



Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

DigiD Checklist Testen

Versie 3.2

Datum	1 februari 2010
Status	Definitief

Colofon

Projectnaam	DigiD
Versienummer	3.2
Locatie	I:/xxx
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl 0900 555 4555 (10 ct p/m)

Inhoud

Colofon	2
Inhoud	3
Inleiding	4
1.1 Doel.....	4
1.2 Doelgroep	4
1.3 Leeswijzer.....	4
1.4 Suggesties.....	4
2 Technische eisen DigiD	5
2.1 Netwerkinfrastructuur.....	5
2.2 Interface tussen webdienst en DigiD	6
2.3 Authenticatie van webdienst.....	8
2.4 Technische eisen aan webdienst.....	8
2.4.1 Sessies.....	8
2.4.2 Browser ondersteuning	8
2.4.3 Secure Socket Layer (SSL).....	9
2.4.4 Aanroep en afhandeling DigiD.....	9
2.4.5 Cookies.....	11
2.4.6 Omgang met beveiligingsincidenten	11
3 Technische eisen Eenmalig inloggen	12
3.1 Infrastructuur.....	12
3.1.1 Proces van Eenmalig inloggen.....	13
3.1.2 Federatief inloggen	13
3.1.3 Secure Socket Layer (SSL).....	14
3.1.4 Geforceerd inloggen	14
3.1.5 Sessie synchronisatie.....	14
3.1.6 Passief uitloggen (SP of IdP geïnitieerd)	15
3.1.7 Actief uitloggen (gebruiker geïnitieerd).....	15
3.1.8 Tussenschermen	15
4 Checklist Testen	17

Inleiding

1.1 Doel

Doelstelling van het hanteren van criteria is te zorgen voor veilig, duidelijk, eenduidig en correct gebruik van DigiD door de aan te sluiten webdienst. Ook het imago van DigiD dient te worden beschermd en opgebouwd, waardoor eisen aan het gebruik van logo's en teksten worden gesteld aan klanten van DigiD.

Deze criteria zijn de minimale eisen die aan een webdienst gesteld worden voordat zij wordt aangesloten op de productieomgeving.

1.2 Doelgroep


Deze Checklist Testen is bedoeld voor:


1. overheidsinstellingen en organisaties met een publiekrechtelijke taak die gebruik willen maken van DigiD als authenticatiemiddel;
2. leveranciers die webdiensten ontwikkelen voor overheidsinstellingen.

Daar waar in de tekst "overheidsinstellingen" staat, kunt u ook "organisaties met een publiekrechtelijke taak" lezen.

1.3 Leeswijzer

In deze handreiking is de informatie voor DigiD en de functionaliteit Eenmalig inloggen gecombineerd. De reden hiervoor is, dat grote delen van informatie voor beide doelgroepen gelden. Er zijn echter hierop toch wat uitzonderingen. Om duidelijk te maken welke informatie voor welke doelgroep bedoeld is, zijn de volgende iconen opgenomen:

 dit icoon in de tekst opgenomen als de tekst alleen voor DigiD aansluitingen geldt.

 dit icoon is in de tekst opgenomen als de tekst alleen voor de functionaliteit Eenmalig inloggen geldt.

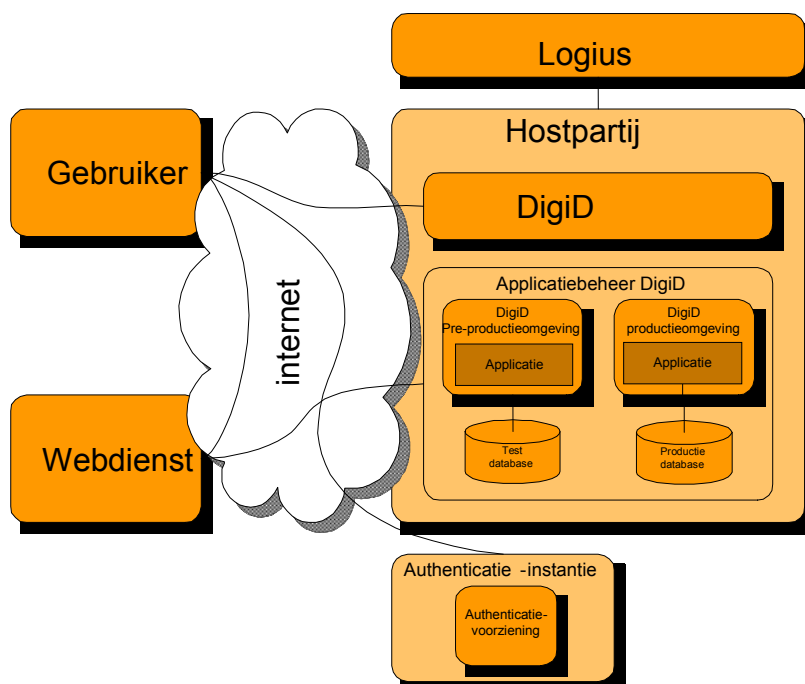
1.4 Suggesties

Logius vindt het belangrijk dat klanten snel en probleemloos gebruik kunnen maken van de diensten van DigiD. Deze handreiking dient hierbij als leidraad. Logius ontvangt graag uw suggesties om dit document te verbeteren. U kunt hiervoor per e-mail contact opnemen met Servicecentrum Logius, servicecentrum@logius.nl.

2 Technische eisen DigiD

2.1 Netwerkinfrastructuur

In figuur 1 is op hoofdlijnen de netwerkinfrastructuur tussen webdienst, gebruiker, Logius, hostingpartij DigiD, applicatiebeheer DigiD en Authenticatie-instansie weergegeven.



Figuur 1: authenticatie processchema DigiD

De DigiD omgeving, inclusief de website, is gehost in een beveiligd datacenter. Van hieruit zijn beveiligde verbindingen ingericht met alle benodigde partijen. De gebruiker benadert de webdienst en de DigiD website via internet. De webdienst heeft verbinding met de DigiD pre-productie- en/of productieomgeving.

