KEURMERK ZEKER-ONLINE

Zeker-OnLine is een onafhankelijk en transparant keurmerk voor online dienstverlening (cloud services)

Achtergrond normenkader

Eerste versie 1.0 : sept 2013
Herziene versie 2.0 juni 2014

Inhoudsopgave

1. Kwaliteitseisen en normenkader

1.1 Inleiding

Ter verkrijging van het keurmerk worden hoge eisen gesteld aan de betrouwbaarheid van de dienstverlening door de deelnemer.
Het keurmerk staat voor betrouwbaarheid, veiligheid, continuïteit, kwaliteit in functionaliteit en juridische zekerheid.

Op basis van deze uitgangspunten is een stelsel van kwaliteitseisen en normen ontwikkeld.
Deze zijn vastgelegd in deze sectie “Kwaliteitseisen en normenkader”.
Hierbinnen zijn 3 kwaliteitsgebieden te onderscheiden:

- Technische infrastructuur (IT Beheer en Beveiliging);
- Applicatie structuur (generieke en specifieke maatregelen in de applicatie);
- Juridische infrastructuur.

Voor elk van deze deelgebieden zijn normen vastgesteld. De samenhang tussen de deelgebieden is uitgewerkt in het raamwerk, het conceptuele model.

De kern van het stelsel is dat ‘de omgeving’ centraal staat. Immers een betrouwbare en veilige infrastructuur staat voorop. De functionaliteit is dan niet van doorslaggevende betekenis. Binnen die infrastructuur zijn verschillende online administratieve diensten te bouwen en kunnen gegevens doelmatig worden uitgewisseld. Het stelsel is daarom een schaalbaar concept, dat in de nabije toekomst nog kan worden uitgebouwd. Hoe snel dat gaat en welke richting gekozen gaat worden is afhankelijk van de marktontwikkelingen. Natuurlijk spelen hier ook de wensen van de ‘community’ en van de klanten een belangrijke rol. Het normenkader evolueert met het raamwerk mee. Er is, met andere woorden, sprake van een dynamisch geheel. De ontwikkelingen ‘in the cloud’ zijn immers van dien aard dat voortdurende vernieuwing nodig zal blijken. Dit wordt ondervangen door een active informatieplicht vanuit de deelnemers naar de auditor. De normcommissie is verantwoordelijk voor het actueel houden van het normenkader, de Raad van Toezicht stelt formeel het normenkader vast op basis van het voorstel van het Bestuur.

Het stelsel wil innovatie aanmoedigen, maar is tegelijkertijd robuust en sluit waar mogelijk aan op bestaande en breed geaccepteerde standaarden. Dit geldt daarmee ook voor het normenkader. Niettemin is dat qua samenstelling uniek, omdat er nog geen vergelijkbare concepten bestaan en omdat het de verschillende deelgebieden verbindt.

Waar mogelijk is het stelsel ‘principle based’. Daar waar het karakter meer rules based worden voorbeelden gegeven. Basis is immers het zorgen voor een vergelijkbaar beveiligingsniveau en een toetsbare norm. Nergens schrijft het normenkader echter het gebruik van specifieke technologieën voor.

1.2 Het stelsel van kwaliteitseisen

1.2.1 Schematische weergave van het stelsel

Hiervoor zijn de deelgebieden genoemd die bij online administratieve dienstverlening onderkennen. Voor elk van deze deelgebieden zijn kwaliteitseisen vastgesteld en is een normenkader ontwikkeld, waarmee een van de belangrijke pijlers voor het keurmerk Zeker-OnLine is gerealiseerd.

Een schematische weergave van het stelsel, het zogenaamde 'lagenmodel' met de deelgebieden in hun onderlinge samenhang, ziet er als volgt uit:

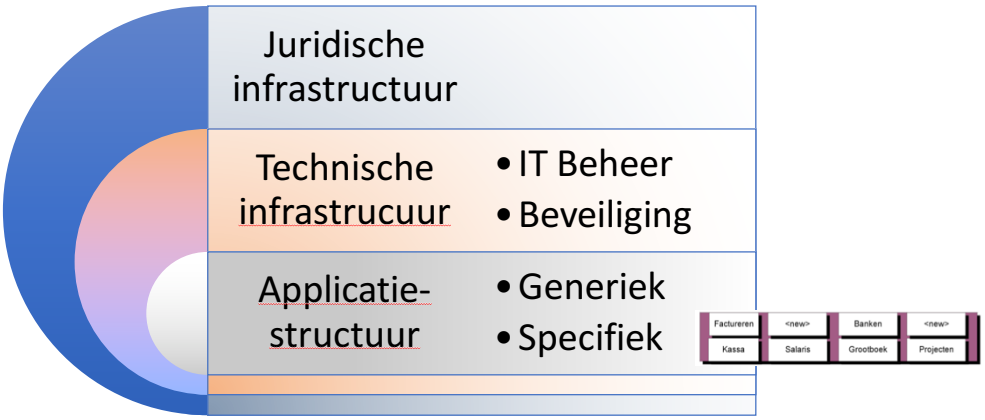


fig. 1

De *juridische infrastructuur* omvat het juridische deel van de kwaliteitseisen. Behalve 'good practices' uit accountancy, IT-audit en informatiebeveiliging zijn immers ook de aspecten van belang die de dienstaanbieder en zijn klanten een duidelijke rechtspositie verschaffen. Daarom is de juridische infrastructuur de basis van het stelsel. De juridische normen schragen immers de andere deelgebieden die we voor de online administratieve dienstverlening onderkennen.

Het onderscheid tussen de *technische infrastructuur* en de *applicatiestructuur* is gebaseerd op het onderscheid binnen de online administratieve dienstverlening tussen de Dienst en de Applicatie (de administratieve toepassing). Met het aanbieden van de applicatie binnen een totaalpakket onderscheidt die online administratieve dienstverlening zich van een installeerbaar softwarepakket door de gebruiker. De online oplossing omvat immers, naast de applicatie, ook het hele scala van IT-beheer door specialisten en de technische infrastructuur.

1.2.2 Dienst en applicatie

De dienst (technische infrastructuur)

Binnen de dienst zijn twee deelgebieden te onderscheiden, namelijk het *IT-beheer* en de *technische beveiligingsmaatregelen*.

Bij IT-beheer ligt de focus op het IT-beleid en de organisatorische aspecten. Met behulp van technische maatregelen in hardware en infrastructuur en door veilige internetverbindingen wordt het IT-beheer - zo veel als technisch en economisch verantwoord is - afgedwongen. In de IT-terminologie wordt dat 'hardening' genoemd. Opzet en werking van het IT-beheer moeten goed zijn. Het samenstel van organisatorische en technische maatregelen zorgt voor een betrouwbare, veilige en continu beschikbare dienst. Vanuit dit perspectief krijgen IT-beheer en technische beveiligingsmaatregelen hun plek in (de schematische weergave van) het raamwerk. Zij vormen immers weer het fundament waarop de applicatie goed genoeg kan werken.

De applicatie (administratieve structuur)

Bij 'de applicatie' staat de softwaretoepassing centraal. De wijze waarop de klant die ervaart is essentieel. De applicatie omvat de programmatuur en de functionele helpdesk. Hier worden eveneens twee deelgebieden onderkend die aandacht vragen, namelijk de *generieke functionaliteit* en de *specifieke functionaliteit*. Alle algemene maatregelen die betrekking hebben op de softwaretoepassing worden gerangschikt onder de generieke functionaliteit.

Bij de specifieke maatregelen is de focus gericht op de mogelijkheden die de softwaretoepassing zelf biedt of, met andere woorden, op wat de klant met de toepassing kan doen.

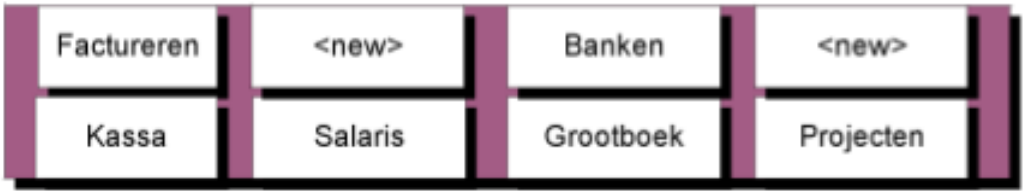
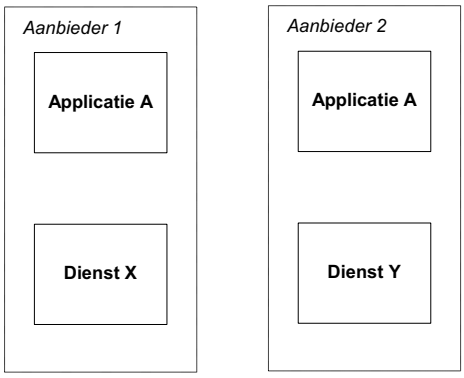


fig. 2

In het raamwerk steunt de generieke functionaliteit op de juridische infrastructuur, het IT-beheer en de technische beveiligingsmaatregelen en ondersteunt ze op haar beurt de specifieke maatregelen in de applicatie.

