



Algemeen Verslag Marktconsultatie

Passwordmanager
Gemeente Eindhoven

Uitgave
Gemeente Eindhoven

Datum
8 juni 2023

Versie
Definitief

Inhoud

1. Inleiding	3
1.1. Algemeen	3
1.2. Openbaarheid van de marktconsultatie	3
1.3. Nota van Inlichtingen	3
2. Resultaten	4
2.1. Beantwoording vragen	4
2.1.1. Bedrijf	4
2.1.2. Oplossing	4
2.1.3. Implementatie	8
2.1.4. Kosten	8
2.1.5. Inkoopstrategie	9
2.1.6. Testperiode	10
3. Ten slotte	11
Bijlage 1 – Nota van Inlichtingen	12
Nota van Inlichtingen I	12

1. Inleiding

1.1. Algemeen

Dit is het markconsultatiedocument met betrekking tot een ICT-oplossing voor een Passwordmanager ten behoeve van de gemeente Eindhoven, hierna tevens te noemen Aanbestedende dienst of opdrachtgever.

1.2. Openbaarheid van de marktconsultatie

Middels dit document wilt de Aanbestedende dienst alle potentiële inschrijvers gelijk informeren door een overzicht te geven van de bevindingen die zijn opgedaan tijdens de uitvoering van de marktconsultatie Passwordmanager. De Aanbestedende dienst dient hierbij rekening te houden met het anoniem verwerken van de verstrekte informatie, op een wijze waarop niet te herleiden is van welke partij deze informatie afkomstig is. De informatie wordt gebruikt bij het verder specificeren van de mogelijk opdracht(en) en bij de keuze(s) van de aanbestedingsvorm(en) c.q. contractvormen.

1.3. Nota van Inlichtingen

De deelnemende partijen hebben de mogelijkheid gehad om vragen te stellen via de berichtenmodule van TenderNed. Van deze vragen met de bijbehorende antwoorden is een geanonimiseerde Nota van Inlichtingen gemaakt, deze is bijgevoegd als bijlage 1. In totaal hebben zes partijen deelgenomen aan de marktconsultatie.

2. Resultaten

2.1. Beantwoording vragen

Uit de marktconsultatie zijn de volgende resultaten naar voren gekomen.

2.1.1. Bedrijf

Algemeen: Geef aan wat algemene (contact)informatie van uw organisatie (naam contactpersoon, functie, telefoonnummer, e-mailadres, website etc.).

Alle partijen hebben algemene informatie toegevoegd. Dit is naar tevredenheid gedaan. Wegens het anonimiseren van de marktconsultatie, worden deze niet gedeeld.

Bedrijfskenmerken: Geef een korte beschrijving van uw organisatie (historie, aantal medewerkers, onderscheidend vermogen t.o.v. van andere partijen in de markt).

Alle partijen hebben een korte omschrijving van de organisatie toegevoegd. Dit is naar tevredenheid gedaan. Wegens het anonimiseren van de marktconsultatie, worden deze niet gedeeld.

2.1.2. Oplossing

Inloggen: Welke mogelijkheden biedt u om in het product in te loggen? (bijvoorbeeld username/wachtwoord, cloud-integratie, multi-factor, biometrisch, hardware, FIDO2).

Partijen geven o.a. het volgende aan:

- Multi-identity met een SSO-koppeling met de AAD-omgeving;
- Device autorisatie;
- Username/wachtwoord;
- Cloud-integratie;
- Multi-factor;
- Biometrisch;
- FIDO2;
- 2FA.

Beveiliging: Welke beveiligingsmaatregelen heeft u in uw oplossing ter bescherming van de (eind)gebruiker?