De DigiD pre-productieomgeving en productieomgeving beschikken over een applicatiedatabase. De DigiD pre-productieomgeving beschikt daarnaast over test-accounts.

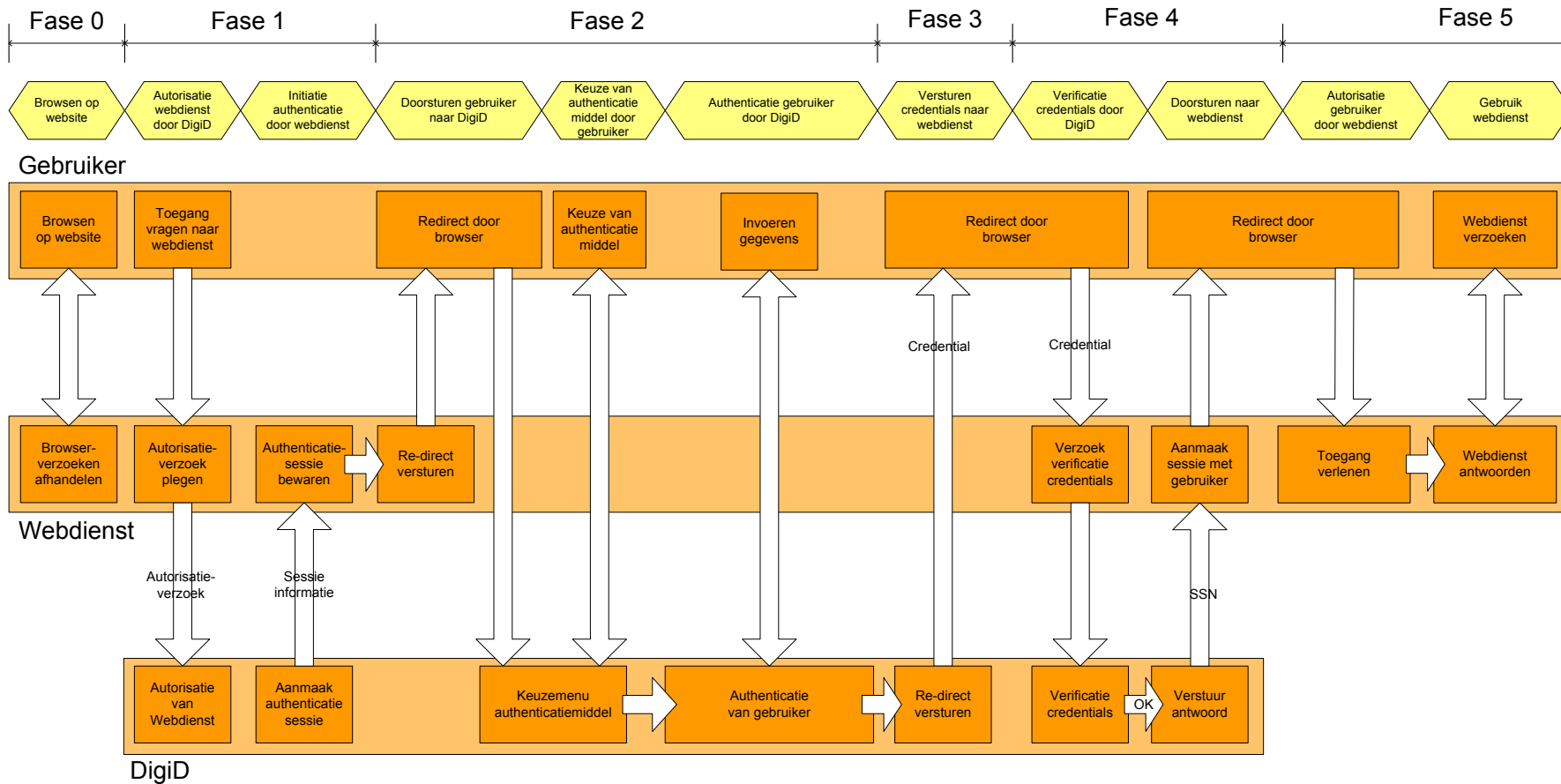
N.B.

- Zorg dat de webdienst de, van toepassing zijnde, databases kan benaderen (wanneer de webdienst zich in een demilitarized zone (DMZ) tussen twee firewalls bevindt).
- Indien een gebruiker de authenticatie annuleert, zal DigiD dit in het antwoord op de API aanroep in Fase 4 d.m.v. een resultcode teruggeven. Een webdienst dient hiermee dan een passende boodschap te tonen. Beheerders van webdiensten dienen de foutafhandeling zelf voor hun rekening te nemen.

2.2 Interface tussen webdienst en DigiD

Om DigiD beschikbaar te maken in de applicatie van de klant is een Application Programming Interface (API) beschikbaar. De Application Programming Interface bevindt zich in Bijlage E. Klanten dienen zich aan het concept en processchema van DigiD te houden (zie Figuur 6), wanneer zij op het punt staan een gebruiker te laten authenticeren. Bij het authenticeren van een gebruiker worden onderstaande fasen onderscheiden:

