Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Functionele beschrijving DigiD: Inloggen met app2app

Datum	11-05-2020
Versie	1.0
Status	Definitief

Colofon

Titel	Functionele beschrijving DigiD: Inloggen met app2app
Versienummer	1.0
Status	Definitief
Organisatie	Logius Postbus 96810 2509JE DEN HAAG servicecentrum@logius.nl

Documentbeheer

Logius is eigenaar van deze Functionele beschrijving. Het document is te vinden op www.logius.nl. Het wordt bij elke release van de DigiD app bekeken en indien noodzakelijk bijgewerkt.

Datum	Versie	Auteur	Opmerkingen
28-04-2020	0.1	Laura van Well	Initiële versie.
11-05-2020	1.0	Laura van Well	Definitieve versie na review door Lisenka Impens en Elise Nabbe.

Documentreferenties

Titel	Versie	Omschrijving
Koppelvlakspecificatie SAML-DigiD	3.5	Document met technische informatie over de SAML-implementatie van DigiD; te vinden op www.logius.nl.
Functionele beschrijving DigiD	1.0	Document dat de functionele werking van DigiD beschrijft; te vinden op www.logius.nl.
Handleiding Aansluiten DigiD	4.2.2	Document dat de stappen beschrijft die een dienstaanbieder moet zetten om aan te sluiten op DigiD; te vinden op www.logius.nl.

Inhoud

1 Inleiding

1.1 Doel

Deze *Functionele beschrijving* beschrijft op hoofdlijnen de functionele werking van het inloggen met de DigiD app vanuit een app van een dienstaanbieder. Na het lezen ervan zal het de dienstaanbieder duidelijk zijn waarvoor hij de app2app-functionaliteit kan inzetten; hoe het inlogproces verloopt voor gebruikers van zijn app; welke fouten daarbij kunnen optreden; en hoe Logius zijn app(s) registreert en beheert.

Het document is geen handleiding voor het implementeren van app2app en bevat geen technische details; daarvoor dient de *Koppelvlakspecificatie SAML-DigiD*.

Voor functionele informatie over DigiD in het algemeen is de *Functionele beschrijving DigiD* beschikbaar. Dit document is daar een uitbreiding op: al het daar beschrevene is ook van toepassing op de DigiD app en de app2app-koppeling. In dit document wordt die algemene DigiD-informatie bekend verondersteld.

1.2 Aansluiten op app2app

Een dienstaanbieder die zijn gebruikers een app aanbiedt waarvoor zij moeten inloggen met DigiD, dient daartoe zijn app met de DigiD app te integreren via een app2app-koppeling. Voorwaarden daarbij zijn:

- Dat hij al een werkende aansluiting heeft op DigiD;
- Dat die aansluiting via het SAML-koppelvlak verloopt.

Een dienstaanbieder die nieuw wenst aan te sluiten op DigiD, raadpleegt hiervoor de *Handleiding Aansluiten DigiD*.

2 DigiD app

2.1 DigiD app in het kort

DigiD kent naast gebruikersnaam en wachtwoord (eventueel aangevuld met sms-controle) nog een inlogmiddel: de DigiD app. Die is ontwikkeld omdat steeds meer burgers hun zaken met de overheid op hun mobiele device afhandelen. Na een initiële activatie, waarbij de gebruiker zichzelf moet authentiseren met een van zijn andere DigiD inlogmiddelen, en een pincode moet kiezen, is de app klaar om mee in te loggen. Dat gaat als volgt:

De gebruiker vraagt toegang tot afgeschermde gegevens op de website van een dienstaanbieder (webdienst). De dienstaanbieder vraagt hem om met DigiD in te loggen en geeft hem daarbij ook de mogelijkheid dat via de DigiD app te doen. De gebruiker hoeft dan alleen zijn pincode in te voeren. De DigiD app zoekt vervolgens contact met de DigiD backend om de authenticatie uit te voeren. Is die succesvol, dan mag de dienstaanbieder de gebruiker toegang verlenen tot de gevraagde gegevens.

