

Handreiking

Wachtwoordkluizen

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

Colofon

**Naam document**

Handreiking Wachtwoordkluizen

**Versienummer**

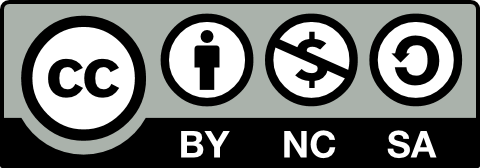
1.0.1

**Versiedatum**

Mei 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 | Februari 2020 | Eerste uitgave |
| 1.0.1 | Mei 2020 | Tekstuele verbeteringen |

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 9.3.1.1 een wachtwoordenkluis 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
* Logisch toegangsbeleid
* Wachtwoordbeleid

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

9.3.1.1 Wachtwoordkluizen en control

9.4.3 Systeem voor wachtwoordbeheer

Inhoudsopgave

[1. Inleiding 6](#_Toc31953678)

[1.1. BIO Eisen 6](#_Toc31953679)

[1.2. Het belang van het beheersen van wachtwoorden 7](#_Toc31953680)

[2. Wachtwoordkluizen 8](#_Toc31953681)

[2.1. Waarom wachtwoordkluizen 8](#_Toc31953682)

[2.2. Wat zijn wachtwoordkluizen 9](#_Toc31953683)

[3. Vormen van wachtwoordkluizen 11](#_Toc31953684)

[3.1. Stand-alone (unmanaged) 11](#_Toc31953685)

[3.2. Centraal beheerd (managed) 11](#_Toc31953686)

[3.3. PAM 12](#_Toc31953687)

[4. Risico’s van wachtwoordkluizen 14](#_Toc31953688)

[4.1. Verliezen van het hoofd wachtwoord (master password) 14](#_Toc31953689)

[4.2. Aanvallen op de wachtwoordkluis 14](#_Toc31953690)

[4.3. Het kiezen van een zwak of eerder gebruikt hoofd wachtwoord 14](#_Toc31953691)

[5. Eisen aan wachtwoordkluizen 15](#_Toc31953692)

[5.1. Hoe verder 16](#_Toc31953693)

[BIJLAGE 1 Voorbeeld wachtwoordkluisbeleid 18](#_Toc31953694)

# Inleiding

In de BIO worden wachtwoordeisen benoemd die het nodig maken dat de organisatie - in aanvulling op het algehele beveiligingsbeleid - nadere regels stelt over wachtwoordbeleid en ondersteunende processen in wachtwoord beleid. Dit document geeft algemene aanwijzingen over het omgaan met wachtwoordenkluizen in relatie tot het wachtwoordbeleid en de maatregelen in de BIO.

## BIO Eisen

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

|  |  |  |  |
| --- | --- | --- | --- |
| **9.3.1** | **1** | **Geheime authenticatie-informatie gebruiken**  Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie. | Secretaris/algemeen directeur  Dienstenleverancier |
| 9.3.1.1 | 2 | Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis. |

Hier wordt gesproken over een wachtwoordenkluis, een wachtwoordenkluis is een applicatie om wachtwoorden op te slaan waar ook ander functionaliteit geboden kan worden, zoals het genereren van sterke wachtwoorden of het delen van wachtwoorden of het controleren van wachtwoorden.

Vervolgens is er nog een eis over wachtwoordbeheer bij 9.4.3.

|  |  |  |  |
| --- | --- | --- | --- |
| **9.4.3** | **1** | **Systeem voor wachtwoordbeheer**  Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen. | Dienstenleverancier |
| 9.4.3.1 | 1 | Als er geen gebruik wordt gemaakt van two-factor authenticatie is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd. |
| 9.4.3.2 | 2 | In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.). |
| 9.4.3.3 | 2 | Het wachtwoordbeleid wordt geautomatiseerd afgedwongen. |
| 9.4.3.4 | 2 | Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd. |
| 9.4.3.5 | 2 | Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden. |

Hier wordt gesproken over het systeem voor wachtwoord beheer, dit slaat op het beheersen van wachtwoorden in toepassingen of de centrale gebruikers database (LDAP/Active directory). Wachtwoordkluizen helpen met name ook bij het ondersteunen bij maatregelen 9.4.3.1 en 9.4.3.2.   
Meer informatie over wachtwoordbeheer is te vinden in de "[Handreiking wachtwoordbeleid BIO](https://www.informatiebeveiligingsdienst.nl/product/wachtwoordbeleid-2/)"

## Het belang van het beheersen van wachtwoorden

Wachtwoorden vormen een belangrijk aspect van de gemeentelijke informatiebeveiliging. Goede wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatie. Een gemakkelijk wachtwoord evenals onduidelijke of niet gevolgde wachtwoord procedures zijn niet alleen een bedreiging voor de vertrouwelijkheid en integriteit van gemeentelijke informatie, maar uiteindelijk ook slecht voor het imago van de gemeente. Alle gebruikers van gemeentelijke informatiesystemen dienen goede wachtwoorden te kiezen en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en login-gegevens.

