Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Functionele beschrijving DigiD app

Datum	10-06-2020
Versie	0.2
Status	Definitief

Colofon

Titel	Functionele beschrijving DigiD app
Versienummer	0.2
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
26-05-2020	0.1	Laura van Well	Initiële versie.
10-06-2020	0.2	Laura van Well	Review Lisenka Impens en Marcel Berg verwerkt.

Documentreferenties

Titel	Versie	Omschrijving
Functionele beschrijving DigiD	1.0	Document dat de functionele werking van DigiD beschrijft; te vinden op www.logius.nl.
Functionele beschrijving DigiD: Inloggen met app2app	1.0	Document dat de functionele werking beschrijft van inloggen in de app van een dienstaanbieder met de DigiD app; te vinden op www.logius.nl.
Koppelvlakspecificatie SAML-DigiD	3.5	Document met technische informatie over de SAML-implementatie van DigiD; te vinden op www.logius.nl.

Inhoud

1 Inleiding

1.1 Doel en scope van dit document

De functionele beschrijving beschrijft op hoofdlijnen de functionele werking van de DigiD app. Het document is bedoeld als naslagwerk voor huidige en toekomstige afnemers van DigiD. Na het lezen van dit document zal het voor de afnemer duidelijk zijn hoe de DigiD app past in de authenticatievoorziening DigiD en hoe burgers hem gebruiken.

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

Dit document is geen handleiding voor het aansluiten op DigiD en bevat geen technische details. Daarvoor dient het document *Koppelvlakspecificatie SAML-DigiD*.

Een beschrijving van de specifieke app2app-functionaliteit van de DigiD app - die ervoor zorgt dat burgers in de app van een afnemer kunnen inloggen met de DigiD app - is *Functionele beschrijving DigiD: Inloggen met app2app* beschikbaar.

Inloggen met rijbewijs of identiteitskaart valt vooralsnog buiten de scope van dit document. Voor dit inlogmiddel kan weliswaar de DigiD app worden ingezet als kaartlezer, maar het is in feite een op zichzelf staand middel, dat bovendien nog niet beschikbaar is voor burgers.

1.2 DigiD app in het kort

Sinds 2017 kent DigiD naast gebruikersnaam en wachtwoord (eventueel aangevuld met sms-controle) nog een inlogmiddel: de DigiD app. Die app past bij de ontwikkeling dat steeds meer burgers hun zaken met de overheid op hun mobiele apparaat afhandelen. Bovendien willen meerdere afnemers hun gebruikers vanuit hun app laten inloggen met DigiD. De DigiD app biedt daartoe een gebruiksvriendelijke en uniforme manier.

De DigiD app voldoet qua veiligheidseisen, juridische en technische eisen aan dezelfde hoge standaarden als inloggen met DigiD via de browser. Hij geldt als gelijkwaardig alternatief voor de sms-controle. Bijkomend voordeel is dat toenemend gebruik van de app de sms-kosten doet dalen en daarmee de kosten van DigiD.

Daarnaast maakt de DigiD app hogere betrouwbaarheidsniveaus voor de publieke dienstverlening mogelijk, zoals gedefinieerd in de Europese eIDAS-verordening (naast niveau Laag zijn dat Substantieel en Hoog).

2 Het inlogmiddel DigiD app

2.1 Inleiding

DigiD kent naast gebruikersnaam en wachtwoord (eventueel aangevuld met sms-controle) nog een inlogmiddel: de DigiD app. De DigiD app is ontwikkeld omdat steeds meer burgers hun zaken met de overheid op hun mobiele device afhandelen. Na activatie, waarbij de gebruiker een pincode kiest, 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). Die stuurt hem naar DigiD om in te loggen. De gebruiker kiest voor inloggen met de DigiD app en voert in de app zijn zelfgekozen pincode in. Als die correct blijkt, mag de dienstaanbieder de gebruiker toegang verlenen tot de gevraagde gegevens.

Inloggen met de DigiD app betreft een twee-factor-authenticatie. Het betrouwbaarheidsniveau is gelijk aan het andere twee-factor-middel van DigiD: gebruikersnaam en wachtwoord, aangevuld met sms-controle (Midden). Door een eenmalige ID-check aan te app toe te voegen is de DigiD app ook geschikt om mee in te loggen op niveau Substantieel.

2.2 Samenhang met DigiD

Met DigiD kunnen natuurlijke personen zich gemakkelijk, veilig en betrouwbaar authentiseren voor digitale dienstverlening in het publieke domein. Een van de inlogmiddelen van DigiD is de DigiD app. Een DigiD app moet gekoppeld zijn aan een DigiD account. Een gebruiker kan maximaal vijf DigiD apps activeren. Van elke app legt DigiD activatiegegevens vast, zodat altijd te herleiden is hoe en wanneer een app geactiveerd werd.

De DigiD app gebruikt een cryptografische sleutel als op ‘bezit gebaseerde authenticatiefactor’, die tijdens activatie gebonden wordt aan het mobiele apparaat van de gebruiker, zodanig dat kopiëren naar een ander mobiel apparaat niet mogelijk is. Hiervoor worden de faciliteiten van het mobiele platform gebruikt (system keystore/ keychain services/ secure element).

Een door de aanvrager zelf gekozen 5-cijferige pincode dient als op ‘kennis gebaseerde authenticatiefactor’. Die pincode wordt in gemaskeerde vorm opgeslagen in de DigiD backend. Bij iedere authenticatie moet de gebruiker aan de DigiD-authenticatiedienst beide authenticatiefactoren aantonen.

De DigiD app wisselt alleen berichten uit met de DigiD backend; communicatie met andere systemen, zoals BRP of CRB, loopt altijd via de DigiD backend.

Alle regelgeving en beveiligingseisen die gelden voor DigiD gelden ook voor de app, zoals:

- Welke organisaties het is toegestaan aan te sluiten op DigiD;
- Voorwaarden voor het aanvragen van DigiD;
- Gebruik van digitale certificaten.

Informatie daarover is te vinden in het document *Functionele beschrijving DigiD*.

2.3 Downloaden en activeren

De app is beschikbaar op de twee meest gangbare besturingssystemen voor mobiele apparaten: iOS en Android. De gebruiker kan de app alleen downloaden via de officiële kanalen, resp. App Store en Google Play. Gebruikers worden daar gewezen op de werking en gebruiksvoorwaarden van de DigiD app.

Een gebruiker moet de app eerst activeren voordat hij of zij er mee kan inloggen. Dit gebeurt door een authenticatie met een ander middel dat al actief is bij het account van de gebruiker.

Voor verdere informatie zie paragraaf 3.3.

2.4 Betrouwbaarheidsniveau van de DigiD app

DigiD kent vier[1] zekerheidsniveaus die de mate van zekerheid bepalen over de identiteit van de gebruiker.

In Europees verband zijn er afspraken gemaakt over betrouwbaarheidsniveaus bij de digitale identificatie van burgers: de zogenaamde eIDAS-verordening onderscheidt drie niveaus. Onderstaande tabel geeft de relatie tussen de DigiD- en de eIDAS-niveaus weer, gerangschikt naar oplopende betrouwbaarheid.

