



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Masterclass “DigiD”

DigiD 4.0 Koppelvlakken

Wim Geurts



Agenda

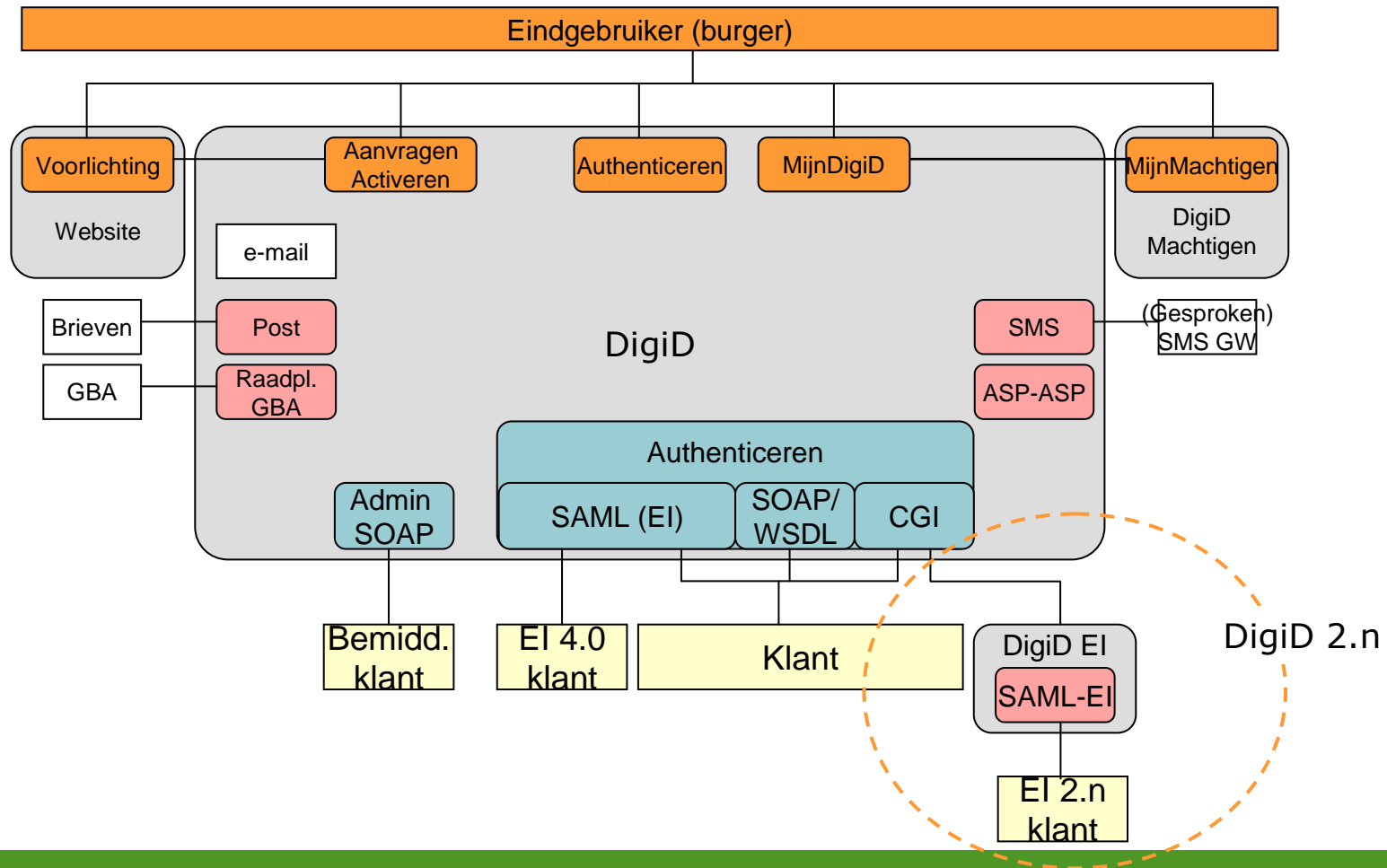
- Koppelvlakken in DigiD 4.0
- Authenticatie KV
- CGI en WSDL/SOAP
- Eenmalig inloggen
- Sectormodel
- Groepsaansluiting
- Vraag & Antwoord