Gemeentelijke ICT-gebruikers hebben voor steeds meer diensten verschillende wachtwoorden nodig en deze moeten ook nog onthouden worden. Een gevolg daarvan is dat wachtwoorden worden opgeschreven op opgeslagen op onveilige plaatsen. Of de medewerkers kiezen een wachtwoord dat steeds lijkt op het vorige wachtwoord en of een bepaald patroon, omdat het anders moeilijk wordt om wachtwoorden te onthouden.

# Wachtwoordkluizen

## Waarom wachtwoordkluizen

Wat zijn de redenen om voor een wachtwoordkluis te kiezen (naast dat het een verplichte BIO-maatregel is):

**Sterkte van wachtwoorden**

Wachtwoordkluizen zorgen ervoor dat men hele sterke wachtwoorden kan maken en onthouden. Een wachtwoordkluis kan eenvoudig op basis van regels unieke sterke wachtwoorden genereren per account of dienst, hierdoor worden wachtwoorden moeilijker om te raden maar ook moeilijker om te onthouden zonder deze wachtwoordkluis[[1]](#footnote-1).

**Het stelen van wachtwoorden**

Wachtwoorden kunnen worden gestolen, zeker bij externe websites gebeurt dit met regelmaat waarna de gebruikers gegevens en wachtwoord hashes en soms wachtwoorden gepubliceerd worden. Als een website het niet zo nauw neemt met beveiliging, en de gebruiker voor meerdere diensten hetzelfde wachtwoord gebruikt in combinatie met hetzelfde e-mailadres, wordt het eenvoudig om misbruik te maken van de digitale identiteit. Er is een website waar men kan controleren of het eigen e-mailadres al bij een bekende inbraak is buitgemaakt, ga hiervoor naar HaveIBeenPwned.[[2]](#footnote-2) Er zijn ook wachtwoordkluizen die gebruik maken van deze HaveIBeenPwned service.

**Wat doen externe websites niet goed:**

* Wachtwoordbestanden worden niet goed beschermd en websites bevatten zwakheden waardoor men bij gebruikers gegevens kan komen.
* Wachtwoorden worden zelf niet afdoende beveiligd door het nalaten van het versleutelen van wachtwoorden door niet "hashen en zouten"[[3]](#footnote-3).

**Het stelen van wachtwoorden voor speciale accounts (bijvoorbeeld beheerders).**

Cybercriminelen proberen bij een computerinbraak wachtwoorden te achterhalen van gebruikers met speciale rechten (beheerders) om zich zo verder toegang te verschaffen tot systemen en informatie van de gemeente. Als dit lukt kunnen cybercriminelen zichzelf ook toevoegen aan de groep "speciale gebruikers", of een willekeurige andere groep De aanvalsvectoren voor beheerders accounts zijn (niet-limitatief):

* Gedeelde accounts tussen IT-beheerders (meerdere beheerders gebruiken dezelfde gedeelde systeemwachtwoorden voor beheertaken) (Er zijn gemeenten die beheerstaken uitsluitend na 2FA laten uitvoeren).
* Serviceaccounts die nooit wijzigen (dus wachtwoorden die gebruikt worden voor systeem tot systeem connecties).
* Phishing bij gebruikers met verhoogde rechten om op die manier toegang te krijgen tot beheer rechten
* Het achterhalen van wachtwoordbestanden en hieruit wachtwoorden bemachtigen.
* Oud-medewerkers en beheerders die nog geldige wachtwoorden kennen. Wachtwoord procedures worden niet gevolgd.
* Standaard wachtwoorden gebruiken, er zijn systemen die ingebakken standaard wachtwoorden hebben die overal bekend zijn, en niet worden aangepast. (Dit is ook een signaal dat hardening beleid niet goed werkt)

Er zijn speciale wachtwoordenkluizen waarmee het mogelijk is om wachtwoorden voor beheerders veilig te beheren en gebruiken zodat er minder kans is dat onbevoegden hier gebruik van maken.

