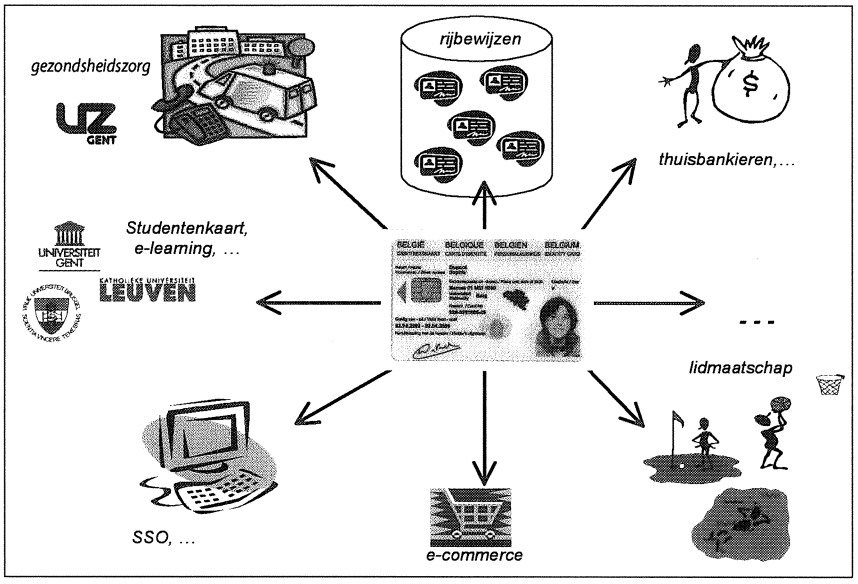
Bart J.V. Sijnave

De elektronische identiteitskaart in UZ Gent

INLEIDING

Dat de nieuwe (elektronische) identiteitskaart een veelzijdig product is, zal iedereen ondertussen beamen. De meeste tijdschriften en magazines rapporteren sinds weken continu over bepaalde verwezenlijkingen op basis van de elektronische identiteitskaart (eID) of integraties van de eID in hun producten. 'The sky is the limit' (figuur 1) werd lang gepredikt, maar blijkt nu meer dan ooit realiteit te worden, ook binnen de gezondsheidssector.

Korter dan een doorsnee zwangerschap, op vijf maand tijd, zag de eerste elektronische identiteitskaart het levenslicht. We spreken maart 2003. Na een pilootfase besliste de Ministerraad eind 2004 om de elektronische identiteitskaart uit te rollen over gans België. De kaart zou meteen beschikbaar worden in alle 589 gemeentes en niet meer in de 11 pilootgemeentes die tussen maart 2003 en 2004 de nieuwe identiteitskaart hadden 'uitgetest'.



Figuur 1: The sky is the limit wat mogelijkheden met eID betreft

Dr. Bart Sijnave is ICT-manager van het UZ Gent en voorheen eID Program Manager bij Fedict (Federale Overheidsdienst Informatie- en Communicatietechnologie).

PATIENTENREGISTRATIE: VAN SIS NAAR eID

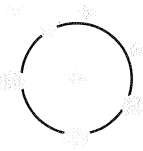
Vandaag wordt in de meeste ziekenhuizen de SIS-kaart (al dan niet in combinatie met een identiteitskaart) gebruikt voor de registratie van patiënten in het ziekenhuisinformatiesysteem. De SIS-kaart bevat immers de 'elektronische identiteit' van de persoon in kwestie, al is dat niet steeds de drager van de SIS-kaart zelf. In het geval van kinderen bijvoorbeeld, wordt de SIS-kaart door een ouder of verantwoordelijke bijgehouden waardoor het persoonlijk karakter van de kaart verdwijnt. Bij de elektronische identiteitskaart is dit niet het geval gezien het hier gaat om een wettelijke verplichting om de kaart persoonlijk bij zich te houden, al geldt dit dan weer enkel voor kinderen vanaf 12 jaar, terwijl de SIS-kaart vanaf de geboorte ter beschikking wordt gesteld. Een zaak is alvast duidelijk: de SIS-kaart laat 'automatische registratie' van patiënten toe zonder dat informatie moet worden overgetikt in het ziekenhuisinformatiesysteem, met alle mogelijke tikfouten van dien.

