# Risicoanalyse EPD-DigiD

## Naar aanleiding van de A5/1 kwetsbaarheid in GSM

Definitief

30 juni 2010

Referentie: 2010-1400/OV/ev/mp

Radboud Universiteit Nijmegen

PricewaterhouseCoopers

Radboud Universiteit Nijmegen

PricewaterhouseCoopers

# Inhoudsopgave


**1 Managementsamenvatting ..... 3**

**2 Inleiding ..... 8**

2.1 Achtergrond en aanleiding ..... 8

**3 Doelstelling en reikwijdte ..... 10**

**4 Aanpak ..... 11**

**5 Kwetsbaarheidanalyse SMS authenticatie het EPD-DigiD ..... 12**

5.1 Conclusie ..... 12

5.2 Aannames ..... 13

5.3 Hoe werkt de aanval? ..... 13

5.3.1 Stap I ..... 13

5.3.2 Stap II ..... 13

5.3.3 Stap III ..... 14

5.3.4 Conclusie ..... 14

5.4 Mogelijke aanvalsscenario's ..... 14

5.4.1 Aanvalsscenario A - Zelf een aanval realiseren ..... 14

5.4.2 Aanvalsscenario B - Wachten tot de open source initiatieven ver genoeg gevorderd zijn ..... 15

5.5 Evaluatie van aanvalscenario's ..... 16

**6 Context en risicobeoordeling SMS kwetsbaarheid ..... 19**

6.1 Context gebruik SMS codes in EPD-DigiD ..... 19

6.1.1 Gebruik van SMS ten behoeve van authenticatie ..... 19

6.1.2 Gebruik van SMS ten behoeve van Wachtwoordherstel ..... 19

6.2 Risicobeoordeling SMS kwetsbaarheid ..... 20

6.3 Daadwerkelijk verlies van (vertrouwelijkheid van) informatie ..... 21

6.4 Verlies van publiek vertrouwen in het landelijk EPD ..... 22

6.5 Non-compliance met regelgeving ..... 23

6.6 Conclusie ..... 24

**7 Risicobehandeling ..... 25**

7.1 Mitigerende maatregelen ..... 25

7.1.1 Versterkte encryptie GSM/SMS verkeer ..... 25

7.1.2 eNIK/eDL ..... 26

7.1.3 RTDA ..... 26

7.1.4 Persoonlijke conversietabel SMS codes ..... 27

7.1.5 TAN code lijsten ....28
7.1.6 Versterking DigiD wachtwoorden ....28
7.1.7 Zodra de kwetsbaarheid (bijna) exploiteerbaar is het EPD-DigiD stopzetten....29
7.2 Samenvatting restrisico's maatregelen ....30

**A Detail uitwerking persoonlijke SMS conversietabel ....31**

**B Geraadpleegde personen....32**
B.1 Ministerie van Volksgezondheid, Welzijn en Sport....32
B.2 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties ....32
B.3 Logius....32
B.4 GOVCERT....32

**C Onderzoeksteam ....33**
C.1 PricewaterhouseCoopers Advisory N.V. ....33
C.2 Institute for Computing and Information Sciences - Radboud Universiteit Nijmegen 33

**D Open initiatieven rond GSM en diens beveiliging....34**
D.1 USRP ....34
D.2 GNU Radio (http://gnuradio.org)....34
D.3 AirProbe (https://svn.berlin.ccc.de/projects/airprobe/wiki) ....34
D.4 OpenBTS (http://openbts.sourceforge.net/) ....34
D.5 OpenBSC (http://openbsc.osmocom.org/trac/wiki/OpenBSC) ....34
D.6 OsmocomBB (http://bb.osmocom.org/trac/)....35
D.7 A5/1 kraak project (http://www.reflextor.com/trac/a51)....35

# 1 Managementsamenvatting

*Achtergrond*

01 Logius ontwikkelt momenteel in opdracht van het Ministerie van Volkgezondheid, Welzijn en Sport het voor het Elektronisch Patiënten Dossier (hierna: EPD) Toegang Patiënt benodigde authenticatiemiddel EPD-DigiD. Het EPD-DigiD maakt gebruik van DigiD op basis van SMS-authenticatie en een face-to-face uitgifteproces. Een pilot op beperkte schaal, met een beperkte set aan functionaliteit is gepland voor het vierde kwartaal 2010. Landelijke live-gang volgt hier later op.

02 In actuele berichtgeving, van onder andere GOVCERT, is een kwetsbaarheid naar voren gekomen in het A5/1 algoritme, dat wordt gebruikt voor de versleuteling van GSM verkeer (waaronder SMS) in Nederland, die mogelijke implicaties heeft voor het gekozen authenticatiemiddel EPD-DigiD.

03 In de periode mei-juni 2010 heeft PricewaterhouseCoopers Advisory (PwC) samen met de Digital Security groep van de Radboud Universiteit (RU) in opdracht van het Ministerie van Volksgezondheid, Welzijn en Sport een risicoanalyse uitgevoerd naar de genoemde beveiligingskwetsbaarheid in SMS. De doelstelling van de analyse was tweeledig:

- Het in kaart brengen van de kwetsbaarheid van het EPD-DigiD ten gevolge van de A5/1 kwetsbaarheid.
- Het uitvoeren van een risicobeoordeling en -behandeling naar de genoemde kwetsbaarheid voor de beveiliging van EPD-DigiD.

04 De risicoanalyse is beperkt tot de A5/1 kwetsbaarheid in de context van het EPD-DigiD authenticatiemiddel. Conclusies en aanbevelingen voortvloeiend uit deze risicoanalyse zijn niet zonder meer van toepassing op andere SMS toepassingen. Verder zijn de risicoanalyse, conclusies en aanbevelingen uit dit onderzoek ook niet van toepassing op andere onderdelen van het EPD daar dit geen onderwerp van onderzoek is geweest.

05 De feitelijke adoptie van mitigerende maatregelen en de acceptatie van eventuele restrisico's is de verantwoordelijkheid van het Ministerie van Volksgezondheid, Welzijn en Sport.

06 In het kader van de risicoanalyse zijn interviews gehouden met betrokken personen werkzaam bij GOVCERT, Logius en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Volksgezondheid, Welzijn en Sport. Daarnaast zijn interne besprekingen tussen PwC en de RU gevoerd. Er zijn geen gesprekken gevoerd met telecommunicatie operators om hun visie te vernemen over de (vermeende) kwetsbaarheden van de GSM algoritmen welke in dit document worden genoemd noch om hun visie te vernemen over mogelijke plannen om hun

netwerken en/of mobiele telefoons en/of producten aan te passen als gevolg van de genoemde kwetsbaarheden.

*Resultaten van de kwetsbaarheidanalyse*

07 Het beschikbaar komen van een werkende opstelling (ontvanger, PC, publiek beschikbare software) die SMS berichten kan onderscheppen levert een reële kwetsbaarheid op voor EPD-DigiD. In realistische zin moet er rekening mee worden gehouden dat een dergelijke opstelling binnen drie jaar ontwikkeld is en kan worden gedemonstreerd. In het meest ongunstige geval moet er rekening mee worden gehouden dat de kwetsbaarheid binnen een half jaar wordt gedemonstreerd, bijvoorbeeld op een congres aan het eind van 2010. De verwachting is echter dat het langer zal duren. De kosten van een dergelijke opstelling (hardware en software) schatten wij in als zeer beperkt. De kosten van inzet van individuen wordt niet door ons gekwantificeerd.

*Resultaten van de risicobeoordeling*

08 Op basis van ons onderzoek komen wij tot drie belangrijke bedreigingen gerelateerd aan de kwetsbaarheid die wij onderstaand toelichten:

1. Verlies van (vertrouwelijkheid van) patiëntinformatie, indien de kwetsbaarheid **daadwerkelijk** wordt geëxploiteerd bij een patiënt. Het risico gerelateerd aan deze bedreiging beoordelen wij als **Matig**.
2. Verlies van publiek vertrouwen in het landelijk Elektronisch Patiënten Dossier (hierna: EPD), indien exploiteerbaarheid van de kwetsbaarheid aantoonbaar in de openbaarheid komt. Het risico gerelateerd aan deze bedreiging beoordelen wij als **Hoog/Zeer Hoog**.
3. Non-compliance met regelgeving; de verzwakking van SMS betekent dat het EPD-DigiD **strikt genomen niet meer aan de eisen van een 'sterk' authenticatiemiddel voldoet** in de zin van de Nederlandse beveiligingsnorm NEN 7512. In een brief[1] rond het EPD aan het Ministerie van Volksgezondheid, Welzijn en Sport stelt het College Bescherming Persoonsgegevens (hierna: CBP) geen expliciete eisen aan het EPD authenticatiemiddel maar stelt dat het gebruik van "two factor authentication voor de hand ligt". Dit is in lijn met de eisen die NEN 7512 stelt aan een 'sterk' authenticatiemiddel'; het niet (meer) voldoen aan deze eisen kan aldus betekenen dat niet wordt voldaan aan de eisen die het CBP stelt. Dit risico gerelateerd aan deze bedreiging beoordelen wij als **Hoog**.

