

Bijlage 8.4 Aansluitvoorwaarden

Parkeerrechtensysteem en native applicatie voor tijdelijke parkeerrechten



**OMDAT
PARKEREN
EEN VAK IS**



Inhoudsopgave

Applicatielandschap	4
Architectuur- en procesplaten.....	4
Specifieke kaders van de oplossingsrichting.....	5
GEMMA-standaarden en FORUM standaardisatie	5
Koppelingen en koppelvlakken	5
Overige kaders en technische aansluitvoorwaarden	5
Algemeen	5
Gebruiksvriendelijkheid	6
Technische aansluitvoorwaarden	6
Stabiliteit en continuïteit	7
Data	7
Archiefwet.....	7
Informatieveiligheid en informatiebeveiliging	7
Onderhoud en eisen en wensen informatiebeveiliging	9
Beheer	11
Technische werkomgeving	11
Relevante standaarden.....	11
Digitoegankelijk (EN 301 549 met WCAG 2.1)	11
DKIM	11
DMARC	11
DNSSEC	12
Geo-standaarden	12
HTTPS en HSTS	12
IPv6.....	12
NEN	12
NEN-ISO/IEC 27002	12
NL GOV Assurance profile for OAuth 2.0	12
OpenAPI Specification	12
PDF (NEN-ISO).....	13
REST-API Design Rules.....	13
RPKI	13
SAML.....	13



SKOS.....	13
SPF	13
STARTTLS en DANE	13
TLS.....	13



Specifieke kaders van de oplossingsrichting

GEMMA-standaarden en FORUM standaardisatie

De Afgesplitste Versie van het Parkeerrechtensysteem voldoet, daar waar van toepassing, aan de GEMMA-standaarden welke zijn gepubliceerd op: standaarden.vng.nl

De Afgesplitste Versie van het Parkeerrechtensysteem voldoet ook aan de verplichte standaarden welke voortvloeien uit de 'pas toe of leg uit'-lijst van Forum standaardisatie welke zijn gepubliceerd op <https://www.forumstandaardisatie.nl/open-standaarden/verplicht>. Coöperatie ParkeerService heeft naar aanleiding van deze aanbesteding de beslisboom van het Forum standaardisatie ingevuld en de uitkomsten opgenomen in deze aansluitvoorwaarden, zie de kop *Vermoedelijk Relevante Standaarden*.

Koppelingen en koppelvlakken

De Afgesplitste Versie van het Parkeerrechtensysteem biedt de mogelijkheid tot het realiseren van standaard koppelvlakken voor het koppelen op basis van REST-API. Indien niet mogelijk mag het op basis van StUF, in dit geval is een roadmap voor doorontwikkeling naar REST-API noodzakelijk. De Afgesplitste Versie van het Parkeerrechtensysteem ondersteunt Digikoppeling waar deze standaard door bron- of doelsystemen wordt vereist. Ondersteuning voor Digikoppeling WUS, ebMS en/of REST-profielen dient beschikbaar te zijn.

Overige kaders en technische aansluitvoorwaarden

Algemeen

De Afgesplitste Versie van het Parkeerrechtensysteem wordt als digitale dienstverlening voor burgers/bedrijven aangeboden en is te benaderen/ gebruiken door middel van webbrowsers op zowel desktop- en laptop- computers, alsmede webbrowsers en/of 'apps' op mobiele apparaten (smartphones, tablets) en is indien nodig van een responsive design voorzien. De Afgesplitste Versie van het Parkeerrechtensysteem wordt middels het Internet ontsloten.

De Afgesplitste Versie van het Parkeerrechtensysteem dient zodanig te zijn ontworpen dat hosting, applicatie en gegevensopslag logisch van elkaar kunnen worden gescheiden. ParkeerService kiest bij aanvang mogelijk voor hosting door de Opdrachtnemer, maar behoudt zich het recht voor om gedurende de contractperiode de gegevensopslag geheel of gedeeltelijk onder te brengen in een eigen of door ParkeerService aangewezen cloudomgeving. De Afgesplitste Versie van het Parkeerrechtensysteem dient deze transitie te ondersteunen zonder verlies van functionaliteit, gegevens of integratiemogelijkheden en met een minimale afhankelijkheid van de Opdrachtnemer.

