Dutch Delta Group B.V.
Kerkenbos 1075 A
6546 BB Nijmegen
088-9109101
info@dutchdeltagroup.nl
www.dutchdeltagroup.nl

KvK 09196799

Nijmegen, 25 mei 2021

Onderwerp: Brochure Certificatenbeheer

Geachte L.s,

Wij danken u voor de getoonde interesse in onze dienst Certificatenbeheer.

Mocht u meer informatie wensen of een offerte, dan kunt u contact opnemen met Michaël Leushuis via telefoonnummer 06-10134178 of via e-mail michael.leushuis@dutchdeltagroup.nl.

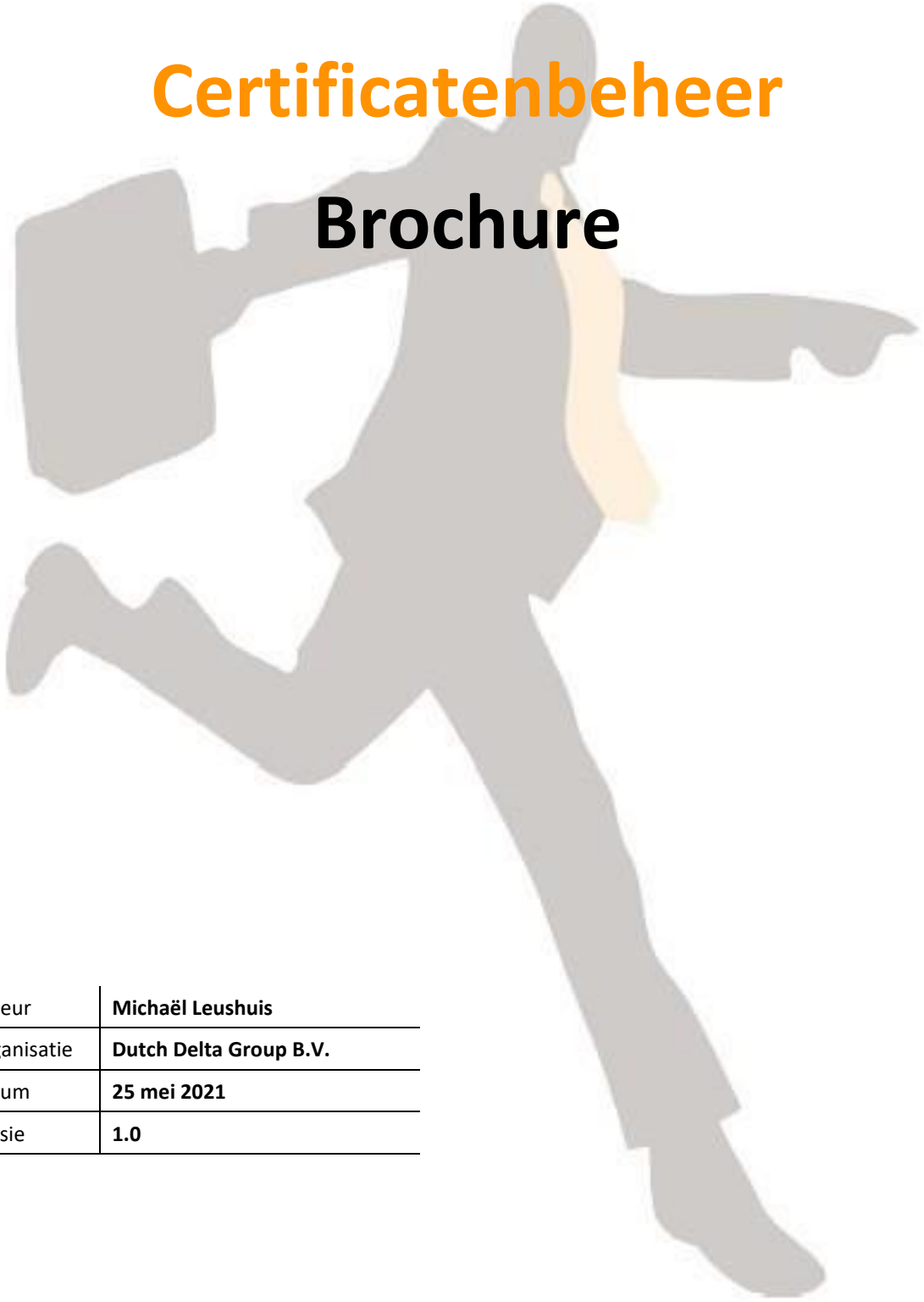
Met vriendelijke groeten,

Dutch Delta Group B.V.

