KONINKRIJK BELGIË
Federale Overheidsdienst
Buitenlandse Zaken,
Buitenlandse Handel en
Ontwikkelingssamenwerking

Politie

ibz Federale Overheidsdienst
Binnenlandse Zaken

Aanbevelingen van de taskforce met betrekking tot de nieuwe initiatieven van gemeenten om de dienstverlening aan de burger te verbeteren

Inhoudsopgave

Inleiding **2**

1. Context **3**

2. Type projecten **3**

2.1. Selfservicekiosk **3**

2.1.1. Aanvragen verplicht in te dienen aan het loket 4

2.1.2. Identificatie van de aanvrager 4

2.1.3. Software en hardware van de kiosk 5

2.1.4. Verantwoordelijkheden van de gemeentebesturen 5

2.2. Levering aan huis **6**

2.2.1. Contractuele aansprakelijkheid 6

2.2.2. Betrokken documenten 7

2.2.3. Bescherming van de persoonsgegevens 7

2.2.4. Traceerbaarheid en status van de paspoorten 8

2.2.5. Identificatie van de bestemmeling 10

2.2.6. Afzonderlijke sealbag voor de paspoorten bestemd voor een levering aan huis? 11

2.3. Automaat **11**

2.3.1. Veiligheidsrisico's 11

2.3.2. Identificatie van de aanvrager 11

2.3.3. Procedurele verplichtingen 12

2.4. Mobiele kit **12**

3. Conclusies **13**

Inleiding

<u>Bevoegde overheden</u>: FOD Binnenlandse Zaken, FOD Buitenlandse Zaken, Dienst Vreemdelingenzaken.

<u>Bestemmelingen</u> : de gemeenten in België.

<u>Betrokken documenten</u> : gewone paspoorten, reisdocumenten voor vluchtelingen, staatlozen of vreemdelingen, identiteitskaarten en verblijfstitels.

<u>Rechthebbenden</u> : burgers die een aanvraag voor de voornoemde documenten indienen bij een gemeente.

<u>Reglementaire basis</u> :

- Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit.
- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (= AVG-regelgeving).
- Verordening (EU) 2025/1208 van het Europees Parlement en de Raad van 12 juni 2025 betreffende de versterking van de beveiliging van identiteitskaarten van burgers van de Unie en van verblijfsdocumenten afgegeven aan burgers van de Unie en hun familieleden die hun recht van vrij verkeer uitoefenen.
- Wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen.
- Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, artikel 8 (BS 21-04-1984).
- Wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten (BS 03-09-1991).
- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS 05-09-2018).
- Consulair Wetboek van 21 december 2013, hoofdstuk 10 "De paspoorten" (BS 21-01-2014).
- Wet van 10 februari 2015 met betrekking tot geautomatiseerde verwerkingen van persoonsgegevens die noodzakelijk zijn voor de Belgische paspoorten en reisdocumenten (BS 02-03-2015).
- Koninklijk besluit van 8 oktober 1981 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen.
- Koninklijk besluit van 25 maart 2003 betreffende de identiteitskaarten (BS 28-03-2003).
- Kadernota Integrale Veiligheid 2026-2029 – punt 9.6. van deel IV.

1. Context

De Kadernota Integrale Veiligheid 2026-2029 (punt 9.6. van deel IV) benadrukt, opnieuw, dat de bestrijding van identiteitsfraude een prioriteit blijft voor de federale overheden. In de kadernota wordt gevraagd de beveiliging van de afgifteprocedures voort te zetten door middel van, onder andere, versterkte regelgevingsaspecten betreffende de preventie en bestrijding van fraude, versterkte veiligheidsaspecten in gemeenten, enz.

Anderzijds vragen verschillende gemeenten de FOD's Binnenlandse Zaken en Buitenlandse Zaken al enkele jaren om advies over innovatieprojecten inzake aanvraag en afgifte van identiteits-, reis- en verblijfsdocumenten: "self enrollment" kiosk, levering aan huis, automaat voor documenten, mobiele kit, enz.

De initiatieven die de lokale overheden momenteel ontwikkelen met het oog op een betere dienstverlening aan de burger, maken de procedures voor de afgifte van deze documenten complexer en soms fraudegevoeliger. Vandaag worden al deze procedures immers aangestuurd door mensen, namelijk door gemachtigde ambtenaren.