Waarom overschakelen naar de eID is dan ook een zinvolle vraag, temeer omdat door middel van de SIS-kaart een logische automatisering bereikt blijkt. Eerder dan 'een nieuwe gril van de overheid' of 'een goeie Belgenmop' is het antwoord samen te vatten onder de noemer 'technologische evolutie'. De SIS-kaart is niet alleen op het vlak van technologie, maar evenzeer conceptueel totaal anders dan de eID. Beide kaarten zijn zogenaamde 'smart-cards', maar op technologisch vlak is de SIS-kaart een zogenaamde geheugenkaart (zoals een bankkaart) waarop een aantal gegevens (zoals de verzekerbaarheidstoestand van de houder) staan gestockeerd terwijl de eID-kaart een processorkaart is, wat betekent dat ze naast opslag van gegevens eveneens bepaalde berekeningen kan uitvoeren, iets wat nodig is in het kader van de elektronische handtekening. De eID is dus eigenlijk een soort kleine computer. Het hoeft geen betoog dat de mogelijkheden van processorkaarten veel groter zijn dan die van geheugenkaarten. Daar waar de geheugenkaarten een hoog USB-stick-gehalte hebben waarop allerlei informatie kan worden gestockeerd, neigen de processorkaarten eerder naar PDA's waarop toepassingen kunnen draaien en waarmee berekeningen worden uitgevoerd.

Ook qua concept is de SIS-kaart grondig verschillend van de eID-kaart. Eerstgenoemde dateert uit de periode waarin interconnectiviteit nog niet de helft was van het niveau van vandaag. Opslag van bepaalde data op de kaart zelf, eerder dan in een centrale databank, was dan ook een logische keuze. Men kon nu immers bij de eerste SIS-kaarten niet verwachten dat alle apotheken waar de SIS-kaart diende te worden gepresenteerd een directe netwerkverbinding konden opzetten met de databanken van sociale zekerheid. De SIS-kaart was dus databank en sleutel tot deze databank tegelijk. Vanaf de start van de elektronische identiteitskaart werd een andere filosofie gehanteerd. Er werd van het principe uitgegaan om geen onnodige gegevens op de kaart zelf te stockeren, met uitzondering van het adres omwille van de praktische overweging dat een burger zich geen nieuwe kaart moet aanschaffen bij elke verhuis. Bovendien maakt het adres in se geen deel uit van de identiteit van een persoon: het is niet omdat iemand verhuist, dat deze persoon van identiteit verandert.

De elektronische identiteitskaart is eigenlijk meer de sleutel tot een databank dan een databank op zichzelf. In plaats van gegevens (weliswaar in versleutelde vorm) te wijzigen op de kaart zelf en dit parallel hiermee centraal te laten registreren, worden de gegevens, na ontsluiting met de juiste sleutel (lees eID en bijhorende PIN-code) direct centraal aangepast. Dit heeft onmiddellijk het grote voordeel dat men van eender waar en op eender welk moment met behulp van de juiste sleutel toegang kan krijgen tot de juiste gegevens. Speciale versleutel- en ontsleutelcomplexiteit zoals die voor de SIS-kaartlezers wordt geïmplementeerd (d.m.v. de zogenaamde SAM-kaart) zijn bij eID niet langer noodzakelijk. De kaart (i.c. de processorchip) neemt deze complexiteit over doordat ze in staat is autonoom versleuteling en ontsleuteling te doen, zolang de kaartlezer maar voldoende voeding hiervoor geeft.

Het is echter geenszins de bedoeling om de SIS-kaart als achterhaald te klasseren. Ze is immers de perfecte voorloper geweest van de eID op allerlei vlakken. In eerste instantie heeft de SIS-kaart de mensen vertrouwd gemaakt met het concept van een 'identificatiemiddel' in de vorm van een 'bankkaart'. Voor de personen die de registratie van patiënten doen, komt het er dus bij de overschakeling van SIS naar eID enkel op neer om naar de 'groene' kaart te vragen in plaats van naar de 'grijze'. Bovendien heeft de SIS-kaart ook de overheid een en ander geleerd over het opzetten en beheersen van dergelijke projecten op grote schaal.