- Fase 0:
De gebruiker navigeert naar de webdienst en wil toegang. De klant weet niet wie de gebruiker is, d.w.z. er is geen applicatie sessie met (de browser van) de gebruiker. De webdienst moet de gebruiker authenticeren en gaat over in Fase 1.
- Fase 1:
De klant neemt contact op met DigiD – door middel van een API aanroep – en verzoekt DigiD om een authenticatie af te handelen. DigiD start een authenticatiesessie met de webdienst. DigiD handelt authenticatieverzoeken van webdiensten alleen maar af als de webdienst zich authenticert. De aanroep van de webdienst wordt door DigiD geautoriseerd door een controle op het ID van de webdienst en de bijbehorende authenticatiecode (deze code wordt aangeleverd door DigiD tijdens de aansluitingsprocedure van de webdienst). DigiD zal een antwoord teruggeven met daarin:
 - gegevens die de authenticatie sessie identificeren;
 - de URL van DigiD welke de klant moet gebruiken om de gebruiker door te sturen naar DigiD.
- Fase 2:
De webdienst redirect (de browser van) de gebruiker naar DigiD. Afhankelijk van het door de webdienst aangegeven gewenste minimale zekerheidsniveau kan de gebruiker hier een authenticatiemiddel kiezen. DigiD authenticert vervolgens de burger. Dit vindt plaats buiten de controle van de webdienst. DigiD bepaalt hiermee de identiteit van de gebruiker (A-nummer of BSN). N.B. Bij het redirecten van de browser van de gebruiker naar DigiD, moet DigiD worden getoond in dezelfde browser instance als de aanroepende (https) pagina.
- Fase 3:
DigiD stuurt de gebruiker terug naar de webdienst. DigiD stuurt hierbij gegevens over de afgehandelde authenticatie sessie naar de webdienst.
- Fase 4:
De webdienst verifieert de gegevens van Fase 3 bij DigiD. DigiD zal hierop de identiteit van de gebruiker (A-nummer of BSN) en het zekerheidsniveau terugsturen.
- Fase 5:
De webdienst weet nu om welke gebruiker het gaat en kan hiermee verder om de gebruiker te autoriseren en een nieuwe sessie met de gebruiker op te zetten. Autorisatie van de gebruiker dient door de webdiensten zelf te worden geïmplementeerd.



Figuur 2: authenticatie processchema DigiD

2.3 Authenticatie van webdienst

DigiD autoriseert klanten voor gebruik van zijn diensten. Hiertoe houdt de Serviceorganisatie Logius in een register per webdienst, het volgende bij:

Item	Opmerkingen
Eén of meerdere ID's voor applicaties van webdiensten	Webdiensten kunnen meer dan één applicatie-ID bij DigiD laten registreren om tussen applicaties onderscheid te kunnen maken. In de praktijk hebben webdiensten meestal genoeg aan één ID <u>per</u> zekerheidsniveau. DigiD gebruikt deze applicatie-ID om te bepalen of een webdienst is geregistreerd en welk zekerheidsniveau gewenst is.
DigiD authenticatiecode (shared secret)	Webdiensten krijgen bij aansluiting een unieke en geheime authenticatie van Serviceorganisatie Logius. Het is een parameter die webdiensten bij elke API aanroep dienen mee te geven.

De Serviceorganisatie Logius zal als onderdeel van de formele aansluitprocedure van een webdienst het volgende doen:

- Voor elke aansluitende webdienst worden één of meerdere unieke applicatie-ID's gedefinieerd en uitgegeven, ten behoeve van identificatie van de bron van aanroepen;

2.4 Technische eisen aan webdienst

2.4.1 Sessies

Als een gebruiker de inlogprocedure bij DigiD start, wordt er een uniek nummer (sessie-ID) voor deze inlogsessie gegenereerd. In elke vervolgstap van het proces van authenticatie (elke communicatie tussen de browser van de gebruiker, de webdienst en DigiD), wordt deze sessie-ID gecontroleerd. Zo wordt de integriteit gegarandeerd. Daarnaast wordt aan het eind van het proces het resultaat ook nog gecontroleerd door de webdienst bij DigiD. Zo weet de webdienst zeker, dat de uiteindelijke authenticatie van DigiD afkomstig is.

De volgende eisen worden gesteld aan het gebruik van sessies door de webdienst:

- Wanneer gebruik wordt gemaakt van sessie-ID's, mogen deze na authenticatie niet worden gewijzigd.
- Sessies mogen door de webdienst niet worden doorgegeven aan derden.
- Sessies mogen niet blijven 'hangen' en moeten door de webdienst actief worden afgesloten.
- De webdienst moet om kunnen gaan met geannuleerde sessies vanuit DigiD.

2.4.2 Browser ondersteuning

De burger wordt via uw webdienst doorverwezen naar DigiD. DigiD biedt ondersteuning voor browsers met de onderstaande configuratie:

- HTML 4.01
- XHTML
- HTTP 1.1

- JavaScript
- SSL (versie 3.0 of hoger)

Uiteraard mogen webbrowsers wel gebruik maken van nieuwere versies van genoemde standaarden en software. In die gevallen geldt wel als bindende voorwaarde dat de gebruikte configuratie backwards compatibel is.

2.4.3 *Secure Socket Layer (SSL)*

De verbinding tussen de productieomgeving van DigiD en de webdienst is beveiligd door middel van eenzijdig SSL uitgegeven door PKIoverheid. De webdienst authenticceert zich aan DigiD door middel van een authenticatiecode (shared secret).

DigiD gebruikt het SSL-protocol voor de communicatie met de gebruiker. DigiD gebruikt daarnaast ook SSL voor communicatie met aangesloten klanten. DigiD vereist hiervoor Services Certificaten (SSL) uitgegeven door een Trusted Third Party (TTP), conform PKIoverheid en op naam van de klant gesteld. SSL is het meest gebruikte veiligheidsprotocol op het internet voor het beveiligen van webdiensten en wordt gebruikt voor het versleutelen van data die wordt uitgewisseld tussen computers.

Het SSL-protocol garandeert:

- Authenticatie: de identiteit van een computer waarmee wordt gecommuniceerd staat vast. Er wordt niet gesimuleerd door iemand met minder goede bedoelingen.
- Integriteit: de data, uitgewisseld met een computer, wordt onderweg niet onderschept en aangepast. Indien dat wel gebeurt, wordt dat gemakkelijk gedetecteerd.
- Vertrouwelijkheid: data wordt versleuteld. Een hacker kan de pakketjes, die worden uitgewisseld tussen de computer(s) en het netwerk, niet lezen.

Op publicatieplein vindt u meer informatie over SSL.

