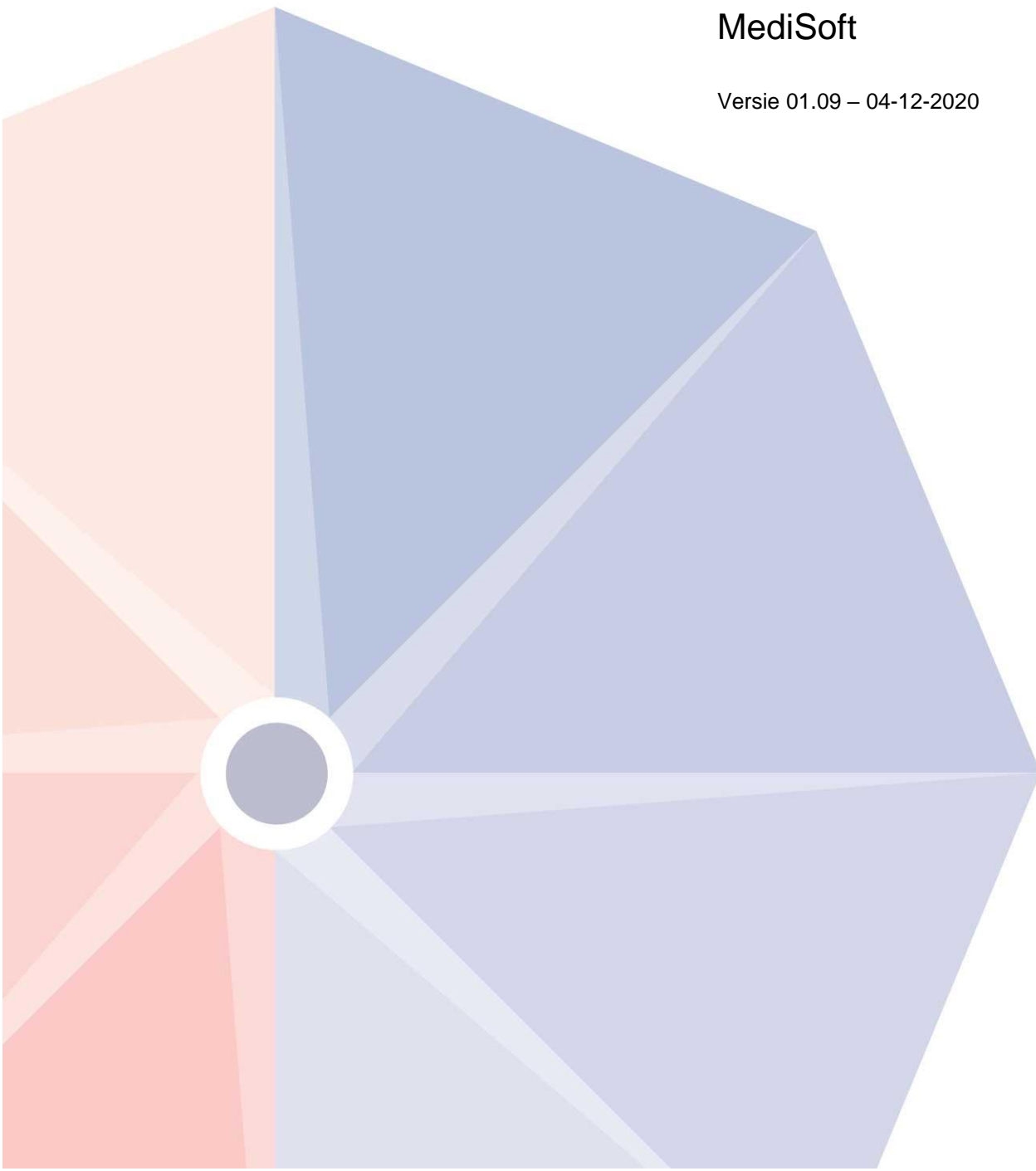


DM WEB PORTAAL  
Functionele handleiding  
tweefactor authenticatie  
Gebruikers

MediSoft

Versie 01.09 – 04-12-2020



## Inhoudsopgave

1.	Inleiding.....	2
1.1.	Tweefactor authenticatie methoden .....	2
1.1.1.	SMS authenticatie .....	2
1.1.2.	Google authenticator .....	2
1.2.	Versiehistorie.....	2
2.	Werking sms token .....	3
2.1.	Inloggen met tweefactor authenticatie .....	3
3.	Telefoonnummer verificatie.....	6
3.1.	Wijzigen van Mobiel 2 .....	6
3.2.	Inloggen zonder Mobiel 2 .....	7
4.	Werking Google authenticator .....	8
4.1.	Instellen van Google authenticator.....	8
4.2.	Inloggen met Google authenticator .....	9

# 1. Inleiding

Ten behoeve van extra beveiliging heeft MediSoft functionaliteit ontwikkeld voor zogenaamde tweefactor authenticatie (ook wel 2FA).