VERDER DAN CAPTATIE VAN DATA: ONLINE AUTHENTISERING EN ELEKTRONISCHE HANDTEKENING

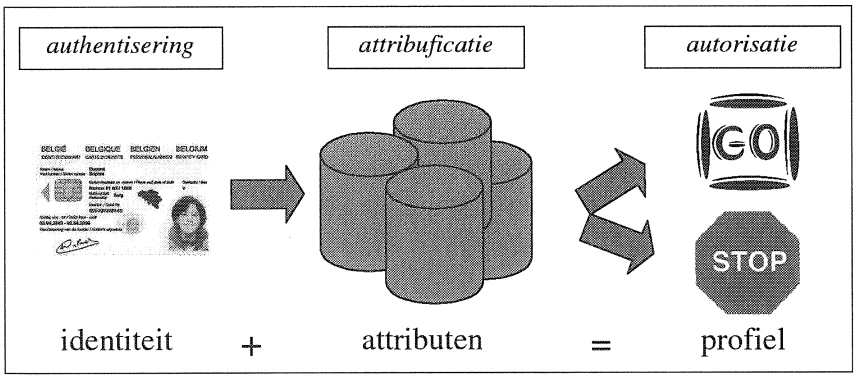
Het lezen van de gegevens op een smartcard is niet spectaculair en gebeurt reeds sinds jaren. Het gedeelte waarbij certificaten worden ingezet voor sterke authentisering enerzijds en een elektronische handtekening met juridisch bindend karakter anderzijds op een schaal van meer dan 8 miljoen personen is dat daarentegen wel. De verdeling van deze technologie op dergelijke schaal maakt het mogelijk om applicaties uit te rollen voor het grote publiek.

Binnen de gezondheidssector is het elektronisch patiëntendossier dé grote toepassing. Zowel (huis)artsen als patiënten zelf kunnen dossiers op een veilige manier van eender waar raadplegen, zolang men maar over de juiste rechten beschikt, wat ons op het domein van autorisatie brengt.

Eerder in dit artikel hebben we het reeds gehad over de filosofie om geen overtollige data op de chip van de eID te stockeren. Dit klinkt evident, maar is het allerminst. Het bepalen van een identiteit is één zaak, maar het toekennen van recht en aan die bepaalde identiteit een compleet andere. Bovendien vindt niemand het leuk om met vijf verschillende badges rond te lopen: een voor toegangscontrole, een voor de parking, een voor authentisering, een voor autorisatie in de rol van neurochirurg en een voor autorisatie in de rol van voorzitter van de lokale zwemvereniging.

Uit voorgaande is al meteen duidelijk dat het toekennen van autorisaties een veel diffuser proces is dan het vastleggen van de identiteit van een persoon, een activiteit die steeds op de gemeente plaatsvindt. Het opslaan van bepaalde attributen van een persoon (neurochirurg, voorzitter zwemvereniging, werknemer firma X, ...) op een eID maakt het proces van toekennen en intrekken van bepaalde autorisaties moeilijk. Stel dat een neurochirurg geschorst wordt door de Orde van Geneesheren maar weigert om zijn eID binnen te brengen waarop staat dat hij/zij neurochirurg is, dan kan de persoon in kwestie nog steeds bepaalde handelingen stellen of bepaalde informatie afdwingen bij andere besturen dan deze die op de hoogte zijn van de schorsing. Wanneer de eID gebruikt wordt als authentiseringsmiddel om zich als individu kenbaar te maken en de Orde centraal een databank ter beschikking stelt waar de attributen van iemand die zich voordoet als arts kunnen worden geverifieerd, bestaat dit probleem niet meer.

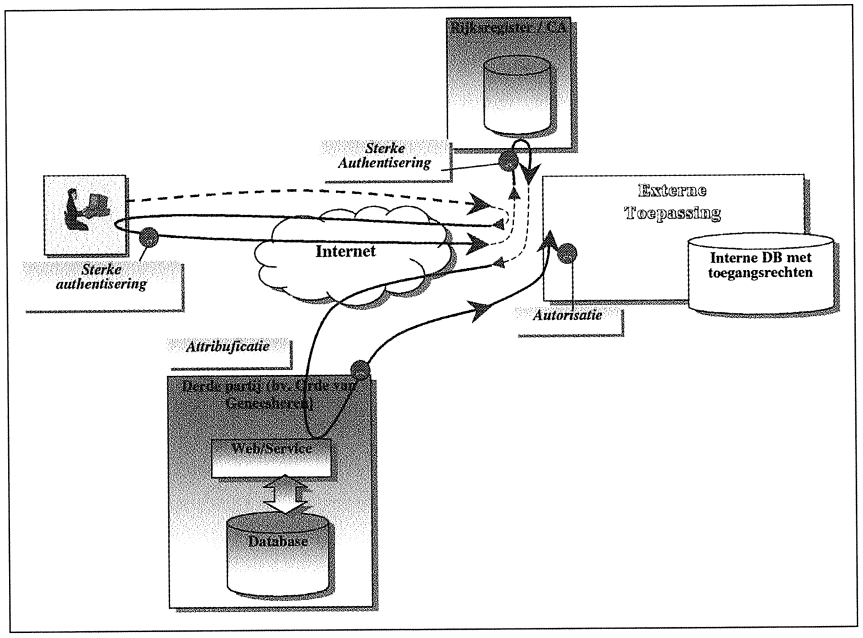
Het proces van 'attribuficatie' (ook wel 'kwalitatieve authentisering' genoemd) of m.a.w. het authentiek toekennen van bepaalde attributen en met deze attributen bepaalde rechten is duidelijk een gedeelde verantwoordelijkheid die best zoveel mogelijk wordt gescheiden van niet-attribuutgebonden processen zoals authentisering en digitale handtekening. Elke organisatie is immers authentieke bron van autorisaties voor elk van zijn leden of werknemers. Het proces voor toegang tot een bepaalde applicatie kan dus worden geschetst zoals in figuur 2.