Impact op het keurmerk

In de vorige paragraaf is aangegeven dat de online administratieve dienstverlening uit de dienst en de applicatie bestaat. Echter, de scheidslijn tussen beide onderdelen kan niet altijd even scherp kan worden getrokken. Voor de praktijk is dit echter minder relevant. Het keurmerk wordt immers alleen afgegeven op het samenstel van de onderdelen, met andere woorden voor de volledige online administratieve dienstverlening en per aangeboden dienst.



Figuur 5

Als twee verschillende online administratieve diensten waarin eenzelfde applicatie actief is beide een keurmerk wensen, dan zal er dus tweemaal een keurmerk moeten worden aangevraagd. Immers 'de omgeving' staat centraal en niet de functionaliteit. In figuur 5 ziet u dit schematisch weergegeven: Aanbieder 1 kan een "eigen" administratieve cloudoplossing aanbieden door gebruik te maken van (white label) oplossing en een hosting dienst. Het eigen is hier de naam/website waaronder de dienst wordt aangeboden. De (white label) oplossing kan hierbij door een externe software ontwikkelaar zijn geprogrammeerd. Bijvoorbeeld door ontwikkelaar A. De hosting dienst kan door aanbieder 1 zelf worden beheerd; ook is het mogelijk dat gebruik wordt gemaakt van een gespecialiseerde derde partij. Bijvoorbeeld hosting partij X.
De (white label) oplossing van X wordt in figuur 5 ook gebruikt als dienst die wordt aangeboden door Aanbieder 2.

Het is mogelijk dat een deel van de audit niet tweemaal uitgevoerd hoeft te worden. Er kan immers gebruik gemaakt worden van eerder uitgevoerde werkzaamheden, waardoor er toch een kostenvoordeel ontstaat. Gelijke 'instances' in applicatie en dienst, die door of namens één dienstaanbieder worden beheerst, worden gezien als één omgeving. Naast de multitenancy-oplossing is er dus ook ruimte voor multi-instancing.

Omwille van de herkenbaarheid en transparantie vindt de community het niet wenselijk dat één dienstaanbieder onder dezelfde 'merknaam' zowel een keurmerkoplossing als een ander product aanbiedt. Het motto luidt hier: 'Één merk, één keurmerk'.

Het raamwerk biedt wel de mogelijkheid dat dezelfde applicatie door verschillende aanbieders in een administratieve cloudoplossing onder hun eigen merknaam wordt aangeboden. De bouwer van die applicatie brengt ze dan uit als 'white label'. Als deze applicatie kwalificeert en de aanbieder zorgt ervoor dat ze in een betrouwbare, veilige en continu beschikbare omgeving wordt opgenomen, dan kan hij voor een keurmerk in aanmerking komen. Zo ondersteunt het Zeker-Online-concept de verwachte specialisatie bij het ontwikkelen van applicaties en het aanbieden van clouddiensten.

1.2.3 Nader toelichting op het stelsel

Algemeen

Het stelsel gaat uit van verantwoordelijkheden. Voor de beheermaatregelen met betrekking tot 'de dienst' (IT-beheer en technische beveiligingsmaatregelen) is de dienstaanbieder verantwoordelijk. Dat geldt bijvoorbeeld voor het verlenen van toegang aan (gedelegeerde) gebruikers tot de juiste administratie binnen een multitenancy-omgeving. De klant blijft echter verantwoordelijk voor zijn eigen administratie. Daarom is de delegatie van bevoegdheden binnen zo'n administratie dan ook belegd bij de klant zelf.

Waar werkzaamheden door de dienstaanbieder worden uitbesteed aan derden blijft de dienstaanbieder wel verantwoordelijk voor de totale online administratieve dienstverlening (cloudoplossing). Uitbesteden mag er bijvoorbeeld niet toe leiden dat de auditor de oplossing niet als geheel zou kunnen beoordelen. Bij de selectie van zijn leveranciers moet de dienstaanbieder hier dus rekening mee houden.