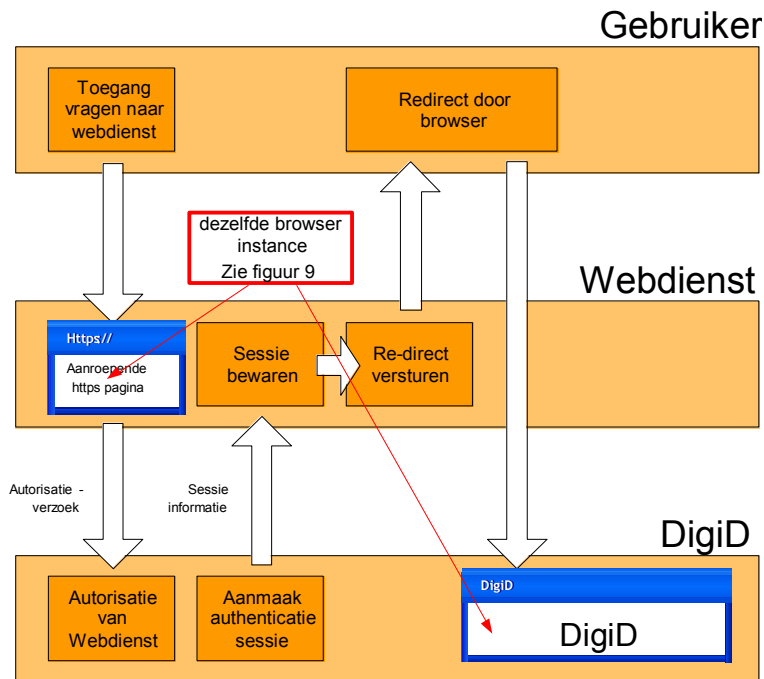
2.4.4 *Aanroep en afhandeling DigiD*

Door de Serviceorganisatie Logius worden eisen gesteld aan de wijze waarop de webdienst DigiD aanroept en de resultaten afhandelt. Deze eisen zijn hieronder opgesomd.

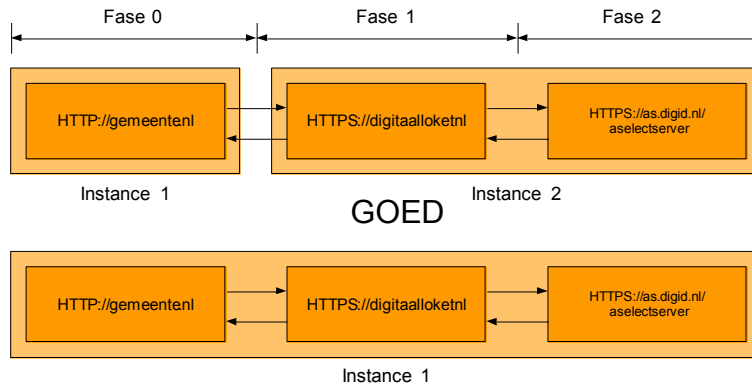
Wijze van aanroepen

Bij het redirecten van de browser van de gebruiker naar DigiD in fase 2, moet DigiD worden getoond in dezelfde *browser instance* als de *aanroepende (https) pagina* (op basis van een gebruikershandeling of automatisch). Zie ook Figuur 4 en 5.

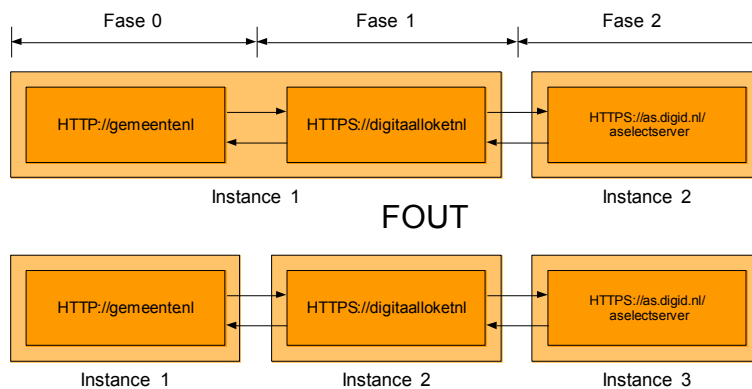
N.B. DigiD mag dus niet worden aangeroepen in een pop-up scherm.



Figuur 3: redirect in dezelfde browser instance



Figuur 4: voorbeelden correcte aanroep DigiD



Figuur 5: voorbeeld foutieve aanroep DigiD

Eigenschappen browser instance

De browser instance met de aanroepende https pagina moet een 'volledig venster' zijn, d.w.z. een venster met adresbalk en knoppenbalk (zie Figuur 6), aangenomen dat deze niet zijn uitgezet door de gebruiker.



Figuur 6: adresbalk en knoppenbalk in browser instance

N.B. Omdat het DigiD venster in dezelfde browser instance verschijnt als de aanroepende https pagina van de webdienst, zijn deze vensters dus altijd even groot. De vensters hoeven niet noodzakelijk beeldschermvullend te zijn. Er mogen geen scrollbars zichtbaar zijn.

Eigenschappen browser instance inhoud


DigiD wordt niet aangeroepen als onderdeel van een frameset in een venster van de browser instance (in de adresbalk wordt niet de DigiD URL weergegeven).

Afhandeling gebruikersacties in DigiD venster (fase 2)

- De door DigiD toegezonden resultcode (zie DigiD API) moet door de webdienst worden afgevangen.
- Indien de resultcode 0040 is (gebruiker heeft het authenticatieproces geannuleerd) moet de webdienst:
 - de aanroepende https pagina (fase 1) tonen binnen dezelfde browser instance.
 - de betreffende sessie met DigiD afsluiten.

2.4.5 Cookies

DigiD maakt geen gebruik van cookies die lokaal worden opgeslagen. Als de klant op zijn webdienst wel gebruik wil maken van cookies adviseert Logius om vóór de authenticatie te controleren of de gebruiker cookies accepteert. Dit voorkomt foutmeldingen na inloggen met DigiD door gebruikers die geen cookies accepteren.