DigiD

Je eigen inlogcode voor de hele overheid



Koppelvlakken in DigiD 4.0





Authenticatie KV

In DigiD 4.0

- CGI
- WSDL/SOAP
- DigiD 4.0 SAML met Eenmalig inloggen
- DigiD 4.0 SAML zonder Eenmalig inloggen
- DigiD 2.n SAML met Eenmalig inloggen



CGI en WSDL/SOAP

Migratie naar 4.0: aanpak:

- Big-bang migratie van 2.n naar 4.0 in 1 service-window

Impact op klanten

- Minimaal (tenzij klant bij inflexibele controles doet op IP-adressen e.d.)

- Migratie stappen

- Testen, ketentesten, proefmigraties

- Migratie

- DNS overname door Consortium
- Synchronisatie 4.0 database met 2.n database
- DNS omzetten naar 4.0: Big-bang migratie
- Post-migratie, evaluatie met verhoogde dijkbewaking
- Afbouwen 2.n (wel t.b.v. logging in stand houden)

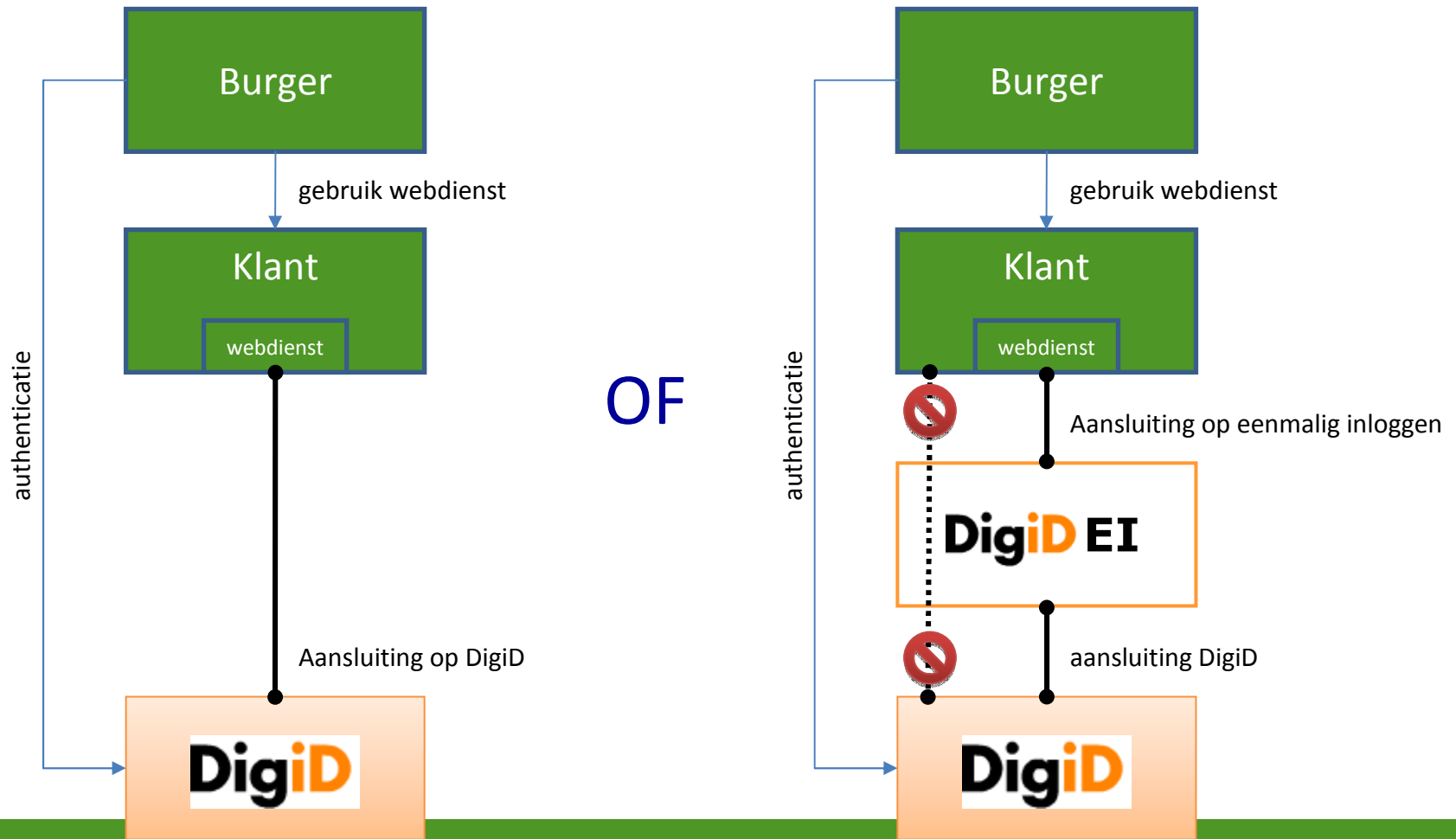


Eenmalig inloggen

- Eenmalig inloggen en de beleving van SSO
- Eenmalig inloggen meer dan alleen SSO
 - Federatief uitloggen
 - Time-outs
 - 15 minuten locale timeout
 - Sessie synchronisatie
 - 120 minuten absolute timeout
- Tussenschermen en Uitlogschermen