Onderstaande antwoorden zijn door partijen gedeeld:

- Sterk encryptie, zero trust door geen wachtwoorden op te slaan, reguliere testen en audits en een beveiligd management systeem.
- Er worden geen wachtwoorden, e-mailadressen of andere persoonlijke informatie opgeslagen. Gebruikers zijn dus anoniem. Er wordt berekend op de sterkst-mogelijke wachtwoorden, die lang, willekeurig en globaal uniek zijn. De wachtwoorden zijn ook phishing-resistent. Doordat wachtwoorden niet bewaard worden en de privacy wordt beschermd, beschikt de partij nooit over gevoelige informatie die op straat kan komen liggen.
- Een andere oplossing beschermt tegen online aanvallen door master passwords, 2FA, API-rate limiting en vault time-out opties. Bij offline aanvallen zijn zij beschermd door de master password van de gebruiker, meerdere versleutelingslagen, inclusief versleuteling op kolomniveau op gevoelige velden via sleutels op een HSM en transparante gegevensversleuteling voor de gehele database in rust.
- Een oplossing heeft alleen een username, display name en email-adres nodig. Verder slaat de partij ook geen persoonlijke data op. Alle data wordt opgeslagen in een database. Deze is niet direct toegankelijk. Technisch applicatiebeheer staat volledig los van het gebruik van de applicatie. Verder zorgt de decentrale denkwijze ervoor dat wanneer één account in verkeerde

handen komt, dit niet kan leiden tot toegang naar alle assets van een bedrijf. Alles gericht op zero-trust.

- Een andere partij adviseert altijd om twee factoren te gebruiken en oplossingen prefereren die gebruikersvriendelijk en veilig zijn. Vaak is dit een password sleutel met FIDO2 ondersteuning, maar een MFA token of biometrie is ook mogelijk.

Opslag: Op welke wijze borgt u de veilige opslag van wachtwoorden? (bijv ISO-certificering, encryptie)

Meerdere partijen geven aan ISO27001-gecertificeerd te zijn. Daarnaast wordt het volgende benoemd:

- Een partij geeft aan dat de oplossing gebruik maakt van encryption at-rest en in-transit. Een wachtwoord zal pas de-encrypted worden op het endpoint - bijvoorbeeld in de browser. De data at-rest gebruikt een multi-layer FIPS 140-2 compliant encryptie hiërarchie. Een AES-256 voor symmetrische encryptie en RSA-2048 voor asymmetrische encryptie. Naast TLS1.2 (minimum) wordt eveneens PGP gebruikt voor de end-to-end encryptie.
- Bij een partij is geen sprake van opslag van wachtwoorden omdat zij zonder kluis werkt. In plaats daarvan worden wachtwoorden berekend als een formule. Hierbij wordt gebruik gemaakt van hashing. Bij deze partij zijn dus zowel de data als de formule gedistribueerd.
- Een partij heeft naast de ISO 27001 certificering, ook een breed bereik tussen andere certificaten, zoals SOC 2, GDPR, CCPA, and HIPAA evenals testing, code testing en audits.
- Een partij geeft aan dat alle wachtwoorden die worden opgeslagen in de kluis worden versleuteld met het wachtwoord van de eigenaar. In het geval van de persoonlijke kluis is deze alleen toegankelijk voor de eigenaar. In het geval van een groepskluis is deze dus alleen toegankelijk voor de groepsleden. Er wordt uitgegaan van decentrale principes.
- Een partij geeft aan dat geen wachtwoorden en data wordt opgeslagen op de servers. Alle gebruikersgegevens worden versleuteld met de 256-bits AES-coderingsengine, SQLCipher.
- Aanbestedende dienst wordt geadviseerd om de kluis zelf te hosten.

Hosting: Indien het een SAAS-oplossing betreft, wordt deze in de EU gehost? Indien nee: waarom niet?

De partijen geven aan dat de oplossing in de EU of in de Verenigde Staten wordt gehost.

