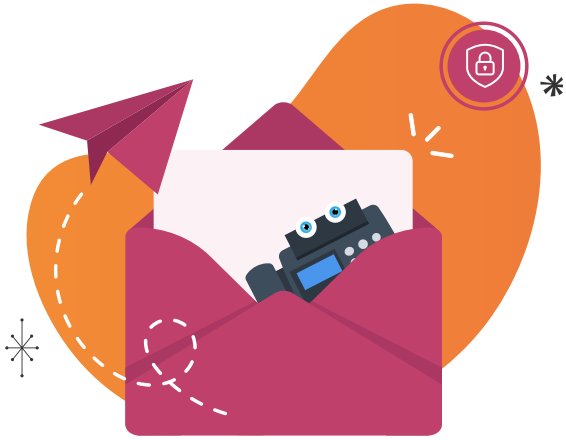


Authenticatie & veilig mailen

Waarom veilig mailen?

We communiceren meer dan ooit online. De zorgverlener gaat steeds bewuster om met het verwerken en versturen van medische gegevens. Dat betekent dat we ook gevoelige informatie, zoals bijvoorbeeld dossiers met persoonlijke (medische) gegevens steeds vaker naar elkaar mailen. Toch is nog niet altijd duidelijk wat de zorgverlener dan moet regelen om aan de geldende wet- en regelgeving te voldoen.

Onbedoelde toegang tot de inhoud van een e-mail is bezwaarlijk, zeker als het gaat om medische gegevens. Deze gegevens verdienen een hoog niveau van bescherming. De NTA7516 biedt deze bescherming. Deze norm beschrijft de eisen waaraan e-mail moet voldoen om veilig te zijn. Als je zonder veilige e-mailoplossing medische gegevens opstuurt naar een andere professional of naar de patiënt zelf, overtreedt je de algemene verordening van gegevensbescherming, ook wel bekend als de AVG.

Veilige communicatie begint bij het beveiligen van de e-mail

Het “gewone” e-mailverkeer vindt ‘onversleuteld’ plaats. Het gevolg daarvan is dat iedereen die de e-mail ontvangt, de e-mail ook kan lezen. Wordt de email naar de verkeerde persoon verstuurt, dan is de informatie altijd leesbaar en is er sprake van een datalek. Je kunt je hiertegen beschermen door het versleutelen van het bericht en het bericht beveiligen met authenticatiefactoren.

Authenticatie, identificatie en verificatie

Authenticatie en verificatie worden veelal door elkaar gebruikt. Authenticatie en verificatie hangen nauw samen met identificatie.

In feite zijn het beveiligingsprocessen met verschillende doelen.

Identificatie: het bepalen van de identiteit van een gebruiker of andere entiteit, dit kan bijvoorbeeld doormiddel van een paspoort of gebruikersnaam.

Verificatie: onderzoek naar de echtheid of juistheid van gedane opgaven (authenticiteit). Met andere woorden toetsing aan de waarheid. Voorbeeld van het paspoort: controleer of de persoon die voor je staat ook degene is die in het paspoort wordt genoemd.

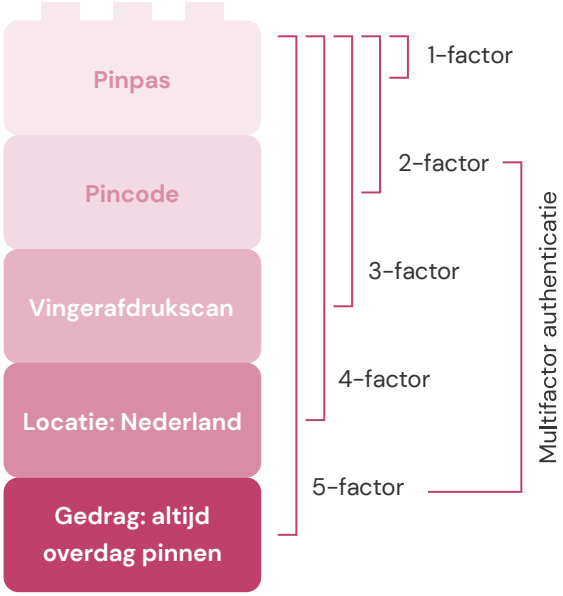
Authenticatie: controleren of het bewijs van identiteit voldoende is voor toegang. Authenticatie gaat een stapje verder, met andere woorden: ben je wel wie je zegt dat je bent? Authenticatie zonder voorafgaande identificatie heeft geen zin. Er zijn verschillende authenticatievormen.