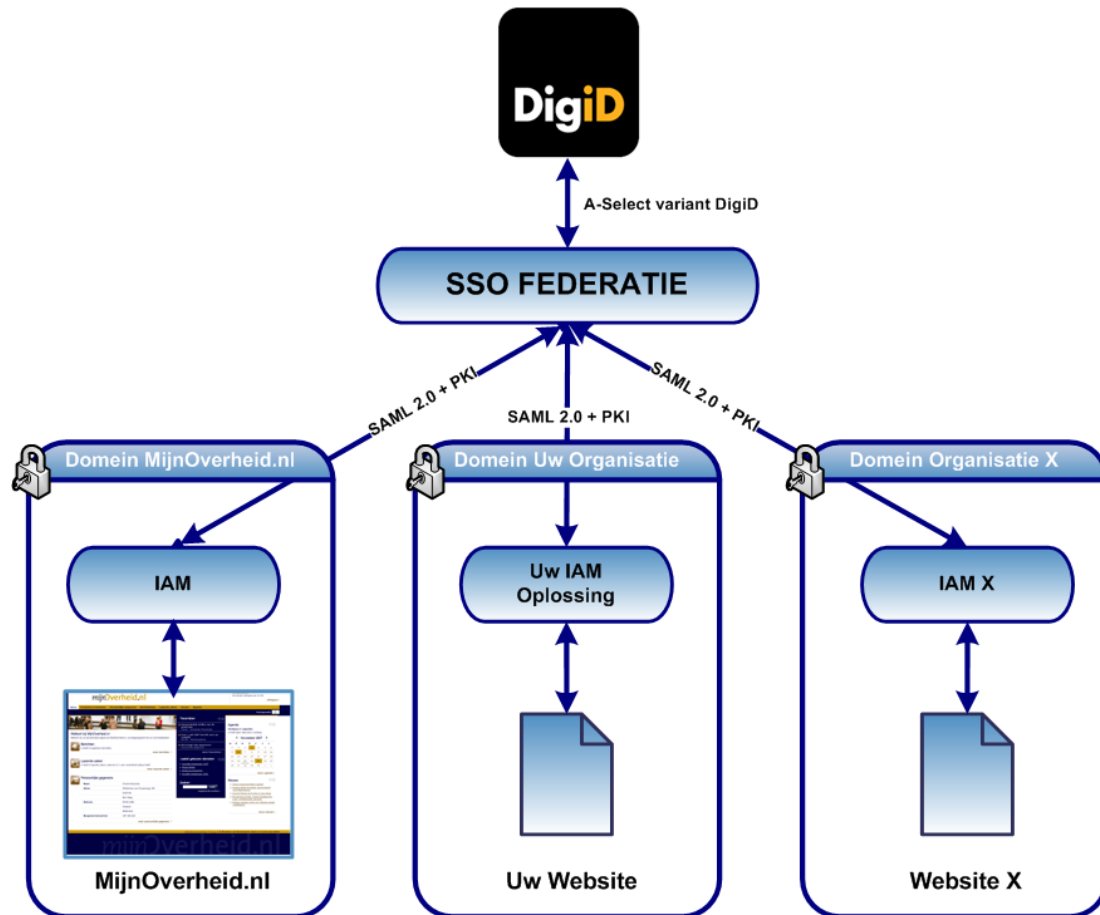


Eenmalig Inloggen in DigiD 2.n





Eenmalig Inloggen



Drie SAML2.0 profielen

1. Web Browser SSO Profile (inloggen)