Omdat het een tweefactorauthenticatie betreft, is het betrouwbaarheidsniveau gelijk aan dat van gebruikersnaam en wachtwoord, aangevuld met sms-controle (*Midden*). Als de gebruiker ook nog een eenmalige ID-check heeft toegevoegd aan zijn app, is het niveau zelfs *Substantieel*.

2.2 Uitbreiding met app2app

In eerste instantie was de DigiD app alleen geschikt voor inloggen op een website van een dienstaanbieder. Maar steeds meer dienstaanbieders introduceren een app waarin de gebruiker met DigiD moet inloggen. Om de inlogflow voor gebruikers herkenbaar en vertrouwd te houden, heeft Logius de functionaliteit van de DigiD app uitgebreid met een app2app-oplossing, die kortgezegd hierop neerkomt:

De app van een dienstaanbieder opent de DigiD app (op hetzelfde apparaat) op het moment dat authenticatie vereist is; de gebruiker voert in de DigiD app zijn pincode in die op de DigiD backend wordt gecontroleerd. Is de authenticatie succesvol, dan leidt de DigiD app de gebruiker terug naar de app van de dienstaanbieder, die hem toegang verleent tot de afgeschermde gegevens.

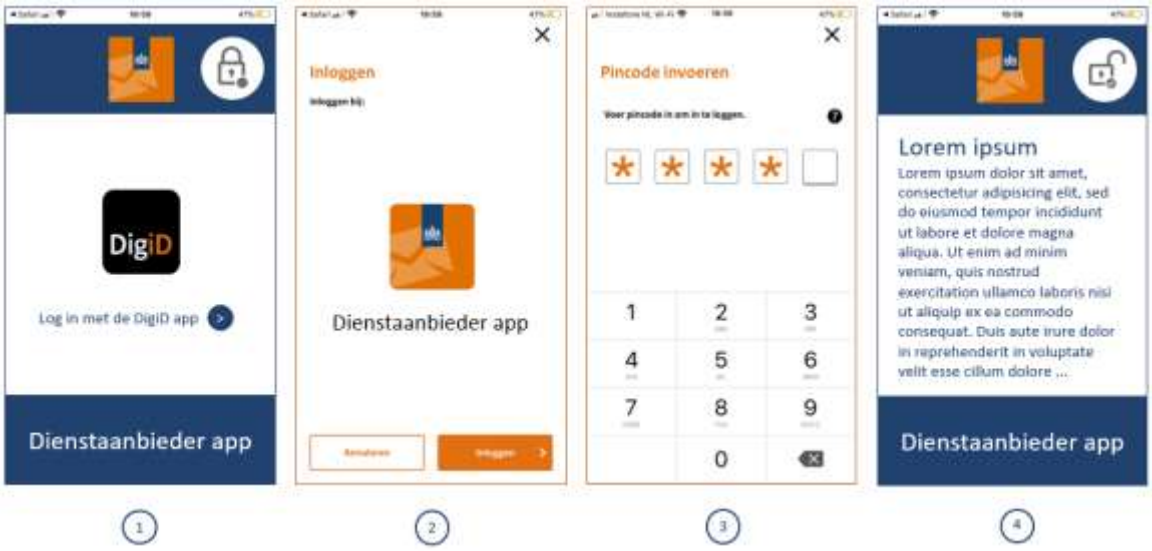
Het volgende hoofdstuk gaat hier in meer detail op in.

3 App2app-functionaliteit

3.1 Schermflow

Onderstaand figuur toont de schermen die de gebruiker doorloopt als hij wil inloggen op de app van een dienstaanbieder:

1. Het inlogscherm in de app van de dienstaanbieder. Dit scherm verzoekt de gebruiker in te loggen met de DigiD app. Als de gebruiker hier gehoor aan geeft, door op de DigiD-link of -knop te klikken, dan opent de DigiD app met:
2. Het scherm in de DigiD app waarop de gebruiker bevestigt dat hij bij de dienstaanbieder wil inloggen. Het scherm toont het icoon en de naam van de dienstaanbieder app. Als de gebruiker kiest voor 'Inloggen', verschijnt:
3. Het scherm in de DigiD app dat de gebruiker vraagt om zijn pincode. Zodra de gebruiker het laatste cijfer van zijn pincode intoetst, en die pincode is correct, dan schakelt de DigiD app terug naar app van de dienstaanbieder.
4. Het scherm in de app van de dienstaanbieder, dat hem de gevraagde gegevens toont (hier weergegeven door de tekst *Lorum ipsum…*). Met andere woorden: de gebruiker is ingelogd in de app van de dienstaanbieder.



