Miinisterie van Binnenlandse Zaken en
Koninkrijksrelaties
T.a.v. Logius
impulseid@logius.nl

Onze referentie	Uw referentie	Datum
Wet generieke digitale infrastructuur (Wet GDI) Uniforme Set van Eisen 1.0 d.d. 15-12-2016	Uniforme Set van Eisen 1.0 d.d. 15-12-2016	30/03/2017

Onderwerp
Zorgen om ontwerp van de Wet GDI, inbegrepen de Memorie van toelichting en de Uniforme Set van Eisen: 'Polymorphic Encryption and Pseudonymisation' (PEP)

Geachte heer, mevrouw,

Het ontwerp van de Wet Generieke Digitale Infrastructuur (GDI) en de aan dit wetsvoorstel toegevoegde Uniforme Set van Eisen geven mij reden, mijn ernstige bezwaren daartegen in dit schrijven uiteen te zetten.

Mijn bezwaren zijn gestoeld op de ervaringen die ik als CTO van AET Europe in de afgelopen decennia heb opgedaan. AET Europe is een Nederlands bedrijf dat al bijna 20 jaar succesvol is bij het leveren van strikt beveiligde eID oplossingen. Deze oplossingen worden breed binnen de Nederlandse overheid (onder meer Rijkspas en Defensiepas) toegepast alsmede in de Nederlandse zorgsector (UZIpas). Daarnaast exporteert AET wereldwijd deze in Nederland ontwikkelde en toegepaste technologie voor eID toepassingen in de verschillende sectoren, onder meer ter beveiliging van het internationale betalingsverkeer tussen banken. Onze eID oplossingen voor sterke authenticatie en digitaal ondertekenen worden door miljoenen gebruikers dagelijks toegepast.

Waarom maken wij ons zorgen?
Het wetsvoorstel Generieke Digitale Infrastructuur (Wet GDI) gaat uit van recente EU verordeningen. Dat is een zeer verstandige keuze. De Wet GDI bevat daarmee een grondslag om bij algemene maatregel van bestuur open standaarden aan te wijzen die overheden dienen te hanteren in het elektronisch verkeer met andere overheden, met burgers en met bedrijven. De Wet GDI bevat verder een verstrekkend voorstel waarin aansluiting in beginsel verplicht wordt gesteld. Hoewel tegen deze uitgangspunten geen enkel principieel bezwaar bestaat, schieten zowel de Wet GDI als de Uniforme Set van Eisen ernstig te kort.

A.E.T. Europe B.V., IJsselburcht 3, NL-6825 BS Arnhem, P.O. Box 5486, NL-6802 EL Arnhem, The Netherlands
Tel: +31 (0)26 3653350, Fax: +31 (0)26 3653351, Email: info@aeteurope.com, http://www.aeteurope.com
V.A.T.: 8092.26.820.B.01, Chamber of Commerce: 09114089

Moderne, veilige, digitale communicatie tussen overheid, burgers en bedrijven is zeer belangrijk en wordt steeds belangrijker. De nationale veiligheidsstrategie schaart de digitale communicatie tussen overheid en burgers dan ook onder de "vitale belangen"[1]. De wet GDI heeft verstrekkende gevolgen voor deze communicatie voor de komende 15 jaar. Daarnaast heeft invoering van de wet GDI aanzienlijke – onbekende - financiële gevolgen voor aanvragers.

De vereiste zorgvuldigheid wordt niet herkend in het huidige voorstel. In dit schrijven worden de bezwaren toegelicht. De zorgen betreffen allereerst de risicovolle uitgangpunten, de inzet van buitenlandse marktpartijen en het te voorziene gebruik van een verouderd algoritme. Ook is het wetsvoorstel in strijd met relevante beleidsuitspraken van de Europese Unie en van de Autoriteit Persoonsgegevens. Daarmee is de juridische grondslag van de Wet GDI ontoereikend.

