

## Communiqué de presse – La carte d'identité électronique est sûre

COSIC, K.U.Leuven, 13 juin 2008

Selon des dépêches parues récemment dans la presse, il serait aisé de pirater la carte d'identité électronique. L'on peut y lire qu'il est possible de se faire passer pour son voisin, à l'aide d'une puce piratée, et d'également consulter la déclaration d'impôts dudit voisin. Ces informations s'appuieraient sur une contribution de l'équipe du Prof. Bart De Decker (Dépt. Sciences informatiques, K.U.Leuven) présentée cette semaine lors de la *European e-ID Card Conference* à La Haye.

Les affirmations en question sont complètement fantaisistes. A l'heure actuelle, il n'existe aucune méthode connue permettant de pirater la sécurité de la carte d'identité électronique. Au vu des évolutions scientifiques actuelles, il est impossible de prélever les données sensibles (clés secrètes) sur la puce qui permettraient de prendre l'identité d'une autre personne ou de falsifier des signatures électroniques. L'architecture de protection de la carte d'identité électronique a été conçue et mise à l'épreuve en collaboration avec différents chercheurs de la K.U.Leuven (Prof. Jos Dumortier, ICRI et Prof. Bart Preneel et Danny De Cock, COSIC).

A l'instar d'une carte d'identité en papier ou d'une carte bancaire contenant une puce, une carte d'identité électronique contient des informations sensibles sur la personne concernée (exemples : adresse, numéro de Registre national). Les données les plus sensibles permettent de consulter des informations personnelles (données du Registre national, Tax-On-Web) et de signer électroniquement des documents. Ces fonctions sont sécurisées par un code secret (code PIN) qui doit être protégé précautionneusement.

Il est important que l'utilisateur emploie sa carte d'identité électronique avec la prudence requise, tout comme il le fait avec sa carte bancaire ou de crédit. Cela implique qu'il faille utiliser à son domicile un lecteur de cartes sûr (comportant de préférence un écran et un clavier propres). En outre, il est nécessaire d'utiliser son PC correctement et de respecter les règles de base requises pour un usage adéquat, telles la mise à jour du logiciel et du système d'exploitation, et l'utilisation d'un anti-virus et d'un anti-*spyware* (logiciels espions). Enfin, Il faut se montrer prudent lors de la visite de sites web ou de l'installation de nouvelles applications. Ces règles ne s'appliquent pas uniquement à l'utilisation de la carte d'identité électronique : elles concernent également toute application présente sur un PC, tel les applications permettant de gérer son compte bancaire en ligne.

D'autre part, il est important de comprendre qu'une sécurité parfaite à 100% n'existe pas. Le maillon le plus faible dans l'utilisation de la carte d'identité électronique n'est assurément pas la carte proprement dite, mais le logiciel qui pilote la carte (le *middleware* – intergiciel) ainsi que les applications. Un logiciel n'est jamais parfait. Néanmoins, le logiciel proposé actuellement par Fedict fait l'objet d'une évaluation régulière. Si des problèmes surviennent, ils sont résolus rapidement et efficacement. A l'heure actuelle, l'on n'a signalé aucun incident au cours duquel la carte proprement dite aurait fait l'objet d'une attaque. Lors du développement du logiciel, l'on doit également poser des choix : va-t-on demander à l'utilisateur son code PIN lors de chaque identification ou va-t-on uniquement le demander lorsque l'utilisateur surfera sur un nouveau site ? Cette décision a été prise sur la base d'un juste milieu entre la convivialité d'utilisation d'une part et les risques d'autre part. A cet égard, il est important d'évaluer les risques en question de manière approfondie. Afin d'aider les programmeurs à poser les choix

susmentionnés, une série d'entreprises ont rédigé un document intitulé « Best Practices for Applications using the electronic Identity Card (eID) ». Enfin, il est important de signaler qu'en matière d'authentification d'utilisateurs, la solution de remplacement est très souvent de recourir au nom d'utilisateur et à un mot de passe. De toute évidence, cette possibilité offre une sécurité bien moins importante (et elle requiert également une gestion correcte de l'ordinateur).

En conclusion, les récentes informations publiées dans la presse sont incorrectes. Actuellement, il est absolument impossible de pirater la carte d'identité électronique. Il est vrai que la carte constitue un élément d'un système de sécurité complexe ; les risques lors de l'utilisation de cette carte doivent être sous-pesés correctement. Cependant, en raison des évolutions scientifiques actuelles, il est parfaitement possible d'atteindre un niveau de sécurisation adéquat en ce qui concerne le logiciel et le matériel existants.

### **Complément : réponse à une série de remarques présentes dans l'étude du Prof. De Decker**

L'étude du Prof. De Decker suggère que la carte d'identité électronique marque une étape en direction de Big Brother. Actuellement, il n'existe *aucune indication* que cela soit vrai. Les autorités belges gèrent les informations relatives aux citoyens avec les plus grandes précautions. D'une part, il existe une protection juridique adéquate qui limite l'utilisation du numéro de Registre national (sous le contrôle de la Commission pour la Protection de la Vie Privée). A la demande de Fedict, la K.U.Leuven a élaboré une solution technique permettant d'utiliser un numéro d'application spécifique pour chaque application, qui diffère à chaque application et qui ne peut être liée au numéro de Registre national ou à un quelconque autre numéro. D'autre part, l'utilisation de la carte d'identité électronique pourra offrir, à l'avenir, une protection de la vie privée plus importante encore, par le biais de techniques de sécurisation plus sophistiquées qui permettront notamment – à l'aide de la carte – de prouver que l'on est âgé(e) de plus de 18 ans sans pour autant divulguer d'autres informations. Ce point fait l'objet d'une étude, entre autres, par le projet IWT ADAPID (applications avancées pour la carte d'identité électronique), dirigé par le groupe de recherche COSIC de la K.U.Leuven (<https://www.cosic.esat.kuleuven.be/adapid/>).

L'étude indique également que si l'on insère sa carte dans le lecteur de cartes, les données de base (photo, données d'identité, adresse) sont lisibles par le logiciel actif sur le PC. Evidemment, le système ne ferait pas preuve d'une grande convivialité d'utilisation s'il ne mettait ces informations à disposition uniquement lorsque l'utilisateur introduirait son code PIN : dans le cas d'un contrôle frontalier, cela s'avèrerait très peu pratique. Sur ce point, rien ne diffère de la carte sous format papier, où les informations de base sont également lisibles si l'on examine la carte. Tout comme l'on ne cède pas sa carte à tort et à travers, à n'importe qui, l'on doit également se montrer prudent lors de l'utilisation de la carte électronique. De plus, Fedict propose un service de protection de la vie privée, qui verrouille le lecteur de cartes et oblige les applications à recourir au logiciel de Fedict. A l'instar de toute autre sécurisation de logiciel, cette sécurisation n'est pas infaillible à 100%. Néanmoins, elle offre selon nous un niveau de protection raisonnable vis-à-vis des logiciels malveillants et des *hackers* (pirates). La plupart des PC contiennent de nombreuses informations personnelles (informations financières, photos, fichiers d'adresses) qui ne font l'objet d'aucune protection complémentaire la plupart du temps.

Contact : Prof. Bart Preneel, Dépt. Electrotechnique-ESAT, COSIC, K.U.Leuven  
016/32 11 48 Bart.Preneel@esat.kuleuven.be