De functionele behoefte van ParkeerService wordt door de Afgesplitste Versie van het Parkeerrechtensysteem ingevuld middels configuratie en vereist daarnaast aanpassing van de Broncode van de Afgesplitste Versie van het Parkeerrechtensysteem.

De Inschrijver levert als onderdeel van zijn 'Oplossingsvoorstel' (dit gebeurt in de volgende fase van deze aanbestedingsprocedure, de 'Onderhandelingsfase') een (technisch) ontwerp aan waarin is aangegeven hoe het datamodel van de oplossingsrichting is opgebouwd. Daarbij dient ook aangegeven te worden in welke mate de aangeboden en over te dragen oplossing modulair is opgebouwd.

De Afsplitste Versie van het Parkeerrechtensysteem (inclusief gekoppelde (door Opdrachtnemer te leveren) componenten die in het kader van de Afsplitste Versie van het Parkeerrechtensysteem worden gebruikt) wordt gehost binnen de EER.

Iedere App behorende bij het systeem is ontwikkeld voor browseronafhankelijk gebruik en ondersteunt in ieder geval de door browser-leveranciers ondersteunde versies van Microsoft Edge en Mozilla Firefox.

Gebruiksvriendelijkheid

De Afsplitste Versie van het Parkeerrechtensysteem is één herkenbaar geheel; de schermen, de kleuren, de navigatie en andere basisfuncties zijn eenduidig herkenbaar.

De schermen (invoer, raadpleeg en beheer) zijn overzichtelijk, duidelijk en eenvoudig opgezet, waardoor de meest voorkomende handelingen intuïtief uitgevoerd kunnen worden.

De navigatie en bediening van de Afsplitste Versie van het Parkeerrechtensysteem is eenduidig. Dat wil zeggen dat deze op elke plaats binnen de Afsplitste Versie van het Parkeerrechtensysteem op dezelfde wijze gebruikt en gedefinieerd zijn.

De Afsplitste Versie van het Parkeerrechtensysteem voorziet in een gebruikersinterface met de mogelijkheid tot 'help'- ondersteuning voor gebruikers.

Technische aansluitvoorwaarden

Koppelingen tussen Opdrachtnemer en ParkeerService kunnen enkel tot stand gebracht worden via een beveiligde https-verbinding.

Voor de beveiliging van HTTPS-verbindingen wordt minimaal gebruikgemaakt van een TLS-certificaat dat gebruikgemaakt van SHA-256 als hashfunctie en een RSA-sleutellengte van minimaal 2048 bits. Toepassing van sterkere hashfuncties (zoals SHA-384) of langere sleutels kan in overleg worden overwogen.

Voor de beveiliging van https-verbindingen wordt minimaal gebruik gemaakt van TLS 1.2. Oudere versies worden niet ondersteund.

De Afsplitste Versie van het Parkeerrechtensysteem ondersteunt een netwerkconfiguratie waarbij slechts één extern IP-adres wordt gebruikt voor inkomend verkeer via onze firewall, met Network Address Translation (NAT) als vereiste.

ParkeerService vereist het gebruik van sterke authenticatie (Multi-Factor Authentication, MFA). Dit wordt voor medewerkers van ParkeerService technisch afgedwongen via Azure Active Directory (Azure AD) Conditional Access. Authenticatie vindt plaats via standaarden zoals SAML 2.0 en/of OAuth 2.0, waarbij het authenticatieverzoeken doorstuurt naar de Identity Provider (IdP) van het RAZU.

De Opdrachtnemer dient deze methode van sterke authenticatie te ondersteunen.

Voor externe gebruikers (bijv. vrijwilligers) dwingt de Afsplitste Versie van het Parkeerrechtensysteem een andere vorm van MFA af.

Indien de Afgesplitste Versie van het Parkeerrechtensysteem een externe website of mailservice betreft dan heeft deze aantoonbaar een 100% score op internet.nl.

