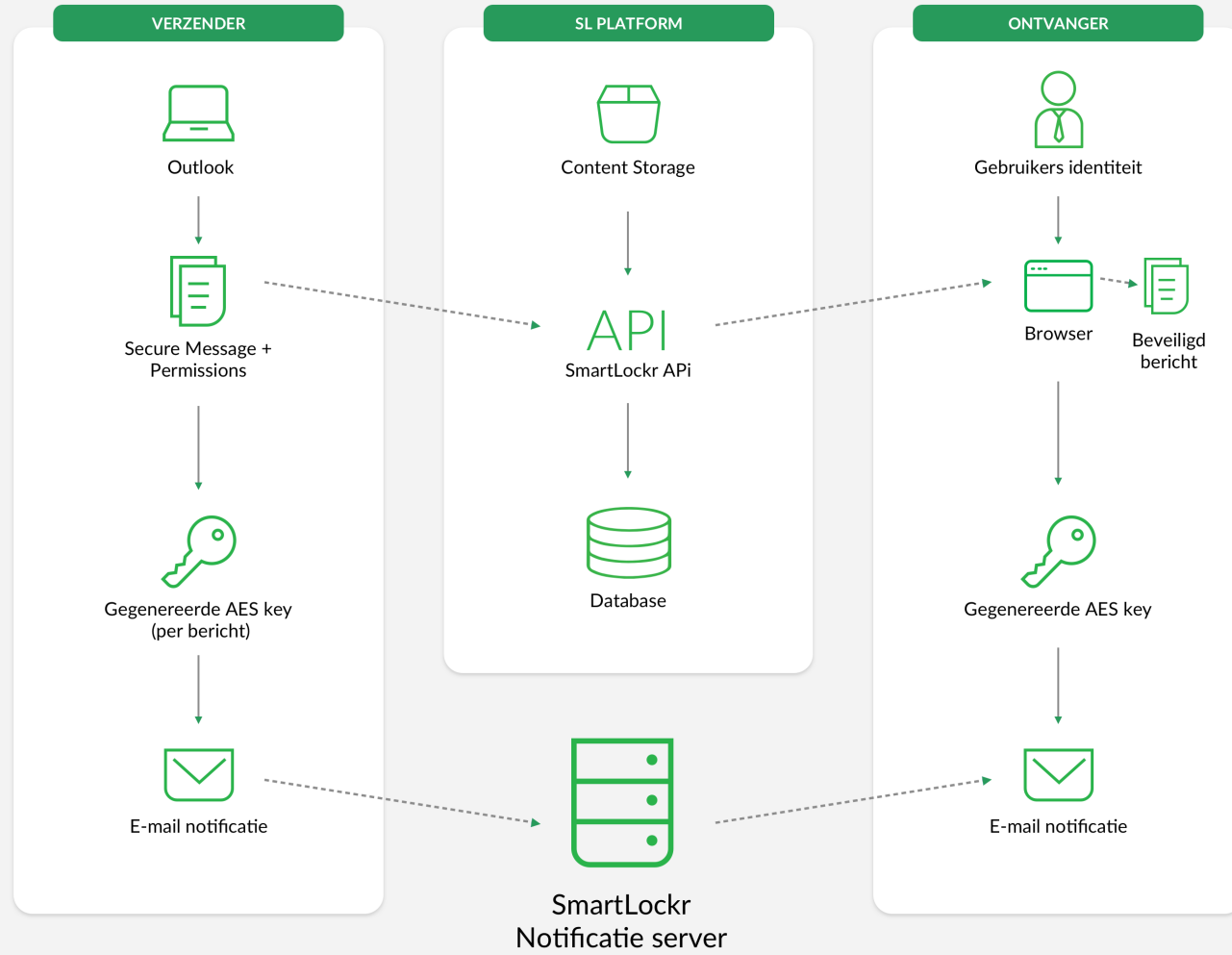


Alle verbindingen, van en naar het SmartLockr platform, worden beveiligd met TLS1.2 verbindingen. Hierbij worden enkel sterke versleutelingsalgoritmen gebruikt.

INHOUDSOPGAVE

1. Encryptie
2. Authenticatie
3. Cookie veiligheid
4. Azure Datacenter W. Europa
5. Backups
6. Redundante opslag
7. Certificeringen
8. NTA 7516 flow

SMARTLOCKR ARCHITECTUUR



Encryptie

Alle verbindingen, van en naar het SmartLockr platform, worden beveiligd met TLS1.2 verbindingen. Hierbij worden enkel sterke versleutelingsalgoritmen gebruikt. Alle informatie wordt per verzending met een automatisch gegenereerde AES-GCM sleutel vergrendeld.

Deze AES-GCM sleutel wordt vervolgens vergrendeld met een 256-bit sleutel, die we genereren op basis van het ID in de downloadlink. 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. Daarnaast stelt het ons in staat om grote blokken data, parallel aan elkaar, te uploaden.

