Connectis

Datum: 17 maart 2017

Betreft: Review GDI & Uniforme Set van Eisen

Geachte heer, mevrouw,

Op uw verzoek heeft Connectis een review uitgevoerd op de Wet GDI en de Uniforme Set van Eisen.

Vooropgesteld: het is belangrijk dat deze wet er komt zodat er eindelijk enige vooruitgang op dit dossier kan worden geboekt. Het is "beter dan niets", maar er zijn wel een aantal fundamentele aanpassingen noodzakelijk om deze wet uitvoerbaar en betaalbaar te maken:

1. De beoogde voordelen van een polymorfe identiteit en pseudoniem wegen niet op tegen de benodigde investeringen en kosten voor de keten (zie bijlage I). Als dit wordt vervangen door reguliere encryptie dan wordt het voor leveranciers en dienstverleners veel eenvoudiger en goedkoper om aan te sluiten. Het Rijk hoeft dan geen BSN-k te financieren (m.u.v. het inzage-register), er zijn geen Single Points of Failure meer en de performantie van het systeem zal substantieel toenemen. Door een verlaagde complexiteit zal bovendien de adoptie van het stelsel veel hoger zijn dan bij de inzet van deze zeer exotische technologie.

2. Het financieringsmodel is complex, werkt kostenverhogend en is in strijd met Europese regelgeving (zie bijlage II). Wij adviseren om dit model te vervangen door een veel eenvoudiger model:

    - Het Rijk belast geen kosten door aan de verschillende partijen in het stelsel. Deze kosten worden gedekt uit de rijksbegroting.
    - De authenticatiedienst heeft geen uitgaande kosten en ontvangt geen vergoeding voor gebruik van het middel vanuit de ontsluitende dienst. Alle kosten van de authenticatiedienst worden betaald door de gebruiker.
    - De ontsluitende dienst heeft geen uitgaande kosten. Alle kosten van de ontsluitende dienst worden betaald door de bestuursorganen en aangewezen organisaties.
    - De overheid vergoedt (een deel van de) eenmalige en periodieke kosten voor de gebruikers die dit nodig hebben.

    Het is onze inschatting dat bovenstaande aanpassingen leiden tot een substantiële reductie van de totale kosten van het stelsel. Indien bovenstaande aanpassingen niet worden uitgevoerd, dan is het zeer waarschijnlijk dat de kosten van dit stelsel voor actieve gebruikers een veelvoud zijn van de kostprijs van een hoogwaardig middel in eigen beheer.

3. De positie van private partijen in het stelsel zou voldoende geborgd moeten worden. Er moet sprake zijn van een “level playing field”, voor zover mogelijk:

    - Een aansluiting zou altijd via private partij moeten verlopen en niet direct op de publieke infrastructuur. Dit voorkomt afhankelijkheid van de publieke infrastructuur te voorkomen alsmede concurrentie van de overheid met de private aanbieders die willen investeren in dit stelsel.
    - Burgers mogen niet verplicht worden om een publiek middel aan te schaffen. Indien een burger niet voor een publiek variant kiest dan moet zij hiermee ze kosten besparen om een private variant aan te schaffen.

Connectis / Connected Information Systems B.V.
PO box 975 • 3000 AZ Rotterdam • Phone: +31 (0) 88 01 20 222 • www.connectis.nl • info@connectis.nl
Chamber of Commerce 24444001 Rotterdam • Value Added Tax NL819935177B01 • Bank IBAN NL 04 ABNA 054 717 7100

4. De wet is op punten inconsistent is met zichzelf en / of het overig wetgevend kader (zie bijlage III). Deze inconsistenties lijken voor een belangrijk deel voort te komen uit de sterke drang om het gebruik van het polymorf id als privacymaatregel te verdedigen.

   Op deze punten wekt de wetgeving de indruk dat er is gezocht naar probleem dat bij de oplossing ”polymorfe encryptie” past in plaats van dat men de meest praktische oplossing voor het voorliggende probleem heeft gezocht. Dit is een belangrijk kenmerk van IT projecten die mislukken en het ministerie hier dan ook aandachtig naar moeten kijken.

   Ik vertrouw u hiermee van dienst te zijn en ben tot nadere toelichting gaarne bereid.

