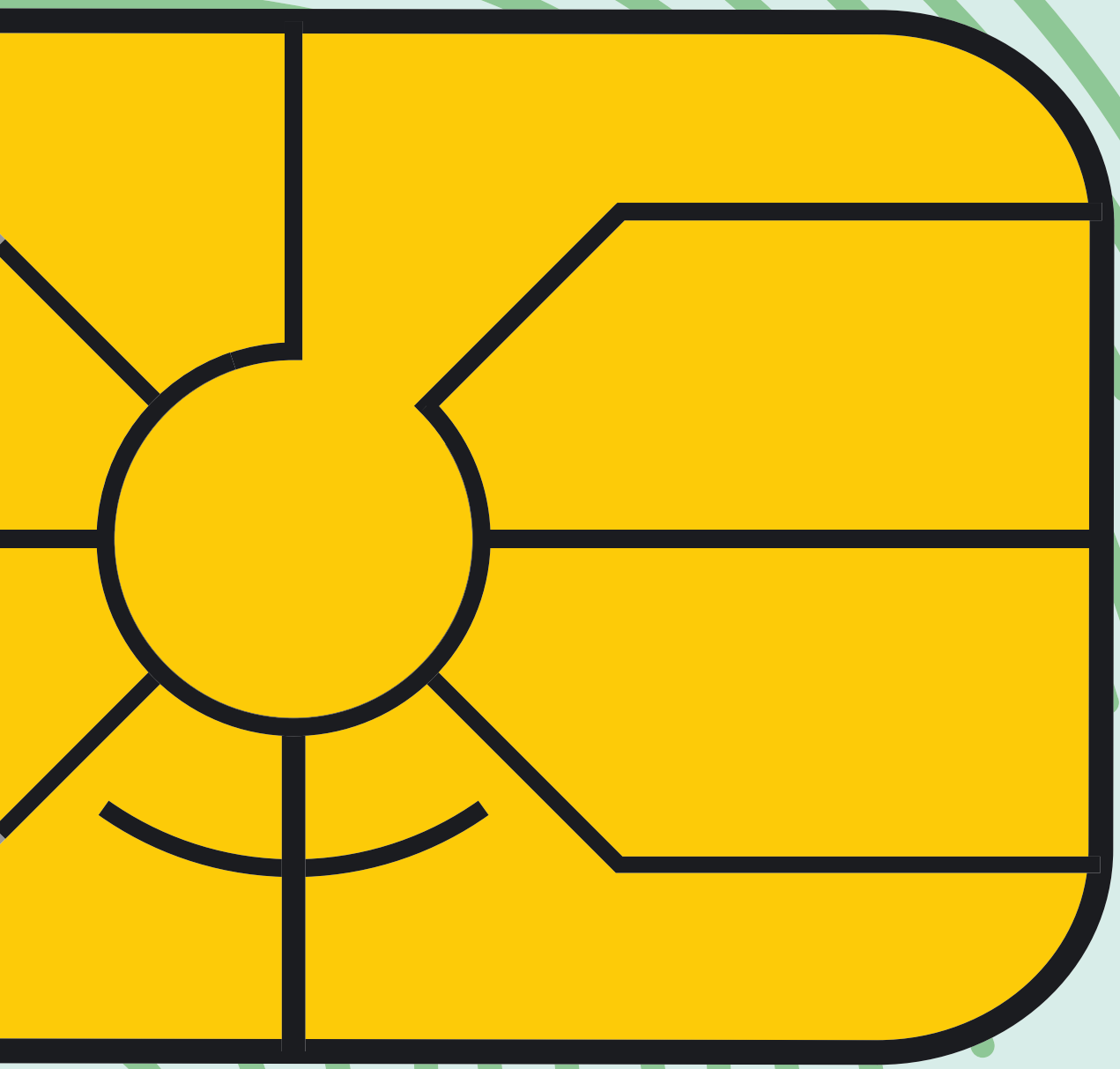


DE ELEKTRONISCHE IDENTITEITSKAART

EEN GIDS VOOR DE GEBRUIKERS EN DE ONTWIKKELAARS VAN TOEPASSINGEN

Voorwoord

De invoering van de elektronische identiteitskaart maakt deel uit van de uitwerking van het e-government die hand in hand gaat met de administratieve vereenvoudiging en de modernisering van de overheidsdiensten. Deze hervormingen hebben de bedoeling de administratie zoveel en zo goed mogelijk ten dienste te stellen van de burger.

De nieuwe identiteitskaart behoudt niet enkel de functies die zij steeds vervuld heeft met name de identificatie van de houder, maar maakt het ook mogelijk dat deze functies elektronisch worden uitgevoerd. Bovendien zal iedere burger een rechtsgeldige handtekening elektronisch kunnen plaatsen. Hierdoor ontstaat een snellere en klantvriendelijke dienstverlening zonder dat de privé-gegevens in het gedrang komen. De privacy wordt immers gegarandeerd door het invoeren van tal van veiligheidsmechanismen en de oprichting van een commissie belast met het toezicht op de strikte toepassing van de regels die toegang verlenen tot persoonsgegevens.