Stabiliteit en continuïteit

- Opdrachtnemer beschikt minimaal over een gescheiden test-, acceptatie- en productieomgeving en maakt gebruik van een ontwikkelstraat. Wijzigingen in de ene omgeving mogen geen invloed hebben op het functioneren van de andere omgeving.
- De acceptatie- en productieomgeving worden aan de gelijknamige omgevingen binnen ParkeerService gekoppeld. Wijzigingen aan de kant van ParkeerService zullen altijd eerst in de acceptatieomgeving doorgevoerd worden, waarna getest kan worden of de Afgesplitste Versie van het Parkeerrechtensysteem, inclusief de diverse koppelingen, nog naar behoren werkt.
- ParkeerService is en blijft te allen tijde eigenaar van de data in de Afgesplitste Versie van het Parkeerrechtensysteem.
- De Opdrachtnemer heeft het beheerproces beschreven en ingericht. Alle relevante documenten en (meta)data die betrekking hebben op aanvraag, mutatie, verlenging of beëindiging van een product/dienst worden opgeslagen.

De Opdrachtnemer kent een gestructureerd patch- en releasemanagement.

Data

- De Afgesplitste Versie van het Parkeerrechtensysteem beschikt over interoperabele (open standaarden) exportformaten voor alle gegevens die opgeslagen zijn in de Afgesplitste Versie van het Parkeerrechtensysteem, zodat de data beschikbaar en toegankelijk is voor ParkeerService.
- De metadata is te extraheren uit de oplossingsrichting. Er vindt datascheiding plaats tussen de verschillende omgevingen (, acceptatie, productie). Geef aan hoe deze datascheiding wordt toegepast.
- Op verzoek van ParkeerService zal de Opdrachtnemer binnen 24 uur alle data op een leesbare manier exporteren naar ParkeerService, waar nodig vergezeld van documentatie over relevante onderdelen van het datamodel.
- Opdrachtnemer dient de data na afloop of bij tussentijdse beëindiging van de Overeenkomst via interoperabele (open standaarden) exportformaten op verzoek van ParkeerService beschikbaar te stellen aan, Opdrachtnemer garandeert hierbij de volledigheid van de data. Na migratie of levering van de data, dient Opdrachtnemer op verzoek van ParkeerService de data te verwijderen van zijn systemen en deze te vernietigen. Voorgaande geldt uitdrukkelijk ook voor data bestaande uit persoonsgegevens.

Archiefwet

De Afgesplitste Versie van het Parkeerrechtensysteem wordt zodanig ingericht dat archiefwet- en informatiebeheervereisten aantoonbaar worden ondersteund, waaronder het toepassen van bewaartermijnen, duurzame toegankelijkheid van informatie en tijdige vernietiging conform geldende selectielijsten. Deze processen worden waar mogelijk geautomatiseerd ingericht, met ondersteuning voor handmatige beoordeling, autorisatie en controle waar dat noodzakelijk is.