Authenticatie is het proces waarbij nagegaan wordt of een gebruiker daadwerkelijk is wie hij beweert te zijn. Over het algemeen wordt hiervoor gebruik gemaakt van een loginnaam en een wachtwoord. Alleen de gebruiker heeft kennis van het wachtwoord en kan zichzelf daarmee authenticeren.

Het kan gewenst zijn om de authenticatie sterker te maken. Hiervoor kan gebruik gemaakt worden van tweefactor authenticatie. Dan wordt er naast hetgeen wat de gebruiker weet (zijn wachtwoord) ook gebruik gemaakt van iets dat de gebruiker heeft (zijn telefoon) om vast te stellen dat het echt de gebruiker zelf is die inlogt.

In dit document staat beschreven hoe de tweefactor authenticatie werkt, en hoe het ingesteld kan worden. Dit document is bedoeld voor gebruikers van Dossier Manager.

## 1.1. Tweefactor authenticatie methoden

### 1.1.1.SMS authenticatie

MediSoft heeft er initieel voor gekozen om gebruik te maken van sms als extra authenticatie. De keuze is hier op gevallen omdat het gebruik van mobiele telefoons de meest brede manier is om dit in te vullen, tegen relatief lage kosten.

### 1.1.2.Google authenticator

Vanaf versie 7.1804 is er een extra methode beschikbaar gekomen, bijvoorbeeld Google Authenticator, deze kan worden ingesteld via de systeeminstellingen ( je kan ook kiezen voor een andere Authenticator).

## 1.2. Versiehistorie

Versie	Datum	Toelichting	Door
00.01	13 juli 2014	Conceptversie	Jeroen Arends
01.00	27 oktober 2014	Definitieve versie	Jeroen Arends
01.01	12 juni 2015	Uitbreiding tweefactor authenticatie met inloggen in DM CLIENT	Jeroen Arends
01.02	19 augustus 2015	Aanpassing sms providers	William Lo
01.03	26 oktober 2015	Telefoonnummer verificatie	Nico Assmann
01.04	24 juni 2016	Tweefactor authenticatie terminologie doorvoeren	Dennis van Hauwe
01.05	22 juli 2016	Revisie	Dennis van Hauwe
01.06	22 september 2016	Splitsing document in gebruikers en beheerder document	Dennis van Hauwe
01.07	31 december 2018	Toevoegen Google authenticator	William Lo
01.08	11 januari 2019	Revisie	Dennis van Hauwe
01.09	04 december 2020	Revisie	Michiel Noordhoek

## 2. Werking sms token

In dit hoofdstuk staat beschreven hoe tweefactor authenticatie wordt gebruikt. Indien ingesteld kan een gebruiker alleen inloggen in het DM WEB PORTAAL als hij zijn mobiele telefoon bij zich heeft. Daar zal namelijk een sms naar verstuurd worden.

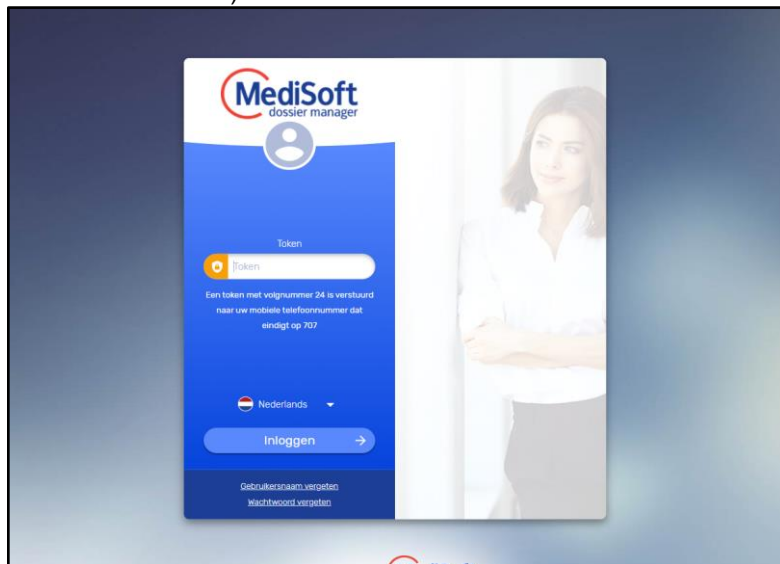
### 2.1. Inloggen met tweefactor authenticatie

Stap 1: Gebruiker logt in met zijn eigen gebruikersnaam en wachtwoord.



