Gemeente Amstelveen

Baseline websites, e-mail & domeinregistratie

Auteur(s): Erik Kamminga
Afdeling: ICT Infrastructuur
VERSIE: 1.7

Versie geschiedenis

Versie	Datum	Omschrijving wijziging	Status	Door
1.0	10 oktober 2018	Eerste oplevering	Vastgesteld: met aanvulling: • Voor hoog geclassificeerde informatie (persoonsinformatie en vertrouwelijke informatie) geldt deze baseline in alle gevallen • Op basis van dataclassificatie kan de gemeente afwijken van de A+ eis. • Daarnaast is het verzoek om ook het SFTP protocol en eventueel andere protocollen (in later stadium) toe te voegen aan dit document	EKA
1.1	12 december 2018	Toevoegen aanvulling tijdens vaststelling		EKA
1.2	9 mei 2019	Aanpassing inleiding. Aanpassing overige eisen. Aanpassing Cipher Suites. https://www.htbridge.com/ssl/ is gewijzigd in: https://www.immuniweb.com/websec/ BIG wordt met ingang van 1-1-2020 BIO.	23-5-2019 Opnieuw vastgesteld	EKA
1.3	9 januari 2020	Gehele herziening op basis van 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0'	29-01-2020 Opnieuw vastgesteld	EKA
1.4	11 augustus 2020	Herziene versie met verwijzing naar 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' i.c.m. onze eisen m.b.t. status niveau. Naamwijziging van het document Toevoeging van: Domein registratie; DNSSEC; IPv6; DMARC/DKIM	26 augustus 2020 Opnieuw vastgesteld.	EKA
1.5	21 januari 2021	Aanpassing op basis van de nieuwe 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.1'		EKA
1.6	14 februari 2022	Aanpassing Categorisering. Toevoegen bestand zijn tegen Log4J kwetsbaarheid. Extra eis toegevoegd aan punt 2.4 Aanpassing hoofdstuk 6 Certificaten i.v.m. eindigen van PKI-Overheid Certificaten voor Websites. Toegevoegd beëindigen websites.		EKA
1.7	24 augustus 2023	Aanpassing aan huidige eisen	12-10-2023 Opnieuw vastgesteld in MT A&I	EKA

Inhoudsopgave

1.0 Inleiding

De gemeenten Amstelveen & Aalsmeer (AA) hechten aan de veiligheid van informatie en het volgen van privacyregels. AA hanteert hierbij de uitgangspunten zoals gesteld in de Baseline Informatiebeveiliging Overheid (BIO) en aanvullende regelgeving zoals https://www.forumstandaardisatie.nl/thema/veilig-internet, https://www.forumstandaardisatie.nl/open-standaarden/verplicht, wet SUWI, DigiD, enz. en daarnaast voorwaarden die de Algemene Verordening Gegevensbescherming (AVG) stelt aan de verwerking van persoonsgegevens, als ook 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.1', of nieuwer, van https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1

1.1 Voor een veilige digitale overheid

Sinds 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. Het gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normen. Helder, actueel en veilig.
De AA-gemeenten hebben op gebied van websites een operationele uitwerking gemaakt van deze leidende wet- en regelgeving en hierbij gebruik gemaakt van de adviezen en uitwerkingen van de Informatiebeveiligingsdienst (IBD), het Nationaal Cyber Security Centrum (NCSC) en de beschikbare testtools van SSL Labs, internet.nl, MXtoolbox en Immuniweb. De onderstaande operationele uitwerking vormen de minimale eisen die aan websites worden gesteld. Dit document zal periodiek worden aangepast om mee te gaan met de nieuwe security-vereisten.