Michaël Leushuis
Commercieel Manager

Certificatenbeheer

Brochure



Auteur	**Michaël Leushuis**
Organisatie	**Dutch Delta Group B.V.**
Datum	**25 mei 2021**
Versie	**1.0**

1. DE AANLEIDING

1.1 Eén overheid, één Baseline voor Informatieveiligheid (BIO)

Rijk, gemeenten, provincies en waterschappen gebruiken **per 1 januari 2020** één uniform normenkader voor informatiebeveiliging; één overheid, één Baseline voor informatieveiligheid. Wat ervoor zorgt dat bestuurders meer grip en inzicht hierin verkrijgen.

"Informatieveiligheid moet in het gemeentelijk DNA" betoogt de IBD. Informatieveiligheid is een harde voorwaarde voor een professionele gemeente. Samenwerkende Nederlandse overheden maken steeds meer gebruik van (elkaars) informatie, ICT en netwerken. Dat vraagt om het impliciet en expliciet kunnen vertrouwen op die informatie, ICT en netwerken: het eist van alle partners een uitmuntende informatiebeveiliging.

Uit publicaties van de informatiebeveiligingsdienst voor gemeenten (IBD) blijkt dat informatiebeveiliging verder gaat dan alleen ICT en de ICT-afdeling. Beveiliging van gegevens en systemen is een zaak van de hele gemeentelijke organisatie. Het gaat dus ook:

- Om de medewerkers en de manier waarop zij met risico's omgaan;
- Om het inrichten van processen en procedures;
- Om kennis en bewustzijn;
- (En in de laatste plaats) om techniek.

Of de dreiging nu komt van een onbewuste medewerker, een criminele organisatie of een stroomstoring: de technische en organisatorische maatregelen om schade te voorkomen, te beperken en te vermijden zijn hetzelfde.

Het beheersen en managen van risico's is de basis van een goede informatiebeveiliging, ofwel:

Informatiebeveiliging = Risicomanagement.

1.2 Gemeentelijke organisaties agenderen informatieveiligheid

De IBD geeft aan dat informatieveiligheid een vaste plaats op de gemeentelijke, bestuurlijke agenda moet hebben. Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dit te realiseren zijn de volgende principes volgens de IBD essentieel:

- Bestuurders bevorderen een veilige cultuur
- Informatiebeveiliging is van iedereen
- Informatiebeveiliging is risicomanagement
- Risicomanagement is onderdeel van de besluitvorming
- Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
- Informatiebeveiliging is een proces
- Informatiebeveiliging kost geld
- Onzekerheid dient te worden ingecalculeerd
- Verbetering komt voort uit leren en ervaring
- Het bestuur controleert en evalueert.

De 5 onderkende risico's

Echter, zijn er een aantal risico's die een goed beveiligde informatieomgeving in gevaar brengen. Er is daarom ook grondig onderzoek verricht naar deze risico's (Bron: IBD Dreigingsbeeld 2021/2022). Uit het onderzoek kan

deconclusie getrokken worden dat een 5 aantal belangrijke risico's zijn voor de Nederlandse gemeenten in 2019:

- **Informatiebeveiliging heeft een imagoprobleem.**
  Het staat laag op de politieke agenda, er is weinig bewustzijn en onvoldoende budget.
- **Risico's zijn niet integraal in beeld.**
  De risico's die wel in beeld zijn, krijgen bovenmatig veel aandacht.
- **De basis is niet op orde.**
  Met als gevolg dat simpele routine-aanvallen vaak succesvol zijn.
- **Te weinig mensen.**
  Er is te veel werk voor te weinig gekwalificeerde medewerkers en specialisten
- **De complexiteit neemt toe en blijft toenemen.**
  Gemeenten zien kansen in innovatie en nieuwe ontwikkelingen, maar niet de bijbehorende risico's.