   Met vriendelijke groet,

   Martijn Kaag
   Algemeen Directeur

Connectis / Connected Information Systems B.V.
PO box 975 • 3000 AZ Rotterdam • Phone: +31 (0) 88 01 20 222 • www.connectis.nl • info@connectis.nl
Chamber of Commerce 24444001 Rotterdam • Value Added Tax NL819935177B01 • Bank IBAN NL 04 ABNA 054 717 7100

Connectis

Bijlage I. De beoogde voordelen van een polymorfe identiteit en pseudoniem wegen niet op tegen de benodigde investeringen en kosten voor de keten.

Het voorstel behelst de introductie van een polymorfe identiteit en pseudoniem. Hierbij plaatsen wij de volgende kanttekeningen.

De polymorfe identiteit is zeer complex en kennis is in de markt niet beschikbaar
De polymorfe identiteit en pseudoniem zijn Nederlandse uitvindingen met een hoog experimenteel gehalte. Het eID stelsel is de eerste project waarin deze buiten een academische setting worden toegepast en niet één van de betrokken (publieke of private) leveranciers heeft expertise op dit gebied. Het is uitermate complex en ook hoogopgeleide softwareontwikkelaars en ervaren systeemanalisten hebben veel moeite om de werking van deze oplossing te begrijpen.

De polymorfe identiteit vereist ontwikkeling van nieuwe software en hardware
De uitvoering van de polymorfe identiteit vereist de ontwikkeling van software én hardware (HSM) die momenteel op de markt nog niet beschikbaar zijn. Het is onwenselijk om een dergelijk experiment op zo'n grote schaal toe te passen. Het brengt hoge kosten met zich mee, verlaagt de adoptie en vanwege het experimentele karakter verhoogt het de risico's; zowel voor het project als voor de beveiliging van het stelsel als geheel.

De extra impact van de polymorfe identiteit t.o.v. reguliere encryptie is zeer beperkt
Vrijwel alle doelstellingen van de polymorfe identiteit worden óók gerealiseerd middels internationale en breed toegepaste encryptie met bestaande software. De enige concessie is dat authenticatiediensten met standaard encryptie ook na registratie over het BSN blijven beschikken[1].

De impact hiervan is echter zeer beperkt. Banken en de overheid hebben het BSN immers al leesbaar in hun administratie staan en moeten deze in hun administratie laten staan voor de uitvoering van hun andere (wettelijke) taken. Ook notarissen beschikken reeds over het BSN.

De overheid, banken en mogelijk ook notarissen zullen waarschijnlijk het leeuwendeel van de transacties voor hun rekening nemen. De extra voordelen van de polymorfe identiteit t.o.v. reguliere encryptie worden derhalve alleen gerealiseerd voor circa 5 private leveranciers die slechts een klein deel van de transacties voor hun rekening nemen. Deze leveranciers staan onder streng toezicht en zijn bovendien gespecialiseerd in informatiebeveiliging.

Dit risico is verwaarloosbaar t.o.v. de duizende partijen in zorg en overheid die geen expert zijn op het gebied van informatiebeveiliging en momenteel ook het BSN verwerken.

De polymorfe identiteit benadeelt kleine participenten
Het systeem benadeelt kleine participanten: die hoeven geen HSM aan te schaffen (duur) als ze bereid zijn te vertrouwen op de beschikbaarheid van BSNk (=single point of failure voor versleuteling als je zelf geen HSM hebt). Dit wordt afgedaan met een vage redenering op p19 van de Toelichting:
"Bij kleinere authenticatiediensten zal deze versleutelde identiteit worden afgegeven door het BSN-K. Grote authenticatiediensten hanteren een bepaalde techniek zodat zij zelf voor een transactie een polymorfe identiteit transformeren in een versleutelde identiteit. Hiermee wordt voorkomen dat het BSN-K overspoeld raakt met aanvragen."
'Kleiner' betekent blijkbaar: 'heeft geen geld over voor een eigen HSM' Maar feitelijk wordt hier dus gevraagd om een investering in de algemene dienstverlening van BSNk door de 'grotere' partijen. Dat grijpt direct in op de concurrentiepositie van participanten onderling, want wie draait

[1] Als gevolg van de polymorfe identiteit kunnen authenticatiediensten het BSN na registratie uit haar administratie verwijderen. De polymorfe identiteit voorkomt echter niet dat deze partijen tijdens registratie over het BSN beschikken

er hier eigenlijk op voor het ontwerpprobleem van een SPoF? En hoeveel HSMs zijn er nodig om BSNk te ontlasten? En met die HSM ben je er nog niet, want vanwege de verplichte splitsing bij polymorfe pseudonimisering ben je dan als authenticatiedienst ook nog verplicht om een Chinese muur in de organisatie in te richten.

