Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2008–2009

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1836

Vragen van de leden **Gerkens** en **Van Raak** (beiden SP) aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Justitie over *het hacken van de chip op Canadese en Mexicaanse identiteitskaarten.* (Ingezonden 5 februari 2009)

1
Wat is uw reactie op het bericht dat chips in identiteitsbewijzen in Amerika gekloond zijn zonder dat de eigenaar daar iets van wist?[1]

2
Kunt u aangeven welke nadelen en risico's het klonen met zich meebrengt?

3
Kunt u garanderen dat in alle situaties waarbij het paspoort als identificatie wordt gebruikt, gebruik wordt gemaakt van «active authentication»? Zo nee, waarom niet?

4
Sluit u uit dat de chip in de Nederlandse reisdocumenten ook op deze wijze, dus zonder medeweten van de eigenaar, gekloond kan worden? Zo ja, kunt u dit toelichten? Zo nee, waarom niet?

5
Welke maatregelen heeft u getroffen om klonen tegen te gaan?

6
Deelt u de mening dat het toepassen van deze technologie uiteindelijk een race tussen hackers en overheid zal zijn? Zo ja, acht u het dan wijs om op deze chip biometrische informatie te zetten? Zo nee, waarom niet?

[1] NU.nl, 3 februari 2009: «Hacker kopieert gegevens paspoort op afstand».

Antwoord

Antwoord van staatssecretaris **Bijleveld-Schouten** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de minister van Justitie (ontvangen 9 maart 2009)

1
Aangenomen wordt dat deze vraag betrekking heeft op het bericht van Nu.nl waarin gerefereerd wordt naar het werk van Chris Paget met betrekking tot de US Passport Card. Ik heb bij de verantwoordelijke autoriteit in de VS, zijnde het US Department of State, nagegaan wat de US Passport Card is en hoe die kaart beveiligd is. Zie ook de antwoorden op de vragen van het lid Azough (GroenLinks) met het nummer 2080912460.

2
Het risico is dat bij een (geautomatiseerde) controle niet wordt gedetecteerd dat de inhoud van de gegevens in de chip gekopieerd zijn. Ik merk hierbij op dat de chip en de gegevens daarin niet los gezien kunnen worden van het fysieke reisdocument en van de gegevens die daarop staan. De chip met de daarin opgeslagen gegevens biedt aanvullende echtheidskenmerken die samen met alle andere echtheidskenmerken in het reisdocument moeten waarborgen dat het document als geheel betrouwbaar is.

3
Het Actieve Authenticatie mechanisme wordt niet afgedwongen door de chip. Het is het uitleesapparaat dat «Actieve Authenticatie» moet uitvoeren.
De uitgevende instanties van de Nederlandse reisdocumenten krijgen in het kader van de invoering van de vingerafdrukken apparatuur en programmatuur om de reisdocumenten uit te lezen. Ik heb de Kamer eerder al laten weten (TK 2007 – 2008, 3296: Antwoorden op de vragen van het lid Gerkens over het klonen van de chip in het paspoort) dat deze apparatuur zal controleren of de inhoud van de chip gekopieerde gegevens bevat. Tevens is daarbij aangegeven dat de apparatuur van de KMAR in het kader van grenscontrole zowel Active Authentication als de elektronische handtekening over de gegevens controleert.
Garanties over de apparatuur die wordt gebruikt in het buitenland bij (grens)controle kunnen niet gegeven worden. Actieve Authenticatie is internationaal niet als verplicht voorgeschreven, maar als optioneel.

KVR35323
2080912060
0809tkkvr1836
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2009

4
Testen die ik heb laten uitvoeren en waarover ik de Kamer heb geïnformeerd wijzen uit dat om persoonsgegevens uit een chip van een Nederlands reisdocument te kopiëren, eerst toegang moet worden verkregen tot de chip van het Nederlandse reisdocument. Hiervoor is het noodzakelijk dat eerst de machine leesbare zone (MRZ) wordt uitgelezen. Daarvoor moet het reisdocument eerst op een uitleesapparaat worden gelegd. Dit mechanisme wordt aangeduid als Basic Access Control. Bekend is dat het Basic Access Control mechanisme kwetsbaarheden kent. Zoals de Kamer weet, spant Nederland zich in internationaal verband in om dit mechanisme te versterken.
De International Civil Aviation Organisation (ICAO) buigt zich over deze kwestie. Nederland is op grond van Europese regelgeving verplicht om Basic Access Control toe te passen in de reisdocumenten.
Als de inhoud van de chip van een Nederlands reisdocument wordt gekopieerd is dat te detecteren. De Nederlandse reisdocumenten zijn immers uitgerust met het beveiligingsmechanisme Active Authentication.

5
Zie het antwoord op vraag 4.

6
Dat geldt voor alle beveiliging van de reisdocumenten. Dat is de reden waarom er continue aandacht is voor de beveiliging van de documenten en de echtheidskenmerken die gebruikt worden. Ik wijs hierbij naar mijn brief van 10 april 2008 (TK 2007 – 2008, 25 764, nr. 38).
In dit kader wil ik u informeren over mogelijke zwakheden in implementaties van het zogenaamde RSA-algoritme. Ik informeer u hierover, omdat het RSA-algoritme wordt gebruikt in de chip van de Nederlandse reisdocumenten om het Active Authentication mechanisme te realiseren dat bedoeld is om te detecteren of gegevens van de originele chip van een reisdocument zijn gekopieerd.
De zwakheden die zijn geconstateerd zijn van toepassing bij implementaties van het RSA-algoritme die gebruik maken van de zogenaamde Chinese Reststelling. Dat is een techniek om het RSA-algoritme snel te kunnen uitvoeren. Het bedrijf DNV-Cibit heeft in mijn opdracht de broncode onderzocht van de leverancier van de Nederlandse reisdocumenten en daarbij vastgesteld dat de Nederlandse reisdocumenten gebruik maken van een RSA-implementatie die niet gebaseerd is op de Chinese Reststelling.