itsme®

memo dd. 11-05-2020

Wet digitale overheid
Besluit identificatiemiddelen voor burgers
AMvB consultatie (keten-ID 10752)

A smarter business
by smarter users

itsme® | Belgian Mobile ID | Sint-Goedeleplein 5 Place Sainte-Gudule | 1000 Brussels, Belgium

Betreffende

Wet digitale overheid
Besluit identificatiemiddelen voor burgers
AMvB consultatie (keten-ID 10752)
https://www.internetconsultatie.nl/identificatiemiddelen.

Introductie

itsme® is een geaccrediteerd Europees identificatiemiddel (eIDAS betrouwbaarheidsniveau “Hoog”).

Intussen is itsme® al meer dan een jaar betrokken bij meerdere initiatieven zowel op niveau van de Rijksoverheid als op gemeentelijk vlak (Rotterdam, Eindhoven, Helmond en Molenlanden). Aanvankelijk via deelname aan het Identiteits-lab en nu actief in de piloot met SesamID (voormalig DigiD App Bronidentiteit genoemd) die mee sturing zal geven aan de verdere verdieping van de Wet digitale overheid.

Wij hebben met veel interesse kennis genomen van de voorliggende teksten en zijn verheugd via deze weg een aantal consideraties te mogen meegeven die volgens ons relevant zijn om te komen tot een performant Europees speelveld op vlak van digitale identiteit en dit in al haar dimensies.

Hierna ter info een aantal elementen die aan de grondslag liggen van het succes van itsme® in België:

- Doelstelling om identificatie-middelen in te zetten voor **zowel publieke als private toepassingen**. Dit heeft mede gezorgd voor digitale bruggen tussen industrie en overheid hetgeen de digitalisatie van heel wat processen X-sector heeft versneld.
- Accreditatie vanwege de overheid gebaseerd op **meetbare resultaten en niet op technologische voorschriften**. *Dit laatste is eigenlijk ronduit gevaarlijk: wat als de opgelegde technologie op zeker moment niet langer veilig blijkt?*
- Creatie van een **globaal wettelijk kader** dat innovatie en het veilig digitaliseren van processen ondersteunt. Hierdoor werd het voor professionele, geaccrediteerde spelers bijvoorbeeld mogelijk om het rijksregisternummer (RRN = equivalent van het BSN) te gebruiken onder welbepaalde voorwaarden.
- Regulatoren zoals bijvoorbeeld de Nationale Bank hebben relatief snel expliciete **verwijzingen naar eIDAS opgenomen in hun nationale richtlijnen** (vb KYC criteria in kader van anti-witwaswetgeving).

Het voorliggende besluit bevat sterke basisprincipes

De principes weerhouden door de Nederlandse overheid vormen een uitstekende basis voor een gelijk speelveld en voor Europese interoperabiliteit:

- “… eisen worden gesteld aan het resultaat, namelijk het **bieden van waarborgen**, maar zo weinig mogelijk aan de wijze waarop dit resultaat gehaald moet worden …”
- “… **zo weinig mogelijk technische aspecten** vast te leggen in de regels voor de toelating, zodat ruimte wordt gelaten voor innovatie …”
- “… eisen zijn gebaseerd op de **eIDAS-verordening** … en op de Algemene verordening **gegevensbescherming** …”

Essentiële vereisten voor middel en aanvrager

We begrijpen dat de Nederlandse overheid een aantal essentiële vereisten wenst te stellen aan middel en aanvrager om de kwaliteit en continuïteit van de service te waarborgen.

Volgende zaken lijken ons daarbij primordiaal:

- Het middel kan de nodige rapporten voorleggen van hiervoor gecertifieerde instanties die toelaten van de **conformiteit** te beoordelen **met de Europese kaders** inzake eIDAS en AVG. Het middel koppelt hierbij een hoge beveiliging aan eenvoud in gebruik en dit met ultiem respect voor gegevensbescherming en controle door de eindgebruiker.
- Het middel maakt bij voorkeur gebruik van internationaal erkende **open standaarden** die gangbaar zijn in het ID-landschap (bv OpenID Connect).
- De aanvrager is in staat van **grote transactie-volumes** te verwerken en kan een 'uptime' van minimaal 99.5% garanderen.
- De aanvrager heeft de nodige financiële draagkracht en opzet om de **continuïteit** van de dienstverlening te waarborgen.
- Het middel is in staat om op een gebruiksvriendelijke manier om te gaan met diverse **'lifecycle events'** zoals wijziging van het mobiele toestel, update van ID-gegevens, blokkeren en heractiveren van het middel, stopzetten van het middel, … .
- Het middel is in staat om aan de verplichtingen te voldoen wat betreft **auditeerbaarheid** en wetgeving voor diverse activiteitsdomeinen. Zo zijn bijvoorbeeld financiële instellingen verplicht van alle transacties minimaal 10 jaar ter beschikking te houden voor audit of gerechtelijk onderzoek.
- Een specifieke eis in het kader van de AVG is "the right to be forgotten" waarbij de eindgebruiker in de mogelijkheid moet zijn om op elk moment zijn data te vernietigen maar waarbij het middel in staat moet blijven om te voldoen aan haar wettelijke verplichtingen zoals vermeld in het vorige punt (vb. transactie-logs).