OS'en en browsers: Welke OS'en en browsers ondersteunt u en hoe ziet de ondersteuning eruit? (bijv. app, plug-ins)

Voor OS'en geldt:

- De oplossingen worden ondersteund in MacOS, Windows en Linux.
- Een aantal van de partijen geven aan dat iOS en Android de oplossing ondersteunt.

Voor browsers geldt:

- Alle oplossingen worden ondersteund in Chrome, Microsoft Edge en Mozilla Firefox.
- Brave wordt door de meeste oplossingen ondersteund.
- Safari wordt door de meeste oplossingen ondersteund. De overige partijen verwachten dit ook vanaf de zomer van 2023 te kunnen.
- Enkele andere browsers die worden benoemd: Vivaldi, Tor Browser en Opera.

Wachtwoorden: Hoe stimuleert u gebruik van veilige en unieke wachtwoorden?

Op deze vraag zijn de volgende antwoorden gegeven:

- Een partij berekent wachtwoorden op basis van een formule die gebaseerd is op meertraps hashen. Het gebruik van deze wachtwoorden wordt afgedwongen door een Adaptive Password Firewall.
- Een andere organisatie heeft een wachtwoordbeleid met minimale eisen waaraan het wachtwoord moet voldoen.
- Een partij geeft aan het gemak van een wachtwoordmanager aan medewerkers te laten inzien. Doelsystemen dwingen de wachtwoordregels af. Een wachtwoordmanager kan dit niet.

- Een andere partij lanceert binnenkort een dashboard waarbij het mogelijk zal zijn om password-reuse te rapporteren en aan te moedigen om te veranderen. In de tweede helft van dit jaar verwacht deze partij te gaan werken met breached brown passwords.
- Een partij geeft aan dat zij het gebruik van veilige en unieke wachtwoorden kunnen afdwingen. Ook geven ze security awareness sessies waarbij de gebruikers uitleg krijgen over het belang van sterke wachtwoorden over de werkwijze van de tegenstander.
- De laatste partij heeft een oplossing die sterke en unieke wachtwoorden creëert. Daarnaast heeft de partij een dashboard die zwakke, gecompromitteerde, herhaalde en verlopen wachtwoorden herkent.

Verplicht gebruik: Welke mogelijkheden biedt de oplossing om gebruik ervan af te dwingen, in elk geval voor zakelijke toepassing, zodat gebruik van slechte wachtwoorden uitgesloten wordt. Hoe ziet dat eruit? Indien dit niet mogelijk is: waarom niet?

Een partij geeft aan dat zij gebruik maken van een veiligheidsooplossing in de vorm van een Adaptieve Password Firewall die, rekening houdend met de AVG-richtlijnen, over de schouders van medewerkers meekijkt en ingrijpt wanneer iets niet goed gaat. Er kan hierbij een onderscheid gemaakt worden tussen zakelijk en privé. Op basis van algemene regels wordt een standaardbescherming ingesteld voor alle applicaties en via specifieke regels een bescherming voor individuele applicaties.

Een andere partij heeft een wachtwoordbeleid met minimale eisen waaraan het wachtwoord moet voldoen voordat deze wordt ingesteld. Rapportages evalueren de veiligheid van de individuele kluis en die van de organisatie.

Een partij geeft aan dat een username en wachtwoord combinatie altijd op een memo briefje geschreven kan worden, waarmee het gebruik van de wachtwoordmanager direct omzeild wordt. Hier zijn gelukkig wel oplossingen voor, zoals bijvoorbeeld een Single Sign On en 2FA key via de oplossing van de partij. Door 2FA van doelsystemen te registreren in de kluis kan gebruik gecontroleerd worden en kunnen wachtwoorden niet meegenomen en succesvol gebruikt worden. Daarnaast worden kluis-lees acties gelogd.

Een laatste partij geeft aan dat dit in diverse stukken software af te dwingen is. Verder is het ook te controleren of bestaande wachtwoorden zwak zijn, op bekende lijsten staan of gegevens gelekt zijn en hier alerting op in te stellen.

