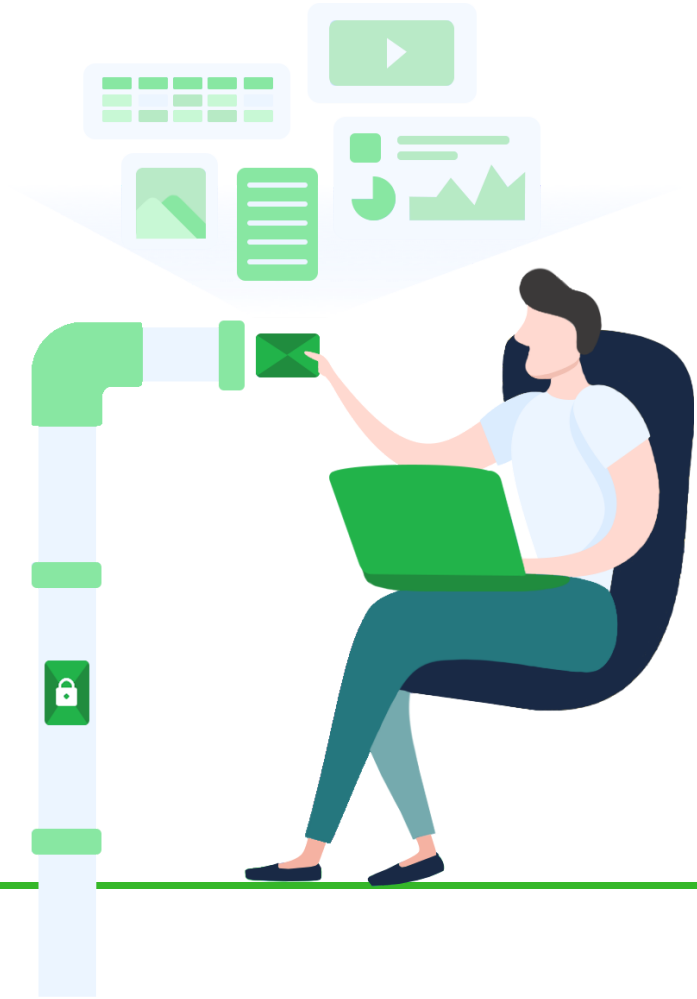
SMARTLOCKR VEILIG MAILEN:

veilig dataverkeer
en data opslag



BASIS BEVEILIGING

Alle bestanden worden per verzending met een automatisch gegenereerde AES-GCM sleutel vergrendeld. De AES-GCM sleutel wordt op zijn beurt vergrendeld met een 256-bit sleutel, die we genereren op basis van het ID in de download link. Hiervoor gebruiken we de PBKDF2 functie* met 10000 iteraties en een 32 byte salt .

Wij maken gebruik van AES-GCM**, omdat deze modus de sterkste cryptografie biedt. Tevens stelt die ons in staat om grote blokken data, parallel aan elkaar, te uploaden.

* meer info:
https://en.wikipedia.org/wiki/PBKDF2
** meer info:
https://en.wikipedia.org/wiki/Galois/Counter_Mode

WACHTWOORD BEVEILIGING

Net als bij de basis beveiliging, worden bestanden met de wachtwoord beveiliging vergrendeld met een automatisch gegenereerde AES-GCM sleutel. Deze wordt vervolgens vergrendeld met een 256-bit sleutel die wij genereren op basis van een wachtwoord. Ook hiervoor gebruiken we de PBKDF2 functie* met 10000 iteraties en een 32 byte salt.
Omdat de sleutel opnieuw kan worden gegenereerd met het juiste wachtwoord, hoeven wij dit niet op te slaan.

Wederom maken wij gebruik van AES-GCM**. Naast dat deze modus de sterkste cryptografie biedt,geeft het ons weer de mogelijkheid om grote blokken data, parallel aan elkaar, te uploaden.