Het doel van dit document is om gemeenten te voorzien van richtlijnen en minimale instructies met betrekking tot die innovatieprojecten. De Taskforce Identiteitsfraude wil ervoor zorgen dat dergelijke initiatieven de veiligheid van de processen voor het aanvragen en afgeven van documenten niet ondermijnen, zoals in de Kadernota Integrale Veiligheid 2026-2029 gevraagd wordt.

Aangezien de gemeenten waarvan sprake voor het uitvoeren van deze projecten bovendien vaak overeenkomsten sluiten met privébedrijven die niet door de FOD's Binnenlandse Zaken en Buitenlandse Zaken zijn erkend, wil de taskforce de respectievelijke verantwoordelijkheden van de voornoemde FOD's en van de gemeenten die een dergelijke overeenkomst sluiten, duidelijk vastleggen.
Om het lezen te vergemakkelijken, is elke richtlijn makkelijk terug te vinden aan de hand van dit pictogram:

2. Type projecten

2.1. Selfservicekiosk

Sommige gemeenten willen in hun gebouwen selfservicekiosken installeren, zodat de burger zijn documentaanvraag kan registreren zonder langs te moeten gaan bij het loket.

2.1.1. Aanvragen verplicht in te dienen aan het loket

Om de risico's te beperken, kunnen niet alle aanvragen worden ingediend via een selfservicekiosk.

De volgende aanvragen zullen steeds moeten worden ingediend aan het loket onder toezicht van een gemachtigd ambtenaar:

- Alle eerste aanvragen van een document (geautomatiseerde controle);
- Alle aanvragen ten gevolge van verlies, diefstal of vernietiging van een document (geautomatiseerde controle);
- Alle aanvragen ingediend via een dringende of zeer dringende procedure;
- Alle aanvragen die niet met de kiosk kunnen worden voltooid: probleem met gezichtsherkenning, handtekening, vingerafdrukken, enz.;
- Alle aanvragen van buitenlandse onderdanen voor wie de vernieuwing van de verblijfstitel onderworpen is aan het voorleggen van aanvullende of nieuwe bewijzen, zoals een verklaring van tewerkstelling;
- Alle aanvragen van reisdocumenten voor vluchtelingen, staatlozen of vreemdelingen;
- Alle aanvragen van diplomatieke of dienstpaspoorten[1] ;
- Alle aanvragen van ambtshalve afgevoerde personen en van personen die in het buitenland verblijven (geautomatiseerde controle);
- Alle aanvragen van minderjarige personen en van personen die onder gerechtelijke bescherming zijn geplaatst (geautomatiseerde controle);
- Alle aanvragen van personen die geseind werden door de politionele, gerechtelijke of veiligheidsautoriteiten en die hetzij in Passban, hetzij in eIDban zijn opgenomen (geautomatiseerde controle).

2.1.2. Identificatie van de aanvrager

Het is absoluut noodzakelijk dat de aanvrager die zijn aanvraag indient via de kiosk, op ondubbelzinnige wijze wordt geïdentificeerd. Daartoe voert hij zijn identiteitskaart en pincode in de kiosk in.

Het systeem moet een gezichtsherkenningsmodule bevatten[2] om de foto die door de kiosk wordt genomen, te vergelijken met de foto's van vroegere documenten, of een module voor de vergelijking van vingerafdrukken[3] erkend door de betrokken FOD's. Het gebruik van zo'n module

[1] De gemeenten zijn niet bevoegd om de aanvragen van diplomatieke of dienstpaspoorten te registreren. De FOD Buitenlandse Zaken kan hen evenwel uitzonderlijk vragen om als vooruitgeschoven loket op te treden om de biometrische gegevens van de aanvragers van deze paspoorten te registreren. Dat kan enkel na het voorafgaand akkoord van de FOD Buitenlandse Zaken en aan het loket van de gemeente.
[2] Vergelijking met de databanken van de vroegere foto's (paspoorten, eID en verblijfstitels).
[3] Eén-op-één vergelijking van de vingerafdrukken op de chip van het document.

moet wettelijk omkaderd zijn en moet een kwaliteitsvol resultaat garanderen. Gelet op de beoogde verwerkingen (gezichtsherkenning en/of vergelijking van vingerafdrukken), gecombineerd met het feit dat de verwerking betrekking zal hebben op een groot aantal individuen, is een DPIA (data protection impact assessment) noodzakelijk