Gedeelde wachtwoorden: Welke mogelijkheden biedt de tool voor gedeelde wachtwoorden?

Alle partijen hebben een mogelijkheid om wachtwoorden te delen. Afhankelijk van de oplossing kan dit op verschillende wijzen worden gedaan:

- Er kunnen teams worden aangemaakt, waarbij een account delen mogelijk is zonder het delen van wachtwoorden. Leden van een team hebben een gedeelde accountwachtwoorden. Elk team heeft één of meerdere beheerders. Deze beheren de leden van een team. Wanneer een lidmaatschap van iemand eindigt, is het niet langer mogelijk om voor deze persoon nog het gedeelde wachtwoord te berekenen. Hierdoor heeft hij dus geen toegang meer tot het gedeelde account.
- Via een open-source wachtwoordbeheerservice die opslag, beheer en delen van websitereferenties en andere beveiligde gegevens biedt via een webinterface en downloadbare clients.
- Het (tijdelijk) delen van wachtwoorden kan tussen groepen, individuen en combinaties met en zonder einddatum. Het is altijd inzichtelijk welke wachtwoorden voor wie beschikbaar zijn.
- Volledige RBAC / rights management / group management is mogelijk. Het is geheel op maat naar uw eisen in te stellen.
- Ook is er een optie om restricties aan te geven zoals read-only en read-only met het een verborgen wachtwoord.

Beheeromgeving: Hoe ziet de centrale (enterprise) beheeromgeving eruit?

- Door middel van een online portal in de vorm van een SaaS applicatie. Deze bevat componenten waarvoor een gebruiker geautoriseerd moet zijn. Één daarvan is een dashboard,

waarin de veiligheid van de organisatie gemonitord kan worden. Daarnaast bevat de portal ook een Control Centre, waar de default en de applicatie-specifieke beschermingsniveaus worden ingesteld.

- Administratie wordt uitgevoerd via de web vault.
- Technisch beheer wordt gedaan vanuit een gescheiden grafische interface. Er is geen enkele mogelijkheid tot toegang tot de accounts.
- De centrale beheeromgeving is een web interface waarin aan rollen of identity source groepen beheerrechten uitgedeeld kunnen worden. Er zijn company governance policies mogelijk die kunnen instellen of gebruikers al dan niet eigen applicaties mogen toevoegen, wat ze exact kunnen aanpassen, kunnen delen, welke domeinen ze niet mogen toevoegen en welke email-adressen al dan niet toegelaten zijn.
- Zowel centraal management als delegated group control is mogelijk.
- De centrale admin console maakt de implementatie van organisatie breed beleid mogelijk, zoals het afdwingen van wachtwoordregels en -voorschriften, wachtwoordcontrole voor inbreuk en monitoring op het dark web, en afdwinging van verschillende app-instellingen. De console bevat ook automatische bevoorrading van werknemers via SCIM.

Beheermogelijkheden: Welke beheermogelijkheden zijn er om instellingen te veranderen (bijv. features uitschakelen en te hanteren wachtwoordbeleid inregelen)?

- Diverse features kunnen aan en uit gezet worden, zoals MFA-everywhere. Ook kunnen algemene en applicatie-specifieke beschermingsniveaus ingesteld of uitgezet worden. De beschermingsniveaus vormen een krachtige en flexibele manier om de kwaliteitseisen van wachtwoorden in te stellen.
- Het beleid stelt organisaties in staat om beveiligingsregels af te dwingen, zoals het resetten van master passwords en het beleid voor het genereren van wachtwoorden.
- Globale instellingen worden beheerd via het dashboard door leden van de groep. Daarnaast kunnen de decentrale groepen hun eigen groep specifieke instellingen beheren. Wachtwoordbeleid is een globale instelling.
- Er zijn verschillende typen van beheermogelijkheden, zoals: business vaults location policy, master password policy, security policies, password audit policy, password rules specification en appinstellingen.