Bovenstaande beschrijft de 'happy flow': de gebruiker heeft, voordat hij begon met inloggen, de DigiD app minimaal geactiveerd op het betrouwbaarheidsniveau dat de dienstaanbieder vereist. Dat hoeft niet het geval te zijn:

- Als hij zijn app nog niet geactiveerd heeft, kan hij toch vanuit de app van de dienstaanbieder inloggen met de DigiD app. Hij zal dan tijdens de inlogflow eerst de activatie moeten uitvoeren. Slaagt hij daarin, dan is hij daarna meteen ingelogd in de app van de dienstaanbieder.
- Als de dienstaanbieder niveau 'substantieel' vereist voor inzage in de gegevens, maar de gebruiker heeft de ID-check nog niet aan zijn app toegevoegd, dan zal hij tijdens het inloggen zijn identiteitsbewijs moeten scannen. Lukt hem dat, dan is hij daarna meteen ingelogd.

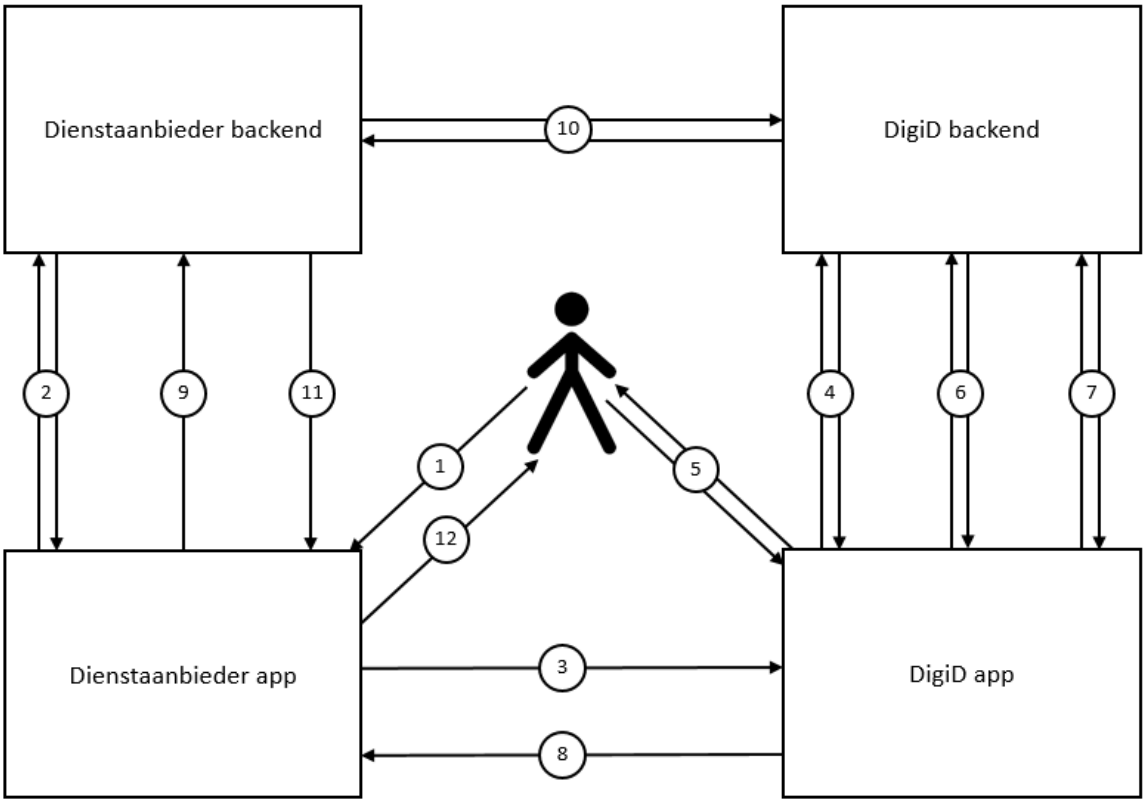
Deze uitgebreidere flows behoren tot de standaard functionaliteit van de DigiD app en zijn niet specifiek voor app2app. Daarom worden ze in dit document niet verder belicht.