2. Single Logout Profile (uitloggen)
3. Assertion Profile (sessie sync)

SAML-termen

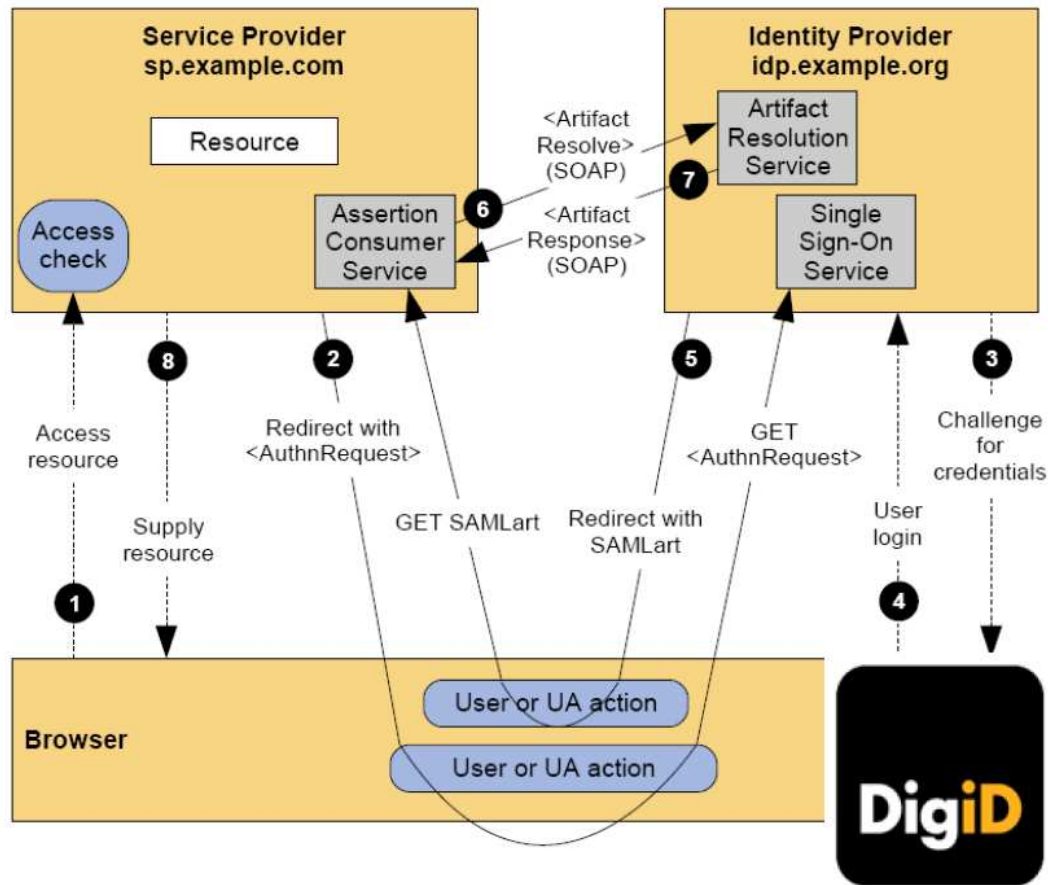
- IDP = Identity Provider
- SP = Service Provider