BIO: Ondersteunt u BIO-compliance? Indien nee: waarom niet?

Drie partijen geven aan dat hun oplossing BIO-compliance ondersteunt. De overige drie partijen zijn wel ISO 27001 gecertificeerd en hebben meerdere aanvullende certificaten.

Zakelijk/privé: Kunt u onderscheid maken tussen zakelijk en privé? En hoe doet u dat? Indien nee: waarom niet?

Drie partijen geven aan een onderscheid te maken tussen zakelijk en privé door middel van een multi-identity of door aparte kluizen. Echter wordt wel aangeraden om beide toch volledig te scheiden. Eén organisatie geeft aan dat zakelijk en privé technisch gezien niet van elkaar gescheiden worden, maar dat privé wachtwoorden wel kunnen worden opgeslagen. Verder is er een partij die aangeeft alleen een zakelijke oplossing te hebben. Bij privégebruik moet bij off-boarding rekening gehouden worden met het exporteren van de persoonlijke wachtwoorden.

Categorisatie: Welke mogelijkheden biedt u voor categorisatie (bijv. typering, groepering, labeling, tagging)?

Vijf van de zes partijen geven aan de mogelijkheid te hebben voor categorisatie. Die gaat op verschillende wijzen, bijvoorbeeld door middel van groeperingen, tags, templates en folders. Een partij geeft aan deze wens nog niet eerder gehoord te hebben bij gemeenten.

Offline: Hoe reageert het product als internet niet beschikbaar is?

Vier van de zes oplossingen hebben een internetverbinding nodig om wachtwoorden te kunnen berekenen en opslaan. Bij twee oplossingen is dit geen probleem en kunnen alle kerntaken uitgevoerd worden zonder verbinding.

2.1.3. Implementatie

Implementatie duur en impact: Voor de planning van het traject is inzicht in de benodigde duur voor de implementatie nodig. Wat is een realistische implementatie impact en duur bij een gemeente vergelijkwaardig qua grootte als de gemeente Eindhoven? Houd hier rekening met eventueel benodigde koppelingen en systeem inrichting.

De implementatieduur is erg afhankelijk van wat de Aanbestedende dienst wilt. De antwoorden verschillen daarin dan ook op het gebied van service:

- Een andere partij heeft bij een vergelijkbare organisatie een implementatie gehad met een duur van 6-8 weken. Na deze periode is een consultant nog enkele weken beschikbaar geweest.
- Een partij geeft aan dat de technische implementatie en uitrol eenvoudig is. Tijd gaat zitten in de menselijke implementatie en het veranderproces binnen de organisatie. Ongeveer 3 maanden voor de voorbereiding, technische implementatie en het trainen van ambassadeurs, ongeveer 6 maanden voor de uitrol in de hele organisatie en ongeveer 6 maanden voor het stap-voor-stap inregelen van beschermingsniveaus.
- Een partij geeft aan dat de technische implementatie binnen een dag te realiseren is, maar dat de inrichting afhankelijk is van de wensen van de Aanbestedende dienst. Het succesvol en breed in gebruik nemen vergt goede communicatie en training. De organisatie helpt hierbij.
- Een partij geeft een inschatting van 120-180 uur voor de implementatie en een totale doorlooptijd van 3 maanden.
- De initiële account setup duurt 1-7 dagen. Het maken van aanvullende pakketten duurt ongeveer 2 dagen. De volledige uitrol duurt naar schatting 2 weken.
- Een andere oplossing kan binnen een dag na de aanschaf geïmplementeerd zijn.

2.1.4. Kosten

Licentiemodel: Welk licentiemodel(len) wordt/worden gehanteerd? Behoort een site-licence tot de mogelijkheden? Welke kosten behoren bij de verschillende onderdelen/modules in het licentiemodel?

