Den Haag

Tactisch beleid Encryptie

Datum: 09 April 2021

Materieel toepassingsgebied

Dit document beschrijft het tactische beleidskader voor encryptie ten aanzien van toegang tot de digitale gegevens en voorzieningen binnen de gemeente Den Haag (zoals netwerken, systemen en applicaties). Dit document is een uitwerking van het Strategisch Beleidskader Informatieveiligheid Gemeente Den Haag en beschrijft specifiek de principes met betrekking tot de vertrouwde en integere berichtuitwisseling tussen daarvoor geautoriseerde personen en/of systemen, het borgen van onweerlegbaarheid van verzending en ontvangst bij berichtuitwisseling en het vertrouwd kunnen opslaan van bestanden. Tevens worden aanwijzingen gegeven over de beheersing van zowel de operationele- als de beheerprocessen die bij het toepassen van encryptie en Public Key Infrastructuur (PKI) van belang zijn. Het gaat hierbij om de gehele levenscyclus van sleutelmateriaal, van het creëren tot en met het vernietigen van sleutels. Binnen de kaders van dit tactische beleid dienen operationele maatregelen te worden getroffen rondom encryptie door de betrokken applicatie-, proces- of gegevenseigenaren.

Formeel toepassingsgebied

Het beleid is van toepassing op:

- Alle medewerkers van Gemeente Den Haag en externen die werkzaamheden verrichten voor de gemeente en ten behoeve van hun werkzaamheden toegang behoeven tot digitale informatie;
- Alle leveranciers van ICT-voorzieningen van de gemeente die ten behoeve van ondersteuning toegang nodig hebben tot de informatie(-systemen).

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO) v1.04:

- 10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen
- 10.1.2 Sleutelbeheer
- 13.2.3 Elektronische berichten
- 14.1.3 Transacties van toepassingen beschermen
- 18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Doel

Dit document heeft tot doel om verantwoordelijkheden vast te stellen en te waarborgen dat de verschillende aspecten van encryptie zijn ingericht conform de uitgangspunten en maatregeldoelstellingen uit het Strategisch Beleidskader voor informatieveiligheid en de Baseline Informatiebeveiliging Overheid (BIO). Op basis van dit beleid kan een operationele procedure opgesteld worden voor een specifieke gegevensverzameling en/of voorziening.

Indien om stringente redenen afgeweken moet worden van de kaders van dit beleid kan er in overleg met de IA security keten beoordeeld worden of de voorgestelde afwijking goedgekeurd kan worden en voor welke tijdspanne deze afwijking voort kan duren. De beoordeling van de voorgestelde afwijking vind plaats op basis van een expliciete risicoafweging.

De gemeentelijke informatiebeveiligingsbeleidsregels met betrekking tot encryptie en PKI zijn:

1. Cryptografische beheersmaatregelen

Alle gegevens anders dan met classificatie 'geen', worden versleuteld conform beveiligingseisen in de gemeentelijke informatiebeveiligingsarchitectuur:

- Classificatieniveau 'Geen: geen
- Classificatieniveau 'Laag': transportbeveiliging
- Classificatieniveau 'Midden': transportbeveiliging
- Classificatieniveau 'Hoog': transport en berichtbeveiliging

De wijze waarop de bepaling van een classificatie dient plaats te vinden is te vinden in het beleidsdocument "Dataclassificatie Gemeente Den Haag".

Versleuteling vindt plaats conform 'best practices' (de stand der techniek), waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn. Hiervoor wordt gebruik gemaakt van de lijst van open standaarden[1] van het Forum Standaardisatie op basis van 'pas toe of leg uit' .

Intern dataverkeer ('machine to machine') wordt conform classificatie beveiligd met certificaten. Beveiligingscertificaten worden centraal beheerd binnen de gemeente.

Om de informatie met het classificatielabel 'vertrouwelijk' en 'zeer geheim' op verwijderbare media te beschermen, zodat deze informatie niet in onbevoegde handen kan vallen bij onjuist gebruik, verlies of diefstal, dient deze te worden versleuteld.

Om authenticatiemiddelen zoals wachtwoorden te beschermen tegen inzage en wijzigingen door onbevoegden tijdens transport en opslag, dienen deze te worden versleuteld.

