

Handreiking

2-Factor authenticatie (2FA) voor gemeenten

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

Colofon

**Naam document**

Handreiking 2-factor authenticatie voor gemeenten

**Versienummer**

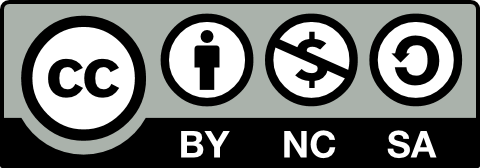
1.0

**Versiedatum**

Oktober 2020

**Versiebeheer**

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).



Vereniging van Nederlandse Gemeenten/ Informatiebeveiligingsdienst voor gemeenten (IBD)

Tenzij anders vermeld, is dit werk verstrekt onder een Creative Commons Naamsvermelding-Niet Commercieel-Gelijk Delen 4.0 Internationaal licentie. Dit houdt in dat het materiaal gebruikt en gedeeld mag worden onder de volgende voorwaarden: Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. De IBD wordt als bron vermeld.
2. Het document en de inhoud mogen commercieel niet geëxploiteerd worden.
3. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door de IBD en/ of de Vereniging van Nederlandse Gemeenten.
4. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Wanneer dit werk wordt gebruikt, hanteer dan de volgende methode van naamsvermelding: “Vereniging van Nederlandse Gemeenten/ Informatiebeveiligingsdienst voor gemeenten”, licentie onder: CC BY-NC-SA 4.0.

Bezoek <http://creativecommons.org/licenses/by-nc-sa/4.0> voor meer informatie over de licentie.

**Rechten en vrijwaring**

De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

**Met dank aan**

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

### Wijzigingshistorie

|  |  |  |
| --- | --- | --- |
| Versie | Datum | Wijziging/ Actie |
| 1.0 | Oktober 2020 | Eerste versie |
|  |  |  |

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT/ CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy/ gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

**Doel**

Het doel van dit document is een handreiking te verschaffen voor gemeenten die volgens de BIO-maatregel 9.4.2.1. 2-factor authenticatie willen implementeren.

**Doelgroep**

Dit document is van belang voor informatiebeveiligers van de gemeente, de CISO, het management van de gemeente, de systeemeigenaren, applicatiebeheerders en de ICT-afdeling.

**Relatie met overige producten**

* Baseline Informatiebeveiliging Overheid (BIO)
* Informatiebeveiligingsbeleid van de gemeente
* Handreiking beleid logisch toegangsbeveiliging
* Wachtwoordbeleid
* Wachtwoordkluizen

**Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)**

9.4.2 Beveiligde inlogprocedures

9.4.2.1 Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.

Inhoudsopgave

[Inhoudsopgave 5](#_Toc53577823)

[1. Inleiding 6](#_Toc53577824)

[1.1. BIO Eisen 6](#_Toc53577825)

[2. De basis 7](#_Toc53577826)

[2.1. 1FA, 2FA en MFA 8](#_Toc53577827)

[2.2. Waarom 2FA? 8](#_Toc53577828)

[2.3. 2FA beschermd tegen 9](#_Toc53577829)

[2.4. Nadelen en risico’s van 2FA 9](#_Toc53577830)

[3. Soorten 2FA 10](#_Toc53577831)

[3.1. Algemeen 10](#_Toc53577832)

[3.2. SMS 11](#_Toc53577833)

[3.3. Apps 12](#_Toc53577834)

[3.4. Tokens 12](#_Toc53577835)

[4. Tips voor gemeenten 15](#_Toc53577836)

[5. Stappenplan 16](#_Toc53577837)

# Inleiding

In de BIO staan diverse eisen die te maken hebben met toegangsbeveiliging in hoofdstuk 9. De gemeente dient hier aanvullend beleid voor te ontwikkelen, er is een handreiking beleid logische toegangsbeveiliging van de IBD die hier op ingaat[[1]](#footnote-1). In paragraaf 9.4 en bij control 9.4.2 staat een maatregel die gericht is op het aanvullend beschermen van login procedures, met name als er vanuit een onvertrouwde zone toegang verleend moet worden op de ICT-systemen van de gemeente (de vertrouwde zone). Deze eis is al van toepassing vanaf BBN1 en zeker sinds het uitbreken van de coronacrisis werken veel gemeenteambtenaren vanuit thuis. Dit betekent dat gemeenteambtenaren inloggen vanaf een onvertrouwde zone op gemeentelijke systemen. Het risico bestaat dan dat indien er geen 2-factor authenticatie (hierna 2FA genoemd) gebruikt wordt om toegang te krijgen tot gemeentelijke systemen, de enige bescherming tot gemeentelijke systemen de gebruikersnaam in combinatie met het wachtwoord is. Hierdoor loopt de gemeente onnodig risico tot toegang door onbevoegden. Op het Darkweb circuleren met regelmaat lijsten met e-mailadressen en wachtwoorden die buitgemaakt zijn en die gebruikt kunnen worden om in te breken. Het misbruiken van een digitale identiteit om in te breken in systemen is de meest voorkomende vorm van aanvallen op webapplicaties. Daarnaast proberen hackers bij een ransomware aanval administrator accounts te misbruiken, als deze voorzien zijn van een 2e inlog factor dan wordt dit bemoeilijkt, zie ook paragraaf 2.3.

