataires, ont été signés :

- L'accord CCRA regroupe 17 pays signataires et 9 pays reconnaissants officiellement les certificats. Il limite la reconnaissance mutuelle au niveau d'évaluation EAL2 (ou EAL4 sous certaines conditions)
- L'accord SOGIS-MRA a été élaboré et signé en Europe par 10 Etats Membres et cible la reconnaissance mutuelle des niveaux les plus élevés de sécurité (jusqu'à EAL7 et AVA_VAN.5 pour certains domaines techniques).

D'autres méthodes d'évaluation de la sécurité existent, mais ne disposent pas d'accords de reconnaissance mutuelle étatiques.

Utilisation de supports physiques sécurisés et de confiance

L'ACN s'est donné pour mission la création de la confiance numérique des acteurs : les critères communs, et plus particulièrement l'accord SOGIS-MRA concourent à l'atteinte de cet objectif.

A ce titre, l'ACN estime qu'un haut niveau de sécurité est nécessaire afin de permettre :

- aux usagers d'accorder leur confiance à des dispositifs techniques aptes à garantir la protection de leurs données privées et à leur permettre de conserver le contrôle de leur identité ;
- aux offreurs de services d'accorder leur confiance aux usagers : en effet, un défaut de sécurité ou une vulnérabilité sur un moyen d'identification électronique pourrait engendrer des dommages économiques ou d'image importants.

L'ACN recommande donc que ces moyens d'identification électronique reposent sur l'utilisation de supports physiques (« élément sécurisé » ou « secure element ») évalués à des hauts niveaux de sécurité. Ces éléments sécurisés sont des objets personnels et transportables, qui peuvent rester sous le contrôle exclusif de leur porteur ; en termes d'attaques, ils sont plus robustes et moins attrayants, pour un attaquant, que les banques de données à caractère personnel bien plus exposées ; ils constituent également un système dont la sécurité est plus aisément maîtrisable. Les éléments

[2] AVA _VAN : classe d'assurance « Vulnerability assessment »

sécurisés sont déjà conçus, évalués et certifiés selon la méthodologie des critères communs et ont des certificats aux niveaux élevés reconnus par le SOGIS-MRA, tant pour leur partie matérielle que logicielle. L'industrie européenne, les évaluateurs et les certificateurs ont atteint un très haut niveau d'expertise.

Concernant la nécessaire reconnaissance des certifications de sécurité, on notera que le SOGIS-MRA est ouvert aux Etats-Membres de l'UE et de l'EFTA qui peuvent être soit consommateurs de certificats, soit, en complément, émetteurs de certificats, qui travaillent ensemble au développement et à la surveillance du système. Par exemple les certificateurs sont audités par leurs pairs sur la base de critères techniques. Aujourd'hui, au travers des appels d'offres internationaux, la reconnaissance de fait des certificats SOGIS-MRA peut être constatée.

L'ACN souhaite donc que le SOGIS-MRA soit mieux compris et que plus d'Etats européens y participent. Elle propose que ce soit la référence de certification sécuritaire des solutions d'identité numérique qui seront déployées en Europe.