

Look & Feel

Responsive Formulieren voor mobiel gebruik	de geconfigureerde formulieren zijn gebruiksvriendelijk in te vullen op een mobiel (telefoon)
Huisstijl kadaster wordt toegepast	De huisstijl van het Kadaster wordt toegepast op de geconfigureerde formulieren Aanpasbaar CSS
Ingevuld formulier als PDF	Ingevuld formulier kan als PDF worden teruggekoppeld aan de invuller (via download of mail) Ook de look&feel hiervan moet aangepast kunnen worden.

Inrichting van de formulieren

Formulieren kunnen worden geconfigureerd	- Drag & drop/Standaardcomponenten om formulieren op te bouwen - Adresblok met automatisch aanvullen (postcode check) - Formulier met meerdere stappen - Toevoegen bijlages -	incl koppeling BGT of BAG (tbv postcode check)
Controlescherm/formuliersamenvatting		
Veilige informatieoverdracht, beveiliging		
persoonsgegevens		
Statistieken		
Invoercontrole (voor bijv. datums en emailadressen)	slimmigheden in formulieren die er voor zorgen dat de invuller geen 'gekke' dingen kan invullen	
Mogelijkheid voor (complexe) berekeningen, validaties en bewerkingen	Denk aan rekenkundige bewerkingen (zoals optellen, aftrekken, vermenigvuldigen en delen), maar ook aan het rekenen o.b.v. datums, het personaliseren van e-mails en geneste conditie	
Gebruikersbeheer voor toegang tot de configurator	autorisaties over wie formulieren mag beheren is mogelijk	
SSO voor medewerkers kadaster	De medewerker logt automatisch in met SSO wanneer hij/zij het formulier configureert	
Ondersteuning bij configuratie	Er is ondersteuning / handleidingen / voorbeelden voor het maken van de formulieren en een mogelijkheid om vragen te stellen	
Gecontroleerde voortbrenging	formulieren en wijzigingen op formulieren kunnen op een gecontroleerde manier worden voortgebracht proefomgeving en productieomgeving	
Digid ondertekening (signing)	Het ingevulde formulier moet als met DigiD gesignde PDF kunnen worden aangeleverd.	
Digid identificatie	Gegevens op het formulier worden voorgevuld na inlog bij DigiD	
eHerkenning ondertekening (signing)	Het ingevulde formulier moet als met eHerkenning gesignde PDF kunnen worden aangeleverd.	
eHerkenning identificatie?	Gegevens op het formulier worden voorgevuld na inlog met eHerkenning	
Ondertekening door meerdere personen	In bepaalde situaties is het nodig dat een formulier door indiener en opdrachtgever beiden worden getekend.	
Mogelijkheid tot embedden formulieren	formulier volledig integreren op site en niet naar een aparte url	

Integratie van de formulieren in Kadaster BO

Aanlevering via email	de gegevens van het ingevulde formulier wordt aangeleverd via mail
------------------------------	--

Aanlevering via SOAP service	De gegevens van het ingevulde formulier worden aangeleverd bij een SOAP/XML service van het Kadaster	Gegevens moeten versleuteld worden verstuurd (SSL/TLS) Authenticatie vindt plaats via OAuth2
Bepalen XML bericht	de definitie van het XML bericht kan worden afgestemd om een bestaande service van het Kadaster	Gegevens moeten versleuteld worden verstuurd (SSL/TLS) Authenticatie vindt plaats via OAuth2

Inkoop-eisen

SLA en responsetijden voor B-dienst mogelijk

SLA en responsetijden voor A-dienst mogelijk

Betrouwbare organisatie/oplossing (bestaat >4jaar)

Proeflicentie mogelijk Het uitvoeren van een POC is mogelijk zonder langdurig contract aan te gaan.

Overheidsrichtlijnen

Voldoet aan webrichtlijnen (WCAG) De geconfigureerde formulieren voldoen aan de webrichtlijnen 2.1 AA

De software moet ook blijven voldoen wanneer de richtlijnen wijzigen in de toekomst.

Gebaseerd op open source software De software is gebaseerd op open source software (25% = 1, 50%=2, 75%=3, 100%=4)

Gebruik binnen de overheid Het product / de dienst wordt gebruikt door % (semi)overheidsklanten (25% = 1, 50%=2, 75%=3, 100%=4)

Kosten

Kosten wat zijn de totale kosten (excl BTW) per jaar uitgaande van de volgende eigenschappen:

150 verschillende formuliertypen

30.000 ingevulde formulieren per jaar (?)