Mapping DigiD > SAML2.0

- DigiD niveau 5 = unspecified
- DigiD niveau 10 = PasswordProtected Transport
- DigiD niveau 20 = MobileTwoFactorContract
- DigiD niveau 30 = SmartcardPKI



Eenmalig Inloggen



SAML Profile

- Webbrowser SSO

SAML Bindings

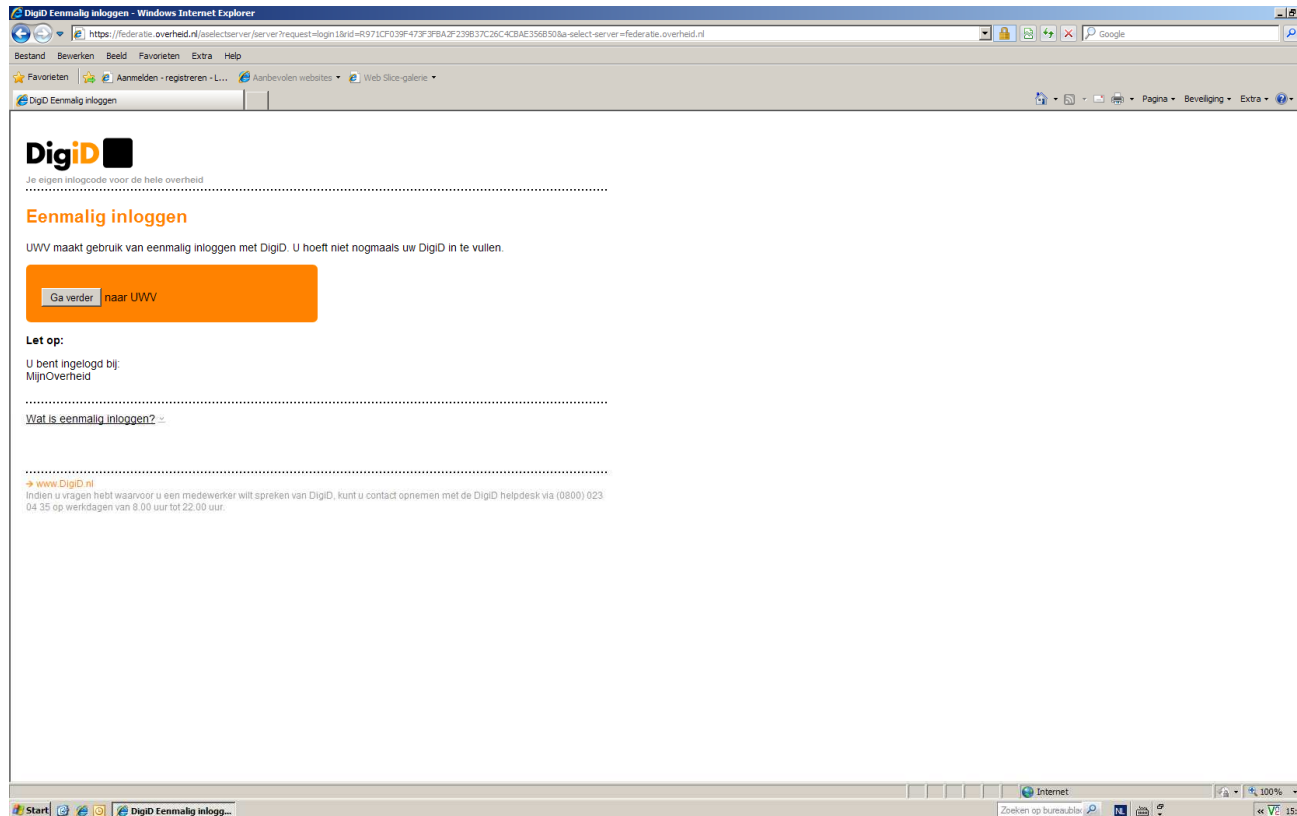
- SP Initiated: HTTP-Redirect binding
- SP Initiated: HTTP-Artifact binding