2.1.3. Software en hardware van de kiosk

De voor de kiosk gebruikte software zal door de bevoegde federale overheden erkend moeten worden teneinde:

- de verschillende aanvraag- en afgifteprocessen van de documenten te uniformeren;
- de toegangen tot de federale databanken met de persoonlijke identificatiegegevens te beveiligen;
- de bescherming van de persoonsgegevens te garanderen;
- externe aanvallen op de informaticasystemen van de federale overheden te voorkomen;
- de beschikbaarheid en de levensvatbaarheid van de informaticasystemen te verzekeren;
- de interoperabiliteit van de systemen die in de verschillende gemeenten worden opgezet, te garanderen;
- de conformiteit van het systeem en de procedures met de Europese eIDAS-Verordening te verzekeren, zodat de Belgische Staat zijn kwalificatie als verlener van vertrouwensdiensten niet verliest.

De hardware van de kiosk zal door de bevoegde federale overheden erkend moeten worden teneinde:

- de kwaliteit en de veiligheid van de gebruikte systemen te garanderen;
- de interoperabiliteit van de systemen die in de verschillende gemeenten worden opgezet, te verzekeren;
- externe aanvallen op de informaticasystemen van de federale overheden te voorkomen;
- een eenvormige configuratie van de hardware in alle gemeenten te garanderen.

2.1.4. Verantwoordelijkheden van de gemeentebesturen

De selfservicekiosken kunnen enkel worden gebruikt in het lokaal waar de kiosken geïnstalleerd zijn en in de fysieke aanwezigheid van een gemeenteambtenaar die gemachtigd is voor het aanvragen en afgeven van identiteits-, reis- en verblijfsdocumenten. Hij moet kunnen optreden wanneer de burger problemen ondervindt bij de registratie van zijn aanvraag aan de kiosk.

De activering van de identiteits- en verblijfsdocumenten moet altijd aan het fysieke loket gebeuren. Paspoorten zullen onder bepaalde omstandigheden zonder menselijke tussenkomst kunnen worden afgegeven (zie hoofdstuk 2.3. Automaat).

De gemeente beschrijft de technische en organisatorische maatregelen om aan de AVG-vereisten te voldoen en om de rechten van de betrokken personen te garanderen, en voert een DPIA (data protection impact assessment) uit.

De gemeente wijst een technisch verantwoordelijke voor de kiosken aan en deelt deze informatie mee aan de FOD Binnenlandse Zaken. In geval van een vermoeden van identiteitsfraude is de gemeentelijke SPOC identiteitsfraude het contactpunt voor de bevoegde FOD's.

2.2. Levering aan huis

Sommige gemeenten willen de identiteits-, reis- en verblijfsdocumenten thuis bij de burger afleveren via een privébedrijf. Andere doen dat reeds voor de paspoorten.

Tot deze initiatieven ontstonden, strekte de centralisatie van de afgifte van identiteits-, reis- en verblijfsdocumenten ertoe het risico op diefstal van de documenten in de gemeenten te verminderen. Het kan niet de bedoeling zijn dat het fenomeen opnieuw opduikt door minder beveiligde afgiftemethoden in te voeren.

De overeenkomst die de gemeente en het privébedrijf sluiten, moet dus de integriteit van de identiteitsketen, waarbij de afgifte van het document slechts de laatste schakel is, waarborgen.

2.2.1. Contractuele aansprakelijkheid

De FOD's Binnenlandse Zaken en Buitenlandse Zaken hebben geen enkele wettelijke of contractuele relatie met een door de gemeente aangewezen koerierbedrijf en kunnen dit bedrijf dus niet aansprakelijk stellen bij problemen (diefstal, verlies, schade, misbruik van persoonsgegevens, ...). Onze FOD's zijn met andere woorden enkel aansprakelijk voor de identiteits-, reis- en verblijfsdocumenten tot het moment van de levering ervan door het productiebedrijf aan de gemeente. In geval van een overeenkomst tussen de gemeente en een verwerker moet worden verwezen naar artikel 28 van de Algemene Verordening Gegevensbescherming (AVG).