[1] Zie de brief "Identificatie en authenticatie bij toegang patiënt tot het EPD" dd. 7 augustus 2008.

De bedreigingen en risico inschattingen zijn in de volgende tabel samengevat.

| Bedreiging | Risico |
|---|---|
| Verlies gegevens | Matig |
| Publiek vertrouwen | Hoog/Zeer Hoog |
| Non-compliance | Hoog |

**Tabel 1 - Risicoschatting Bedreigingen**

*Risicobehandeling*

09 Op basis van ons onderzoek komen wij tot de volgende mitigerende maatregelen die toegepast zouden kunnen worden. De huidige opzet van het EPD-DigiD authenticatiemiddel is geopperd in het rapport *"Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)"*, d.d. 2 december 2008. De onderstaand als tweede en derde genoemde mitigerende maatregel zijn in dat rapport geopperde alternatieven.

- Versterkte encryptie GSM/SMS verkeer.
  Dit omvat het toepassen van de versleutelingstandaard A5/3 door de telecommunicatie operators. Deze standaard is de opvolger van standaard A5/1 die de basis van de kwetsbaarheid vormt. Deze maatregel neemt in opzet de SMS kwetsbaarheid weg. Deze maatregel zal naar onze inschatting pas over een aantal jaren (i.e. > 5 jaar) effectief kunnen zijn, ook doordat bestaande toestellen mogelijk A5/3 niet ondersteunen.
- eNIK/eDL.
  Dit behelst het gebruik van een Elektronische Identiteitskaart (eNIK), een Elektronisch Rijbewijs (eDL) met elektronische Identiteit (eID) functionaliteit door alle zorgconsumenten als fysiek authenticatiemiddel ter vervanging van de SMS authenticatie. Ook deze maatregel neemt de SMS kwetsbaarheid weg. Maar ook deze maatregel zal, conform de huidige plannen van de betrokken organisaties, pas over een aantal jaren effectief kunnen zijn.
- RTDA.
  Bij Remote Travel Document Authentication (RTDA) wordt het elektronisch paspoort via een draadloze lezer als fysiek authenticatiemiddel gebruikt. Het gebruik van RTDA in combinatie met DigiD-Midden kan het gebruik van SMS authenticatie als fysiek authenticatiemiddel aanvullen. Deze maatregel neemt de SMS kwetsbaarheid weg, omdat het face-to-face uitgegeven elektronisch paspoort als extra benodigd fysiek middel wordt ingezet. Deze

maatregel zal, mits de benodigde contactloze lezers door de betrokken organisaties voor die tijd kunnen worden uitgerold, binnen twee jaar effectief kunnen zijn.

- Persoonlijke conversietabel SMS codes.
  Om een extra controle in te bouwen kan aan de houders van een EDP-DigiD een zogenaamde persoonlijke conversietabel voor de ontvangen SMS codes worden uitgereikt, dit als onderdeel van het registratie en uitgifteproces. Hierbij krijgt iedere houder een tabel met voor ieder karakter een conversie naar een ander karakter. De houder dient bij het ontvangen van een SMS code ieder karakter te converteren volgens zijn persoonlijke tabel en deze op de DigiD website in te voeren. In Bijlage A van dit rapport hebben wij dit verder toegelicht. Deze maatregel reduceert het risico rond de SMS kwetsbaarheid tot **Matig**. Op basis van onze inschatting van de aanpassingen in het voorziene EPD-DigiD schatten wij in dat het gebruik van de conversietabel binnen een jaar operationeel kan zijn. Daarbij merken wij op dat deze inschatting niet besproken is met Logius en adviseren wij dit in een vervolgtraject zo spoedig mogelijk te doen indien de conversietabel overwogen wordt.
- TAN code lijsten.
  Deze maatregel behelst het uitgeven van een lijst met persoonlijke unieke codes (Transaction Authentication Number of TAN) voorzien van een volgnummer. Na een succesvolle initiële DigiD authenticatie middels gebruikersnaam en wachtwoord dient de zorgconsument vervolgens de correcte TAN code (geïdentificeerd middels het volgnummer) in te voeren om de authenticatie succesvol te doorlopen. Hierdoor is het gebruik van SMS berichten voor authenticatie niet nodig. Deze maatregel neemt de kwetsbaarheid wel weg, maar de inschatting is dat dit middel niet voldoende conform is met eisen die de Nederlandse norm NEN 7512 stelt aan ‘sterke’ authenticatie. De reden hiervoor is dat TAN codes (ongemerkt) te kopiëren zijn. Deze maatregel reduceert de risico's onvoldoende (het restrisico ligt op **Hoog**).
- Versterking DigiD wachtwoorden.
  Bij deze maatregel worden in DigiD extra beveiligingseisen afgedwongen bij houders zoals lengte en complexiteit. Deze maatregel versterkt in feite de eerste factor (gebruikersnaam/wachtwoord) maar mitigeert de kwetsbaarheid in de tweede factor (SMS) niet. Daarmee blijft de non-conformiteit met de Nederlandse norm NEN 7512 bestaan, zodat deze maatregel niet volstaat. Deze maatregel reduceert de risico rond non-conformiteit daarmee onvoldoende (het restrisico is **Hoog**).
- Zodra de kwetsbaarheid (bijna) exploiteerbaar is het EPD-DigiD stopzetten.
  Deze maatregel is reactief van aard. Hierbij worden de ontwikkelingen in de *open source* gemeenschap goed in de gaten gehouden. Zodra er indicaties zijn dat de kwetsbaarheid (bijna) exploiteerbaar is, wordt het EPD-DigiD stopgezet door het Ministerie van Volksgezondheid, Welzijn en Sport. Een aandachtspunt daarbij is wel wat dan het alternatief is. Punt daarbij is of het Ministerie van Volksgezondheid, Welzijn en Sport op tijd is, zowel in praktische zin als in de perceptie van het publiek en dat het vertrouwen in EPD(-DigiD) beschadigd kan worden. Deze maatregel reduceert de risico's onvoldoende (het restrisico is **Hoog**).

*Conclusie*

10 Uit bovenstaande analyse komt naar voren dat de GSM kwetsbaarheid, zoals deze is gesignaleerd door GOVCERT, hoge tot zeer hoge risico's met zich meebrengt voor de huidige ontwikkeling en toekomstige landelijke uitrol van EPD-DigiD. Wanneer het Ministerie van Volksgezondheid, Welzijn en Sport EPD-DigiD wil toepassen in een pilot in het vierde kwartaal van 2010 en in een later stadium landelijk live wil gaan met het patiëntenportaal en de restrisico's tot accepteerbare proporties wil terugbrengen, lijkt toepassing van een conversietabel (of een soortgelijke oplossing) het meest realistisch. Immers het restrisico wordt hiermee gereduceerd van Hoog naar Matig en het theoretische tijdpad is korter dan bij de andere varianten. Daarbij merken wij op dat toepassing van de conversietabel reeds snel overleg met Logius behoeft, ook omdat de noodzaak tot beschikbaarheid (in het vierde kwartaal van 2010) eerder is dan de door ons ingeschatte periode van een jaar.

11 Het gebruik van de conversietabellen moet daarbij gezien worden als een oplossingsrichting waarbij nog een aantal aandachtspunten bestaat die nader moeten worden uitgezocht, waarna dan nog een aanpassing van de huidige EPD-DigiD omgeving moet volgen.

# 2 Inleiding

## 2.1 Achtergrond en aanleiding

12 Het Ministerie van Volksgezondheid, Welzijn en Sport ontwikkelt het landelijk Elektronisch Patiënten Dossier (landelijk EPD), waarmee op den duur alle zorgverleners in Nederland elektronisch patiëntinformatie in het kader van medische behandelingen zullen uitwisselen. Tot op heden hebben alleen zorgverlenende instanties, via het Landelijk Schakelpunt (LSP) toegang tot de gegevens in het landelijk EPD.

13 Met de in het EPD Toegang Patiënt ontwikkelde patiëntenportaal en het klantenloket krijgen ook zorgconsumenten, via het internet, toegang tot hun eigen (medische gegevens in) het landelijk EPD.

14 Aangezien het hier medische gegevens betreft, dient het patiëntenportaal adequaat beveiligd te zijn. Dit is reeds onderzocht in het rapport *"Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)"*, d.d. 2 december 2008, waarin de volgende eisen aan het authenticatiemiddel zijn geïdentificeerd:

- De identificatie van cliënten vindt plaats met het **BSN**.
- Het authenticatieniveau moet **Sterk** zijn.
- Identificatoren met **registratieniveau 3** moeten worden toegepast.

15 Deze eisen zijn overigens gebaseerd op de Nederlandse Norm NEN 7512. In hetzelfde rapport is tevens een studie gedaan naar de authenticatiemiddelen welke geschikt zouden zijn in deze context, daarbij ook de financiële en praktische gevolgen voor het Ministerie van Volksgezondheid, Welzijn en Sport en de burger meenemend. Uiteindelijk zijn er twee authenticatiemiddelen geadviseerd die aan bovenstaande eisen voldoen en tevens geen onoverkomelijke financiële dan wel praktische gevolgen hadden, namelijk: SMS+[2] en RTDA[3]. Voor een beschrijving van deze varianten verwijzen wij naar het eerdergenoemde rapport *"Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)"*.