Risicovol uitgangspunt: de "polymorfe identiteit"
Om te komen tot een toekomstvast stelsel open standaarden is de keuze voor de juiste eisen van zeer groot belang. Dit belang is des te groter, omdat het als gevolg van de Wet GDI in te voeren stelsel dient te voldoen aan aanzienlijk zwaardere beveiligingseisen dan de huidige stelsels (zoals DigiD). Zowel de memorie van toelichting als de Uniforme Set van Eisen spreekt over "Polymorphic Encryption and Pseudonymisation" (PEP) als middel om veilig gebruik te kunnen maken van de generieke data infrastructuur (GDI). PEP bestaat op dit moment alleen als theoretisch concept. PEP is dan ook uiterst risicovol, omdat de techniek nog nergens wordt toegepast en niet is gecertificeerd door een onafhankelijke instantie. Bovendien wijkt PEP af van gangbare internationale concepten.

Inzet van een buitenlandse marktpartij in een Proof of Concept van PEP
In september 2016 is op de Radboud universiteit begonnen met een "Proof of Concept"(PoC) genaamd *'Parkinson op Maat'*. Dit is de eerste keer dat PEP zal worden gebruikt in een operationeel IT systeem. Deze PoC heeft een geringe omvang van 650 patiënten[2] en heeft daarnaast een zeer beperkte doelstelling: analyse van patiëntgegevens ten behoeve van wetenschappelijk onderzoek. Er is op dit moment niet bij mij bekend of deze PoC al werkt. Ook is deze PoC op dit moment geen enkele realistische basis voor de Wet GDI. Immers, er is nog niets bekend over de robuustheid en schaalbaarheid van het toegepaste algoritme[3]. Het in het kader van de Wet GDI te ontwikkelen stelsel is immers bedoeld voor een groot aantal toepassingen. De PoC Parkinson op Maat is daarom niet representatief.

Daarnaast wekt het bevreemding, dat de PoC wordt uitgevoerd door het buitenlandse bedrijf Verily Life Sciences (voorheen bekend onder Google Life Sciences)[4]. Dat is in strijd met het Nederlandse beleid, omdat uitwerking van PEP een fundamenteel onderdeel is van de vitale infrastructuur van Nederland. Immers, PEP is de beoogde basis waarop de beveiliging van de in het kader van de Wet GDI te ontwikkelen digitale diensten is gebaseerd. Inzet van een buitenlandse marktpartij is hoogst ongebruikelijk en alleen

---

[1] Zie onder meer Kamerbrief 784590, Minister van Veiligheid en Justitie, 16 september 2016.
[2] PEP project page: http://pep.cs.ru.nl/
[3] Cryptology ePrint Archive: Report 2016/411 - Polymorphic Encryption and Pseudonymisation for Personalised Healthcare door E. Verheul, B. Jacobs, C. Meijer, M. Hildebrandt en J. de Ruiter (2016). Hoofdstuk 2.7 Conclusions and future work, blz. 34 en 35. (3) Develop formal security proofs to substantiate the reasoning in Subsection 2.6.2.
(4) Analyse the relevant security protocols with tools like ProVerif7 . https://eprint.iacr.org/2016/411
[4] Verily: https://verily.com/projects/precision-medicine/personalized-parkinson-project/

toegestaan, nadat de betrouwbaarheid van de marktpartij is vastgesteld. Omdat Verily een Amerikaans bedrijf is, is dit niet mogelijk. Bovendien verplicht de Amerikaanse wetgeving Verily om de privacygevoelige kennis die wordt opgedaan bij de PoC te delen met de Amerikaanse overheid.

Dat de PoC wordt uitgevoerd door een Amerikaans bedrijf is des te meer uiterst merkwaardig, omdat de hoogleraar van de vakgroep waar de PoC wordt ontwikkeld, prof. Jacobs, onlangs een prijs heeft gehad voor zijn werkzaamheden op het gebied van privacy.

Verouderd algoritme

Het bij PEP gebruikte algoritme ElGamal public key encryption[5] is inmiddels 32 jaar oud[6]. Het is weliswaar inmiddels enigszins aangepast, maar is zo oud dat er vanuit moet worden gegaan dat dit waarschijnlijk binnen afzienbare tijd wordt ontcijferd.[7][8][9][10].

Privacy van de burger

Het voorziene gebruik van PEP is bovendien strijdig met de EU richtlijnen[11] waarop de Wet GDI is gebaseerd. Die stellen, dat het gebruik van gepseudonimiseerde data zoals in PEP het geval is, niet overeenkomt met de noodzaak om geanonimiseerde data te gebruiken. Pseudonimiseren is niet gelijk aan anonimiseren, ondanks wat vaak wordt gedacht.[12] Als uitvloeisel van de Wet GDI zal PEP dermate algemeen worden gebruikt, dat de privacy betrekkelijk eenvoudig geweld kan worden aangedaan. Met andere woorden: het EU beleid acht PEP onvoldoende basis voor bescherming van de privacy van de burger.