2.0 Eisen

2.1 Algemeen

- Websites waar de gemeente iets laat hosten inclusief de bijbehorende mailservers en domeinen moeten naast de onderstaande eisen, voldoen aan de richtlijnen van het NCSC zoals beschreven in het document 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.1.1' of de opvolger daarvan. Hierbij moet worden voldaan aan de status van de betreffende beveiligingsmaatregel zoals vermeld in onderstaande tabel. Wanneer de eisen door het NCSC worden aangescherpt zal de webserver zo nodig moeten worden aangepast aan de nieuwe eisen, om ook in de toekomst een veilige en betrouwbare site te hebben. De genoemde eisen gelden ook voor sites waar geen certificaat van de AA-gemeenten op zit, maar waarbij WEL een DPIA verplicht is vanwege de hoge risico's bij de verwerking van persoonsgegevens. Hierbij geldt dan het pas-toe-of-leg-uit principe. Ook moet worden voldaan aan nieuwe en/of aangepaste eisen in dit document. Dit dient zo snel mogelijk na wijziging plaats te vinden, maar tenminste binnen:

Categorie website	3) Websites waar uitsluitend informatie wordt verstrekt en geen formulieren kunnen worden ingevuld.	2) Alle overige websites zonder DigiD, eIDAS, iDIN of eHerkenning	1) Alle overige websites met DigiD, eIDAS, iDIN of eHerkenning
Minimale status	Uit te faseren	Voldoende *4)	Goed & Voldoende *4)
Aanpassen website bij terugval naar lagere waardering	Bij terugval naar **Onvoldoende** moet de website binnen **Zes** maanden teruggebracht worden naar MINIMAAL het niveau **Uit te faseren.**	Bij terugval naar **Uit te faseren** moet de website binnen **Zes** maanden teruggebracht worden naar MINIMAAL het niveau **Voldoende.** Bij terugval naar **Onvoldoende** moet de website binnen **Drie** maanden teruggebracht worden naar MINIMAAL het niveau **Uit te faseren.** En binnen **Zes** maanden naar **Voldoende.**	Bij terugval naar **Uit te faseren** moet de website binnen **Drie** maanden teruggebracht worden naar MINIMAAL het niveau **Voldoende.** Naast onderdelen op niveau **Voldoende** moeten ook onderdelen van niveau goed beschikbaar zijn. Bij terugval naar **Onvoldoende** moet de website binnen **Een** maand teruggebracht worden naar MINIMAAL het niveau **Voldoende** Naast onderdelen op niveau **Voldoende** moeten ook onderdelen van niveau goed beschikbaar zijn.

Het betreft hier sites waarvan de gemeente domeineigenaar/opdrachtgever is van de gebruikte URL. Dus ook bij gebruik van een CNAME.

- De partij die de website host of laat hosten is zelf verantwoordelijk voor het in de gaten houden van wijziging van de normen. De gemeente zal wekelijks een test uitvoeren op de in dit document genoemde eisen.
- De partij die het domein host of laat hosten waar de gemeente domeinhouder van is, dient de gemeente in staat te stellen om een PEN-TEST/Vulnerability-scan uit te laten voeren door een derde partij & de scanner van de gemeente zelf. Deze scanner van de gemeente heeft een werking die vergelijkbaar is met *Internet.nl*. Deze testen hebben slechts tot doel om kwetsbaarheden te achterhalen en zijn uitdrukkelijk GÉÉN performance tests die de hosting zouden kunnen verstoren. Eventuele gevonden kwetsbaarheden zullen aan de partij die de website host of laat hosten worden gemeld en dienen binnen de in de bovenstaande tabel genoemde tijd opgelost te worden. Deze testen dienen op alle systemen te kunnen worden uitgevoerd, dus naast Productie ook op ontwikkel-, test- en acceptatie-systemen. Als alternatief voor de PEN-TEST/Vulnerability-scan kan de gemeente in overleg ook akkoord gaan met een verklaring, door een externe auditor die aantoont dat de website aan de door de gemeente gestelde normen voldoet.
- Voor hoog geclassificeerde informatie (BIV classificatie) geldt deze baseline in alle gevallen. Deze classificatie is gebaseerd op het document "Gemeentebreed informatieveiligheidsbeleid" van de Gemeente Amstelveen & Aalsmeer.
- Op basis van dataclassificatie kan de gemeente in uitzonderingsgevallen afwijken van de gestelde eisen. (MT-besluit)
- Deze eisen zijn ook van toepassing op sites met SFTP, FTPS en SSH.
- De verplichte 'Pas toe leg uit' standaarden op de website https://www.forumstandaardisatie.nl/open-standaarden/verplicht?trefwoord=All zijn **verplicht** en kunnen dus **niet** worden **uitgelegd**.
- Voor TLS versies & Cryptografsche algoritmes zijn zowel niveau Goed als Voldoende verplicht bij Categorie 1) websites, ziet tabel bij punt 2.1. Dus zowel TLS1.2 als TLS1.3 en de bijbehorende Cryptografsche algoritmes!