De uitreiking van de identiteitskaarten zal plaatsvinden via de gemeentebesturen met wie de burger in nauw contact staat. De gemeenten zijn elektronisch verbonden met de federale overheid, de erkende firma's en de certificatieautoriteiten die op verschillende niveaus aan het proces deelnemen. Het Rijksregister van de natuurlijke personen speelt een sleutelrol zowel bij de inrichting als bij de controle van het systeem.

Het succes van het gebruik van de elektronische kaart zal grotendeels afhangen van de toepassingen die aan de burgers zullen aangeboden worden niet enkel door de overheidsdiensten (on line consulteren van eigen dossiergegevens bij de overheid, toegang tot allerhande diensten via een portalsite) maar ook door de privé-instanties. De nieuwe toepassingen die zullen gecreëerd worden zullen een meerwaarde betekenen zowel voor de gebruiker als voor de betrokken instantie. Deze brochure is dan ook bestemd voor al diegenen die nood hebben aan algemene en technische informatie. De gebruikers zullen eruit leren hoe het systeem in elkaar zit en welke uitrusting zij nodig hebben. De ontwikkelaars van toepassingen zullen er de nodige informatie vinden om de elektronische identiteitskaart op de best mogelijke wijze aan te wenden in overeenstemming met hun doelstellingen. Zo zal door het gebruik van dit nieuwe elektronische product een belangrijke stap gezet worden in het digitale tijdperk.

Inhoudstafel

Algemene informatie

Invoering van de elektronische identiteitskaart (afgekort EIK)

De elektronische identiteitskaart komt eraan.

Alle inwoners van één van de elf volgende pilootgemeenten zullen weldra kunnen beschikken over een elektronische identiteitskaart en als eersten kunnen deelnemen aan het nieuwe tijdperk van het E-government:

11 pilootgemeenten:	Provincie of Administratief Arrondissement
Borsbeek	Antwerpen
Geraardsbergen	Oost-Vlaanderen
Jabbeke	West-Vlaanderen
Leuven	Vlaams-Brabant
Tongeren	Limburg
Sint-Pieters-Woluwe	Administratief Arrondissement Brussel-Hoofdstad
Lasne	Waals-Brabant
Marche-en-Famenne	Luxemburg
Rochefort	Namen
Seneffe	Henegouwen
Seraing	Luik

Het is de bedoeling de elektronische identiteitskaart geleidelijk in te voeren. De invoering in de 11 gemeenten zal op de voet gevolgd worden en de Ministerraad zal het project tijdig evalueren en bijsturen.

Hoe zal de nieuwe identiteitskaart eruit zien ?

De elektronische identiteitskaart zal het formaat van een bankkaart hebben en een microchip bevatten.

Zichtbare informatie
Zoals op de huidige identiteitskaart zal de nieuwe kaart zichtbare informatie bevatten: de naam en twee eerste voornamen, de eerste letter van de derde voornaam, de nationaliteit, de geboorteplaats- en datum, het geslacht, de plaats van afgifte van de kaart, de begin- en einddatum van geldigheid van de kaart, de benaming en het nummer van de kaart, het identificatienummer van het Rijksregister van de natuurlijke personen, de foto van de houder, de handtekening van de houder en van de gemeentelijke ambtenaar.

Onzichtbare, elektronisch leesbare informatie
De elektronisch leesbare informatie is dezelfde als de informatie die met het blote oog leesbaar is. Het adres van de houder zal enkel elektronisch opgeslagen zijn zodat de kaart niet moet vervangen worden bij iedere verhuizing. Verder zal de kaart volgende gegevens bevatten: de identiteits- en handtekeningsleutels, de identiteits- en handtekeningscertificaten, de geaccrediteerde certificatendienstverlener, de informatie nodig voor de authenticatie

van de kaart en voor de beveiliging van de elektronisch leesbare gegevens en voor het gebruik van de bijhorende gekwalificeerde certificaten.

De houder van de kaart beslist zelf of hij al dan niet zijn kaart wenst te 'initialiseren' (dit betekent: al dan niet zijn identiteits- en handtekeningencertificaten wenst te gebruiken). Wenst hij dat niet, dan worden de gegevens in verband met de identiteits- en handtekeningsleutels, de identiteits- en handtekeningscertificaten en de geaccrediteerde certificatendienstverlener bij de certificatieautoriteit in de status "niet actief" gehouden en de kaarthouder ontvangt geen pincode.

Wie zal een EIK ontvangen?

In 4 gevallen kan de burger uit de 11 voornoemde gemeenten een elektronische identiteitskaart verkrijgen:

1. de oude kaart van een inwoner van één van de pilootgemeenten vervalt. Op dat ogenblik ontvangt deze burger automatisch een convocatie om zich naar het gemeentehuis te begeven om een nieuwe elektronische kaart aan te vragen: hij/zij ontvangt een nieuwe elektronische identiteitskaart;
2. alle twaalfjarigen krijgen ook tegen de datum van hun verjaardag een convocatie om een elektronische identiteitskaart aan te vragen;
3. in geval de oude identiteitskaart verloren of gestolen is of aan vervanging toe door beschadiging, wordt ze vervangen door een elektronische identiteitskaart;
4. bij vrijwillige aanvraag wordt de oude kaart ingeruild tegen een nieuwe, elektronische.

Hoe wordt de EIK geactiveerd?

