Vingerafdrukken op de Belgische eID
Technische analyse

Jens Hermans Roel Peeters

KU Leuven - ESAT/COSIC

Samenvatting Door een recente wetswijziging zullen vingerafdrukken als biometrisch kenmerk toegevoegd worden aan de Belgische elektronische identiteitskaart (eID) en de vreemdelingenkaart[1]. In dit rapport analyseren we de technologie die gebruikt zal worden voor het opnemen van de vingerafdrukken op de eID, onder andere op het vlak van effectiviteit in het bestrijden van identiteitsfraude, performantie, gegevensbescherming en veiligheid. Gelet op de vele tekortkomingen die in dit document geïdentificeerd worden, formuleren we ook tal van alternatieven die beter presteren en de grondrechten van burgers veel minder aantasten.

[1] Dit document maakt verder abstractie van het onderscheid tussen de identiteitskaart en de vreemdelingenkaart.

Inhoudsopgave

1 Inleiding

De "Wet houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters" d.d. 25 november 2018 bepaalt dat vingerafdrukken als bijkomend biometrisch kenmerk toegevoegd worden aan de identiteitskaart. Het opnemen van het digitaal beeld van de vingerafdrukken in de chip van de eID wordt door de wetgever verantwoord met de strijd tegen identiteitsfraude, in casu om personen zo doeltreffend mogelijk te identificeren.

Voorafgaand aan de invoering van de wet was het enige biometrische kenmerk de foto van de houder (en de handtekening, voor zover deze als biometrisch kenmerk beschouwd wordt). De foto wordt digitaal in de chip opgeslagen en is tevens afgedrukt op de identiteitskaart. Het digitaal beeld van de vingerafdrukken zal uitsluitend digitaal in de chip opgeslagen worden.

Het gebruik van biometrische gegevens om, in combinatie met een authentiek identiteitsdocument, de identiteit van een persoon te kunnen bevestigen is een evidentie. In de context van een identiteitscontrole is er vaak geen andere manier om na te gaan of de aanwezige persoon overeenstemt met de persoon vermeldt op het document[2].

De keuze van de biometrische kenmerken om te gebruiken in de context van identiteitsdocumenten is echter helemaal geen evidentie. Er bestaat immers een zeer breed spectrum van biometrische kenmerken die gebruikt kunnen worden voor identificatie van personen. Goed bestudeerde biometrische kenmerken zijn o.a. het gezicht, vingerafdrukken, palmafdrukken, bloedvatpatronen van hand/vinger/oog, de iris, de vorm van de oren, de retina, de manier van wandelen, thermografie van het gezicht, een handtekening en DNA.

Bij de selectie van de gepaste biometrische kenmerken voor het identificeren van personen dient met uiteenlopende parameters rekening gehouden worden[3]:

- Onderscheidend vermogen (hoe verschillend is de gemeten eigenschap bij verschillende personen)
- Invariantie (in de tijd)
- Verzamelbaarheid (hoe eenvoudig is het om de eigenschap te meten)
- Universaliteit (beschikken alle personen over de gemeten eigenschap)
- Performantie (snelheid, accuraatheid; in uiteenlopende omstandigheden)
- Aanvaardbaarheid (hoe aanvaardbaar is het voor personen dat deze eigenschap gebruikt wordt)
- Omzeilbaarheid (hoe eenvoudig een vals biometrisch sample aangemaakt kan worden)
- Privacy-aspecten, zoals het risico op function creep (gebruik voor andere doeleinden dan origineel voorzien)

In Sectie 2 wordt de formulering van de wet onderzocht, in het bijzonder de elementen die betrekkening hebben op de technische implementatie van de

[2] Bij gebrek aan enig identiteitsdocument, of aan mogelijkheden om dit document te verifiëren, wordt er in sommige situaties gewerkt met getuigen. Voor een reguliere identiteitscontrole is dit echter praktisch niet haalbaar.

[3] A.K. Jain, A. Ross, S. Prabhakar, "An introduction to biometric recognition." IEEE Trans. Circuits Syst. Video Techn. 14(1): 4-20 (2004)

opname van vingerafdrukken in de eID. Sectie 3 gaat dieper in op de identiteitsfraude die men tracht te bestrijden en de mogelijkheden en problemen van biometrische gegevens in deze context, in het bijzonder van het gezicht en vingerafdrukken. Sectie 4 demonstreert hoe de chip zeer eenvoudig vernietigd kan worden, waardoor controle van de vingerafdrukken de facto onmogelijk wordt gemaakt.

Secties 5, 6 en 7 gaan dieper in op de technologie voor respectievelijk het opslaan van de vingerafdrukken op de eID, de aanmaakprocedure voor de eID en de toegang tot de vingerafdrukken op de eID. Basis voor deze analyse is de wet en, in het bijzonder voor Sectie 7, de technologie die momenteel gebruikt wordt voor de Belgische ePaspoorten.

2 Formulering van de wet

Artikel 27 van de bovenvermelde wet voegt de bepalingen met betrekking tot de vingerafdrukken toe aan de "Wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten". De voor de technische analyse relevante stukken van de wet worden hieronder overlopen, net als de interpretatie ervan die noodzakelijk is voor de verdere technische analyse.

2.1 Digitale beeld van de vingerafdrukken als elektronisch leesbaar gegeven

Er wordt een nieuw derde lid, 8° ingevoegd in Artikel 6, waarbij *"het digitale beeld van de vingerafdrukken van de wijsvingers van linker- en van de rechterhand"* (of een andere vinger bij invaliditeit of ongeschiktheid) toegevoegd wordt aan de *"elektronisch leesbare gegevens"* van de identiteitskaart.

Dit impliceert dat de vingerafdrukken opgeslagen zullen worden op de elektronische chip van de identiteitskaart. Zoals verder uiteengezet wordt in Sectie 5, heeft de bepaling dat het moet gaan over het *"digitale beeld"* van de vingerafdrukken verregaande implicaties op de beschikbare beschermingstechnieken. Ook het feit dat de gegevens *"elektronisch leesbaar"* moeten zijn heeft negatieve gevolgen voor de bescherming van de gegevens, zoals verder uiteengezet in Secties 5 en 7.

2.2 Bewaring van de vingerafdrukken

"De informatie als bedoeld in het derde lid, 8°, mag enkel worden bewaard gedurende de tijd die nodig is voor het aanmaken en afgeven van de identiteitskaart en in elk geval niet langer dan drie maanden, met dien verstande dat na die periode van drie maanden de gegevens hoe dan ook moeten worden vernietigd en verwijderd."

Het is niet duidelijk wat er juist begrepen dient te worden onder "bewaring". Het kan hier evident niet gaan om de opslag in de chip, aangezien deze opgeslagen

blijft voor een langere termijn dan voorzien in deze bepaling. De memorie van toelichting verduidelijkt echter dat het gaat om een centrale opslag.