Informatieveiligheid en informatiebeveiliging

- Opdrachtnemer zal om het jaar een audit laten uitvoeren door een daartoe geautoriseerde externe partij op de eigen dienstverlening. Deze audit richt zich met name op het nakomen van de afspraken omtrent beveiliging en privacy en op kwetsbaarheden. De kosten voor deze audit zijn een integraal onderdeel van de Inschrijving.
- De Afsplitste Versie van het Parkeerrechtensysteem ondersteunt het principe van zero trust. Een medewerker van ParkeerService hoeft zich slechts eenmaal aan te melden bij de Identity Provider (Single Sign-On). De Afsplitste Versie van het Parkeerrechtensysteem dient hier notie van te hebben en de medewerker niet nogmaals om inloggegevens te vragen. Het gebruik van IdP initiated SSO is niet toegestaan.
- De volgende acties van medewerkers van ParkeerService dienen gelogd te worden en herleidbaar te zijn naar natuurlijke personen:
 - Het muteren van data;
 - Het exporteren van data;
 - Ook data die de Afsplitste Versie van het Parkeerrechtensysteem verlaat en daarmee niet meer getraceerd kan worden dient gelogd te worden. Voorbeelden hiervan zijn het al dan niet automatisch versturen van e-mail, het maken van data-dumps en het uitwisselen van data met andere systemen;
 - Het verwijderen van data.
- De log-regels dienen minimaal de volgende informatie weer te geven:
 - de gebeurtenis;
 - de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;
 - het gebruikte apparaat;
 - het resultaat van de handeling;
 - een datum en tijdstip van de gebeurtenis.
- Het opvragen van loggegevens dient automatisch uitgevoerd te kunnen worden zonder dat daar bij de Opdrachtnemer handmatige acties aan verbonden zijn. Eventueel kan de informatie ook op gezette tijden op voldoende wijze beveiligd naar ParkeerService worden verstuurd.
- Logbestanden dienen als leesbare tekst opgeslagen te worden in een standaardformaat zoals XML, CSV of JSON en voor een functioneel beheerder te downloaden zijn vanuit de Afsplitste Versie van het Parkeerrechtensysteem. Ieder bestand dient te zijn voorzien van informatie die een beschrijving geeft van de data in het bestand.
- Het is niet toegestaan gevoelige informatie zoals persoonsgegevens, anders dan de gebruikersnaam of het gebruikers ID, op te slaan als gelogde informatie.
- Opdrachtnemer dient log informatie ook zelf veilig te stellen. Tevens dient Opdrachtnemer te garanderen dat log informatie ouder dan 3 jaar verwijderd wordt, behalve voor de audittrail van individuele objecten in de Afsplitste Versie van het Parkeerrechtensysteem welke bewaard dient te worden.
- Wanneer Opdrachtnemer gebruik maakt van een shared omgeving, is de data van ParkeerService niet te benaderen door derden die dezelfde shared omgeving gebruiken.
- De Afsplitste Versie van het Parkeerrechtensysteem biedt de mogelijkheid voor het instellen van meerdere autorisatieniveaus, waardoor inzage of mutatie van gegevens voor medewerkers van Coöperatie ParkeerService beperkt of uitgebreid kan worden afhankelijk van de taak/functie/rol waarvoor zij gemachtigd zijn om specifieke gegevens in te zien of te wijzigen.
- De Afsplitste Versie van het Parkeerrechtensysteem is in staat een totaaloverzicht te presenteren waarop de autorisaties per functie(groep) weergegeven worden.



- De Afsplitste Versie van het Parkeerrechtensysteem beschikt over een adequate back-up voorziening die aansluit bij de gestelde eisen ten aanzien van RPO en RTO die Opdrachtnemer in zijn SLA aanbiedt. Opdrachtnemer voert periodiek restore-testen uit om te controleren of de back-ups consistent en herstelbaar zijn.
- De Afsplitste Versie van het Parkeerrechtensysteem werkt met encryptie standaarden.