Figuur 2: Authentisering, attribuficatie en autorisatie

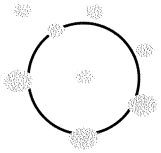
Als we even terugkeren naar het elektronisch patiëntendossier, dan zien we meteen een aantal mogelijke toepassingen van dit principe, zowel binnen als buiten de grenzen van een ziekenhuis. Intern in het ziekenhuis kan het lokale identity management een basis vormen voor de juiste autorisaties en toegangen tot bepaalde systemen en dossiers. Zoals verder zal worden verduidelijkt is het gebruik van de eID intern geen optie. Voor alle externe toegangen tot ziekenhuissystemen en medische dossiers daarentegen is eID de 'way to go'. Een sterke authentisering van de persoon die zich on line aanbiedt is noodzakelijk om zekerheid te hebben over de identiteit van deze persoon en om dus de juiste rechten aan de juiste persoon te kunnen koppelen. Patiënten zijn op die manier zeker dat ze enkel hun eigen medische informatie kunnen consulteren en niet die van hun vrienden en kennissen.

Met de huidige stand van zaken wat technologie betreft, kan er nog een stap verder worden gegaan, over de grenzen van ziekenhuizen heen. Net zoals elke burger bij het rijksregister kan nagaan wie er op welk moment voor welke doeleinden consultatie heeft gedaan van een persoonlijk dossier (cf. https://www.mijndossier.rrn.fgov.be), zou elke burger op basis van de eID kunnen nagaan welke medische informatie over hem/haar is gekend. Praktischer nog, een huisarts hoeft zich niet langer te bekommeren rond de keuze van het ziekenhuis wanneer hij informatie over zijn/haar patiënt opzoekt, maar kan rechtstreeks informatie over zijn patiënt opvragen waarna het systeem deze info kan doorspelen, eventueel geordend per ziekenhuis wanneer de patiënt in kwestie meerdere zorginstellingen heeft bezocht. Er bestaan in de regio Gent initiatieven tussen verschillende ziekenhuizen (GZO - Gents Ziekenhuis Overleg) die momenteel een gezamenlijk project opstarten hieromtrent. Een typische set-up van dergelijke configuratie is weergegeven in figuur 3.



Figuur 3: Typische set-up bij gebruik online authentisering

Op het vlak van de elektronische handtekening ligt de drempel nog een stuk hoger. Het certificaat dat gebruikt wordt voor de elektronische handtekening is van een zwaarder kaliber (lees: gekwalificeerd) dan dat voor de authentisering, wat (gelukkig) niet betekent dat de gebruiksvriendelijkheid ervan lager ligt. De reden voor deze keuze is gebaseerd op juridische richtlijnen die zijn vastgelegd in de Belgische wetgeving en steunen op een Europese richtlijn rond elektronische handtekeningen. Opnieuw werd hier voor de eID geopteerd voor de meest generieke oplossing op het vlak van elektronische handtekening, niettegenstaande veel stemmen opgingen en nog steeds opgaan voor de attribuutgebonden elektronische handtekening, of een handtekening per rol die men opneemt. Vaak wil men immers met IT de complexiteit onnodig opdrijven 'omdat het technologie is en deze de facto onbetrouwbaar is'. In de fysische wereld heeft toch ook niet iedereen een aparte handtekening voor elke rol die men opneemt?!