Voor het traject tussen de gemeente en de burger is alleen de gemeente aansprakelijk. De gemeenten moeten deze aansprakelijkheid dus zelf met het koerierbedrijf regelen, want tussen hen bestaat er wel degelijk een wettelijke en contractuele relatie. De FOD's Binnenlandse Zaken en Buitenlandse Zaken raden de gemeenten dus aan om in de overeenkomst met het bedrijf de noodzakelijke bepalingen op te nemen voor het vergoeden van iedere schade die zou voortvloeien uit de thuislevering (diefstal, verlies, schade, misbruik van persoonsgegevens, ...). Bovendien moeten in de overeenkomst de voorwaarden voor de machtiging van het personeel dat belast is met de verwerking van de paspoorten

worden vastgelegd. Iedere vorm van onderaanneming door het privébedrijf waarmee de gemeente een overeenkomst heeft gesloten, is verboden.

Om die redenen zouden bepaalde informatiegegevens te gelegener tijd moeten worden overgezonden naar de betrokken FOD (Buitenlandse Zaken; zie 2.2.2. hierna), zoals de naam van het bedrijf waarmee een overeenkomst werd gesloten, de maatschappelijke zetel en de contactgegevens ervan, de datum waarop de overeenkomst zou ingaan en de vervaldatum van de overeenkomst. Deze informatiegegevens kunnen worden overgezonden naar de Directie C2 Reis- en identiteitsdocumenten van de FOD Buitenlandse Zaken: paspoort@diplobel.fed.be

2.2.2. Betrokken documenten

De afgifte van **identiteits- en verblijfsdocumenten** houdt een matching van de vingerafdrukken van de houder in, alsook de eventuele activering van de certificaten op de documenten. Deze handelingen mogen in geen geval worden uitgevoerd door een privébedrijf. Ze moeten worden uitgevoerd door een gemachtigd gemeenteambtenaar.

Een levering aan huis kan dan ook niet worden overwogen voor deze documenten (behalve voor bepaalde specifieke situaties via biometrische stations).

Aangezien de matching van vingerafdrukken en de activering van certificaten daarentegen nog niet van toepassing zijn voor **de paspoorten en reisdocumenten**, zou de gemeente een overeenkomst voor thuislevering kunnen sluiten met een privébedrijf onder de voorwaarden die in de volgende hoofdstukken worden opgesomd.

Levering aan huis zal echter niet mogelijk zijn:

- indien het vorige paspoort bij de aanvraag van het nieuwe paspoort niet werd teruggegeven aan en geannuleerd bij de gemeente;
- indien de FOD Buitenlandse Zaken u, zelfs na de indiening van de aanvraag, laat weten dat het paspoort niet zonder zijn voorafgaand akkoord zal mogen worden afgegeven (vermoeden van fraude). In dat geval moet de aanvrager zich melden bij de gemeente.

2.2.3. Bescherming van de persoonsgegevens

Bij het sluiten van een overeenkomst voor thuislevering moet de gemeente zich houden aan een bepaald aantal juridische en praktische voorwaarden betreffende de verwerking van persoonsgegevens:

- **Gevoelige persoonsgegevens op de chip van het paspoort:**

  De chip van het paspoort bevat een bepaald aantal persoonsgegevens van de houder:
  - de persoonsgegevens;
  - de biometrische kenmerken (foto, vingerafdrukken).

In tegenstelling tot de vingerafdrukken zijn de persoonsgegevens en de foto niet beschermd tegen niet-toegestane uitlezing en opslag. Het koerierbedrijf zou dus een paspoortlezer en bijhorende software (beschikbaar in de handel) kunnen gebruiken om de persoonsgegevens en de foto uit te lezen of te bewaren, of in het slechtste geval, er misbruik van te maken.

De taskforce raadt dus aan dat de gemeenten de nodige maatregelen treffen om te verhinderen dat het bedrijf rechtstreeks toegang kan krijgen tot de chip van de paspoorten die het vervoert. Dat kan bijvoorbeeld door de paspoorten in een verzegelde enveloppe, ongeopend door het bedrijf, af te leveren aan de aanvrager.

- **Gebruik van persoonsgegevens voor de afgifte van het paspoort:**

Teneinde het paspoort aan de aanvrager te kunnen bezorgen, zal het koerierbedrijf in alle gevallen een minimum aan persoonsgegevens moeten verwerken en gebruiken. De taskforce herinnert u eraan dat iedere verwerking van persoonsgegevens onderhevig is aan de bepalingen van de AVG-regelgeving en van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (zie artikel 2 voor de definitie van "verwerking van persoonsgegevens").