16 Het Ministerie van Volksgezondheid, Welzijn en Sport is voornemens SMS+ te implementeren in voorbereiding op de start van fase 1 van EPD Toegang Patiënt. Aan Logius[4] is de opdracht verleend SMS+ te implementeren als uitbreiding van de huidige DigiD dienstverlening: het zogenaamde EPD-DigiD. Op dit moment is de feitelijke ontwikkeling van het EPD-DigiD grotendeels afgerond en bevindt het EPD-DigiD zich in de testfase.

[2] Feitelijk DigiD niveau midden met een face-to-face uitgifte-/activatieproces.
[3] Remote Travel Document Authentication: hierbij wordt het elektronisch paspoort via een draadloze lezer als authenticatiemiddel gebruikt.
[4] Voormalig GBO.Overheid en beheerder van DigiD.

17 Eind 2009 heeft GOVCERT[5] een factsheet gepubliceerd waarin wordt gewezen op de recent gepubliceerde kwetsbaarheid in de A5/1 encryptie die wordt toegepast voor het GSM spraak- en data (SMS) verkeer in Nederland.

18 Na overleg met de betrokken partners (Logius, GOVCERT en het Ministerie van Binnenlandse Zaken) heeft het Ministerie van Volksgezondheid, Welzijn en Sport besloten een eigen risicoanalyse op het EPD-DigiD (de gekozen SMS+ variant) uit te voeren. Met deze analyse wil het Ministerie van Volksgezondheid, Welzijn en Sport een beeld krijgen van de mogelijke risico's die het gevolg zijn van deze kwetsbaarheid en naar de mogelijke maatregelen die deze risico's (voldoende) kunnen beperken. Het Ministerie van Volksgezondheid, Welzijn en Sport heeft PricewaterhouseCoopers Advisory (PwC) in samenwerking met de Radboud Universiteit Nijmegen (RU) gevraagd deze risicoanalyse uit te voeren.

[5] Zie www.GOVCERT.nl.

# 3 Doelstelling en reikwijdte

20 Dit onderzoek heeft de volgende twee doelstellingen:

- Het in kaart brengen van de kwetsbaarheid van het EPD-DigiD ten gevolge van de A5/1 kwetsbaarheid en het schatten van het tijdstip waarop de middelen (met name software, apparatuur) beschikbaar zijn om deze kwetsbaarheid praktisch te exploiteren.
- Het uitvoeren van een risicobeoordeling en -behandeling naar de genoemde kwetsbaarheid voor de beveiliging van EPD-DigiD. Hierbij wordt de opzet van de Nederlandse norm NEN 7512[6] rond informatiebeveiliging gevolgd: bij de risicobeoordeling worden de (grote) risico's geschat die manifest zouden kunnen worden als gevolg van de kwetsbaarheid, en bij de risicobehandeling worden mitigerende maatregelen geselecteerd en de restrisico's beoordeeld.

21 In dit onderzoek hebben wij ons beperkt tot de A5/1 kwetsbaarheid in de context van het EPD-DigiD authenticatiemiddel. Conclusies en aanbevelingen voortvloeiend uit dit onderzoek mogen niet zonder meer van toepassing worden verklaard op andere SMS toepassingen. Verder zijn de risicoanalyse, conclusies en aanbevelingen uit dit onderzoek ook niet van toepassing op andere onderdelen van het landelijk EPD daar dit geen onderwerp van onderzoek is geweest.

22 Onze rol is het uitvoeren van een risicobeoordeling en -behandeling rond bovengenoemde kwetsbaarheid. De feitelijke adoptie van mitigerende maatregelen en de acceptatie van eventuele restrisico's is de verantwoordelijkheid van het Ministerie van Volksgezondheid, Welzijn en Sport.

[6] Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor Gegevensuitwisseling.

# 4 Aanpak

23 Dit rapport is tot stand gekomen aan de hand van reeds opgebouwde kennis en expertise binnen de Security & Technology groep van PricewaterhouseCoopers Advisory (PwC) en van de Digital Security groep van de Radboud Universiteit (RU), aangevuld met literatuurstudie en interviews met betrokken experts[7] van de betrokken partijen in EPD-DigiD. Hierbij heeft de RU zich met name geconcentreerd op de technische analyse van de kwetsbaarheid, terwijl PwC zich met name heeft gericht op het uitvoeren van de risico beoordeling en -behandeling.

24 De opzet van dit rapport weerspiegelt deze aanpak. Hoofdstuk 5 bevat een technische analyse van de kwetsbaarheid waaronder een inschatting wanneer deze in de toekomst praktisch exploiteerbaar zal zijn. Hoofdstuk 6 beoordeelt de risico's die de kwetsbaarheid (zodra die kan worden geëxploiteerd) heeft op het EPD-DigiD. In Hoofdstuk 7 worden de mogelijke mitigerende of corrigerende maatregelen geïnventariseerd.

[7] Zie voor de lijst van geïnterviewde personen Bijlage B.

# 5 Kwetsbaarheidanalyse SMS authenticatie het EPD-DigiD

25 De beveiliging van het GSM systeem is voortdurend onderwerp van onderzoek. Recent is er een aantal aanvallen bekend geworden (zie GOVCERT factsheet) waardoor de vraag naar de beveiliging van het EPD-DigiD gerechtvaardigd is. De aanleiding is dat kort geleden een groep hackers een grote tabel heeft geproduceerd (een zogenaamde *Rainbow table*) die hen in staat stelt de meest gebruikte versleuteling in GSM (het zogenaamde A5/1 algoritme) snel te breken. Deze versleuteling is naar ons bekend op dit moment de enige die in Nederland voor GSM gebruikt wordt. Hiermee is een belangrijke stap gezet op de weg naar het onderscheppen van GSM verkeer (en dus ook SMS berichten), maar nog niet de laatste stap.

26 In deze analyse proberen wij een inschatting te maken van de kosten (in tijd, geld en expertise) die nodig zijn om het SMS deel van de EPD-DigiD authenticatie aan te vallen. Het concrete aanvalsscenario is een aanvaller die een SMS met EPD-DigiD toegangscode wil onderscheppen.

27 In de analyse wordt verwezen naar een aantal open initiatieven die bezig zijn met GSM en diens beveiliging. Wij hebben deze beschreven in Bijlage D.

## 5.1 Conclusie

28 De beveiliging van GSM is voortdurend onderwerp van onderzoek in zowel de academische, operationele en hackers wereld. Hierdoor worden steeds nieuwe aanvallen bekend op (delen) van de GSM beveiliging. Maar zelfs als de laatste praktische problemen in sommige aanvalscenario's zijn opgelost is het onderscheppen van GSM verkeer, waaronder SMS berichten, nog zeer lastig. De kans op een proof-of-concept aanval, onder laboratoriumcondities, in de komende paar jaar lijkt zeer groot, maar gemeengoed zal dit niet zo snel gaan worden. Daarnaast zal een dergelijke eerste proof-of-concept aanval gepresenteerd worden als generieke aanval op de internationale GSM standaard, en niet specifiek als een aanval op het EPD-DigiD in de Nederlandse context. Dat laatste kan wel vrij snel daarna volgen, aangezien er in Nederland mensen zijn met de juiste expertise en motivatie om dit te demonstreren.

29 De feitelijke apparatuurkosten van een werkende opstelling (ontvanger, PC, software) schatten wij in als zeer beperkt (EUR 3.000,-). Ten tijde van het onderzoek is de inschatting dat een dergelijke opstelling die SMS kan onderscheppen binnen drie jaar zal worden gedemonstreerd. Deze inschatting is mede gebaseerd op een inschatting van de hoeveelheid tijd en geld die wordt geïnvesteerd in een aantal (in Bijlage D genoemde) open source initiatieven. In het ongunstigste geval wordt een dergelijke opstelling al gedemonstreerd op een congres eind 2010. Uit het interview met GOVCERT komt naar voren dat zij bovenstaande inschatting delen.

30 De kosten van inzet van individuen wordt niet door ons gekwantificeerd. Dit omdat er een grote variëteit aan individuen met een variabele inzet tijd aan besteedt, waarbij het lastig is een waarde toe te kennen aan die tijd.

## 5.2 Aannames

31 De moeilijkheid van het onderscheppen van een SMS bericht is sterk afhankelijk van de instellingen van het GSM netwerk. Wij gaan er in deze analyse van uit dat GSM zendmasten in Nederland de verbinding met telefoons versleutelen met het A5/1 algoritme en dat iedere verbinding frequency hopping toepast. Frequency hopping is een techniek waarbij een signaal tussen zendmast en telefoon zeer regelmatig van frequentie verandert. Tussen welke frequenties het signaal hopt wordt bij het aanmelden van de telefoon bij de zendmast bepaald. Dit is op zichzelf geen beveiligingstechniek, maar dit maakt het afluisteren van deze signalen erg lastig voor een aanvaller. Ook gaan wij ervan uit dat de zendmasten zelf afdoende beschermd zijn tegen fysieke en logische aanvallen.

