Terug naar het publieke Web
Manifest voor een duurzame digitale identiteit

De intentie achter de 'NL Wallet' en eIDAS 2.0 is nobel: burgers controle geven over hun eigen gegevens, los van de grillen van Big Tech. Maar in de jacht op innovatie zijn we in een technologische valstrik gelopen: **de Appificatie van de Overheid**.

Door publieke identificatie af te dwingen in private smartphone-applicaties, bouwen we vitale overheidsinfrastructuur op verschuivende zandgronden. We maken de toegang tot burgerrechten afhankelijk van de grillige API-updates van Apple en Google. We dwingen burgers in een consumptiemodel waarin een perfect functionerende smartphone van een paar jaar oud plotseling verouderd en onveilig wordt verklaard. Dit is geen inclusieve overheid; dit is onvrijwillige uitsluiting.

Het kan anders. Niet door méér apps te bouwen, maar door de verborgen kracht van het open internet te herontdekken. We kunnen de complexiteit aan de burgerkant reduceren tot nul, de privacy structureel borgen conform de privacywetgeving, én de Staat de absolute regie teruggeven.

De architectuur: decentraal identificeren, centraal controleren

Het alternatief is een elegant hybride model: we gebruiken de onverslijtbare, app-vrije cryptografie van de browser voor de burger, en leggen het volledige beheer bij een **Nationale Intrekkings-Hub (Revocation Core)** van de overheid.

1. De inclusieve burgerkant (app-vrij & tijdloos)
In plaats van een zware app die constant updates vereist, krijgt de burger eenmalig via een minimalistisch hulpprogramma een hoogwaardig, hardware-beveiligd **client-certificaat (mTLS)** geïnstalleerd in de locale opslag van hun eigen apparaat of browser.

- **Geen app-store:** Dit werkt onafhankelijk van Google of Apple. Het draait op een moderne iPhone, maar net zo stabiel op een oude Android 7-telefoon of een Linux-desktop.
- **Volledige privacy via pseudonimisatie:** Het certificaat bevat *nooit* het BSN in platte tekst. Dit sluit aan bij de strenge eisen van Artikel 87 van de AVG (GDPR-Text) omtrent de verwerking van nationale identificatienummers. Via een deterministische hashing-formule (HMAC) met een geheime overheidssleutel, genereert het certificaat per overheidssector een uniek, onkoppelbaar pseudoniem. Mocht een malafide server het certificaat onderscheppen, dan steelt men een waardeloze bit-reeks die op geen enkele andere overheidssite functioneert. [1]

2. Het overheidsmonopolie (de nationale revocation core)
Dit is de strategische sleutel voor Logius. We verschuiven de miljoenen aan ontwikkelbudget van fragiele frontends naar één soevereine, gecentraliseerde kerntaak: de **real-time intrekkings-infrastructuur**.

- **De digitale grensbewaking:** Net zoals een fysiek paspoort 10 jaar geldig is maar direct kan worden gesignaleerd in het Basisregister Reisdocumenten, zo werken we hier met langdurige certificaten (5 tot 10 jaar) gekoppeld aan een centraal overheidsregister.
- **De kill-switch:** Verliezen burgers hun apparaat? Dan melden zij dit. Logius activeert de digitale 'kill-switch' in de centrale database. Binnen een fractie van een seconde is het certificaat landelijk ongeldig.

- **Flitsende performance:** Via hyper-gecomprimeerde cryptografische bit-arrays (Bloom Filters) wordt de status van ingetrokken certificaten continu gepusht naar de lokale geheugenblokken van de webservers van de Belastingdienst, DUO of de zorg. De controle vindt lokaal plaats in minder dan een microseconde, zonder vertragende netwerkoproepen tijdens het inloggen.

Waarom dit het DigiD-debacle oplost

1. **Geen single point of failure bij inloggen:** Als de centrale inloghub van DigiD nu hapert, ligt heel digitaal Nederland plat. In dit model vindt de cryptografische controle decentraal plaats op de webserver van de instantie zelf. Zelfs als de centrale overheidskern onder stroom staat, blijft de toegang tot de rest van de overheid open.
2. **Echte soevereiniteit:** We zijn niet langer de gijzelaar van Google's Play Store of Apple's App Store policies. De overheid bepaalt de cryptografische standaard, niet Silicon Valley. Dit model voldoet aan de richtlijnen van de European Data Protection Board (EDPB) door dataminimalisatie structureel af te dwingen.
3. **Privacy by design:** Het simpelweg kopiëren of blootstellen van een nationaal ID-nummer voor identificatie is riskant. Dit werd eerder al bestraft door de Belgische Gegevensbeschermingsautoriteit (INPLP), die een boete oplegde voor het disproportioneel eisen van eID-gegevens. Dit ontwerp herstelt de wettelijke plicht uit Artikel 25 van de AVG (Privacy-Regulation) om gegevensbescherming door ontwerp en standaardinstellingen te integreren. We minimaliseren data-overdracht aan de poort. De overheid acteert niet als een alziende identiteitsprovider die elke inlogbeweging logt, maar als de ultieme, passieve scheidsrechter die enkel valideert of een sleutel nog rechtmatig is. [2, 3, 4]

Conclusie

Laten we stoppen met het bouwen van de zoveelste bug-gevoelige app die burgers dwingt mee te doen aan de hardware-ratrace. Laten we terugkeren naar de principes van het open, robuuste web. Geef de burger een onverslijtbare digitale sleutel, en geef Logius het soevereine beheer over het nationale slot.

[1] https://gdpr-text.com
[2] https://www.edpb.europa.eu
[3] https://inplp.com
[4] https://www.privacy-regulation.eu