**De hoeveelheid wachtwoorden**

Het andere probleem is het grote aantal wachtwoorden dat gebruikers moeten onthouden. De gemiddelde Nederlander heeft al gauw tientallen tot honderden online login gegevens voor bankrekeningen, sociale media-accounts, onze e-mail en hulpprogramma's, vele andere onlinediensten en daarnaast niet te vergeten zakelijke toegang tot applicaties. Het lijkt makkelijk om dan één wachtwoord te gebruiken en dit gebeurt in de praktijk dan ook. Dit maakt 'credential stuffing' eenvoudiger[[4]](#footnote-4). Een ander probleem hierbij is dat men vaak maar één e-mailadres als gebruikersnaam gebruikt. Een wachtwoordkluis lost het gebruik van maar één zakelijk e-mailadres natuurlijk niet op. Het gebruik van een wachtwoordbeheerder maakt het zoveel gemakkelijker om sterkere wachtwoorden te genereren en op te slaan die uniek zijn voor elke site of dienst, waardoor aanvallen met inloggegevens kunnen worden voorkomen.

En een ander voordeel is dat een wachtwoordbeheerder je kan helpen als je je op een (publieke)drukke plek bevindt - zoals een koffiebar of een vliegtuig. Er zijn dan heel veel mensen om je heen die het invoeren van wachtwoorden kunnenzien, kopiëren en later het wachtwoord gebruiken. Door een wachtwoordbeheerder te gebruiken, die het wachtwoord voor u invoert, , hoeft u helemaal geen wachtwoorden in te typen.

Er zijn ook eindgebruikers die een privé wachtwoord gebruiken binnen de organisatie, als de identiteit eenmaal achterhaald is kan men eenvoudig voor varianties in mogelijk privé e-mailadressen aan te brengen bij andere diensten inloggen. Omgekeerd kan een buitgemaakt privé wachtwoord dan ook gebruikt worden bij de gemeente om in te loggen.

## Wat zijn wachtwoordkluizen

Zie een wachtwoordkluis als een applicatie met een verzameling van alle opgeslagen accountgegevens, dus gebruikersnaam en wachtwoord en wat verder relevant is. Deze kluis is beveiligd met een wachtwoord die doorgaans alleen bij de eigenaar van de kluis bekend is.

Dat wachtwoord voor toegang klinkt als een slecht idee, want er is maar één wachtwoord nodig om bij alle andere wachtwoorden te komen. Dit betekent dan ook dat voor de wachtwoordkluis een uniek en sterk en wachtwoord gekozen moet worden dat onthoudbaar is. Dit wachtwoord zorgt ook voor versleuteling van de inhoud van de wachtwoordkluis.

Wachtwoordkluizen slaan niet alleen wachtwoorden op, ze helpen ook bij het genereren en bewaren van sterke, unieke wachtwoorden of wachtwoordzinnen wanneer men zich aanmeldt bij nieuwe websites. Dat betekent dat wanneer de gebruiker van een wachtwoordkluis naar een website of app gaat, hij/zij de wachtwoordkluis kan openen, het wachtwoord kan kopiëren, het in het aanmeldvak kunt plakken om dit wachtwoord vervolgens te gebruiken. Tegenwoordig kan men al een soort van wachtwoordkluis hebben zonder dat men daarbij stilstaat omdat browsers als Chrome, Firefox en Internet Explorer een wachtwoord bewaarfunctie hebben die wachtwoorden automatisch invullen.

Het bovenstaande lijkt dan wel weer iets tegenstrijdigs te hebben, met een wachtwoordkluis is er maar één plek waar alles te halen is. Echter het hergebruiken van wachtwoorden en het gebruiken van slechte wachtwoorden is vele malen slechter. Het onthouden van vele goede wachtwoorden is daarnaast gewoon niet te doen.

# Vormen van wachtwoordkluizen

Er zijn vele soorten wachtwoordkluizen en sommigen zijn ook al ongemerkt binnen de gemeente aanwezig. In deze paragraaf komen de verschillende soorten wachtwoordkluizen aan bod. De eenvoudigste vorm zit in sommige browsers als functionaliteit om gebruikersnamen en wachtwoorden versleuteld op te slaan. Als de browser opnieuw wordt geïnstalleerd en er geen Cloud opslag is, dan is men deze wachtwoorden doorgaans gewoon kwijt. Daarnaast zijn er aparte wachtwoordkluizen waarin door gebruikers namen en wachtwoorden en andere soorten informatie versleuteld kunnen worden opgeslagen. Als laatste categorie worden wachtwoordkluizen behandeld die organisatie breed ingezet kunnen worden en als wachtwoordkluizen voor het beheersen van beheerder en systeemwachtwoorden.

