Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2009–2010

Aanhangsel van de Handelingen

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

1173

Vragen van het lid **Zijlstra** (VVD) aan de minister van Volksgezondheid, Welzijn en Sport over *de beveiliging van het elektronisch patiëntendossier (EPD).* (Ingezonden 26 november 2009)

1
Staat u nog steeds achter uw uitspraak dat «het landelijk EPD moet veilig zijn en de privacy van de mensen moet zijn gewaarborgd. Daar werken wij niet alleen hard aan, die privacy is zelfs gegarandeerd»?[1]

2
Bent u bekend met de uitspraak van Price Waterhouse Coopers, de Radboud Universiteit Nijmegen en de Universiteit Tilburg in een gezamenlijk rapport dat DigiD+ een te lage bescherming biedt voor medische patiëntgegevens?[2] Wat is uw mening over deze uitspraak?

3
Bent u bekend met de beveiligingstechniek die gebruik maakt van Public Key Infrastructure (PKI)-overheid certificaten? Kunt u ingaan op de stelling dat deze techniek aanzienlijk veiliger en ook goedkoper is dan DigiD+?

4
Is het waar dat DigiD+ een beveiligingsniveau van 2+ kan leveren en dat de beveiligingstechniek met PKI-overheid certificaten een beveiligingsniveau van 5 en daarmee het hoogst mogelijke niveau kan leveren?

5
Is het waar dat het ministerie van Binnenlandse Zaken en Koninkrijksrelaties gebruik gaat maken van de beveiligingstechniek met PKI-overheid certificaten? Is het waar dat de Belastingdienst vanwege veiligheidsredenen afscheid neemt van DigiD en zal overstappen naar de beveiligingstechniek met PKI-overheid certificaten?

6
Is het waar dat het Nationaal ICT Instituut in de Zorg (Nictiz) u heeft voorgesteld een pilot met deze techniek op te zetten en dat u tot op heden hieraan geen gevolg heeft gegeven? Kunt u toelichten waarom u een dergelijke pilot tot op heden niet hebt opgestart?

7
Kunt u uiteenzetten hoe u de uitspraak «het landelijk EPD moet veilig zijn en de privacy van de mensen moet zijn gewaarborgd. Daar werken wij niet alleen hard aan, die privacy is zelfs gegarandeerd» denkt waar te maken als u vast blijft houden aan DigiD+ als beveiligingstechniek voor het EPD?

8
Bent u bereid de beveiligingstechniek met PKI-overheid certificaten, of een andere niveau 5 beveiligingstechniek, als basis te nemen voor de beveiliging van het EPD? Zo niet, waarom niet?

[1] Handelingen II, vergaderjaar 2008–2009, nr. 43, blz. 3769–3794.
[2] «Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)» PWC, Radboud Universiteit Nijmegen en Universiteit Tilburg (2 december) 2008.

Antwoord

Antwoord van minister **Klink** (Volksgezondheid, Welzijn en Sport) (ontvangen 11 januari 2010)

1
Ja. Zoals ik heb vermeld in mijn brief van 27 november jl. (MEVA/ICT-2973937) biedt de landelijke infrastructuur van het EPD een hoogwaardig beveiligingsniveau met strenge privacyeisen, die met het College Bescherming Persoonsgegevens is afgestemd.

2
Ja. Dit rapport, dat in opdracht van mij is gemaakt, heb ik als bijlage aan u aangeboden bij mijn brief over het EPD van 12 december 2008 (TK 2008–2009, 27 529, nr. 53).
In het rapport wordt beargumenteerd dat het huidige niveau DigiD-midden niet voldoet vanwege het uitgifteproces. Het rapport beveelt daarom een variant aan op DigiD-midden, met een verbeterd uitgifteproces op basis van

KVR38922
2009Z22694
0910tkkvr1173
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2010

face-to-face uitgifte aan een balie. Volgens de analyse van het rapport kan daarmee het vereiste beveiligingsniveau worden gerealiseerd. Deze aanbeveling wordt op dit moment opgevolgd met de ontwikkeling van EPD-DigiD.

3
Ja. Voor de toegang van de zorgaanbieder tot het EPD met de UZI-pas wordt gebruik gemaakt van PKI-overheid certificaten. In mijn brief van 12 december 2008 heb ik aangegeven hoe ik, rekening houdend met deze context, ben gekomen tot de ontwikkeling van EPD-DigiD. Hierbij is aangesloten bij het generieke middel voor authenticatie voor burgers voor diensten van de overheid (DigiD), dat zodanig wordt aangevuld dat het aansluit bij het niveau van beveiliging en privacy uit eerder genoemd rapport van PWC en adviezen van het CBP.

4
In het rapport is aangegeven dat bij het ontwerp van DigiD is uitgegaan van drie zekerheidsniveaus voor authenticatie, namelijk basis (niveau 1), midden (niveau 2) en hoog (niveau 3). De onderzoekers stellen dat gelet op de juridische en technische beveiligingseisen rondom het EPD, een zekerheidsniveau van meer dan 2 noodzakelijk is.
Het hoogste zekerheidsniveau zoals benoemd in het rapport is niveau 3. In het rapport wordt aangegeven dat authenticatie met zekerheidsniveau 3 via de eNIK zal kunnen plaatsvinden. Bij de eNIK zal gebruik worden gemaakt van PKI-overheid. Zoals ik heb aangegeven in mijn brief van 12 december 2008 is echter uit gesprekken met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties duidelijk geworden dat de eNIK de komende jaren niet gereed zal zijn.
Gelet op de prioriteit om de zorgconsument toegang te geven tot een deel van diens medische gegevens, is besloten om alternatieve toegangsmiddelen in kaart te brengen met een zekerheidsniveau hoger dan het huidige zekerheidsniveau «midden». Op basis hiervan heb ik besloten het EPD-DigiD te laten ontwikkelen.

5
Het ministerie van BZK, dat de beheerder is van het stelsel van PKI-overheid, maakt zelf – net als een groot aantal andere overheidsorganisaties – gebruik van beveiligingstechnieken op basis van PKI-overheid.
De Belastingdienst heeft destijds een belangrijke impuls aan het gebruik van DigiD gegeven door het gebruik van (het basisniveau van) DigiD verplicht te stellen voor het doen van elektronische aangifte inkomstenbelasting. De met DigiD opgedane ervaringen zijn zonder meer positief, zodat de Belastingdienst geen enkel voornemen heeft om af te stappen van DigiD.

6
Bij de gedachtevorming over de toegang van de patiënt tot het EPD is de eNIK onderwerp van gesprek geweest tussen Nictiz en VWS. Vanwege de onzekere realisatietermijn van de eNIK is hier geen verdere uitwerking aan gegeven. Het Nictiz is op dit moment nauw betrokken bij de ontwikkeling van de toegang van de patiënt tot het EPD. Vanuit Nictiz heeft mij geen concreet voorstel bereikt voor een pilot op basis van PKI-overheid techniek.

7
Zie het antwoord op vragen 2 en 3.

8
Zie het antwoord op vragen 2 en 3.