2.2 Protocollen, algoritmes, hashfuncties, sleutels, elliptische krommen etc. die ondersteund moeten/mogen worden

Zie https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1 voor de actuele versie en de tabel in punt 2.1 van dit document voor de vereiste status van de maatregel.

2.3 De Server moet beschermd zijn tegen:

- DROWN
- BEAST attack
- POODLE (SSLv3)
- POODLE (TLS)
- Zombie POODLE
- GOLDENDOODLE
- OpenSSL 0-Length
- Sleeping POODLE
- Downgrade attack prevention
- SSL/TLS compression
- RC4
- Heartbeat (extension)
- Heartbleed (Vulnerability)
- Ticketbleed (Vulnerability)
- OpenSSL CCS Vulnerability (CVE-2014-0224)
- OpenSSL Padding Oracle Vulnerability (CVE-2016-2107)
- ROBOT (Vulnerability)
- De Log4J kwetsbaarheid
- overige bekende kwetsbaarheden

2.4 Overige eisen

- ALLE websites moeten beveiligd zijn met de standaarden HTTPS en HSTS welke per 1 juli 2023 wettelijke verplicht zijn conform https://www.forumstandaardisatie.nl/open-standaarden/https-en-hsts en TLS conform de richtlijnen van het Nationaal Cyber Security Centrum (NCSC) met in achtneming van de tabel van punt 2.1.
- Strict Transport Security (HSTS) is verplicht! Minimale duur van 1 jaar (31536000).
- "Perfect Forward Secrecy" (PFS) moet worden ondersteund
- De server moet op de juiste wijze een http redirect naar https bieden (.HTTP/1.1 301 Moved Permanently)
- De server mag geen "client-initiated secure renegotiation" ondersteunen. Deze eis is opgenomen om DoS-attacks te voorkomen.
- De server moet "secure server-initiated renegotiation" ondersteunen.
- De server moet de "cipher suites preference" afdwingen. Hierbij moeten de betere sleutels de voorkeur krijgen. Dus de beste sleutel die zowel client als server ondersteunen moet worden afgedwongen.
- Websites die onderdelen van een andere website afhalen zoals afbeeldingen, scripts etc. dienen er tevens voor de zorgen dat ook deze sites aan de in dit document genoemde eisen voldoen.

2.5 Site-to-Site VPN

Voor het gebruik van een Site-to-Site VPN hanteren we de volgende instellingen:

2.5.1 Phase 1

- Mode: IKEv2
- DH Group Identifier: Group 21 en indien niet mogelijk Group 20
- Encryption algorythm: AES-256-GCM
- Hash: SHA384
- Lifetime: 28800
- PSK: Uitwisseling via SMS/Whatsapp
- Eisen PSK: minimaal 16 tekens, 1 hoofdletter, 1 speciaal karakter, 1 cijfer.

2.5.2 Phase 2

- Perfect Forward Secrecy enabled: Ja
- Perfect forward secrecy (PFS): Group 21 en indien niet mogelijk Group 20
- Protocol: ESP
- Encryption algorythm: AES-256-GCM
- Hash: SHA384
- Lifetime: 28800

2.6 Security.txt

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

# Domeinen van Amstelveen, Aalsmeer & gemeentebelastingenamstelland
# kunnen met een 302 redirect verwijzen naar het centrale bestand op
# https://www.amstelveen.nl/.well-known/security.txt
# omdat het Amstelveen het centrale meldpunt is voor kwetsbaarheden en incidenten
# voor de alle domeinen van de AA-Organisatie.