Als de gebruiker de DigiD app in het geheel nog niet op zijn toestel heeft staan, zal het operating systeem van zijn device hem niet kunnen openen. In dat geval zal een DigiD-pagina getoond worden in de browser, waarvandaan de gebruiker zelf verdere actie kan ondernemen. Dit zal later in dit document verder toegelicht worden.

3.2 Procesflow

Het proces van app2app-inloggen verloopt als volgt (de stapnummers komen overeen met de nummers in de onderstaande figuur):

1. De gebruiker heeft de app van de dienstaanbieder geopend, wil inzage in gegevens waarvoor een DigiD-authenticatie vereist is en is zodoende op de inlogpagina beland. Daar kiest hij voor inloggen met DigiD.
2. De app van de dienstaanbieder vraagt aan zijn backend toegang tot de afgeschermde informatie. De backend van de dienstaanbieder geeft als antwoord een authenticatieverzoek (SAML) terug.
3. De app van de dienstaanbieder stuurt dat authenticatieverzoek door naar de DigiD app via Android App link of iOS Universal link.
4. De DigiD app vraagt met dat authenticatieverzoek een authenticatiesessie aan bij de DigiD backend.
5. De DigiD app vraagt de gebruiker om zijn pincode.
6. De DigiD app stuurt de pincode naar de DigiD backend ter controle. Die meldt het resultaat van de authenticatie terug.
7. Als de authenticatie geslaagd is, vraagt de DigiD app aan de DigiD backend om een verwijzing naar het authenticatiebericht.
8. De DigiD app stuurt die verwijzing via Android App link of iOS Universal link naar de app van de dienstaanbieder.
9. De app van de dienstaanbieder stuurt de verwijzing door naar zijn backend.
10. De backend van de dienstaanbieder vraagt met de verwijzing bij de DigiD backend het echte authenticatiebericht op (dat het BSN van de gebruiker bevat).
11. De backend van de dienstaanbieder verstuurt de in stap 2 opgevraagde gegevens naar de dienstaanbieder app.
12. De app van de dienstaanbieder toont de gegevens aan de gebruiker.



4 Beheer en rapportage

4.1 Registratie dienstaanbieder app

Om zijn app aan te sluiten op de DigiD app zal een dienstaanbieder hem moeten toevoegen aan zijn al bestaande aansluiting van zijn webdienst op DigiD. Een dienstaanbieder kan bij zijn aansluiting maximaal drie apps aanmelden.

DigiD legt bij de registratie van een dienstaanbieder app bij een webdienst de volgende gegevens vast:

- Naam van de app: deze naam toont de DigiD app ter bevestiging aan de gebruiker tijdens het inloggen.
- Return-URL van app: naar deze URL schakelt de DigiD app terug nadat de gebruiker succesvol is geauthentiseerd.

De DigiD app toont tijdens het inloggen op het bevestigingsscherm ook het app-icoon van de dienstaanbieder, maar dat dient deze bij elk authenticatieverzoek mee te sturen. Ook de return-URL dient in dat verzoek te staan, zodat DigiD daarop een controle kan uitvoeren (zie paragraaf 5.6).

Logius kan ‘Inloggen met de DigiD app’ in één keer voor alle gebruikers uitschakelen. Daarnaast kan voor een specifieke dienstaanbieder al zijn geregistreerde apps in een keer aan- of uitgezet worden. (Zie resp. paragraaf 5.4 en 5.5.)

