

**Betreft: Nota van Inlichtingen Marktconsultatie Veilig Mailen
14-11-2022**

Vraag: Om hoeveel verschillende soorten devices gaat het en om hoeveel in totaal waarop de software geïnstalleerd moet worden?"

Antwoord:

- 5000 Managed laptop
- 4000 Managed en 2000 unmanaged mobiele devices
- 600 Managed Tablets
- 1500 Azure Virtual Desktop, wordt ingezet voor unmanaged laptops

Het heeft de voorkeur om iedereen te voorzien van de mogelijkheid om veilig mailen. Of dit via geïnstalleerde software moet is natuurlijk nog de vraag en afhankelijk van de oplossing.

Vraag 2. Wat wordt er bedoeld met "een gebruikte verificatie methoden"?

Antwoord:

- Verificatie email
- Verificatie door toegangscode
- Verificatie SMS
- De ontvanger heeft al een Zivver account

Vraag 6: Kan op meerdere manieren geïnterpreteerd/ beantwoord worden. Kunt u dit wellicht beschrijven met een voorbeeld en/of toelichten? (Indien uw oplossing een volledige SaaS oplossing betreft hoe vindt de integratie plaats met de gemeente en op welke wijze wordt authenticatie toegepast.

Antwoord: Betreft hier vooral de integratie zonder plugin en de wijze waarop dan de integratie naar bv de EOL omgeving van de gemeente Utrecht.

Vraag 17: Wat bedoeld u met: "Ziet u ook mogelijkheden om de ontvangende kant de verantwoordelijkheid te geven over de account die dan toegang hebben te de beveiligde email?"

Antwoord: Op welke wijze zou je de verantwoordelijkheid over wie er toegang heeft (accounts) tot de beveiligde mail kunnen beleggen bij de ontvangende partij. Het is met name een uitdaging bij algemene mailboxen om de toegang te organiseren voor verschillende medewerkers en bij ziekte/afwezigheid dit last minute te organiseren. Wij snappen dat dit in basis niet wenselijk is, maar misschien zijn er ideeën hoe dit onder bepaalde voorwaarden georganiseerd kan worden.