Cryptografiebeleid Gooise Meren

Uitgangspunten en eisen cryptografie en VPN

Opsteller	*Jeroen Berkenbosch / Alexander Zagkotsis*
Versie	*1.0*
Datum	*11 maart 2025*
Status	*Definitief*
Classificatie	*Vertrouwelijk*

gemeente gooisemeren

Inhoudsopgave

Versiebeheer

Versie nummer	Omschrijving	Auteur
0.1	Initiële versie op basis van BIO en template ISMS	I.W. Rigters
0.2	Aanpassingen n.a.v. herijking	J. Berkenbosch
0.3	Comprimeren en review tekst	A. Zagkotsis
1.0	Definitieve versie 2025	J. Berkenbosch

Akkoord procesverantwoordelijke

S. Nijs	Manager FIA	Datum invullen

Reviewmoment

December 2025

Relevante normen BIO 1.04

Norm	Omschrijving
10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: wanneer cryptografie ingezet wordt; • wie verantwoordelijk is voor de implementatie; • wie verantwoordelijk is voor het sleutelbeheer; • welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast; • de wijze waarop het beschermingsniveau wordt vastgesteld; • bij inter-organisatiecommunicatie wordt het beleid onderling vastgesteld.
10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.
18.1.5	Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.
18.1.5.1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum.

Gebruikte documenten

1. Baseline Informatiebeveiliging Overheid (BIO), 2021
2. Handreiking Encryptiebeleid-PKI-v2.02, IBD 2019
3. Het PQC-migratie handboek, AIVD/CWI/TNO 2024

1 Cryptografiebeleid

1.1 Doel en reikwijdte

Het doel van dit cryptografiebeleid is het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van gevoelige informatie van gemeente Gooise Meren. In het beleid komen onder meer de volgende onderwerpen aan bod:

- Wanneer cryptografie (en PKI) ingezet wordt.
- Wie verantwoordelijk is voor de implementatie.
- Wie verantwoordelijk is voor het sleutelbeheer.
- Welke cryptografie normen en standaarden worden toegepast.
- De wijze waarop het beschermingsniveau wordt vastgesteld.
- Hoe bij communicatie tussen organisaties encryptie wordt ingezet.

De maatregelen hebben betrekking op de gehele ICT-infrastructuur van gemeente Gooise Meren, met inbegrip van (SaaS-)diensten die bij derden worden afgenomen.

2 Uitgangspunten beleid

2.1 Verantwoordelijkheden

- Manager FIA is verantwoordelijk voor het tot stand komen en de borging van het beleid (aansturing), de uitvoering is primair belegd bij Systeembeheer en Functioneel Beheer.
- Sleutelmateriaal en (PKI) beveiligingscertificaten worden centraal beheert en uitgegeven door Systeembeheer van de gemeente.
- Rechten en plichten voor (eind)-gebruikers (de gebruikersvoorwaarden) die raken aan encryptie zijn opgenomen in andere beleidsstukken zoals het Beveiligingsbeleid hybride werken en het Wachtwoordbeleid.
- De managers dragen zorg voor het borgen van passende afspraken over veilige gegevensuitwisseling met ketenpartners en leveranciers, door het (laten) uitvoeren van DPIA's en het tijdig betrekken van Team IB&P.
- De (C)ISO houdt toezicht op de naleving van het beleid en rapporteert bij inbreuk hierover aan de manager FIA.

