

Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

**Macro Economische
Vraagstukken en
Arbeidsvoorwaardenbeleid**

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.minvws.nl

Inlichtingen bij

Datum 31 maart 2009
Betreft Smartcard

Ons kenmerk
MEVA/ICT-2922193

Bijlagen

Geachte voorzitter,

Uw brief

In de brief van 19 februari 2009 (MEVA/ICT-2914041) naar aanleiding van de wetsbehandeling elektronisch patiëntendossier is gemeld dat er maatregelen worden getroffen om een onlangs in een laboratoriumomgeving geconstateerde kwetsbaarheid in het rekenmechanisme van de chip op de UZI-pas te onder-
vangen.

*Correspondentie uitsluitend
richten aan het retouradres
met vermelding van de datum
en het kenmerk van deze
brief.*

De smartcards die te maken hebben met deze kwetsbaarheid worden breed (inter-
nationaal) toegepast, zowel in de publieke als de private sector. In Nederland be-
treft het in de publieke sector de UZI-pas en de Defensiepas. Ook het ministerie
van Verkeer en Waterstaat maakt gebruik hiervan gebruik in de Digitale Tacho-
graaf en heeft ze voorzien voor de Boordcomputer Taxi.

Kwetsbaarheid

De geconstateerde kwetsbaarheid betreft de toepassing van het Chinese
Remainder Theorem (CRT) om het uitvoeren van bepaalde berekeningen te ver-
snellen. In een laboratoriumsituatie zijn experts in staat gebleken om de private
sleutel van een chip te achterhalen. Om een private sleutel te achterhalen is het
telkens weer nodig om te beschikken over de smartcard én bijbehorende pincode,
grote deskundigheid en gespecialiseerde apparatuur. Hiermee kan een private
sleutel van een chip worden verkregen. Deze is overigens dan alleen te gebruiken
zolang de originele smartcard niet ingetrokken is door de rechtmatige eigenaar.

Gevolgen voor UZI-pas

Na contact met leveranciers is door VWS vastgesteld dat de kwetsbaarheid een
zeer gering operationeel risico vormt voor het gebruik van de UZI-passen voor de
toegang tot het EPD. Dit mede gezien het feit dat de UZI-pas niet de enige
beveiligingsmaatregel vormt. Een zorgaanbieder moet bijvoorbeeld vóór aan-
sluiting op het landelijk schakelpunt voldoen aan de eisen voor een Goed Beheerd
Zorgsysteem (GBZ). Het gaat dan om waarborgen omtrent een juiste en zorg-
vuldige registratie, verwerking en verstrekking van gegevens. Voor toegang tot
het EPD kan de UZI-pas alleen worden gebruikt binnen een GBZ waarbinnen de
betreffende pas geautoriseerd is. Bovendien wordt in het landelijk schakelpunt en
in de GBZ permanent vastgelegd wie wanneer welke gegevens inziet, de zoge-
naamde loggegevens.

Wel is het belangrijk de kwetsbaarheid op korte termijn weg te nemen. Voor de UZI-pas is deze overgang naar een modernere chip (zonder de geconstateerde kwetsbaarheid) voorzien voor medio derde kwartaal 2009. Vanaf dat moment zal elke nieuwe UZI-pas zijn voorzien van de nieuwe chip.

**Macro Economische
Vraagstukken en
Arbeidsvoorwaardenbeleid**

In de communicatie naar de huidige gebruikers van de UZI-pas zal extra worden benadrukt dat de pas en pincode gescheiden moeten worden gehouden en zorgvuldig moeten worden beheerd. Bij verlies of diefstal van de pas dient de pas direct ingetrokken te worden. Dit kan 24 uur per dag via de website van het UZI-register.

Ons kenmerk
MEVA/ICT-2922193

De geldigheid van UZI-passen is drie jaar. Vanaf het moment dat de nieuwe chip beschikbaar is, zullen de al verstrekte passen niet na drie jaar, maar na twee jaar worden vervangen. Indien een gebruiker dit wenst, kan eerder omwisseling plaatsvinden.

Gevolgen voor Defensiepas

Voor Defensie is de kwetsbaarheid op dit moment niet relevant, omdat de private sleutel nog niet wordt gebruikt. Defensie heeft maatregelen getroffen om de kwetsbaarheid in het rekenmechanisme weg te nemen voordat de private sleutel in gebruik wordt genomen.

Gevolgen voor Boordcomputer taxi-pas

Vanwege de geconstateerde kwetsbaarheid in de smartcards heeft de leverancier van de beoogde smartcards van de boordcomputer mij laten weten dat hij deze niet kan leveren per 1 november. Hierdoor zal de invoering van de boordcomputer met drie tot vijf maanden verschuiven. Verkeer en Waterstaat volgt de ontwikkeling op de voet, samen met de leverancier. Dit heeft geen gevolgen voor de geplande publicatie van de regelgeving in juli 2009.

Gevolgen voor Digitale Tachograaf-pas

In welke mate de ontdekte kwetsbaarheid een probleem is voor de passen van de digitale tachograaf, is op dit moment onderwerp van overleg met collega-ministeries van Verkeer en de Europese Commissie. Zodra daarover meer bekend is, wordt u nader geïnformeerd.

**Macro Economische
Vraagstukken en
Arbeidsvoorwaardenbeleid**

Ons kenmerk
MEVA/ICT-2922193

Hoogachtend,

de Minister van Volksgezondheid,
Welzijn en Sport,

dr. A. Klink

de Staatssecretaris van Defensie

drs. J.G. de Vries

de Staatssecretaris van Verkeer en Waterstaat,

J.C. Huizinga-Heringa