Een juridisch bezwaar

PEP maakt gebruik van centrale opslag van privacy gevoelige informatie. De Autoriteit Persoonsgegevens (AP) heeft in haar, ook voor de Wet GDI relevant advies[13] aan het Ministerie van Onderwijs, Cultuur en Wetenschap (MIN OC&W), van november 2016 gesteld dat een pseudoniem uitsluitend mag worden gebruikt voor het oorspronkelijke doel. Dat heeft tot gevolg dat de beoogde flexibiliteit bij het gebruik van PEP nagenoeg niet zal bestaan. Daarmee wordt een van de hoofddoelstellingen van de wet GDI onhaalbaar. Immers, nieuwe toepassingen kunnen pas na een complex goedkeuringstraject worden toegevoegd. Vanwege dit probleem heeft de AP het MIN van OC&W geadviseerd om het wetsvoorstel,

---

[5] Cryptology ePrint Archive: Report 2016/411 - Polymorphic Encryption and Pseudonymisation for Personalised Healthcare door E. Verheul, B. Jacobs, C. Meijer, M. Hildebrandt en J. de Ruiter (2016) https://eprint.iacr.org/2016/411

[6] Elgamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory (1985) blz.. 469-472

[7] "The ElGamal Cryptosystem" door Andreas V. Meier (2005). Hoofdstuk 5 Summary blz. 12 http://wwwmayr.in.tum.de/konferenzen/Jass05/courses/1/papers/meier_paper.pdf

[8] CS395T Advanced Cryptography" Lecture 9: CCA security door B. Waters - University of Texas (2009). Deel 2: Vulnerability of ElGamal cryptosystem under CCA. https://www.cs.utexas.edu/~rashid/395Tcrypt/5_1.pdf

[9] "Why Textbook ElGamal and RSA Encryption Are Insecure" door D. Boneh, A. Joux en P.Q. Nguyen (2000) https://www.ssi.gouv.fr/archive/fr/sciences/fichiers/lcr/bojong00.pdf gepubliceerd voor event ASIACRYPT 2000: 6th International Conference on the Theory and Application of Cryptology and Information Security, Japan 2000.

[10] Modified ElGamal over RSA Digital Signature Algorithm (MERDSA) door K. Madhur, J.S. Yadav en A.Vijay. Gepubliceerd in International Journal of Advanced Research in Computer Science and Software Engineering (2012). Hoofdstuk 2 Security threats against discrete logarithm and factorization problem based algorithms. Blz. 289 en 290. https://www.ijarcsse.com/docs/papers/8_August2012/Volume_2_issue_8/V2I800240.pdf

[11] De Groep Gegevensbescherming - onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer over artikel 29 (0829/14/NL WP 216): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf (2016)

[12] Zie ook Advies 4/2007 van de Groep gegevensbescherming artikel 29, blz. 18-20.

[13] Autoriteit Persoonsgegevens, Advies wetsvoorstel pseudonimisering (kenmerk z2016-14321): https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_pseudonimisering_onderwijs.pdf

waar bij leerlingenregistraties pseudonimisering zou moeten worden toegepast, niet in te dienen[14]. Omdat de Wet GDI beoogt om digitale toepassingen mogelijk te maken waarvoor veel zwaardere privacy eisen gelden dan voor het MIN van OC&W gelden, moet er van uit worden gegaan, dat dezelfde bezwaren van de AP in heviger mate van toepassing zijn.

PEP is geen internationale standaard

Het gebruik van PEP wijkt af van de standaarden zoals die in vrijwel alle Europese landen wordt gebruikt voor communicatie tussen overheid en burger.[15] Een in het kader van GDI in te voeren stelsel moet optimaal kunnen functioneren in combinatie met standaard besturingssystemen. Immers, ook in Nederland ontwikkelde IT systemen zijn in hoge mate gebaseerd op internationale standaarden. Wanneer – in afwijking van alle vergelijkbare Europese landen - wordt gekozen voor PEP, zijn hoge kosten te verwachten gedurende de gehele levensduur van het stelsel.