 **Enmalig inloggen maakt wel gebruik van cookies die lokaal worden opgeslagen.**

2.4.6 Omgang met beveiligingsincidenten

De klant dient, bij een vermoeden van misbruik van DigiD, contact op te nemen met Logius.

De klant geeft een contactpersoon aan met wie Logius kan overleggen in het geval dat beveiligingsincidenten optreden.

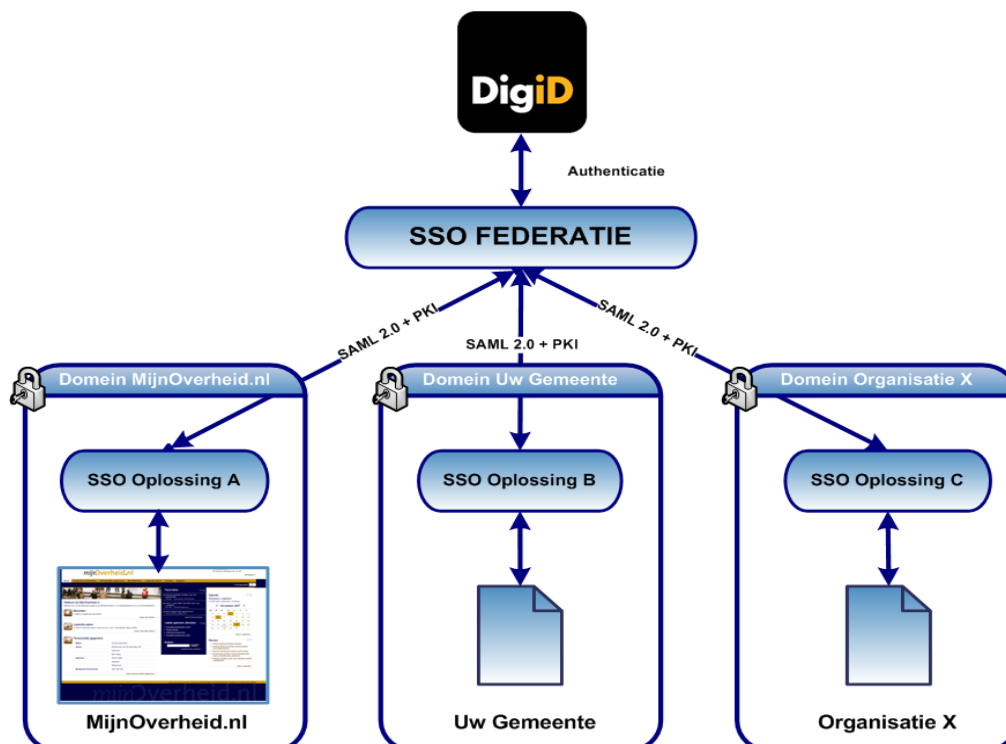
3 Technische eisen Eenmalig inloggen

3.1 Infrastructuur

Binnen de Eenmalig inloggen-Federatie voorziening wordt gebruik gemaakt van federatie-technologie om ervoor te zorgen dat een burger zonder meerdere malen in te loggen, gebruik kan maken van verschillende gepersonaliseerde overheidsdomeinen. De Eenmalig inloggen-Federatie voorziening bestaat globaal uit de volgende partijen, zoals te zien is in figuur 7:

- **DigiD**: de centrale en gezaghebbende bron voor authenticatie van burgers is DigiD.
- **Eenmalig inloggen-Federatie**: beheert alle actieve sessies en stelt vast of een partij een sessie kan aangaan. Dit component, oftewel een *Identity Provider* (IdP), fungeert feitelijk als een verkeersplein en verkeersagent voor de aangesloten deelnemers. De IdP is het software component dat zorg draagt voor het verstrekken van gegevens over de burger aan de aangesloten *Service Providers* (SP). Deze gegevens worden bij de authenticatiebron (DigiD) opgehaald.
- **Deelnemer** (Uw organisatie, organisatie X, MijnOverheid.nl): regelt de administratie en communicatie met de Eenmalig inloggen-Federatie. De communicatie vanuit de deelnemer met de IdP wordt gefaciliteerd door een *Service Provider* (SP). De SP is het software component dat bij een aanvraag van een burger naar een beveiligde pagina het beveiligingsniveau van deze gebruiker controleert. Dit gebeurt door middel van communicatie met de IdP om informatie over de gebruiker op te halen. Zodra de burger is geauthenticeerd geeft de SP identificeerbare gegevens door naar de achterliggende applicaties van de deelnemer om de uiteindelijke persoonlijke pagina's te tonen. Naast het verzorgen van de authenticatie, dienen deelnemers gebruiksactiviteiten van de burger door te geven. Hierbij hoort ook het correct verwerken van een door de burger geïnitieerde logout.

Er wordt met de Eenmalig inloggen-Federatie gecommuniceerd via het SAML2.0 protocol¹. De keuze voor SAML2.0 is gemaakt omdat het een open standaard is en ondersteund wordt door een groot aantal leveranciers en producten. Daarnaast biedt SAML2.0 een Single Logout procedure. Daarmee hoeft een burger slechts eenmaal binnen de Eenmalig inloggen-Federatie uit te loggen om dan binnen de gehele Eenmalig inloggen-Federatie uitgelogd te worden.



Figuur 7: Overzicht Eenmalig inloggen-Federatie

3.1.1 *Proces van Eenmalig inloggen*

In figuur 7 is globaal te zien wat het Eenmalig inloggen principe inhoudt. Hieronder zal nader worden ingegaan op de verschillende functies binnen het proces van Eenmalig inloggen.

3.1.2 *Federatief inloggen*

Het federatief inloggen hoeft niet te beginnen met het inloggen op MijnOverheid.nl. Een burger kan net zo goed eerst inloggen op een gepersonaliseerde pagina van uw organisatie en vanuit daar naar andere deelnemers van de federatie surfen zonder opnieuw in te loggen. In onderstaand voorbeeld wordt er vanuit gegaan dat de burger direct bij uw organisatie inlogt.