## Stand-alone (unmanaged)

Standalone wachtwoordkluizen zijn wachtwoordkluizen die als applicatie gebruikt kunnen worden. Net als iedere andere applicatie zijn deze wachtwoordkluizen als toegestane applicatie ter beschikking te stellen aan gemeentelijke medewerkers. Deze wachtwoordkluizen zijn er vaak ook nog voor verschillende besturingssystemen geschikt zodat er een mogelijkheid ontstaat om op meerdere plaatsen dezelfde wachtwoordkluis en gegevens te gebruiken, mits er een vorm van delen van wachtwoorden kan worden ingesteld. Wachtwoordkluizen zijn er in gratis en betaalde varianten.

Daarnaast hebben de meeste webbrowsers ook een vorm van wachtwoordkluis functionaliteit waarbij dan de login gegevens van websites en webapplicaties kunnen worden onthouden. Deze wachtwoordkluizen kunnen wachtwoorden lokaal en versleuteld op de werkplek opslaan, nadeel hiervan kan zijn dat men bij een browser wissel of herinstallatie de wachtwoorden wel kwijt is. Als er geen schermvergrendeling gebruikt wordt, zullen deze opgeslagen wachtwoorden voor iedereen beschikbaar zijn op de werkplek waar men het wachtwoord in de browser heeft opgeslagen. Daarnaast is de beveiliging van deze wachtwoorden niet voldoende. Browserkluizen worden afgeraden.

## Centraal beheerd (managed)

Centraal beheerde wachtwoordkluizen kunnen een uitbreiding zijn op een standalone variant van een wachtwoordkluis. Er zijn ook centraal beheerde wachtwoordkluizen zonder standalone variant. Dit zijn aparte producten die geschikt zijn om gemeentebreed uit te rollen en waarbij de wachtwoordkluizen centraal beheerd kunnen worden. Deze wachtwoordkluizen maken gebruik van toegangscontrole en encryptie en kunnen worden gebruikt om login informatie, wachtwoorden, sleutels, eenmalige wachtwoorden generatie te beschermen en te gebruiken voor toegang tot gemeentelijke systemen. Deze wachtwoordkluizen kunnen binnen de gemeente draaien maar ook in de (gemeentelijke) Cloud. Aan centraal beheerde wachtwoordkluizen zitten naast softwarekosten ook beheerkosten.

Voor en nadelen standalone en centraal beheerd.

|  |  |  |
| --- | --- | --- |
|  | Standalone | Beheerd/centraal |
| Voordelen | * Snel in te zetten * Lage kosten voor de wachtwoordkluis zelf * Weinig beheer nodig * Minder calls voor vergeten wachtwoorden * Wachtwoorden worden niet meer zomaar ergens opgeschreven * Wachtwoord generator helpt bij sterkere wachtwoorden | * Audit proof * Draagt bij aan andere eisen zoals certificering / compliance * Koppeling met AD, Radius, LDAP mogelijk * Integratie met IAM-oplossingen * Wachtwoord controle/regels makkelijker centraal af te dwingen * Geen/minder calls voor vergeten wachtwoorden * Wachtwoord generator helpt bij sterkere wachtwoorden * Toegang met 2FA mogelijk * Meer backup mogelijkheden * Ook andere functionaliteit mogelijk |
| Nadelen | * Minder goed of geen centraal beheer mogelijk * Opslag van de wachtwoordkluis kan minder goed bewaakt worden (dus waar staat het) * Hogere beheerkosten omdat iedereen zelf wachtwoordkluizen en mogelijk problemen heeft * Single point of failure * Browserkluizen zijn vaak onveilig. | * Moeilijk uit te rollen, dit is een serieus project * Kost meer beheer capaciteit voor de wachtwoordkluis toepassing * Hogere kosten voor implementatie |

## PAM

De BIO maakt geen onderscheid in wachtwoordkluizen en toch is dat onderscheid wel te maken. Zoals eerder beschreven bij "waarom wachtwoordkluizen" zijn beheerders rechten bijzonder interessant voor een aanvaller en bij veel APT[[5]](#footnote-5) zijn de beheerder accounts dan ook een gewild doel. Ook gemeenten zijn een doelwit van hackers en het verkrijgen van een beheerders account en wachtwoord is beter en makkelijker voor hackers dan jezelf naar binnen hacken. Bovendien valt het gebruik van een beheerders login account toch al niet op, omdat hier vaak niet op gemonitord wordt. Hier bestaan wel monitoring tools voor. Voor het beschermen van beheerders accounts en systeem accounts bestaan oplossingen die verder gaan dan een standaard wachtwoordkluis.