Dit document geeft algemene aanwijzingen over het 2FA in relatie tot het logisch toegangsbeleid en de maatregelen in de BIO.

## BIO Eisen

In de BIO staan een aantal onderwerpen die raken aan wachtwoordveiligheid, dit zijn:

|  |  |  |  |
| --- | --- | --- | --- |
| **9.4.2** | **1** | **Beveiligde inlogprocedures**  Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure. | Proceseigenaar  Dienstenleverancier |
| 9.4.2.1 | 1 | Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie |

# De basis

Dagelijks heeft men te maken met het identificatie, authenticatie en autorisatie (het IAA-) concept en het is belangrijk om te weten wat deze termen inhouden en waarom deze drie termen in samenhang gebruikt worden. Het IAA-concept is de basis en essentieel voor gegevensbescherming en daarom eerst een korte uitleg en een voorbeeld uit de fysiek wereld.

Een nieuwe gemeentemedewerker komt voor het eerst naar het gemeentehuis en meld zich bij de receptie, verteld zijn naam met de mededeling erbij dat hij een nieuwe medewerker is. De medewerker identificeert zichzelf hiermee, hij vertelt wie hij is.

De receptioniste wil graag zeker weten of de nieuwe medewerker is wie hij zegt dat hij is en vraagt om een identificerend document, bijvoorbeeld een ID-kaart of een ander vergelijkbaar geschikt bewijs. De nieuwe medewerker toont het gevraagde document. De receptioniste vergelijkt de foto met de persoon en stelt vast dat de bewering klopt. De werknemer heeft zijn identiteit bevestigd en is geauthentiseerd door de receptioniste.

Vervolgens vraagt de receptioniste bij wie de nieuwe medewerker zich moet melden en controleert dit door de bewuste persoon op te bellen en spreekt af dat de nieuwe medewerker wordt opgehaald. Als de nieuwe medewerker vervolgens, onder begeleiding, mag meelopen het pand in, dan is hij geautoriseerd om het pand binnen te gaan.

Bovenstaande voorbeeld geeft drie duidelijke stappen aan die voor het IAA-concept doorlopen zijn.



Alle drie stappen - identificatie, authenticatie en autorisatie - zijn de fasen van één proces dat de toegang van gebruikers tot hun accounts controleert. In de digitale wereld gaat dit vergelijkbaar, onderstaand een voorbeeld.

Om bijvoorbeeld in te loggen op een website of dienst, moet de gebruiker "zichzelf introduceren" in het systeem. De identificatie is in dit geval het invoeren van een gebruikersnaam of e-mailadres waarmee eerder de gebruiker is aangemaakt door een beheerder van het systeem of de gebruiker zelf. De gebruiker maakt zijn identiteit kenbaar en die kan door de webserver worden geverifieerd in de database met gebruikersgegevens.

Tegelijkertijd of in een tweede stap voert de gebruiker van het systeem ook zijn wachtwoord in, dit wachtwoord wordt vergeleken met het eerder opgegeven wachtwoord en als de naam en bijbehorend wachtwoord kloppen wordt de gebruiker geauthentiseerd. Vervolgens kan de volgende stap doorlopen worden, er wordt gecontroleerd welke rechten de gebruiker heeft in het systeem, en deze rechten zorgen ervoor dat geregeld wordt wat deze gebruiker wel of niet mag. De gebruiker wordt dus geautoriseerd om bepaalde taken uit te voeren binnen het systeem.

Het alleen gebruiken van een wachtwoord is handig maar introduceert ook risico’s. Deze risico’s staan beschreven in het IBD-document Handreiking Wachtwoordbeleid, hoofdstuk 2.4.

## 1FA, 2FA en MFA

De afkortingen 1FA, 2FA en MFA staan voor verschillende vormen van het authenticatie proces. 1FA staat voor 1-factor authenticatie en 2FA staat voor 2-factor authenticatie en MFA staat voor multi-factor authenticatie. Dus deze termen worden gebruikt om aan te duiden hoeveel factoren gebruikt worden voor het authenticatieproces. In het bovenstaande voorbeeld wordt alleen het wachtwoord gebruikt, dit wachtwoord is 1-factor. Er kunnen meerdere factoren gebruikt worden om de mate van zekerheid te verhogen waarmee vastgesteld kan worden dat iemand is die hij zegt dat hij is. Daarnaast werpen die factoren extra drempels op, bijvoorbeeld iemand heeft toegang tot wachtwoorden en mailadressen die zijn buitgemaakt bij een hack. Zonder een extra authenticatie factor kan die informatie gebruikt worden om als iemand in te loggen in een systeem. De factoren die meestal gebruikt worden zijn:

1e factor: iets wat je weet, bijvoorbeeld je wachtwoord of een pincode

2e factor: iets wat je hebt, bijvoorbeeld een token of een app

3e factor: iets wat je bent, bijvoorbeeld biometrie als vingerafdruk of gezicht.