Afbeelding 2-1: Inloggen op het DM WEB PORTAAL

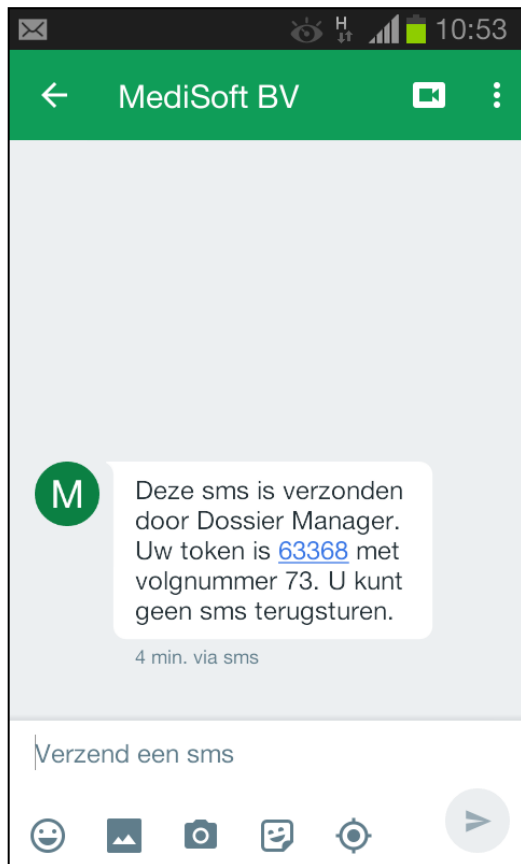
Stap 2: De gebruiker ziet nu een box verschijnen (in verschillende browsers kan dit er iets verschillend uitzien):



Afbeelding 2-2: Invoerbox tokencode op het DM WEB PORTAAL

N.B. Er is een volgnummer in het bericht opgenomen dat per inlogpoging steeds met 1 wordt verhoogd. Hiermee kan de gebruiker gemakkelijker bijbehorende sms-bericht achterhalen.

Tevens ontvangt de gebruiker vrijwel direct een sms-bericht, met daarin hetzelfde volgnummer en een token:



Afbeelding 2-3: sms-bericht is ontvangen

De token uit het sms-bericht moet ingevoerd worden in de verschenen box.



Afbeelding 2-4: Gebruiker voert de code in op het DM WEB PORTAAL

Hierna komt de gebruiker op normale wijze in het dashboard terecht op het DM WEB PORTAAL.



### 3. Telefoonnummer verificatie

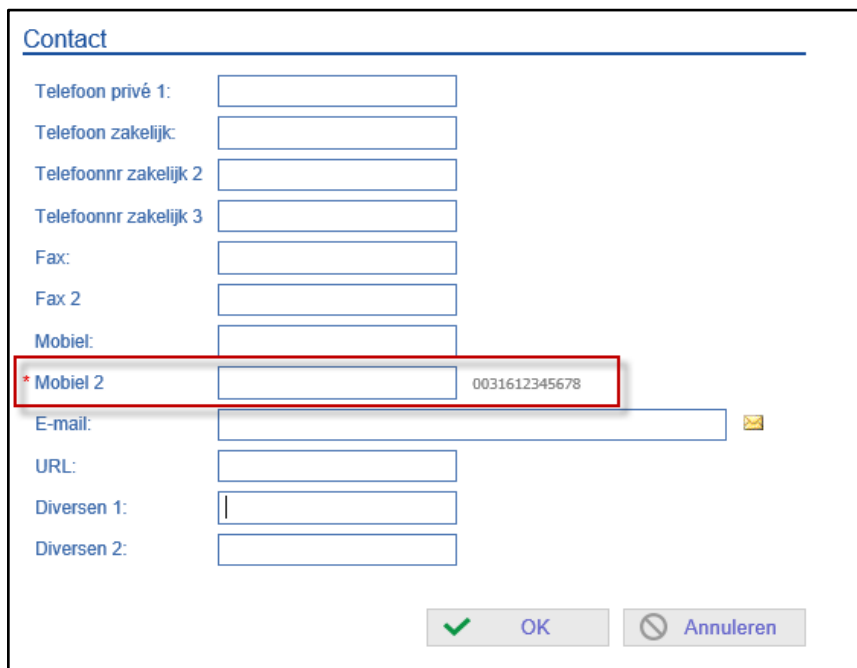
In dit hoofdstuk wordt de nieuwe functionaliteit "telefoonnummer verificatie" beschreven. Deze functionaliteit treedt op twee momenten in werking:

- Een DM WEB PORTAAL-gebruiker wijzigt zelf Mobiel 2
- Een DM WEB PORTAAL-gebruiker heeft nog geen Mobiel 2, en logt in

Bij beide situatie geldt dat de gebruiker via tweefactor authenticatie dient in te loggen.

