Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

De voorzitter van de Tweede Kamer der
Staten-Generaal
Postbus 20018
2500 EA Den Haag

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Kenmerk
2012/52782
Uw Kenmerk
2012Z14564

Bijlagen
1

Datum 15 augustus 2012
Betreft Kamervragen over de nieuwe paspoorten die grote beveiligingsproblemen kennen

Hierbij bied ik u de antwoorden aan op de vragen die zijn gesteld door het lid Elissen (PVV) over de nieuwe paspoorten die grote beveiligingsproblemen kennen. De vragen zijn ingezonden op 17 juli 1012.

Met het antwoord op de vragen van het lid Elissen geef ik tevens antwoord op vraag 13 uit de vragen van het lid Schouw over de veiligheid van paspoortgegevens (nr 2012Z14576). De staatssecretaris van Veiligheid en Justitie heeft op 23 juli 2012 de overige vragen van het lid Schouw over dit onderwerp beantwoord.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

Mevrouw mr. drs. J.W.E. Spies

Datum
15 augustus 2012

Kenmerk
2012/52782

Vragen van het lid Elissen (PVV) aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over de nieuw paspoorten die grote beveiligingsproblemen kennen (ingezonden 17 juli 2012)

Vraag 1
Bent u bekend met het bericht “Nieuwe pas is onveilig”?[1]

Antwoord:
Ja

Vraag 2
Ziet u net als de ontdekker van de kwetsbaarheden ernstige bedreigingen voor de maatschappelijke veiligheid? Zo nee, waarom niet?

Vraag 3
Gaat u maatregelen nemen om identiteitsfraude te voorkomen? Zo ja, welke en kunt u deze nader toelichten?

Vraag 4
Wat gaat u doen om de kwetsbaarheden in de nieuwe paspoorten te verhelpen? Welke maatregelen gaat u treffen in het kader van nationale veiligheid en terrorismebestrijding?

Vraag 5
Wat gaat u op lange termijn doen om te voorkomen dat er opnieuw paspoorten met beveiligingsproblemen ontworpen worden?

Antwoorden vragen 2 t/m 5:
Het betreffende artikel heeft betrekking op twee aspecten, te weten het op afstand kunnen activeren van de Rfid-chip die in de reisdocumenten is opgenomen en het kunnen kopiëren van de gegevens die in de chip zijn opgeslagen.
Ik memoreer dat over beide aspecten uw Kamer geïnformeerd is. Reeds in september 2005, dus voor de invoering in 2006 van de chip in de reisdocumenten, is in antwoord op vragen van het TK-lid De Wit[2] aan de Kamer gemeld dat het door de Europese Unie voorgeschreven mechanisme dat gebruikt wordt om toegang te krijgen tot de gegevens in de chip (Basic Access Control) zwakheden kent.

1

2

De Telegraaf, 14 juli 2012 "Nieuwe pas is onveilig"
[2] TK 2004-2005, nr 2293

In 2008 heeft de toenmalige staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties de Kamer geïnformeerd[3] over het op afstand kunnen activeren van de chip in de reisdocumenten en de resultaten van onderzoek naar de mogelijkheden om dat tegen te gaan. De betreffende onderzoeksrapporten zijn met deze brief aan de Kamer aangeboden. Voor de verdere details verwijs ik naar de stukken die eerder aan uw Kamer zijn gezonden.

Ik teken hierbij aan dat de vingerafdrukken die sinds 2009 in de chip van de reisdocumenten worden opgeslagen extra beveiligd zijn. Binnen de Europese Unie is hiervoor het

[3] TK 2007-2008, 15 764 nr 39

beschermingsmechanisme Extended Access Control (EAC) ontwikkeld. Naast bescherming van de toegang tot de vingerafdrukken middels Terminal Authenticatie, voorziet EAC in de beveiliging van de communicatie tussen chip en uitleesapparaat (d.m.v. Chip Authenticatie). Sinds de invoering van de vingerafdrukken in 2009 wordt dit toegepast. Door de toepassing van EAC kunnen alleen daartoe geautoriseerde voorzieningen de vingerafdrukken uit de chip lezen. Voor de Nederlandse reisdocumenten geldt dat thans alleen de voorzieningen van de uitgevende instanties van de reisdocumenten over een dergelijke autorisatie beschikken.

In de beantwoording van meerdere schriftelijke vragen[4] is ook ingegaan op de mogelijkheid dat de gegevens die in de chip zijn opgeslagen worden gekopieerd en de mogelijkheid om dat te detecteren. Uiteraard is het zo dat controlerende instanties wel moeten controleren of het om gekopieerde gegevens gaat. Dat geldt ook voor de fysieke echtheidskenmerken van de reisdocumenten. Er kan alleen maar worden vastgesteld dat er met een document wordt gefraudeerd als goed gecontroleerd wordt of het document integer is.

[4] TK 2007-2008, nr 3296, TK 2008-2009, nr 328, TK 2008-2009, nr 1836 en TK 2008-2009, nr 1840