Hoewel er verwezen wordt naar "de tijd die nodig is voor het aanmaken en afgeven van de identiteitskaart", is het niet gespecificeerd in de wet wat het doel van de bewaring is. De memorie van toelichting suggereert een centrale opslag gedurende maximaal de vermelde termijn om in geval van een probleem bij het aanmaken van de identiteitskaart een nieuwe kaart te maken, zonder dat de burger opnieuw zijn vingerafdrukken moet laten inlezen.

Verder is het niet gespecificeerd wie er toegang heeft tot deze databank (gegevens lezen en/of schrijven). Het is evenmin gespecifieerd of er, en zoja, welke, veiligheidsmechanismes voorzien moeten worden om de toegang tot deze databank en overdracht van gegevens van en naar deze databank te beveiligen.

2.3 Machtiging tot lezen van het digitaal beeld van de vingerafdrukken

"Zijn ertoe gemachtigd de informatie als bedoeld in het derde lid, 8°, te lezen:", gevolgd door een opsomming van verscheidene categorieën van personen en diensten in binnen- en buitenland. Gezien de verwijzing naar het derde lid, 8°, kan verondersteld worden dat het gaat om het lezen van de data op de chip van identiteitskaart en niet de centrale opslag; al is het gebrek aan enige expliciete bepaling rond het lezen/schrijven van de centrale opslag problematisch voor een sluitende interpretatie. De wet maakt niet duidelijk of voor het afdwingen van de machtiging technische maatregelen genomen worden (i.e. om toegang tot deze data technisch onmogelijk te maken voor andere personen), dan wel dat het gaat om een machtiging van louter juridische aard.

2.4 Leesbare gegevens op de elektronische identiteitskaart

"De gegevens die op de elektronische identiteitskaart staan, zowel de gegevens die zichtbaar zijn met het blote oog als die welke gelezen kunnen worden met een kaartlezer, met uitzondering van de foto van de houder, van het Rijksregisternummer en van het digitale beeld van de vingerafdrukken, kunnen gelezen en/of opgenomen worden, in overeenstemming met de wettelijke en reglementaire bepalingen inzake de bescherming van de persoonlijke levenssfeer en de bescherming van de persoonsgegevens."

De formulering lijkt te suggereren dat de foto, het Rijksregisternummer en het digitaal beeld van de vingerafdrukken niet (vrij) uitgelezen of opgenomen kunnen worden. De bepaling bevat evenwel geen uitdrukkelijk verbod, hetgeen in het bijzonder voor de vingerafdrukken zorgwekkend is: indien slechts bepaalde personen of organisaties gemachtigd zijn om deze uit te lezen, dan zou een (afdwingbaar) verbod voor de niet-gemachtigden het logische complement zijn. Deze bepaling voorziet evenmin technische maatregelen voor het beschermen van het digitale beeld van de vingerafdrukken zoals opgeslagen op de chip.

2.5 Conclusie

De wet laat enorm veel elementen open met betrekking tot de werking van de centrale opslag en de toegang tot deze centrale opslag. Bovendien maakt de wet geen enkele melding of nog maar een suggestie van technische maatregelen die de gegevens moet beschermen, noch wat betreft de opslag op de chip van de identiteitskaart, noch wat betreft de toegang tot deze opslag en evenmin wat betreft de centrale opslag. Het totaal gebrek aan technische beschermingsmaatregelen in de wet is zorgwekkend.

Aangezien de wet geen technische informatie bevat baseren we ons voor een deel van de analyse op de technologie zoals gebruikt voor het opnemen van de vingerafdrukken in paspoorten.

3 Beoogde bestrijding van identiteitsfraude

Vooreerst is het van belang om 'identiteitsfraude' correct te definiëren. Het gaat hierbij uitsluitend om het fraudescenario waarbij een persoon een geldige identiteitskaart, die echter niet aan hem toebehoort, ter controle aanbiedt. Dergelijke fraude kan gedetecteerd worden met behulp van de biometrische kenmerken aanwezig op de kaart, aangezien deze toelaten de legitieme houder te onderscheiden van de fraudeur.

Er zijn echter verscheidene andere scenario's van identiteitsfraude die onmogelijk verhinderd kunnen worden door de voorgenomen maatregel:

- vervalsing van een identiteitskaart;
- onklaar maken van de elektronische chip, bv. door elektromagnetische straling, mechanische beschadiging van de chip, overspanning... teneinde uitlezing van de digitale gegevens onmogelijk te maken. Het valt op te merken dat een identiteitskaart met een defecte chip nog steeds een geldig identiteitsdocument is;
- aanvragen en laten aanmaken van een geldige identiteitskaart met biometrische gegevens van een andere persoon dan de op de kaart vermelde houder;
- aannemen van een andere identiteit 'op afstand', aangezien hierbij geen betrouwbare controle van de biometrische kenmerken mogelijk is;
- aannemen van een andere identiteit tegenover private organisaties, aangezien deze geen toegang krijgen tot de vingerafdrukken op de eID;
- identiteitsfraude waar de identiteitskaart niet aan te pas komt (bv. paspoorten, bank- en kredietkaarten, rijbewijzen, geboorteaktes... of zelfs zonder enig officieel document).

3.1 Bestaande gegevens

Op dit ogenblik kan absoluut niet gesteld worden dat de overheid bij identiteitscontroles performante en accurate biometrische vergelijkingsalgoritmes gebruikt. In quasi alle gevallen blijft de biometrische vergelijking beperkt tot een manuele vergelijking van de foto op de identiteitskaart en de gecontroleerde persoon. Voor

zover bekend wordt de chip van de eID amper uitgelezen bij identiteitscontroles aan bijvoorbeeld grenzen en al helemaal niet om de opgeslagen foto uit te lezen, laat staan te vergelijken.

Er bestaan nochtans accurate algoritmes voor het vergelijken van gezichten, die veel moeilijker misleid kunnen worden dan een menselijke controleur[4]. Het is belangrijk hierbij het onderscheid te maken tussen enerzijds gezichtsherkenningsalgoritmes, in een context waarbij een beeld van een subject vergeleken dient te worden met een databank van foto's (1-op-n vergelijking), en de 1-op-1 vergelijking in het kader van een identiteitscontrole. In dit laatste geval zijn veel accuratere resultaten mogelijk aangezien slechts twee foto's met elkaar vergeleken worden en de foto van het subject ook in gecontroleerde omstandigheden kan worden genomen. De controle is bovendien goedkoop, gezien de verwaarloosbare kostprijs van camera's (in o.a. smartphones).