- De burger kiest een URL van (of wordt verwezen naar) de inlogpagina binnen het domein van uw organisatie.
- Uw applicatie start de inlogprocedure op en vraagt de burger zich te identificeren.
- De burger doorloopt de identificatieprocedure, waarbij authenticatie in twee fasen plaatsvindt. Allereerst via een component van uw applicatie (de SP) en in tweede instantie de Eenmalig inloggen-Federatie. Dit gebeurt doordat uw SP de burger doorleidt naar de Eenmalig inloggen-Federatie, dit is een transparant proces; de burger merkt hier niets van. Als blijkt dat de burger geen sessie heeft met de Eenmalig inloggen-Federatie, wordt via DigiD een sessie aangemaakt. De burger krijgt hierbij een Eenmalig inloggen-Federatie Ticket Granting Ticket2 (TGT) en een lokale ticket3 (LT) voor uw applicatie.
- Uw lokale applicatie stelt op basis van gegevens vanuit de Eenmalig inloggen-Federatie het volgende vast:
 - Het Burgerservicenummer (BSN).
 - Het zekerheidsniveau. Dit is indicatie *Basis*, *Midden* en *Hoog*.

- Deze zekerheidsniveaus zijn gelijk aan de DigiD zekerheidsniveaus. De Eenmalig inloggen-Federatie accepteert authenticaties vanaf zekerheidsniveau *Basis*. DigiD zekerheidsniveau *Laag* is niet voldoende voor toegang tot de Eenmalig inloggen-Federatie.
- Uw lokale applicatie bepaalt of het zekerheidsniveau voldoende is.
- Uw lokale applicatie creëert een lokale sessie voor de burger, en geeft de burger toegang tot het gepersonaliseerde domein. Indien de burger opnieuw bij dezelfde applicatie toegang probeert te krijgen, zal aan de hand van de lokale ticket vastgesteld worden dat deze burger zich al geauthenticeerd heeft. Indien de burger bij een andere applicatie toegang probeert te krijgen en reeds een actieve sessie heeft binnen de federatie, zal op basis van het TGT toegang verleent worden. Er hoeft dan dus niet opnieuw ingelogd te worden bij DigiD.

3.1.3 *Secure Socket Layer (SSL)*

De verbinding tussen de productieomgeving van DigiD en de webdienst is beveiligd door middel van tweezijdig SSL met PKIoverheid services-certificaten. Voor elke webdienst wordt het SSL-certificaat opgeslagen in de certificate-store.

De webdienst authenticceert zich aan DigiD door middel van een authenticatiecode (shared secret).

DigiD gebruikt het SSL-protocol voor de communicatie met de gebruiker. Deze wordt voor communicatie met DigiD gebruikt voor het opzetten van een tweezijdige SSL sessie. DigiD slaat dit certificaat op in haar certificate-store. DigiD vereist hiervoor Services Certificaten (SSL) uitgegeven door een Trusted Third Party (TTP), conform PKIoverheid en op naam van de klant gesteld. SSL is het meest gebruikte veiligheidsprotocol op het internet voor het beveiligen van webdiensten en wordt gebruikt voor het versleutelen van data die wordt uitgewisseld tussen computers.

Het SSL-protocol garandeert:

- Authenticatie: de identiteit van een computer waarmee wordt gecommuniceerd staat vast. Er wordt niet gesimuleerd door iemand met minder goede bedoelingen.
- Integriteit: de data, uitgewisseld met een computer, wordt onderweg niet onderschept en aangepast. Indien dat wel gebeurt, wordt dat gemakkelijk gedetecteerd.
- Vertrouwelijkheid: data wordt versleuteld. Een hacker kan de pakketjes, die worden uitgewisseld tussen de computer(s) en het netwerk, niet lezen.

3.1.4 *Geforceerd inloggen*

In sommige gevallen kan het wenselijk zijn om een extra authenticatie te vragen aan de burger. Bijvoorbeeld als uw organisatie te allen tijde een authenticatie vereist voor een specifiek gedeelte van het persoonlijk domein. Een geforceerde authenticatie wordt altijd gevraagd, ook als de burger reeds een geldige sessie heeft met de Eenmalig inloggen-Federatie.

3.1.5 *Sessie synchronisatie*

Sessie synchronisatie zorgt ervoor dat wanneer een burger actief is op meerdere applicaties in de Eenmalig inloggen-Federatie deze allemaal actief (ingelogd) blijven. Hierdoor is het mogelijk om meerdere applicaties

van verschillende deelnemers gelijktijdig te gebruiken zonder te worden uitgelogd door time-outs.

- De burger voert een activiteit uit binnen uw applicatie die bij de Eenmalig inloggen-Federatie is aangesloten.
- Per vastgesteld tijdsinterval wordt een zogenaamd sessie synchronisatiebericht verstuurd naar de IdP, waarmee wordt aangegeven bij de IdP dat de laatste 15 minuten activiteit is geweest van de ingelogde burger binnen uw applicatie.

3.1.6 *Passief uitloggen (SP of IdP geïnitieerd)*

Sessie time-out zorgt ervoor dat wanneer er een time-out op uw lokale applicatie plaatsvindt deze ook wordt doorgegeven naar de Eenmalig inloggen-Federatie. Dit betekent niet dat dit leidt tot een uitlog bij de Federatie. Als de burger nog actief is bij andere deelnemers blijft de federatiesessie actief. Op federatieniveau wordt ook een time-out van 15 minuten bijgehouden. Als er op federatieniveau gedurende 15 minuten geen activiteit van een ingelogde burger wordt ontvangen zal er een federatieve uitlog plaatsvinden:

- Uw applicatie stelt vast dat de sessie verlopen is conform de DigiD time-out van 15 minuten.
- Uw applicatie stuurt een logoutbericht naar de Eenmalig inloggen-Federatie met de reden: SP time-out.

Een burger die langer dan 120 minuten actief is binnen de Eenmalig inloggen-Federatie wordt gevraagd om opnieuw in te loggen. De IdP zal na 120 minuten een zogenaamd logout request sturen naar alle SP's waar de burger actief is.