Wil je als gemeente werk maken van het verbeteren van je informatieveiligheid dan vraagt dat om het stellen van prioriteiten die de bovengenoemde 5 belangrijkste risico's aantoonbaar verkleinen:

- **Zet informatiebeveiliging op de agenda**
  Zorg ervoordat informatiebeveiligingaandachtkrijgtconform'de10principes'die in paragraaf 1.2 zijn vermeld.
- **Breng de basis op orde!**
  Verhoog de digitale weerbaarheid van uw gemeente.
- **Versterk de menselijke schakel.**
  Bewuste medewerkers zijn de beste beveiligingsmaatregel.
- **Versterk de rol en functie van de Chief Information Security Officer (de CISO).**
  En stel uw CISO in staat om u optimaal te kunnen adviseren.
- **Verwerf inzicht in nieuwe technologieën.**
  En pas *security- & privacy- by-design*-principes toe.

Dooralsgemeenteactiefaandeslagtegaanmetdezeprioriteitenwerkjeeraan'incontrol' tekomenop risicomanagement en dus informatieveiligheid. Dat is belangrijk, niet alleen om negatieve nieuwsberichten te voorkomen, maar ook om aan diverse verplichtingen te voldoen: in het kader van interne en externe verantwoording en audits aantoonbaar te voldoen aan wet-, regelgeving en normen.

De Eenduidige Normatiek Single Information Audit (ENSIA) die tot doel heeft het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren, is een van de initiatieven om gemeenten te helpen zicht te krijgen op alle verschillende normen, regels en verplichtingen. Dit gebeurt door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen. De uitgave van de Baselinetoets Beveiligings Niveau (BBN) Baseline Informatiebeveiliging Overheid (BIO[1]) kan daarbij als leidraad dienen en als toetsmiddel.

De organisatorische gevolgen en inbedding van risicomanagement, informatieveiligheid, auditnormen, zichtbaarheid en bestuurlijke aandacht zijn voor veel gemeenten pittige vraagstukken. Die al veel van de aanwezige denk- en arbeidskrachten opsouperen. Hoe kun je dan slim en effectief ook in de dagelijkse uitvoering van werkzaamheden stappen zetten? Welke activiteiten of dienstenvan derdenhelpenjedirect'in control' tekomen?

[1] Baseline Informatiebeveiliging Overheid (BIO) is per 1 januari 2020 de opvolger van Baseline Informatiebeveiliging voor Gemeenten (BIG)

2. DIENSTVERLENING DDG OM 'IN CONTROL' TE KOMEN

2.1 De basis op orde brengen

Dutch Delta Group (DDG) is gespecialiseerd in het pragmatisch ondersteunen van gemeenten bij functionele-, technische vraagstukken en werkzaamheden. Onze eerste bijdrage in uw gemeente is uw gemeente te ondersteunen bij het prioriteitsitem **'De basis op orde'.**

Volgenshet Center for Internet Security (CIS) begintdiebasis meteenvijftal 'CIS-Controls'. Datzijn vijf maatregelen die consequent en continu genomen dienen te worden:

