

## Persbericht - De Elektronische Identiteitskaart is Veilig

COSIC, K.U.Leuven, 13 juni 2008

Recente berichten in de pers geven aan dat de elektronische identiteitskaart gemakkelijk te kraken zou zijn. Er wordt beweerd dat men zich met een gekraakte chip kan uitgeven voor zijn buurman en dan ook diens belastingaangifte kan bekijken. Deze berichten zouden steunen op een bijdrage van het team van Prof. Bart De Decker (Dept. Computerwetenschappen, K.U.Leuven) die deze week gepresenteerd werd op de European e-ID Card Conference in den Haag.

Deze beweringen zijn volledig uit de lucht gegrepen. Er is op dit moment geen enkele methode bekend om de beveiliging van de elektronische identiteitskaart te kraken; bij de huidige stand van zaken in de wetenschap is het niet mogelijk om gevoelige gegevens (geheime sleutels) uit de chip te halen die het mogelijk maken om zich als iemand anders voor te doen of om digitale handtekeningen te vervalsen. De beveiligingsarchitectuur van de elektronische identiteitskaart is ontworpen en geverifieerd in samenwerking met verschillende onderzoekers van de K.U.Leuven (Prof. Jos Dumortier, ICRI en Prof. Bart Preneel en Danny De Cock, COSIC).

Juist zoals een papieren elektronische identiteitskaart of een bankkaart met chip bevat een elektronische identiteitskaart gevoelige gegevens over een persoon (zoals het adres en het rijksregisternummer). De meest gevoelige gegevens laten toe om persoonsgegevens te raadplegen (gegevens in het rijksregister, tax-on-web) en om documenten elektronisch te ondertekenen. Deze functies zijn beveiligd door een geheime code (de PIN code), die zorgvuldig beschermd moet worden.

Het is belangrijk dat de gebruiker met de nodige voorzichtigheid omspringt met een elektronische identiteitskaart, juist zoals hij dat doet met zijn bankkaart of kredietkaart. Dit houdt in dat men thuis een veilige kaartlezer moet gebruiken (bij voorkeur met eigen scherm en toetsenbord). Daarnaast moet men zijn PC correct beheren en de basisregels van goed gebruik respecteren: software en besturingssysteem geregeld updaten, een anti-virus en anti-spyware programma gebruiken en tenslotte voorzichtig zijn bij het bezoeken van websites of bij het installeren van nieuwe toepassingen. Deze regels gelden niet alleen voor het gebruik van de elektronische identiteitskaart, maar voor alle toepassingen op een PC zoals internetbankieren.

Aan de andere kant is het belangrijk om te begrijpen dat 100% perfecte veiligheid niet bestaat. De zwakste schakel in het gebruik van de elektronische identiteitskaart is zeker niet de kaart zelf, maar de software die de kaart aanstuurt (de middleware) en de toepassingen. Software is nooit perfect, maar de huidige software aangeboden door Fedict wordt geregeld geëvalueerd; als er problemen zijn, worden die snel en efficiënt opgelost. Op dit moment is er geen enkel incident bekend waarbij de kaart zelf zou aangevallen zijn. Bij het ontwikkelen van de software moet men ook keuzes maken: gaat men aan de gebruiker voor elke

identificatie zijn PIN code vragen of gaat men dit maar doen als er naar een nieuwe website gesurfd wordt? Deze beslissing wordt genomen op basis van een afweging tussen de de gebruiksvriendelijkheid en risico's; hierbij is het van belang om deze risico's grondig te evalueren. Om de programmeurs te helpen bij het maken van deze keuzes is er door een aantal bedrijven een document ontwikkeld "Best Practices for Applications using the electronic Identity Card (eID)." Tenslotte is het belangrijk om aan te geven dat voor authenticatie van gebruikers het alternatief heel vaak gebruikersnaam en paswoord is. Het is overduidelijk dat dit veel minder veiligheid biedt (en ook eisen oplegt aan het correct beheer van de computer).

Conclusie: de recente berichten in de pers zijn onjuist. Op dit moment is het absoluut niet mogelijk om de elektronische identiteitskaart te kraken. Het is wel zo dat de kaart een element vormt in een complex beveiligingssysteem; de risico's bij het gebruik van de kaart moeten correct afgewogen worden, maar het is bij de huidige stand van zaken van de wetenschap perfect mogelijk om met de bestaande software en hardware een adequaat beveiligingsniveau te bereiken.

### **Aanvulling: antwoord op een aantal opmerkingen in de studie van Prof. De Decker**

De studie van Prof. De Decker suggereert dat de elektronische identiteitskaart een stap is naar Big Brother. Op dit moment is er *geen enkele aanwijzing* dat dit het geval is; de Belgische overheid springt zeer zorgvuldig om met de gegevens van de burgers. In eerste instantie is er een adequate juridische bescherming die het gebruik van het rijksregisternummer beperkt (onder controle van de privacycommissie). De K.U.Leuven heeft in opdracht van Fedict een technische oplossing uitgewerkt om voor elke toepassing een specifiek applicatienummer te gebruiken dat verschillend is voor elke toepassing en dat niet gekoppeld kan worden aan het rijksregisternummer of aan enig ander nummer. Daarnaast is het zo dat het gebruik van een elektronische identiteitskaart in de toekomst een nog betere privacybescherming kan bieden door gesofisticeerde beveiligingstechnieken die bijvoorbeeld toelaten om – met behulp van de kaart - te bewijzen dat men ouder is dan 18 jaar zonder enige andere informatie vrij te geven. Dit wordt o.a. bestudeerd in het IWT project ADAPID (geavanceerde toepassingen van de elektronische identiteitskaart) dat geleid wordt door de onderzoeksgroep COSIC van de K.U.Leuven (<https://www.cosic.esat.kuleuven.be/adapid/>).

De studie wijst er ook op dat indien men zijn kaart in de kaartlezer stopt, de basisgegevens (digitale foto, identiteitsgegevens, adres) leesbaar zijn door software die actief is op de PC. Het zou zeker niet gebruiksvriendelijk zijn om deze gegevens maar beschikbaar te stellen als de gebruiker een PIN code zou ingeven: dat zou bijvoorbeeld bij een grenscontrole heel onpraktisch worden. Dit verschilt niet met de papieren kaart, waar de basisgegevens ook leesbaar zijn als men de kaart bekijkt. Net zoals men deze kaart niet zomaar aan iedereen overhandigt, moet men ook voorzichtig zijn bij het gebruik van de elektronische kaart. Daarnaast biedt

Fedict een privacy service, die de kaartlezer vergrendelt en toepassingen verplicht om gebruik te maken van de Fedict software. Deze beveiliging is – zoals alle beveiliging in software - niet 100% waterdicht, maar biedt volgens ons een redelijk niveau van bescherming tegen aanvallen door kwaadaardige software en hackers. De meeste PCs bevatten heel wat meer persoonlijke informatie (financiële gegevens, foto's, adresbestanden) die meestal helemaal niet bijkomend beveiligd zijn.

Contact: Prof. Bart Preneel, Dept. Elektrotechniek-ESAT, COSIC, K.U.Leuven

016/32 11 48 [Bart.Preneel@esat.kuleuven.be](mailto:Bart.Preneel@esat.kuleuven.be)