Resultaat van inloggen

- SSO sessie start op IDP
- BSN met zekerheidsniveau bekend bij SP (= klant)

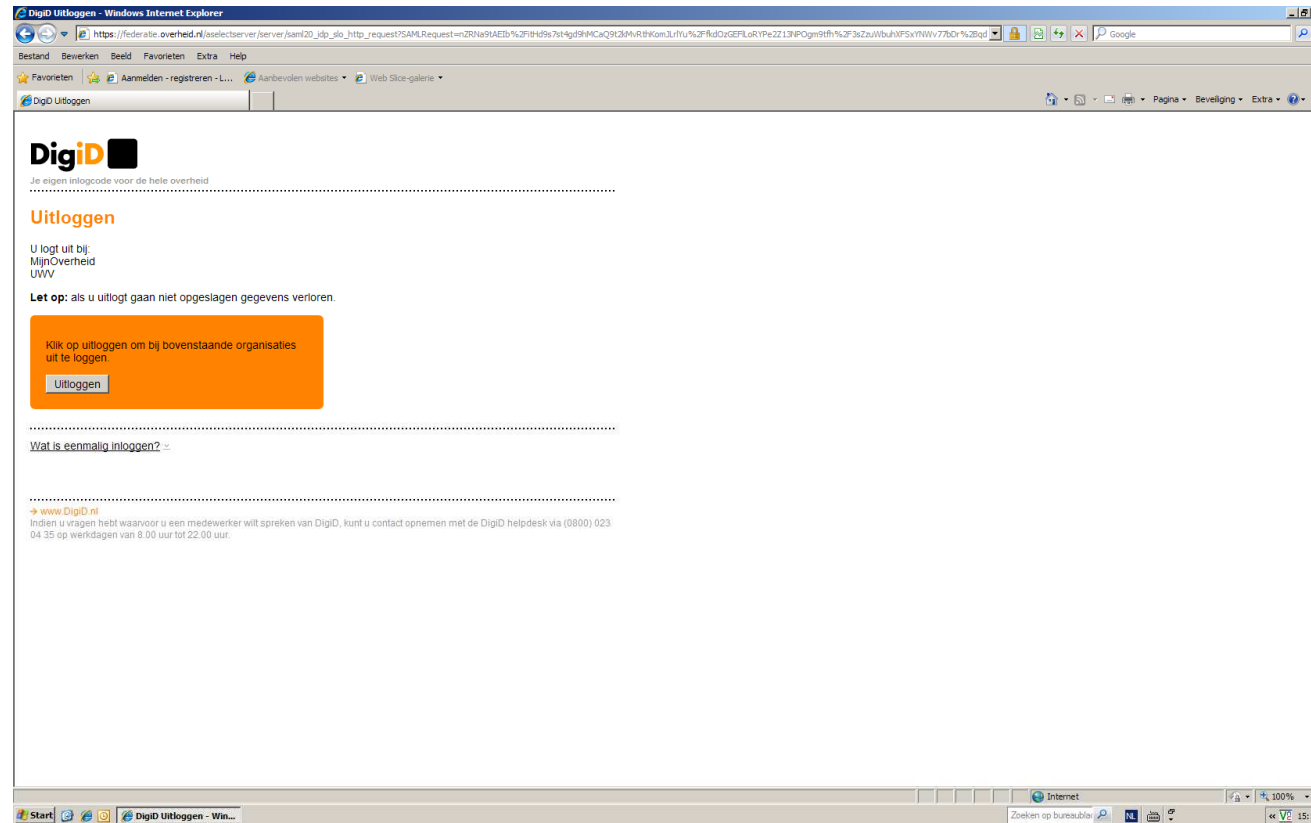


Eenmalig Inloggen: Tussenscherm





Eenmalig Inloggen: Uitloggen





Eenmalig inloggen

Belangrijkste verschillen tussen Eenmalig inloggen in DigiD 2.n en DigiD 4.0

- Signing: SAML assertion in 4.0 gesigned
- Sessie sync: Authorisation Req in 2.n (backchannel), Authentication Req in 4.0 (browser)
- Time-outs: flexibeler in 4.0 met behoud van 15 min inactiviteit
- Uitloggen: via SP (klant) in 2.n, via Eenmalig inloggen scherm in 4.0
- Sectorcode informatie: alleen BSN in 2.n, alle sectoren in 4.0



Eenmalig Inloggen