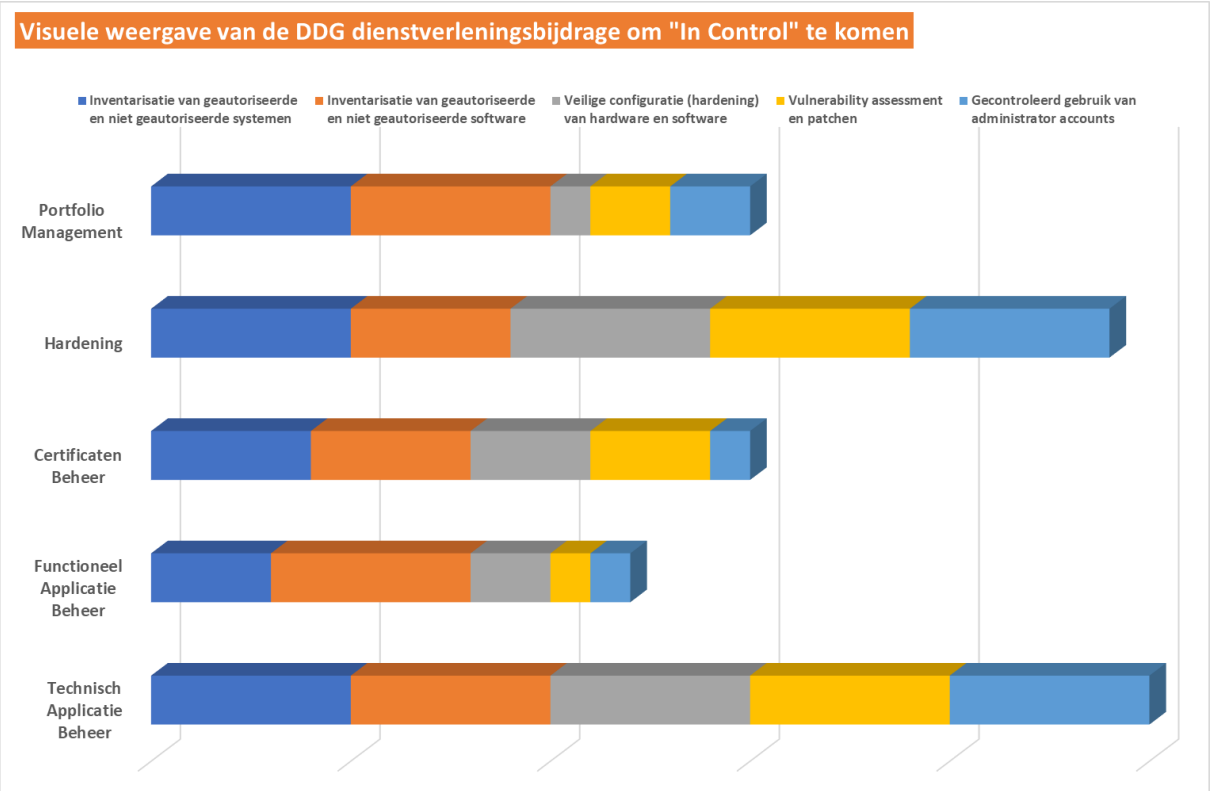
- Inventarisatie van geautoriseerde en niet geautoriseerde systemen.
- Inventarisatie van geautoriseerde en niet geautoriseerde software.
- Veilige configuratie (hardening) van hardware en software.
- Vulnerability assessment en patchen.
- Gecontroleerd gebruik van administrator accounts.

Wanneer deze vijf maatregelen succesvol worden ingevoerd én structureel onderhouden, dan biedt dat al een bescherming tegen zo'n **85%** van de meest gebruikelijke cyberaanvallen. De implementatie kan complex en tijdrovend zijn en daarom biedt DDG bij ieder van deze maatregelen zijn specialisme aan.

De volgende DDG-diensten dragen bij aan het realiseren van de 'CIS Controls':

- **Technische Applicatie Beheer**
  - Release Management (onafhankelijk van applicatieleverancier)
  - Dagelijks Technisch Systeembeheer
  - Monitoring 24/7
  - Database Beheer
  - Uitwijk- en Testfaciliteiten
  - Migraties
- **Functioneel Applicatie beheer**
  - Burgerzaken, Datadistributie, Financiën, Sociaal Domein en Omgevingswetgeving (2022)
  - Kwaliteit van gegevens
  - Functioneel Voor- en Nawerk
  - Gegevensmanagement
  - Autorisatie
- **Certificatenbeheer**[2]
  - Inventariseren
  - Beheren
- **Hardening**
  - Servers, Databases, Werkplekken en Telefoons
  - Vulnerability scans
  - Patchwerk
- **Portfoliomanagement**
  - Application- en Infrastructure Portfoliomanagement
  - Interfaces
  - Contractmanagement

[2] Deze dienst wordt in deze brochure beschreven.



Hoe groter de horizontale balk is, hoe meer de geboden dienst bijdraagt aan het “In Control” komen.

3. CERTIFICATENBEHEER

3.1 Beschrijving van dienstenpakket Certificatenbeheer

Een decennia geleden hadden we binnen het gemeentelijk ICT-landschap enkele PKI-certificaten in gebruik. Dat was te overzien en de certificaatverstrekker gaf ruim voor tijd ook een signaal af wanneer het certificaat dreigde te verlopen, moest je wel de contactgegevens actueel hebben! In het huidige ICT-landschap is het inmiddels een wirwar geworden aan certificaten met diverse verstrekkers, een overzicht en gecontroleerd beheer is noodzakelijk geworden.