## 5.3 Hoe werkt de aanval?

32 Alle hieronder beschreven scenario's om een eenvoudig uitvoerbare aanval te realiseren gaan uit van het onderscheppen en kraken van de benodigde GSM signalen. Ze werken allemaal volgens de volgende stappen:

i. ontvangst van het GSM signaal;

ii. ontcijferen van het ontvangen signaal;

iii. interpreteren van het ontcijferde signaal.

### 5.3.1 Stap I

33 Stap I is, ten tijde van dit onderzoek, voor aanvallen op GSM (nog) niet eenvoudig te realiseren. Dit heeft zijn oorzaak in het feit dat door de gebruikte frequency hopping het, met de op dit moment vrijelijk beschikbare apparatuur en software, niet eenvoudig uitvoerbaar is om deze signalen goed op te vangen. Daarnaast moet de aanvaller in de buurt van de doeltelefoon (en als gevolg ook de zendmast waarbij de telefoon is aangemeld) zijn om het signaal te kunnen ontvangen. Dit is vooral van belang bij een aanval gericht op een specifiek persoon.

### 5.3.2 Stap II

34 Stap II is waar sinds kort een nieuwe aanval tegen bestaat. Hackers hebben een *Rainbow table* gemaakt waarmee het in theorie[8] mogelijk is deze fase snel uit te voeren. Omdat stap I nog een

[8] Zie "*Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication*", door Barkan, Biham en Keller.

groot probleem is hebben wij van de werking van deze aanval nog geen praktijkvoorbeeld gezien, maar op basis van de theorie is deze aanval effectief. Wij moeten er dus vanuit gaan dat deze fase eenvoudig uitvoerbaar is.

### 5.3.3 Stap III

35 Voor stap III is open source software beschikbaar die waarschijnlijk volledig of met zeer kleine aanpassingen zal voldoen. Deze fase is daarom eenvoudig uitvoerbaar.

### 5.3.4 Conclusie

36 Aangezien stap II en stap III (relatief) eenvoudig uit te voeren zijn, bepaalt de moeilijkheid van het uitvoeren van stap I de moeilijkheid van het uitvoeren van de gehele aanval.

## 5.4 Mogelijke aanvalsscenario's

37 Wij proberen hieronder de kosten in te schatten van twee mogelijke aanpakken:

A. Zelf een aanval realiseren.

B. Wachten tot de open source initiatieven ver genoeg gevorderd zijn.

### 5.4.1 Aanvalsscenario A - Zelf een aanval realiseren.

38 Zoals hierboven is geconcludeerd ligt de grootste uitdaging erin om een succesvolle aanval op te kunnen zetten in het ondervangen van het frequency hopping probleem. Iemand die nu aan een oplossing wil werken zal zeer veel expertise moeten hebben in draadloze communicatie en signaalverwerking in het algemeen en op het gebied van GSM in het bijzonder.

39 De financiële kosten voor de aanschaf van apparatuur zijn echter niet zeer groot. Er is geen reden om aan te nemen dat dit onevenredig duurder zou uit pakken dan de mogelijkheden die nu in de open source communities worden uitgewerkt, dat wil zeggen in de orde van een paar duizend euro. Als er echter ook expertise moet worden ingehuurd dan zal deze optie veel duurder uitvallen.

40 Het tijdspad tot aan het stadium waarin de aanval eenvoudig uitvoerbaar zal zijn is erg lastig in te schatten. Een echte expert die direct begint kan wellicht in enkele maanden dit stadium bereiken. Iemand die nog veel kennis en ervaring moet opdoen is daar veel langer mee bezig. Of mensen hier op dit moment mee aan het werk zijn en hoever zij zijn gevorderd is voor ons onbekend.

### 5.4.2 Aanvalsscenario B - Wachten tot de open source initiatieven ver genoeg gevorderd zijn.

41 Er zijn diverse open source initiatieven gestart die belangrijke componenten kunnen gaan leveren voor het onderscheppen van GSM signalen. Wij kunnen hierbij twee manieren onderscheiden:

B.1 PASSIEF, waarbij enkel geluisterd wordt naar bestaande GSM communicatie door de lucht.

B.2 ACTIEF, met een zogenaamde Man-in-the-Middle (MitM) aanval, waarbij de aanvaller over een gemanipuleerde telefoon en GSM gemanipuleerde zendmast beschikt. Deze gemanipuleerde zendmast simuleert het netwerk tegen de aan te vallen telefoon, en de gemanipuleerde telefoon simuleert deze telefoon tegen het echte netwerk, waardoor de aanvaller toegang heeft tot het spraak- en dataverkeer wat wordt doorgegeven tussen de gemanipuleerde telefoon en zendmast.

42 Complicatie bij een actieve aanval is dat de gemanipuleerde GSM zendmast de echte GSM zendmast moet overstemmen, en dus sterker en/of dichter in de buurt van de aangevallen telefoon moet zijn.

#### 5.4.2.1 B.1 - Wachten tot een passieve aanval mogelijk is.

43 Op dit moment lijkt de beste mogelijkheid om te wachten op ontwikkelingen in de AirProbe gemeenschap (zie Bijlage D). Wanneer hier het frequency hopping probleem wordt opgelost, wordt hiermee ook eenvoudig SMS onderscheppen mogelijk. De benodigde expertise om deze aanval dan op te zetten is laag.

44 De financiële kosten liggen rond de EUR 2.000,- voor de aanschaf van de USRP[9] 2, of de USRP 1 met extra FPGA[10]rekenkracht in combinatie met een standaard laptop en rond de 2 terabyte (TB) harde schijf ruimte (voor de *rainbow table*).

45 Een inschatting van het tijdspad naar aanleiding van de ontwikkelingen binnen AirProbe in de laatste maanden, is minimaal een paar jaar. De afgelopen maanden lijkt men hier op een dood punt aangekomen en wordt er weinig meer ontwikkeld. Het is natuurlijk altijd mogelijk dat er ineens grote vooruitgang wordt geboekt (bijvoorbeeld doordat een groep experts hier plotseling hard mee aan de slag gaat).

[9] Universal Software Radio Peripheral.
[10] Field Programmable Gate Array.

#### 5.4.2.2 B.2 - Wachten tot een actieve aanval mogelijk is.

46 Een aanvaller zou kunnen proberen om een klassieke Man-in-the-Middle (MitM) aanval op te zetten door zich voor te doen als authentieke zendmast naar de doel telefoon toe en zich voor te doen als de doel telefoon naar een authentieke zendmast toe[11].

47 Voor het zich voordoen als zendmast zijn al goed werkende open source mogelijkheden voorhanden (OpenBTS, OpenBSC), maar deze zijn er nog niet voor het zich voordoen als telefoon. Het open source project dat op dit moment hiermee bezig is, is het OsmocomBB project. Zij proberen een open source implementatie van de base-band processor te maken die moet functioneren op goedkope telefoon hardware. Wanneer dit project zijn doel haalt dan zou een aanvaller deze code kunnen combineren met de al bestaande projecten om een zendmast na te bootsen om een MitM aanval op te zetten. Deze twee componenten dienen dan nog wel eerst met elkaar te worden verbonden.

48 De benodigde expertise is in dit geval groter dan in het vorige voorbeeld, omdat beide aan elkaar te koppelen projecten niet bewust ontwikkeld zijn om op deze manier te combineren. Dit zal de nodige aanpassing en dus een brede kennis van het GSM protocol vergen, net als kennis van elektronica. Diepgaande theoretische kennis, zoals van alle benodigde signaalverwerking is hier echter niet meer bij nodig.

49 De financiële kosten zullen rond de EUR 3.000,- voor de aanschaf van een microBTS of een SIEMENS BS11 zendmast (beide worden ondersteund door OpenBSC), de OsmocomBB hardware, een standaard laptop en een 2TB aan harde schijf ruimte (wederom voor de *rainbow table*).

50 De ontwikkelingen in OsmocomBB gaan veel sneller dan in het eerder genoemde AirProbe. Wellicht zijn zij in staat op de CCC bijeenkomst in december 2010 een werkende demonstratie te tonen. Vanaf dat moment zou een aanvaller dus nog het OsmocomBB project aan het OpenBTS/OpenBSC project moeten kunnen koppelen. Het zal naar verwachting een expert op dat punt nog zeker een maand kosten om een soort proof-of-concept voor elkaar te krijgen.

## 5.5 Evaluatie van aanvalscenario's

51 De tabel hieronder geeft een ruw overzicht van de kosten, moeite, en expertise vereist voor een aanval:

[11] Door zich zo in het communicatiepad tussen de doel telefoon en de zendmast te plaatsen heeft de aanvaller toegang tot alle communicatie tussen beiden.

| Aanvalsscenario | Kosten aan apparatuur | Tijdsinspanning | Benodigde expertise |
|---|---|---|---|
| **A – zelf een aanval realiseren** | EUR 2.000 – EUR 3.000 | Manjaren | Extreem hoog |
| **B – wachten op open source gemeenschap** | EUR 2.000 – EUR 3.000 | Manmaanden (hierbij wordt dus niet de inspanning van de open source gemeenschap meegenomen in de schatting) | Hoog |

**Tabel 2 - Evaluatie aanvalscenario's**

Bij alle mogelijkheden hierboven zullen de financiële investeringskosten voor hardware en software in de orde van EUR 2.000 – EUR 3.000 zijn.