Onderhoud en eisen en wensen informatiebeveiliging

Categorie	Item	Adviesnorm
Technische continuïteit	Beschikbaarheid productieomgeving	>= 99,99% per maand tijdens kantooruren (08.00 – 18.00 uur) en 99,9% tijdens overige uren
Technische continuïteit	Geplande downtime	Maximaal 4 onderhoudsvensters per jaar
Technische continuïteit	Onderhoudsvenster	Buiten kantooruren, standaard 18:00 - 07:00
Technische continuïteit	Aankondiging gepland onderhoud	Minimaal 10 werkdagen vooraf
Technische continuïteit	Calamiteitendienst	24x7 beschikbaar voor kritieke verstoringen
Technische continuïteit	Servicedesk	Werkdagen 08:00 - 18:00
Technische continuïteit	RPO - maximaal dataverlies	<= 1 uur
Technische continuïteit	RTO - herstel primaire dienstverlening	<= 4 uur
Technische continuïteit	RTO volledige omgeving na calamiteit	<= 8 uur
Technische continuïteit	Back-up frequentie	Minimaal elk uur
Technische continuïteit	Restore-test	Minimaal jaarlijks aantoonbaar uitgevoerd
Technische continuïteit	Monitoring	24x7 monitoring van applicatie, database, koppelingen en infrastructuur
Technische continuïteit	Service- en beschikbaarheidsrapportage	Maandelijks
Technische continuïteit	Root Cause Analyse bij P1-incident	Binnen 5 werkdagen beschikbaar
Technische continuïteit	Exit na einde contract	Volledige overdracht binnen 30 dagen
Incidentmanagement	P1 kritiek - reactietijd	<= 30 minuten
Incidentmanagement	P1 kritiek - hersteltijd	<= 4 uur
Incidentmanagement	P2 hoog - reactietijd	<= 1 uur
Incidentmanagement	P2 hoog - hersteltijd	<= 8 uur
Incidentmanagement	P3 middel - reactietijd	<= 4 uur
Incidentmanagement	P3 middel - hersteltijd	<= 24 uur
Incidentmanagement	P4 laag - reactietijd	<= 1 werkdag
Incidentmanagement	P4 laag - hersteltijd	<= 5 werkdagen
Cloud en hosting	Leveringsmodel	Software as a Service
Cloud en hosting	Hostinglocatie	Europese Economische Ruimte
Cloud en hosting	Datalocatie	Europese Economische Ruimte
Cloud en hosting	Multi-tenant architectuur	Verplicht
Cloud en hosting	Gegevensscheiding per gemeente	Volledige logische scheiding
Cloud en hosting	Testomgeving	Verplicht
Cloud en hosting	Acceptatieomgeving	Verplicht
Cloud en hosting	Productieomgeving	Verplicht
Cloud en hosting	Scheiding omgevingen	Logisch en aantoonbaar gescheiden
Cloud en hosting	Hostingverantwoordelijkheid	Opdrachtnemer is verantwoordelijk
Informatiebeveiliging	BIO2	Aantoonbaar conform
Informatiebeveiliging	AVG	Aantoonbaar conform
Informatiebeveiliging	ISO 27001 certificering	Aantoonbaar conform
Informatiebeveiliging	Jaarlijkse externe audit	Verplicht



Categorie	Item	Adviesnorm
Informatiebeveiliging	Encryptie dataverkeer	TLS 1.2 of hoger
Informatiebeveiliging	Encryptie opslag	AES-256 of gelijkwaardig
Informatiebeveiliging	Multi-factor authenticatie beheerders	Verplicht
Informatiebeveiliging	Multi-factor authenticatie gebruikers	Ondersteund
Informatiebeveiliging	Logging beheeracties	Verplicht
Informatiebeveiliging	Audittrail transacties	Verplicht
Informatiebeveiliging	Bewaartermijn auditlogs	Minimaal 12 maanden
Informatiebeveiliging	Kwetsbaarheidsscans	Minimaal maandelijks
Informatiebeveiliging	Penetratietest	Jaarlijks onafhankelijk
Informatiebeveiliging	Kritieke kwetsbaarheden	Oplossen binnen 48 uur
Informatiebeveiliging	Hoog risico kwetsbaarheden	Oplossen binnen 14 dagen
Koppelingen en openheid	Volledig gedocumenteerde API	Verplicht
Koppelingen en openheid	API-documentatie	Beschikbaar en actueel
Koppelingen en openheid	Realtime berichtenverkeer	Verplicht voor kritieke processen
Koppelingen en openheid	Koppeling NPR	Verplicht
Koppelingen en openheid	Koppeling RDW	Verplicht
Koppelingen en openheid	Koppeling BRP	Verplicht waar nodig
Koppelingen en openheid	Koppeling BAG	Verplicht
Koppelingen en openheid	Koppeling Handelsregister	Verplicht
Koppelingen en openheid	Koppeling AFAS	Verplicht
Koppelingen en openheid	Export van alle data	Verplicht
Koppelingen en openheid	Open bestandsformaten	CSV, XML en JSON
Koppelingen en openheid	Geen leveranciersafhankelijkheid bij data-export	Verplicht
Privacy en gegevensbescherming	Verwerkersovereenkomst	Verplicht
Privacy en gegevensbescherming	Datalek melding aan ParkeerService	Binnen 24 uur
Privacy en gegevensbescherming	Verwijderen persoonsgegevens	Ondersteund conform AVG
Privacy en gegevensbescherming	Recht op inzage	Ondersteund
Privacy en gegevensbescherming	Recht op dataportabiliteit	Ondersteund
Privacy en gegevensbescherming	Ondersteuning privacy impact assessment	Verplicht
Privacy en gegevensbescherming	Subverwerkersregister	Verplicht
Privacy en gegevensbescherming	Nieuwe subverwerkers	Vooraf melden en akkoordproces
Exit en migratie	Volledige data-export	Verplicht
Exit en migratie	Database-export	Verplicht
Exit en migratie	Configuratie-export	Verplicht
Exit en migratie	Export documentarchief	Verplicht
Exit en migratie	Migratieondersteuning	Verplicht
Exit en migratie	Kosten data-uitlevering	Geen extra licentiekosten
Exit en migratie	Vernietigingsverklaring	Verplicht na overdracht