De taskforce herinnert de gemeenten aan het evenredigheidsbeginsel van de gegevensverwerking met betrekking tot het nagestreefde doeleinde en raadt de gemeenten dus aan:

- om de persoonsgegevens die ter beschikking worden gesteld van het privébedrijf (naam, voornaam, adres, telefoonnummer, e-mail, ...), zoveel mogelijk te beperken,
- om het gebruik van het rijksregisternummer te vermijden,
- en om het bedrijf te beletten de gegevens langer te bewaren dan strikt noodzakelijk is om het paspoort aan de bestemmeling te bezorgen.

Aangezien de gemeente de verwerkingsverantwoordelijke van de persoonsgegevens is die zij eventueel ter beschikking zou stellen van het privébedrijf, zal zij in de overeenkomst met dit bedrijf een AVG-clausule moeten opnemen waarin de gegevens die mogen worden gebruikt en de nadere regels voor dit gebruik, nauwkeurig worden omschreven.

2.2.4. Traceerbaarheid en status van de paspoorten

Een authentiek biometrisch paspoort is een zeer gegeerd product en, als het in verkeerde handen valt, is misbruik niet uitgesloten. Dat is de reden waarom de bewegingen van het paspoort steeds moeten worden getraceerd (inclusief op de route tussen de gemeente en de aanvrager) en waarom de status van het paspoort altijd up-to-date moet zijn en moet overeenstemmen met de realiteit.

Bijgevolg moeten de volgende voorwaarden worden nageleefd:

- **Traceerbaarheid op de route gemeente-aanvrager:**

Om de risico's op diefstal, verlies of misbruik van een authentiek paspoort te minimaliseren, is een perfecte traceerbaarheid van het paspoort verplicht. De traceerbaarheid wordt gegarandeerd door de bepalingen van de overeenkomst met de fabrikant van het paspoort tot het paspoort aan de gemeente wordt geleverd. De fabrikant werd al verschillende keren gecontroleerd op vlak van veiligheid en traceerbaarheid en heeft, wanneer dat nodig geacht werd, zijn procedures moeten aanpassen.

Geen enkele van de door de gemeente georganiseerde leveringen aan huis valt onder de bepalingen van de overeenkomst "paspoorten" tussen de FOD Buitenlandse Zaken en de fabrikant van de paspoorten en moet dus in de overeenkomst tussen de gemeenten en het koerierbedrijf worden geregeld. Die overeenkomst moet de **bepalingen bevatten die noodzakelijk zijn om de traceerbaarheid te garanderen** (bijvoorbeeld via een "track & trace"-systeem). Het kan tevens erg nuttig zijn om een voorafgaande audit uit te voeren bij het koerierbedrijf met betrekking tot de maatregelen die zij zullen nemen voor de veiligheid en de traceerbaarheid.

- **Aanpassing van de status van het paspoort:**

Het is zeer belangrijk dat de status van het paspoort altijd up-to-date is en overeenstemt met de realiteit teneinde misbruik te voorkomen (zelfs oude vervallen paspoorten kunnen nog op frauduleuze wijze worden gebruikt). Bovendien geeft de ***wet van 10-02-2015 met betrekking tot geautomatiseerde verwerkingen van persoonsgegevens die noodzakelijk zijn voor de Belgische paspoorten en reisdocumenten*** een ander bedrijf dan de fabrikant van het paspoort geen toelating om toegang te hebben tot de databank van de paspoorten, waarin de status van de paspoorten wordt geregistreerd en bijgewerkt.

Bijgevolg moet de gemeente er zelf voor zorgen dat de status van het paspoort (bv. "afgegeven", "vernietigd", "geannuleerd") correct wordt aangepast. **Dit mag niet worden toevertrouwd aan het privébedrijf**.

- **Terugnemen & annuleren/vernietigen van het vorige paspoort:**

Aangezien er ook misbruik kan worden gemaakt van oude vervallen paspoorten (bijvoorbeeld niet-toegestaan gebruik van gegevens op de chip, gebruik van lege visumpagina's om een vals paspoort te maken, ...), is het belangrijk dat deze fysiek worden teruggenomen en vervolgens worden geannuleerd of vernietigd **door de gemeente zelf**, niet door het koerierbedrijf..