PAM staat voor Privileged Access (Account) Management (PAM). Met een PAM-oplossing is het mogelijk om beheerder en systeem wachtwoorden extra beveiliging mee te geven. De extra beveiligingsfunctionaliteiten die een PAM kan ondersteunen zijn:

* Multifactor authenticatie (MFA) voor beheerders.
* Een toegangsbeheerder waarmee autorisaties en beheerder informatie wordt bijgehouden.
* Een wachtwoordkluis voor het veilig opslaan van beheerders accounts, serviceaccounts en wachtwoorden.
* Het loggen van (beheerders) sessies nadat toegang is verleend doormiddel een beheerders account.
* Dynamische autorisaties: bijvoorbeeld alleen toegang verlenen gedurende bepaalde tijdstippen.
* Geautomatiseerd toevoegen en verwijderen van beheerders op basis van een IAM proces.
* Audit logging tooling zodat men compliance kan aantonen over alle beheeractiviteiten.

Er zijn daarnaast ook wachtwoordkluizen die sterk zijn in het beschermen van beheerdersaccounts, waarbij de systeemtoegang beschermd blijft en de logins die gebruikt zijn, zodanig worden gelogd dat achteraf een audit trail mogelijk is. PAM kan uit nog meer onderdelen bestaan volgens Gartner[[6]](#footnote-6):

* Shared Access Password Manager (SAPM) (gedeelde toegang)
* Superuser Password Manager (SUPM) (super user toegang)
* Privileged Session Manager (PSM) (Beveiligde sessie toegang)
* Application Access Password Manager (AAPM) (applicatie toegang)

SAPM levert een extra beschermingslaag voor administrators / beheerders en het volgen van de wachtwoord regels voor beheerders. SAPM monitort de toegang en levert een audittrail op die later weer geraadpleegd kan worden. Wachtwoorden kunnen zelfs eenmalig in gebruik zijn en de toegang wordt dan geregeld door sessie brokers (PSM). Met een PSM zien de beheerders zelf geen wachtwoorden meer. Met AAPM is het mogelijk om op sessie gebaseerde toegang tussen applicaties te leveren die alleen dan toegang levert wanneer het nodig is (dit moet dan wel eerst vastgesteld worden). Met PAM is het ook mogelijk om multifactor authenticatie te gebruiken.

# Risico’s van wachtwoordkluizen

Hoewel vaak gezegd wordt dat het hebben van een wachtwoordkluis beter is dan het niet hebben van een wachtwoordkluis zijn er ook risico’s verbonden aan het gebruik van een wachtwoordkluis. Deze risico’s zijn:

## Verliezen van het hoofd wachtwoord (master password)

Wachtwoordkluizen vragen bij het aanmaken van een kluis om het maken van een hoofdwachtwoord, dit hoofdwachtwoord geeft toegang tot de inhoud van de kluis. Het dient dus voldoende sterk te zijn en mag niet vergeten worden. Wordt het hoofdwachtwoord vergeten dan is het bij de meeste wachtwoordkluizen niet meer mogelijk om bij de inhoud van de kluis te komen, tenzij er een noodprocedure bestaat. Enkele wachtwoordkluizen hebben deze mogelijkheid, bij centraal beheerde wachtwoordkluizen is dit meestal een standaard functionaliteit. Het is belangrijk je te verdiepen in de mogelijkheid om bij verlies van een hoofdwachtwoord toegang te kunnen herstellen (recovery optie). Doe dit vooraf. Het bewaren van de recovery mogelijkheid zorgt dan wel weer voor meer risico dat die in verkeerde handen kan vallen. Er zijn ook wachtwoordkluizen die je de mogelijkheid bieden om een back-up te maken van de inhoud, echter dat introduceert weer nieuwe risico’s zoals het niet sterk genoeg versleutelen van die back-up en het vergeten van het gekozen back-up wachtwoord. Dit risico geldt sterker voor standalone wachtwoordkluizen dan voor beheerde/centrale wachtwoordkluizen.