52 Ook in het slechtste geval, dat wil zeggen als de open source initiatieven de benodigde componenten leveren, zal er de nodige expertise en tijd voor nodig zijn om hiermee effectief een aanval op te zetten. Dit is niet iets wat de gemiddelde computerhobbyist gaat lukken, maar er zijn naar verwachting mensen te vinden in Nederland die dit kunnen, en dit willen demonstreren (bijvoorbeeld voor een actualiteitenprogramma op TV).

53 De expertise om zelf oplossingen te maken ter vervanging van deze open source oplossing (aanvalsscenario A) is extreem hoog, en is naar onze inschatting in Nederland niet aanwezig. Ook omdat succes zeker niet gegarandeerd is verwachten wij niet dat er mensen met dit soort activiteiten bezig zijn.

54 Schatten van het moment waarop het mogelijk zou worden GSM communicatie te onderscheppen en te ontsleutelen blijft lastig. De grote onbekende hierbij is de vooruitgang die geboekt gaat worden in open source projecten. In het meest ongunstige geval voor het Ministerie van Volksgezondheid, Welzijn en Sport zijn er binnen een jaar demonstraties van het onderscheppen van GSM verkeer, maar het is tevens mogelijk dat dit nog meerdere jaren zal duren.

55 Op dit moment lijkt de meeste vooruitgang te zitten in het OsmocomBB project, doordat updates in het laatste half jaar aan de AirProbe code schaars zijn. In het meest ongunstige geval voor het Ministerie van Volksgezondheid, Welzijn en Sport zou het toch waarschijnlijk nog een jaar moeten duren voordat deze OsmocomBB ontwikkeling leidt tot een demonstreerbare aanval.

56 Hoewel het tijdspad zeer lastig in te schatten is, zullen ontwikkelingen op dit gebied niet onaangekondigd plaatsvinden. Alle hierboven beschreven aanvallen zijn aanvallen op de wereldwijde GSM standaard. Aangezien er weinig tot geen Nederlandse inbreng is op dit gebied

in de hackersgemeenschap, zal een werkende aanval eerst onder de aandacht komen als generieke aanval op GSM. Deze ontwikkelingen zijn waarschijnlijk goed aan te zien komen door een organisatie als GOVCERT.

# 6 Context en risicobeoordeling SMS kwetsbaarheid

57 Als achtergrond wordt het gebruik van SMS in het EPD-DigiD op hoofdlijnen beschreven in Sectie 6.1. In Sectie 6.2 van dit hoofdstuk wordt het risico geanalyseerd dat verbonden is met de kwetsbaarheid in SMS bij het gebruik daarvan in EPD-DigiD.

## 6.1 Context gebruik SMS codes in EPD-DigiD

58 SMS codes worden, zoals nu voorzien in de context van het EPD-DigiD voor twee doeleinden gebruikt: (1) Authenticatie van zorgconsumenten en (2) Wachtwoordherstel. Deze worden hieronder kort toegelicht. SMS codes worden tevens gebruikt voor de bij de twee bovenstaande doeleinden noodzakelijke administratieve handelingen (bijvoorbeeld aanvragen, wijzigen).

### 6.1.1 Gebruik van SMS ten behoeve van authenticatie

59 EPD-DigiD gebruikt nadat de identiteit van de houder middels een face-to-face controle is vastgesteld hetzelfde authenticatiemechanisme als DigiD Midden. De face-to-face controle is voorzien bij TNT Postkantoren middels een document conform de Wet op de Identificatieplicht (WID), welke moet zijn voorzien van een leesbaar BSN nummer. Hierbij wordt aan de zorgconsument het tweede gedeelte van de activatiecode overhandigd die later (bijvoorbeeld thuis), in combinatie met zijn reeds eerder op het GBA adres ontvangen eerste gedeelte, kan worden gebruikt om zijn EPD-DigiD account te activeren.

60 Indien de zorgconsument zich vervolgens wil identificeren bij het patiëntenportaal dient deze allereerst de gebruikersnaam, vervolgens het wachtwoord en ten slotte de op de mobiele telefoon ontvangen SMS code op te geven. Slechts indien de combinatie gebruikersnaam, wachtwoord en SMS code correct zijn wordt de zorgconsument positief geauthenticeerd op EPD-DigiD niveau. De SMS code wordt alleen naar de mobiele telefoon verstuurd indien de opgegeven combinatie gebruikersnaam en wachtwoord correct is.

### 6.1.2 Gebruik van SMS ten behoeve van Wachtwoordherstel

61 In 2007 heeft Logius de functie Wachtwoordherstel toegevoegd aan DigiD. Middels Wachtwoordherstel is het mogelijk om, zonder een nieuw DigiD aan te vragen, het wachtwoord van het betreffende DigiD account te resetten. Dit is alleen mogelijk voor het niveau EPD-Digid indien de DigiD houder een Nederlands mobiel nummer en een e-mailadres heeft opgegeven. Bij een vergeten wachtwoord kan de houder Wachtwoordherstel activeren. Het is vooralsnog voorzien Wachtwoordherstel ook voor het EPD-DigiD toe te passen.

62 Het volgende proces wordt vervolgens doorlopen:

1. De houder geeft aan dat het wachtwoord is vergeten door BSN en DigiD gebruikersnaam in te vullen.

2. De houder beantwoordt de zelf geselecteerde spiegelende vraag correct.

3. DigiD stuurt een e-mail met daarin een gepersonaliseerde link naar de reset website.

4. De houder surft naar de via e-mail ontvangen gepersonaliseerde link en vult zijn gebruikersnaam en BSN nummer in;

5. DigiD stuurt daarna een SMS met daarin een activatiecode naar het mobiele nummer van de houder;

6. De houder voert de via SMS ontvangen activatiecode in.

7. Indien de activatiecode correct is wordt de houder gevraagd een nieuw wachtwoord in te voeren en is het wachtwoord gereset.

63 Indien wordt aangenomen dat de SMS door de aanvaller te onderscheppen is, is hiermee, voor de DigiD houders die Wachtwoordherstel hebben geactiveerd, in feite de bescherming van het wachtwoord equivalent met de beschikking hebben over de in-box van het bij DigiD opgegeven e-mailadres én het antwoord kennen op de spiegelende vraag.

## 6.2 Risicobeoordeling SMS kwetsbaarheid

64 Op basis van de interviews, komen wij tot drie bedreigingen gerelateerd aan de kwetsbaarheid die wij onderstaand toelichten:

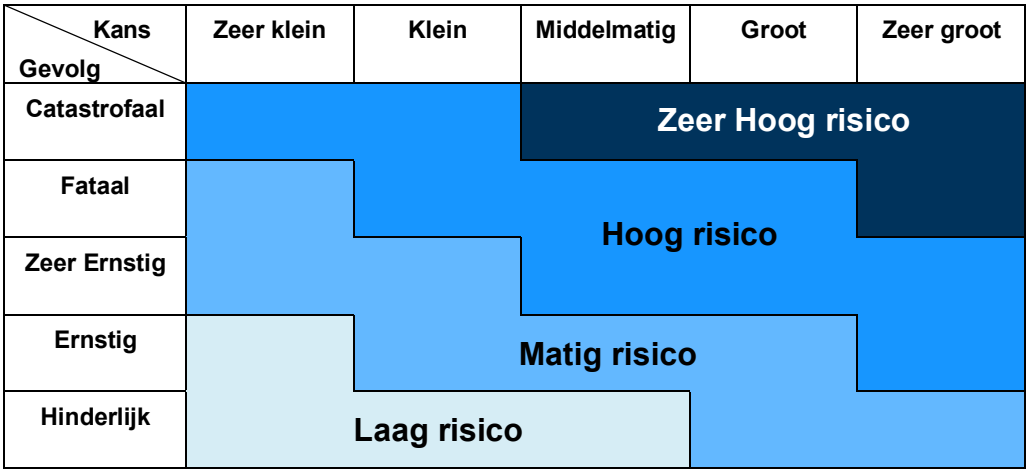
1. Daadwerkelijk verlies van (vertrouwelijkheid van) informatie.
2. Verlies van het publiek vertrouwen in het landelijk EPD.
3. Non-compliance met regelgeving.

65 Voor deze bedreigingen is het risico geschat conform Figuur 1 van de Nederlandse norm NEN 7512. Daarbij kent deze norm de volgende betekenis toe aan de Kans en Gevolgen van bedreigingen:

Kans:
- zeer klein (verwaarloosbare mogelijkheid van optreden);
- klein (zou kunnen optreden, maar zal in vrijwel alle gevallen niet optreden);
- middelmatig (mogelijk; optreden niet onwaarschijnlijk);
- groot (zeer goed mogelijk; zal in een groot deel van de gevallen optreden);

- zeer groot (zal zeker of vrijwel zeker optreden).

Impact:
- hinderlijk (eenvoudig herstelbaar);
- ernstig (moeilijk herstelbaar);
- zeer ernstig (niet herstelbaar);
- fataal (voor een patiënt);
- catastrofaal (fataal voor meer patiënten).