2.2.5. Identificatie van de bestemmeling

Bij de afgifte van een paspoort aan het loket van de gemeente kan de gemeenteambtenaar zich ervan vergewissen dat de persoon die het paspoort ontvangt, wel degelijk de aanvrager is. Zelfs in geval van afhaling door een derde die gemandateerd is door de aanvrager, kunnen aan het loket de nodige controles plaatsvinden (volmachtformulier, identiteitskaart van de derde, ...).

Dat is minder evident in het kader van een thuislevering door een koerierbedrijf. Om te voorkomen dat het paspoort in verkeerde handen terechtkomt, moeten de volgende zaken in acht worden genomen:

- **Uitwerking van een coherente afgifteprocedure:**

  Het paspoort mag enkel worden afgegeven aan de **aanvrager zelf** (verificatie van zijn identiteit op basis van zijn identiteitskaart). Indien het gaat om een paspoort **van een minderjarige**, wordt u gevraagd dezelfde procedure te volgen als aan het loket, dit wil zeggen het paspoort overhandigen aan één van beide ouders overeenkomstig de regels op het ouderlijke gezag.

  In het geval dat de aanvrager op het moment van de thuislevering niet aanwezig zou zijn, mag het pakket **in geen geval** afgeleverd worden, maar moet het weer meegenomen worden door het koerierbedrijf. In afwachting van een eventuele tweede levering moet het paspoort bewaard worden op een beveiligde plaats die enkel toegankelijk is voor het gemachtigde personeel van hetzij de gemeente, hetzij het privébedrijf (zie punt 2.2.1. supra).

Het is aan te raden **al deze afgifteprocedures op te nemen in de overeenkomst met het koerierbedrijf**. Het kan tevens erg nuttig zijn om een voorafgaande audit uit te voeren bij het koerierbedrijf met betrekking tot de maatregelen die zij zullen nemen voor de veiligheid en de traceerbaarheid.

- **Eventuele invoering van een controle van de vingerafdrukken als identiteitscontrole:**

  Het is niet uitgesloten dat in de toekomst een vergelijking (*matching*) wordt ingevoerd van de vingerafdrukken van de aanvrager (= bestemmeling van de levering) met deze op de chip van het afgegeven paspoort. Dat kan nuttig zijn als kwaliteitscontrole enerzijds en in de context van de bestrijding van identiteitsfraude anderzijds. Een dergelijke *matching* zal waarschijnlijk niet systematisch worden opgelegd, maar gericht worden uitgevoerd in geval van twijfel.

  Deze controle is een **exclusieve bevoegdheid van de uitvoerende macht** (= de openbare overheden) en niet van een privébedrijf. Bovendien bestaan er juridische en technische bezwaren tegen het uitlezen van vingerafdrukken door een privébedrijf (misbruik van gevoelige biometrische gegevens, de paspoortlezers moeten individueel gecertificeerd zijn door de centrale overheid om vingerafdrukken te mogen uitlezen, enz.).

Het is in ieder geval aan te bevelen om bij de minste twijfel over de identiteit van de bestemmeling van het paspoort, een afhaling aan het loket te vragen!

2.2.6. Afzonderlijke sealbag voor de paspoorten bestemd voor een levering aan huis?

De fabrikant van de paspoorten zou de paspoorten bestemd voor thuislevering eventueel in een afzonderlijke sealbag aan de gemeente kunnen leveren. Hiervoor zullen dan wel bijkomende kosten worden aangerekend, kosten die niet gedekt worden door de overeenkomst "paspoorten" tussen de FOD Buitenlandse Zaken en de fabrikant van de paspoorten.

De geïnteresseerde gemeenten zullen contact kunnen opnemen met de fabrikant van de paspoorten om dit te organiseren en de facturering zal rechtstreeks tussen de gemeente en de fabrikant van de paspoorten worden geregeld.

2.3. Automaat

Sommige gemeenten wensen de identiteits-, reis- en verblijfsdocumenten af te geven via een automaat, zodat de burger zijn document kan ophalen zonder langs te moeten gaan bij het loket.