3.1.7 *Actief uitloggen (gebruiker geïnitieerd)*

De burger kiest op een van de websites die op de Eenmalig inloggen-Federatie aangesloten is om uit te loggen. Er wordt een scherm getoond aan de burger waarmee duidelijk wordt gemaakt dat het beëindigen van de sessie (door uit te loggen) betekent dat de burger op alle deelnemende websites waar hij of zij is ingelogd uitgelogd wordt.

Uw Eenmalig inloggen applicatie beëindigt de lokale sessie en stuurt een bericht naar de Eenmalig inloggen-Federatie om uit te loggen bij de Eenmalig inloggen-Federatie en dus ook bij de andere deelnemers. Dit laatste wordt op twee manieren gerealiseerd. Als eerst wordt de gebruiker via redirects langs alle deelnemers waar hij of zij actief was gestuurd met een logout bericht. Als backup wordt er vanuit de Eenmalig inloggen-Federatie ook een backchannel bericht verstuurd naar Eenmalig inloggen applicaties waar de gebruiker in kwestie ingelogd was. Deze backup stap is feitelijk een passieve uitlog.

3.1.8 *Tussenschermen*


Indien een burger inlogt via de Eenmalig inloggen-Federatie zullen er in het authenticatieproces specifieke Eenmalig inloggen-Federatie-schermen getoond worden. Het gaat hierbij om twee schermen:

- **Tussenscherm:** Wanneer de burger van partij A naar partij B gaat krijgt deze een scherm te zien waarop wordt uitgelegd waarom er niet opnieuw ingelogd hoeft te worden bij partij B. Daarnaast wordt in dit scherm aangegeven waar de burger nog meer is ingelogd in de huidige sessie.
- **Uitlogscherm:** Wanneer de burger bij een partij op uitloggen klikt krijgt deze een scherm te zien waarop wordt uitgelegd wat uitloggen precies betekent. Federatief uitloggen houdt in dat er bij

alle partijen waarbij is ingelogd ook uitgelogd wordt. In dit scherm wordt aangegeven bij welke partijen er uitgelogd wordt.

4 Checklist Testen

✓	Nr	Criterium DigiD en Eenmalig inloggen	Toelichting
<input type="checkbox"/>	1*	De pagina's van de webdienst direct voor en na het inloggen op DigiD bevatten geen teksten of plaatjes die duidelijk maken dat de site "under construction" is, alsmede geen testgegevens of links naar testpagina's.*	
<input type="checkbox"/>	2	De website vertoont geen errors met: Internet Explorer 6.x of hoger Firefox 2.x of hoger óf De website voldoet aan minimaal HTML 4.01 transitional en kan worden gevalideerd met de HTML-validator van het W3C: http://validator.w3.org .	
<input type="checkbox"/>	3	De server waarop de website wordt gehost ondersteunt minimaal HTTP 1.1 en SSL versie 3.0	
<input type="checkbox"/>	4	Na het inloggen houdt de webdienst een sessie met de gebruikers bij: Na maximaal 15 minuten, zonder activiteiten, verloopt de sessie. Bij uitloggen of als alle browser instances afgesloten worden vervalt de sessie ook.	
<input type="checkbox"/>	5	Indien er van deeplinks gebruik wordt gemaakt, dan wordt voldaan aan de volgende eisen. Deeplinks op de website verwijzen naar de DigiD http site, en niet naar de applicatieserver: Voor aanvragen verwijst u door naar http://www.digid.nl/aanvragen/ ; Voor activeren verwijst u door naar http://www.digid.nl/activeren/ ; Voor vragen en antwoorden verwijst u door naar http://www.digid.nl/vraag-en-antwoord/ .	
<input type="checkbox"/>	6	Uitingen over DigiD op uw website moeten voldoen aan de gestelde eisen in de Communicatie Toolkit DigiD. Zie in de bijlage van de Handreiking DigiD: Toolkit Communicatie.	
<input type="checkbox"/>	6a	U schrijft DigiD met hoofdletters 'D';	
<input type="checkbox"/>	6b	U spreekt over 'DigiD' in plaats van bijvoorbeeld 'de DigiD';	
<input type="checkbox"/>	7	Daar waar u over DigiD spreekt op uw website, maakt u gebruik van de basisteksten. U vermeldt tenminste de volgende informatie: DigiD staat voor Digitale Identiteit; het is een gemeenschappelijk systeem waarmee de overheid op internet	Gebruikersnaam en wachtwoord is ook goed, dit was bij de vorige Checklist Testen namelijk het geval. I.p.v. 'u' mag er ook gebruik worden gemaakt van 'je'.

		uw identiteit kan verifiëren. U kunt zelf uw DigiD aanvragen op www.digid.nl . Met uw DigiD kunt u bij steeds meer overheidsinstellingen terecht.	
<input type="checkbox"/>	8	Voordat de gebruiker van de website wordt doorverwezen naar DigiD, om in te loggen, heeft hij ten minste 1 keer de volgende tekst gezien: "Bij <naam_organisatie> kunt u inloggen met uw DigiD. Voortaan kunt u met DigiD naar steeds meer overheidsinstellingen op internet."	Gebruikersnaam en wachtwoord is ook goed, dit was bij de vorige Checklist Testen namelijk het geval. Ipv 'u' mag er ook gebruik worden gemaakt van 'je'.
<input type="checkbox"/>	9	Op elke plaats waar u op uw website doorverwijst naar DigiD voor authenticatie gebruikt u het website-icoon conform de aanwijzingen: 	
<input type="checkbox"/>	10	Er staan geen DigiD faq's op uw website.	
<input type="checkbox"/>	11*	Indien een zoekfunctie aanwezig is op de website (voor zoeken binnen de website) is DigiD te vinden door 'DigiD' in te tikken in de zoekfunctie.	
✓	Nr	Criterium alleen voor DigiD	Toelichting
<input type="checkbox"/>	12	Het te gebruiken SSL servercertificaat: moet zijn uitgegeven door een trusted party binnen de PKIoverheid; <ul style="list-style-type: none"> • moet op naam zijn gesteld van de klant; • mag niet verlopen zijn; • een gebruiker met het stamcertificaat in de browser moet zonder een foutmelding in de browser verbinding kunnen maken met het https deel van de webdienst. 	
<input type="checkbox"/>	13	De afhandeling van DigiD door de webdienst voldoet aan alle eisen die zijn genoemd in hoofdstuk 2:	
<input type="checkbox"/>	13a	De DigiD inlogschermen worden getoond in dezelfde browser-instance als de pagina van de webdienst die wordt getoond direct vòòr het inloggen op DigiD (deel 1). De delen 2 en 3 worden in dezelfde browserinstance getoond.	
<input type="checkbox"/>	13b	De pagina van de webdienst voor het inloggen op DigiD wordt getoond in een browser-instance waarbij tenminste de URL van de pagina zichtbaar is in de adresbalk.	
<input type="checkbox"/>	13c	Het (nieuwe) scherm moet minimaal alle functionaliteit tonen zonder schuifbalken (scroll-bars).	