DigiD	eIDAS
Basis	Laag
Midden	
Substantieel	Substantieel
Hoog	Hoog

Afhankelijk van de aard van de te raadplegen gegevens of uit te voeren transacties kan een dienstaanbieder meer zekerheid wensen over de identiteit van de persoon die een dienst wil afnemen. In deze gevallen kan (of moet) hij authenticatie op betrouwbaarheidsniveau Substantieel vereisen.

Met de DigiD app kan de gebruiker twee van de niveaus bereiken: Midden en Substantieel.

Een proces gebaseerd op Remote Document Authentication (RDA) maakt de DigiD app geschikt voor gebruik op betrouwbaarheidsniveau Substantieel: De DigiD app scant de NFC-chip van een identiteitsdocument en stelt bezit, echtheid en geldigheid vast op basis van het bij het account al bekende BSN. Na deze eenmalige ID-check is elke authenticatie met de DigiD app er een op betrouwbaarheidsniveau Substantieel. De DigiD app op Substantieel voldoet geheel aan de in de eIDAS-verordening gestelde eisen voor dit niveau.

[1] Momenteel zijn er slechts drie niveaus voorhanden: Basis, Midden en Substantieel. In de toekomst komt met 'inloggen met identiteitsbewijs' niveau Hoog beschikbaar.

3 Processen in de DigiD app

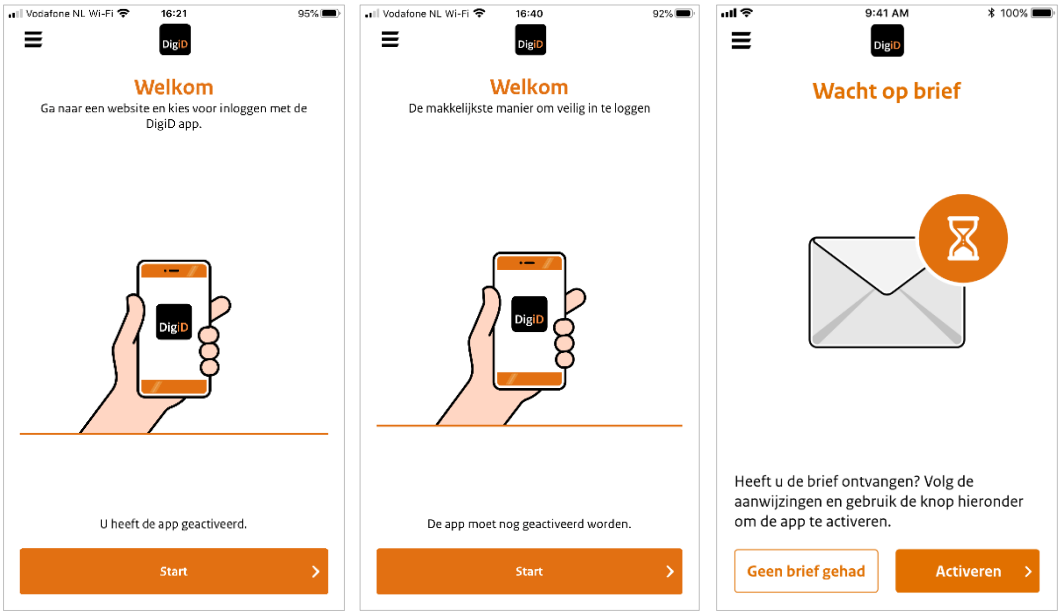
Dit hoofdstuk beschrijft de meest relevante processen die een gebruiker met de DigiD app kan doorlopen.

3.1 Openen van de app

Als de gebruiker de app opent komt hij of zij op het startscherm. Dat scherm past zich aan, afhankelijk van de activatiestatus van de app, zie figuur 1:

- Als de app geactiveerd is, en dus geschikt om mee in te loggen, geeft het startscherm een aanwijzing hoe te beginnen met inloggen [1].
- Als de gebruiker de app nog niet heeft geactiveerd, wijst de app daarop [2]. De app moet eerst geactiveerd worden, voordat die gebruikt kan worden om in te loggen.
- Als de gebruiker een activatiecode heeft aangevraagd, maar nog wacht op de brief, maakt de app daar melding van [3].

[1] [2] [3]



Figuur 1: Drie varianten van het startscherm

3.2 Authenticatie

Het belangrijkste proces is het inloggen bij een webdienst.

3.2.1 Gebruikersperspectief

De gebruiker geeft op de website van een dienstaanbieder aan dat hij of zij wil inloggen, en wordt naar het inlogscherm van DigiD geleid. Dit kan op een mobiel apparaat of op een desktop. Beide mogelijkheden worden hier omschreven, omdat ze enigszins van elkaar afwijken. Mijn DigiD dient hier als voorbeeld van een webdienst.

<u>Inloggen in een browser op een mobiel apparaat</u>

Figuur 2 toont de webpagina's die de gebruiker doorloopt tijdens het inloggen bij een webdienst in een mobiele browser.

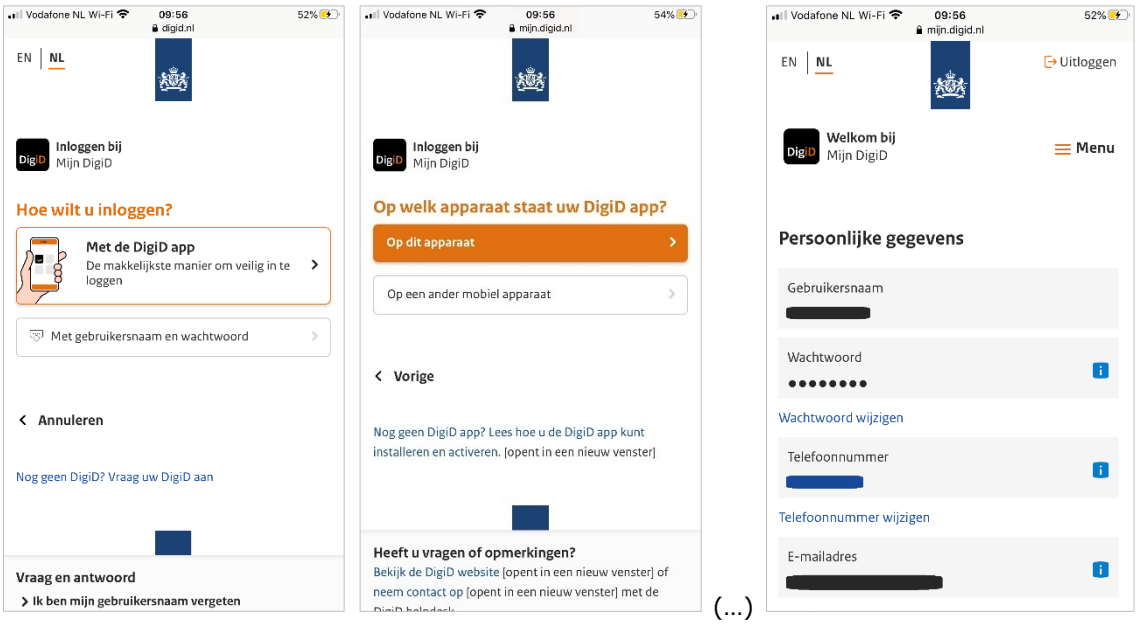
De gebruiker kiest eerst voor de inlogmethode 'Met de DigiD app' [1]. Er zijn nu twee opties. De gebruiker kiest de optie die voor de situatie van toepassing is [2]:

- De gebruiker logt in bij een webdienst via een browser die op hetzelfde apparaat staat als de DigiD app. De app wordt automatisch geopend en de gebruiker logt in zoals weergegeven in figuur 4.