#### 3.1. Wijzigen van Mobiel 2

Een DM WEB PORTAAL-gebruiker kan via Mijn gegevens, sub-pagina "Adres en Contact", zijn Mobiel 2 wijzigen.



Afbeelding 3.1: Contactinformatie gebruiker, Mobiel 2 is een verplicht veld.

Het veld Mobiel 2 is een verplicht veld als tweefactor authenticatie middels sms is ingesteld, maar kent geen verplicht formaat voor een geldig mobiel nummer waar aan voldaan moet worden. Het is wel aan te raden om een nummer in te geven dat voldoet aan het formaat van Nederlandse mobiele nummers (beginnend met 00316, totale lengte = 13 posities). Sommige providers kunnen hier namelijk niet goed mee omgaan.

### **3.2. Inloggen zonder Mobiel 2**

Van gebruikers die voor het eerst via tweefactor authenticatie moeten inloggen, kan Mobiel 2 nog ontbreken.

Deze gebruikers kunnen op dezelfde manier (zoals beschreven in de vorige paragraaf) een mobiel nummer opgeven en via een sms verifiëren.



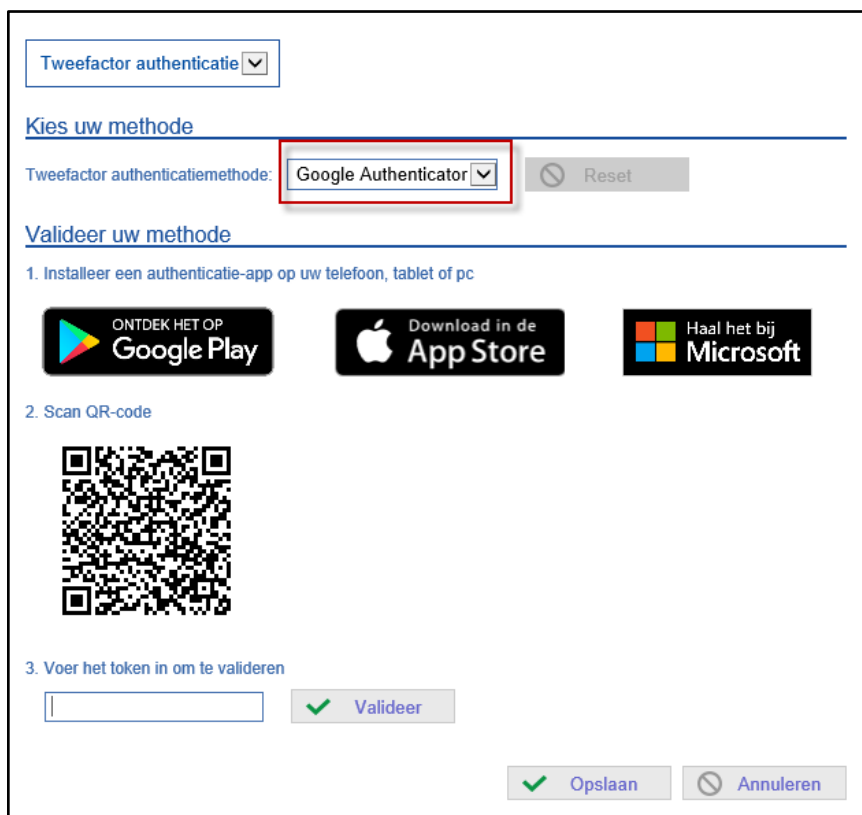
## 4. Werking Google authenticator

In dit hoofdstuk hebben wij de Google Authenticator als voorbeeld genomen maar je kan ook kiezen voor een andere Authenticator.

Indien ingesteld kan een gebruiker alleen inloggen in het DM WEB PORTAAL, indien hij zijn smartphone bij zich heeft met een geïnstalleerde Google authenticator app.