Er zijn publicaties die hier nog andere factoren aan toevoegen, bijvoorbeeld locatie of tijd, In dit document gaan we hier niet verder op in. In dit document gaan we wel in op 2FA, dus iets wat je weet en iets wat je hebt.

Dat iets wat je hebt is doorgaans iets, wat een eenmalig wachtwoord genereerd of vergelijkbaar, maar er zijn ook andere varianten, daarover verderop meer.

Door deze drie factoren te combineren is met redelijk hoge zekerheid vast te stellen of het klopt dat wie iemand beweert te zijn. Er zijn zelfs situaties denkbaar waar meerdere vormen van factor 2 – iets wat je hebt en factor 3 – iets wat je bent worden gebruikt, maar dit is erg uitzonderlijk. Denk hier bijvoorbeeld aan te toegang tot een datacenter of een afdeling/ruimte/systeem waar hoog geclassificeerde informatie wordt verwerkt.

Voor dit document gaan we niet in op factor 3 biometrie, dit is in de eerste plaats een bijzonder persoonsgegeven in de zin van de Algemene verordening gegevensbescherming (AVG)[[2]](#footnote-2) en het gebruik hiervan is aan strikte regels gebonden. Het is niet waarschijnlijk dat een gemeente ergens een toepassing heeft die het noodzakelijk maakt dat biometrie als factor gebruikt moet worden. Verwar biometrie niet met het ontsluiten van bijvoorbeeld een mobiele telefoon of app met een vingerafdruk. In dat geval wordt één factor, bijvoorbeeld biometrie gebruikt om de pincode of gebruikersnaam en wachtwoord in de vullen op bijvoorbeeld een website of de bankieren app. Hier gaat het meer om gebruiksgemak en het door de telefoon laten vaststellen dat de persoon waarschijnlijk wel de eindgebruiker is, dat heeft niets te maken met 2FA.

## Waarom 2FA?

Het implementeren van 2FA is een van de meest effectieve acties die een gemeente kan ondernemen om de beveiliging van de online toegang tot gemeentelijke applicaties te verhogen, zodat alleen geautoriseerde gebruikers toegang hebben tot de vertrouwelijke gegevens van de gemeente.

2FA, gebruikt in combinatie met een gebruikersnaam, kan ongeoorloofde toegang voorkomen door ervoor te zorgen dat alleen een eindgebruiker, die kan worden gevalideerd tegen een tweede authenticatiefactor, toegang krijgt tot de (online) bron of applicatie. Het misbruiken van authenticatie gegevens zoals gebruikersnaam en wachtwoorden is de meest voorkomende vorm van aanvallen op webapplicaties.

Door het toevoegen van de extra factor wordt meer zekerheid verkregen.

We hebben momenteel de Corona pandemie en gebruikers van gemeentelijke systemen worden gedwongen thuis te werken. Thuis werken in combinatie met 2FA stelt de gemeente in staat net die mate van veiligheid toe te voegen die noodzakelijk is om meer zekerheid te krijgen over wie inlogt in de gemeentelijke systemen, waardoor werknemers taken op afstand kunnen uitvoeren met veel minder beveiligingsproblemen. Dit geldt natuurlijk ook voor medewerkers met systeembeheertaken die op afstand vanuit een onvertrouwde zone beheertaken moeten uitvoeren met meer rechten dan standaard gebruikers. Dit geldt ook voor het gebruik van software waarmee beheer op afstand kan worden gedaan, daarvoor is alleen gebruikersnaam en wachtwoord te zwak.

Gemeenten voeren audits en pentesten uit, installeren firewalls hebben antivirus oplossingen en zijn bezig met netwerk bewaking, allemaal noodzakelijk beveiligingsoplossingen. Echter zonder gedegen gebruikersauthenticatie staat de voordeur echter wijd open voor indringers. Het is zelfs aan te raden om 2FA in te voeren voor alle gemeentelijke systemen onafhankelijk of deze van “buiten” of van “binnen” benaderd worden.

## 2FA beschermt tegen

Er zijn er al een paar voorbeelden genoemd, maar 2FA beschermt tegen een aantal soorten aanvallen die gebaseerd zijn op het verkrijgen van gebruikersnamen en wachtwoorden:

* Vele soorten aanvallen gaan over het bemachtigen van gebruikers authenticatie informatie. Het proberen om geldige inloggegevens te krijgen, maakt deel uit van vele aanvalsstijlen en -patronen, zo ook het verspreiden van malware, waarna gebruikers accounts worden misbruikt waardoor uiteindelijk een ransomware aanval kan worden uitgevoerd.
* Wachtwoorden worden hergebruikt, zo kan een wachtwoord van een webwinkel of hobby forum worden hergebruikt door de eindgebruiker en ook de gemeente worden gehackt.
* Het ouderwetse hacken door middel van brute force- en woordenboekaanvallen, waarbij daders software gebruiken om enorme hoeveelheden combinaties van gebruikersnaam en wachtwoord te genereren in een poging de inloggegevens van een gebruiker te raden. Deze bestanden met gebruikers informatie en dus ook wachtwoorden circuleren met regelmaat in het Darkweb.
* Mystery guest of social engineering-aanvallen, bijvoorbeeld doormiddel van phishing e-mails en spear-phishing (gericht op een specifiek individu), die proberen een gebruiker te misleiden om gevoelige gegevens te onthullen, inclusief hun gebruikersnaam en wachtwoord.
* Het delen van wachtwoorden wordt bemoeilijkt omdat sommige varianten van de 2e-factor niet of niet makkelijk gedeeld kunnen worden.