Samenvattend kan gesteld worden dat de overheid onvoldoende gebruik maakt van de mogelijkheden die de huidige biometrische kenmerken bieden. Eventuele cijfers over identiteitsfraude dienen dan ook geïnterpreteerd te worden in dit licht. Slechts na een analyse van de huidige gevallen van identiteitsfraude, het uitsluiten van identiteitsfraude die niet gerelateerd is aan de eID, en het bepalen welke gevallen hiervan onmogelijk bestreden kunnen worden met biometrische vergelijkingsalgoritmes op basis van de foto van het gezicht van de houder, kan het overwogen worden om bijkomende biometrische gegevens in te zamelen. Dergelijke evaluatie is echter, voor zover ons bekend, nooit gemaakt. De noodzaak van de bijkomende registratie van vingerafdrukken is dus niet aangetoond.

3.2 Vingerafdrukken

In wetenschappelijke studies rond vingerafdrukken komen de volgende probleempunten naar voren (vaak omwille van de hoge kostprijs om betere studies op te zetten):

- te kleine populaties, hetgeen de betrouwbaarheid van de studie volledig ondermijnt
- een te homogene populatie (bv. geen oudere personen, geen personen die handenarbeid verrichten, genderonevenwicht...)
- biometrische samples die allemaal met hetzelfde meettoestel bekomen zijn (in de realiteit worden uiteenlopende lezers van verschillende producenten

[4] Zie o.a. P. Jonathon Phillips, Amy N. Yates, Ying Hu et al. "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms", PNAS June 12, 2018 115 (24) 6171-6176. (https://www.pnas.org/content/115/24/6171)

De beste 1-op-1 gezichtsvergelijkingsalgoritmes presteren even goed als forensisch experts, die ruim de tijd kregen om een volledige analyse uit te voeren van de foto's. De dataset was samengesteld uit paren van foto's van hetzij dezelfde persoon, hetzij een look-a-like, telkens in verschillende omstandigheden genomen. De algoritmes en experts moesten louter beoordelen of het in elk paar om dezelfde persoon ging of niet.

Het combineren van algoritmes met het oordeel van experts levert nog betere resultaten op.

gebruikt en is de kans klein dat eenzelfde toestel voor beide te vergelijken samples gebruikt is)
- biometrische samples die in dezelfde omstandigheden zijn afgenomen (weer – cruciaal voor de hoeveelheid zweet op de vingers), of, alle samples zijn op hetzelfde tijstip afgenomen – waardoor er geen evolutie in de tijd van de vingerafdrukken in rekening genomen wordt
- manueel filteren van de gebruikt populatie (verwijderen van afwijkende samples hoewel deze reëel zijn)

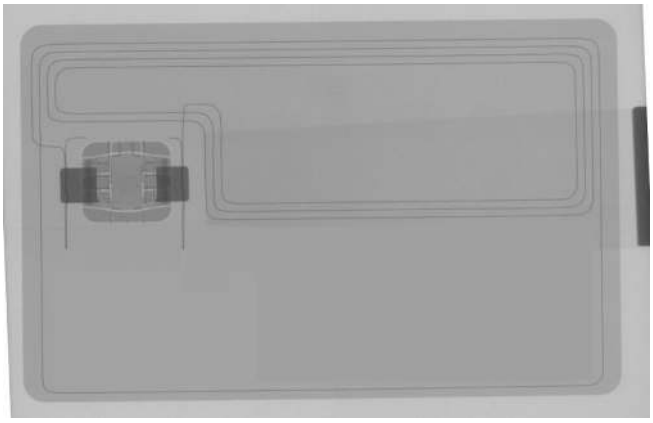
Omwille van de bovenstaande problemen wordt de accuraatheid van vingerafdrukken in studies typisch overschat. In werkelijkheid en wanneer toegepast op de volledig bevolking zullen de resultaten dus slechter zijn dan gerapporteerd.

Hoewel de patronen op de vingers relatief constant zijn in de tijd, stelt 'slijtage' van de vinger veel problemen. Door ouderdom gaat de elasticiteit van de huid achteruit, hetgeen een negatieve invloed heeft op de kwaliteit van de afname van vingerafdrukken. Bij het verrichten van handenarbeid kunnen de richels die de vingerafdruk vormen snel afslijten, hetgeen afname onmogelijk maakt. Naast mechanische wrijving vormt ook de chemische inwerking van bepaalde stoffen een probleem. In het kader van identiteitsfraude is het denkbaar dat bewust gebruik gemaakt wordt van voorgaande technieken om de vingerafdruk te vervagen en controle onmogelijk te maken. Ook bepaalde verwondingen maken controle onmogelijk.

4 Omzeilen van de maatregel

Het digitaal beeld van de vingerafdrukken wordt opgeslagen in de chip van eID kaart. In deze sectie zullen we aantonen dat de chip op eenvoudige wijze onklaar gemaakt kan worden. Een eID zonder werkende chip is echter nog steeds een geldig identiteitsdocument. In de veronderstelling dat gelijkaardige technologie als in ePaspoorten gebruikt zal worden voor de eID, zal het digitaal beeld van de vingerafdrukken draadloos uitgelezen kunnen worden. Dit kan door het opslaan van het beeld van de vingerafdrukken in een contactloze chip naast de reeds bestaande chip in de eID of door één enkele chip met zowel een contact als contactloze interface. Afhankelijk van de situatie is het dus mogelijk om enkel de contactloze interface onklaar te maken, waardoor de burger nog steeds ten volle gebruik kan maken van de huidige functionaliteit die de eID biedt: namelijk inloggen op overheidswebsites en het digitaal ondertekenen van documenten.

Een zeer eenvoudige wijze om het gebruik van vingerafdrukken te verhinderen is het vernietigen van de chip. Dit kan eenvoudig door het toedienen van een elektromagnetisch puls aan de chip. Een primitieve variant hiervan is het kort plaatsen van de chipkaart in een microgolfoven. Een microgolfoven is eigenlijk te krachtig en er is dus een groter risico op bijkomende - zichtbare - schade aan de kaart. Door het correct doseren van de elektromagnetisch puls, wat eenvoudig kan door gebruik te maken van een spoel en één of meer condensatoren (Figuur 2



Figuur 1. Contactloze chipkaart met duidelijk zichtbare lussen van de antenne - Afbeelding genomen met Röntgenstraling. (Bron: https://hackaday.com/2014/08/23/disabling-tap-to-pay-debit-cards/)

en 3), kan de vernietiging volledig onzichtbaar gebeuren[5]. Er dient benadrukt te worden dat de vereiste kennis en infrastructuur hiervoor zeer minimaal is. De problematiek is reeds bekend van bij de contactloze chip van paspoorten, waar men reeds jaren doelbewust overgaat tot het vernietigen van de chip.

Omdat de vernietiging van de chip onzichtbaar is, kan de burger in kwestie bovendien steeds zijn onwetendheid staande houden. Te meer aangezien een burger slechts kennis kan nemen (of lijken te nemen) van het 'defect' indien bij een controle getracht wordt de chip uit te lezen. Een accidentele vernietiging of een vernietiging door derden kan uiteraard ook nooit uitgesloten worden.