- De gebruiker logt in bij een webdienst in een browser en gebruikt de DigiD app die op een ander apparaat is geactiveerd. De gebruiker moet de twee apparaten aan elkaar koppelen door het invoeren van een koppelcode en het scannen van een QR-code, net als bij inloggen op een desktop. Zie figuur 3.

Na succesvolle authenticatie komt hij terug bij de webdienst, ingelogd en wel [3].

[1] [2] [3]



(...)

Figuur 2: Inloggen bij een webdienst in een mobiele browser

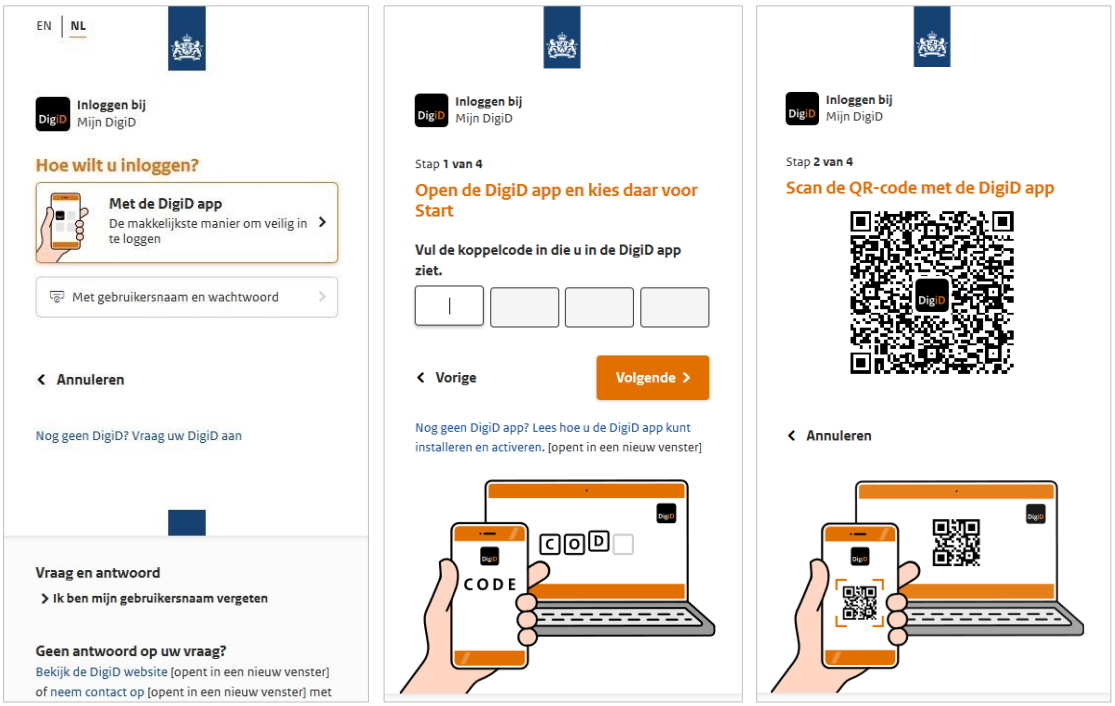
Inloggen in een browser op een desktop

Figuur 3 geeft de webpagina's weer die de gebruiker doorloopt tijdens het inloggen bij een webdienst in een browser op een desktop.

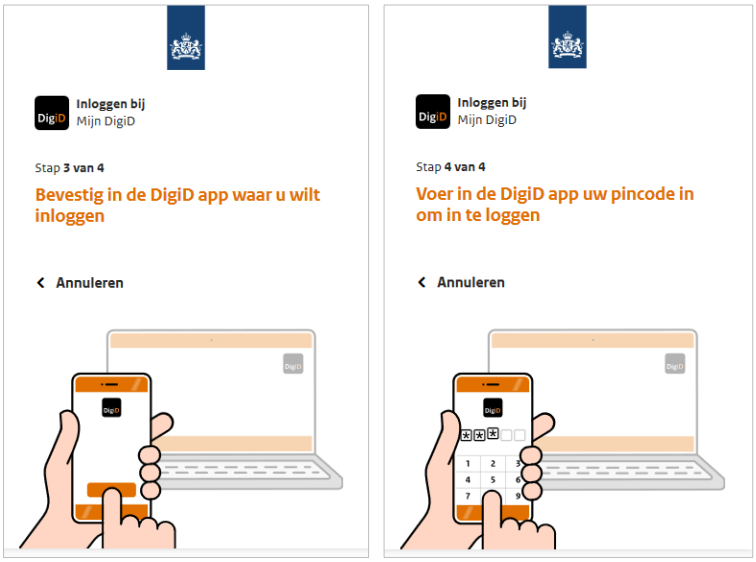
De gebruiker kiest eerst voor de inlogmethode 'Met de DigiD app' [1]. Vervolgens opent hij of zij de DigiD app en voert de koppelcode in die wordt weergegeven in de browser [2]. Die toont daarop een QR-code [3] die met de app gescand moet worden. Nu volgt het inloggen in de app (als weergegeven in figuur 5): De schermen in de browser volgen de stappen die de gebruiker in de app uitvoert: het bevestigen van het inloggen bij de webdienst [4] en het invoeren van de pincode [5].

Na succesvolle authenticatie komt de gebruiker ingelogd terug bij de webdienst [6].

[1] [2] [3]



[4] [5]



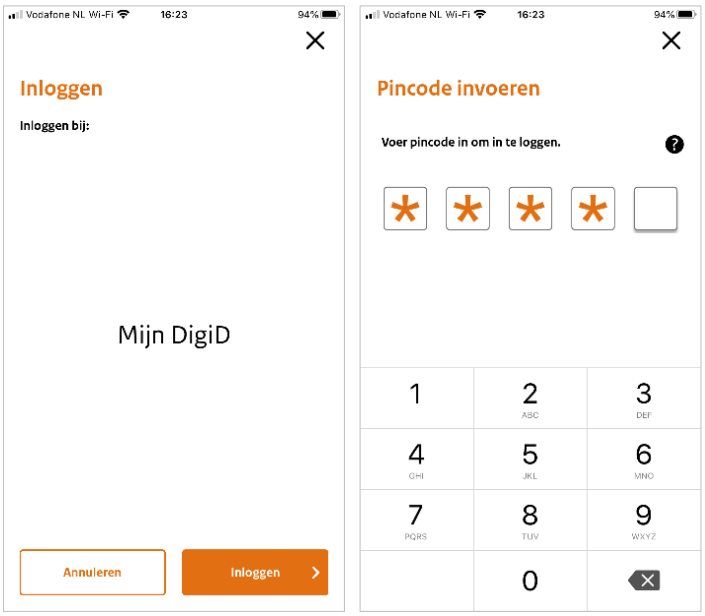
[6]

Figuur 3: Inloggen bij een webdienst op een desktop

Inlogstappen in de DigiD app

Als de app op hetzelfde apparaat staat, wordt de app vanzelf geopend. Figuur 4 toont de stappen die gebruiker in dat geval moet doorlopen. Wanneer de DigiD app niet op het toestel staat toont DigiD een webpagina met een link naar de app store om de DigiD app te downloaden.