In alle vier gevallen wordt de kaart door de burger geactiveerd in het gemeentehuis van de gemeente waar hij zijn woonplaats heeft. De burger zal daarbij de keuze maken tussen het gebruik van de kaart als louter identiteitsbewijs dan wel als kaart die niet alleen zijn identificatie verzekert, maar ook zijn elektronische handtekening bevat.

In beide gevallen gaat de burger naar het gemeentehuis met zijn convocatieformulier en een paar pasfoto's. Op het aanvraagformulier van de identiteitskaart wordt de foto gekleefd van de aanvrager en het formulier wordt ondertekend zowel door de toekomstige houder van de kaart als door de ambtenaar van de gemeente.

Wie kiest voor het gebruik van een elektronische handtekening zal ook een formulier moeten ondertekenen waarin hij/zij zich akkoord verklaart met het gebruik van deze handtekening. Dit formulier blijft in de gemeente. De kostprijs voor de kaart zonder elektronische handtekening en deze met elektronische handtekening is dezelfde.

Binnen korte termijn zal de aanvrager van een kaart thuis een brief ontvangen waarin hij wordt uitgenodigd zijn kaart af te halen op het gemeentehuis. Hij ontvangt ook een tweede brief met een PIN-code en een PUK-code.

De PIN-code (Private Identification Number) is het privaat identificatienummer. De PUK-code (Personal Unblokked Key) is de activeringscode. Net zoals bij een bankkaart zijn de codes beschermd door een beschermlaag die moet afgekrabd worden om leesbaar te zijn.

Met de ontvangen brieven gaat de burger naar het gemeentehuis waar een ambtenaar zijn kaart in een kaartlezer brengt om het activeringsproces op gang te brengen en de digitale

handtekening te controleren.

Gebruikt de houder van de kaart geen elektronische handtekening dan zal hij enkel zijn PUK-code moeten invoeren om de kaart te activeren. Daardoor wordt de kaart beveiligd en zo kunnen de elektronische gegevens (zoals het adres en de digitale foto) geactiveerd worden en gelezen worden door de diensten die daartoe bevoegd zijn.

Om een elektronische handtekening te genereren brengt de houder van de kaart zelf zijn PIN-code in. Via het systeem wordt hij ervan verwittigd of alles al dan niet correct is verlopen. Is het antwoord OK dan is het afgelopen, zoniet, dan is er een fout opgetreden: een verkeerde code? Tot driemaal toe kan de code worden ingetikt, daarna wordt de kaart geblokkeerd, maar met de PUK-code kan de ambtenaar het proces herstellen. Een laatste mogelijkheid bestaat in het genereren van een nieuwe PIN door gebruik te maken van een PUK 3-code. De burger ziet de nieuwe code verschijnen en neemt er nota van.

Bij een productiefout wordt de kaart ingetrokken ofwel fungeert de kaart enkel als identiteitskaart en wordt de handtekening niet geactiveerd. Een nieuwe kaart wordt aangevraagd.

Als er zich problemen voordoen met het leestoestel, dan krijgt de ambtenaar een foutmelding op zijn scherm en dankzij de opleiding die hij zal gekregen hebben, zal hij in staat zijn de problemen op te lossen. Zoniet, kan hij een beroep doen op de helpdesk die 24 uur op 24 beschikbaar zal zijn op het Ministerie van Binnenlandse Zaken.

Zodra de kaart geactiveerd is wordt ze door de ambtenaar aan de houder overhandigd. Op het einde van deze handeling heeft de houder nog de kans, als hij dit wenst, zijn PIN-code te veranderen en dus een andere, persoonlijke code in te voeren.

Wie zijn de actoren van dit proces?

• **De kaartproducent, de kaartpersonalisator en de kaartinitialisator.**

De kaartproducent ook CM genoemd (Card Manufacturer): zorgt voor het maken van de materiële kaart en de chip.

De kaartpersonalisator of CP (Card Personalisator): bedrukt de kaart met de persoonlijke gegevens en zorgt voor de veiligheidsmaatregelen daaromtrent (vermijden van vervalsing en dergelijke).

De kaartinitialisator of CI (Card Initialisator) houdt zich bezig met de digitale kant van de handeling.

Deze drie handelingen kunnen door een en dezelfde of door twee of drie firma's uitgevoerd worden op voorwaarde dat ze erkend zijn door een Europese openbare aanbesteding. Momenteel worden deze handelingen verzorgd door de firma ZETES, in het kader van een overheidsopdracht.

• **Het Rijksregister van de natuurlijke personen** (RR) is het knooppunt van het systeem. Deze dienst zorgt voor de coördinatie tussen de aanvrager van de EIK in de gemeenten en het contact met de CM, de CP en de CI. Alle stappen in het productieproces worden gemeld aan het Rijksregister.

Het Rijksregister vraagt ook de certificaten van de authenticatie en van de digitale handtekening aan aan de certificatieautoriteit. De CI maakt de veiligheidssleutels aan. Het RR gaat na of het toegekende sleutelpaar slechts eenmaal bestaat: de publieke sleutel wordt gecontroleerd, de privé-sleutel is niet gekend. Het RR maakt de gegevens klaar om een certificaat aan te vragen voor het gecontroleerde sleutelpaar: het RR maakt een certificaatnummer aan en vraagt aan een erkende certificatieautoriteit een certificaat toe te kennen. De erkenning van een certificatieautoriteit beantwoordt aan de wet van 9 juli 2001 van het Ministerie van Economische zaken en aan de Europese eisen op dat vlak.