Een andere manier om de contactloze interface uit te schakelen (doch niet te vernietigen) is het aanbrengen van een kleine inkeping in de kaart, zoals in Figuur 4. Op deze manier wordt de antenne van de chip onderbroken en is verdere communicatie met de chip onmogelijk. In dit geval kan de chip - mits het herstellen van de onderbreking in de antenne - wel terug uitgelezen worden.

5 Opslagwijze op de chip van de eID

5.1 Voorgenomen opslag

De wet legt op dat het "digitaal beeld" van de vingerafdrukken bewaard moet worden in de chip van de eID. Gelet op de woordkeuze wordt hiermee een digitale afbeelding (typisch in JPEG- of JPEG2000-formaat) van de vingerafdrukken bedoeld[6]. Hierdoor beschikt de terminal die de kaart uitleest over een 'letterlijke'

[5] Zie o.a. https://hackaday.com/2009/12/22/terminate-rfid-tags/ ;https://www.youtube.com/watch?v=U_TyoJJkQsY ; http://bgdevs.com/portfolio/?p=93

[6] International Civil Aviation Organization's (ICAO) Doc 9303

Figuur 2. Paspoort waarvan de chip vernield wordt met een elektromagnetische puls..

Figuur 3. Opstelling (met zichtbare componenten) voor het vernietigen van contactloze chips.

weergave van de vingerafdruk, zoals deze geregistreerd werd bij de aanvraag van de identiteitskaart.

5.2 Alternatieven

Er zijn uiteenlopende mechanismen in de literatuur beschreven om een letterlijke opslag van het digitaal beeld van de vingerafdrukken te vermijden. Het overzicht hieronder is een niet-limitatieve lijst van mogelijke alternatieven, die beter presteren op het vlak van databescherming.

Sensor-on-card Bij sensor-on-card is de eID zelf voorzien van een sensor voor het inlezen van de vingerafdrukken (Figuur 5). De terminal heeft dus geen vingerafdruklezer en komt zelfs niet meer in contact met deze biometrische gegevens. De kaart zal zelf een score geven aan de overeenkomst tussen de aangeboden

Figuur 4. Kaart met een inkeping ter hoogte van de antenne. (Bron: https://linuxcentre.net/disabling-contactless-cards)

vingerafdruk en de opgeslagen vingerafdruk of zelfs louter een ja/nee-antwoord. De terminal kan deze score dan uitlezen, uiteraard na verificatie dat het om een legitieme kaart gaat.

Figuur 5. Vingerafdruksensor op een kredietkaart. (Bron: Mastercard)

Match-on-card Bij match-on-card technieken wordt het uitlezen van vingerafdrukgegevens uit de eID ook overbodig gemaakt (Figuur 6). De terminal is in dit geval wel voorzien van een vingerafdruklezer, maar de identiteitskaart voert wel zelf de vergelijking uit van de vers uitgelezen vingerafdruk (of de hieruit geëxtraheerde gegevens) en de opgeslagen vingerafdruk. Het is evident dat deze werkwijze een enorme verbetering oplevert van de privacy aangezien het onmogelijk wordt gemaakt om de referentie-vingerafdruk te bekomen. Deze techniek wordt momenteel reeds gebruikt in de Spaanse eID[7].

Figuur 6. Illustratie van de werkwijze van een match-on-card systeem.

Templates Het gebruik van templates waarbij de biometrische gegevens (i.e. afbeelding) worden omgezet. Typisch worden hierbij de kenmerken van de vingerafdruk, zoals de positie en oriëntatie van de minutiae, geëxtraheerd en opgeslagen. Op deze wijze wordt het reconstrueren van de originele vingerafdruk op zijn minst bemoeilijkt zonder afbreuk te doen aan de mogelijkheden tot het vergelijken van de vingerafdruk. In casu worden de minutiae vergeleken in plaats van het volledige beeld van de vingerafdruk.

Template protection en fuzzy extractors Meer geavanceerde varianten van template protection maken gebruik van o.a. fuzzy hashing technieken om de minutiae nog eens extra te transformeren op een niet-inverteerbare wijze. Een alternatief is het gebruik van protocollen zoals BioPACEv2[8], waarbij een sleutel

[7] https://www.dnielectronico.es/PDFs/Guia_de_Referencia_DNIe_con_NFC.pdf

[8] N. Buchmann, R. Peeters, H. Baier, and A. Pashalidis, "Security Considerations on Extending PACE to a Biometric-Based Connection Establishment,"In Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Lecture Notes in Informatics (LNI), A. Brömme, and C. Busch (eds.), Bonner Köllen Verlag, pp. 15-26, 2013. https://www.esat.kuleuven.be/cosic/publications/article-2348.pdf

geëxtraheerd (met een fuzzy extractor) wordt uit de vingerafdruk die gebruikt wordt tijdens het opzetten van een beveiligde connectie met de identiteitskaart.

5.3 Conclusie

Door het opleggen in de wet van de registratie in de eID van het digitaal beeld, verhindert de wet het nemen van de gepaste technische maatregelen om een optimale bescherming te bekomen van de biometrische data. Bovendien stelt de wet dat het *digitaal beeld* uitgelezen kan worden door bepaalde personen en organisaties, hetgeen technieken zoals match-on-card en sensor-on-card onmogelijk maakt. Nochtans volstaat het dat de desbetreffende personen en organisaties in staat zijn om de opgeslagen vingerafdrukken te *vergelijken* met de vingerafdrukken van de houder van de kaart, hiervoor is het *uitlezen* niet noodzakelijk. Kaarten uitgerust met een sensor (sensor-on-card) bieden veel betere garanties op het vlak van gegevensbescherming, aangezien uitsluitend de kaart zelf in aanraking komt met de vingerafdrukken en er geen mogelijkheid is tot het uitlezen van de vingerafdrukken opgeslagen in de chip.

6 Aanmaken van de eID - centrale database

6.1 Stappen en voorgenomen procedure

Op basis van de wet, het huidige KB[9], de "Algemene Onderrichting betreffende de elektronische identiteitskaarten van Belg"[10] (verder "AO") en de memorie van toelichting komen we tot de volgende procedure voor het aanmaken van de eID:

1. De burger begeeft zich naar het gemeentebestuur voor de aanvraag van een identiteitskaart. Het KB spreekt nog steeds van een 'basisdocument' waarop de persoonsgegevens voor de aanmaak van de identiteitskaart op moeten aangebracht worden, waaronder het 'aanhechten' van de foto en het plaatsen van de handtekening. Uit de AO blijkt echter dat het basisdocument reeds volledig digitaal is en via de BELPIC-toepassing door de ambtenaar ingevuld wordt[11]. De AO spreekt vervolgens over het elektronisch verzenden van het basisdocument naar de producent van de identiteitskaarten, zonder verdere specificatie van hoe deze verzending gebeurt.