**Figuur 1 - NEN 7512 risicotabel**

66 Zoals uit de tabel blijkt, onderscheidt deze opzet vier soorten risico's voor een organisatie: Zeer Hoog, Hoog, Matig en Laag. Daarbij kunnen risico's aangemerkt als Laag in beginsel zonder nadere motivering worden geaccepteerd door de organisatie en kunnen risico's aangemerkt als (Zeer) Hoog in beginsel niet worden geaccepteerd. Risico's aangemerkt als Matig kunnen worden geaccepteerd door de organisatie mits dit bewust gebeurt en vergezeld wordt van een motivering.

## 6.3 Daadwerkelijk verlies van (vertrouwelijkheid van) informatie

67 De (gekraakte) SMS code wordt, door een kwaadwillende, gebruikt om zich als zorgconsument te authenticeren en om zo vervolgens, indien dit succesvol is, toegang te krijgen tot de medische gegevens in het landelijk EPD van de zorgconsument.

68 Aangezien het gevolg niet herstelbaar is (dat is immers met vertrouwelijkheid niet mogelijk), maar ook niet fataal (er kunnen namelijk geen medische gegevens worden gewijzigd via het patiëntenportaal), schatten wij, conform de gekozen methodiek, dit in als **Zeer Ernstig**.

69 Tegelijkertijd schatten wij de kans dat deze bedreiging zich voordoet bij een individuele patiënt in als **Klein**. Hierbij geldt de volgende motivering:

1. Het is noodzakelijk, voordat succesvol kan worden geauthenticeerd, om ook beschikking te hebben over het wachtwoord of het e-mailadres en antwoord op de spiegelende vraag (in het geval dat Wachtwoordherstel is geactiveerd). Dit verkleint de kans dat de aanval succesvol kan worden uitgevoerd

2. In vergelijking met overige aanvallen is het onderscheppen van SMS een relatief bewerkelijk aanvalspad. Gerichte aanvallen op iemands medische gegevens die via het patiëntenportaal opvraagbaar zijn lijken veel waarschijnlijker via al bestaande aanvalsmogelijkheden, zoals een rechtstreekse aanval op de computer die een slachtoffer gebruikt, spyware te installeren op de telefoon van het slachtoffer, of gewoon die telefoon te stelen.

3. Als laatste moet de aanval per zorgconsument worden herhaald en is het door deze kwetsbaarheid niet mogelijk in één keer medische gegevens van meerdere patiënten in te zien.

70 Als gevolg van een **Zeer Ernstig** gevolg en een **Kleine** kans schatten wij (conform Figuur 1 van de norm NEN 7512) het totale risico van deze bedreiging in als **Matig**.

| | |
|---|---|
| **Kans** | **Klein** |
| **Gevolg** | **Zeer Ernstig** |
| **Risico** | **Matig** |

**Tabel 3 - Risicoschatting Verlies Gegevens**

## 6.4 Verlies van publiek vertrouwen in het landelijk EPD

71 Naast het daadwerkelijke verlies van (vertrouwelijkheid van) informatie is voor het landelijk EPD tevens het publiek vertrouwen in de veiligheid van het landelijk EPD van groot belang. Dit gezien de grote politieke gevoeligheid van het onderwerp. Zodra GSM ‘gekraakt’ wordt zal het immers een kwestie van tijd zijn voordat ook in Nederland gedemonstreerd wordt dat een EPD-DigiD SMS kan worden onderschept.

72 Indien het publiek vertrouwen in het landelijk EPD sterk vermindert, dan wel geheel verloren gaat, zal het zeer moeilijk zijn dit te herstellen. Voor de nabije toekomst kan dit betekenen dat het patiëntenportaal geen doorgang vindt. Daarom schatten wij het gevolg in op **Ernstig** of mogelijk **Zeer Ernstig**.

73 Aangezien slechts één onderschepte SMS in beginsel genoeg is en het een kwestie van tijd is voordat GSM zal worden gekraakt, schatten wij de kans hierop in als **Zeer Groot**.

74 Als gevolg van een **Ernstig/Zeer Ernstig** gevolg en een **Zeer Grote** kans schatten wij (conform Figuur 1 van de norm NEN 7512) het totale risico van deze bedreiging in als **Hoog / Zeer Hoog**.

| | |
|---|---|
| **Kans** | **Zeer Groot** |
| **Gevolg** | **Ernstig/Zeer Ernstig** |
| **Risico** | **Hoog / Zeer Hoog** |

**Tabel 4 - Risicoschatting verlies van publiek vertrouwen in het landelijk EPD**

## 6.5 Non-compliance met regelgeving

75 In het rapport *"Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)"* is geconcludeerd dat het Authenticatieniveau van het authenticatiemiddel voor toegang van zorgconsumenten tot het landelijk EPD **Sterk** dient te zijn. In het geval van gebruik van een fysiek middel (waaronder de SIM kaart in de mobiele telefoon wordt gerekend) zegt de norm NEN 7512 daar het volgende over:

*"De authenticatiesterkte wordt bij toepassing van een fysiek authenticatiemiddel bepaald door het geheel van de processen waarin het wordt gebruikt. Sterke authenticatie is mogelijk, mits het middel wordt gebruikt in combinatie met wachtwoord of PIN-code, of in combinatie met biometrie. Echter alleen wanneer ook bij het initialiseren van het authenticatiemiddel en de uitreiking aan de houder wordt gewaarborgd dat het eenduidig aan de houder wordt gebonden, biedt het geheel het authenticatieniveau: **Sterk**.*

*Is aan deze voorwaarden niet voldaan, dan is het authenticatieniveau ten hoogste: **Matig**."*

76 Indien de kwetsbaarheid niet wordt gemitigeerd of weggenomen en dus een SMS met authenticatiecodes kan worden onderschept zonder in bezit te zijn van het fysieke middel (namelijk de mobiele telefoon met daarin de SIM kaart), wordt er niet langer aan de NEN 7512 norm voldaan. Hierdoor is het patiëntenportaal niet in conformiteit met de NEN 7512 norm. In een brief (getiteld "Identificatie en authenticatie bij toegang patiënt tot het EPD" dd. 7 augustus 2008) rond het EPD aan het Ministerie van Volksgezondheid, Welzijn en Sport stelt het CBP geen expliciete eisen aan het EPD authentiatiemiddel maar stelt dat het gebruik van "two factor

authentication voor de hand ligt". Dit is in lijn met de eisen die NEN 7512 stelt aan een 'sterk' authenticatiemiddel'; het niet (meer) voldoen aan deze eisen kan aldus betekenen dat niet wordt voldaan aan de eisen die het CBP stelt.

77 De kans dat deze niet-conformiteit optreedt schatten wij als **Zeer Groot** in en het gevolg daarvan als Ernstig. Dit leidt daarmee tot een **Hoog** risico.

| Kans | Zeer Groot |
|---|---|
| Gevolg | Ernstig |
| Risico | Hoog |

**Tabel 5 - Risicoschatting Non-compliance**

## 6.6 Conclusie

78 De bedreigingen en risico inschattingen zijn in de volgende tabel samengevat:

| Bedreiging | Risico |
|---|---|
| Verlies gegevens | Matig |
| Publiek vertrouwen | Hoog/Zeer Hoog |
| Non-compliance | Hoog |

**Tabel 6 - Risicoschatting Bedreigingen**

79 Als gevolg van deze risico-inschattingen zijn additionele maatregelen noodzakelijk. Deze worden in het volgende hoofdstuk onderzocht.

# 7 Risicobehandeling

80 In dit hoofdstuk beschouwen wij mogelijke mitigerende maatregelen die kunnen worden getroffen om het beveiligingsniveau van het EPD-DigiD te verhogen. Hierbij geven wij per mogelijke maatregel aan in hoeverre deze het risico van de in Hoofdstuk 5 geïdentificeerde bedreigingen reduceren.

81 Op basis van interviews en de ervaring binnen PwC en RU komen wij tot de volgende mitigerende maatregelen die toegepast kunnen worden.

## 7.1 Mitigerende maatregelen

### 7.1.1 Versterkte encryptie GSM/SMS verkeer

82 Een tegenmaatregel die de Nederlandse telecommunicatie operators tegen het afluisteren van GSM verkeer zouden kunnen nemen is het overstappen van het huidige versleutelingalgoritme, A5/1, naar de nieuwe variant A5/3. De GSM Association heeft dit al jaren geleden geadviseerd, maar de telecommunicatie operators hebben deze stap tot nu toe nog niet genomen. Dit is een maatregel op langere termijn en is vergelijkbaar met de langzame overstap van zorgconsumenten op het tot nu toe nog veilig geachte UMTS.

83 Voor het gebruik van A5/3 is het noodzakelijk dat de telecommunicatie operators dit implementeren in hun infrastructuur en dat de GSM toestellen van de gebruikers dit ook ondersteunen. Met name het laatste punt is een aandachtpunt. Zelfs al zouden alle Nederlandse telecommunicatie operators A5/3 implementeren, dan nog is de vraag op welke termijn ondersteuning van de GSM toestellen van de gebruikers voldoende gemeengoed is om te kunnen stellen dat de maatregel voldoende effectief is. Hierbij moet ook de (naar waarschijnlijkheid) aanwezige mogelijkheid automatisch terug te vallen op A5/1 kritisch worden bekeken.