### 4.1. Instellen van Google authenticator

Om gebruik te maken van de Google authenticator als tweefactor authenticatie, moet de gebruiker dit instellen in 'Mijn instellingen' onder sectie 'Tweefactor authenticatie', hierbij moet de gebruiker nogmaals zijn wachtwoord invoeren. Daarna kan men pas de instelling wijzigen.



Afbeelding 4-1: Mijn instellingen Tweefactor authenticatie.

Selecteer hier bij 'Tweefactor authenticatiemethode' voor Google Authenticator.

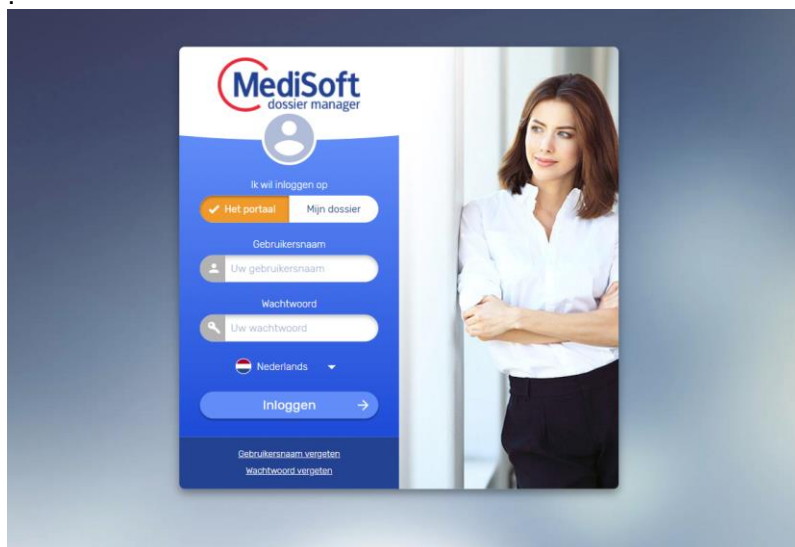
Zorg ervoor dat er een Google authenticator app is geïnstalleerd op jouw smartphone. Open de app en scan de getoonde QR-code, hierna zal er een token worden gegenereerd, voer deze in bij punt 3 en klik op de knop '**Valideer**'.

Er zal een bevestigingsmelding omhoog komen, klik hier op de knop '**OK**' om de validatie te bevestigen. Klik daarna op '**Opslaan**' om de instelling te bewaren.

De Google authenticatie is nu ingesteld en wordt bij de eerstvolgende keer inloggen op het DM WEB PORTAAL.

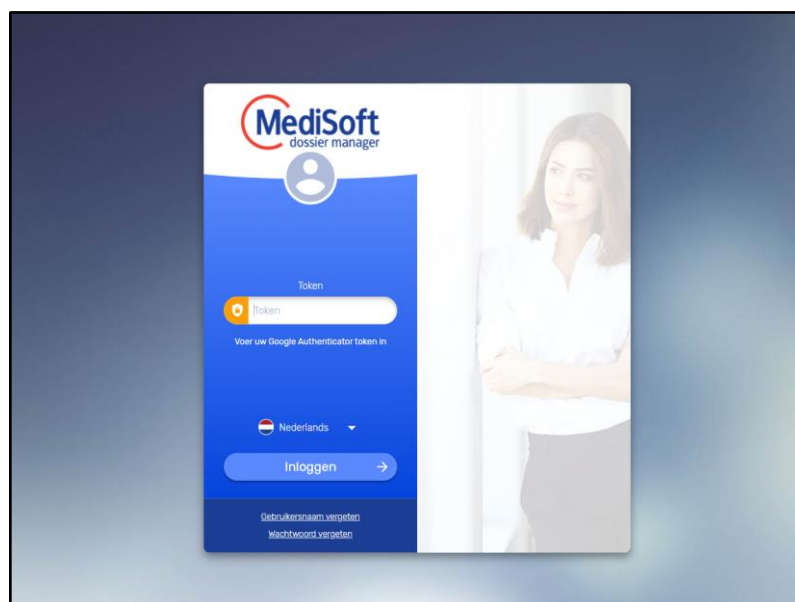
## 4.2. Inloggen met Google authenticator

Stap 1: Gebruiker logt in met zijn eigen gebruikersnaam en wachtwoord



Afbeelding 4-2: Aanmeldscherm DM WEB PORTAAL.

Stap 2: De gebruiker ziet nu een box verschijnen (in verschillende browsers kan dit er iets verschillend uitzien).



Afbeelding 4-3: Google Authenticator token.

Na het invoeren van de token kan men op normale wijze in het dashboard terecht op het DM WEB PORTAAL.