Het DDG-dienstenpakket Certificatenbeheer valt uiteen in 2 fasen:

- Fase 1 (Inventarisatiefase)
- Fase 2 (Beheerfase)

3.1.1 CERTIFICATENBEHEER FASE-1: DE INVENTARISATIEFASE

Het doel van de inventarisatiefase is:

- **Inzicht verkrijgen** om hoeveel certificaten het gaat binnen het ICT-landschap van uw gemeente;
- **Verzamelen van alle benodigde informatie**, voor het bewaken van de verloopdatums van certificaten, zodat de gemeente weet wanneer ze in actie moet komen om de geldigheid van het certificaat te verlengen of het certificaat compleet te vervangen; In het laatste geval is het ook handig om te weten welkeachterliggende Collaboration Protocol Agreements (CPA’s) medevervangen moeten worden;

- **Vaststellen bedrijfskritische certificaten**, die onderdeel zijn van belangrijke interfaces tussen applicaties of mogelijke keten(s);
- **Beheerimpact bepalen** om de aanwezige certificaten op een gestructureerde wijze te kunnen organiseren binnen uw gemeente.

Het eindproduct van de inventarisatiefase is:

- DDG levert een CSV-bestand aan waarin alle gevonden certificaten staan geregistreerd. Dit doen wein een CSV-bestand zodat de gemeente het bestand eventueel kan uploaden naar haar eigen monitoringsysteem of CMDB-systeem. Het CSV-bestand bevat de volgende attributen:
    - Common naam van het certificaat;
    - Datum geldig tot;
    - Type certificaat;
    - Applicatie(s) waarin het certificaat wordt gebruikt;
    - Verbindingen waarin het certificaat wordt gebruikt;
    - Contactpersoon bij de gemeente die eigenaar is van de verbinding, de applicatie of het werkproces waarin het certificaat een rol speelt;

Wat verwachten wij van de gemeente tijdens de inventarisatiefase:

- DDG voert het beheer van applicatieomgevingen onder contract uit bij meer dan 130 gemeenten. De applicatieomgevingen zijn divers en geleverd door verschillende applicatieleveranciers. Veel certificaten zijn door onze tool te vinden. Handmatig moeten we certificaten ook terugvinden binnen een applicatieomgeving zelf. Grotendeels weten we ze wel te traceren maar we ontkomen er niet aan dat we toch de hulp nodig hebben van de systeem-, technische- en functionele applicatiebeheerders van de gemeente;
- Hetzouonsveeltijdschelenalsuwgemeentereedsinhetbezitisdezogenaamde“plaat”vanhet applicatielandschap van uw gemeente. Mogelijk heeft u een up to date GEMMA-softwarecatalogus overzicht of uw gemeente maakt al gebruik van een managementsysteem waarmee infrastructuren en/of application Portfoliomanagement is vastgelegd[3];
- Om toegewezen eigenaren te kunnen koppelen aan bepaalde certificaten willen we hen graag kort interviewen.;
- Sommige werkzaamheden zal DDG op afstand uitvoeren (remote). Wij willen uw gemeente dan ook graag verzoeken ons een veilige inbelvoorziening te leveren. DDG geeft zelf de voorkeur aan een beveiligde Teamviewer sessie.

Wat is de doorlooptijd van de inventarisatiefase:

Gemiddeld genomen is de doorlooptijd ongeveer 2 weken. In deze 2 weken worden diverse activiteiten remote en op locatie van uw gemeente door DDG uitgevoerd. De werkzaamheden die wij op ons nemen staan hieronder opgesomd en worden met uw gemeente afgestemd:

- Automatische inventarisatie, hiervoor gebruiken wij een tool;
- Handmatige inventarisatie, hierbij is ondersteuning noodzakelijk van uw systeem-, technische- en functionele applicatiebeheerders;
- Interviews met de diverse genoemde functionarissen binnen uw gemeente ten behoeve van het achterhalen hoe zij het vervangingsproces geregeld hebben tot dusverre;
- Schikken van alle informatie in ons registratiesysteem;
- Opleveren van de eerste versie van het CSV-bestand;

[3] DDG heeft dienstverlening hiervoor ontwikkeld waarmee wij gemeenten kunnen ondersteunen. Wenst u meer informatie hierover, stuur dan een mail naar info@dutchdeltagroup.nl

- Resultaat bespreken met de betrokken functionarissen waaronder de CISO en/of FG, mogelijke wijzigingen worden nog aangebracht waarna we het definitieve CSV-bestand opleveren.

