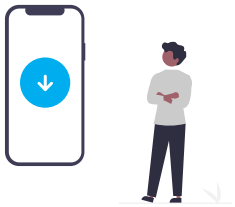
Secudoc



Data-uitwisseling en communicatie conform ISO 27001 / NEN 7510

One-sheeter

SecuDoc garandeert veilige bericht- en bestandsuitwisseling voor onze afnemers, hun ontvangers en overige betrokkenen. Dit document geeft een overzicht van de technieken en voorzorgsmaatregelen die wij treffen om veiligheid en compliancy door de hele keten heen te garanderen.

Certificeringen organisatie	SecuDoc is ISO 27001 en NEN 7510 gecertificeerd (door Brand Compliance). Conform voorgenoemde certificeringen hebben wij een ISMS geïmplementeerd dat conform PDCA veiligheidsaspecten intern, extern, organisatorisch en technisch continu monitort en verbetert. Raadpleeg de volgende link voor de actuele certificaten: https://secudoc.nl/compliancy
Certificeringen keten	Onze volledige upstream keten van onze dienstverlening (leveranciers en diens leveranciers) is ISO 27001 en NEN 7510 gecertificeerd. Hiervoor voeren wij jaarlijks leveranciersonderzoeken uit.
Wetgeving en overige compliancy	SecuDoc is ingericht om afnemers te ondersteunen zoveel mogelijk aan de AVG/GDPR te voldoen, alsook aanvullende wetgevingen voor bijv. zorg (NEN 7510 / NEN 7512). Screening van aangepaste wetgeving vindt jaarlijks plaats.
Toepassing van cryptografie	Opslagversleuteling (data-at-rest): XCHACHA20 + POLY1305 (keyless), E2EE met RSA-keys (keyring). Verbindingsversleuteling (data-in-transit): Expliciet TLS1.2 en TLS1.3 met RSA2048/EC-256.
Keyless	Uploads n.a.v. bestandsoverdrachten slaan wij in-stream op met asymmetrische encryptie, waarna de sleutel direct in de downloadlink wordt verwerkt die naar ontvanger(s) toe wordt gemaild. Sleutel is daarna niet op server aanwezig.
Keyring	Veilige berichten worden versleuteld met end-to-end encryptie, waarbij wordt versleuteld met een private key die afgeleid is van het wachtwoord van de gebruiker (met herstelcode).
Datacenter en dataopslag	Hosting van de SecuDoc applicatie, opslag, on-site en off-site back-ups vindt plaats bij jaarlijks gescreende leveranciers. Dataopslag vindt uitsluitend binnen de EU plaats op geprivatiseerde netwerken (uitgesloten: Amerikaanse platformen als AWS en Azure).

Onderbouwing toepassing van xChaCha20 i.c.m. Poly 1305

Technische Kenmerken
xChaCha20 is een symmetrische streamcipher die bekend staat om zijn snelheid en veiligheid, vooral in software-implementaties. Het gebruikt een langere nonce (192-bit) dan ChaCha20, wat de beveiliging verhoogt door het risico op nonce-hergebruik in versleutelde communicatie uit te sluiten. Poly1305 fungeert als een cryptografische handtekening om de integriteit en authenticiteit van de berichten te waarborgen. Deze combinatie zorgt voor een veilige en efficiënte encryptie die vergelijkbaar is met de prestaties van AES-256.

Veiligheid en Efficiëntie
De veiligheid van xChaCha20 is gebaseerd op de ChaCha-familie van ciphers, die uitgebreid geanalyseerd en beoordeeld zijn door de cryptografische gemeenschap. xChaCha20 is bijzonder resistent tegen verschillende aanvalstechnieken, inclusief timingaanvallen, waardoor het geschikt is voor een breed scala aan platforms en apparaten. De implementatie is gestandaardiseerd en wordt breed ondersteund in cryptografische bibliotheken.

Voordelen voor SecuDoc
SecuDoc heeft xChaCha20-Poly1305 gekozen vanwege de uitmuntende balans tussen beveiliging en prestatie. Dit is van bijzonder belang in een omgeving waar de versleutelingssnelheid en systeemefficiëntie directe invloed hebben op de gebruikerservaring. Daarnaast biedt de langere nonce ruimte een extra beschermingslaag zonder de noodzaak voor complex nonce-management.

Industrie Acceptatie
De acceptatie van xChaCha20-Poly1305 binnen de industrie is groeiend, mede door de adoptie in standaard protocollen zoals TLS en in bekende open-source cryptografische bibliotheken. Deze trend is een bevestiging van de betrouwbaarheid en toekomstbestendigheid van het algoritme.

Conclusie
Na grondige overweging en analyse is de keuze voor xChaCha20-Poly1305 voor SecuDoc een geïnformeerde beslissing geweest. Deze technologie biedt een sterke beveiliging die equivalent of beter is dan AES-256 of RSA-2048. Het ondersteunt de missie van SecuDoc om veilige en efficiënte versleutelingstechnologieën te implementeren, terwijl het ook flexibiliteit en schaalbaarheid biedt voor de toekomst. We zijn ervan overtuigd dat deze keuze de juiste is voor onze klanten, ons product en de continuïteit van onze dienstverleni