In het kader van het vermijden van het opnemen van bedrijfs- en/of commercieel gevoelige gegevens worden er geen kosten gedeeld van afzonderlijke inschrijvers.

Kosten: Met in achtneming van het antwoord op de andere vragen, kunt u een inschatting geven van de totale eenmalige kosten en de totale jaarlijkse kosten, rekening houdend met aanschaf, implementatie, beheer en onderhoud van de oplossing? Graag de benoemde onderdelen separaat benoemen.

In het kader van het vermijden van het opnemen van bedrijfs- en/of commercieel gevoelige gegevens worden er geen kosten gedeeld van afzonderlijke inschrijvers.

Functioneel beheer: Onze voorkeur gaat uit naar een cloud/SaaS oplossing. Hoe wordt het functioneel beheer door u geleverd en als dat niet mogelijk is wat is uw inschatting van benodigde capaciteit voor functioneel beheer? Hoe ziet een samenwerking op de beheeractiviteiten vanuit uw organisatie en beheer van de gemeente Eindhoven eruit?

- Een partij geeft aan dat hun oplossing een SaaS oplossing is. Functioneel beheer gebeurt volledig automatisch en hiervoor is nagenoeg geen capaciteit nodig van de gemeente. De organisatie staat in nauw contact met de beheersafdeling van de gemeente en is direct bereikbaar voor allerlei vormen van samenwerking.
- Een andere oplossing biedt zowel een cloud-hosted optie en een optie voor self-host-on-premises.
- Een andere partij heeft twee mogelijkheden: via een on-premise/SaaS entiteit of managed via een cloud volgens de wet- en regelgeving in Nederland. Functioneel beheer wordt meegeleverd in een cloud-uitgifte.
- Een partij geeft aan dat de werkzaamheden voornamelijk zitten in de uitbreiding van de tooling en additionele wensen. De gemeente zou deze werkzaamheden zelf kunnen uitvoeren, maar ook kunnen uitbesteden aan de leverancier.

- De laatste partij geeft aan het beheer volledig uit handen te kunnen nemen en ook een private omgeving te kunnen bouwen.

2.1.5. Inkoopstrategie

Procedure: Welke aanbestedingsprocedure adviseert u en waarom?

- Een partij geeft aan geen specifieke voorkeur te hebben van procedure, maar adviseert de Aanbestedende dienst wel om rekening te houden met de snelheid van de procedure, in verband met de risico's voor de organisaties en ook om scherpe eisen op te stellen die zich richten op gegevensbescherming.
- Twee partijen adviseren een concurrentiegericht dialogo of een bidding procedure.
- Een partij denkt onder de Europese aanbestedingsgrens te blijven en adviseert in dit geval een meervoudig onderhandse EMVI aanbesteding en om met alle uit te nodigen partijen fysiek in gesprek te gaan.
- Een andere partij geeft aan dat het belangrijk is dat op kwaliteit wordt beoordeeld.
- Een partij geeft geen concreet antwoord over welke procedure het meest passend is.

Procedure: Heeft uw onderneming ervaring met het inschrijven op een aanbesteding o.b.v. de beste prijs/kwaliteitverhouding?

Vijf van de zes partijen geven aan hier ervaring mee te hebben. Eén van deze vijf adviseert om de eisen van de aanschaf niet te beperken tot het technische middel, maar deze af te stemmen op informatieveiligheid en privacybescherming. Een andere partij geeft aan dat zij selectief zijn in het inschrijven op aanbestedingen en niet vaak mee doen. De partij vindt dat veel vraagstellingen niet gericht zijn op het veiliger maken van de organisatie, maar op het verkrijgen van een technische oplossing. Zij passen meer in een omgeving waar integraal wordt nagedacht over veiligheid en verandering een onderdeel is van het proces.

Kwaliteitscriteria: Wat zijn volgens u geschikte kwaliteitscriteria om de verschillende aanbieders te onderscheiden?