[9] Koninklijk besluit betreffende de identiteitskaarten, 25 maart 2003, tekstbijwerking tot 31-10-2018. http://www.ejustice.just.fgov.be/eli/besluit/2003/03/25/2003000227/justel

[10] http://www.ibz.rrn.fgov.be/fileadmin/user_upload/nl/kaarten/eid/onderrichtingen/AO-eID-25052018.pdf

[11] Het KB voorziet nu reeds de mogelijkheid dat de gemeente het basisdocument elektronisch aan de burger bezorgt, die dan zelf zijn gegevens kan aanvullen en een scan van een foto kan toevoegen. Het ingevulde basisdocument wordt dan elektronisch terugbezorgd aan de gemeente.

De vingerafdrukken zullen ook digitaal ingelezen worden. Het digitale beeld van de vingerafdrukken wordt vervolgens naar alle waarschijnlijkheid overgemaakt aan de centrale opslag die in de wet gesuggereerd wordt. De wijze waarop dit gebeurt is echter niet gespecificeerd, mogelijk gebeurt dit ook via BELPIC.

2. De kaartpersonalisator print de gegevens op de voor- en achterzijde van de blanco identiteitskaart. De kaartpersonalisator stuurt de kaart vervolgens naar de kaartinitialisator. Uit de AO blijkt dat ZETES in de praktijk zowel kaartpersonalisator als kaartinitialisator is[12].
3. De kaartinitialisator schrijft de gegevens (o.a. foto, beeld van de handtekening, naam, adres, digitale certificaten...) in de chip van de eID. De kaartinitialisator zal dus ook het digitale beeld van de vingerafdrukken uit de centrale opslag moeten halen en wegschrijven op de chip van de eID. De kaartinitialisator is volgens het KB ook verantwoordelijk voor het 'optekenen' van de gegevens in het centraal register van de identiteitskaarten, het opsturen van PIN- en activatiecodes aan de burger en het bezorgen van de eID aan de gemeente.
4. De burger ontvangt zijn eID via het gemeentebestuur, waarbij de kaart geactiveerd wordt.

Cruciale vraag is hoe het digitale beeld van de vingerafdrukken, zoals genomen door de vingerafdruklezer op het gemeentehuis, in de chip van de eID terechtkomt. Zoals reeds eerder gesteld is de wet onduidelijk over de hiervoor voorziene centrale opslag.

6.2 Risico's van een centrale opslag

Als we veronderstellen dat er ongeveer 9 miljoen identiteits- en vreemdelingenkaarten[13] in omloop zijn, die om de 10 jaar vernieuwd worden, dan impliceert dit dat er op elk moment, gemiddeld genomen, vingerafdrukken van 225.000 inwoners in de centrale opslag zitten. Hierbij gaan we ervan uit dat de maximale opslagtermijn van 3 maanden gehanteerd wordt, aangezien de wet niet voorziet in een verplichte verwijdering bij correcte aflevering van de kaart. Gezien de tijd voorzien voor productie van een identiteitskaart (ongeveer 3 weken) is een minimale opslag van 1 maand realistisch. In dit minimaal scenario gaat het nog steeds om 75.000 inwoners.

Een evident risico van een dergelijke opslag is function creep, waarbij de gegevens aangewend worden voor een ander doel dan oorspronkelijk voorzien (al dan

[12] Uit de AO: "Zodra ZETES CARDS de basisdocumenten elektronisch ontvangt, kan de productiecyclus van de elektronische identiteitskaarten beginnen. Naar aanleiding van een zeker aantal beveiligde uitwisselingen van gegevens tussen het Rijksregister en de producent van de kaarten (meer bepaald de toelating om de productie op te starten) en de uitwisseling van informatie tussen de producent van de kaarten, het Rijksregister en de certificatiedienst (genereren van de certificaten), wordt de kaart uiteindelijk geproduceerd."

[13] Volgens Statbel bedraagt de bevolking van 12 jaar en ouder van België ongeveer 9.825.508 personen.

niet door het aanpassen van de wetgeving). In het bijzonder valt hierbij te denken aan een gebruik door politie en gerecht in een forensische context. Door het herhaaldelijk bevragen van de centrale opslag, kan een match gevonden worden met de wijsvingers van een mogelijke verdachte. Aangezien identiteitskaarten om de 10 jaar vernieuwd worden en er op dat moment vingerafdrukken ter beschikking zijn in de databank, duurt het vinden van een overeenkomst gemiddeld 5 jaar.

Andere risico's zijn inherent aan alle IT-systemen, zoals het uitlekken van de gegevens (door technische kwetsbaarheden), misbruik van de gegevens door gemachtigde gebruikers, niet-toegelaten manipulatie van de gegevens... Omwille van de gevoeligheid van de opgeslagen vingerafdrukken en de grote schaal van de verwerking is de impact van een incident bijzonder groot. Bij een eenmalig incident kan 0,8-2,5% van de bevolking (12j+) getroffen worden, bij herhaling de volledige bevolking. Aangezien het niet mogelijk is biometrische gegevens te wijzigen is de impact levenslang, op de eventuele graduele verandering van de vingerafdrukken bij het verouderen na.

6.3 Analyse en alternatieven

De voorgestelde centrale opslag is vanuit technisch oogpunt volstrekt overbodig. In tegenstelling tot de foto van het gezicht, die ook afgedrukt wordt op de voorzijde van identiteitskaart, zijn de vingerafdrukken louter in de chip opgeslagen en dus niet afgedrukt. **Het is dus niet nodig dat deze op het moment van het personaliseren van de kaart beschikbaar zijn. Zowel het inlezen van de vingerafdrukken als het wegschrijven in de chip van het beeld van de vingerafdrukken kan dus gebeuren bij het uitreiken van de eID aan de burger.** Op die manier is er bovendien een absolute zekerheid dat de vingerafdrukken overeenstemmen met de persoon die de eID in ontvangst neemt. Bovendien wordt vermeden dat de burger – in geval van problemen bij het aanmaken van de identiteitskaart – meerdere malen zijn vingerafdrukken moet laten inlezen; het inlezen van de vingerafdrukken gebeurt immers pas helemaal op het einde van de procedure, als de kaart al gepersonaliseerd en deels geïnitialiseerd is.