De sleutels worden echter niet opgeslagen in het SmartLockr platform. Deze worden bij verzending zowel op de lokale machine, als op de lokale machine van de ontvanger gebruikt. Hierdoor kan SmartLockr zelfs informatie die met een publieke link wordt gedeeld niet inzien.



Authenticatie

Met SmartLockr worden bestanden en berichten op een veilige manier verzonden en ontvangen. Wij bieden namelijk zowel een-factor als twee-factor-authenticatie aan:

- Met één-factor-authenticatie wordt er een wachtwoord per e-mail wordt verzonden naar de ontvanger. Als dit e-mailadres juist is, dan kan de ontvanger het toegestuurd wachtwoord gebruiken om toegang te krijgen tot de berichten. Dit is een veilige oplossing, maar dat hangt natuurlijk af van het gekozen wachtwoord van, in dit geval, uw e-mail.
- Twee-factor-authenticatie is een sterkere beveiligingsoptie. Zowel het e-mailadres als het telefoonnummer van de ontvanger moeten worden geverifieerd. Niet alleen krijgt de ontvanger een e-mail, maar ook een toegangscode die per SMS gestuurd wordt. De combinatie van twee beveiligingsfactoren zorgt er dus voor dat het moeilijker wordt voor onbevoegden om bij het bericht te komen.

Dit betekent dat slechts de geauthentiseerde ontvanger toegang heeft tot het bericht. Zelfs als u deze beveiligde gegevens naar een verkeerde persoon stuurt, kan deze de gegevens niet inzien. Zonder de juiste toegangscode, geen toegang!

Cookie veiligheid

Om gebruikers in sessies te houden worden authenticatie cookies gebruikt. Deze worden voorzien van de Secure en HttpOnly flag. Hiermee kunnen de cookies alleen over HTTPS worden verzonden naar de SmartLockr servers.



Microsoft Azure Datacenter West Europa

SmartLockr maakt gebruik van het Microsoft Azure Cloud platform, locatie West-Europa. Microsoft Azure biedt een vertrouwd en zeer stabiel opslagmedium. Wij gebruiken deze opslag om de data op te slaan. Deze data wordt uitsluitend opgeslagen binnen de Europese Unie, omdat daar de Europese privacywetgeving van kracht is (AVG/GDPR). De data die wij versturen, wordt opgeslagen in het Microsoft 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 is.

Voordelen van de Azure Cloud opslag:

- Data is middels een kopie altijd terug te halen;
- Voor elke klant is er een aparte opslag, waardoor klantdata gescheiden blijft;
- Alle data wordt per document vergrendeld;
- Er is voor elke klant een unieke sleutel per e-mail. Hiermee blijft data ontoegankelijk voor onbevoegden.

Back-ups

De SmartLockr Database ondersteunt Point-in-time Restore (PITR), door volledige back-ups, differentiële back-ups en back-ups van transactie logboeken te automatiseren. Volledige database back-ups worden wekelijks gemaakt, differentiële back-ups van data bases doorgaans elke 12 uur en back-ups van transactie logboeken over het algemeen elke 5-10 minuten. De frequentie is gebaseerd op zowel de reken grootte, als ook de hoeveelheid database activiteit.



Redundante opslag

Database back-ups worden net als verzonden documenten redundant opgeslagen. Elk document wordt naast de drie locaties binnen het Azure datacenter in Nederland ook in het Azure datacenter in Dublin (Ierland) opgeslagen.

Wanneer het datacenter in Nederland door een incident of calamiteit niet beschikbaar zou zijn, neemt het datacenter in Dublin het automatisch over. Na een herstel worden documenten en back-ups automatisch gesynchroniseerd.

Certificeringen

SmartLockr is ISO/IEC 27001, NEN-7510 en NTA 7516:2019 gecertificeerd. Het Microsoft Azure Datacenter en bijbehorende diensten zijn sterk gecertificeerd (ISO/IEC27018) op het gebied van privacy en security. Het volledige overzicht kunt u [hier](#) vinden.

De data die de klant opslaat heeft een standaard retentieperiode van 14 dagen. Dit is in het geval wij de data voor u 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.



NTA 7516 Flow

In onderstaand schema staat aangegeven hoe berichten veilig worden verzonden en opgeslagen. De omgeving van de verzender controleert eerst of de ontvangende omgeving aan de NTA 7516 voldoet. Indien eraan wordt voldaan, wordt er een TLS 1.2 of 1.3 verbinding gemaakt.

Als verzender

1. De verzender stuurt een bericht naar de ontvanger.
2. SmartLockr controleert of de ontvanger net als de verzender aan de NTA 7516 voldoet middels een gepubliceerde DNS-record en een aantal verificatie technieken.
3. Wanneer de ontvanger aan de NTA 7516 blijkt te voldoen, wordt er een NTA 7516 header aan de e-mail toegevoegd. Vervolgens wordt deze verzonden naar de ontvanger.
4. De ontvanger zal controleren of de verzender ook aan de NTA 7516 voldoet.
5. Wanneer de verzender is gevalideerd, zal het bericht worden afgeleverd in de inbox van de ontvanger.