## Aanvallen op de wachtwoordkluis

Een aanvaller kan proberen de wachtwoordkluis aan te vallen op het apparaat waarop het staat. Er zijn vele wachtwoordkluizen die op vele vormen van devices werken. Daarmee wordt de veiligheid van het host-systeem en de wachtwoordkluis belangrijk. Daarnaast wordt doorgaans een wachtwoordkluis een bepaalde tijd ontgrendeld door het hoofdwachtwoord in te voeren en in die tijd is het mogelijk om via het host-systeem bij de inhoud van de wachtwoordkluis te komen[[7]](#footnote-7). Zorg daarom voor een up-to-date host-systeem en wachtwoordkluis en kies de ontgrendelperiode niet te lang. Er kunnen ook aanvallen uitgevoerd worden op het geheugen van de host om daarin tijdelijk opgeslagen wachtwoorden te bemachtigen. Een andere mogelijkheid is het gebruiken van multifactor authenticatie of een FIDO2 hardware token.

## Het kiezen van een zwak of eerder gebruikt hoofd wachtwoord

Hergebruik van een makkelijk wachtwoord is nooit een goed idee en toch doen eindgebruikers dit omdat het onthouden van vele wachtwoorden praktisch onmogelijk (en onpraktisch) is. De kans bestaat dan ook dat bestaande wachtwoorden ooit ergens bij een digitale inbraak bekend geworden zijn. Aangezien het hoofdwachtwoord toegang geeft tot alle andere wachtwoorden moet hiervoor een uniek en sterk wachtwoord gekozen worden. Een maatregelen hiertegen is om een uniek en sterk hoofdwachtwoord te kiezen. Dit moet lang genoeg en ingewikkeld genoeg zijn om stand te houden tegen brute forcing. Oefen dit wachtwoord om het goed te leren onthouden.

# Eisen aan wachtwoordkluizen

Er zijn diverse eisen te stellen aan wachtwoordkluizen. Onderstaand is een lijst van functionele eigenschappen en niet-functionele eigenschappen die gehanteerd kan worden bij het zoeken naar een oplossing. Als de gemeente plannen heeft om naar een gemeentebreed beheerde oplossing over te gaan dan is het belangrijk om te kijken naar importmogelijkheden vanuit eenvoudigere wachtwoordkluizen. Functionele eigenschappen die aan wachtwoordkluizen te stellen zijn

|  |  |
| --- | --- |
| Nummer | Functionele eigenschap |
| 1 | Product ondersteunt de Nederlandse taal. |
| 2 | Multi-user/single user mogelijk (kunnen meerdere personen tegelijkertijd werken) (of is het juist een standalone oplossing) |
| 3 | Audit trail mogelijk (is het mogelijk acties te loggen die ook geschikt zijn om bijvoorbeeld beheerder activiteiten achteraf te auditen) |
| 4 | Wachtwoord delen mogelijk (soms is het delen van een wachtwoord wenselijk, ondersteunt de oplossing dit?) |
| 5 | Ingebouwde authenticator voor 2FA (zoals de authenticator app op de smartphone). |
| 6 | Ondersteunt BIO eisen (9.3.1; 9.4.1; 9.4.3.1). |
| 7 | Met 2 - factor authenticatie inloggen in wachtwoordkluis (TOTP)[[8]](#footnote-8), let wel op dat dan de periode van inactiviteit niet te kort gekozen wordt anders moeten medewerkers gedurende de dag meerdere keren inloggen, waardoor de wachtwoordkluis minder gebruikt zal worden. Overweeg een FIDO2 hardware sleutel[[9]](#footnote-9). |
| 8 | Browser-integratie, plug-ins voor meest gebruikte browsers beschikbaar. |
| 9 | Import / export mogelijk (i.v.m. migratie van/naar andere wachtwoordkluizen) |
| 10 | Bevat een wachtwoordgenerator, (kun je met het systeem sterke wachtwoorden en wachtwoordzinnen genereren). |
| 11 | Is het mogelijk om automatisch te checken of een wachtwoord al ergens anders voor gebruikt is (tegengaan hergebruik van wachtwoorden). |