IT-beheer

Uitgangspunt is dat de dienstaanbieder de IT steeds afstemt op de dienstverlening aan de klant. Die dienstverlening richt zich op het helpen van de klant bij zijn bedrijfsprocessen en de administratieve vastleggingen die daarmee te maken hebben. Hiervoor moet de dienstaanbieder goed weten welke wensen en eventuele problemen de klant heeft. Het goed inrichten van het IT-beheerproces is de expliciete verantwoordelijkheid van het management van de dienstaanbieder. Ook in dit opzicht mogen we van het management voorbeeldgedrag verwachten. Het inrichten en beheersen van de organisatie en de processen hoort daarbij. De dienstverlening moet ertoe leiden dat hetgeen met de klant werd afgesproken ook daadwerkelijk voortdurend wordt geleverd.

Bij het opstellen van de normen voor IT-beheer heeft de werkgroep 'COBIT' als basis genomen. Voor Zeker- Online is dit breed geaccepteerde normenkader toegespitst op het specifieke karakter van een administratieve cloudoplossing.

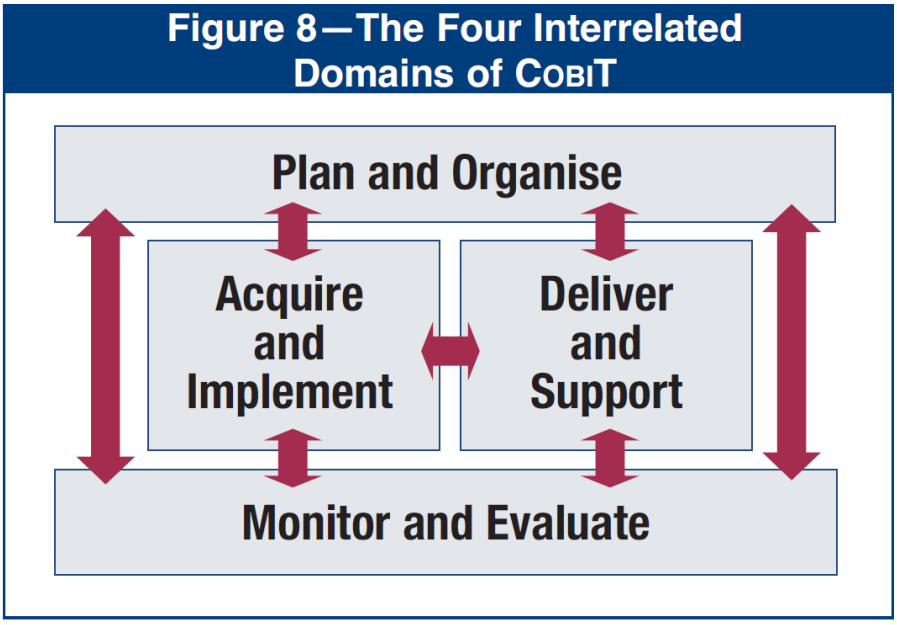


fig. 3

Beveiliging

De dienstaanbieder moet gebruik maken van up-to-date en veilige IT-oplossingen, die in lijn zijn met het IT-beheer. Omdat de techniek zich voortdurend ontwikkelt, heeft de Normcommisie gezocht naar een dynamisch normenkader. De normcommisie heeft dit gevonden bij de ICT-beveiligingsrichtlijnen van het National Cyber Security Center. Daarmee sluit het normenkader van de Stichting goed aan bij een gezaghebbend en praktisch haalbaar normenkader en is ook het toekomstig onderhoud goed geborgd. Het normenkader Zeker- Online en de ICT-beveiligingsrichtlijnen versterken elkaar.

