

OSAGE

DigiD & het nieuwe stelsel eindverslag

8 december 2020

Inhoud

Samenvatting

1 Onderzoeksvraag

2 Testopzet

3 Onderzoekspopulatie

4 Samenvatting resultaten

5 Enkele citaten

6 Conclusies

7 Aanbevelingen

Bijlage 1 Alle onderzoeksresultaten

Bijlage 2 Weergave heatmaps

Samenvatting

- Digid wordt ervaren als vertrouwd, betrouwbaar en veilig. Onder ruim 200 respondenten is onderzocht hoe deze kracht van het merk kan worden benut binnen een omgeving met private inlogmiddelen.
- Uit het onderzoek blijkt: door private inlogmiddelen als een net zo veilig en betrouwbaar alternatief te presenteren naast DigiD worden deze nieuwe private inlogmiddelen ook als veilig en betrouwbaar ervaren.
- Belangrijkste aanbeveling is daarom: gebruik de kracht van het merk DigiD door toegelaten private inlogmiddelen als een veilig en betrouwbaar alternatief te presenteren naast DigiD. Deze manier van presenteren is op dit moment voor de eindgebruiker het eenvoudigst en duidelijkst: in één oogopslag een rij met middelen waar je uit kunt kiezen.

1 Onderzoeksvraag

*“Ik laat onderzoeken **hoe ik de kracht van het “merk” DigiD kan blijven benutten.** Het “merk” DigiD wordt immers door vrijwel alle burgers van de doelgroep een of meerdere malen per jaar gebruikt en wordt door hen ervaren als herkenbaar en vertrouwd. Zo wil ik bezien hoe gewerkt kan worden met private inlogmethoden binnen een omgeving met DigiD.”*

(uit de BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN
EN KONINKRIJKSRELATIES aan de Tweede Kamer, st-26643-636, 23 september 2019)

2 Testopzet (1)

Digid wordt ervaren als vertrouwd, betrouwbaar en veilig. Om te onderzoeken hoe deze kracht van het merk kan worden benut zijn twee informatiepagina's over “*Het nieuwe inloggen*” ontwikkeld. Op de ene pagina is DigiD niet alleen een inlogmiddel maar ook de afzender van de informatie. Op de andere pagina is de Rijksoverheid de afzender en DigiD alleen een inlogmiddel náást andere, private inlogmiddelen. De afzender en de vormgeving verschillen, de content is grotendeels gelijk.

De testopzet was als volgt:

- A/B test met de twee informatiepagina's, online uitgezet bij 2 x 100 respondenten.
- De test bevatte zowel kwantitatieve (KPI's en waardescores) als kwalitatieve (open vragen, heatmap*) onderdelen.


**Een heatmap geeft met warmtebeelden weer welke handelingen bezoekers op een webpagina uitvoeren. Op deze manier krijg je een goed beeld van waar bezoekers op klikken, tot hoever ze scrollen en hoe ze zich door een webpagina bewegen. Zie bijlage 2 voor de heatmaps horend bij dit onderzoek*

2 Testopzet (2)

- Te toetsen met behulp van deze A/B-test: hoe betrouwbaar worden de nieuwe, private inlogmiddelen ervaren als DigiD de afzender is van de informatie over het nieuwe inloggen én als inlogmiddel naast andere, private inlogmiddelen staat? Dit gebruik van de merknaam DigiD wordt vergeleken met de ervaren betrouwbaarheid als de Rijksoverheid de afzender is van de afzender en DigiD alleen een inlogmiddel naast andere, private inlogmiddelen.

2 Testopzet (3) de twee varianten afzender Rijksoverheid of DigiD

Home > Het nieuwe inloggen



Het nieuwe inloggen: veilig, makkelijk en betrouwbaar


Veilig inloggen bij de overheid, het onderwijs en de zorg verandert. Voortaan kunt u niet alleen inloggen met DigiD. Er zijn nu ook andere inlogmiddelen die net zo veilig zijn. U kunt zelf kiezen welk inlogmiddel bij u past.

Uw gegevens goed beschermd


U regelt steeds meer via internet. Ook met de overheid, het onderwijs, de zorg of pensioenfondsen. Vaak gaat het om hele persoonlijke gegevens. Daarom zorgt de overheid voor veilige inlogmiddelen. Als u daarmee inlogt weet een organisatie zeker dat u het bent. Zo zijn uw gegevens goed beschermd.