De gemeentebesturen zijn voorzien van de nodige apparatuur om deze initialisatie uit te voeren. Bovendien is er fundamenteel geen verschil tussen het opladen van het beeld van de vingerafdrukken en bv. het doorvoeren van een adreswijziging, die nu reeds louter op de chip kan plaatsvinden. Ook certificaten (voor de digitale handtekening en authenticatie) kunnen louter op de chip vervangen worden. Aangezien het KB nu reeds voorziet in de mogelijkheid voor een burger om de volledige aanvraag (i.e. het invullen en opsturen van het basisdocument) elektronisch te doen, is het zelfs denkbaar dat de burger niet meer in persoon naar het gemeentebestuur moet komen voor de aanvraag van de identiteitskaart. De burger doet de volledige aanvraagprocedure op afstand en komt dan slechts één maal naar het gemeentebestuur, namelijk voor het afhalen van de nieuwe kaart. Bij het afhalen worden dan alle biometrische gegevens gecontroleerd en de vingerafdrukken geregistreerd in de kaart.

Daarnaast zijn er nog tal van andere alternatieven om de centrale opslag te vermijden of te beveiligen zodanig dat misbruik van de gegevens of aanwending buiten het voorziene doel vermeden wordt:

1. door gebruik te maken van publieke sleutel encryptie kan de centrale opslag beperkt worden tot een centrale opslag van versleutelde gegevens. Op deze manier zijn de opgeslagen gegevens onbruikbaar, behalve voor de bedoelde ontvanger van gegevens. Met behulp van de publieke sleutel wordt het beeld van de vingerafdrukken versleuteld vlak na het inlezen van de vingerafdrukken door het gemeentebestuur. De versleutelde gegevens worden dan overgemaakt aan de centrale opslag. De kaartinitialisator leest de centrale opslag uit en ontsleutelt de gegevens met behulp van de private sleutel, die vereist is om tot ontsleuteling over te gaan. Op deze wijze bekomt de kaartinitialisator terug het originele digitale beeld van de vingerafdrukken en kan hij overgaan tot het opladen van het digitale beeld in de chip van de eID. Aangezien uitsluitend de kaartinitialisator (of beter nog: uitsluitend de fysieke machine bij de kaartinitalisator die de kaarten initialiseert) beschikt over de private sleutel, zijn er sterke technische garanties dat de gegevens opgenomen in de centrale opslag onbruikbaar zijn voor andere partijen.
2. door gebruik te maken van symmetrische encryptie, waarbij de sleutel uitsluitend bij het gemeentebestuur wordt gehouden. De vingerafdrukken worden geëncrypteerd op de eID geplaatst, zelfs de producent heeft dus geen toegang tot de eigenlijke vingerafdrukken. Bij uitreiking/activatie eID wordt de decryptiesleutel mee op de kaart geplaatst zodat bij controle de vingerafdrukken wel leesbaar zijn.
3. bij gebruik van (beschermde) templates kunnen bovenstaande maatregelen ook toegepast worden. Door onmiddellijk in het gemeentehuis de (beschermde) template af te leiden kan misbruik ingeperkt worden. Niettegenstaande het voorgaande, biedt het louter gebruik maken van een (beschermde) template geen afdoende bescherming hiertegen en moet dit steeds gezien worden in combinatie met punt 1. of 2.
4. de wet specificeert niet wie er toegang heeft tot de centrale opslag. Minstens dienen er bepalingen toegevoegd te worden wie er enerzijds kan schrijven in de centrale opslag (i.e. gemeentebesturen en de bevoegde ambtenaren) en wie er kan lezen uit de centrale opslag (i.e. de kaartinitialisator). Daarnaast dienen er bepalingen opgenomen worden met betrekking tot de minimum veiligheidsmaatregelen voor de overdracht van gegevens van en naar deze centrale opslag.

6.4 Conclusie

Er is geen nood aan een centrale databank voor de tijdelijke opslag van vingerafdrukken, aangezien de vingerafdrukken perfect bij het afhalen van de eID bij op de chip geschreven kunnen worden door het gemeentebestuur. Gebruik maken van een centrale opslag introduceert bovendien onnodig grote risico's op misbruik van de biometrische data. Indien er toch met een centrale databank

gewerkt wordt dient men zich ervan te verzekeren dat de vingerafdrukken voldoende beschermd zijn tegen oneigenlijk gebruik (enig ander gebruik dan het doel waarvoor ze verzameld zijn). Hiervoor moet de wet op zijn minst de bepalingen opnemen met betrekking tot toegang tot en transfer van data van en naar deze centrale databank. Men kan deze bescherming ook technisch afdwingen door gebruik te maken van cryptografie zoals aangegeven in de voorgaande paragraaf. Bijkomstig kan men ook nog gebruik maken van (beschermde) templates.

7 Wijze van uitlezen van de opgeslagen data

De wet bevat een opsomming van personen en organisaties die een machtiging hebben om het digitaal beeld van de vingerafdrukken uit te lezen uit de chip van de eID.

In de memorie van toelichting wordt gesproken over het afschermen van de data met 'certificaten'. In wat volgt gaan we ervan uit dat hetzelfde proces wordt gevolgd voor het uitlezen van vingerafdrukken zoals dit vandaag het geval is voor ePaspoorten. Met name: Password Authenticated Connection Establishment (PACE), gevolgd door Extended Access Control (EAC) met terminalcertificaten. Beide protocollen worden gedefinieerd door de BSI in TR-03110[14].

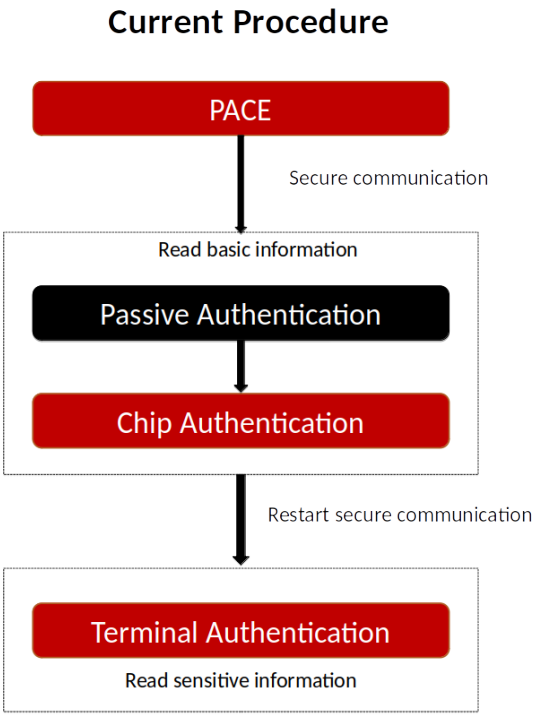
7.1 PACE protocol

Het PACE protocol vormt de eerste beschermingslaag om toegang te krijgen tot de gegevens opgeslagen op de chip van de eID. Het PACE protocol zet namelijk een veilig kanaal op tussen de chip op de eID en de terminal op basis van een wachtwoord. Het doel van het PACE protocol is te verzekeren dat een eID enkel draadloos kan uitgelezen worden door diegene die de eID ook daadwerkelijk in handen heeft, en dus toegang heeft (of in het verleden heeft gehad) tot wat er op de eID-kaart gedrukt staat, in casu het "wachtwoord". Dit paswoord is een subset van de Machine Readable Zone (MRZ), zoals afgedrukt op de achterzijde van de eID.

