55

Nederland ICT reageert bij deze graag op de in consultatie gebrachte Regels inzake de generieke digitale infrastructuur, de 'Wet GDI'.

ALGEMEEN

Nederland ICT is positief dat het wetsvoorstel een basis is voor een digitaal werkende overheid. Het belang van een goed werkende digitale overheid is groot. Een betrouwbaar werkend systeem van online identificatie en authenticatie is de basis voor het vertrouwen dat burgers en bedrijven hebben in de overheid, en in de digitale economie in het algemeen.

Inloggen bij (overheids)dienstverleners moet voor burgers en bedrijven gewoon goed, betrouwbaar, veilig en simpel zijn. Vertrouwen in het systeem is essentieel, en keuzevrijheid is daar een onderdeel van. De nagestreefde multimiddelenaanpak is wat dat betreft een stap in de goede richting; het geeft de eindgebruiker een keuze (mits er voldoende aanbod komt). De robuustheid van het systeem neemt toe als ondernemers, overheden en burgers een keuze hebben. Bovendien zal de te verwachten competitie tussen verschillende aanbieders een positief effect hebben op de kosten, op innovatie, gebruiksgemak en daarmee op de waarde voor de gebruiker.

LEVEL PLAYING FIELD

Een level playing field is van groot belang: gelijke kansen voor alle partijen. Het risico bestaat bij het ontbreken daarvan, dat het voor private partijen niet meer interessant is om te investeren in eID oplossingen, waar door een sub optimale situatie ontstaat. Er moeten maatregelen worden getroffen om het commerciële perspectief van de multimiddelenaanpak voor private middelenleveranciers te vergroten, anders bestaat het risico dat er onvoldoende private middelen beschikbaar komen voor een gezonde, concurrerende markt. Dit zal ook verstrekkende gevolgen hebben voor de authenticatiemarkt in het private domein.

Een aansluiting zou altijd via private partij moeten verlopen en niet direct via de publieke infrastructuur. Dit voorkomt afhankelijkheid van de publieke infrastructuur 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 publieke variant kiest dan moet zij hiermee ze kosten besparen teneinde een private variant aan te kunnen schaffen.

Om de private aanbieders perspectief te bieden, is het van groot belang dat zo snel mogelijk inzicht komt in de publieke business case. Bedrijven moeten weten hoe hoog de leges voor het publieke middel zullen worden en waarop deze gebaseerd gaan worden.

Tevens moet er duidelijkheid zijn over de voorwaarden voor de uitrol van het publieke middel substantieel. Voor een gelijkwaardig speelveld is het essentieel dat dit middel aan dezelfde eisen voldoet als de uitrol van private middelen op hetzelfde niveau.

UNIFORME SET VAN EISEN

Vertrouwen is essentieel voor de digitale overheid. Daarom geldt dat eID altijd volledig veilig en correct moet zijn, want bij authenticatie is slechts 100% zekerheid relevant. Duidelijke regels voor de technologie en alle rollen binnen eID zijn dus van belang. Daarom is het van belang dat alle relevante partijen binnen het eID systeem ook volledig voldoen aan de Uniforme Set van Eisen. Daar mag geen enkele twijfel over bestaan.

Er moet zo spoedig mogelijk, maar niet later dan eind 2017, duidelijkheid komen over de voorwaarden die aan leveranciers en dienstverleners worden gesteld in het kader van de wet. Dit betekent in ieder geval dat de nog ontbrekende hoofdstukken van de USvE, alsmede de AMvB's en ministeriële regelingen worden uitgewerkt.

POLYMORFE PSEUDONIEMEN

De introductie van Polymorfe Pseudoniemen is een interessante ontwikkeling waar goed naar gekeken moet worden. Potentieel kan dit de privacy van de eindgebruiker optimaal waarborgen. Nederland kan op dit gebied een voortrekkersrol gaan vervullen. Het is echter wel zeer complex en kostbaar. Het risico bestaat dat hiermee een zeer kostbaar en complex pad wordt ingeslagen dat vertragend werkt waardoor, bij ingang van de wet, onvoldoende eindgebruikers zullen zijn met het juiste betrouwbaarheidsniveau.

OPEN STANDAARDEN

Veilige en betrouwbare toegang (authenticatie) wordt geregeld via erkende publiek en privaat uitgegeven middelen. Ten behoeve van die betrouwbare digitale dienstverlening in het publieke domein, kunnen standaarden worden aangewezen. Het is wel van groot belang de concept-AMvB's, waarin bepaalde standaarden worden verplicht, te consulteren, zodat belanghebbenden uit de overheid en uit bedrijfsleven en wetenschap een directe mogelijkheid hebben om te reageren en betrokken partijen actief uitgenodigd worden om te reageren. Het proces zoals het Forum Standaardisatie dit heeft ingericht, dient leidend te zijn.

ACCEPTATIEPLICHT

Het is belangrijk dat alle overheden, inclusief ZBO's, verplicht worden alle erkende middelen te accepteren. Ondernemers moeten kunnen kiezen voor de voor hun meest relevante en optimale authenticatieoplossing. Deze keuzevrijheid stimuleert marktwerking in de markt van middelen, waardoor ook continue innovatie en prijsoptimalisatie plaatsvindt, hetgeen telkens een versnelling in de digitale dienstverlening teweegbrengt.

TOEZICHT

Toezicht op de kwaliteit en de betrouwbaarheid moet onafhankelijk ingericht worden. De overheid is zelf ook leverancier in deze markt. Hier door zijn extra waarborgen nodig in de vorm van een strikte scheiding en een onafhankelijke toezichthoudersrol van een ZBO. Op zijn minst is transparantie een voorwaarde voor een onafhankelijk toezicht.

Tenslotte moet voorkomen worden dat private partijen in de knel komen door een overlap aan verschillende toezichthouders. Indien sprake is van overlappende bevoegdheden richting middelen-leveranciers en hun authenticatie oplossingen (bijvoorbeeld door sectorale toezichthouders) moet dit in samenwerkingsprotocollen worden afgedekt en openbaar gemaakt.