• **Een erkende certificatieautoriteit:** maakt het certificaat aan dat door het RR aangevraagd werd.

Een certificaat is een elektronisch document dat onder meer de verbinding legt tussen de veiligheidssleutels en de identiteit van de kaarthouder. Het bevat informatie over de houder van een identiteitskaart, een publieke sleutel en het adres van de site van de certificatieautoriteit. Het certificaat wordt ondertekend door de Certificatieautoriteit met zijn privé-sleutel. De kaart kent ook de publieke sleutel van de Certificatieautoriteit en zo kan worden nagegaan of het certificaat geldig is en geen wijzigingen heeft ondergaan.

De geldigheid van het certificaat wordt nagegaan door een OCSP[1]-opvraging bij de certificatieautoriteit. Een verzonden bericht wordt beveiligd door toevoeging van een hashwaarde. Dit is de alfanumerieke waarde (uitgedrukt in cijfers en letters) van het bericht dat gecomprimeerd wordt verstuurd. Bij iedere wijziging van het document zal ook deze alfanumerieke waarde veranderen. Iedere hash is vercijferd met een privé-sleutel. Deze hash wordt ontcijferd met de publieke sleutel van de verstuurder. Het systeem zal bij de ontvangst van een bericht nagaan of de hashwaarde dezelfde is gebleven als deze van de oorspronkelijke tekst. Zo zal de ontvanger met zekerheid weten dat het document dat hij ondertekent en goedkeurt niet gewijzigd werd.

Welke zijn de toepassingen en de voordelen van de elektronische identiteitskaart?

Dankzij de elektronische identiteitskaart zal iedere burger met een elektronische handtekening:

- Toegang hebben tot zijn dossiers bij de overheid: hij zal bijvoorbeeld zijn dossier "bevolking" kunnen raadplegen, documenten kunnen aanvragen waarvoor hij zich nu moet verplaatsen en soms lang in de rij staan.

- Informatie on line uitwisselen met de overheid, privé-firma's of organisaties via een beveiligd elektronisch verkeer.

- Contact nemen met de gemeentelijke overheid: heel wat gemeenten beschikken nu reeds over een website waar alle nuttige inlichtingen over de diensten aangeboden door de gemeenten te vinden zijn: bibliotheek, sport, bevolking, openbaar vervoer, enz. Sommige gemeenten zijn trouwens reeds uitgerust met e-loketten waar een aanvraag kan plaatsvinden met elektronische formulieren. In Gent en in Seneffe is dit bijvoorbeeld het geval. Zie http://www.gent.be of http://www.seneffe.be. Dankzij de identificatie aan de hand van de elektronische identiteitskaart en de elektronische handtekening zullen de contacten met het gemeentebestuur in de toekomst gemakkelijker en efficiënter worden.

[1] On line certificate status protocol.

- Contact nemen met de gewesten en de federale overheid: ook de gewesten en de federale overheid stellen hun administratie ter beschikking van de burgers via het internet. FEDICT heeft de opdracht een strategie uit te werken om de Belgische Federale overheid tot een koploper in zake E-government te maken. Via de website van Fedict op het adres http://www.fedict.be of de federale portaalsite http://www.belgium.be/ kan men bij alle andere departementen terecht. De Vlaamse portaalsite vindt men op http://www.vlaanderen.be/; de Waalse op http://www.wallonie.be/; de Brusselse op http://www.brussel.irisnet.be/; de Duitstalige op http://www.dglive.be/; die van de Franstalige Gemeenschap op http://www.cfwb.be/.

- Commerciële transacties via het internet op een veilige manier uitvoeren, zowel als koper of als verkoper (aankoop en verkoop on line).

- Documenten elektronisch ondertekenen en ze dezelfde juridische waarde geven als met een gewone handtekening op papier. Rechtsgeldig ondertekende berichten versturen en zelfs contracten afsluiten met medeburgers, enz.

- Deelnemen aan alle toepassingen die in de toekomst zullen beschikbaar worden gesteld zowel door de overheid als door de privé-sector: reserveren, inschrijven, bestellen, betalen, afzeggen, en zoveel meer, dit zal allemaal mogelijk worden op een volkomen veilige manier. Andere toepassingen kunnen zijn: ondernemingsbadge, elektronische betaalkaart, aangifte van de BTW on line, enz.

- Als werknemer toegang hebben tot het bedrijfsnetwerk en eventueel het werk thuis via teleworking uitvoeren.

De bedrijven die reeds aanwezig zijn op het net zullen de kans hebben om over te schakelen van louter informatief gebruik naar toepassingen waar transacties zullen mogelijk zijn. Testkaarten zullen kunnen verkregen worden op het Ministerie van Binnenlandse Zaken op het Rijksregister, Directie van de Verkiezingen en van de Bevolking, Pachecolaan, 19 bus 20 – 1010 Brussel. Tel. 02/210.21.21. Fax: 02/210.21.86 – 02/210.21.49, e-mail: info@rijksregister.fgov.be

De kaart zal kunnen getest worden op de website van het Rijksregister op het volgende adres: http://www.rijksregister.fgov.be

Dankzij de EIK authenticatie en handtekening zullen de gangbare webservers veel toegankelijker zijn dan tot nog toe het geval was.