De entropie van de subset van de MRZ is eerder beperkt aangezien deze bestaat uit de geboortedatum, vervaldatum en nummer van de identiteitskaart. Voor ePaspoorten is dit in 2008 in detail bestudeerd[15]: indien men geen enkele vorm van bijkomende informatie heeft over het doel-ePassport (datgene men wil uitlezen), is de entropie, omwille van de redundantie van de informatie in de MRZ, slechts 40 bit. Indien men de geboortedatum weet (als men bijvoorbeeld heel doelgericht de vingerafdrukken van een bepaalde persoon wilt uitlezen), daalt dit tot 23 bit entropie. Een bijkomend nadeel van eIDs tov van ePaspoorten is dat iedere burger zijn eerste identiteitskaart ontvangt op zijn twaalfde

[14] https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html

[15] Avoine G., Kalach K., Quisquater JJ. (2008) ePassport: Securing International Contacts with Contactless Chips. In: Tsudik G. (eds) Financial Cryptography and Data Security. FC 2008. Lecture Notes in Computer Science, vol 5143. Springer, Berlin, Heidelberg https://doi.org/10.1007/978-3-540-85230-8_11



Figuur 7. Opeenvolging van cryptografische protocollen (PACE+EACv1) om toegang te krijgen tot biometrische data in paspoorten.

verjaardag en dat deze telkens vernieuwd wordt als de vorige vervallen is (behoudens wanneer de identiteitskaart in tussentijd verloren zou gaan en er een nieuwe moet aangevraagd worden). Hierdoor is er dus een heel sterke correlatie tussen de geboortedatum en de vervaldatum van de eID, waardoor het verwachte aantal bits entropie voor eIDs nog een stuk lager ligt.

Verder valt ook op te merken dat door behulp van visiesystemen de leeftijd van passanten tot op zekere hoogte kan bepaald worden en wanneer men dit op een slimme manier combineert met publieke informatie zoals men deze kan terugvinden op onder andere sociale medianetwerken, het niet zo moeilijk is om een verjaardag, al dan niet de exacte geboortedatum te achterhalen.

7.2 EAC - diefstal/misbruik van een geautoriseerde terminal

Het succesvol uitvoeren van PACE geeft enkel toegang tot de basisgegevens op de chip van de eID. Om toegang te krijgen tot gevoelige gegevens (o.a. vingerafdrukken) moet bijkomend EAC uitgevoerd worden.

Als onderdeel van EAC wordt Terminal Authentication (TA) uitgevoerd. Hierbij controleert de identiteitskaart dat de terminal (i.e. de kaartlezer, bijhorende systemen en software) beschikt over een certificaat, direct of indirect

Figuur 8. Schets van het verloop van EAC Terminal Authentication.

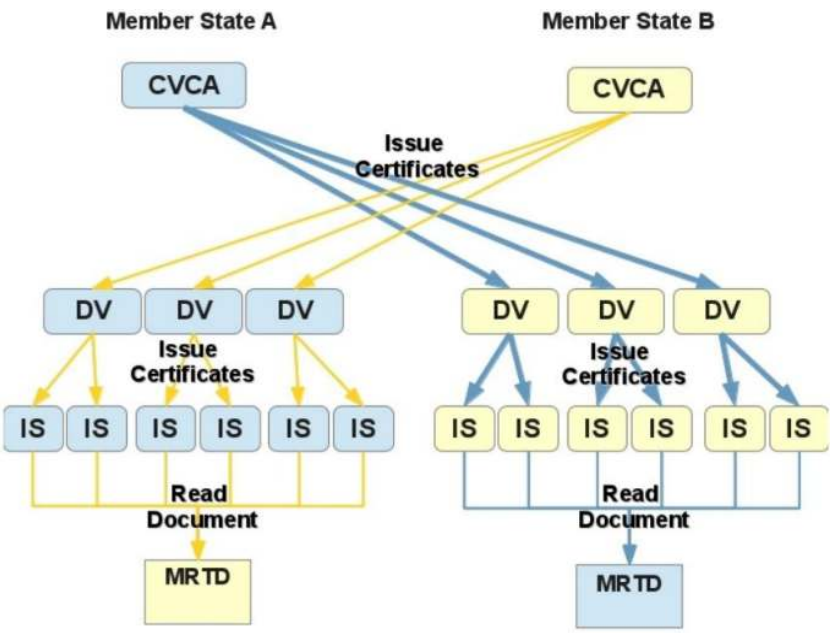
afgeleverd door de Belgische overheid, dat toelating geeft om de biometrische data uit te lezen (Figuur 8). Voor het uitvoeren van Terminal Authentication is het noodzakelijk dat de terminal ("Foreign Inspection System" beschikt over een certificaat dat afgeleverd is door België ("Belgian CVCA Root"). Met behulp van dit certificaat kan de terminal bewijzen aan de eID dat deze gemachtigd is door de Belgische overheid om toegang te krijgen tot de gevoelige biometrische data op de chip van de eID.

Het afleveren van certificaten is een complexe operatie, waarbij één of meerdere tussenlagen voorzien zijn, zoals getoond in Figuur 9. Een land zal nooit rechtstreeks certificaten afleveren voor terminals (IS - Inspection System), maar voor een tussenliggende laag van Document Verifiers (DV). Gezien de opsomming van gemachtigde personen zullen op zeer ruime schaal certificaten afgeleverd moeten worden voor terminals. Dit creëert een enorme proliferatie van dergelijke certificaten, hetgeen het risico op diefstal (o.a. via hacking) reëel maakt. Bovendien zullen eveneens certificaten afgeleverd worden aan buitenlandse instanties voor grenscontroles, wat vragen oproept over de controle die de overheid nog zal hebben hierover.

Het is aan de identiteitskaart om te bepalen of een terminalcertificaat geldig is of niet. De chip op de eID heeft echter geen idee of het terminalcertificaat mogelijk gestolen is aangezien er geen mechanisme voorzien is om een certificaat in te trekken ("revocatie")[16]. Om dit revocatieprobleem op te vangen voorzien de meeste opstellingen in terminalcertificaten met een zeer beperkte levensduur, typisch 3 dagen. Een cruciaal probleem is het gebrek aan een accurate tijdsbron op de identiteitskaart.

De chip beschikt slecht over een zeer rudimentaire tijdsreferentie, in vele gevallen is dat de datum van initialisatie van de chip. In theorie is het mogelijk

[16] FIDELITY D9.2, "Prototype of a secure certificate management architecture", Restricted document, available upon request.



Figuur 9. Architectuur van de EAC certificaten.