Expires: 2024-08-24T12:00:00.000Z
Canonical: https://www.amstelveen.nl/.well-known/security.txt

Policy: https://www.amstelveen.nl/bestuur-organisatie/publicatie/informatieveiligheid-en-pri-
vacy_coordinated-vulnerability-disclosure

Contact: https://www.amstelveen.nl/bestuur-organisatie/publicatie/informatieveiligheid-en-pri-
vacy_coordinated-vulnerability-disclosure
Encryption: https://www.amstelveen.nl/contact/pgp-key
Preferred-Languages: nl, en
-----BEGIN PGP SIGNATURE-----

iHUEARMIAB0WIQQh5ZKwLyKU56+sJtk/MvHbtL8RAwUCZOc78AAKCRA/MvHbtL8R
A6kOAQCpdykdezLTTJdSIZvqOQIBJheRBx/QbRsSoHqpm3dfQAD/SRLhzTu7mCiD
7bm23WVuYET5wTSerul28pLmXQi8sFA=
=0sf0
-----END PGP SIGNATURE-----
```

2.7 RPKI

RPKI Resource Public Key Infrastructure is verplicht conform https://www.forumstandaardisatie.nl/open-standaarden/rpki

3.0 Domein registratie

Op dit moment worden de domeinen van de gemeenten Amstelveen & Aalsmeer, alsmede gemeentebelastingenamsteland bij twee verschillende registrars ondergebracht. ALLE domeinen van de gemeente worden door de gemeenten zelf geregistreerd. (aanvraag via Self Service Portal).

3.1 Hoofd domeinen

- Amstelveen.nl
- Aalsmeer.nl
- Gemeentebelastingenamstelland.nl

Deze genoemde domeinen zijn ondergebracht bij KPN Lokale Overheid.

3.2 Overige domeinen

De overige domeinen zijn ondergebracht bij VDX. Alle nieuwe domeinen zullen bij VDX worden ondergebracht.

3.3 DNSSEC

Conform de regels die gelden voor de overheid zijn al onze domeinen voorzien van DNSSEC.
Een CNAME die doorverwijst naar een domein dat niet over DNSSEC beschikt is niet toegestaan, omdat dan de keten van DNSSEC wordt onderbroken. Een CNAME mag alleen verwijzen naar een domein dat over DNSSEC beschikt.

3.4 Opheffen domeinnamen

Conform adviesrapport "Domeinnamen advies rapport 210811" van "Informatieveiligheid & Privacy" geldt onderstaande advies:

Team Informatieveiligheid & privacy adviseert, om als gemeente de volgende stappen te nemen om de risico's van misbruik te voorkomen bij het opheffen van een domeinnaam:

*- **Stap 1**. Parkeer de domeinnamen waardoor we alleen betalen voor de registratie van het domein. Men kan ook de desbetreffende domeinnamen doorverwijzen naar nieuwe websites (als hier sprake van is). De kosten van het behoud van domeinnamen liggen rond de 8-10 euro per jaar.*

*- **Stap 2**. Controleer of er andere websites zijn die naar de opgeheven domeinnamen verwijzen. Als dit het geval is, dan zal je deze zogeheten referral links moeten laten weten dat de websites niet langer actief zijn, zodat doorverwijzing naar deze websites voorkomen wordt.*

*- **Stap 3**. Zorg voor goede communicatie richting derden en burgers over het feit dat we als gemeente de desbetreffende domeinnamen niet meer gebruiken voor de aanvankelijke doeleinden.*

*- **Stap 4**. Zorg ervoor dat wij als gemeente alle mails, verstuurd naar de e-mailadressen van onze oude domeinnamen, opvangen door een catch-all in te stellen. De gemeente zou ervoor kunnen kiezen om deze mails door te laten sturen naar het nieuwe e-mailadres om vervolgens een automatisch antwoord in te stellen met de melding dat het oude e-mailadres niet langer in gebruik is.*