3.1.2 CERTIFICATENBEHEER FASE-2: DE BEHEERFASE

In deze brochure kunnen we nog niets roepen over de maandelijkse kosten die DDG voor deze dienst zal vragen. Dat heeft enkele redenen:

- Mogelijk gaat uw gemeente zelf het beheren van de certificaten uitvoeren als het aantal bekend is en de impact van het beheer binnen uw eigen gemeente zelf is te behapstukken. Waarom zou je uitbesteden als voldoende kennis, kunde en capaciteit aanwezig is?;
- DDG hanteert een staffel bij het bepalen van de kosten. Het gaat om het aantal tebeheren certificaten. Het aantal is pas bekend bij de afronding van fase-1;
- Stel dat uw gemeente het beheer gaat uitbesteden dan moet nog bepaald worden welk dienstniveau wordt afgenomen. DDG kent diverse dienstniveaus bij het beheren van de certificaten:
    - **Dienstniveau-1**. Alleen alerts worden naar de gemeente doorgezet. De handeling[4] en installatie[5] doet uw gemeente zelf. De DDG Service Desk kan daarbij eventueel ondersteuning leveren;
    - **Dienstniveau-2**. We zetten de alert door naar uw gemeente. DDG maakt de CSR aan. De gemeente verricht de rest van de handeling en wij voeren de installatie uit met ondersteuning van uw gemeente;
    - **Dienstniveau-3**. DDG geeft de alerts af aan uw gemeente. DDG maakt de CSR aan. De gemeente verricht de rest van de handeling en wij doen de installatie geheelzelfstandig uitvoeren;
    - **Dienstniveau-4**. DDG doet alles. We leveren de alerts, doen de handeling en voeren de installatie uit.

In bijlage-1 hebben wij bovenstaande dienstniveau's grafisch weergegeven ter verduidelijking. In bijlage-2 hebben wij een voorbeeldrapportage toegevoegd.

Verdere uitwerking van de genoemde dienstniveaus leveren we op zodra we offerte mogen uitbrengen van het Certificatenbeheer Fase-2. Is het aantal certificaten binnen uw gemeente al bekend en de behoefte bestaat om het Certificatenbeheer uit te besteden, dan horen we dat graag van u. U kunt een offerte aanvragen door een mail te sturen naar info@dutchdeltagroup.nl.

[4] De handeling bestaat uit de volgende activiteiten:
- CSR aanmaken;
- Contact opnemen met de Certificaat Autoriteit (CA) voor het aanvragen van een nieuwe digitale ondertekening;
- Overdracht van de CSR aan de CA;
- Ontvangst en registratie van het ondertekende certificaat.

[5] De installatie bestaat uit de volgende activiteiten:
- Het publieke en private deel van het certificaat importeren in de applicatie, server of hardware;
- Het publieke deel van het certificaat distribueren naar de desbetreffende aangesloten partijen.

4. UW VOORDELEN

Het organiseren van het Certificatenbeheer start met de eerste fase. DDG hoopt deze voor u te mogen uitvoeren. Het brengt de volgende voordelen met zich mee:

- U voldoet aan de BIG eis 12.3 Crypto grafische beheersmaatregelen (vanaf 1 januari 2020 geldt BIO eis -10.1), namelijk:
  - Binnen de gemeente moet beleid gerealiseerd worden voor het gebruik van cryptografische beheersmaatregelen;
  - Sleutelbeheer moet ingeregeld zijn;
- De kans op ongewenste storingen bij belangrijke functionaliteiten neemt aanzienlijk af doordat vervangen van de certificaten voorspelbaar is geworden. Vroegtijdig wordt gesignaleerd wanneer certificaten verlopen en kunnen daarom tijdig vervangen worden;
- U brengt de basis op orde. In het IBD Dreigingsbeeld 2019/2020 staat vermeld dat gemeenten "de basis van haar ICT" niet op orde hebben. Volgens het Center for Internet Security (CIS) begint die basis met een vijftal "CIS-Controls":
  1) Inventarisatie van geautoriseerde en niet geautoriseerde systemen;
  2) Inventarisatie van geautoriseerde en niet geautoriseerde software;
  3) Veilige configuratie (hardening) van hardware en software;
  4) Vulnerability assessment en patchen;
  5) Gecontroleerd gebruik van administrator accounts;

  DDG ondersteunt u bij deze CIS- Controls.