84 Versterkte encryptie neemt in opzet de SMS kwetsbaarheid weg.

85 Een praktisch probleem is dat de migratie door de Nederlandse telecommunicatie operators naar A5/3 niet afgedwongen kan worden door het Ministerie van Volksgezondheid, Welzijn en Sport en dat er zeer waarschijnlijk een fall-back optie naar A5/1 door de telecommunicatie operators zal worden ondersteund. Met name doordat het vele jaren kan duren voordat de (‘oude’) GSM toestellen die geen A5/3 ondersteunen uitgefaseerd zijn, is ook deze maatregel pas effectief over een flink aantal jaren.

### 7.1.2 eNIK/eDL

86 Deze maatregel is gebaseerd op het beschikbaar komen van een Elektronische Identiteitskaart (eNIK), een Elektronisch Rijbewijs met eID functionaliteit (electronic Drivers Licence - eDL) of UZI-pas voor alle zorgconsumenten. Deze authenticatiemiddelen zouden vervolgens in EPD-DigiD kunnen worden gebruikt als alternatief voor de SMS daarmee de kwetsbaarheid daarin wegnemend.

87 Echter deze maatregel zal naar verwachting gepaard gaan met zeer grote investeringen en operationele kosten, aangezien naast de passen tevens lezers en software moeten worden uitgegeven. Hierdoor is beschikbaarheid van dit middel moeilijk te voorzien. Voor een verdere beschrijving verwijzen wij naar het rapport *"Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)"*.

88 Voor zover wij konden vaststellen is er nog geen concrete planning voor de uitgifte van de eDL. Voor de eNIK is de mogelijkheid tot realisatie opgenomen in de aanbestedingsvoorwaarden rondom de nationale identiteitskaart. De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties zal de Kamer dan ook zo snel mogelijk informeren wanneer de eNIK operationeel kan zijn (referentie: Tweede Kamer "Vragenuur inloggen op DigiD niet waterdicht", d.d. 13 april 2010). Omdat het kan enige tijd duren voordat de populatie uitgegeven kaarten voldoende groot is, is de verwachting dat deze oplossing pas over meerdere jaren operationeel zal kunnen zijn. Daarnaast is de verspreidingsgraad van zowel de identiteitskaart als het rijbewijs mogelijk onvoldoende hoog.

89 Voor een verdere beschrijving verwijzen wij naar het rapport *"Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)"* waar deze maatregel als alternatief werd geopperd.

### 7.1.3 RTDA

90 Deze maatregel is gebaseerd op het gebruik van het Elektronische Paspoort als extra fysiek middel in aanvullign op DigiD Midden. Deze authenticatiemiddelen zouden vervolgens in EPD-DigiD kunnen worden gebruikt en daarmee de kwetsbaarheid daarin wegnemend.

91 Elektronische Paspoorten worden sinds 2006 uitgegeven. Hierdoor zullen vanaf 2011 alle in omloop zijnde paspoorten dit ondersteunen. Om het zorgconsumenten mogelijk te maken vanuit huis hiervan gebruik te maken dienen er wel contactloze lezers worden verstrekt. Daarom zal deze maatregel naar verwachting gepaard gaan met grote investeringen en operationele kosten. Daarnaast is de verspreidingsgraad van paspoorten op dit moment niet zeer hoog. Voor een verdere beschrijving verwijzen wij naar het rapport *"Beveiligingeisen ten aanzien van identificatie*

*en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)"* waar deze maatregel als alternatief werd geopperd.

### 7.1.4 Persoonlijke conversietabel SMS codes

92 Om een extra controle in te bouwen kan aan zorgconsumenten een zogenaamde persoonlijke conversietabel voor de ontvangen SMS codes worden uitgereikt als onderdeel van het registratie en uitgifteproces. Hierbij krijgt iedere zorgconsument een tabel met voor ieder karakter een conversie naar een ander karakter. De zorgconsument dient bij het ontvangen van een SMS code ieder karakter te converteren volgens zijn persoonlijke tabel en deze op de DigiD website in te voeren. In Bijlage A van dit rapport hebben wij dit verder toegelicht.

93 Een conversietabel versterkt het authenticatiemiddel, omdat de aanvaller naast het onderscheppen van de SMS code dan tevens de beschikking moet hebben over de conversietabel. Feitelijk voert de zorgconsument handmatig een extra versleuteling uit op de ontvangen SMS code, daarmee de beveiliging van het authenticatiemiddel versterkend.

94 Het gebruik van een persoonlijke conversietabel moet gezien worden als een oplossingsrichting die in een vervolgonderzoek verder moet worden uitgewerkt. Aandachtpunten daarbij zijn ondermeer:

- Op welke wijze de conversietabel wordt uitgereikt binnen het registratie en uitgifteproces.
- De grootte en keuze van de karakterset en de lengte van de code.
- De wijze waarop de methode voldoende gebruikersvriendelijk kan worden toegepast. Dit is ook gerelateerd aan het vorige punt. Daarbij kan bijvoorbeeld overwogen worden gebruikerstesten uit te voeren met conversietabellen.
- De wijze waarop - in samenspraak met Logius - conversietabellen veilig kunnen worden gegenereerd en het gebruik daarvan kan worden ingepast in DigiD.
- De fasering waarbinnen de conversietabellen worden uitgegeven, ingezet en gedeactiveerd.

95 Een ander aandachtspunt is de planning: de conversietabellen kunnen in principe worden uitgegeven vanaf de start van het EPD-DigiD of op een later tijdstip als reactie op het beschikbaar komen van exploitatie tools. Bij de eerste opzet kan ook nog worden gekozen om het daadwerkelijk gebruik uit te stellen als reactie op het beschikbaar komen van exploitatie tools. Tot de-activatie van het gebruik van de conversietabel kan worden besloten als bijvoorbeeld het gebruik van A5/3 voldoende gemeengoed is.

96 De inschatting met betrekking tot de restrisico's is dat deze voor alle drie de bedreigingen worden gereduceerd tot **Matig**: de gevolgen blijven ongewijzigd, maar de kans van voorkomen is tot **Klein** gereduceerd. Een voordeel is dat deze maatregel geheel zelfstandig door het Ministerie van

Volksgezondheid, Welzijn en Sport kan worden genomen, aangezien zij opdrachtgever van het EPD-DigiD is.

### 7.1.5 TAN code lijsten

97 Deze maatregel behelst het uitgeven van een lijst met persoonlijk unieke codes (Transaction Authentication Number of TAN) voorzien van een volgnummer. Feitelijk vervangen deze de codes die in het EPD-DigiD via SMS worden gestuurd. Na een succesvolle initiële DigiD authenticatie middels gebruikersnaam en wachtwoord dient de zorgconsument vervolgens de correcte TAN code (geïdentificeerd middels het volgnummer) in te voeren om de authenticatie succesvol te doorlopen. Voor een volgende authenticatie(poging) dient de TAN code met het opvolgende volgnummer te worden gebruikt.

98 Deze persoonlijke TAN codes zijn een vorm van One-Time-Passwords (OTP), aangezien de zorgconsument deze slechts eenmaal voor een authenticatiepoging kan gebruiken. Voor een betrouwbare uitgifte dient deze lijst direct na een face-to-face controle te worden uitgegeven aan de zorgconsument. Een beheersmatig probleem bij TAN codes is dat een nieuwe lijst met TAN codes moet worden verstrekt aan de zorgconsument zodra de oude uitgeput is. Dit probleem introduceert ook additionele beveiligingsrisico's rond de verstrekking van de nieuwe lijsten.

99 Een fundamenteel nadeel ten opzichte van tokens en mobiele telefoons als fysiek authenticatiemiddel is dat de TAN code lijst eenvoudig (en mogelijk zonder dat de zorgconsument dit bemerkt) kan worden gekopieerd. Deze eigenschap wordt niet expliciet geëist van een fysiek authenticatiemiddel in de zin van de Nederlandse norm NEN 7512 maar de voorbeelden impliceren dit wel. In praktische zin introduceert het gebruik van TAN codes in vergelijking met het gebruik van SMS, nieuwe risico's als gevolg van het gebruik van maar één kanaal (namelijk het internet).

100 Hiermee wordt het restrisico van de non-compliance bedreiging onvoldoende teruggebracht. De kans van voorkomen op dit punt schatten wij onverminderd als **Zeer Groot** in en daarmee het restrisico als **Hoog**.

### 7.1.6 Versterking DigiD wachtwoorden

101 Bij deze maatregel worden in DigiD extra beveiligingseisen afgedwongen bij de gebruiker zoals lengte en complexiteit.

102 Hoewel dit wel het algehele beveiligingsniveau van (EPD-)DigiD ten goede komt kan deze maatregel niet in voldoende mate de restrisico's van de geïdentificeerde bedreigingen reduceren. De non-compliance bedreiging wordt met deze maatregel immers niet geadresseerd. Onze

inschatting met betrekking tot de restrisico's is dat deze voor deze bedreiging niet worden gereduceerd en **Hoog** blijven.