Uiteraard kost het behouden/parkeren van een domeinnaam geld. Echter zijn de kosten relatief laag. Dit weegt niet op tegen de mogelijke risico's die het opzeggen met zich mee brengt. Met name bij websites waar burgers genegen kunnen zijn om gevoelige informatie mee te delen, bijvoorbeeld belastingenamstelland.nl, is het risico groot dat criminelen juist deze domeinnaam zullen gebruiken om burgers door te verwijzen naar een website met dubieuze content, zoals vernoemd in de lijst met risico's. Bij het gebruik van dezelfde soort domeinnamen is tevens het risico groot dat er onder de identiteit van deze websites Phishing mails worden uitgestuurd, waar gevraagd wordt om een bedrag te betalen via bijgevoegde link. Dit alles kan leiden tot o.a. imagoschade voor de gemeente en schadeclaims vanuit burgers. Concluderend is daarom ons advies om domeinnamen niet op te zeggen en de stappen hierboven te nemen om de risico's van misbruik te voorkomen.

4.0 IPv6

Al onze websites die via Internet raadpleegbaar zijn, moeten naast een IPv4 adres ook over een IPv6 adres beschikken. Dit is vastgelegd op https://www.digitaleoverheid.nl/nieuws/overheid-eind-2021-via-ipv6-bereikbaar/.
De meeste websites zijn inmiddels op IPv6 bereikbaar.
Alle Webservers (zowel intern gehost als extern) moeten worden voorzien van een eigen IPv6-adres. Voor onze interne hosting hebben we IPv6 adresblokken binnen het Overheidsbreed IPv6-nummerplankader van Logius gekregen. Deze worden gebruikt op onze eigen hosting.IPv6 is ook een verplichte standaard: https://www.forum-standaardisatie.nl/open-standaarden/ipv6-en-ipv4
Ook mailservers die niet onder de hoofddomeinen vallen, zoals genoemd bij punt 3.1, maar wel horen bij een website die binnen de werking van dit document valt, moeten via IPv6 kunnen communiceren.

5.0 SPF/DMARC/DKIM/DANE en Mail relay

5.1 SPF

Alle mailservers moeten bekend zijn in het SPF-record van het betreffende domein. Ook voor inactieve domeinen moet er een SPF-record aanwezig zijn. Daar is de inhoud: "*v=spf1 -all*"

5.2 DMARC

Elk domein moet over een geldige DMARC-policy beschikken. Voor alle inactieve domeinen moet er een CNAME zijn met de naam *_dmarc* met als inhoud "*reject.dmarc.amstelveen.nl*"
Voor de Nederlandse (lokale)overheid is het verplicht om *p=reject* te gebruiken in de policy.

5.3 DKIM

Voor het versturen van mail moet er met DKIM worden ondertekend. Ook wanneer er gebruik wordt gemaakt van b.v. Mailchimp of soortgelijke diensten. Mailservers die niet in het SPF-record zijn opgenomen of kunnen worden opgenomen, worden door een spamfilter alleen maar geaccepteerd als afzender, indien de mail met een geldige DKIM sleutel is ondertekend.

5.3.1 DKIM op Mailchimp

Voor een dienst als Mailchimp moet er een CNAME-record worden aangemaakt, op elk domein dat vanaf Mailchimp moet kunnen verzenden, met de naam k1._domainkey met als inhoud "dkim.mcsv.net". Dit wordt in het beheer van het Mailchimp account aangegeven.
Voordat je met Mailchimp iets kunt versturen moet het domein gevalideerd worden en vervolgens na het aanmaken van het CNAME-record moet het worden geauthentiseerd.
Pas daarna kan er vanuit Mailchimp mail worden verzonden uit naam van ons domein.
Deze stappen moeten voor ELK Mailchimp account worden uitgevoerd.
Voor andere systemen die niet bekend zijn in SPF kan op vergelijkbare manier DKIM worden toegevoegd, zodat de mail toch geverifieerd kan worden door een spamfilter.

5.4 Mail Relay

Voor systemen die Mail niet met DKIM kunnen ondertekenen en toch uit amstelveen.nl of aalsmeer.nl mail moeten kunnen verzenden is het mogelijk om de mail via IP-Whitelisting (Op zowel firewall als Exchange) over poort tcp/587 aan te bieden aan onze exchangeserver voor relay. Dit moet wel een "eigen" IP-adres zijn.
Deze functionaliteit zal in de loop van 2023 worden opgeheven.

5.5 DANE

Elk actief maildomain moet voorzien zijn van DANE (DNS-based Authentication of Named Entities).

5.6 Mail versturen uit naam van amstelveen.nl of aalsmeer.nl