Veilig, makkelijk en betrouwbaar


De overheid stelt strikte eisen op het gebied van veiligheid, betrouwbaarheid, privacy en gebruiksgemak. Deze inlogmiddelen voldoen aan die strikte eisen:




DigiD App
De vertrouwde manier van inloggen
[Meer informatie](#)




iDin via je bank
Gemakkelijk inloggen via je eigen bank
[Meer informatie](#)




Its Me App
Je digitale ID op je gsm
[Meer informatie](#)




IRMA App
je digitaal paspoort op je mobiel
[Meer informatie](#)



Veilig
De inlogmiddelen die voldoen aan de eisen van de overheid maken het crimineel moeilijker misbruik te maken van valse of gestolen identiteitsgegevens.
[Meer over veiligheid](#)




Makkelijk
Er zijn vier verschillende inlogmiddelen. U kiest zelf wat bij u past.
[Bekijk de inlogmiddelen](#)



Betrouwbaar
De inlogmiddelen die voldoen aan de eisen van de overheid hebben zich bewezen. Bovendien worden ze steeds verder ontwikkeld. Zo kunt u erop vertrouwen dat ze ook in de toekomst blijven werken.
[Meer over betrouwbaarheid](#)

Home > Het nieuwe inloggen



DigiD het nieuwe inloggen


Veilig inloggen bij de overheid, het onderwijs en de zorg verandert. Voortaan kunt u niet alleen inloggen met DigiD. Er zijn nu ook andere inlogmiddelen die net zo veilig zijn. U kunt zelf kiezen welk inlogmiddel bij u past.

Uw gegevens goed beschermd


U regelt steeds meer via internet. Ook met de overheid, het onderwijs, de zorg of pensioenfondsen. Vaak gaat het om hele persoonlijke gegevens. Daarom zorgt DigiD voor veilige inlogmiddelen. Als u daarmee inlogt weet een organisatie zeker dat u het bent. Zo zijn uw gegevens goed beschermd.

Veilig, makkelijk en betrouwbaar


DigiD stelt strikte eisen op het gebied van veiligheid, betrouwbaarheid, privacy en gebruiksgemak. Deze inlogmiddelen voldoen aan die strikte eisen:




DigiD App
De vertrouwde manier van inloggen
[Meer informatie](#)




iDin via je bank
Gemakkelijk inloggen via je eigen bank
[Meer informatie](#)




Its Me App
Je digitale ID op je gsm
[Meer informatie](#)




IRMA App
je digitaal paspoort op je mobiel
[Meer informatie](#)



Veilig
De inlogmiddelen die voldoen aan de eisen van DigiD maken het crimineel moeilijker misbruik te maken van valse of gestolen identiteitsgegevens.
[Meer over veiligheid](#)



Makkelijk
Er zijn vier verschillende inlogmiddelen. U kiest zelf wat bij u past.
[Bekijk de inlogmiddelen](#)



Betrouwbaar
De inlogmiddelen die voldoen aan de eisen van DigiD hebben zich bewezen. Bovendien worden ze steeds verder ontwikkeld. Zo kunt u erop vertrouwen dat ze ook in de toekomst blijven werken.
[Meer over betrouwbaarheid](#)

3 Onderzoekspopulatie

- 116 respondenten beoordeelden de pagina met de Rijksoverheid als afzender, 102 deden dat bij DigiD als afzender.
- Leeftijdsopbouw was bij beide pagina's gelijk (redelijk gelijkmatig verdeeld tussen 18 en 64 met een uitschieter tussen de 40 en de 50). Dat komt overeen met de bevolkingsopbouw in Nederland (<https://www.cbs.nl/nl-nl/visualisaties/bevolkingspiramide>)
- Bij beide pagina's heeft de grootste groep (boven de 25%) middelbaar beroepsonderwijs als hoogste opleiding. Bij de Rijksoverheid-pagina ligt het opleidingsniveau gemiddeld iets hoger dan bij de DigiD-pagina. Ook dat komt grofweg overeen met de statistieken van het cbs (<https://longreads.cbs.nl/trends18/maatschappij/cijfers/onderwijs/>).
- Het overgrote deel van de respondenten logt wel eens in met DigiD bij een website van de overheid (rond de 90%). Een klein deel regelt alles op papier (rond de 5%) of laat iemand anders de zaken regelen (rond de 5%).
- Ca 40% gebruikt bij het inloggen de DigiD-app, de rest met gebruikersnaam en wachtwoord of gebruikersnaam, wachtwoord en sms-controle.