Niet functionele eigenschappen die aan wachtwoordkluizen te stellen zijn

|  |  |
| --- | --- |
| Nummer | Niet functionele eigenschappen. |
| 1 | Open Source . |
| 2 | Cloud opslag (maakt de wachtwoordkluis al of niet gebruik van een Cloud opslag). |
| 3 | Lokale opslag mogelijk (dus ook centraal binnen de gemeente). |
| 4 | Multiplatform (Windows/Linux/Android/iOS). |
| 5 | Sterke opslag versleuteling. |
| 6 | Sterke transport versleuteling (SSL/TLS). |
| 7 | Lage latency (lage vertraging). |
| 8 | Groeimodel mogelijk van standalone naar enterprise/managed. |
| 9 | De wachtwoordkluis beschikt over een hoofdwachtwoord herstel functie. |

## Hoe verder

De verschillende mogelijkheden zijn dan te implementeren als standalone en centraal beheerd. Als gemeente is het meest eenvoudig om te starten met een standalone oplossing die dan wel centraal als applicatie gedistribueerd moet worden. Voorzien van een handleiding, bij voorkeur in de Nederlandse taal. Door op die manier een wachtwoordkluis aan te bieden kunnen alle gemeentelijke gebruikers in een eigen profiel hun wachtwoorden opslaan en gebruiken[[10]](#footnote-10). Volg onderstaand stappenplan om te komen tot het in gebruik nemen van een standalone oplossing:

* Onderzoek welke wachtwoordkluis het beste past bij de gemeentelijke situatie, maak hiervoor zelf een programma van eisen op basis van de eisen in dit document;
* maak beleid voor het gebruik van wachtwoordkluizen binnen de gemeente, zie bijlage met voorbeeld beleid;
* Maak een handleiding of gebruik de bijbehorende documentatie als die er is;
* communiceer hierover naar alle medewerkers;
* Distribueer de wachtwoordkluis software naar de gebruikers;
* Monitor het gebruik van de wachtwoordkluis.

De gemeente kan ook kiezen voor een centraal beheerde wachtwoordkluis, een zogenaamde managed oplossing. Deze wachtwoordkluizen bestaan dan uit een totaaloplossing waar niet alleen wachtwoorden mee beheerst kunnen worden maar ook voorzien in centrale opslag, beheer, delen van wachtwoorden en centraal afdwingen van wachtwoordregels. Daarnaast heeft een centraal beheerde oplossing doorgaans goede audit mogelijkheden. Het kan natuurlijk zijn dat de gemeente al een standalone oplossing heeft. In dat geval moet er een mogelijkheid zijn om vanuit de standalone oplossing te migreren door middel van export- en importmogelijkheden van wachtwoorden en andere informatie. Het bovenstaande stappenplan kan hiervoor ook gebruikt worden.

Centraal beheerde wachtwoord managers kosten doorgaans geld en de kosten zijn afhankelijk van het licentiemodel. Er zijn oplossingen die geld kosten per gebruiker of per administrator. Deze centraal beheerde oplossingen moeten wel voldoen aan meer eisen. Kies bij voorkeur een oplossing die in de eigen infrastructuur kan draaien maar ook voorbereid is op Cloud gebruik.

Het invoeren van een centrale passwordmanager moet niet onderschat worden. De directe kosten vormen maar een klein deel van de totale kosten en de tijd die aan het hele project besteed moet worden. Opbrengsten zijn er echter ook: sterkere wachtwoorden, verschillende wachtwoorden, op termijn minder calls bij vergeten wachtwoorden, nog maar één autorisatie standaard, voldoen aan normen op het vlak van autorisatiebeheer, kostenbesparing om er maar een paar te noemen. Door consequent gebruik te maken van de wachtwoordkluis kan de kans op incidenten (en dus ook de kans op imago schade, et cetera) afnemen terwijl de het niveau van beveiliging significant toeneemt.

### Aandachtspunten bij PAM

Er zijn aanvallen van kwaadwillenden waarbij steeds vaker beheeraccounts worden aangemaakt en misbruikt. PAM kan een prima middel zijn om je extra te beschermen tegen deze vorm van misbruik van beheer- en andere accounts. Dit vooral omdat met name beheer accounts een extra zwakheid in zich hebben (je kunt er nagenoeg alles mee). Zet stappen om met PAM verder te gaan als preventieve maatregel en monitoring maatregel. Maak een gedetailleerde functionele architectuur en ontwerp voor het inzetten van PAM en het koppelen van de PAM-oplossing met LDAP/AD, identiteit beheer, helpdesk, SIEM en andere tools. Het is raadzaam om de PAM-implementatie goed te plannen. Maak hiervoor gebruik van externe ondersteuning door de PAM leveranciers als er intern kennis ontbreekt. Communiceer goed met het management, de medewerkers en beheerders die dit mogelijk als extra last of controle zullen zien. Bouw voldoende tijd in voor integratie en testen.