2.2 Implementatie

- De uitgangspunten in dit cryptografiebeleid worden op zo veel mogelijk plekken afgedwongen, zowel binnen de gemeentelijke organisatie als bij (SaaS-)leveranciers en andere samenwerkingspartners.
- De beveiliging van informatie, zowel gedurende transport ('in transit') als opslag ('at rest'), en het interne dataverkeer ('machine to machine') wordt conform beveiligingseisen in de informatiebeveiligingsarchitectuur en -classificatie beveiligd.
- Versleuteling vindt plaats conform geldende standaarden (best practices) op basis van risicoclassificatie. We maken hierbij gebruik van de normen en standaarden van het Forum Standaardisatie en actuele richtlijnen van het NCSC.
    - Mocht een informatiesysteem niet kunnen voldoen aan de normen/standaard, dan kan er op basis van een risico-afweging in samenspraak met de (C)ISO een uitzondering worden gemaakt (door mitigerende maatregelen te treffen).
- Digitale documenten van de gemeente waar burgers en bedrijven rechten aan kunnen ontlenen, voldoen aan de wettelijke voorschriften voor certificaten voor tekenen en/of encryptie (zoals AdES Baseline Profile Standaard en PKIoverheid).
- Sleutelmateriaal en (PKI) beveiligingscertificaten worden centraal beheert door de IT-beheerorganisatie van de gemeente.
    - In geval van PKIoverheid-certificaten hanteren we de PKIoverheid-eisen ten aanzien van het sleutelbeheer. In overige situaties hanteren we de norm ISO 11770-1 voor het beheer van cryptografische sleutels.
    - We maken contractuele afspraken met leveranciers van reservecertificaten.
- Gemeente Gooise Meren hanteert classificatieregels (op basis van de BIV) voor gegevens, en zorgt voor passende maatregelen om deze gegevens te beschermen.
- Bij communicatie/gegevensuitwisseling met andere (overheid)organisaties of leveranciers worden de uitgangspunten uit dit beleid geborgd.
    - Op basis van een risico-afweging in samenspraak met de (C)ISO een uitzondering worden gemaakt.

3 Technische eisen en standaarden

- Gemeente Gooise Meren volgt de actuele normen van het Forum Standaardisatie voor cryptografie, waarbij de voorkeur uitgaat naar het gebruik van 'open standaarden'. Mochten de normen van Forum Standaardisatie niet toegepast kunnen worden, kan er gebruik worden gemaakt van NIST-standaarden.
- Alleen goedgekeurde cryptografische algoritmen mogen worden gebruikt, zoals aanbevolen door NIST. Bijvoorbeeld AES-256, RSA-2048, SHA-256

Algoritmen en sleutels worden periodiek geëvalueerd op veiligheid en vervangen indien verouderd.

3.1 Versleuteling van hardware

Op werkdevices, zoals laptops, iPhones en iPads van gemeente Gooise Meren wordt Full Disk Encryption (FDE) gebruikt.

3.2 (Web)servercertificaten

- Gebruik TLS 1.3.
- Onversleutelde (http-)verbindingen zijn niet toegestaan.
- Sleutellengte is minimaal 2048 bits voor RSA, minimaal 256 bits voor ECC (Elliptic Curve Cryptography).
- Gebruik een hash in de vorm van SHA384 of SHA512
- Cipher suites: Voorkeur voor AEAD-suites zoals CHACHA20_POLY1305 en AES-GCM
- Implementeer waar mogelijk Forward Secrecy (PFS): Gebruik cipher suites die ECDHE of DHE ondersteunen voor sleuteluitwisseling
- Betreffende (functioneel) beheerder is verantwoordelijk voor toezicht op certificaten en het tijdig verlengen hiervan.
- Waar mogelijk worden certificaten van Gooise Meren gebruikt bij (SaaS-)diensten. Als dit niet mogelijk is, moet het certificaat van de leverancier aan de overige uitgangspunten van dit Cryptografiebeleid voldoen.
- Certificaten worden aangevraagd door de daarvoor gemandateerde (in beginsel een systeembeheerder) bij gemeente Gooise Meren.
  - Bij openbaar webverkeer maken we gebruik van publiek vertrouwde Organization Validated (VA) certificaten, bij intern webverkeer voor gevoelige gegevens maken we gebruik van publieke vertrouwde OV-certificaten of private PKIo-certificaten.
  - In principe is het gebruik van OV-certificaten voldoende. Waar nodig kunnen EV-certificaten worden gebruikt.
  - Certificaten worden alleen aangevraagd bij een partij waar de gemeente een contract mee heeft.
  - In afstemming met de (C)ISO kan gebruik worden gemaakt van LetsEncrypt-certificaten.
- Gegevensuitwisseling tussen overheden dient te voldoen aan de daarvoor geldende standaarden. Bijvoorbeeld PKIoverheid.