Indien het noodzakelijk is om mail te versturen uit naam van amstelveen.nl of aalsmeer.nl vanaf een andere server dan de eigen server van Amstelveen/Aalsmeer, dan is dit **NIET** mogelijk vanuit het hoofddomein.

In ALLE gevallen dient er dan gebruik te worden gemaakt van een sub-domein!
Voor dit sub-domein zullen wij dan de benodigde SPF, DMARC & DKIM-records aanmaken evenals een MX null record. https://www.rfc-editor.org/rfc/rfc7505

5.7 Mail versturen via Graph-koppeling in Exchange Online

Het is ook mogelijk om mail via een Graph-koppeling te versturen.

6.0 Certificaten

- Websites waarvan de gemeente Domeinhouder is, dienen voorzien te worden van een door de gemeente aan te leveren certificaat. Bij websites die uitsluitend intern worden gebruikt kan worden volstaan met een ad-certificaat uitgegeven door de eigen interne "Active Directory Certificate Services". Alle overige websites dienen van een Publiek vertrouwd certificaat te worden voorzien.
- Websites die publiek toegankelijk zijn worden uitgerust met een DV-Certificaat.
- Websites die uitsluitend intern worden benaderd kunnen gebruik maken van een DV-Certificaat of een AD-Certificaat.
- Websites voor geautomatiseerde berichtenuitwisseling worden uitgerust met een PKI-Overheid Certificaat.
- Maximale geldigheid certificaten: 1 jaar voor DV-Certificaten.
- Géén wildcard-certificaat toegestaan, maar wel SAN-Certificaten.
- De server mag géén Root-certificaat meesturen, tenzij aangetoond kan worden dat dit strikt noodzakelijk is.
- De Intermediate certificaten moeten worden meegestuurd.
- Indien een domeinnaam naast externe hosts ook interne hosts bevat, dan worden de intern gebruikte URL's en extern gebruikte URL's elk in een eigen SAN-Certificaat worden opgenomen. Hetzelfde geldt voor Certificaten op Diginetwerk. Dus voor b.v. amstelveen.nl kennen we tot 3 verschillende SAN-Certificaten voor dezelfde leverancier:
  - Op Internet gebruikte URL's — Staan in Publiek toegankelijke DNS met bijbehorend SAN-Certificaat
  - Intern (VPN) gebruikte URL's — Staan in alleen intern toegankelijke DNS met bijbehorend SAN-Certificaat
  - Op Diginetwerk gebruikte URL's — Staan of in host-file van de betreffende machine of private dns van de leverancier. IP-adressen van Diginetwerk staan NIET in een publiek toegankelijke DNS. In het SAN-Certificaat (PKI-Overheid) staan alleen URL's die op Diginetwerk worden gebruikt.
- De AA-gemeenten maken gebruik van de certificaten van:
  - Certificaten van Sectigo worden geleverd door Xolphin.
  - Xolphin levert naast de Sectigo certificaten ook certificaten van:
    - Thawte — SSL123
    - Digicert — Secure
    - Geotrust — RapidSSL
    - GlobalSign — Domein
    - In geval van problemen met de Sectigo certificaten kan eenvoudig worden overgestapt op een van de overige certificaatverstekkers die Xolphin kan leveren.
  - Certificaten van KPN PKI-overheid voor *machine-to-machine-koppelingen* (Staat der Nederlanden Private Root CA - G1)

6.1 De controle: DV, OV, EV, QWAC (Bron: Nationaal Cyber Security Centrum)

Voor openbare websites en de meeste andere toepassingen van webservercertificaten, voldoet een DV (Domain Validation)-certificaat. Bij DV-certificaten controleert de leverancier de vermelde domeinnaam, maar niet de identiteit van de aanvrager. Vraagt u bijvoorbeeld een DV-certificaat voor ncsc.nl aan, dan controleert de leverancier wel dat u de houder bent van de domeinnaam ncsc.nl, maar hij vraagt u niet de naam van uw organisatie, of verder bewijs dat u namens deze organisatie handelt.