## Nadelen en risico’s van 2FA

Naast de voordelen heeft 2FA ook nadelen en brengt risico’s met zich mee. In deze paragraaf worden deze beschreven.

### Nadelen 2FA

2FA heeft ook nadelen die met name door gebruikers ervaren worden. Een nadeel is dat het inloggen met nog een extra methode natuurlijk tijd en handelingen kosten die de gebruiker moet uitvoeren. Een ander nadeel is dat de tweede factor, “iets dat je hebt” ook meegenomen moet worden. Dat nadeel is wat kleiner bij een smartphone app dan bij een hardware token, gelukkig zijn de hardware tokens tegenwoordig erg klein. Het is dus raadzaam om al van tevoren na te denken welke back-up men zou willen in het geval dat een token/ app niet beschikbaar is.

Een ander punt is dat het 2FA-systeem ook beheerd moet worden en er moet ook nagedacht worden hoe lang het inloggen met de tweede factor geldig is. Als men bijvoorbeeld bij een bank inlogt met een tweede factor dan wordt de sessie met de bank applicatie na verloop van tijd afgesloten, dan kan men alleen verder na een nieuwe inlog met de tweede factor. Als dit met bijvoorbeeld een online applicatie gedaan wordt waar continue in gewerkt wordt dan is dit niet praktisch. Er moet dus worden nagedacht over de levensduur van de sessie waarop ingelogd is met 2FA, dus gerelateerd aan het gebruiksdoel en het risico dat men onderkend.

### Risico’s 2FA

Naast de hierboven beschreven nadelen zijn er ook risico’s die genoemd moeten worden. Overigens zijn deze risico’s ook van toepassing als alleen gebruik gemaakt wordt van gebruikersnaam en wachtwoorden. Het gebruik van 2FA is nog steeds vele malen veiliger dan alleen een wachtwoord gebruiken!

Onderscheppen sessie cookie

Door het gebruik van een 2FA token wordt er door de webserver een zogenaamd sessie cookie teruggegeven aan de browser welke wordt opgeslagen. Als een aanvaller dat sessie cookie kan onderscheppen hoeft hij helemaal niet meer in te loggen om toegang te krijgen tot een dienst.

Phishing

Als een gebruiker een phishing-mail/bericht ontvangt waarin hem wordt gevraagd in te loggen op bijvoorbeeld een bankrekening en de gebruiker vult op een nagemaakte, niet van echt te onderscheiden, inlog-pagina de gebruikersnaam, wachtwoord en token in dan is het kwaad geschied en kan de aanvaller deze informatie gebruiken om zich voor te doen als de gebruiker.

# Soorten 2FA

## Algemeen

Een eenmalig wachtwoord (OTP = One Time Password), ook bekend als eenmalige pincode of dynamisch wachtwoord, is een wachtwoord dat geldig is voor slechts één inlogsessie of transactie, op een computersysteem of ander digitaal apparaat. OTP's vermijden een aantal tekortkomingen van wachtwoord gebaseerde authenticatie. Zie voor meer informatie ook het document, “Factsheet Gebruik Tweefactorauthenticatie” van het NCSC.

Meestal worden eenmalige wachtwoorden gegenereerd door middel van een klein apparaatje, een keyfob genaamd of een mobiele telefoon met een app of een smartcard achtig token. Hierbij gebruik je meestal iets wat je weet (een pincode) om een eenmalig wachtwoord te genereren. Er zijn ook oplossingen die op tijd gebaseerd om een bepaalde tijdseenheid een nieuwe code tonen. Soms worden eenmalige wachtwoorden per SMS verzonden.

Een van de belangrijkste voordelen van eenmalige wachtwoord generatoren is dat ze in tegenstelling tot statische wachtwoorden, niet kwetsbaar zijn voor herhalingsaanvallen (replay attacks). Dit betekent dat een potentiële indringer die erin slaagt een eenmalig wachtwoord te onderscheppen die al werd gebruikt om in te loggen op een dienst of om een transactie uit te voeren, deze niet kan misbruiken, omdat deze niet langer geldig is. Een tweede groot voordeel is, dat als een eindgebruiker zwakke wachtwoorden gebruikt of wachtwoorden hergebruikt, niet op alle systemen kwetsbaar is als het wachtwoord voor een van deze systemen wordt verkregen door een aanvaller. Er is immers nog een eenmalig wachtwoord dat gevraagd wordt, dus door een hacker buitgemaakte (zwakke) wachtwoorden kunnen niet eenvoudig worden misbruikt. Een ander voordeel is dat als een eenmalig wachtwoord opgegeven moet worden voor belangrijke beheertaken een aanvaller niet in staat zal zijn om voor zichzelf een administrator account te maken. Dit laatste is een van een aanvals vectoren van bijvoorbeeld een ransomware aanval.