Ook de banken zullen kunnen genieten van de interoperabiliteit die de EIK mogelijk zal maken.

Aan de Universiteiten zal de EIK eveneens als studentenkaart kunnen gebruikt worden.

Waarom is de elektronische identiteitskaart veilig?

Omdat de functies met betrekking tot de identificatie en de elektronische handtekening beschermd zijn door twee paar sleutels: de identificatiesleutel en de handtekeningsleutel.

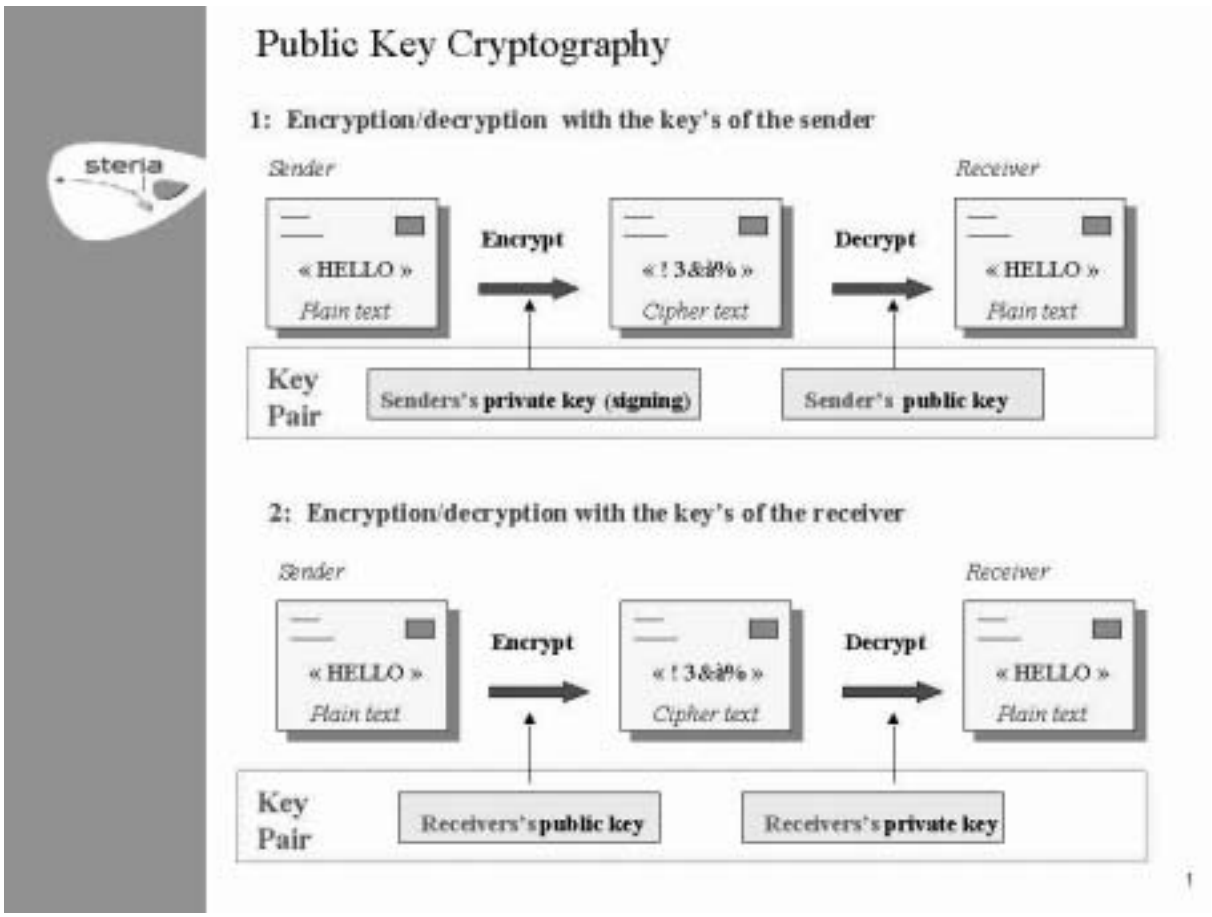
Door de identificatiesleutel maakt de houder van een kaart zijn identiteit bekend, hij zegt wie hij is. Dat doet hij door een PIN-code in te tikken, net zoals wanneer men een gsm gebruikt.

Dankzij de handtekeningsleutel kan de houder van een kaart met het gebruik van zijn PIN-code een elektronische handtekening plaatsen op formulieren. Deze handtekening zal dezelfde waarde hebben als een handtekening op papier.

Waarom zijn deze sleutels veilig? Omdat zij een combinatie zijn van twee sleutels: een privé-sleutel en een publieke sleutel. De privé-sleutel is geheim. Iedere sleutel is samengesteld uit 128 letters en cijfers. Met deze sleutels beschikt de houder van een kaart aldus over een handtekening die uniek is.