Certificaten van het type Organisation Validation (OV), Extended Validation (EV) en Qualified Website Authentication Certificate (QWAC) kennen een oplopend niveau van controle op de identiteit van de aanvrager. Deze certificaten vermelden die identiteit ook, zodat het voor de bezoeker van een website mogelijk is om op te vragen wie de eigenaar van de website is. Vroeger leidde het gebruik van een EV-certificaat ook tot een zogenaamde 'groene balk' in de browser van bezoekers, maar geen van de populaire browsers doet dit nog. De meerwaarde van een OV-, EV- of QWAC-certificaat is daarmee beperkt voor toepassingen waar een lager niveau, zoals DV, ook geaccepteerd wordt.
In sommige sectoren is het gebruik van een certificaat met een zeker controleniveau voor bepaalde toepassingen verplicht. Deze verplichting volgt dan uit sectorale wet- en regelgeving. Het NCSC is op de hoogte van één geval waarin dit speelt. Bedrijven in de financiële sector zijn op basis van de PSD2wetgeving verplicht om voor bepaalde machine-to-machine-koppelingen een QWAC-certificaat te gebruiken.

Sommige toepassingen vereisen een certificaat dat een OIN (Organisatie-Identificatienummer) bevat. Dit speelt een rol bij geautomatiseerde berichtenuitwisseling met de overheid. Digikoppeling [1]is hiervan het belangrijkste voorbeeld. Het OIN staat vermeld op OV-certificaten van PKI-overheid. U kunt na de deadline dergelijke OV-certificaten nog steeds bij PKI-overheid afnemen, onder het stamcertificaat "Staat der Nederlanden Private Root CA - G1". Meer informatie vindt u op de website van Logius[2]. Omdat certificaten onder dit stamcertificaat niet publiek vertrouwd zijn, kunt u deze niet gebruiken voor openbare websites.

6.2 De vermelding van de domeinnaam (Bron: Nationaal Cyber Security Centrum)

Veel certificaten vermelden maar een of twee domeinnamen, maar het is mogelijk om een certificaat te maken dat voor veel meer domeinnamen tegelijk geldt. De domeinnamen waarvoor een certificaat geldt, staan vermeld in het Subject Alternative Name-veld. (SAN-Certificaat)
Voor verschillende toepassingen kunt u het beste ook verschillende certificaten gebruiken. Als er dan iets misgaat met een certificaat, hoeft u het niet op allerlei andere plaatsen ook te vervangen. Maar als één toepassing meerdere domeinnamen betreft, kunt u deze wel samenvoegen op hetzelfde certificaat. Websites zijn hiervan een voorbeeld. Is één website onder meerdere domeinnamen te bereiken, dan is het logisch om een certificaat voor al die domeinnamen tegelijk aan te vragen. Gaat het om meerdere aparte websites? Gebruik dan aparte certificaten. Ook als het om meerdere websites op één webserver gaat.

In sommige toepassingen is van tevoren niet bekend welke subdomeinen er precies zullen worden aangeroepen, of wilt u niet dat deze subdomeinen openbaar worden. In zulke gevallen kunt u een wildcardcertificaat gebruiken. Dat is een certificaat dat voor alle subdomeinen van een domein tegelijk geldt. De vermelding is dan '*.example.nl'. Als u een wildcardcertificaat gebruikt, loopt u een iets groter risico dan bij een certificaat waar alle domeinnamen apart op staan. Een aanvaller die over de geheime sleutel beschikt, kan het immers ook gebruiken om andere toepassingen met een subdomein van die domeinnaam aan te vallen. Sommige certificaatleveranciers ondersteunen geen wildcardcertificaten. Overweegt u om een wildcardcertificaat te gebruiken, voer dan eerst een risicoanalyse uit. *Om deze reden staan de AA-gemeenten geen wildcardcertificaten toe.*

7.0 Tenslotte

Voor alle zaken genoemd in dit document dient voor aanschaf/aanbesteding contact opgenomen te worden met de afdeling ICT (via de Servicedesk ICT).

[1] Zie https://www.logius.nl/diensten/digikoppeling
[2] Zie https://www.logius.nl/diensten/oin