Eenmalige wachtwoorden zijn dus een aanvulling op, of een vervanging van traditionele wachtwoorden.

OTP's zijn besproken als een mogelijke vervanging voor, en als verbetering van, traditionele wachtwoorden.

Er zijn drie typen van eenmalige wachtwoorden, SMS, apps en tokens. Deze worden in onderstaande paragrafen worden toegelicht.

## SMS

Sms-codes die worden gegenereerd en verzonden, zijn de meest voorkomende factoren die worden gebruikt bij mobiele 2FA. Veel mensen hebben wel een telefoon die SMS kan ontvangen, dit is laagdrempelig en het kost niet veel tijd. Bovendien is deze controle in de meeste gevallen effectief, bijvoorbeeld om te beschermen tegen geautomatiseerde aanvallen, phishing, bruteforcing van wachtwoorden, virussen en dergelijke.

Het omzeilen van sms-verificatie is mogelijk voor een hacker als hij daar moeite voor wil doen. Het telefoonnummer dat aan het gebruikersaccount is gekoppeld, is meestal geen geheim want telefoonnummers zijn te vinden omdat ze worden gebruikt voor vele doeleinden, op visitekaartjes, op social media en in adresboeken van bekenden. Nadat kwaadwillenden de persoonlijke informatie van de eigenaar van het nummer hebben ontvangen, kan men een valse identiteitskaart maken en gebruiken deze bij het kantoor van de mobiele operator. Er zijn ook gevallen bekend waar men telefonisch alle informatie kon aanpassen die men wilde, en dit ondanks het feit dat in sommige landen de wetgeving een volledige controle van de ID-gegevens vereist. Er kan dan een SIM worden geautoriseerd voor heruitgifte door de telefoon winkel, zonder de moeite te nemen om de authenticiteit van het identificerend document te verifiëren. Zo wordt er een nieuwe SIM kaart met het bestaande nummer gemaakt waarna de kwaadwillende de tweede authenticatiestap, de ontvangen van een SMS kan gebruiken als tweede factor. Als uw eigen SIM kaart blijft werken bij deze aanval dan kunnen de sms-berichten helpen erachter te komen dat iemand probeert het account te hacken.

### Voordelen

* Eenvoudig in gebruik - de gebruiker hoeft alleen de code in te voeren van het sms-bericht dat naar zijn mobiele telefoon is verzonden.
* Als er een poging tot het hacken van uw account plaatsvindt, dan zal de eindgebruiker een eenmalig wachtwoord met een SMS ontvangen terwijl hij of zij niks heeft aangevraagd.

### Nadelen

* Het verzenden van een SMS is niet gratis. Dus op de lange termijn kan een sms-oplossing duurder zijn dan een andere vorm van 2FA.
* Om SMS te ontvangen is er een mobiele telefoon nodig en verbinding met het netwerk. SMS kan niet worden gebruikt in geval van afwezigheid van de mobiele dekking. Daarnaast is er ook een afhankelijkheid van de telefoon die leeg kan zijn, of gestolen. Het kan dus nodig zijn om een alternatief ernaast te zetten (controlevragen)
* Er is tegenwoordig een aanval techniek die SIM-Swap heet, aanvallers kunnen het telefoonnummer stelen.
* Sms-berichten kunnen op verschillende manieren worden onderschept, tijdens transmissie, op de telefoon in het geheugen en als ze opgeslagen zijn.

## Apps

Code generatie apps zijn een steeds meer gebruikt alternatief voor sms-codes. De meest gebruikte van dergelijke toepassingen is de authenticatie-oplossing van Google - Google Authenticator. Dergelijke software genereerd dus eenmalige wachtwoorden op basis van een bepaald algoritme, een pincode of op tijd gebaseerde willekeurige volgorde. Er zijn verschillende algoritmen en de belangrijkste algoritmen voor het genereren van dergelijke eenmalige codes zijn:

* HOTP (op hash gebaseerd eenmalig wachtwoord);
* TOTP (op tijd gebaseerd eenmalig wachtwoord);
* OCRA (OATH challenge-response-algoritme).

Voorbeelden van TOTP waar leveranciers een app voor ontwikkeld hebben zijn bijvoorbeeld: Google Authenticator, Free-OTP app en MS Authenticator. Een voorbeeld van een app met HOTP, waarbij je dus een pincode invoert om toegang te krijgen tot een profiel in de app, om daarna met de app de OTP-code kunt genereren is Mobilepass. Ook wachtwoord kluizen bevatten Authenticator functionaliteit, zie hiervoor de handreiking wachtwoordkluizen van de IBD.