SMARTLOCKR
Powered by AttachingIT

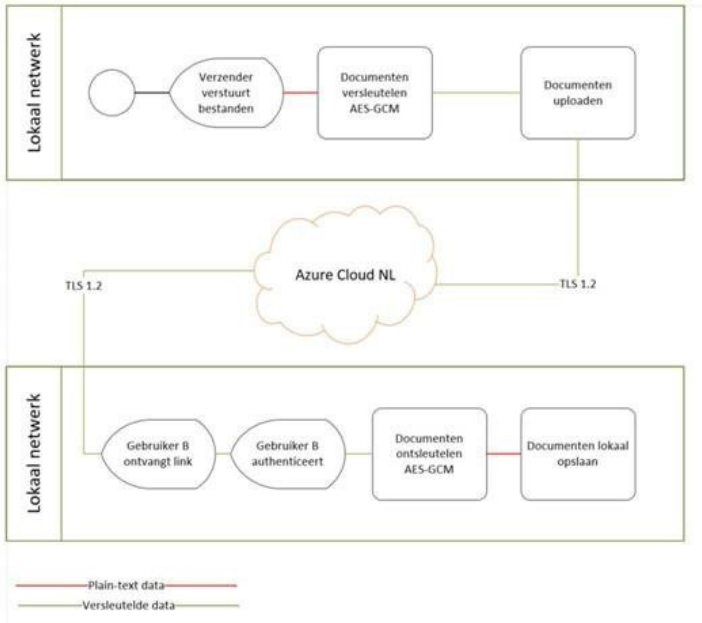
AZURE CLOUD OPSLAG

Windows Azure biedt een vertrouwd en zeer stabiel opslagmedium. Wij gebruiken deze opslag om de data op te slaan. Deze data worden uitsluitend opgeslagen binnen de Europese Unie, omdat daar de Europese privacywetgeving van kracht is (AVG). De data die wij versturen, worden opgeslagen in het Windows Azure Datacenter in Amsterdam. Daarnaast wordt er een reservekopie opgeslagen in het Windows Azure Datacenter in Dublin, Ierland. Deze reservekopie wordt slechts gebruikt wanneer de data in Amsterdam, door bijvoorbeeld calamiteiten, niet beschikbaar zijn.

Voordelen Azure Cloud opslag:

* data zijn middels een kopie altijd terug te halen;
* voor elke klant een aparte opslag, waardoor klantdata gescheiden blijven;
* alle data worden per document vergrendeld;
* unieke sleutel voor elke klant. Hiermee blijven data ontoegankelijk voor onbevoegden.

De sleutels worden veilig opgeslagen, middels een zogeheten keyvault. Wanneer een gebruiker documenten met een wachtwoord verstuurt, dan zullen de bestanden worden vergrendeld met dit wachtwoord. Al het verkeer tussen zowel de klant en ons, en tussen ons en de ontvanger is vergrendeld met een TLS-verbinding



ON-PREMISES

Wanneer je liever zelf zorgt voor de hosting en het onderhoud, dan is dit uiteraard ook mogelijk.

In dit geval maak je geen gebruik van het Windows Azure Datacenter, maar dien je zelf een server in te richten. Wat je hiervoor nodig hebt, zijn een Windows Server 2008 R2 of hoger, een domeinnaam en SSL-Certificaat. Jouw data, zowel je verzonden als ontvangen, worden dan ook op jouw eigen server opgeslagen.

Uiteraard kan dit ook via een IT dienstverlener.

CERTIFICERING DATACENTER MS AZURE

Het Windows Azure Datacenter en bijbehorende diensten zijn sterk gecertificeerd (ISO/IEC27018) op het gebied van privacy en security. Het volledige overzicht kun je vinden via onderstaande link: https://azure.microsoft.com/nl-nl/overview/trusted-cloud/

De data die de klant opslaat hebben een standaard retentieperiode van 14 dagen,indien wij de data voor je hosten. Wanneer de retentieperiode is verstreken worden de data, metadata en de reservekopieën volledig verwijderd van de servers. De duur van de retentieperiode kan echter afwijken: dit hangt af van het abonnement of wat er contractueel is vastgelegd.