Door het gebruik van de privé-sleutels, de codes en de wachtwoorden wordt de privacy van de kaarthouder beschermd. Bovendien biedt een specifieke beveiliging de zekerheid over de authenticiteit van de afzender en van de ontvanger. Geen van beiden zullen kunnen beweren dat de boodschap niet verstuurd of niet ontvangen werd.

Voor een beter begrip, zie hierna de schema's opgesteld door de firma Steria, belast, in het kader van een overheidsopdracht, met de aanpassing van de informatica-infrastructuur van het Rijksregister en van de pilootgemeenten.



Geschikte apparatuur

Om een elektronische handtekening te gebruiken heeft men een leestoestel nodig dat aangesloten wordt op een gewone PC. De leestoestellen die compatibel zijn met de EIK zijn te vinden op http://www.rijksregister.fgov.be/.

Technische toelichting

Onder voorbehoud van het testen met de echte EIK kaart.

Deze toelichting beschrijft enkele mogelijkheden om aanpassingen te doen voor erkenning van de EIK in het kader van commerciële activiteiten –e-commerce-, en om bestaande toepassingen om te vormen naar een beveiligd platform (secure platform) op basis van de EIK.

Momenteel zijn heel wat gratis programma's (freeware) en commerciële producten in ontwikkeling om een smartcard te ondersteunen.

Enkele bestaande producten worden als voorbeeld genomen.

➢ Gebruikersgids voor bedrijven

- Web
  - ⊙ Apache
    Momenteel beschikt 65% van de webbrowsers over een apache versie.
    Er bestaan plug-in modules om de beveiliging op te drijven, ook wel eens Pam –plugable authentication modules- genoemd. Eén van dergelijke modules is mod_ssl, die de mogelijkheid biedt gebruik te maken van SSLv2 en v3 evenals TLS. Hierdoor kan men zijn site beveiligen met https. Mod ssl maakt gebruik van de library's van openssl.

    Er bestaan ook plugins in beta versie die gebruik maken van de mod_ssl plugin. Dit project is gebaseerd op een plugin voor een smartcard die door een smartcard reader gelezen wordt. Hierdoor ontstaat de mogelijkheid om een versterkte authenticatie (strong authentication) te verrichten met de "uitgebreide" apache web server d.m.v. een certificaat. Dit project noemt men smartcard netlogin. Een ander gelijkaardig project met dezelfde functionaliteiten is scas.

  - ⊙ Microsoft IIS – webserver van Microsoft
    Het project om smartcards te ondersteunen in de webbrowser van Microsoft noemt Fortezza.
    Enkel toepasbaar op IIS 5.0 of hoger.
    De cliënt pc moet fortezza-bestendig (compliant) zijn.

  - ⊙ Medium en high end integratie voor management van webacces

Momenteel bestaan er softwarepakketten die authenticatie combineren met gedistribueerd serverbeheer (distributed server management), en tevens de webservers beveiligen.
Zo'n pakket kan met authenticatiecombinaties werken en toegang verlenen naar gelang van autorisatie van de gebruiker. Zo kan men bijvoorbeeld toegang krijgen op basis van een certificaat, een controle uitvoeren of dit certificaat nog niet ingetrokken (revoked) is en dan nog een bijkomende authenticatie vragen zoals login /paswoord, ..

Dergelijke pakketten bieden zeer veel mogelijkheden, maar de standaardpakketten moeten verder ontwikkeld worden om ze aan te passen aan de eisen van elke toepassing of bedrijf. Deze producten veronderstellen meestal een grondige kennis en zijn meestal duur. Het centraal beheer geeft echter wel een zeer goed functioneel overzicht van het hele proces.

Sommige pakketten omvatten role-based access control (toegang voorbehouden aan personen op basis van hun functie), personalisatie van de gebruikersomgeving, user self-registration en verbindingen met andere beveiligingsproducten, zoals firewalls, intrusion detections, e.d. in combinatie met user databanken (ldap, nt, racf, ..). Deze duurdere oplossingen bevatten meestal controle-instrumenten (auditing tools) voor het beheer van het geheel.

- High end applicatieservers

  Applicatieservers bieden de mogelijkheid om granulaire toegang te creëren, vaak met een eigen ontwikkelde bibliotheek met tools.
  Vele van deze toepassingen hebben het voordeel dat men "out of the box" toepassingen kan ontwikkelen. Bij veel producten kent men de problemen van toegangscontrole (access control) tussen verschillende domeinen: men logt zich éénmalig in, en indien men naar een andere webserver doorverbindt, wordt opnieuw gevraagd om zich te identificeren.
  Om dit probleem op te lossen hebben leidinggevende bedrijven de standaard SAML aanvaard om interoperabiliteit tussen diverse producten te verwezenlijken.

• Host access

- Microsoft

  Windows 2000 en Windows XP ondersteunen het gebruik van een smartcard om in te loggen.

- Linux

  In Linux worden plugins ontwikkeld waar een smartcard ondersteund wordt voor versterkte authenticatie (strong authentication) login. Deze plugins zijn voortdurend in evolutie.
  Meer informatie over de huidige smartcard projecten kan men vinden onder het MUSCLE project. Gegevens over Linux projecten zijn te vinden op de site www.linuxnet.com

  Mits een beperkt aantal aanpassingen zouden sommige projecten de EIK kunnen ondersteunen.