### Voordelen

* Het belangrijkste voordeel van dergelijke 2FA-software is de mogelijkheid om te gebruiken zonder de mobiele dekking of de toegang tot internet. Het werkt dus zolang de telefoon werkt.
* In een app kunnen meerdere tokens zitten, er zijn geen losse hardware tokens nodig
* Er zijn meerdere apps die hetzelfde werken en de meeste toepassingen gebruiken hetzelfde algoritme, er is keuze genoeg.

### Nadelen

* Noodzaak om een smartphone of ander soortgelijk apparaat te gebruiken;
* De applicatie kan worden gehackt;
* Smartphone-batterij kan leeg zijn;
* Als de smartphone wordt teruggezet naar de fabrieksinstellingen of verloren gaat, of er een nieuwe telefoon wordt gekocht, of als de authenticatietoepassing per ongeluk wordt verwijderd, gaat het token dat de app nodig heeft verloren en is het herstel ervan lastig.
* Er kan weerstand zijn bij medewerkers die een BYOD-device hebben om daar software voor de gemeente op te installeren. Aan de andere kant bestaat de kans dat eindgebruikers zelf al een 2FA app hebben draaien.

## Tokens

De volgende in de rij zijn de contactloze hardware tokens. Deze tokens worden beschouwd als erg veilige tweede factor:

* Het zijn op zichzelf staande, niet-koppelbare apparaten, het is niet mogelijk om van buiten toegang te krijgen;
* De SIM kaart kan niet gestolen worden, want die zit er niet in;
* De gegevens van de code generator zijn ongevoelig voor een aanval waarbij een aanvaller de codes onderschept in het geheugen van de telefoon of computer (man-in-the-middle (MITM)-aanval)).
* De batterijen van de tokens gaan jarenlang mee, meestal langer dan de levensduur van de codegenerator.
* Ze hebben geen mobiel netwerksignaal of roaming nodig om te werken zoals bij SMS.

Er zijn momenteel 2 soorten contactloze hardware tokens op de markt:

### Contactloze tokens

Deze eenmalige wachtwoord tokens (OTP-tokens) worden vrij veel gebruikt, wie kent deze niet, het zijn tokens met een klein beeldschermpje waar om de bepaalde tijd een nieuwe code zichtbaar is. Deze tokens worden al jaren beschouwd als de meest betrouwbare tokens voor het genereren van wachtwoorden. Er zijn twee varianten van: één met voorgeïnstalleerde sleutels (seeds) en één variant met zelf te installeren sleutels (flashen)

### Voordelen

* Contactloos apparaat, beschermd tegen elke mogelijkheid van malware-injectie;
* Eenmalig wachtwoord wordt gegenereerd door het apparaat zelf, waardoor de kans op onderschepping tot een minimum wordt beperkt;
* Vereist geen enkele netwerkverbinding;
* Ingebouwde stroombron is voldoende voor jarenlang onafhankelijk gebruik, bij normaal gebruik gaan deze wel 5 jaar mee;
* De goedkoopste van alle hardwaretokens;
* De zelf flashbare tokens kunnen worden hergebruikt.

### Nadelen

* Als een token is gecompromitteerd, hoeft u alleen een nieuwe te bestellen/verstrekken en er zijn ook zelf flashbare tokens met een secret/seed;
* Tokens kosten geld, en zijn duurder dan de software apps en vereisen meer beheer.
* Bij meerdere bronnen/ organisaties leidt deze oplossing tot meerdere tokens, in tegenstelling tot een app, waar heel veel tokens in kunnen draaien. Dus de eindgebruiker krijgt ook steeds meer fysieke tokens om mee te dragen.
* De geheime sleutel in de voorgeïnstalleerde tokens wordt in de fabriek voorgeladen, vervolgens doorgegeven aan de leverancier en vervolgens overgedragen aan de eindklant. Er zijn de nodige waarborgen en maatregelen, echter er zijn dus partijen die de voorgeïnstalleerde geheimen kunnen kennen. Er blijft een kleine kans bestaan dat op een bepaald moment een gewetenloze werknemer of een hacker geheime sleutels zal lekken. Een zelf flashbaar token heeft dit nadeel niet, daar bent u zelf verantwoordelijk voor de geheimen.

### Connected tokens (U2F)

U2F is een open standaard voor universele 2FA, ontwikkeld door de FIDO Alliance. De laatste versie van de standaard heet FIDO2. Authenticatie via dit protocol wordt uitgevoerd met behulp van een hardware module, in de rol waarvan een fysiek medium - USB-tokens wordt gebruikt. Deze tokens zijn in de productiefase uitgerust met speciale software en een digitale sleutel. De USB-stick wordt eenvoudig in de bijbehorende desktop- of laptopconnector gestoken. Deze authenticatiefactor werkt als volgt:

De gebruiker logt in op een (web) toepassing door middel van een gebruikersnaam en wachtwoord.

