Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Logius
Programma eID

Routeringsvoorziening
Logius

Contactpersoon
Coen Glasbergen

Datum
7 november 2018

notitie Ter informatie: Routeringsvoorziening en OIDC koppelvlak

1 INLEIDING

Deze notitie geeft een update over de ontwikkelingen rondom de OpenID Connect (OIDC) standaard, waartoe besluiten en later praktische toepassing binnen het programma eID aanleiding geven. Deze notitie is bedoeld ter informatie van Forum Standaardisatie.

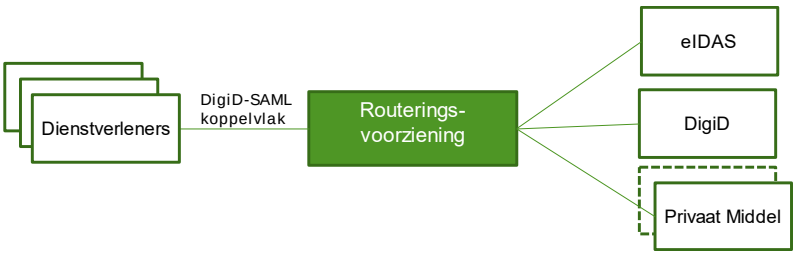
2 UITGANGSSITUATIE

Op dit moment is SAML de standaard voor authenticatie die op de 'Pas toe of leg uit'-lijst staat. Forum Standaardisatie heeft eerder uitspraken gedaan over OpenID Connect:

1. In adoptieadvies SAML d.d. 3 april 2014 adviseerde het Forum Standaardisatie over OpenID Connect het volgende: "De standaard [d.w.z. SAML] is 'proven technology' en lijkt daarom voor de komende jaren ook een goede keuze, alhoewel nieuwkomer OpenID Connect veelbelovend is. […] Volg de ontwikkelingen rondom OpenID Connect actief [Forum Standaardisatie i.s.m. eID]."
2. In het expertadvies Oauth d.d. 24 februari 2017 staat:
   "Daarbij is vastgesteld dat OpenID Connect niet voor opneming op de lijst open standaarden in aanmerking komt."
   De motivering ontbreekt daar. Maar betrokkenen geven aan dat men het toen te vroeg vond om de keuze voor OpenID Connect (dat voortbouwt op Oauth) te maken, mede gelet op de reeds bestaande opname van SAML en gelet op dat men eerst een Nederlands profiel voor Oauth wilde ontwikkelen. Bovendien was Oauth aangemeld en niet OpenID connect.
3. In een SAML2.0 evaluatie, besproken met een oplegnotitie in de vergadering van maart 2018: "Geadviseerd wordt om SAML 2.0 op de 'pas toe of leg uit'-lijst te handhaven, maar de ontwikkeling rond Open ID Connect nauw te volgen. Nu al moet worden geanticipeerd op een overgangsfase waarin OIDC naast SAML steeds meer toegepast gaat worden, ook bij de overheid. Er moet worden nagedacht over hoe deze geleidelijke overgang van SAML naar OIDC dit binnen het 'pas toe of leg uit'-beleid vormgegeven kan worden."

3 ONTWIKKELINGEN BINNEN HET PROGRAMMA EID

Het Programma eID is gebaseerd op de Wet Digitale Overheid die momenteel in behandeling is in de Tweede Kamer. In deze wet worden dienstverleners verplicht authenticatie voor hun elektronische diensten aan te bieden middels DigiD en een privaat alternatief voor DigiD (welke wordt verworven middels een aanbesteding). Daarnaast legt de eIDAS-verordening diezelfde partijen de verplichting op om authenticatiemiddelen uit het buitenland (onder voorwaarden) te accepteren. Dienstverleners worden voor deze aansluitverplichting 'ontzorgd' door het ter beschikking stellen van een Routeringsvoorziening, welke als doel heeft de dienstverlener één aanspreekpunt, één contract, één factuur en één koppelvlak te bieden, zie figuur.



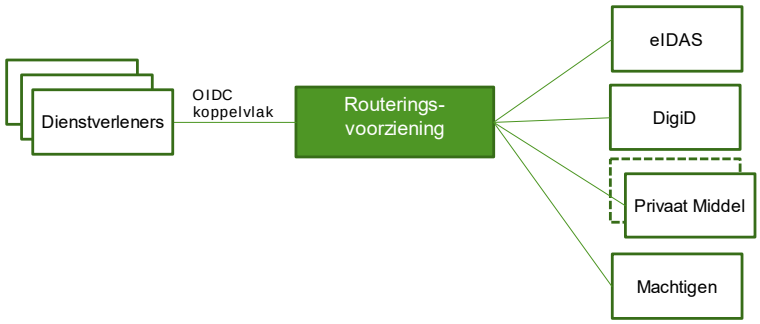
Dienstverleners in de eID-governance hebben aangedrongen op het in eerste instantie aanbieden van het DigiD-SAML koppelvlak. Via de Routeringsvoorziening worden de oudere DigiD-koppelvlakken (CGI/a-select) niet meer aangeboden omdat de wens al langer bestond deze uit te faseren.

Echter, het DigiD-SAML koppelvlak volstaat niet om de gehele set aan technische en functionele wensen te kunnen bieden op langere termijn. Dit geldt bijvoorbeeld op de volgende gebieden:

- Levering van (polymorfe) pseudoniemen i.p.v. BSN's.
- Machtigingsinformatie – de ambitie bestaat ook de nieuwe Machtigingsvoorziening uit het programma Machtigen via de Routeringsvoorziening aan te bieden.
- Attribuutlevering, vooral de minimale dataset vanuit eIDAS.

Een nieuw koppelvlak is dus (op termijn) noodzakelijk. Hiervoor heeft de eID-governance (waarin dienstverleners breed vertegenwoordigd zijn) opgeroepen om niet een nieuw koppelvlak te baseren op SAML, maar op OpenID Connect. Bureau Forum Standaardisatie is hierover geïnformeerd. Belangrijkste redenen zijn de beperkte doorontwikkeling van de SAML standaard en juist de actieve ontwikkelingen binnen de OIDC standaard. Verder vormen de eenvoud en de ondersteuning van de mobile-first strategie van diverse dienstverleners belangrijke redenen hiervoor. SAML voorziet hier minder in.

Op deze manier ontstaat op termijn (enkele jaren) de volgende situatie:



Als uitgangspunt voor de transitie naar deze doelsituatie is bepaald dat eerst beide koppelvlakken naast elkaar worden aangeboden, waarna SAML wordt uitgefaseerd.

4 VERVOLG

Het Programma eID werkt momenteel aan de OIDC specificaties. Het is de bedoeling deze in een lopende pilot met de Routeringsvoorziening te beproeven en de bevindingen te verwerken. Het is de ambitie om OIDC in april 2018 formeel aan te melden voor de ‘pas toe of leg uit’-lijst. De totstandkoming en aanmelding gebeurt met betrokkenheid van de Werkgroep Autorisatie / Authenticatie binnen Kennisplatform API’s.