Autorisatie: valideert of de gebruiker inderdaad toestemming heeft om toegang te krijgen.

Authenticatievormen

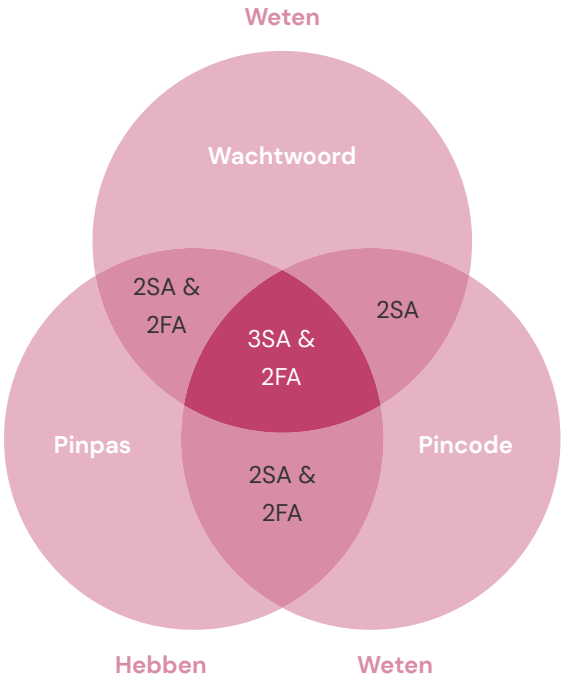
Er zijn verschillende authenticatievormen die gebruikt worden ter bescherming van gegevens en gecombineerd worden om een hoger of lager niveau van beveiliging te krijgen. Daarbij zijn de volgende vormen van bewijs bruikbaar:

- Iets wat je weet: zoals een wachtwoord, wachtzin of pincode.
- Iets wat je hebt: zoals een pasje, token of los apparaat.
- Iets wat je bent: biometrische kenmerken zoals een vingerafdruk, irisscan of aderpatroon.
- Iets wat toetsbaar is: zoals een digitaal certificaat.



Afb. 1: Multifactor authenticatie.

Meerfactorauthenticatie of Multi-Factor Authenticatie (MFA) is een vorm van (toegangs) beveiliging waarbij de gebruiker zich met een combinatie van minimaal twee verschillende typen authenticatiefactoren moet authentiseren om toegang te krijgen tot een computer, (besturings) systeem of applicatie.



Afb. 2: Tweefactorauthenticatie (2FA) vs. Tweestapsverificatie (2SA).

Dit soort authenticatie wordt ook wel Twee-Factor Authenticatie (2FA) genoemd. Hoewel 'twee-factor authenticatie' een populaire term blijft, is MFA steeds meer de overkoepelende term geworden. MFA voegt een extra beveiligingslaag toe aan het aanmeldingsproces.

Wanneer gebruikers toegang willen tot een account of app, moeten ze hun identiteit nog een keer extra verifiëren, bijvoorbeeld via een scan van hun vingerafdruk of door het invoeren van een code die ze hebben ontvangen op hun telefoon.

Tweefactorauthenticatie versus Tweestapsverificatie

Tweefactorauthenticatie (2FA) betekent dat je twee manieren gebruikt om te verifiëren dat jij het bent.

Voor **Tweestapsverificatie (2SA)** geldt iets anders. Hier heb je ook twee manieren om te laten zien dat jij het echt bent die op je account inlogt, maar dat hoeven niet per se twee verschillende factoren te zijn, zoals hierboven beschreven. Inloggen met tweefactorauthenticatie (2FA) is een stuk veiliger en verkleint de kans dat onbevoegden toegang krijgen tot het account of gegevens. Er wordt gebruik gemaakt van twee verschillende authenticatievormen (factoren) om in te loggen.