<input type="checkbox"/>	13d	De inlogschermen worden niet in een frame gepresenteerd aan de gebruiker.	
<input type="checkbox"/>	13e	Indien DigiD een resultcode teruggeeft aan de webdienst (met uitzondering van resultcode 0000 of 0040) bevat de pagina die wordt getoond de letterlijke foutmelding "Er is een fout opgetreden in de communicatie met DigiD. Probeer u het later nogmaals."	
<input type="checkbox"/>	13f	Als de gebruiker het authenticatieproces annuleert (resultcode 0040) komt de gebruiker terug in het scherm waar vandaan hij vertrok. Eventueel wordt een apart tussenscherm getoond met de mededeling dat het inloggen geannuleerd is. Dit gebeurt in dezelfde browser instance.	
<input type="checkbox"/>	14	Het authenticatieproces verloopt conform de API	
<input type="checkbox"/>	14a	De webdienst roept DigiD voor authenticatie aan via de URL die in het aansluitpakket wordt genoemd of in de testsituatie, de URL die in het testpakket wordt gebruikt.	
<input type="checkbox"/>	14b	Het éérste verzoek tot authenticatie "request=authenticate" (hoofdstuk 2, fase 1) slaagt en verloopt conform specificaties.	
<input type="checkbox"/>	14c	De URL waarnaar de browser in fase 4 (zie hoofdstuk 7.2, fase 4 in de Handreiking DigiD) wordt geredirect is gelijk aan de "URL-aansluiting" (zie hoofdstuk 2, fase 1).	
<input type="checkbox"/>	14d	Het tweede request tot verificatie "request=verify_credentials" (zie hoofdstuk 2, fase 4) slaagt en verloopt conform specificaties.	
<input type="checkbox"/>	15	Bij verificatie van de authenticatie (paragraaf 3.6 van de API, bijlage van de Handreiking) moet de webdienst elk door DigiD teruggekoppeld authenticatieniveau dat gelijk is of hoger dan het door de webdienst minimaal vereiste zekerheidsniveau accepteren.	
<input type="checkbox"/>	16	Er worden door de webdienst geen veldwaarden op het scherm getoond.	
<input type="checkbox"/>	17	De inloggegevens moeten rechtstreeks door de gebruiker op het scherm van DigiD worden ingevoerd.	
<input type="checkbox"/>	18	De applicatie-id wordt niet doorgegeven aan de browser van de gebruiker.	
<input type="checkbox"/>	19	De shared secret wordt niet doorgegeven aan de browser van de gebruiker.	

✓	Nr	Criterium alleen voor Eenmalig inloggen	Toelichting
<input type="checkbox"/>	20	Situatie 2: Gebruiker is niet ingelogd. De gebruiker gaat naar <persoonlijke pagina in testomgeving van klant> en logt in. Hierdoor is de gebruiker ingelogd.	
<input type="checkbox"/>	21	Situatie 3: Gebruiker is ingelogd bij https://toets.mijnoverheid.nl . In een nieuw tabblad <persoonlijke pagina in testomgeving van klant> openen. Doorklikken naar digitaal loket/mijn aanvragen (of Persoonlijke pagina). Zonder opnieuw DigiD te moeten invoeren kan de gebruiker zijn aanvragen zien.	
<input type="checkbox"/>	22	Situatie 4: Gebruiker is ingelogd bij klant X. Als hij in een nieuw tabblad https://toets.mijnoverheid.nl opent ziet de gebruiker direct zijn persoonlijke startpagina en wordt direct herkend.	
<input type="checkbox"/>	23	Situatie 5: Gebruiker is ingelogd bij https://toets.mijnoverheid.nl . Via P&D wordt een product van klant X aangeklikt daarna wordt de productpagina van klant X geopend zonder dat hij opnieuw moet in loggen en kan de gebruiker het product aanvragen.	
<input type="checkbox"/>	24	Situatie 6: Gebruiker is in 2 tabbladen ingelogd bij https://toets.mijnoverheid.nl en bij klant X. Als de gebruiker uitlogt via de uitlogknop bij klant X is de gebruiker ook uitgelogd bij https://toets.mijnoverheid.nl (hij wordt gevraagd om opnieuw in te loggen).	
<input type="checkbox"/>	25	Situatie 7: Gebruiker is in 2 tabbladen ingelogd bij https://toets.mijnoverheid.nl en bij klant X. Als de gebruiker uitlogt via de uitlogknop bij https://toets.mijnoverheid.nl is de gebruiker ook uitgelogd bij klant X (hij wordt gevraagd om opnieuw in te loggen).	
<input type="checkbox"/>	26	De webdienst biedt een voor de gebruiker zichtbare uitlogfunctionaliteit.	

* Deze technische en communicatieve eisen in de Checklist zijn nog niet verplicht in de testomgeving. Voor de juiste implementatie in de productieomgeving is dit wel een goede vaardigheidsoefening.