- Smartcard enabled secure web access.
  Hiermee kan een document worden ondertekend vooraleer het te verzenden. Bij de opstartfase wordt een SSL[2] verbinding gemaakt met de webserver. Zodra deze verbinding bestaat wordt een hash gemaakt van de webpagina die verzonden wordt. Nadien wordt deze hash gesigneerd of geëncrypteerd via de privé-sleutel (private key) op de smartcard. De originele pagina wordt teruggezonden naar de webserver, waar aan de hand van de hash een controle uitgevoerd wordt. Op deze wijze kan worden nagegaan of de webpagina gewijzigd werd.

➢ Gebruikersgids voor burgers

• Netscape vs Internet explorer
Netscape gebruikt bijvoorbeeld pkcs-11, een bibliotheek van functies.
Microsoft gebruikt pc/sc en de bijhorende crypto api, geïntegreerd in internet explorer en andere windows producten.

• Mail

- Microsoft.
  Bij de installatie van MS office 2000 of andere recente besturingssystemen beschikt men over een mailpakket dat het gebruik van certificaten ondersteunt. Met deze basispaketten kan men met "S/MIME" werken, en op die wijze op een veilige manier een e-mail verzenden en ondertekenen.

- Netscape
  Netscape beschikt over een plug-in die ondersteuning biedt van een smartcard met netscape mail.

- Plug-ins

  - Adobe Acrobat
    Adobe vereist een bijkomende plug-in om documenten te beveiligen d.m.v. een digitale handtekening.

Waarborgen met betrekking tot de integratiemogelijkheden van de EIK in informaticasystemen.

De EIK beantwoordt aan de volgende normen:

01. ISO 7810	bepaalt de afmetingen van de kaart; in dit geval ID1-formaat.
02. ISO 7816-1	bepaalt het niveauverschil tussen de contacten en de kaart.
03. ISO 7816-2	bepaalt de lokalisatie van de contacten.
04. ISO 7816-3	bepaalt de elektronische signalen en transmissieprotocollen.
05. ISO 7816-4	bepaalt de intersectoriële commando's voor de uitwisselingen.
06. ISO 7816-5	bepaalt de nummeringsystemen en procedure voor het registreren van de identificatie van de toepassingen
07. ISO 7816-8	bepaalt de intersectoriële veiligheidscommando's.
08. ISO 7816-9	bepaalt bijkomende intersectoriële commando's en veiligheidsattributen.

[2] S/MIME: Secure/Multipurpose Internet Mail Extensions: een methode om vzilige internet boodschappen te zenden en te ontvangen.

Waarborgen met betrekking tot de technische kwaliteit van de EIK

De EIK beantwoordt aan de volgende normen:

01. MILSTD-883c	reglementeert de statische elektriciteit.
02. ISO 7811-1	bepaalt de reliëfdruk.
03. ISO 7811-3	bepaalt de plaats van de letters in reliëfdruk op de ID1-kaarten.
04. ISO 10373	reglementeert de dynamische torsie, de aanvaardingsgraad van de vibraties, de bestandheid tegen scheikundige producten
04. CECC 90 000	Salt Atmosphere and chip assembly humidity.

Waarborgen met betrekking tot de compatibiliteit van de programma's met de bestaande en toekomstige Windows omgevingen.

De compatibiliteit is verzekerd door 'CRYPTO API' van Microsoft en met de norm PKCS11 van RSA Labs.

De configuratie van het bestand stemt overeen met de norm PKCS15 versie 1.1 van RSA Labs.

De configuratie van de authentificatie- en handtekeningscertificaten zal overeenstemmen met de norm RFC 3039 (Qualified Certificate Profiles), die zelf gebaseerd is op de norm RFC2459 die de certificaten X509 Versie 3 beschrijft.

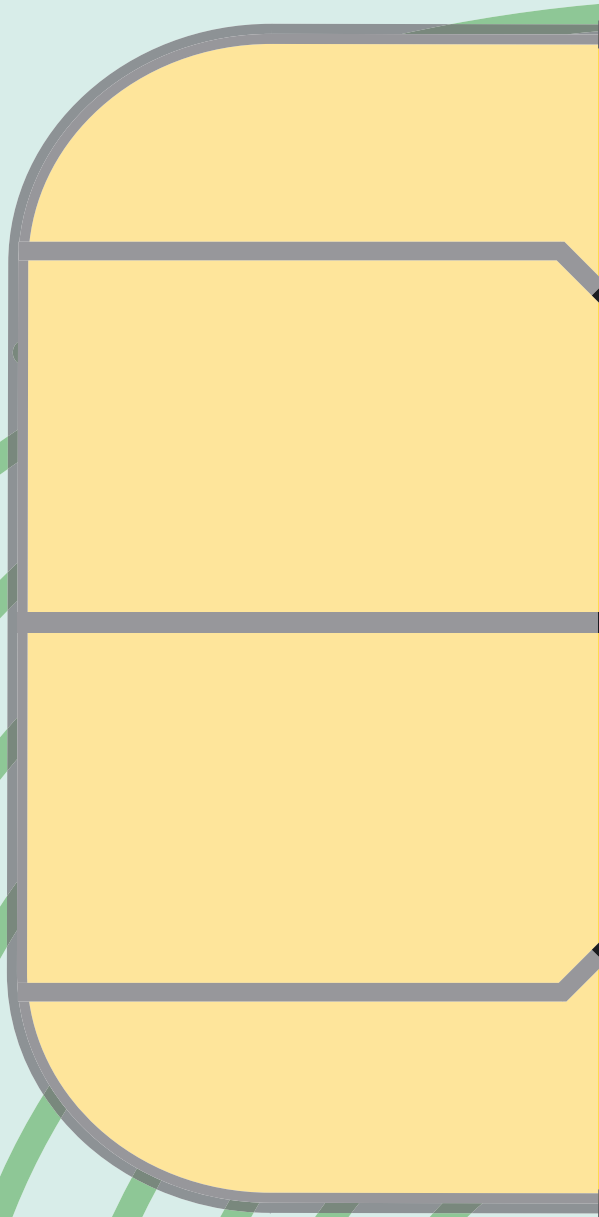
In het kader van de functie 'elektronische handtekening', zijn de volgende standaarden eveneens van belang :