Aansluiten

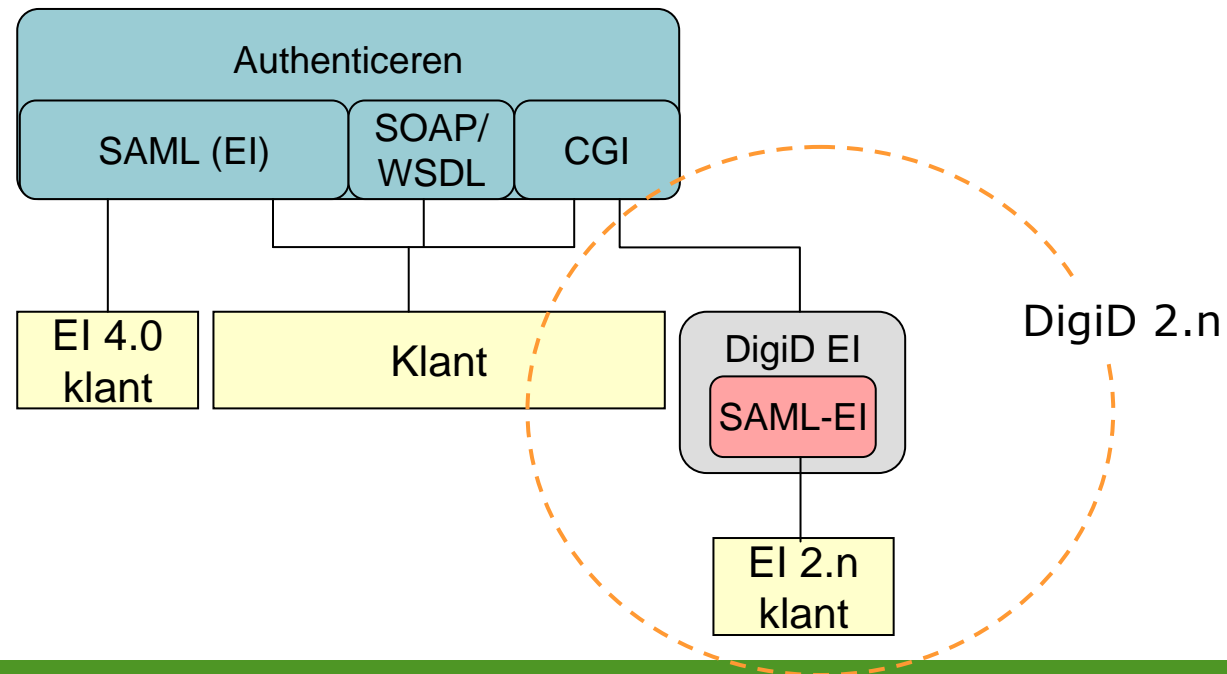
- Metafiles
- Activering vereist Beheerhandeling



Eenmalig Inloggen

Migratie

- Met live-gang van DigiD 4.0 migreert DigiD Eenmalig inloggen mee als gewone klant (en daarmee alle 60 aangesloten Eenmalig inloggen klanten)
- Overgangsscenario's in onderzoek, ondersteuning voor DigiD 2.n Eenmalig inloggen koppelvlak





Sectormodel

Persoonsnummer of sectorale nummer is meestal BSN niet altijd, oa:

- BSN
- A-nummer
- Sofi-nummer
- Bijzondere sectoren

Nieuwe SAML KV

- Naast het sectorale nummer wordt ook de sectorcode meegestuurd.
- Subject: S12345678:012345678



Groepsaansluiting

Wat is een groepsaansluiting?