De bovenvermelde documenten moeten echter beschouwd worden als zeer waardevolle documenten die bijzonder gevoelige persoonsgegevens bevatten. Ze moeten in de meest veilige omstandigheden worden afgegeven om zo de risico's op misbruik of verduistering te beperken. In die zin is de verdeling van documenten via een automaat om de volgende redenen niet mogelijk:

2.3.1. Veiligheidsrisico's

De veiligheidsrisico's met betrekking tot zo'n automaat, die 24/7 toegankelijk is voor het publiek, zijn aanzienlijk:

- Aantrekkelijk doelwit voor fraudeurs en georganiseerde bendes. Een automaat die buiten het gebouw staat, zal altijd gevoeliger zijn voor diefstal of hacking, ook al is hij gepantserd.
- Risico's voor de burgers die naar de automaat komen.
- Risico's op vandalisme ten aanzien van de automaat.

2.3.2. Identificatie van de aanvrager

De afgifte van documenten moet in een beveiligde omgeving gebeuren en onder toezicht van een gemeenteambtenaar. De gemeenteambtenaar moet (via het Rijksregister) de identiteit van de persoon die het document komt ophalen, controleren. Een automaat is niet aan het Rijksregister, aan Belpic of Belpas gekoppeld om de nodige verificaties van de identiteit van de houder te kunnen uitvoeren.

Het is dus onmogelijk om de persoon die het document komt ophalen, met zekerheid te identificeren.

2.3.3. Procedurele verplichtingen

Voor het afhalen van de verschillende documenten bestaan er reglementaire procedures die moeten worden nageleefd :

- Wat de **paspoorten** betreft: moet de status van het paspoort worden aangepast wanneer het overhandigd wordt aan de houder ervan (status "afgegeven") om de perfecte traceerbaarheid van het document te garanderen. Dat is des te belangrijker wanneer het document, tijdens zijn levenscyclus, als zijnde "gestolen" of "verloren" zou worden aangegeven, waardoor een onderzoek noodzakelijk is. Wanneer het nieuwe document overhandigd wordt, moet het vervangen document bovendien worden geannuleerd en worden teruggegeven aan de gemeenteambtenaar voor onmiddellijke vernietiging.
- Wat de **identiteitskaarten en verblijfstitels** betreft: moet de status van het document aangepast worden en moeten de certificaten van de kaart geactiveerd worden via Belpic, zodat men zich online kan identificeren en een digitale handtekening kan plaatsen om een perfecte traceerbaarheid van het document te garanderen. Wanneer het nieuwe document overhandigd wordt, moet het vervangen document worden geannuleerd en worden teruggegeven aan de gemeenteambtenaar voor onmiddellijke vernietiging. Op het ogenblik van de afgifte van de kaart dient tevens een matching van de vingerafdrukken te worden uitgevoerd.

2.4. Mobiele kit

Sommige gemeenten hebben ons kennis gegeven van hun wens om mobiele kits te kopen voor de aanvraag en afgifte van identiteits-, reis- en verblijfsdocumenten. Het doel is om de aanvragen te kunnen registreren van personen die zich niet naar het gemeentebestuur kunnen verplaatsen (bv. gevangenen, zieken, ouderen, enz.).

De FOD Binnenlandse Zaken heeft een mobiele kit ontwikkeld in de vorm van een tablet met alle benodigde randapparatuur en software om identiteits- en verblijfsdocumenten buiten het gemeenteloket aan te vragen en af te leveren.

Gemeenten kunnen deze mobiele kit aanschaffen via hun informaticaleverancier.

3. Conclusies

De taskforce wil met deze aanbevelingen de gemeenten in geen geval beletten om dienstverleningsovereenkomsten te sluiten met privébedrijven teneinde de dienstverlening aan de burger te verbeteren. Dat is immers ook waar de verschillende in de taskforce vertegenwoordigde FOD's naar streven.

Deze dienstverleningsovereenkomsten moeten evenwel aan bepaalde voorwaarden voldoen om de veiligheid van de processen voor het aanvragen en afgeven van identiteits-, reis- en verblijfsdocumenten, de bescherming van de persoonsgegevens van burgers en de integriteit van de databanken van de betrokken FOD's te verzekeren.

Dat is bovendien in het belang van de gemeenten en hun burgers.

Daarom vraagt de taskforce de gemeenten om daadwerkelijk gevolg te geven aan deze aanbevelingen.