De server controleert de referenties en, als ze correct zijn, vraagt hij de handtekening (genereert een uitdaging/challenge) voor het token en stuurt dit terug naar het gebruikersprogramma, in dit geval de website waarop men wil inloggen. De browser verzendt deze challenge naar het U2F token waarbij de gebruiker bijvoorbeeld een druk op een knop op het token een eenmalig wachtwoord teruggeeft dat wordt gegenereerd op basis van het algoritme in de token. De webserver verzendt het antwoord naar de server. Klopt dit antwoord dan wordt de gebruiker geauthentiseerd. Varianten: Sommige U2F tokens werken met een vingerafdruk of een pin. Er zijn tegenwoordig ook U2F tokens die werken met NFC (Android) of Bluetooth (iOS).

### Voordelen

* Er is geen verbinding met Internet nodig, omdat alle benodigde gegevens al op het U2F token zijn opgeslagen.
* Een U2F token is ongelimiteerd te gebruiken in veel applicaties, mits deze het U2F FIDO-protocol ondersteunen.
* Gebruiksgemak - sluit het token gewoon aan op de USB-poort en druk op de knop wanneer daarom wordt gevraagd.
* Er zijn U2F tokenmodellen met twee soorten aansluitingen, zodat een USB-C en Lightning connector apparaten gebruikt kunnen worden

### Nadelen

* U2F is vrij nieuw en wordt al wel ondersteund door steeds meer partijen zoals Gmail, Google-accounts, GitHub, Dropbox en sommige wachtwoordkluizen, waardoor er ook hier een extra beveiligingslaag kan worden toegevoegd tot de toegang tot de wachtwoordkluis;
* U2F tokens worden nog niet door alle browsers en browser versies ondersteund, zoek dus uit wat mogelijk is;
* Aangezien U2F tokens veelal in een USB-poort zitten mogen deze niet geblokkeerd zijn.
* U2F-tokens zijn nog relatief duur;
* U2F tokens zijn erg klein en moeten wel worden meegedragen en kunnen dus ook verloren worden, zorg dan voor een back-up die ook geregistreerd wordt[[3]](#footnote-3);
* Eindgebruikers laten het token in de computer zitten wat het hele concept van 2FA ondermijnt, zeker als men ook nog het wachtwoord kent. Dit nadeel geldt niet voor tokens met vingerafdruk.
* Het is niet direct een nadeel, maar bedenk hoe men wil omgaan met medewerkers die een U2F token ook privé gebruiken en de organisatie verlaten.

# Tips voor gemeenten

Als u als gemeente nog niet bent begonnen met 2FA, begin dan klein, bijvoorbeeld eerst met de beheerders toegang naar de gemeente. Klein beginnen heeft ook als voordeel dat de eigen beheerders zich de technologie eigen maken. Bedenk wel van tevoren welke technologie gebruikt gaat worden, er is meer info te vinden op Internet dan dat wij in dit document kunnen meenemen[[4]](#footnote-4).

Rol vervolgens 2FA uit naar alle gebruikers die vanaf buiten de gemeenten willen werken op gemeentelijke systemen.

Daarna is het zeker het overwegen waard om 2FA uit te rollen voor alle gebruikers in alle situaties.

Het stappenplan staat in de volgende paragraaf.

# Stappenplan

De gemeente die aan de slag wil met het invoeren van 2FA moet hier van tevoren goed over nadenken, 2FA is belangrijk als middel tegen het misbruiken van buitgemaakte wachtwoorden en misbruik maken van wachtwoorden. Daarnaast biedt 2FA een extra bescherming als medewerkers vanuit huis met gemeentelijke systemen moeten werken, het is niet voor niets een BIO-maatregel die minimaal van toepassing is als men vanuit een onvertrouwde omgeving een netwerkverbinding wil maken met het vertrouwde gemeentelijke netwerk. Het brengt een extra beveiligingslaag aan waardoor misbruik van gemeentelijke systeem kan worden voorkomen.

Een voorbeeld stappenplan:

Voordat u begint:

Het is belangrijk om van tevoren na te denken waar u 2FA voor wilt inzetten, er zijn vele opties om te overwegen van bijvoorbeeld het inzetten van 2FA voor alles en iedereen tot en met het gericht en risico gebaseerd inzetten van 2FA. Bijvoorbeeld op basis van gevoeligheid van systemen, het verwerken van persoonsgegevens of bijzondere persoonsgegevens of geheime informatie (dataclassificatie kan daarbij helpen) en de locatie waarvan gewerkt wordt en de locatie waar de systemen draaien. Vergeet ook niet dat veel legacy systemen van de gemeente waarschijnlijk helemaal niet om kunnen gaan met 2FA. Het is ook mogelijk om de toegang tot interne systemen middels een virtualisatie oplossing een extra bescherming te geven door middel van 2FA, vaak hoeft dat alleen nog maar geactiveerd te worden. Begin met een overzichtplaat van de architectuur van de gemeentelijke systemen, waar ze draaien, van waar toegang verleend moet worden en welke extra bescherming mogelijk nodig is. Hier is gezien de diversiteit van de gemeentelijke ICT-infrastructuur en applicaties geen pasklaar antwoord op te geven.