[1] [2]



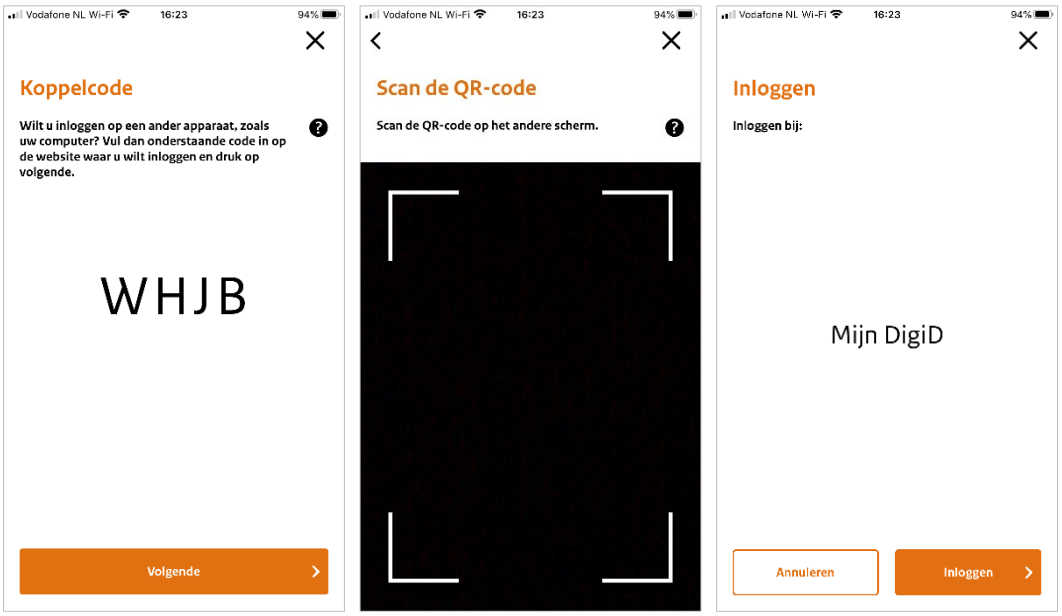
Figuur 4: Inloggen met de DigiD app op hetzelfde apparaat

De app toont de webdienst waar de gebruiker wil inloggen [1]. Als die het inloggen bevestigt, moet de pincode ingevoerd worden die tijdens het activeren van de app is ingesteld [2]. Als de pincode correct is, komt de gebruiker ingelogd terug bij de webdienst.

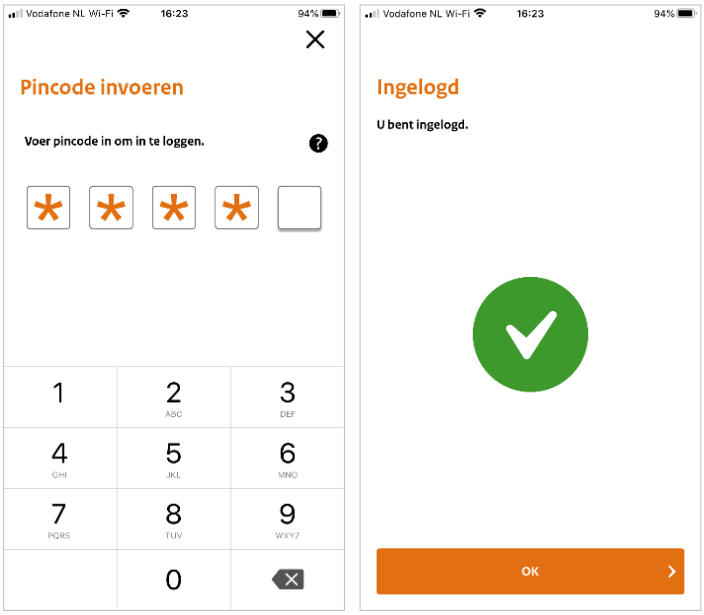
Figuur 5 toont de andere optie: als de app op een ander apparaat staat dan de website van de dienstaanbieder.

De gebruiker moet dan eerst de twee apparaten koppelen, door een koppelcode uit de app [1] in te voeren op de website en vervolgens een QR-code te scannen [2]. Vervolgens vraagt de app ook hier om bevestiging [3] en pincode [4]. Als de pincode correct is, toont de app dat het inloggen gelukt is [5]. Op de website van de dienstaanbieder (op het andere apparaat) is nu ingelogd.

[1] [2] [3]



[4] [5]



Figuur 5: Inloggen met de DigiD app op een ander apparaat

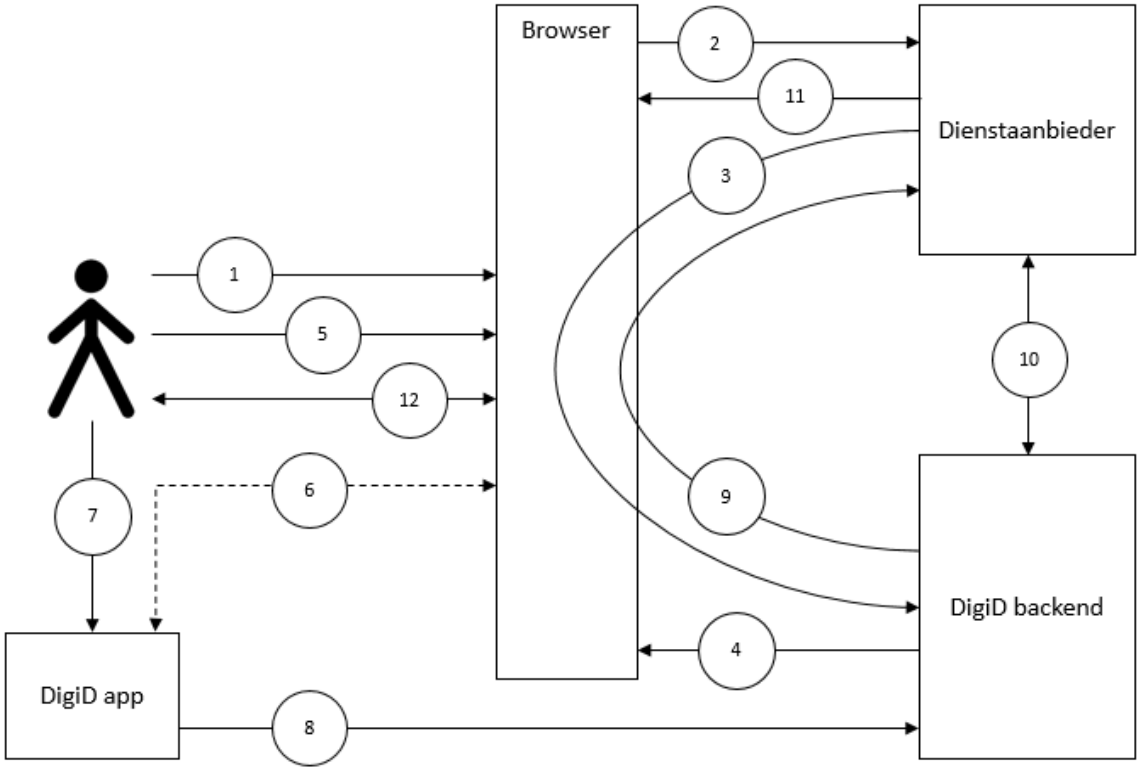
Bovenstaande scenario's beschrijven de 'happy flow': de gebruiker heeft, voorafgaand aan het inloggen, de DigiD app geactiveerd op het minimale betrouwbaarheidsniveau dat de dienstaanbieder vereist. Dat hoeft niet het geval te zijn:

- Als de app nog niet geactiveerd is, leidt hij de gebruiker eerst door de activatie.
- Slaagt die, dan is de gebruiker daarna meteen ingelogd bij de dienstaanbieder. Voor de activatie van de app, zie paragraaf 3.3.
- Als de dienstaanbieder niveau Substantieel vereist voor inzage in de gegevens, maar de gebruiker heeft de app geactiveerd op niveau 'Midden', dan moet tijdens het inloggen eerst de ID-check uitgevoerd worden om het niveau van de app op te hogen. Slaagt die, dan is de gebruiker daarna meteen ingelogd bij de dienstaanbieder. Voor het uitvoeren van de ID-check, zie paragraaf 3.4.

Behalve op een website kan de gebruiker ook met de DigiD app inloggen in een app van een dienstaanbieder. Meer informatie over dit proces staat in een apart document: functionele beschrijving DigiD: Inloggen met app2app.

3.2.2 Procesflow

Inloggen met de DigiD app op een webdienst van een dienstaanbieder is een samenspel tussen de dienstaanbieder, de browser, de DigiD app en de DigiD backend.



Figuur 6: Authenticatieflow DigiD app

Figuur 6 geeft weer hoe een authenticatie met de DigiD app verloopt:

1. De gebruiker opent de website van een dienstaanbieder in een browser.
2. De gebruiker vraagt toegang tot persoonlijke informatie op die website.
3. De dienstaanbieder wil de identiteit van de eindgebruiker vaststellen en stuurt de gebruiker door naar DigiD. Daarbij wordt het vereiste betrouwbaarheidsniveau meegegeven.
4. De DigiD backend start het inlogproces in de browser.
5. De gebruiker kiest voor inloggen met de DigiD app.
6. De DigiD app wordt aan de inlogsessie gelinkt. Dit kan op twee manieren:
    a. Als de app op een ander apparaat staat dan de browser waarin de gebruiker wil inloggen bij de webdienst:
        - De gebruiker voert in de browser de koppelcode in die de DigiD app hem toont.
        - De DigiD backend genereert een QR-code met de sessiegegevens, en verwerkt daarin ook de koppelcode.
        - De gebruiker scant de QR-code met de DigiD app. Als de app de koppelcode uit de QR-code herkent, wordt de sessie geaccepteerd.
    b. Als de app op hetzelfde apparaat staat als de browser waarin de gebruiker wil inloggen bij de webdienst: DigiD opent de DigiD app middels een URL.
7. De gebruiker bevestigt in de DigiD app dat hij of zij wil inloggen bij de betreffende webdienst en voert de pincode in.
8. De DigiD app vraagt de DigiD backend de gebruiker met de pincode te authentiseren.
9. Als de authenticatie slaagt, leidt DigiD de gebruiker terug naar de website van de dienstaanbieder.

10. De dienstaanbieder haalt bij DigiD het authenticatieresultaat op, waarin het BSN van de gebruiker verwerkt is (alleen als de authenticatie geslaagd is).
11. De dienstaanbieder geeft de gebruiker toegang tot de gegevens op de website.
12. De gebruiker handelt de zaken met de dienstaanbieder af.

Zie voor een gedetailleerdere, technische beschrijving de koppelvlakspecificatie SAML-DigiD.

3.3 Activatie

Voordat een gebruiker met de DigiD app kan inloggen moet de app eerst geactiveerd worden.

3.3.1 Gebruikersperspectief

Tijdens de activatie van de app moet de gebruiker aantonen wie hij of zij is door zich te identificeren met een geldig identiteitsbewijs (een paspoort, rijbewijs of identiteitskaart), oftewel door de ID-check uit te voeren.

Het activatieproces begint met het invoeren van gebruikersnaam en wachtwoord. Voert de gebruiker die correct in, dan vraagt de app een 5-cijferige pincode te kiezen. Daarna moet de gebruiker ter controle de chip op het identiteitsbewijs scannen met de NFC-lezer van het toestel. Na afloop is de DigiD app actief op betrouwbaarheidsniveau **Substantieel**.

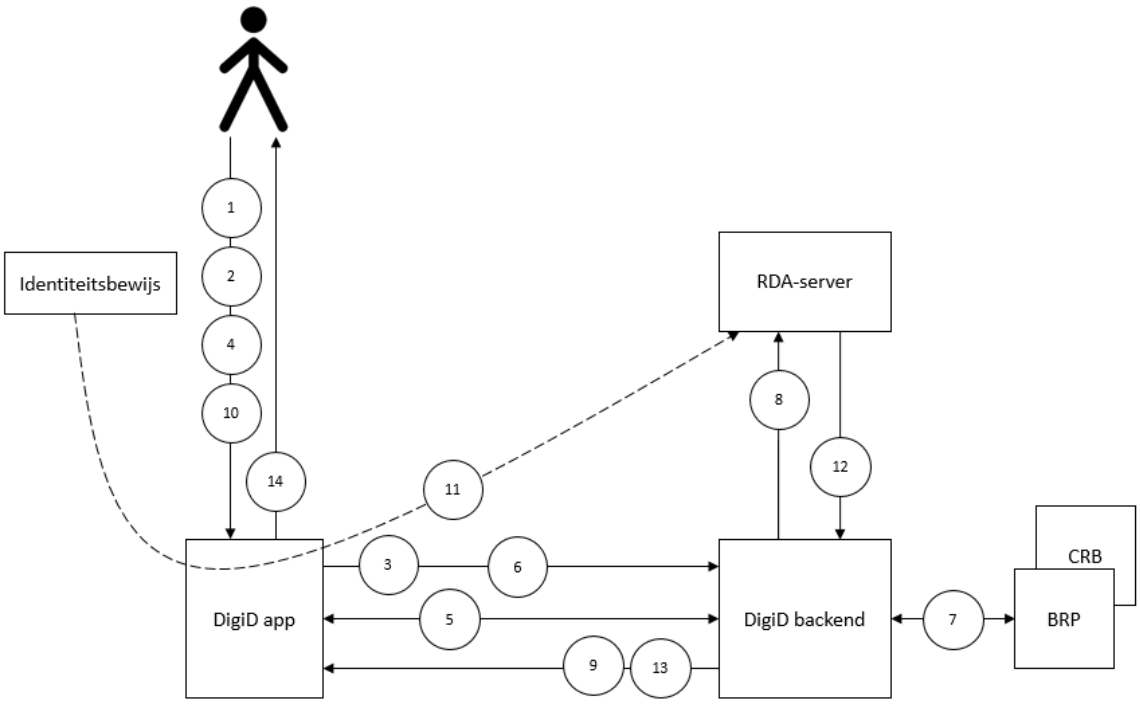
Als blijkt dat de gebruiker niet in staat is de ID-check uit te voeren, omdat het toestel niet is uitgerust met een geschikte NFC-lezer, omdat hij of zijn geen geldig identiteitsbewijs heeft, of omdat het scannen niet lukt, wordt er een alternatieve activatiemethode aangeboden:

- Met een sms-controle: Als de gebruiker een telefoonnummer in zijn of haar account heeft geregistreerd, kan de app geactiveerd worden door een sms-controle uit te voeren. De app heeft na activatie betrouwbaarheidsniveau **Midden**.
- Met een activatiecode in een brief: Als er geen telefoonnummer bij het account geregistreerd is, dan kan de gebruiker een activatiecode aanvragen. Die komt per brief, dus de activatie kan pas na enkele dagen afgerond worden, op niveau **Midden**.

Voor gebruikers die al een geactiveerde app hebben op een ander apparaat is er overigens nog een methode: zij kunnen een nieuwe app activeren door een authenticatie uit te voeren met de andere app (het invoeren van gebruikersnaam en wachtwoord is dan niet nodig). De nieuwe app heeft na activatie betrouwbaarheidsniveau **Midden**.

3.3.2 Procesflow

De app activeren gebeurt bij voorkeur met de ID-check, omdat de app dan meteen op niveau Substantieel geactiveerd wordt.



Figuur 7: Activatieflow met ID-check

Figuur 7 toont de stappen in geval van een activatie met ID-check:

1. De gebruiker opent de nog niet geactiveerde DigiD app en start de activatie.
2. De gebruiker voert zijn of haar gebruikersnaam en wachtwoord in.
3. De DigiD app vraagt de DigiD backend de gebruiker te authentiseren.
4. Als de authenticatie slaagt, kiest de gebruiker een pincode.
5. De app maskeert die pincode, om hem onherkenbaar te maken (#pincode).
6. De DigiD app wisselt cryptografische gegevens uit met DigiD backend en versleutelt daarmee de #pincode.
7. De DigiD app stuurt de versleutelde #pincode naar de DigiD backend. Die ontsleutelt de #pincode, maakt de app tijdelijk aan bij het account van de gebruiker, en slaat daarbij de #pincode op.
8. De DigiD backend haalt op basis van zijn BSN de documentgegevens van de gebruiker op bij de registers BRP en CRB.
9. De DigiD backend start met die documentgegevens een sessie bij de RDA-server[2].
10. De DigiD backend stuurt die sessiegegevens door naar de DigiD app.
11. De gebruiker scant zijn of haar identiteitsbewijs met de NFC-lezer in het toestel.
12. De DigiD app zet een tunnel op tussen identiteitsbewijs en RDA-server, via welke de uitgelezen documentgegevens worden verstuurd, die de RDA-server controleert.
13. Als de ID-controle geslaagd is, laat de RDA-server dat weten aan de DigiD backend.
14. De DigiD backend activeert de DigiD app op niveau Substantieel en meldt dat aan de DigiD app.
15. De DigiD app meldt de succesvolle activatie aan de gebruiker.

[2] *De RDA-server is een aparte component binnen het DigiD-landschap voor het uitvoeren van de Remote Document Authentication, oftewel de ID-check. Op basis van documentgegevens die met het BSN bij de BRP en het CRB zijn opgehaald, kan deze server de sleutels genereren waarmee de DigiD app de chip op het identiteitsbewijs kan uitlezen.*

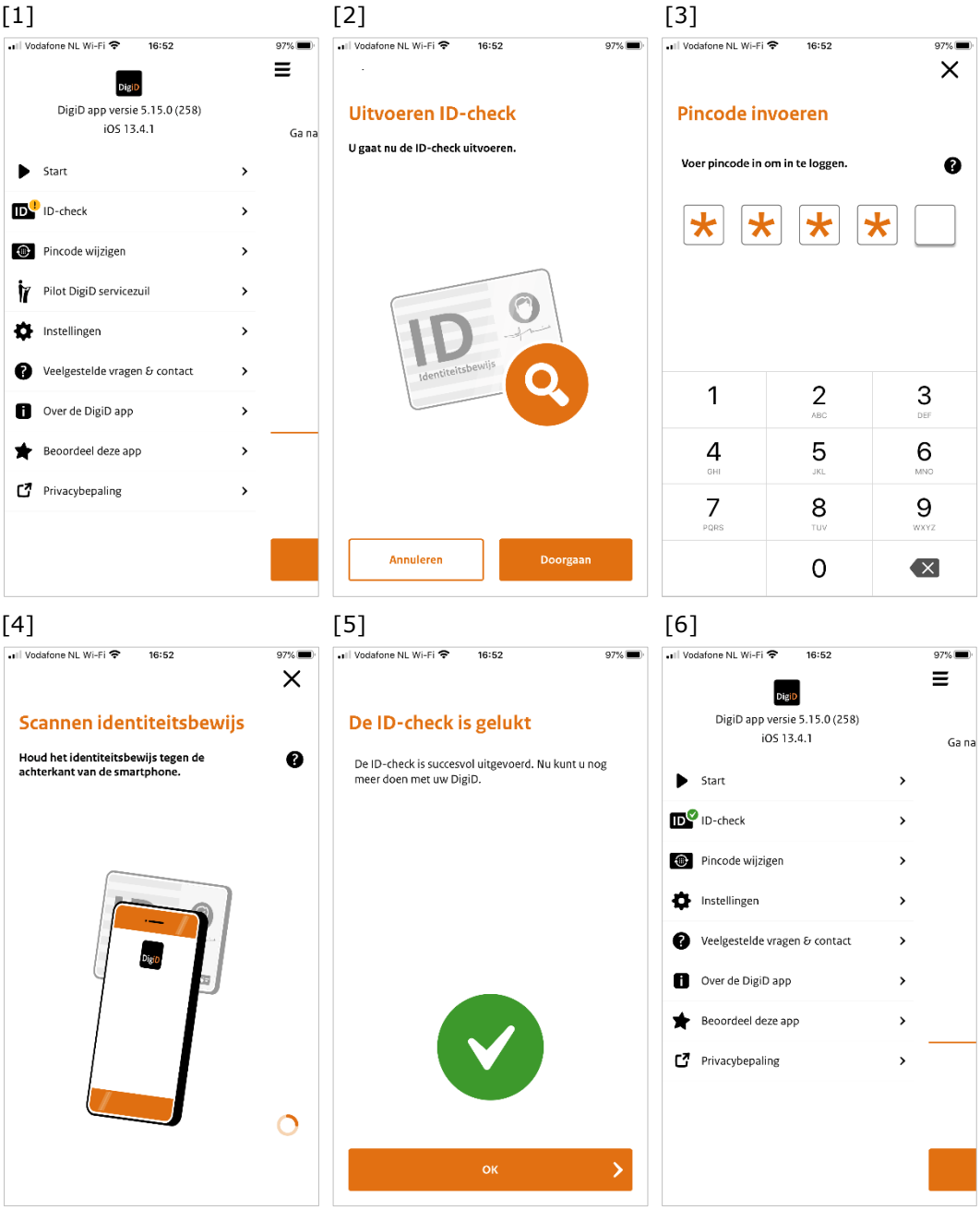
3.4 ID-check

3.4.1 Gebruikersperspectief

Steeds meer dienstaanbieders zullen niveau Substantieel vereisen bij het inloggen (bijvoorbeeld om meer privacygevoelige gegevens te raadplegen, zoals een patiëntendossier). Als de gebruiker de activatie van de DigiD app niet met ID-check heeft gedaan, staat het betrouwbaarheidsniveau van de DigiD app op Midden. Tijdens het inloggen bij zo'n dienst, zal de ID-check alsnog toegevoegd moeten worden aan de DigiD app. Dat kan op twee manieren: in de DigiD app zelf, of met behulp van een aparte app, de CheckID app.