BIJLAGE-1 GRAFISCHE WEERGAVE DIENSTNIVEAU'S

Activiteit		Dienstniveau			
		1	2	3	4
Alert	Signaleren wanneer een certificaat gaat verlopen	DDG	DDG	DDG	DDG
Handeling	CSR aanmaken		DDG	DDG	DDG
	Contact opnemen met Certificaat Autoriteit (CA) voor het aanvragen van een nieuw digitale ondertekening				DDG
	Overdracht van de CSR aan de CA				DDG
	Ontvangst en registratie van het ondertekende certificaat				DDG
Installatie	Het publieke en private deel van het certificaat importeren in de applicatie, server of hardware		DDG i.s.m. gemeente	DDG	DDG
	Het publieke deel van het certificaat distribueren naar de desbetreffende aangesloten partijen		DDG i.s.m. gemeente	DDG	DDG

BIJLAGE-2 VOORBEELDRAPPORTAGE CERTIFICATENBEHEER

AFGELOPEN PERIODE

Omschrijving	*Aantal*
Aantal certificaatmeldingen binnengekomen	*3*
Aantal certificaatmeldingen openstaand (in behandeling)	*2*
Aantal certificaatmeldingen afgehandeld	*1*

TOPdesk id	Datum/tijd	Status	Monitoring melding	Opvolging door DDG
DDG-I1901 095	11-01-2019 09:27	Open	Certificaat IOB01MSN.Corp.Gemeente.local van RO en type MKS-Publiek vervalt binnen 90 dagen. Het certificaat verloopt op 11-Mrt-19 09:40:40	De change 'Signed PKI certificate vervangen' is gestart en is in behandeling in DDG-W1901 314. Verwachte implementatiedatum: 31-01-2019.
DDG-I1901 013	01-01-2019 12:20	Gereed	Certificaat PRT121 van PRT121 en type Scan vervalt binnen 90 dagen. Het certificaat verloopt op 16-Feb-15 00:00:00	De change 'Self-signed certificate' is uitgevoerd in DDG-W1901 017 en is voltooid.
DDG-I1901 120	13-01-2019 09:27	Open	Certificaat APP01MSN.Corp. Gemeente.local van APP01MSN.Corp. Gemeente.local en type Scan vervalt binnen 90 dagen of is reeds vervallen. Het certificaat verloopt op 30-Mrt-17 00:00:00	De change 'Signed PKI certificate vervangen' is gestart en is in behandeling in DDG-W1901 403. Verwachte implementatiedatum: 31-01-2019.

Samenvatting afgelopen periode

Er zijn geen bijzonderheden te melden. Het aantal certificaatmeldingen en de afhandeling daarvan past bij een normaal, gemiddeld verloop van certificaten over het jaar.

PROGNOSE

Certificaten die binnen nu en 6 maanden zullen vervallen.

Koppeling	Certificaat common name	Verloopdatum	Applicatie(s)	Contactpersoon
kpnpkioverheidorganisatiecag2	KPN PKIoverheid Organisatie CA - G2	23-06-19	Key2Percelen	dhr. H. Landmeter
lap_bcgba_idm_diginetwerk_net	lap.bcgba.idm.diginetwerk.net	16-08-19	MKS, Cipers, BCGBA	mevr. B. Burgerzaken
lap_bvbsn_idm_diginetwerk_net	lap.bvbsn.idm.diginetwerk.net	16-08-19	MKS, Cipers, BVBSN	mevr. B. Burgerzaken
lap_gbav_idm_diginetwerk_net	lap.gbav.idm.diginetwerk.net	16-08-19	MKS, Cipers, GBA-V	mevr. B. Burgerzaken