Generieke functionaliteit

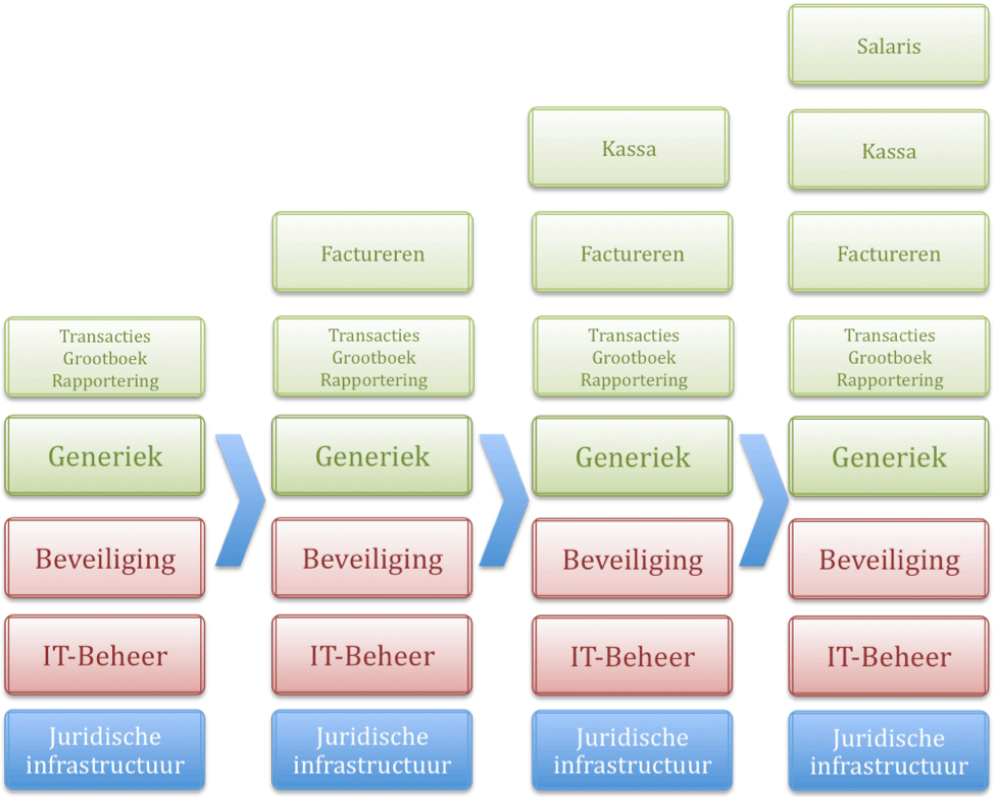
Alle algemene maatregelen die betrekking hebben op de softwaretoepassing zijn gerangschikt onder de generieke functionaliteit. Dit wordt daarmee een breed aandachtsgebied. Onderwerpen die aan de orde komen zijn onder andere logische toegangsbeveiliging, isolatie van data, verwerken en bewaren van aangeboden transacties, zorgen voor data-integriteit, bewerkstellingen van een adequate audit trail, logging door de gebruiker, het creëren van mogelijkheden om het verwerkingsproces te monitoren, change-management en documentatie. Daarnaast zijn de maatregelen die toezien op de wijze waarop koppelingen met externe systemen, zoals andere cloudoplossingen, worden gerealiseerd en over de documenten en de rapporten die kunnen worden gemaakt onderdeel van de audit.

Specifieke functionaliteit

De specifieke functionaliteit betreft de mogelijkheid die de softwaretoepassing zelf biedt of, met andere woorden, over datgene wat de klant met de toepassing kan doen. Voorbeelden van specifieke functionaliteit zijn boekhouden of het elektronisch aanmaken, inlezen en verwerken van facturen of het automatisch inlezen en verwerken van bankafschriften. Om te komen tot een betrouwbare administratie is software nodig waarmee de gebruiker transacties juist, volledig en tijdig kan vastleggen. Specifieke applicatieve maatregelen zorgen ervoor dat dit ook feitelijk gebeurt. De kwaliteit van de data en compliance aan wet-en regelgeving staan daarbij centraal.

1.2.4 Verdere ontwikkeling

Vooralsnog richt Zeker-OnLine zich op de kernfunctionaliteit van de financiële administratie. De community, het samenwerkingsverband van aanbieders van online administratieve diensten, bepaalt in onderling overleg de volgorde en het tempo van de normontwikkeling voor andere en/of nieuwe functionaliteit. Het is een dynamisch proces, dat als volgt schematisch kan worden uitgetekend:



Aangezien de infrastructuur centraal staat en niet de functionaliteit, kunnen ook andere web based-cloudoplossingen dan alleen financieel-administratieve in de nabije toekomst ook in aanmerking komen voor het keurmerk. Voorbeelden zijn e-factureren, e-bankieren,web based-salarisverwerkingsdienst of een online kassasysteem.

Het Zeker-Online-platform biedt zo een basis voor een naadloze samenwerking tussen verschillende administratieve cloudoplossingen en moedigt innovatie aan.