### 7.1.7 Zodra de kwetsbaarheid (bijna) exploiteerbaar is het EPD-DigiD stopzetten.

103 Deze maatregel is reactief van aard. Hierbij worden de ontwikkelingen in de open source gemeenschap goed in de gaten gehouden. Zodra er indicaties zijn dat de kwetsbaarheid (bijna) exploiteerbaar is, wordt het EPD-DigiD stopgezet door het Ministerie van Volksgezondheid, Welzijn en Sport. Punt daarbij is of het Ministerie van Volksgezondheid, Welzijn en Sport op tijd is, zowel in praktische zin als in de perceptie van het publiek.

104 Deze maatregel kan worden ingericht door contact te onderhouden met GOVCERT, eventueel aangevuld met overige expertisecentra op dit gebied. Verder moet er een volledig draaiboek klaarliggen in geval bovengenoemde situatie zich voordoet.

105 Deze reduceert de risico's doordat de kans van voorkomen wordt gereduceerd. Maar onze inschatting is dat het restrisico **Hoog** is: rond de bedreiging 'Publiek vertrouwen' blijft het gevolg ongewijzigd, maar daalt de kans van voorkomen naar **Middelmatig**.

## 7.2 Samenvatting restrisico's maatregelen

106 In onderstaande tabel is de schatting van de restrisico's per maatregel schematisch weergegeven:

| Maatregel | Bedreigingen | | | Inschatting beschikbaarheid |
|---|---|---|---|---|
| | Verlies gegevens | Publiek vertrouwen | Non-compliance | |
| **Huidige situatie (ter referentie)** | **Matig** | **Hoog/Zeer Hoog** | **Hoog** | Direct |
| **Versterkte[12] encryptie GSM/SMS** | **n.v.t.*** | **n.v.t.*** | **n.v.t.*** | > 5 jaar |
| **eNIK/eDL[12]** | **n.v.t.*** | **n.v.t.*** | **n.v.t.*** | > 5 jaar |
| **RTDA[12]** | **n.v.t.*** | **n.v.t.*** | **n.v.t.*** | < 2 jaar |
| **Persoonlijke conversietabel SMS codes** | **Matig** | **Matig** | **Matig** | < 1 jaar |
| **TAN code lijsten** | **Matig** | **Matig** | **Hoog** | < 1 jaar |
| **Versterking DigD wachtwoorden** | **Matig** | **Matig** | **Hoog** | < 6 maanden |
| **Zodra de kwetsbaarheid (bijna) exploiteerbaar is het EPD-DigiD stopzetten** | **Matig** | **Hoog** | **Matig** | Direct |

**Tabel 7 - Restrisico's per maatregel**

107 Bovenstaande inschattingen rond de beschikbaarheid zijn de onze; overleg met betrokken partijen hierover maakte geen onderdeel uit van de opdracht.

[12] Deze maatregelen zijn een alternatief voor SMS zoals in dit onderzoek onderzocht zodat restrisico's rond de onderzochte SMS kwetsbaarheid geen betekenis hebben.

# A Detail uitwerking persoonlijke SMS conversietabel

108 Hier geven wij een voorbeeld voor een SMS conversietabel gebaseerd op de huidig gekozen opzet van SMS codes. In de huidige, voorziene situatie wordt uitgegaan van SMS codes uit een set van 31 karakters (23 hoofdletters behalve de I, L en O en de cijfers behalve 0 en 1).

109 Als onderdeel van het EPD-DigiD registratieproces wordt aan de zorgconsument een geprinte conversie tabel overhandigd, die onderstaand geïllustreerd is. Elke conversietabel is zorgconsument specifiek.

| A | B | C | D | E | F | G | H | J | K | M | N | P | Q | R | S | T | U | V | W | X | Y | Z | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| p | q | r | 4 | y | 3 | g | 9 | s | 8 | k | t | 4 | 6 | 7 | m | a | 5 | N | h | 2 | j | w | x | f | e | z | v | u | c | b |

**Tabel 8 - Voorbeeld conversietabel**

110 De gedachte is dat de zorgconsument bij ontvangst van de SMS niet de code zelf intypt op de betreffende DigiD webpagina, maar de conversie. Dus als de SMS code is

U-8-K-R-Z-N-7-Z

111 dan is de geconverteerde code:

5-c-8-7-w-t-u-w

112 Dus dan moet ‘5-c-8-7-w-t-u-w’ worden ingevoerd op de webpagina.

113 Om dit proces te vergemakkelijken voor zorgconsumenten, suggereren wij dat de SMS karakter set en de in te typen karakter set in grote mate verschillend zijn, zodat de DigiD applicatie de zorgconsument kan informeren als deze de SMS code intypt in plaats van de geconverteerde. Een voorbeeld hiervan is dat de ontvangen code bestaat uit slechts cijfers, die geconverteerd moeten worden naar een code bestaand uit slechts letters.

114 Verder kan overwogen worden de zorgconsument zowel de SMS code zelf als de geconverteerde code in te laten typen om op die manier het proces goed te kunnen begeleiden.

# B Geraadpleegde personen

115 In het kader van deze risicoanalyse hebben wij gesprekken gevoerd met de volgende personen (titulatuur toegevoegd voor zover bekend):

## B.1 Ministerie van Volksgezondheid, Welzijn en Sport

- mevrouw drs. E. Maat MPA
- de heer drs. M. Bosch RE

## B.2 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

- de heer mr. L. Oberendorff
- de heer drs. J. Timmermans

## B.3 Logius

- de heer W. Geurts
- de heer M. Claessen

## B.4 GOVCERT

- de heer T. Slewe

# C Onderzoeksteam

116 Het team bestond uit een samenwerkingsverband tussen PricewaterhouseCoopers Advisory N.V. en het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen.

## C.1 PricewaterhouseCoopers Advisory N.V.

- prof. dr. E.R. Verheul CISA CISSP
- ir. J.P. Prins FRM
- ir. O.A. Vermeulen RE FRM CISSP
- A.J.M. de Bruijn RE RA

## C.2 Institute for Computing and Information Sciences - Radboud Universiteit Nijmegen

- dr. E. Poll
- F. van den Broek MSc.

# D Open initiatieven rond GSM en diens beveiliging

## D.1 USRP

117 De USRP (Universal Software Radio Peripheral) is een open-hardware apparaat ontwikkeld door Matt Ettus. Het hieromheen opgerichte bedrijf Ettus Research (www.ettus.com) verkoopt dit.

118 Het is een hardware component dat gespecialiseerd is in het opvangen en digitaliseren van radio golven, welke vervolgens naar een computer kunnen worden doorgestuurd. Via bepaalde insteekmodulen (zogenaamde dochterborden) en andere antennes kan een bepaald deel van het radio spectrum worden gedigitaliseerd. De aansturing gebeurt door middel van open-source software (Gnu Radio).

## D.2 GNU Radio (http://gnuradio.org)

119 GNU Radio is een open source software toolkit, uitgebracht onder een open source licentie (GPL), voor het implementeren van software-radio's. Het werkt met verschillende typen hardware samen, zoals geluidskaarten, maar wordt vooral gebruikt in combinatie met de USRP. GNU Radio is in de basis een bibliotheek met allerlei standaard signaal bewerkingsfuncties. GNU Radio werkt op zichzelf niet als GSM sniffer, maar zowel AirProbe, als OpenBTS en OpenBSC gebruiken de GNU Radio code als basis.

## D.3 AirProbe (https://svn.berlin.ccc.de/projects/airprobe/wiki)

120 AirProbe is een open source project gericht op het maken van een analyse tool voor de GSM frequenties. Momenteel kan het slechts 1 frequentie per keer beluisteren en analyseren. Doordat AirProbe nog niet in staat is het frequency hopping van het GSM verkeer te volgen is het nog niet in staat een gesprek af te luisteren.

## D.4 OpenBTS (http://openbts.sourceforge.net/)

121 Een open source implementatie van een GSM zendmast (BTS). In combinatie met een USRP en GNU Radio kan hiermee een GSM zendmast worden gesimuleerd.

## D.5 OpenBSC (http://openbsc.osmocom.org/trac/wiki/OpenBSC)

122 Een open source implementatie van een zendmast controller (BSC). Op dit moment ondersteund deze implementatie twee soorten zendmasten, de SIEMENS BS-11 en de nanoBTS. De software draait op een computer en kan dan een GSM zendmast besturen. Dit project werkt niet samen met het OpenBTS project, maar is in feite een alternatief voor OpenBTS.

## D.6 OsmocomBB (http://bb.osmocom.org/trac/)

123 OsmocomBB is een Open Source GSM Baseband software implementatie. Het probeert de volledige verwerking van de laagste niveau GSM signalen (de baseband processing) in een telefoon te implementeren. Wanneer dit werkt is het mogelijk een volledig open source telefoon te ontwikkelen.

## D.7 A5/1 kraak project (http://www.reflextor.com/trac/a51)

124 A5/1 is de encryptie die in Nederland op het GSM netwerk wordt gebruikt. In augustus 2009 werd dit project gestart om zogenaamde rainbow tabellen uit te rekenen die het kraken van A5/1 veel makkelijker maken. Aan deze tabellen kan iedereen thuis meerekenen en ze worden vervolgens gepubliceerd via torrents. Momenteel heeft dit project nog geen code vrijgegeven om de gepubliceerde tabellen ook echt te gebruiken.