Er zijn verschillende voorbeelden gegeven:

- Alle (zakelijke) wachtwoorden moeten ten minste voldoen aan de nieuwe BIO-eisen.
- Het gebruik van de wachtwoordoplossing moet organisatie breed afgedwongen kunnen worden om orde te scheppen in de huidige chaos in wachtwoordgebruik. Dit moet gemeten en gerapporteerd kunnen worden.
- Wachtwoorden mogen niet in een kluis bewaard worden vanwege de veiligheidsrisico's die dat met zich meebrengt. Een partij waarschuwt hier voor schijnveiligheid.
- Implementatie van een passwordmanager.
- Integrale kennis over digitale toegang, waar wachtwoorden een onderdeel van zijn.
- Beveiliging van de oplossing met de beveiligingsreputatie van de aanbieder.
- De stabiliteit en visie van het bedrijf rondom beheer van wachtwoorden.
- De (door)groeimogelijkheden die de leverancier biedt. Bijvoorbeeld de mogelijkheid om highly privileged accounts en wachtwoorden onder te brengen in een volwaardige Privileged Access Management oplossing of het wachtwoord portaal te gebruiken voor andere reguliere toegang tot applicaties.
- Controle over de dataopslag.
- Cross-platform availability.
- Third-party security audit.
- Beveiligingsstandaarden en certificering.

Aanbestedingsplatform: Heeft uw onderneming ervaring met het indienen van inschrijvingen/offertes middels TenderNed of een ander aanbestedingsplatform?

Vier van de zes partijen geven aan ervaring te hebben met inschrijvingen in TenderNed. Twee andere partijen hebben ervaring met andere platforms, zoals SAP Ariba.

Referentie: Beschikt u over ervaringen/referenties bij andere gemeenten?

- Een partij heeft ervaring bij meerdere gemeenten die opgegeven kunnen worden als referentie.
- Een partij verwijst naar de reviews en ervaringen op hun website.
- Een partij heeft ervaring bij andere gemeenten en ook bij forensische diensten en landelijke en lokale overheidsorganisaties.
- Een partij is partner van meerdere overheidsinstellingen op het gebied van IGA/PAM/IAM. De eindgebruikers wachtwoord kluis is echter een relatief nieuw product in hun portfolio. De partij heeft dit bij één overheidsinstelling geïmplementeerd.
- Een partij geeft aan ervaring te hebben, maar dat de inhoud vaak is onder DNA.
- Een andere partij geeft aan ervaring te hebben met Europese organisaties en adviesbureaus, maar niet met gemeenten binnen Europa. De partij heeft hier echter wel ervaring mee binnen de VS.

Verkoopkanalen: Maakt u gebruik van resellers of levert u zelf direct aan de opdrachtnemer?

- Twee partijen geven aan dat ze beiden zijn.
- Twee partijen zijn zelf een reseller.
- Twee partijen geven aan hun service aan te bieden aan zowel klanten als partners/resellers.

2.1.6. Testperiode

Proefaccount: Kunt u ons beschikking geven over een proefaccount waarmee wij uw product een periode kunnen uitproberen?

Iedere partij geeft aan deze mogelijkheid te hebben.

3. Ten slotte

Gemeente Eindhoven kan nog geen informatie verstrekken of en wanneer een mogelijke aanbesteding voor Passwordmanager wordt uitgezet. De gegevens die de Aanbestedende dienst heeft verkregen vanuit de marktconsultatie dienen als input voor deze beslissing. Indien de gemeente verwacht om een aanbesteding Passwordmanager te publiceren, zal dit naar verwachting in Q3 2023 zijn.

De verkregen gegevens uit de marktconsultatie dienen als input. De Aanbestedende dienst gebruikt deze om een eventuele aanbestedingsdocumenten op te stellen en een aanbestedingsstrategie te bepalen. De gemeente beslist welke informatie van toepassing en relevantie is op haar dienstverlening, waardoor het mogelijk is dat bepaalde gegeven antwoorden vanuit de marktconsultatie niet worden opgenomen en toegepast.