De gemeente die Cloudvoorzieningen gebruiken of een SaaS toepassing doet er ook goed aan om bij de leverancier in informeren of 2FA aangezet kan worden. Veel leveranciers zouden dit moeten kunnen ondersteunen/beschikbaar hebben. Het is goed mogelijk dat 2FA zonder veel inspanning aangezet kan worden, maar let wel op: technisch kan veel, verlies niet de eindgebruiker uit het oog.

Zorg er in ieder geval voor om de beleidskeuzes voor 2FA op te nemen in het beleid voor logische toegangsbeveiliging van de gemeente. Heb hierbij ook aandacht voor de volgende onderwerpen:

* Registratie/ beheer van tokens
* Hoe gaan tokens worden uitgegeven en ingenomen, registratie van gebruikers en of men zich ook moet identificeren/legitimeren voor uitgifte.
* Vereisen dat er een meldproces is voor verlies of diefstal van tokens
* Een back-up proces, hoe om te gaan met medewerkers die wel toegang nodig hebben maar hun token of iets van dien aard vergeten zijn.

**Stap 1: maak een Business case, goed voorbereiden is het halve werk!**

In de business case moet verder aandacht zijn voor de volgende onderwerpen:

* Kosten voor:
  + Het maken van beleid voor 2FA;
  + Kosten van de oplossing die gewenst is;
  + Projectkosten;
  + Kosten van het beheer en onderhoud;
  + Implementatiekosten zoals opleidingen/ handleidingen en communicatie;
* Opbrengsten zoals:
  + Verbeterde bedrijfsvoering en meer veiligheid (minder risico);
  + Minder helpdesk verzoeken voor wachtwoord resets;
  + Minder incidenten die voor verstoringen zorgen, zoals;
    - Minder kans op een ransomware uitbraak
    - Minder kans op datalekken
    - Minder kans op oneigenlijk gebruik van (beheerders) accounts door kwaadwillenden of fraude
* De keuze: koop of huur of bouw?
* Welke oplossingsrichting?
* Wie gaat het project uitvoeren?
* Wie gaat het in beheer nemen?
* Wie is de opdrachtgever en -nemer en beoogd projectleider

**Stap 2: Maak een projectplan**

Als er goed nagedacht is over het wat, het waar, het waarmee en de kosten en opbrengsten is het tijd om een gedegen plan te maken. Het invoeren van 2FA heeft veel techniek in zich en het risico bestaat dat het als een IT-project wordt aangevlogen terwijl dat maar een deel van de lading dekt. De oplossing moet ook gebruikt gaat worden en daar moeten medewerkers op worden voorbereid.

Het plan moet bevatten:

* Scope: waar gaat de gemeente 2FA inzetten, in termen van processen, systemen en applicaties.
* Op te leveren producten:
  + Authenticatie beleid (waar ook 2FA in benoemd is)
  + Architectuur aanpassen/ maken
  + Programma van eisen voor het product of dienst (inclusief beveiligingseisen)
  + Ingevoerde 2FA
* Projectplanning (strokenplanning, fasering)
* Resources/ mensen (projectleider, een architect een oplossingsspecialist, beheerders etc.)
* Risico’s (project risico’s)
* Budget (staat als het goed is in de business case)
* Kritieke succesfactoren
* Randvoorwaarden
* Testen
* Communicatie

**Stap 3: het project uitvoeren**

* Zorg dat de mensen er zijn die het project uitvoeren
* Voer het project uit zoals gepland.
* Schaf de producten of diensten aan
* Voer de implementatie en communicatie uit
* Test de oplossing
* Voer een pilot uit (begin klein en breid later uit)
* Communiceer
* Uitrollen

**Stap 4: in beheer nemen, project afsluiten**

Aan ieder project komt een eind, zorg ervoor dat de beheerfase kan starten en de oplossing in beheer genomen is.



Nassaulaan 12

2514 JS Den Haag

CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)

CERT 24x7: Piketnummer (instructies via voicemail)

[info@IBDGemeenten.nl](mailto:info@IBDGemeenten.nl) / [incident@IBDGemeenten.nl](mailto:incident@IBDGemeenten.nl)

Kijk voor meer informatie op:

www.informatiebeveiligingsdienst.nl

1. Zie ook de handreiking “beleid logische toegangsbeveiliging” van de IBD.” [↑](#footnote-ref-1)
2. <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wat-verstaat-de-avg-onder-bijzondere-persoonsgegevens-6339> [↑](#footnote-ref-2)
3. De back-up is een tweede sleutel die bij dezelfde dienst is geregistreerd en op een veilige plaats (kluis) wordt bewaard. In geval de eerste sleutel verloren gaat kan de back-up sleutel worden gebruikt om alsnog toegang te krijgen. [↑](#footnote-ref-3)
4. <https://veiliginternetten.nl/themes/situatie/wat-tweestapsverificatie/> [↑](#footnote-ref-4)