Om een correcte en veilige bediening van mobiele (privé-)apparatuur en thuiswerkplek te waarborgen, is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit heeft betrekking op zowel door de gemeente verstrekte middelen, als privé-apparatuur ('bring your own device' (BYOD)). Dit betreft onder meer versleuteling.

Om bedrijfsinformatie op mobiele apparaten te beveiligen zijn deze zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ('zero footprint'). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, wordt de toegang tot het apparaat beschermd door middel van een wachtwoord en is apparaatversleuteling geïmplementeerd (conform classificatie-eisen). Dit gebeurt in ieder geval bij beveiligde opslag van gemeentelijke informatie en bedrijfsinformatie van derde partijen, waar de gemeente niet de bronhouder is, maar via het gemeentelijk platform wordt ontsloten. Als deze informatie al wordt toegestaan op het apparaat.

Voor Clouddiensten (bijvoorbeeld toepassingen in SaaS, O365) geldt dat versleuteling geregeld is op een manier die recht doet aan de gemeentelijke beschermingseisen.

2. Cryptografische normen

Het gebruik van https is verplicht waar van toepassing. Voor veilige berichtenuitwisseling met basisregistraties wordt er gebruik gemaakt van een actuele versie van Digikoppeling. Daarnaast gebruikt de gemeente encryptie conform de PKIoverheid standaard. Dit houdt onder andere in dat de digitale documenten van de gemeente waar burgers en bedrijven rechten aan kunnen ontlenen, gebruik maken van PKIoverheid-certificaten voor tekenen en/of encryptie. Hiervoor wordt de richtlijn PKI van het NCSC voor gevolgd. De gemeente adopteert verder de standaarden uit de Pas Toe of Leg Uit (PTOLU) lijst van het

[1] https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht

Forum voor Standaardisatie. PKIoverheid-certificaten worden verder gebruikt bij:

a) het zetten van een rechtsgeldige elektronische handtekening;
b) het beveiligen van websites;
c) het authenticeren op afstand van personen of services; en
d) het versleutelen van berichten.

3. Sleutelbeheer

Sleutelbeheer/keymanagement is het proces van administratie en beheer van cryptografische sleutels. Dit proces omvat de gehele keten van generen, opslaan, uitwisselen, intrekken en vernietigen van cryptografische sleutels. Voor de uitvoering van het proces omtrent sleutelbeheer worden procedures opgesteld. Sleutelbeheer is binnen de Gemeente Den Haag centraal belegd. Hiervoor is een sleutelbeheerder aangesteld ter bewaking van het proces omtrent sleutelbeheer en dus voor het voor het autoriseren van aanvragen voor certificaten en het muteren, intrekken en verlengen van certificaten.

4. Rollen en verantwoordelijkheden

De proces-/systeemeigenaar is verantwoordelijk voor de naleving van het encryptiebeleid, het bepalen van de classificatie van de in het proces of systeem verwerkte gegevens en draagt zorg voor het juiste niveau van bescherming van de gegevens.

De ISO's ondersteunen bij de uitvoering van een classificatie en adviseert over de te treffen beveiligingsmaatregelen bij een classificatie.

IDC/a is verantwoordelijk voor het beschikbaar stellen van de kennis en technologie ter ondersteuning van de uitvoering van het encryptiebeleid.

Gebruikers dienen bewust te zijn van het vertrouwelijkheidsniveau van de informatie en het encryptiebeleid en te handelen naar het beleid.

De CISO is verantwoordelijk voor de controle op het beleid en een controle op een juiste uitvoering van het beleid door de gemeente (Beleidscontrole). De CISO kan hiertoe een auditor opdracht geven. Op halfjaarlijkse basis wordt er in opdracht van de CISO een controle uitgevoerd op het juiste gebruik van certificaten.

Op jaarbasis onderzoekt Forum Standaardisatie op welke wijze er wordt omgegaan met het 'pas toe of leg uit'-beleid voor open standaarden. Hierbij wordt gemeten in hoeverre de PTOLU-beleid gebruikt wordt in aanbestedingen en in hoeverre relevante verplichte standaarden gebruikt worden in gemeentelijke voorzieningen.

Jaarlijks dient de beoordeling van dit beleid plaats te vinden, door een onafhankelijke partij, die gespecialiseerd is in informatiebeveiliging. Tussentijdse controles kunnen plaatsvinden door de interne accountantsdienst van de gemeente zelf. De bevindingen en verbeteringen zijn onderdeel van de jaarlijkse controle door een onafhankelijke partij.