waarvan 250 formulieren digitaal ondertekend (gesignd) met DigiD per jaar

nr	Omschrijving	Type	BIO ref	Van toepassing
1	De leverancier logt op systematische manier security events en beschikt over een Computer security incident management proces.			
4	Leverancier meldt beveiligingsincidenten bij de Kadaster Servicedesk (088-183 21 00) en levert op verzoek een rapportage binnen 5	Functioneel	16.1 Beheer van informatiebeveiligingsincidenten	X
4	De leverancier heeft een schaalbare oplossing en dat kan worden op en/of down geschaald als daar behoefte aan is	Continuïteit	17.1 Informatiebeveiligingscontinuïteit	X
7	Performance: response van het systeem, beschikbaarheid, blijft hetzelfde ook bij een grotere belasting. De dienst heeft een schaalbare oplossing dat kan worden op en/of down geschaald om te voldoen aan de door Kadaster gestelde response-tijden. In de Kadaster SLA is een maximale response gesteld. De definitie prestaties is opgenomen in de SLA. De leverancier	Continuïteit	17.1 Informatiebeveiligingscontinuïteit	X
8	De leverancier voldoet aan interoperabiliteit en maakt gebruik van (defacto) open standaarden voor uitwisselen van data als bestand en in overdracht. De voorkeur heeft data uitwisseling via een API. REST, SOAP en sFTP zijn integratie protocol, waarbij REST de voorkeur heeft.	Prestatie-efficiëntie	09.4 Toegangsbeveiliging van systeem en toepassing	X
12	Het product voldoet aan de W3C web standaarden zodat het werkt in de laatste twee gangbare versies van de gangbare browsers	Prestatie-efficiëntie	14.2 Beveiliging in ontwikkelings- en ondersteunende processen	X
13	De leverancier beschikt over een continuïteitsplan welke aansluit bij de SLA van Kadaster. (Leverancier moet aantonen welke maatregelen	Continuïteit	17.1 Informatiebeveiligingscontinuïteit	X
15	De leverancier beschikt over een kwaliteitssysteem waarmee de informatie beveiliging op systematische wijze worden beheerst en geborgd conform ISO/IEC 27001: 2013/2017 of gelijkwaardig. Bewijsstukken te overleggen bij verificatie.	Beveiligbaarheid	18.1 Naleving van wettelijke en contractuele eisen	X
16	De dienst dient te voldoen aan Baseline Informatiebeveiliging Overheid	Beveiligbaarheid	18.1 Naleving van wettelijke en contractuele eisen	X
17	De leverancier kent een beleid voor risicobeheer, informatiebeveiliging en compliance. Het beleid is gedocumenteerd en wordt door het	Beveiligbaarheid	06.1 Interne organisatie	X
18	Binnen de organisatie van de leverancier zijn de verantwoordelijkheden voor het risicobeheer, Informatiebeveiliging en compliance	Beveiligbaarheid	06.1 Interne organisatie	X
19	Significante gebeurtenissen die de dienstverlening bedreigen worden geïdentificeerd, geregistreerd en geëvalueerd.	Beveiligbaarheid	18.2 Informatiebeveiligingsbeoordelingen	X
21	Daar waar de gebruiker en/of beheerder kan inloggen op de webapplicatie is expliciete functionaliteit aanwezig om uit te loggen (het	Beveiligbaarheid	13.1 Beheer van netwerkbeveiliging	X
23	Gegevens bij de leverancier zijn versleuteld opgeslagen.	Versleuteling	10.1 Cryptografische beheersmaatregelen	X
24	Indien cookies nodig zijn, dienen deze versleuteld te worden.	Versleuteling	10.1 Cryptografische beheersmaatregelen	X
28	Datalekken worden altijd gemeld door de leverancier aan het Kadaster binnen 24 uur. Het meldpunt is de ServiceDesk. Telefoon: +31 (0)88- 183 21 00, KSD@kadaster.nl	Privacy	18.1 Naleving van wettelijke en contractuele eisen	X
29	De locatie van de data in rust en verwerking zowel productie als backup is altijd binnen de Europese Economische Ruimte waar minimaal Europees recht van toepassing is. Buiten Europa kan gesteund worden op Adequacy besluiten van de Europese commissie.	Privacy	18.1 Naleving van wettelijke en contractuele eisen	X
30	De leverancier geeft aan welke data versleuteld is, zowel in opslag als in transport en welke niet. Ook welk encryptieprotocol wordt gebruikt en of deze voldoet aan de laatste richtlijn vanuit het NCSC. (https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mel/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls/ICT-	Versleuteling	10.1 Cryptografische beheersmaatregelen	X
32	Subcontracting vindt alleen plaats na goedkeuring van het Kadaster	Beveiligbaarheid	15.1 Informatiebeveiliging in leveranciersrelaties	X
33	De leverancier gebruikt de OWASP richtlijnen voor applicatie security. Behalve een check op de code, controle op de procedures, is een penetratietest onderdeel van deze richtlijn en levert daarmee het bewijs dat een systeem voldoet aan de hoogste veiligheidseisen. De resultaten van check op de OWASP richtlijn dient jaarlijks overhandigd te worden aan het Kadaster. De kosten voor het aanpassen op deze	Onwikkeling	14.2 Beveiliging in ontwikkelings- en ondersteunende processen	X
35	Klanten (tenants) van leverancier zijn logisch gescheiden en kunnen elkaar onderling niet beïnvloeden als gevolg van verstoringen in de	Beschikbaarheid	17.1 Informatiebeveiligingscontinuïteit	X
37	Indien in een nieuwe aangeboden versie nieuwe functionaliteiten bevat voorziet de leverancier in documentatie omtrent gewijzigde of nieuw	Onderhoudbaarheid	12.5 Beheersing van operationele software	X
38	De leverancier kan op verzoek of Kadaster door middel van selfservice extra gescheiden omgevingen (tenants) aanmaken voor het Kadaster.	Functioneel	18.1 Naleving van wettelijke en contractuele eisen	X
39	De helpdesk van de leverancier is beschikbaar voor technische vragen vanuit het Kadaster zonder dat daarvoor aanvullende kosten in rekening worden gebracht. De helpdesk van de leverancier beantwoordt vragen binnen de reactietijd benoemd in de Kadaster SLA De leverancier verhelpt storingen binnen de oplostijden in de Kadaster SLA. Afwijkingen van deze termijnen vinden plaats in overleg en	Onderhoudbaarheid	15.2 Beheer van dienstverlening van leveranciers	X
40	Bij beëindiging van de overeenkomst is er een mogelijkheid om alle binnen de leverancier opgeslagen Kadaster gegevens (via bijvoorbeeld export bestanden) over te dragen aan het Kadaster. Daarna zullen de Kadaster gegevens door leverancier gegarandeerd en aantoonbaar	Overdraagbaarheid	18.1 Naleving van wettelijke en contractuele eisen	X
41	Het Kadaster blijft ten alle tijden eigenaar van haar gegevens (data).	Overdraagbaarheid	08.1 Verantwoordelijkheid voor bedrijfsmiddelen	X
42	Om data over te dragen bij een eventuele andere leveranciers wordt volledige medewerking verleend. Leverancier moet maatregelen hebben getroffen om een eventuele exit zo makkelijk mogelijk te maken.	Overdraagbaarheid	15.1 Informatiebeveiliging in leveranciersrelaties	X
43	De leverancier voldoet en blijft voldoen aan de Algemene Verordening Gegevensbescherming (AVG) gedurende de looptijd van de overeenkomst	Privacy	18.1 Naleving van wettelijke en contractuele eisen	X