De polymorfe identiteit wordt niet verplicht door Europese wetgeving

Tot slot merken wij op dat er ook Europese landen zijn waar het nationale identificatienummer niet is aangemerkt als bijzonder persoonsgegeven. Europees wordt het breed gedeeld en toegepast buiten de publieke sector. Ook in Nederland kan het BSN nummer van alle ZZP'ers eenvoudig worden achterhaald omdat dit onderdeel is van het BTW nummer.

Indien en voor zover Europese wet en regelgeving een technologie als polymorfe identiteit zou verplichten dan zal dit verregaande impact hebben op al deze lidstaten. En ook in Nederland zouden onder meer de belastingdienst, de KvK en alle administratiepakketten in Nederland hun volledige primaire proces moeten herzien. Hiervan is nu geen sprake.

Bijlage II. Het financieringsmodel is complex, werkt kostenverhogend en is in strijd met Europese regelgeving.

Het voorstel onderscheidt in ieder geval onderstaande financiële stromen. Alle met een * gemarkeerde posten zijn hierbij zeer onzeker en de overheid behoudt zich het recht voor om deze opbrengsten en/of uitgaven op enig moment aan te passen en/of te reguleren.

Rol:	Wordt betaald door:	Betaald aan:
Authenticatie-dienst	○ Gebruiker voor aanschaf en gebruik middel ○ Ontsluitende dienst voor gebruik middel*	○ Het Rijk voor: a. verstrekken middel* b. periodieke vergoeding voor toezicht en BSN-k*
Ontsluitende dienst	○ Bestuursorganen en aangewezen organisaties voor: a. aansluiting b. gebruik middel*	○ Authenticatiediensten voor gebruik middel* ○ Het Rijk voor periodieke vergoeding voor toezicht en BSN-k*
Bestuursorganen en aangewezen organisaties		○ Ontsluitende diensten voor: a. aansluiting b. gebruik middel*

Bij dit financieringsmodel plaatsen wij de volgende kanttekeningen.

Geld uit rijksbegroting wordt "rondgepompt" en groot deel van het geld stroomt hierdoor weg
Bestuursorganen en aangewezen organisaties worden gefinancierd met publiek geld, vaak (ook) via de rijksbegroting. Met dit publieke geld betalen zij ontsluitende diensten, die hieruit het rijk en authenticatiediensten betalen. Ook authenticatiediensten betalen hieruit weer het Rijk.

Geld uit de rijksbegroting stroomt daarom over twee of drie partijen om uiteindelijk weer in de rijksbegroting te komen. Door administratiekosten, risico-opslag en winstmarge stroomt een belangrijk deel van het geld weg zonder dat hiermee toegevoegde waarde wordt gecreëerd.

Grote onzekerheid maakt business case voor alle partijen onmogelijk
Er is een zeer grote onzekerheid voor alle partijen voor zowel de inkomende en uitgaande kosten. Zelfs indicatieve schattingen van experts van de uiteindelijke kosten en/of opbrengsten per transactie ontlopen elkaar met een factor honderd. En als deze kosten op een gegeven moment zijn vastgesteld door één of meerdere partijen, dan behoudt de overheid zich het recht voor om hierop in te grijpen.

Dit maakt het onmogelijk voor partijen om een betrouwbare business case op te stellen: zowel de kosten als de baten kunnen niet geschat worden. Daar waar partijen uiteindelijk toch besluiten om tot investeren over te gaan, dan zullen zij hiervoor een (zeer) hoge risico-opslag moeten hanteren. Dit heeft een sterk prijsopdrijvend effect.

eIDAS wetgeving verbiedt transactiekosten bij grensoverschrijdende transacties
De eIDAS wetgeving verbiedt lidstaten om transactiekosten in rekening te brengen voor grensoverschrijdende transacties. Het beoogde financieringsmodel maakt het daarom onmogelijk om aan de eIDAS wetgeving te voldoen.