Bijlage 1 – Nota van Inlichtingen

Nota van Inlichtingen I

Betreft	Marktconsultatie	Datum	2 mei 2023
Van	Gemeente Eindhoven	Ref.	Wachtwoordmanager
Project	Marktconsultatie Wachtwoordmanager		

Nr.	Betreft	Vraag
1.	Authenticatie	However, it looks like your system wants us to purchase some 3rd party authentication software... is it correct? It looks very suspicious that we have to purchase something to participate. Het lijkt erop dat uw systeem wil dat wij een derde partij authenticatie software kopen, klopt dit? Het lijkt erop dat wij iets moeten kopen om mee te kunnen doen.
Antwoord	The Municipality of Eindhoven has started this market consultation to find out what the market has to offer. There is no intention whatsoever from the contracting authority that you should purchase something from a third party. Gemeente Eindhoven heeft deze marktconsultatie gestart om te achterhalen wat de markt allemaal te bieden heeft. Er is geen enkele intentie vanuit aanbestedende dienst dat u iets dient aan te kopen bij een derde partij.	

Nr.	Betreft	Vraag
2.	BIO	Ondersteunt u de BIO compliancy – wat bedoelt u daarmee? Welke richtlijnen mikt u specifiek op.
Antwoord	Hiermee wordt ‘Baseline Informatiebeveiliging Overheid’ bedoeld. Dit is het basishorizontaal kader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Had voorheen iedere overheidslaag zijn eigen baseline, nu is er met gezamenlijke inspanning één BIO voor de gehele overheid. Alle informatie over de BIO vindt u op: Baseline Informatiebeveiliging Overheid Cybersecurity - Digitale Overheid	

Nr.	Betreft	Vraag
3.	Beheerdersorganisatie	Is er onderscheid tussen de gebruikersorganisatie en de beheerdersorganisatie?
Antwoord	De gebruikersorganisatie zal bestaan uit medewerkers van gemeente Eindhoven. De beheerdersorganisatie (functioneel beheer) zal bij een of meerdere medewerkers van gemeente Eindhoven belegd worden. Graag ontvangen wij informatie over hoe u het functioneel beheer levert en welke capaciteit, kennis en activiteiten nodig zijn vanuit gemeente Eindhoven.	

Nr.	Betreft	Vraag
4.	Beheerdersorganisatie	Gaat de beheerdersorganisatie ook gebruik maken van deze tooling, of heeft deze separate tooling voor hun processen?
Antwoord	De beheerdersorganisatie maakt ook gebruik van deze tooling, mits dit mogelijk is binnen de aangeboden oplossing. Beheer zal plaatsvinden conform de mogelijkheden die de oplossing biedt.	

Nr.	Betreft	Vraag
5.	Categorisatie	In de lijst met vragen staat onder "Oplossing" een vraag over "Categorisatie". a) Wat wordt precies bedoeld met "Categorisatie"? b) Wat is het beoogde gebruik/doel van deze functionaliteit? c) Waarom is dit belangrijk? d) Hoe belangrijk is dit t.o.v. de andere onderdelen bij "Oplossing"?
Antwoord	a) Bijvoorbeeld het categoriseren van authenticatiegegevens in een groep of op basis van functie te kunnen labelen binnen de oplossing. b) Efficiënter en gemakkelijker gebruik maken van de tool. c) Aanbestedende dienst heeft gezien dat er verschil zit tussen tools, via deze marktconsultatie willen wij inzichtelijk krijgen wat de markt te bieden heeft. d) Het doel van de marktconsultatie is alle mogelijkheden in kaart brengen met betrekking tot een wachtwoordmanager. Tussen alle gestelde vragen en/of onderdelen die benoemd zijn is geen onderscheid in belang.	