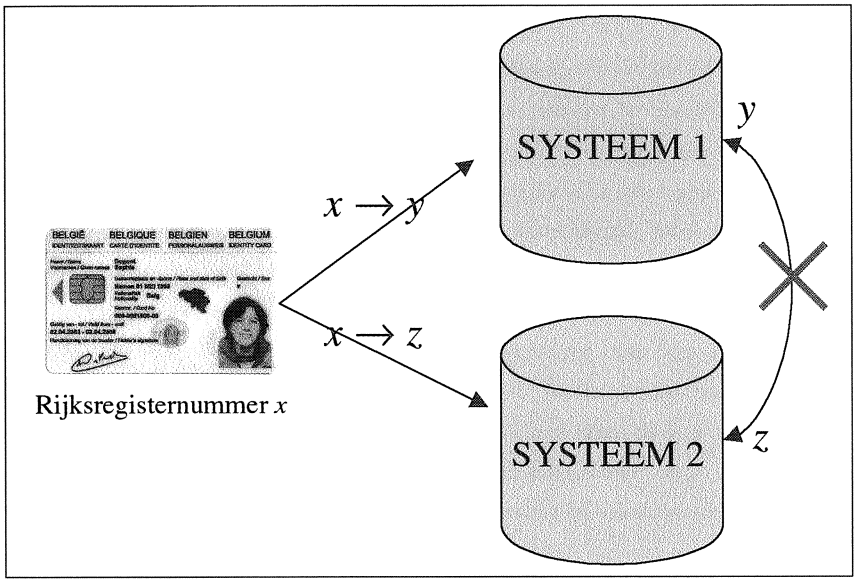
EEN CONTACTKAART

Het is echter niet allemaal rozengeur en maneschijn als het eID betreft. De huidige beschikbare technologie biedt reeds een stuk meer dan wat op de elektronische identiteitskaart beschikbaar is. Het feit dat een kaart in een lezer moet worden gestopt vooraleer eender welke functie ervan bruikbaar wordt, is niet meer van deze tijd en beperkt de bruikbaarheid ervan. Stel u even voor dat u de kaart moet gebruiken om de slagboom van de openluchtparking van uw bedrijf te openen. Als het niet te hard regent, is er geen probleem om het venster te openen. In het andere geval, rekening houdend met de snelheid (of volgens sommigen traagheid) van de kaart, kan je behoorlijk nat worden.

Het is uiteraard niet evident om de kaart volledig 'contactloos' te maken. De elektronische handtekening en de berekeningen (RSA-encryptie) die de chip hiervoor moet uitvoeren zijn de grote boosdoener. Het zou echter perfect denkbaar zijn om bepaalde gegevens van de kaart ook 'draadloos' ter beschikking te stellen. De gegevens die nodig zijn voor bovenvermeld proces van parkeertoegang zijn een mooi voorbeeld, maar leggen meteen een gevaar bloot: hoe blijft het vrijgeven ervan onder controle van de eigenaar? Wie zal er m.a.w. garanderen dat mijn gegevens die nodig zijn om de parking op te rijden ook niet in een grootwarenhuis worden uitgelezen om mij te bestoken met reclame op basis van mijn koopgedrag?

Ook voor het probleem van controle op persoonsgebonden data heeft de technologie al lang zijn oplossingen. Het is bijvoorbeeld mogelijk om de kaart enkel welbepaalde gegevens te laten ontsluiten wanneer ze een bepaalde context (lezer, toepassing, ...) waarneemt. Het finaliteits- en proportionaliteitsprincipe blijven op die manier volkomen gehonoreerd. Bovendien kan de intelligentie zo ver gaan dat er per context een aparte 'sleutel' bestaat zodat de informatie uit verschillende contexten niet op automatische wijze kan worden gelinkt. Wanneer bijvoorbeeld een individu met rijksregisternummer *x* zich presenteert aan een eerste systeem, dan wordt het unieke nummer *x* voor dit systeem (context) geconverteerd naar een uniek nummer *y* en is dit individu in dit systeem verder enkel gekend onder dit nieuwe nummer *y*. Voor een tweede systeem kan op analoge wijze rijksregisternummer *x* worden omgezet in een uniek nummer *z*. De nummers *y* en *z* zijn uiteraard verschillend van elkaar en

beiden rechtsreeks afleidbaar uit x. Vanuit de nummers y en z kan het origineel nummer x echter nooit gereconstrueerd worden, gezien de algoritmes die gebruikt worden voor de conversie van x in y enerzijds en voor de omzetting van x naar z anderzijds irreversibel zijn. Wanneer het eerste systeem informatie over persoon x wil uitwisselen met het tweede systeem, dan moet de eID van persoon x aanwezig zijn en met de eID de toestemming van de persoon om informatie uit te wisselen. Men weet immers nooit dat nummer y uit het eerste systeem overeenkomt met nummer z uit het tweede systeem, gezien er geen link vanuit y en z naar x bestaat. De privacy van persoon x wordt dus perfect gegarandeerd. In figuur 4 wordt dit grafisch voorgesteld.