Beheer

Item	Norm
Geplande downtime	≤ 4 x / jaar
Minimale Openstellingstijd servicedesk	08.00 – 20.00
Herstellenvenster incidenten	Werkdagen gedurende Openstellingstijd
Dataverlies (RPO)	≤ 2 uur
Ongeplande downtime volledige ICT-infrastructuur (RTO)	≤ 8 uur
Specifieke afspraak voor Parkeerrechtensysteem ^(RTO) Parkeerrechtensysteem)	≤ 4 uur (H)
Beschikbaarheid ICT-infrastructuur	99,99% gedurende een maand tijdens Kantoortijden (08.00 – 20.00) en 99,9% tijdens de overige tijden

Technische werkomgeving

De ICT-omgeving van ParkeerService kan globaal als volgt worden gekenmerkt:
 Binnen ParkeerService wordt gebruik gemaakt van een werkplek gebaseerd Microsoft 365 E5.
 Medewerkers beschikken over een recente laptop voorzien van Windows 11 en centraal beheerd via Microsoft Intune.

Relevante standaarden

Op basis van de beslisboom van het Forum standaardisatie zijn de volgende standaarden vermoedelijk relevant.

Digitoegankelijk (EN 301 549 met WCAG 2.1)

Door toepassing van Digitoegankelijk worden websites, webapplicaties en documenten voor iedereen toegankelijk, ook voor mensen met permanente, tijdelijke of situationele functiebeperkingen. Zo krijgt iedereen dezelfde toegang tot overheidsinformatie.
 Let op: per 1 juli 2018 zijn overheidsorganisaties wettelijk verplicht om Digitoegankelijk (EN 301 549 en WCAG 2.1) te gebruiken voor de toegankelijkheid van websites en mobiele applicaties. Kijk voor meer informatie.

<https://www.forumstandaardisatie.nl/open-standaarden/digitoegankelijk-en-301-549-met-wcag-21>

DKIM

DKIM faciliteert van het vaststellen van organisatorische herkomst voor e-mail afkomstig van overheidsdomeinen, als deze over een onbeveiligde, publieke internetverbinding wordt verstuurd wanneer verdere authenticatie ontbreekt.

<https://www.forumstandaardisatie.nl/open-standaarden/dkim>

DMARC

DMARC is een standaard die het voor organisaties mogelijk maakt om te bepalen hoe e-mailproviders, die DMARC ondersteunen, omgaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het eigen domein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie.

<https://www.forumstandaardisatie.nl/open-standaarden/dmarc>

DNSSEC

DNSSEC zorgt voor de beveiliging van DNS door aan het DNS-record een digitale handtekening toe te voegen en deze bij uitwisseling te verifiëren.

<https://www.forumstandaardisatie.nl/open-standaarden/dnssec>

Geo-standaarden

Geografische gegevens worden uitwisselbaar gemaakt conform de relevante Geo-standaarden vanuit het principe Pas-Toe-Of-Leg-Uit.