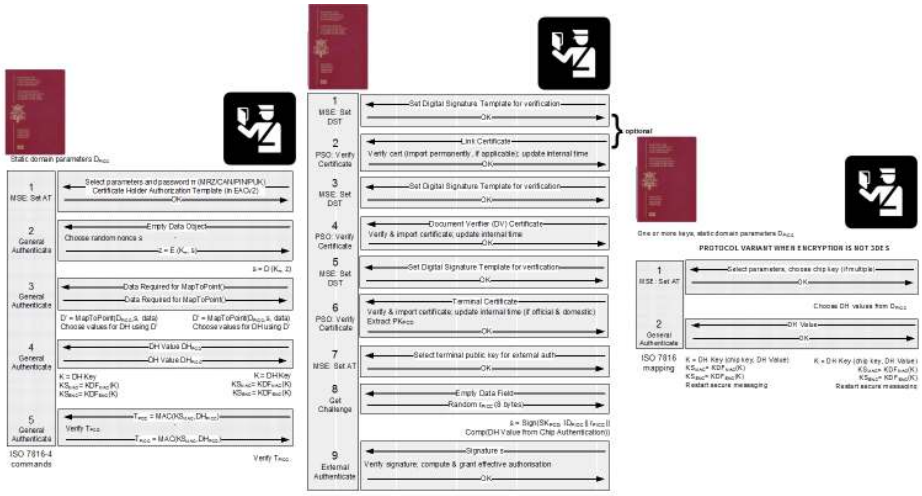
dat deze tijdsreferentie in de chip later nog bijgewerkt wordt, namelijk op het moment van een eventuele controle door een terminal die geauthenticeerd is hiervoor[17]. Er zijn bovendien geen indicaties van een werkelijke implementatie hiervan. Dit maakt dat men met een terminal, zelfs indien deze gerapporteerd is als gestolen/gecompromitteerd, nog jaren vingerafdrukken van eIDs kan uitlezen. Slechts één certificaat dat in verkeerde handen valt is voldoende om toegang te geven tot de biometrische data in alle identiteitskaarten, zonder mogelijkheid om het certificaat te deactiveren.

Een bijkomend probleem is dat de opeenvolging van de verschillende protocollen bijzonder complex is, zoals Figuur 10 treffend illustreert. Dit leidt tot een aanzienlijk risico op implementatiefouten, waarbij de werkelijke uitvoering niet overeenstemt met de technische specificatie.

Reeds in de periode 2012-2015 zijn er in het kader van het EU-onderzoeksproject FIDELITY[18] zeer kritische analyses gemaakt over de gehele paspoorttechnologie, o.a. het gebrek aan een functioneel revocatie(controle)mechanisme en de

[17] In de praktijk zou dit enkel door Belgische terminals kunnen gebeuren. Vaak overschrijdt men de Schengen-grenzen echter buiten België, waar uiteraard geen Belgische terminals aan te pas komen en er dus ook geen aanpassing van de tijdsreferentie van de chip kan gebeuren.

[18] http://www.fidelity-project.eu/, zie o.a.
– J. Hermans, A. Abidin, N. Buchmann, and R. Peeters, ëPassport Protocols and Certificate Architecture,"In European Conference on ePassports (FIDELITY



Figuur 10. Detail van de opeenvolging van PACE en EAC voor toegang tot biometrische data.

behandeling van biometrische gegevens. Ondanks de vele voorstellen tot verbetering zijn alle aanbevelingen uit het FIDELITY-project op dit vlak genegeerd en niet in de praktijk gebracht.

7.3 Impact van de kwetsbaarheden

Met behulp van het certificaat uit een gestolen/misbruikte terminal kan men het digitale beeld van de vingerafdrukken uit de chip van eIDs uitlezen. Het enige resterende veiligheidsmechanisme, PACE, kan immers eenvoudig uitgevoerd worden als er toegang is tot de MRZ, zoals afgeprint op de achterzijde van de eID.

Aangezien de chips draadloos werken en het feit dat het gebruikte paswoord in het PACE protocol (te) weinig entropie bevat is het daarenboven mogelijk om op veel grotere schaal en grotendeels ongemerkt de vingerafdrukken uit te lezen zonder toegang tot de MRZ.

event), 8 pages, 2015. https://www.esat.kuleuven.be/cosic/publications/article-2596.pdf

– FIDELITY D18.3, "Recommendations towards stakeholders.", Restricted document, available upon request.

8 Conclusies en aanbevelingen

Op basis van onze analyse komen we tot de conclusie dat:

1. de wet onduidelijk is, geen technische beschermingsmaatregelen oplegt, en sommige bepalingen in de wet bovendien adequate technische beschermingsmaatregelen verhinderen.
2. een betere inzet van de reeds beschikbare biometrische informatie op de eID, i.e. de foto van het gezicht van de burger, ook al tot een terugdringing van identiteitsfraude zal leiden.
3. het invoeren van de vingerafdrukken op de eID niet effectief is voor het terugdringen van identiteitsfraude, gelet op de eenvoudige manieren om de maatregel te omzeilen door de chip te vernietigen.
4. het toelaten van het uitlezen van het beeld van de vingerafdrukken uit de eID overbodig en disproportioneel is aangezien met sensor-on-card (o.a. gebruikt door Mastercard) of match-on-card (o.a. gebruikt in de Spaanse eID) het beoogde doel ook bereikt kan worden.
5. de (tijdelijke) centrale opslag van de vingerafdrukken voor de aanmaak van de eID overbodig is en daarenboven bijzonder risicovol.

Op basis van de technologie voor het opnemen van de vingerafdrukken in Belgische ePaspoorten komen we tot de conclusie dat:

6. de paspoorttechnologie (EAC) gedateerd is en niet meer voldoet aan de huidige stand van de techniek. De technologie zoals momenteel gebruikt biedt onvoldoende garanties om het uitlezen van de vingerafdrukken door onbevoegden te verhinderen.

Gelet op de bovenstaande problemen en de risico's, adviseren we:

1. De vingerafdrukken vooralsnog niet op te nemen op de eID, en eerst na te gaan of de specifieke types van identiteitsfraude en de schaal hiervan wel bijkomende maatregelen verantwoorden.
2. Een grondige evaluatie uitvoeren of de bestaande gegevens – de foto van het gezicht van de houder – niet beter gebruikt kunnen worden en of er alternatieven zijn voor het gebruik van vingerafdrukken.
3. Indien alsnog zou blijken dat vingerafdrukken noodzakelijk zijn, gebruik te maken van sensor-on-card technologie, zodat uitsluitend de kaart in aanraking komt met de vingerafdrukken, zonder enige (tijdelijke) centrale opslag en zonder interventie van de terminal.
4. In ondergeschikte orde, gebruik maken van match-on-card technologie, zonder (tijdelijke) centrale opslag en zonder de mogelijkheid om het beeld van de vingerafdrukken uit te lezen uit de chip van de eID.