Prijs per transactie contrasteert met kostenmodel
De kosten voor een veilig authenticatiemiddel bestaan voor het grootste deel uit eenmalige

(verificatie, uitreiking middel) en periodieke (ondersteuning, infrastructuur) kosten. De marginale kostprijs per transactie is voor veel moderne middelen (app, token, certificaat) verwaarloosbaar[2]. Het aantal transacties is daarom geen belangrijke kostprijsbepalende factor. Om deze reden is het verwonderlijk dat er in de wetgeving wordt voorgesorteerd op een model waarin er door partijen naar gebruik moet worden afgerekend.

Een logischer financieringsmodel van authenticatiediensten zou uitgaan van een prijs per middel per jaar, ongeacht het aantal transacties en / of dienstverleners die op het stelsel zijn aangesloten.

[2] De totale kosten voor een middel dat dagelijks wordt gebruikt zijn vaak zelfs lager dan een middel dat slechts één keer per jaar wordt gebruikt om infrequent gebruik leidt tot een hogere support last. De gemiddelde marginale kosten per transactie zijn daarom vaak negatief.

Bijlage III. De wet is op punten inconsistent is met zichzelf en / of het overig wetgevend kader

Beperken van de kosten vs kostbare implementatie
Als doelstelling van het wetsvoorstel wordt "Het beperken van de kosten voor publieke dienstverleners voor de beveiliging van de gegevens" genoemd (Toelichting p3). Toch wordt er een complexe en exotische technologie voorgeschreven die zich nog nergens ter wereld op grote schaal heeft bewezen.

Bescherming BSN in wetgeving inconsistent
De Uniforme Set Van Eisen, p8, stelt het volgende:

> "De voorziening moet voldoen aan de principes van de Europese verordening gegevensbescherming van 27 april 2016, waaronder het principe van minimale gegevensverwerking: persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit principe is ook van toepassing op de Nederlandse overheid; het BSN zou alleen verwerkt moeten worden als dat noodzakelijk is. In andere gevallen moeten pseudoniemen worden gebruikt, indien een persistent identificerend kenmerk überhaupt noodzakelijk is. "

Gesuggereerd wordt dat er van “noodzakelijk” geen sprake kan zijn als het mogelijk is om met een pseudoniem te werken. Dit volgt evenwel niet uit de wetgeving, en als dat al zo zou zijn dan zou je dit een stuk strakker moeten regelen, over de volledige keten en bij alle gegevensverwerking.

Banken, notarissen, werkgevers, administratiepakketten en overheden zouden dan altijd verplicht moeten worden om het BSN nummer in hun administraties te vervangen door een polymorf pseudoniem. Dit vraagt overkoepelende wetgeving. Om dit alleen binnen deze context te realiseren is inconsistent.

Inzage gebruik contrasteert met uitgangspunten
De Memorie van Toelichting, p 28, stelt het volgende:

> "Tevens wordt de gegevensverwerking zodanig ingericht dat geen enkele van de bij authenticatie betrokken partijen (inclusief publieke dienstverleners) kan zien welke andere websites door een gebruiker worden bezocht in het publieke domein."

Dit wordt niet gerealiseerd. De authenticatiedienst moet immer alsnog een overzicht verstrekken aan de gebruiker met al haar transacties:

> "De Authenticatiedienst kan de authenticatie detail transacties namelijk registreren onder een pseudoniem en zo een scheiding aanbrengen tussen de gebruikersregistratie (waar de Gebruiker onder volledige identiteit bekend is) en de transactieregistratie (onder pseudoniem). Deze scheiding tussen gebruikersregistratie en transactieregistratie, waarmee de privacy hotspot bij de Authenticatiedienst vermeden wordt, is een eis vanuit de Uniforme Set van Eisen, de manier waarop deze wordt gerealiseerd is vrij gelaten."

> "de transacties die zijn uitgevoerd met het Authenticatiemiddel dat is gekoppeld aan de identiteit van de Gebruiker. Het geboden inzicht bestaat in elk geval uit de datum en tijd van inloggen en de dienst of Dienstverlener waarop is ingelogd." (p25)

Deze inzage in het gebruik is een belangrijke privacy mitigerende maatregel: de gebruiker wordt in staat gesteld om eventueel misbruik met haar middel te signaleren en kan hiernaar handelen.