Nederland is een open economie. Al onze handelspartners, in Europa en daar buiten, hebben inmiddels gekozen voor systemen die voldoen aan internationale standaarden. PEP wijkt hier van af. De invoering van PEP zal mogelijk negatieve gevolgen hebben voor de internationale handel van Nederland, omdat Nederland dan zal hebben gekozen voor een "eiland" IT systeem.

Big data analytics

De opkomst van big data doet de pseudonimisatie van persoonsgegevens of data geheel of gedeeltelijk te niet. De opstellers van het concept erkennen dit expliciet, aangezien de in de PoC te behandelen persoonsgegevens juist bedoeld zijn om te worden verwerkt in "big data". Immers, er kan re-identificatie aan de hand van losse gegevenselementen plaatsvinden.[16] Bovendien ondergraaft het beoogde gebruik van de PoC ten behoeve van big data de representativiteit voor de Wet GDI. Die Wet beoogt nu juist het voorkomen dat persoonsgegevens kunnen worden gebruikt voor big data. Ook gaat de wet GDI uit van federatieve identiteiten. Daaruit ontstaan bij het gebruik van PEP aanvullende juridische en privacy risico's.

Het BIT-advies; financiën

Niet voor het eerst gaat het ontwerp van de Wet GDI geheel voorbij aan het advies van bureau BIT. De businesscase[17] "Geactualiseerde Business Case Inloggen in het BSN domein" laat het advies van het Bureau ICT-toetsing (BIT) van mei 2016[18] compleet buiten beschouwing. Het BIT-advies stelt onder meer dat de aanpak te complex is. Uit de memorie van toelichting blijkt, dat aan de bezwaren van het BIT niet is tegemoet gekomen.

---

[14] Advies wetsvoorstel pseudonimisering, Autoriteit Persoonsgegevens, Z2016-14321, 3 oktober 2016.

[15] Enhancing privacy of users in eID schemes door K. Shrishak, Z.Erkin en R.Schaar TU Delft (2016) http://cybersecurity.tudelft.nl/sites/default/files/SES16.pdf . (Rapport is opgesteld op het verzoek van het MIN van BZK).

[16] De Groep Gegevensbescherming - onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer - over artikel 29 (0829/14/NL WP 216): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf
Hoofdstuk 2.2.2. Identificeerbaarheid van geanonimiseerde gegevens blz 9, Hoofdstuk 4. Pseudonimisering blz. 23. (2016)

[17] Rijksoverheid, Rapport Businesscase inloggen in het BSN domein (2016) : https://www.rijksoverheid.nl/documenten/rapporten/2016/11/09/rapport-businesscase-inloggen-in-het-bsn-domein

[18] Brief BIT aan de minister van Binnenlandse Zaken en Koninkrijkrelaties, BIT-advies programma eID, 12 mei 2016.

Het BIT advies stelt, dat de financiële gevolgen van de Wet GDI onduidelijk zijn. In het wetsvoorstel GDI worden deze onduidelijkheden in het geheel niet weggenomen (MvT, blz. 43). Dat stelt doodleuk, dat aansluitkosten kunnen worden doorberekend aan aanvragers. Daarmee wordt een grote, nog volstrekt onbekende, financiële druk gelegd op de vele, krachtens de Wet GDI verplichte, aan te sluiten partijen.

Integriteit

Het is opvallend dat diverse opstellers van de wet GDI meerdere rollen in dit proces hebben vervuld. Dat leidt mogelijk tot belangenverstrengeling. Bovendien heeft dit geleid tot het selectief gebruik van algemeen geldend beleid. Beleid dat voortvloeit uit verdragsrechtelijke verplichtingen en nationale wetgeving.

Aanbeveling

Het huidige wetsvoorstel GDI bevat talrijke risico's. Geadviseerd wordt, om het wetsvoorstel GDI in de huidige vorm niet in te dienen. Het wetsvoorstel dient zodanig te worden gewijzigd, dat wordt aangesloten bij de gangbare, internationale standaarden en dat voldoende waarborgen bestaan voor: privacy, toekomstvastheid en financiële beheersbaarheid. Uiteraard ben ik graag bereid aan de leden van de commissie een nadere toelichting te geven.

Hoogachtend,

Ing. J.L.A. Rochat
A.E.T. Europe B.V.
Chief Technology Officer