ID-check uitvoeren in de DigiD app zelf

Beschikt het toestel waarop de gebruiker de DigiD app heeft geactiveerd een geschikte NFC-lezer, dan kan de ID-check uitgevoerd worden in de app zelf, zoals getoond in figuur 8.



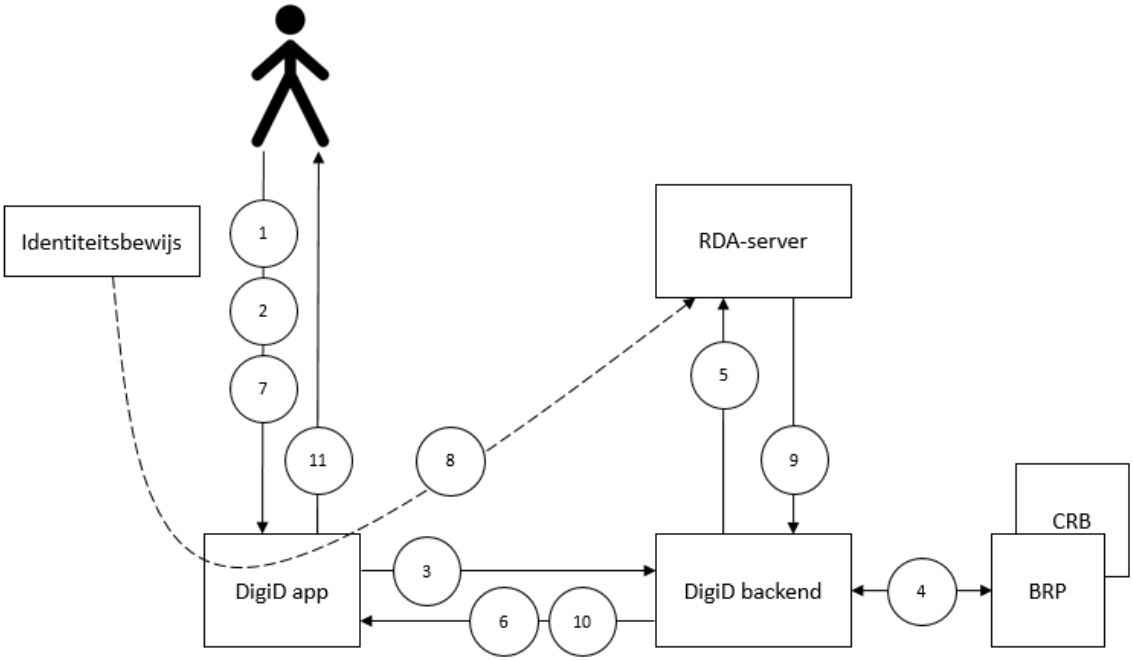
Figuur 8: Uitvoeren van de ID-check in de DigiD app

De gebruiker start vanuit het startscherm het menu [1] met daarin de optie *ID-check*. Het gele uitroepteken duidt erop dat de ID-check nog niet is uitgevoerd. De gebruiker kiest de optie *ID-check* en bevestigt de keuze [2]. De gebruiker authentiseert zichzelf met een pincode [3] en als dat gelukt is, vraagt de app een identiteitsbewijs tegen het toestel te houden [4]. De gebruiker mag zelf kiezen met welk ID hij dat doet: paspoort, identiteitskaart of rijbewijs. Het type document wordt vanzelf gedetecteerd door de app. Er vindt nu op de achtergrond een controle plaats op de echtheid en geldigheid van het gescande ID, en of het wel toebehoort aan de gebruiker van de app. Als de ID-check geslaagd is, meldt de app dat aan de gebruiker [5]. In het menu geeft een groen vinkje bij de optie ID-check nu aan dat de DigiD app versterkt is met de ID-check [6].

ID-check uitvoeren met de CheckID app

Voor een gebruiker die niet beschikt over een bruikbare NFC-lezer in het apparaat waarop de DigiD app staat is er een alternatief. De gebruiker kan de CheckID app downloaden op een toestel dat wel geschikt is; dat mag ook op een toestel van een andere persoon zijn. De CheckID app fungeert als NFC-lezer tijdens de ID-check. Dus de gebruiker logt in met de pincode in de DigiD app die op toestel A geactiveerd is en voert vervolgens de ID-check met de CheckID app uit op toestel B. Daarna is de DigiD app op toestel A verhoogd naar niveau Substantieel.

3.4.2 Procesflow



Figuur 9: Flow voor het uitvoeren van de ID-check

Figuur 9 toont de flow van de ID-check vanuit de DigiD app zelf:

1. De gebruiker opent het menu in de geactiveerde DigiD app en start de ID-check.
2. De gebruiker voert de pincode in.
3. De DigiD app vraagt de DigiD backend de gebruiker met de pincode te authentiseren.
4. Als de authenticatie slaagt, haalt de DigiD backend op basis van zijn BSN de documentgegevens van de gebruiker op bij de registers BRP en CRB.
5. De DigiD backend start met die documentgegevens een sessie bij de RDA-server.
6. De DigiD backend stuurt die sessiegegevens door naar de DigiD app.
7. De gebruiker scant zijn identiteitsbewijs met de NFC-lezer in zijn toestel.
8. De DigiD app zet een tunnel op tussen identiteitsbewijs en RDA-server, via welke de uitgelezen documentgegevens worden verstuurd, die de RDA-server controleert.

9. Als de ID-controle geslaagd is, laat de RDA-server dat weten aan de DigiD backend.
10. De DigiD backend hoogt het betrouwbaarheidsniveau van de DigiD app op naar Substantieel en meldt dat aan de DigiD app.
11. De DigiD app meldt aan de gebruiker dat de ID-check gelukt is.

3.5 Overige processen

Naast de drie hoofdprocessen zoals beschreven in de vorige paragrafen, kent de app nog enkele functies.