nr	Omschrijving	Type	BIO ref	Van toepassing
	De leverancier beschikt over certificering en hanteert de best practices m.b.t. informatiebeveiliging: a. Leverancier is ISO/IEC 27001 gecertificeerd of kan opzet en bestaan van beveiligingsmaatregelen aantonen middels een assessment die is goedgekeurd door een A&R Officer; b. Idealiter hanteert de leverancier de standaarden ISO/IEC 27002, 27017 en 27018 ; c. Indien de leverancier aan andere beveiligingsstandaarden voldoet worden deze aan de hand van de Cloud Controls Matrix (CCM) Framework zoals gepubliceerd door de Cloud Security Alliance beoordeeld.			
44	d. De leverancier beschikt over een Third Party Memorandum (accountantsverklaring, bij voorkeur ISAE 3402 type 2 of SOC 2 verklaring) die	Betrouwbaarheid	18.1 Naleving van wettelijke en contractuele eisen	x
	De leverancier beschikt over documentatie op basis waarvan Kadaster zich inhoudelijk een beeld kan vormen over de wijze waarop informatiebeveiliging door de leverancier wordt ingevuld. Deze documentatie gaat idealiter in op: a. de richtlijn m.b.t. informatiebeveiligingseisen die van toepassing zijn bij het ontwerp en de implementatie van de cloud dienst; b. risico's van geautoriseerde interne medewerkers; c. meerdere afnemers en scheiding van klanten binnen de cloud, inclusief virtualisatie; d. toegang tot cloud middelen van de klant door de leverancier van de clouddoplossing; e. toegangsbeveiligingsprocedures, zoals sterke authenticatie voor beheertoegang tot de cloud diensten; f. communicatie richting cloud klanten tijdens wijzigingenbeheer; g. beveiliging van de virtualisatie technologie (systeem waar virtuele systemen op draaien, zoals windows servers, virtuele firewalls etc.); h. toegang tot en bescherming van klantdata in de cloud; i. communicatie bij inbreuken en datalekken en informatieuitwisselings procedures ter ondersteuning van (forensische) onderzoeken; j. logging en monitoring van de dienst en de mogelijkheid om security logging aan te sluiten op de SIEM oplossing van het Kadaster;			
45	k. hoe beveiligingsmaatregelen ingeregeld zijn voor data die opgeslagen en uitgewisseld wordt.	Beveiligbaarheid	18.1 Naleving van wettelijke en contractuele eisen	x