4 Samenvatting resultaten (1)*

Ervaren betrouwbaarheid

- **Beide pagina's komen grotendeels betrouwbaar over.** Ze scoren allebei gemiddeld een 7.7 .
- **DigiD wordt ervaren als betrouwbaar en veilig inlogmiddel.** Daarmee worden resultaten uit eerdere onderzoeken bevestigd.
- **DigiD naast de andere inlogmiddelen presenteren draagt bij aan het vertrouwen** in die andere inlogmiddelen. Ruim 50% is het eens of helemaal eens met de stelling '*dat DigiD naast de andere inlogmiddelen staat vergroot mijn vertrouwen in die inlogmiddelen*', ca 13% is het oneens. De rest is neutraal. Tussen beide pagina's zijn kleine verschillen: de DigiD-pagina heeft iets vaker 'mee eens' én iets vaker 'mee oneens'.
- **Een ruime meerderheid geeft aan dat ze alle middelen veilig achten.** Meer dan 65% is het (helemaal) eens met de stelling '*ik ga ervan uit dat alle inlogmiddelen die op de webpagina staan even veilig en betrouwbaar zijn*'. Het percentage instemmers met de stelling ligt iets hoger als de Rijksoverheid de afzender is.

*Voor alle resultaten van het onderzoek: zie de bijlagen

4 Samenvatting resultaten (2)

- Voor enkelen doet de boodschap dat er meer inlogmiddelen komen **afbreuk aan de betrouwbaarheid**. Dit ligt deels in lijn met de onbekendheid van sommige middelen. Hoe betrouwbaar zijn deze nieuwe, onbekende inlogmethodes? De onduidelijkheid over de meerwaarde geldt vooral voor de pagina met DigiD als afzender.

Ervaren duidelijkheid en leesbaarheid

- **Beide pagina's scoren goed op de twee KPI's: duidelijkheid en leesbaarheid.** De Rijksoverheid-pagina scoort iets hoger dan de DigiD-pagina. Op leesbaarheid scoort de pagina van de Rijksoverheid zelfs significant hoger dan de benchmark. (*De benchmark betreft webpagina's van de overheid die zijn getest bij Blauw.*)
- Op de open vraag *'Vertel ons wat u duidelijk of onduidelijk vindt, en hoe het beter kan'* wijzen de respondenten op beide pagina's ruim meer onderdelen aan als 'duidelijk' dan als 'onduidelijk'. Op de pagina waar DigiD afzender én inlogmiddel is werd bij deze open vraag een paar keer aangegeven **dat deze combinatie verwarrend is** (*'Verwarrend dat er staat DigId het nieuwe inloggen en vervolgens wordt gesproken over andere manieren dan DigId'*).

4 Samenvatting resultaten (3)

- Vooral voor de pagina van de Rijksoverheid is het **duidelijk wie de afzender** van de pagina is. Bij de DigiD pagina worden zowel DigiD als de Rijksoverheid als afzender genoemd.
- De boodschappen in de tekst komen duidelijk over. Voor de meesten zijn de private middelen nieuw en er daarom hebben sommigen **behoefte aan meer uitleg over de verschillende inlogmiddelen**.
- Bij Rijksoverheid als afzender begrijpen iets meer mensen dat er nieuwe inlogmiddelen komen. Ondanks de duidelijkheid van de pagina's, overwegen maar weinigen een andere inlogmethode te gebruiken. **Dit komt omdat men zich afvraagt waarom meerdere inlogmethodes nodig zijn**.
- Op de heatmap is te zien dat **als Digid de afzender is de aandacht meer naar DigiD gaat dan naar de andere inlogmiddelen**. Als de Rijksoverheid de afzender is, is de aandacht meer verdeeld. (Zie bijlage 2 voor de heatmap.)

5 Enkele citaten informatiepagina Rijksoverheid afzender

- *Positief en vertrouwd.*
- *Duidelijk tekst. Vraag me alleen af wat er mis is met DigiD. Ben benieuwd wat er nog meer voor mogelijkheden zijn.*
- *Waarom investeren in meerdere inlog mogelijkheden ipv focussen op 1 goede en daardoor de veiligheid meer kunnen waarborgen. En minder kosten maken misschien.*
- *De Overheid en veilig IT nooit van gehoord, zal wel flagrant fout gaan.*
- *Oke, ik ben benieuwd welke nieuwe methodes er zijn ontwikkeld.*
- *o nee , niet nog meer mogelijkheden erbij*
- *Geen goede naam: Irma is de tolk van Rutte. Wordt hiermee geassocieerd denk ik.*
- *Ik zou dit niet doen omdat je bankgegevens en overheidgegevens niet samen moet kunnen worden gebruikt*
- *duidelijk overzicht inlogmiddelen.*
- *voortaan niet alleen inloggen met digid, klinkt mij vreemd in de oren*
- *Houd het nou gewoon eens simpel bij 1 methode. Waarom nu weer verschillende manieren van inloggen introduceren??*
- *Het is van de Rijksoverheid dus zal goed zijn*