1. RFC 3161 Internet X509 Public Key Infrastructure, Time-Stamp Protocol (protocol beveiligde registratieklok).
2. RFC 2044 UTF-8, a transformation format of Unicode and ISO 10646 (behelst de informatie die opgeslagen wordt op de elektronische chip van de EIK).
3. RFC 2527 Internet X509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework.
4. RFC 2560 Internet X509 Public Key Infrastructure, Online Certificate Status Protocol – OCSP.
5. Directive ETSI TS 101 456 : Policy Requirements for Certification Authorities Issuing Qualified Certificates.

Lijst van de gebruikte afkortingen

API	Application Programming Interface	Set functies voor het gebruik van een programmabibliotheek.
CA	Certicate Authority	Certificatieautoriteit: instantie die het certificaat uitreikt.
CI	Card Initialisator	Kaartinitialisator: maakt de kaart klaar op het digitale vlak.
CM	Card Manufacturer	Kaartproducent: zorgt voor het maken van de materiële kaart en de chip.
CP	Card Personalisator	Kaartpersonalisator: bedrukt de kaart met persoonlijke gegevens en beschermt ze tegen vervalsingen.
EIK		Elektronische identiteitskaart.
ETSI	European Telecommunications Standards Institute	Europees instituut dat richtlijnen opstelt voor de standaardisering van de telecommunicatie.
FEDICT		Federale overheidsdienst Informatie – en Communicatietechnologie.
HTTP	Hypertext tranfer protocol	Protocol voor de uitwisseling van hypertext-documenten op het World Wide Web.
ID	Indentity Card	Identiteitskaart.
IETF	Internet Engineering Task Force	Een informele Internetgroep voor standaardisatie.
ISO	International Standards Organisation	Internationale normen vastgesteld om het kwaliteitsmanagement te bevorderen.
LDAP	Lightweight Directory Access Protocol	Protocol dat gebruikt wordt om toegang te hebben tot "directory servers" (een directory is een soort database waar de informatie in een boomstructuur bewaard wordt).
MUSCLE	Movement for the Use of Smart Cards in a Linux Environment	Een project om de ontwikkeling van digitale kaarten en Linux-toepassingen te coördineren.
NT	New Technology	Besturingsprogramma van Windows.
OCSP	On line certificate status protocole	Protocol waarmee de revocatiestatus van een certificaat snel (in real time) kan worden nagegaan.
PAM	Pluggable Authentication Modules	Een flexibele, open architectuur voor de authenticatie van gebruikers op Linux-systemen.
PIN	Personal Identifcation Number	Het privaat identificatienummer van de elektronische kaart.
PKCS	Public Key Cryptography Standards	Een reeks specificaties uitgaande van RSA gegevensbeveiliging.
PUK	Personal Unblocking Key	De activeringssleutel van de elektronische kaart.
RACF	Resource Access Control Facility	Beheersinstrument met betrekking tot de veiligheid gebruikt door IBM.
RFC	Request For Comments	Een reeks specificaties uitgegeven door de IETF.
RR		Rijksregister van de natuurlijke personen.
RSA	Rivest, Shamir, Adleman	Asymmetrisch cryptografisch systeem uitgevonden door Rivest, Shamir en Adleman.

S/MIME	Secure/ Multipurpose Internet Mail Extensions	Een methode om veilige internetboodschappen te zenden en te ontvangen.
SAML	Security Assertion Markup Language	Een systeem gebaseerd op XML om informatie veilig uit te wisselen.
SSL	Secure Socket Layer	Een veiligheidsprotocol voor authenticatie en encodering op het internet.
TLS	Transport Layer Security	Een versie van SSL.
TS	Technical Specification	Technische specificatie van het ETSI.
UCS UTF-8	Universal Charter Set	Standaard voor tekensets voor XML. Tekenset voor XML, volgens UCS standaard.
X.509	The Directory Authentication Framework	Een gedetailleerde beschrijving van digitale certificaten en van het gebruik ervan.
XML	eXtensible Markup Languagae	Een internetstandaard voor de flexibele en logische opbouw van documentbestanden; het gebruik van XML maakt de informatie in de bestanden relatief eenvoudig toegankelijk.



V.U.: M. Van Oversteyens - • 03/03