4.2 Rapportage over authenticaties

Logius levert maandelijks rapportages op die inzicht geven in het aantal authenticaties bij een dienstaanbieder. De app2app-authenticaties zijn daarin opgenomen.

5 Foutsituaties

Dit hoofdstuk beschrijft de foutsituaties die kunnen optreden tijdens het inloggen met app2app, en hoe die worden afgehandeld.

5.1 DigiD app niet gevonden

Als de app van de dienstaanbieder naar de DigiD app schakelt om de gebruiker te laten inloggen, kan het zijn dat de DigiD app niet geopend kan worden. Dat kan verschillende oorzaken hebben:

- De gebruiker heeft de DigiD app niet op zijn apparaat geïnstalleerd.
- Universal links werken niet (iOS): Sinds de release van iOS 13.0 worden de Universal links – die nodig zijn om een app te herkennen op het apparaat – niet altijd direct geïnstalleerd na het downloaden van een app. Zonder die registratie lijkt het alsof de DigiD app niet op het apparaat staat terwijl dat wel zo is; de gebruiker kan onterecht niet inloggen in de dienstaanbieder app.

Als de DigiD app niet geopend kan worden, toont DigiD een webpagina in de browser. Omdat niet bekend is om welke de reden de app niet geopend kon worden, reikt die pagina de gebruiker voor beide oorzaken een oplossing aan:

- Voor het geval de DigiD app nog niet op het apparaat staat: De gebruiker kan via een link de store openen om de app te downloaden. Pas als hij dat gedaan heeft, kan hij opnieuw proberen in te loggen in de app van de dienstaanbieder.
- Voor het geval de app wel op het apparaat staat, maar de Universal links niet werken: De gebruiker kan de DigiD app alsnog handmatig openen via een URL-schema[1, 2]. Staat de app tóch niet op het apparaat, dan toont DigiD een melding, inclusief een link naar de app store.

5.2 DigiD app niet geactiveerd

Als blijkt dat de gebruiker de DigiD app nog niet heeft geactiveerd, wordt zijn authenticatie niet afgebroken, maar zal hij tijdens de inlogflow de activatie moeten uitvoeren. Slaagt hij daarin, dan kan hij daarna de authenticatie vervolgen.

Zie ook paragraaf 3.1

5.3 DigiD app op te laag betrouwbaarheidsniveau

Als blijkt dat de gebruiker de DigiD app niet geactiveerd heeft op het betrouwbaarheidsniveau dat de dienstaanbieder vereist, wordt zijn authenticatie niet afgebroken, maar zal hij tijdens het inloggen de ID-check moeten uitvoeren. Slaagt hij daarin, dan kan hij daarna de authenticatie vervolgen.

Zie ook paragraaf 3.1.

5.4 Inloggen met DigiD app uitgeschakeld

Op de DigiD backend kan het inloggen met de DigiD app in zijn geheel worden uitgeschakeld. Is dat het geval, dan kan een gebruiker ook niet met app2app inloggen bij zijn dienstaanbieder.

---

[1] De werking van dit uitwijkmechanisme wordt alleen gegarandeerd als de dienstaanbieder zijn SAML-authenticatieverzoek via redirect binding verstuurt; zie voor meer informatie Koppelvlakspecificatie SAML-DigiD.

[2] Het wordt de dienstaanbieder aangeraden datzelfde mechanisme te implementeren voor het geval dat zijn app na het inloggen met de DigiD app niet geopend kan worden: ook hij kan de gebruiker de app handmatig laten openen vanaf een webpagina.

De dienstaanbieder kan Logius vragen app2app voor zijn eigen app(s) op te heffen via een wijzigingsformulier op de website van Logius.

5.5 App2app voor dienstaanbieder uitgeschakeld

Voor een dienstaanbieder kan op de DigiD backend de app2app-functionaliteit worden uitgeschakeld. In dat geval zal een gebruiker in géén van de apps van die dienstaanbieder kunnen inloggen met de DigiD app.