3.3 Quantumcryptografie

Met de opkomst van quantumcomputers, worden cryptografische algoritmen die bestemd zijn tegen decryptie (ontsleuteling) steeds relevanter. Hoewel de implementatie van deze encryptiemethoden nog in de spreekwoordelijke kinderschoenen staan, wordt er in dit cryptografiebeleid al wel rekening mee gehouden. Bijvoorbeeld door het gebruik van TLS 1.3.

Quantumveilige cryptografie kan worden toegepast indien dit op basis van een risicoafweging noodzakelijk wordt geacht. Hiervoor biedt Het PQC-migratie handboek van de AIVD, CWI en TNO een stappenplan.

De Nederlandse overheid heeft nog geen officiële standaarden vastgesteld voor quantumveilige cryptografiestandaarden, maar raadt aan de NIST-standaarden FIPS 203, FIPS 204 en FIPS 205 te hanteren.

3.4 VPN-tunnel

3.4.1 Uitgangspunten

In principe wordt het gebruik van VPN-tunnels ontmoedigd. Als er geen alternatieven zijn, kan een VPN-tunnel worden toegestaan mits het voldoet aan de voorwaarden in dit Cryptografiebeleid.

- Servers/applicaties die gebruik maken van VPN-tunnels dienen passend te worden geconfigureerd (gehardened) door de leverancier.
- Servers/applicaties die voorzien zijn van een VPN-tunnel worden zo veel mogelijk in een afgescheiden netwerkzone/VLAN geplaatst.
- Tunnels worden vormgegeven op applicatieniveau en niet op poortniveau.
- VPN-tunnels dienen te worden geïmplementeerd op de firewall van gemeente Gooise Meren, zodat de gemeentelijke organisatie het verkeer kan monitoren. VPN-tunnels die worden geconfigureerd op bijvoorbeeld (monitorings)machines van een derde partij (zoals een leverancier) zijn in beginsel niet toegestaan.

3.4.2 Werkwijze

Voor het verkrijgen van toestemming en het inrichten van VPN-tunnels hanteert Gooise Meren de volgende werkwijze:

1. Aanmelden bij Systeembeheer
2. Review met (C)ISO
3. Opstellen/aanpassen overeenkomst leverancier (hierin worden de eisen voor Fase 1 en Fase 2-verbindingen zoals hieronder beschreven vastgelegd)
4. Ondertekening overeenkomst
5. Inrichting VPN-tunnel door GM/Leverancier
6. Toetsing op borging verbindingseisen

3.4.3 Phase 1 Technische eisen/configuratie

Mode	IKEv2 Only
DH-groep	Diffie-Hellman group 19 - 256 bit elliptic curve Diffie-Hellman group 20 - 384 bit elliptic
Encryptie-algoritme	AES256 (CBC)
Hash	SHA384 of SHA 512
Lifetime	8 uur
PSK	40 karakters, wordt niet gedeeld via e-mail

3.4.4 Phase 2 Technische eisen/configuratie:

IPSEC-protocol	ESP
Perfect Forward Secrecy (PFS)	Ja, enabled
FPS DH-groep	Diffie-Hellman group 19 - 256 bit elliptic curve Diffie-Hellman group 20 - 384 bit elliptic curve
Encryptie-algoritme	AES256 (CBC/GBC)
Hash	SHA384 of SHA 512
Lifetime	8 uur

4 Vaststelling beleid

Aldus vastgesteld op ..... - ..... - .....

Seretse Nijs
Manager FIA