<https://www.forumstandaardisatie.nl/open-standaarden/geo-standaarden>

HTTPS en HSTS

HTTPS en HSTS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser).

Let op: per 1 juli 2023 zijn overheidsorganisaties wettelijk verplicht om HTTPS en HSTS te gebruiken voor beveiligen van publiek toegankelijke websites en webapplicaties. Kijk voor meer informatie.

<https://www.forumstandaardisatie.nl/open-standaarden/https-en-hsts>

IPv6

IPv6 en IPv4 standaardiseren communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren.

<https://www.forumstandaardisatie.nl/open-standaarden/ipv6>

NEN-ISO/IEC 27001

NEN-ISO/IEC 27001 specificeert de eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

<https://www.forumstandaardisatie.nl/open-standaarden/nen-isoiec-27001>

NEN-ISO/IEC 27002

NEN-ISO/IEC 27002 omvat "best practices" op het gebied van het organiseren van informatiebeveiliging voor een organisatie, bestaande uit het beheer van bedrijfsmiddelen, veilig personeel, toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging in de bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties, beheer van informatiebeveiligingsincidenten, informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer, naleving en de acquisitie, ontwikkeling en het onderhoud van informatiesystemen.

NL GOV Assurance profile for OAuth 2.0

NL GOV Assurance profile for OAuth 2.0 zorgt ervoor dat de autorisatie van gebruikers van REST APIs van de overheid op een uniforme en eenduidige wijze plaatsvindt.

<https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20>
ODF

<https://www.forumstandaardisatie.nl/open-standaarden/odf>

OpenAPI Specification

Een OpenAPI Specification (OAS) beschrijft de eigenschappen van de data die een API als input accepteert en als output teruggeeft. Met OAS 3.0 kunnen zowel mensen als machines de dataset attributen van een REST API vinden, bekijken en verwerken zonder toegang tot de programmatuur en zonder aanvullende documentatie.

<https://www.forumstandaardisatie.nl/open-standaarden/openapi-specification>



PDF (NEN-ISO)

<https://www.forumstandaardisatie.nl/open-standaarden/pdf-nen-iso>

REST-API Design Rules

De standaard REST-API Design Rules geeft een verzameling basisregels voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST-API's aanbiedt ten behoeve van het ontsluiten van overheidsinformatie en/of functionaliteit.

<https://www.forumstandaardisatie.nl/open-standaarden/rest-api-design-rules>

RPKI

Met Resource Public Key Infrastructure (RPKI) kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routing vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routing negeren.

<https://www.forumstandaardisatie.nl/open-standaarden/rpki>

SAML

SAML standaardiseert federatieve (web)browser-gebaseerde single-sign-on (SSO). Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen.

<https://www.forumstandaardisatie.nl/open-standaarden/saml>
security.txt

security.txt moet worden toegepast op alle systemen die via HTTPS publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is.

<https://www.forumstandaardisatie.nl/open-standaarden/securitytxt>

Het systeem ondersteunt federatieve authenticatie op basis van SAML 2.0 en OpenID Connect (OIDC), conform de relevante Forum Standaardisatie-profielen.

SKOS

SKOS betreft het in een gestructureerde vorm op het Web publiek beschikbaar stellen van een 'niet geformaliseerd' Knowledge Organization System (KOS), met als doel kennis over de betekenissen en samenhang van de onderliggende begrippen te ordenen en toegankelijk te maken.

<https://www.forumstandaardisatie.nl/open-standaarden/skos>

SPF

Met SPF kan worden gecontroleerd of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden.

<https://www.forumstandaardisatie.nl/open-standaarden/spf>

STARTTLS en DANE

STARTTLS in combinatie met DANE gaan afluisteren of manipuleren van mailverkeer door internetcriminelen tegen.

<https://www.forumstandaardisatie.nl/open-standaarden/starttls-en-dane>

TLS

TLS beveiligt met behulp van certificaten de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.

<https://www.forumstandaardisatie.nl/open-standaarden/tls>