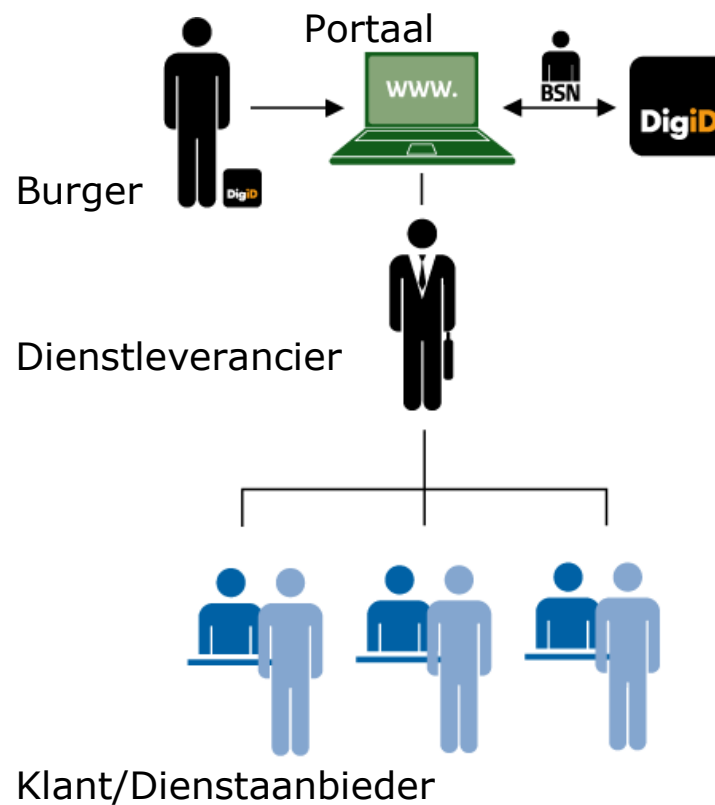
- Een enkele aansluiting van een webportaal op DigiD waarop grote aantallen (zorg)aanbieders zoals apotheken of huisartsen zijn aangesloten.
- Een groepsaansluiting heeft een aantal kenmerken:
 - Minimaal 10 dienstverleners, die verbonden zijn aan hetzelfde webportaal.
 - Iedere dienstverlener in de groep heeft een publieke taak en is daarmee gerechtigd tot gebruik van het [BSN](#).
 - Iedere dienstverlener is verantwoordelijk voor de communicatie richting de eindgebruiker over het webportaal en de diensten.
 - De leverancier van het webportaal rapporteert periodiek aan Logius welke zorgverleners aangesloten zijn op het webportaal.
- Voordeel:
 - Veel kleine dienstverleners kunnen eenvoudig, snel en met weinig kosten op DigiD worden aangesloten



Groepsaansluiting

Aansluiten

- Bij een groepsaansluiting wordt het webportaal, waar de dienstaanbieder aan verbonden is, aangesloten op DigiD.





Groepsaansluiting

- Bij losse aansluitingen is directe zichtbaarheid en zekerheid van de klant vereist (o.a. gerealiseerd door een PKloverheid certificaat op naam van de klant).
- Bij de huidige inrichting van Groepsaansluitingen dient de burger hiervoor een aanvullende controle uit te voeren. Hiervoor is op de DigiD website een controle mogelijkheid ingericht waar hij kan checken of de klant via een Groepsaansluiting daadwerkelijk is aangesloten op DigiD.

<http://www.digid.nl>

“Wie doen mee?”



Vraag & Antwoord