5.6 Onjuiste return-URL

De dienstaanbieder heeft bij het aanmelden van zijn app2app-aansluiting de return-URL van zijn app opgegeven. Hij dient die ook in elk authenticatieverzoek mee te sturen, zodat DigiD kan controleren of de meegestuurde URL overeenkomt met de geregistreerde. Is dat niet het geval, dan breekt DigiD de authenticatie af.

5.7 Onjuiste pincode

Als de gebruiker er niet in slaagt de juiste pincode in te voeren in de DigiD app, raakt hij niet ingelogd. Hij krijgt drie kansen; daarna breekt DigiD de authenticatie af en deactiveert de DigiD app.

5.8 Gebruiker annuleert

Als de gebruiker het inloggen in de DigiD app annuleert, breekt DigiD de authenticatie af.

5.9 Sessie verlopen

Als de gebruiker te lang de tijd neemt tijdens het inloggen, en de DigiD backend ontvangt 15 minuten lang geen bericht van de DigiD app, dan breekt DigiD de authenticatie af. Dat gebeurt ook als de gebruiker het toestel waarop hij de DigiD app heeft geactiveerd in ‘private mode’ heeft staan.

5.10 Technische storing

Er kan een technische storing optreden in de koppeling tussen DigiD en de dienstaanbieder, of intern bij DigiD, waardoor inloggen niet mogelijk is.

6 Woordenlijst

Woord/afkorting	Betekenis
Android App link	Mechanisme om op Android-apparaten vanuit een website of app rechtstreeks naar content binnen een andere app te linken. Staat de te openen app niet op het apparaat, dan wordt de corresponderende webpagina geopend in de browser. Android controleert het eigenaarschap van het betreffende domein waartoe de App links behoren.
Betrouwbaarheidsniveau	Het niveau van het middel waarmee de gebruiker inlogt. DigiD kent de volgende betrouwbaarheidsniveaus: • Basis: Gebruikersnaam & wachtwoord, • Midden: Gebruikersnaam, wachtwoord en sms-controle, of DigiD app zonder ID-check, • Substantieel: DigiD app met uitgevoerde ID-check, • Hoog: Applet op een identiteitsdocument.
Dienstaanbieder	De aanbieder van de webdienst waarbij een gebruiker inlogt met DigiD. Voorbeelden van dienstaanbieders zijn de Belastingdienst, de gemeente Amsterdam en Achmea.
DigiD app	Inlogmiddel van DigiD met betrouwbaarheidsniveau Midden of Substantieel; het is een applicatie voor een mobiel apparaat (telefoon, tablet, etc.) waarmee gebruikers zich identificeren met een pincode.
Gebruiker	De burger die zich met zijn DigiD (app) authentiseert.
ID-check	Eenmalige controle van paspoort, identiteitskaart of rijbewijs van de gebruiker, door het document uit te lezen met behulp van een NFC-lezer. Na de ID-check is de DigiD app geactiveerd op betrouwbaarheidsniveau Substantieel.
iOS Universal link	Mechanisme om op Apple-apparaten vanuit een website of app rechtstreeks naar content binnen een andere app te linken. Staat de te openen app niet op het apparaat, dan wordt de corresponderende webpagina geopend in de browser. iOS controleert of een Universal link geregistreerd is voor het betreffende domein; het is daarom veiliger dan het gebruik van een URL-schema.
Logius	De beheerorganisatie van DigiD.
SAML	Security Assertion Markup Language; Standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen.
URL-schema	Mechanisme om naar een app te linken middels een omleiding via de browser. Staat de app niet op het apparaat, dan wordt de gebruiker doorgestuurd naar de app store. Een URL-schema is minder veilig dan een iOS Universal link: het biedt niet de garantie dat de bedoelde app wordt geopend, vanwege minder strikte controle op de registratie van de schema's.
Webdienst	Dienst van een (semi-)publiekrechtelijke of privaatrechtelijke instelling met een publieke taak, die via het internet ontsloten wordt.