5 Enkele citaten informatiepagina DigiD afzender

- *Veilig inloggen met alternatieven voor de Digid*
- *Op andere manieren inloggen bij de overheid dan met je DigiD*
- *Digid past bij iedereen*
- *Verbaasd?! De overheid die aangeeft dat je op meerdere manieren veilig kunt inloggen dan DigiD. Ik bekijk dit wantrouwend...*
- *Super handig dat er ook andere manieren zijn om in te loggen, fijn dat je zelf kunt bepalen, wat bij je past.*
- *Verwarrend dat er staat Digid het nieuwe inloggen en vervolgens wordt gesproken over andere manieren dan Digid*
- *Veranderd er weer iets aan digi-d?*
- *Hoe verhoudt zich Digid tot Digid, staat het er nou naast of is het een van de manieren*
- *Ik vind de pagina duidelijk dus kan ik jullie geen tips verschaffen*
- *[Veilig inloggen bij de overheid] verandert, maar dat hoeft niet als je alleen je DigiD gebruikt*
- *Die [inlogmiddelen] ken ik allemaal niet.meer info.*

6 Conclusies

- Het is goed mogelijk de kracht van dit merk te benutten binnen een omgeving met niet alleen het publieke DigiD, maar ook private inlogmiddelen. Dat kan door die private inlogmiddelen als een net zo veilig en betrouwbaar alternatief te presenteren náást DigiD:
 - op een centrale informatiepagina over het nieuwe stelsel (nu getest onder de werktitel ‘Het Nieuwe Inloggen’),
 - op de websites van publieke dienstverleners ,
 - op het keuzescherf waarop burger of bedrijf kiest met welk middel hij of zij inlogtVoorwaarde is wel dat de afzender van deze informatie de overheid is.
- Als DigiD als de afzender én als één van de middelen wordt gepresenteerd, kan dat leiden tot verwarring. Ook bestaat de kans dat dan de aandacht meer naar DigiD gaat dan naar de andere inlogmiddelen.
- Dat de andere inlogmiddelen door veel respondenten even veilig worden geacht als DigiD - onder andere door ze náást DigiD te plaatsen - betekent nog niet dat respondenten direct de meerwaarde van (de) nieuwe inlogmiddelen zien.

7 Aanbevelingen (1)

Presentatie

- **Gebruik de kracht van het merk DigiD door toegelaten private inlogmiddelen als een veilig en betrouwbaar alternatief te presenteren náást DigiD.** Deze manier van presenteren is op dit moment voor de eindgebruiker het eenvoudigst en duidelijkst: in één oogopslag een rij met middelen waar je uit kunt kiezen. Met de minste kans op verwarring (DigiD als afzender van het geheel en als inlogmiddel).

Communicatie

- **Zorg voor eenduidige communicatieboodschappen en termen.** Dat draagt bij aan het gevoel van betrouwbaarheid.
- **Zorg voor gerichte en regelmatige communicatie over dat ‘nieuwe inloggen’.** Voorafgaand aan én na de toelating van private inlogmiddelen. Met daarin niet alleen uitleg over de komst van nieuwe middelen, maar ook over het belang van veilig inloggen (en wat dat inhoudt).
- **Laat de aanbieders zelf communiceren over de specifieke voordelen van hun middelen.** Benadruk als overheid de voordelen van het hebben van meer inlogmiddelen.
- Ga aan de slag met de verdere uitwerking van een **centrale informatiepagina.**

7 Aanbevelingen (2)

Organisatie & samenwerking

- **Houd bij de uitwerking rekening met de langere termijn** - ineenschuiven middelen voor bedrijven en burgers, machtigingsvoorziening (niet alleen vrijwillig machtigen), mogelijkheid om laatst gekozen inlogmiddel te onthouden - **maar verlies daarbij de korte termijn** - over een half jaar tot een jaar - **niet uit het oog**.
- **Betrek de leveranciers bij gemaakte en te maken communicatieve keuzes**. Zodat ook zij kunnen bijdragen aan eenduidige communicatie. Dat komt uiteindelijk de eindgebruiker ten goede.
- **Doe in nauwe samenwerking met dienstverleners én waar mogelijk leveranciers op onderdelen nader onderzoek**, of sluit aan bij voorgenomen (UX-)onderzoeken. Doe dat zoveel mogelijk in kleine brokjes (voor een dienstverlener is het makkelijker twee varianten van een kernboodschap te testen dan een complete klantreis). Onder andere over:
 - voorgestelde en tot nu toe in tests gebruikte termen (inlogmiddelen, inlogmethodes, ect)
 - voorgestelde en tot nu toe in tests gebruikte boodschappen (het nieuwe inloggen, machtigen)