BIJLAGE 1 Voorbeeld wachtwoordkluisbeleid

Beleidsuitgangspunten voor het gebruik van wachtwoordkluizen van gemeente <naam gemeente>

Ten behoeve van de beveiliging van informatie binnen gemeentelijke systemen is er beleid dat erop gericht is de omgang met wachtwoorden vast te leggen. Dit wachtwoordkluizen beleid is een aanvulling op het wachtwoordbeleid met dien verstande dat het specifiek over het gebruik van wachtwoordkluizen binnen de gemeente gaat.

Het doel van dit wachtwoordkluizenbeleid is tweeledig:

* Het vaststellen van regels waar wachtwoordkluizen aan moeten voldoen
* Het bevorderen van het gebruik van wachtwoordkluizen.

De gemeente <naam gemeente> hanteert onderstaande beleidsuitgangspunten, ontleend aan de Baseline Informatiebeveiliging Overheid (BIO).

Algemeen beleid

1. De gemeente zet wachtwoordkluizen in zodat eindgebruikers in staat worden gesteld om hun wachtwoorden op een veilige en verantwoorde manier te beheren[[11]](#footnote-11).
2. De wachtwoordkluizen zijn voor iedereen beschikbaar.
3. Aanvullende beleidsregels voor wachtwoordkluizen:

* Wachtwoordkluizen slaan wachtwoordbestanden op gemeentelijke systemen op.
* Wachtwoordkluizen worden gebruikt voor het genereren van wachtwoorden.
* Toegang tot wachtwoordkluizen is bij voorkeur met multifactor authenticatie.
* Wachtwoordkluizen ondersteunen het gemeentelijke wachtwoordbeleid.

1. Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende:

* Wachtwoorden worden uitsluitend opgeslagen in de wachtwoordkluis die de gemeente als applicatie aanbiedt;
* Gebruikers genereren sterke wachtwoorden door middel van de wachtwoordkluis;
* Het is niet toegestaan om wachtwoordkluis functionaliteit van webbrowsers te gebruiken;
* De wachtwoordkluis bestanden moeten worden opgeslagen op een veilige gemeentelijke share en niet in de Cloud;
* Gebruikers kiezen een sterk wachtwoord voor toegang tot de wachtwoordkluis en dit wachtwoord wordt niet gedeeld.

Aldus vastgesteld door burgemeester en wethouders van *[gemeente]* op *[datum],*

[Naam. Functie] [Naam. Functie]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



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 handreiking wachtwoordbeleid [↑](#footnote-ref-1)
2. <https://haveibeenpwned.com/> [↑](#footnote-ref-2)
3. een Zout of Salt is een willekeurig getal dat wordt toegevoegd aan een wachtwoord voordat de hash gemaakt wordt. Hierdoor is het niet mogelijk met de gevonden wachtwoord hash om doormiddel van een woordenboek aanval het wachtwoord uit te zoeken. [↑](#footnote-ref-3)
4. Dat is wanneer hackers uw wachtwoord van een gehackte site halen en proberen in te loggen op uw account op andere sites. [↑](#footnote-ref-4)
5. APT betekent Advanced Persistant Threat, zie: <https://nl.wikipedia.org/wiki/Advanced_Persistent_Threat> [↑](#footnote-ref-5)
6. https://www.gartner.com/reviews/market/privileged-access-management [↑](#footnote-ref-6)
7. Meer technische informatie over aanvallen op wachtwoordkluizen: https://crypto.stanford.edu/~dabo/pubs/papers/pwdmgrBrowser.pdf [↑](#footnote-ref-7)
8. Time-based One-Time Password algorithm [↑](#footnote-ref-8)
9. https://en.wikipedia.org/wiki/FIDO2\_Project [↑](#footnote-ref-9)
10. Zie hiervoor ook de aanpakken van gemeenten die op het besloten IBD forum staan (alleen voor gemeenten). [↑](#footnote-ref-10)
11. Het is aan de gemeente of wachtwoordkluizen alleen zakelijk of ook voor privé wachtwoorden gebruikt mogen worden, neem hier eventueel een regel voor op in dit beleid. [↑](#footnote-ref-11)