Centrale of decentrale opslag?

Inzake veiligheid & privacy zien we in de media vaak principiële debatten ontstaan in verband met centrale of decentrale opslag van gegevens. Intussen is voldoende aangetoond dat dit debat geen winnaars of verliezers kent en dus **in de realiteit een 'fetisj'** is. Beide modellen hebben hun voor- en nadelen én de reële kwaliteit hangt louter af van de implementatie. Net dit laatste wordt uitvoerig beproefd bij een gedegen accreditatie-onderzoek. Een volledig decentrale opzet waarbij er zich enkel gegevens bevinden op het mobiele toestel van de gebruiker zonder enige centrale controle blijkt vaak veel moeite te hebben met de hogergenoemde 'lifecycle events', pro-actieve fraudeopsporing en auditeerbaarheid van de oplossing.

Vrijgave van broncode?

Ook hier is de roep in de media groot. Echter de vrijgave van de broncode van een beveiligings-product is iets waar grondig moet over worden nagedacht. Indien er in deze geen 'level playing field' is – hetgeen 'de facto' het geval is gezien deze eis niet op Europees vlak wordt gesteld – **stelt zich een probleem van oneerlijke competitie** met andere internationale oplossingen.

Erkenning van een middel dat reeds Europees genotifieerd is

Een middel dat reeds behoort tot een genotifieerd stelsel hoeft het nationale toelatingstraject niet te doorlopen en wordt verondersteld aan te sluiten via het eIDAS-knooppunt.

Gezien de connectie via het eIDAS-knooppunt inzake gebruikservaring niet gelijkwaardig is met een rechtstreekse aansluiting stelt zich de vraag of een genotifieerd middel, zonder het doorlopen van het nationale toelatingstraject, ook rechtstreeks kan aansluiten op voorwaarde dat het middel kan samenwerken met de technische standaarden en de delen van de generieke digitale infrastruktuur?

Evaluatie van een aantal andere aanvullende eisen

Reële administratieve vereenvoudiging voor de burger wordt slechts gerealiseerd als identificatie-middelen breed inzetbaar zijn. Een aantal van de voorziene aanvullende eisen kan hierop een belangrijke rem plaatsen en kan bovendien de interoperabiliteit van deze identificatie-middelen binnen Europa hypothekeren.

- Art. 2.2, 2de lid, punt (f) / De Aanvrager verwerkt gegevens over een gebruiker van een middel op een wijze die is **afgescheiden** van gegevens over het gebruik van dat middel door die gebruiker.

  De consequenties van deze vereiste zijn vandaag moeilijk te beoordelen zonder verdere verduidelijking van het objectief dat wellicht op meerdere manieren kan worden bereikt.

- Art. 2.3 Eisen aan middel / Het middel functioneert met de daarvoor benodigde onderdelen van de generieke digitale infrastruktuur.

  Het verdient aanbeveling dat de digitale infrastruktuur van de overheid toch ook de algemeen aanvaarde open standaarden zou ondersteunen die hiervoor gangbaar zijn in de markt (vb OpenID Connect).

- Art. 2.19 Omgaan met gegevens / Een houder van een erkenning … alle gegevens … niet worden gebruikt voor een ander doel dan **authenticatiedienstverlening**.

  Het is zo dat eIDAS zeer stringente eisen oplegt aan 'Electronic Identification Means' (EIM) en 'Qualified Trust Service Providers' (QTSP) met betrekking tot de opslag en het gebruik van data. Het beoogde doel kan derhalve makkelijker bereikt worden door aanbieders van privatieve middelen te verplichten van te voldoen aan de eIDAS regelgeving voor EIM of QTSP.

Over itsme®

Sinds 2017 is de itsme®-app de eenvoudige en veilige referentie voor mobiele identificatie & authenticatie met optimale bescherming van je ID-gegevens.

Het ontwerp en de opzet van itsme® gebeurde in lijn met de meest veeleisende Europese wetgeving zoals daar zijn eIDAS (identificatie- en vertrouwensdiensten), GDPR (gegevensbescherming), AML (anti-witwas wetgeving), PSD2 (sterk authenticatiemiddel in het domein van betalingen en open-bankieren). itsme® werd door de Belgische overheid erkend als digitale identiteit in januari 2018 en genotifieerd binnen Europa in december 2019 als 'Electronic Identification Means' conform eIDAS betrouwhaarheidsniveau "hoog". Bijkomend is itsme® onder eIDAS tevens erkend als 'Qualified Trust Service Provider' en beschikt het over een ISO27001-certificaat.

itsme® werd ontwikkeld door een consortium van 7 Europese bank- en telecombedrijven (Belfius, BNP Paribas Fortis, ING, KBC, Orange, Proximus en Telenet).