Figuur 4: Gebruik van eID in verschillende contexten

TOEKOMSTMOGELIJKHEDEN VOOR eID IN UZ GENT

Net zoals de meeste bedrijven en instellingen wordt de eID in het UZ Gent in eerste instantie gebruikt voor datacaptatie bij de registratie van nieuwe patiënten. Voor bestaande patiënten worden adresaanpassingen gedaan op basis van de eID. De plannen voor gebruik van geautomatiseerde authentisering van personeel op basis van eID zijn groot, maar zullen niet voor morgen zijn, gelet op het type kaart waarvoor de overheid gekozen heeft (zie hoger). De praktische haalbaarheid van het gebruik van eID als personeelsbadge is m.a.w. nog ver af. Wat wel kan, is het koppelen van een personeelsbadge aan de eID en een authentieke bron van (toegangs)rechten.

Nemen we het voorbeeld van een spoedafdeling waar patiënten van verschillende medische disciplines door elkaar liggen. De doelstelling zou moeten zijn dat de arts die zijn/haar patiënt bezoekt automatisch het elektronisch patiëntendossier van de betrokken patiënt krijgt gepresenteerd op het moment dat de arts zich voldoende dicht bij de pc begeeft en dat de pc de arts aflogt van zodra deze weer uit het bereik van de pc is. Dergelijke systemen zijn geen dromen, maar bestaan. Het gebruik van de eID in zijn huidige constellatie hiervoor is echter uitgesloten gelet op eerder aangehaalde argumenten.

Het gebruik van de elektronische handtekening binnen de zorgsector biedt eveneens een waaier aan mogelijkheden. Op het ogenblik dat bijvoorbeeld radiologen on line met spraakherkenning in het PACS-luik van het ziekenhuisinformatiesysteem kunnen protocolleren en tekenen, zal er veel tijd (en vooral papier) kunnen gespaard worden. Bovendien kan elke arts die online dossiers bekijkt meteen de reeds getekende protocollen onderscheiden van de niet-ondertekende en hiermee een zicht krijgen op welke verslagen al dan niet reeds gefinaliseerd zijn. De benutting van het ziekenhuisinformatiesysteem wordt op die manier een stuk efficiënter. De tijdsspanne tussen levering en gebruik van informatie wordt immers tot nul gereduceerd.

Het is duidelijk dat de eID nog veel toekomst kan hebben in het UZ Gent evenals in andere zorginstellingen, maar dat ze hiervoor nog wat extra mogelijkheden moet bieden, vooral op het vlak van contactloze informatiedoorstroming. Het is vandaag koffiedik kijken of de overheid hiervoor in de nabije toekomst tijd en middelen zal vrijmaken.

VERDERE TOEKOMSTPERSPECTIEVEN VOOR DE eID

Het is reeds eerder gezegd in dit artikel: de tijd staat niet stil en met de tijd de technologische evolutie. De mogelijkheden voor uitbreiding van de eID zijn vandaag reeds legio, denken we maar aan bijvoorbeeld het toevoegen van biometrie of het gebruik van RFID technologie.

De integratie van RFID is zoals reeds aangehaald met de huidige technologie geen inbreuk meer op de persoonlijke levenssfeer van personen en kan snel worden ingevoerd. Voor de introductie van biometrie zijn er nog een paar andere hindernissen te overwinnen, zoals bijvoorbeeld de keuze van het type biometrie (retinascan, vingerafdruk, gelaatsherkenning, ...) die men wil gebruiken. Aligneren op één bepaalde technologie heeft zijn voordelen op het vlak van complexiteit, maar eveneens zijn nadelen. Denken we maar aan de problematiek dat een vingerafdruk na een lange vliegtuigreis moeilijke herkenning kan opleveren omdat ons lichaam door de reis wat uitgedroogd is. Een matrix van een aantal biometrische componenten kan hier een oplossing zijn. Ook het proces en de infrastructuur die nodig is voor het capteren van deze gegevens bij individuele personen moeten worden bekeken.

Wat er ook van zij, de eID is mooie technologie en een product om als Belg fier op te zijn. We mogen met volle teugen genieten van de internationale aandacht voor onze kaart, maar moeten vermijden dat de kopieën beter worden dan het origineel ...