Verkrijgen tweefactor authenticatie voor veilige e-mail

Nadat verificatie in twee stappen is ingeschakeld, moet de tweede stap ook geverifieerd worden. Dat kan op de volgende manieren:

1. SMS

De bekendste optie is het ontvangen van een code via sms. Dat is ook de minst veilige methode wegens gevaar voor sim swapping.

- *Voordeel:* Laagdrempelig en voor de meeste mensen is tweestapsverificatie via sms echter voldoende en veel beter dan helemaal geen tweestapsverificatie.
- *Nadeel:* Een SMS is in theorie relatief makkelijk te onderscheppen.

2. E-mail

De eenmalige toegangscode wordt verzonden naar een e-mailadres bekend bij de ontvanger. Hierbij kan de keuze gemaakt zijn om dit naar een separaat e-mailadres te sturen maar ook om dit naar hetzelfde e-mailadres te sturen als het beveiligde bericht.

- *Voordeel:* Laagdrempelig toe te passen door de verzender (indien deze geen mobiel telefoonnummer van de ontvanger heeft).
- *Nadeel:* In de meeste e-mailprogramma's worden e-mails niet direct ontvangen, maar gaat het per minuut of een iets langer tijdvak. Het kan ook onveilig zijn bij het gebruik van dezelfde e-mailadres. Want als onbevoegden toegang hebben tot je e-mailaccount kunnen ze ook bij de e-mail.

3. Authenticator applicatie

Een authenticator applicatie is een app die gekoppeld wordt aan een account, zodat je een andere manier hebt om in twee stappen in te loggen. Zodra de app aan je account is gekoppeld, levert deze een wisselende en unieke code die toegang geeft tot je account.

- *Voordeel:* Je inlogcodes zijn altijd beschikbaar zijn, ook als je geen of een slechte internetverbinding hebt.
- *Nadeel:* Je bouwt een security gevoelige sleutel in je toepassing die toegang heeft tot al je wachtwoorden en creëert daarmee mogelijk een goudmijn voor onbevoegden.

4. Fysieke beveiligingssleutel

PKI (Public Key Infrastructure) authenticatie oftewel inlogsleutel, waarbij gebruik wordt gemaakt van een certificaat op een USB-token of smartcard gecombineerd met een wachtwoord. In de zorg wordt gebruik gemaakt van een token of UZI-pas. Het UZI-register koppelt de fysieke identiteit van een zorgverlener aan een elektronische identiteit en legt deze vast in een certificaat.

Het UZI-register vervult hiermee de rol van Trusted Service Provider (TSP) en verstrekt en beheert de certificaten en sleutelinformatie. Bij het certificeren wordt gebruik gemaakt van een Public Key Infrastructure (PKI).

- *Voordeel:* Zeer veilige vorm van authenticatie met één toegangspunt dat niet gedupliceerd kan worden.
- *Nadeel:* Bij verlies van de fysieke sleutel kan de dienst niet meer worden gebruikt.

5. Vooraf afgesproken code/gedeelde toegangscode

In sommige gevallen is het mogelijk om doormiddel van een vooraf afgesproken code/ wachtwoord toegang te verkrijgen tot beveiligde informatie. Deze code wordt afgesproken tussen twee specifieke partijen waardoor er niet iedere keer een nieuwe code wordt gedeeld. Variant is dat een code voor 30 of 90 dagen geldt en dan opnieuw moet worden aangevraagd/ gedeeld.

- *Voordeel:* Je hoeft maar één toegangscode te onthouden.
- *Nadeel:* De gedeelde toegangscode eenmaal is ingesteld kan alleen een beheerder deze nog aanpassen of verwijderen.

Bronnen

- https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens?qa=meerfactorauthenticatie&scrollto=1

- https://www.techtarget.com/searchsecurity/definition/three-factor-authentication-3FA

- https://www.uziregister.nl/over-het-register/certificeringsbeleid