3.5.1 Activeren account na aanvraag via website

Nadat een nieuwe DigiD-gebruiker een account heeft aangevraagd via de DigiD-website, moet hij of zij wachten op een brief met activatiecode. Met die code kan het DigiD account via de website geactiveerd worden, maar dit kan ook in de DigiD app:

De gebruiker voert de gebruikersnaam en wachtwoord in die tijdens de aanvraag is opgegeven en voert eventueel de sms-controle uit (als tijdens de accountaanvraag geen telefoonnummer is opgegeven), voert de activatiecode uit de brief in en kiest tot slot een pincode. Slaagt de activatie op deze manier, dan heeft de gebruiker naast het inlogmiddel gebruikersnaam en wachtwoord (eventueel aangevuld met sms-controle), ook een DigiD app als inlogmiddel geactiveerd bij zijn of haar DigiD account.

3.5.2 Bevestigen wijzigingen in Mijn DigiD

Behalve voor inloggen bij een webdienst kan een authenticatie met de DigiD app ook dienen om een wijziging in Mijn DigiD te bevestigen. Als de gebruiker bij Mijn DigiD inlogt met de DigiD app om een wijziging door te voeren in zijn of haar account, bijv. om een e-mailadres aan te passen, dan moet de wijziging bevestigd worden door nogmaals in te loggen met de DigiD app.

3.5.3 Beheer via het menu

In het menu van de DigiD app kan de gebruiker enkele instellingen wijzigen, zie voor meer informatie paragraaf 4.1.

4 Beheer en rapportage

Een gebruiker kan zijn DigiD beheren in Mijn DigiD. Hij of zij kan bijvoorbeeld de historie van authenticaties inzien, middelen aanvragen, activeren of herroepen, en notificatiekanalen toevoegen. Voor meer informatie, zie de *Functionele beschrijving DigiD*.

4.1 Beheerfuncties in de DigiD app

De DigiD app heeft ook enkele eigen beheerfuncties, bijvoorbeeld het deactiveren van de app. Overigens heeft het verwijderen van de DigiD app van het apparaat hetzelfde effect als deactiveren.

Ook kan een gebruiker de pincode wijzigen, mits de huidige pincode bekend is. Als dit niet het geval is, zal de app opnieuw geactiveerd moeten worden.

Na driemaal foutief invoeren van de pincode wordt de DigiD app gedeactiveerd. De gebruiker moet dan de app opnieuw activeren om er weer mee in te kunnen loggen.

Via het menu in de app kan de gebruiker ook enkele instellingen wijzigen:

- De taal in de app instellen op Engels of Nederlands (Na downloaden staat de taal op Nederlands; als de gebruiker kiest voor Engels blijft die instelling voortaan behouden).
- Switchen tussen lichte en donkere modus.

4.2 DigiD app in Mijn DigiD

De gebruiker kan op maximaal 5 apparaten de DigiD app activeren (elke app heeft een eigen pincode). In Mijn DigiD kunnen de gegevens van alle geactiveerde DigiD apps ingezien worden, zie figuur 10. Aan iedere DigiD app dient apart een ID-check toegevoegd te worden.

De gebruiker kan de DigiD app in de app zelf, maar ook in Mijn DigiD deactiveren.

Figuur 10: Overzicht van geactiveerde app in Mijn DigiD

4.3 Rapportage over authenticaties

Logius levert maandelijks rapportages op die inzicht geven in het aantal authenticaties bij een dienstaanbieder. De authenticaties met de DigiD app zijn daarin opgenomen.

5 Storingen

Dit hoofdstuk beschrijft de mogelijke storingen/incidenten die het gebruik van de DigiD app kunnen belemmeren.

5.1 Deelfunctionaliteiten uitgeschakeld

In geval van calamiteiten/veiligheidsincidenten kan Logius op de DigiD backend deelfunctionaliteiten uitschakelen. Hier worden alleen de gevallen genoemd die van invloed zijn op de werking van de DigiD app.

5.1.1 Koppeling met DigiD app uitgeschakeld

Het gebruik van de DigiD app kan in zijn geheel worden uitgeschakeld. In dat geval kan geen enkele gebruiker nog met de DigiD app inloggen bij een dienstaanbieder; er zal een ander inlogmiddel gebruikt moeten worden. Het activeren van een app of het uitvoeren van een ID-check is op dat moment ook niet mogelijk.

5.1.2 Koppeling met RDA-server uitgeschakeld

De koppeling met de RDA-server kan worden uitgezet. Het uitvoeren van de ID-check is dan niet mogelijk, inloggen met de app nog wel.

5.1.3 Koppeling met CheckID app

Het gebruik van de CheckID app kan worden uitgezet. Gebruikers kunnen de ID-check dan niet aan de DigiD app toevoegen met behulp van de CheckID app. Op andere manieren kan dat nog wel.

5.2 Storing bij externe afhankelijkheden

5.2.1 BRP

Als er een storing is bij de BRP zijn de volgende processen in de DigiD app niet beschikbaar:

- Het uitvoeren van de ID-check;
- Het aanvragen van een activeringscode per brief.

5.2.2 CRB

Als er een storing is bij de CRB is het uitvoeren van de ID-check niet mogelijk.

5.2.3 Sms-dienst

Bij een storing van de sms-dienst is het activeren van de app met sms-controle niet mogelijk.

5.3 Technische storing

Er kan een technische storing optreden in de koppeling tussen DigiD en de dienstaanbieder, of intern bij DigiD, waardoor inloggen in het geheel niet mogelijk is, dus ook niet met de app.

6 Woordenlijst

Woord/afkorting	Betekenis
Afnemer	De organisatie die is aangesloten op DigiD, zodat gebruikers daarmee kunnen inloggen in hun webdienst.
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.
BRP	*Basisregistratie Personen*; Register beheerd door de RvIG dat persoonsgegevens bevat van inwoners van Nederland (ingezetenen) en van personen die Nederland hebben verlaten (niet ingezetenen).
CRB	*Centraal Rijbewijzen- en Bromfietscertificatenregister*; Register beheerd door de RDW met daarin gegevens over rijbewijs, rijvaardigheid en rijgeschiktheid van burgers.
Dienstaanbieder	De aanbieder van de webdienst waarbij een gebruiker inlogt met DigiD. Voorbeelden van dienstaanbieders zijn de Belastingdienst, de gemeente Amsterdam en Achmea. Ook wel: *Afnemer*.
DigiD	Authenticatiedienst die authenticatieverzoeken van burgers afhandelt voor aangesloten dienstverleners.
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.
eIDAS	*Electronic Identities And Trust Services*; Europese verordening waarin de lidstaten afspraken hebben gemaakt om bij de digitale identificatie van burgers dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen.
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.
Logius	De beheerorganisatie van DigiD.
RDA	*Remote Document Authentication*, zie RDA-server.
RDA-server	Een aparte component binnen het DigiD-landschap voor het uitvoeren van de Remote Document Authentication, oftewel de ID-check. Op basis van documentgegevens die met het BSN bij de BRP en het CRB zijn opgehaald, kan deze server de sleutels genereren waarmee de DigiD app de chip op het identiteitsbewijs kan uitlezen.

Woord/afkorting	Betekenis
RvIG	*Rijksdienst voor Identiteitsgegevens*; organisatie die onder meer de BRP beheert.
SAML	*Security Assertion Markup Language*; Standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen.
Webdienst	Dienst van een (semi-)publiekrechtelijke of privaatrechtelijke instelling met een publieke taak, die via het internet ontsloten wordt.