



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Digikoppeling Compliancevoorziening en Requirements

Versie 1.1

Datum 6 januari 2010

Colofon

Projectnaam	Digikoppeling
Versienummer	Definitief
Organisatie	Servicecentrum Logius Postbus 96810 2509 JE Den Haag T 0900 555 4555 servicecentrum@logius.nl
Bijlage(n)	0

Inhoud

Colofon	2
Inhoud	3
1 Inleiding	4
1.1 <i>Doel en Doelgroep</i>	4
1.2 <i>Opbouw Digikoppeling documentatie</i>	4
1.3 <i>Digikoppeling</i>	4
1.4 <i>Opbouw van dit document</i>	5
2 Positionering Compliancevoorzieningen 1.0	6
3 Belanghebbenden en gebruikers	7
3.1 <i>Rollenoverzicht belanghebbenden en gebruikers</i>	7
3.2 <i>Gebruikers en Compliancevoorziening WUS</i>	7
3.3 <i>Gebruikers en Compliancevoorziening ebMS</i>	9
3.4 <i>Systeemperspectief</i>	10
4 Functionele en niet-functionele requirements	11

1 Inleiding

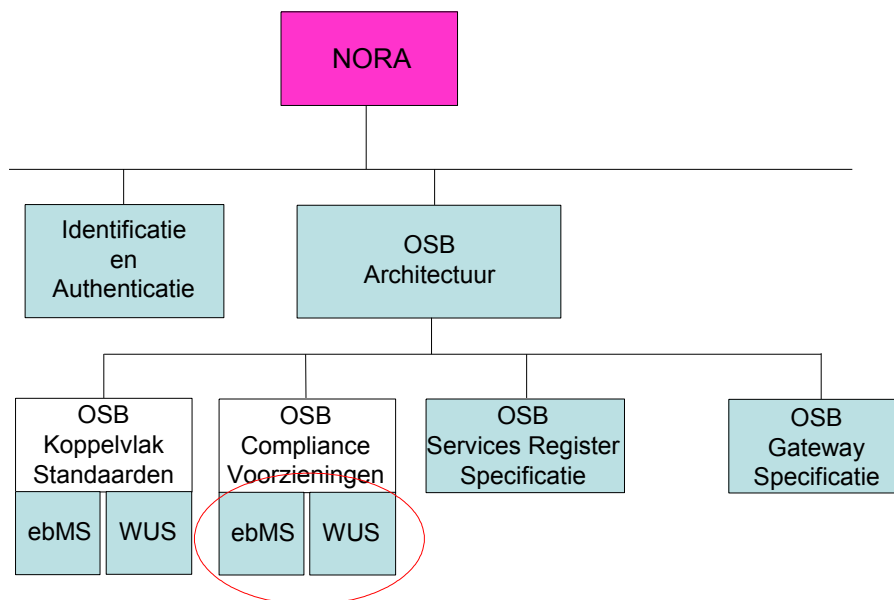
1.1 Doel en Doelgroep

Dit document geeft een overzicht van de requirements voor de Compliancevoorzieningen.

Het document is bestemd voor projectleden van Digikoppeling (voorheen Overheidsservicebus).

1.2 Opbouw Digikoppeling documentatie

Digikoppeling is beschreven in een set van documenten. Deze set is als volgt opgebouwd.



Dit document betreft de beschrijving van requirements (vereisten) voor de Compliancevoorzieningen.

1.3 Digikoppeling

Deze paragraaf bevat zeer beknopt een aantal hoofdpunten uit de overige documentatie.

Doel en scope van Digikoppeling

Digikoppeling biedt de mogelijkheid om op sterk gestandaardiseerde wijze berichten uit te wisselen tussen service providers (serviceaanbieders) en service requesters (serviceafnemers).

Digikoppeling richt zich in eerste instantie uitsluitend op uitwisselingen tussen overheidsorganisaties.

De uitwisseling tussen service providers en requesters wordt in drie lagen opgedeeld:

- Inhoud: op deze laag worden de afspraken gemaakt over de inhoud van het uit te wisselen bericht, dus de structuur, semantiek,

waardebereiken etc.

Digikoppeling houdt zich niet met de inhoud bezig, heeft "geen boodschap aan de boodschap".

- Logistiek: op deze laag bevinden zich de afspraken betreffende transportprotocollen (HTTP), messaging (SOAP), adressering, beveiliging (authenticatie en encryptie) en betrouwbaarheid.
- Transport: deze laag verzorgt het daadwerkelijke transport van het bericht. Digikoppeling richt zich uitsluitend op de logistieke laag. Deze afspraken landen in de koppelvlakstandaarden en andere voorzieningen.

Leidend principe (requirement)

De koppelvlakstandaarden dienen te leiden tot een maximum aan interoperabiliteit met een minimum aan benodigde ontwikkelinspanning. Daarom is gekozen voor bewezen interoperabele internationale standaarden.

Digikoppeling maakt uitwisseling van berichten mogelijk op basis van de ebXML/ebMS en WUS families van standaarden incl. de daarbij behorende andere standaarden.

De voor Digikoppeling vereiste interoperabiliteit van de WUS standaarden van OASIS en W3C is gebaseerd op de profielen (en tests) van WS-I. De interoperabiliteit van ebMS is gebaseerd op de standaard ebMS versie 2 (ISO standaard), en Drummond tests/certificering.

1.4 Opbouw van dit document

Dit hoofdstuk 1 bevat de inleiding. In hoofdstuk 2 volgt een overzicht van de positionering van de compliancevoorzieningen. Hoofdstuk 3 is een toelichting van de gebruikers en hoofdstuk 4 beschrijft de requirements.

2 Positionering Compliancevoorzieningen 1.0

De communicatieprotocollen voor berichtenverkeer in het domein van Digikoppeling staan beschreven in de Koppelvlakstandaarden voor ebMS en WUS webservices. Voor de implementatie van deze standaarden zijn verschillende producten op de markt. Deze producten, en dan vooral hun configuratie, voldoen echter niet altijd aan de Koppelvlakstandaarden.

Digikoppeling stelt een aantal compliancevoorzieningen ter beschikking om overheidsorganisaties te helpen bij het inrichten van berichtenverkeer in het domein van Digikoppeling. Met deze compliancevoorzieningen kunnen overheidsorganisaties verifiëren of de koppelvlakstandaard op de juiste manier is geïmplementeerd.

De achterliggende gedachte is, dat er bij een eerste implementatie van protocollen vaak onduidelijkheid is over de exacte betekenis van de koppelvlakstandaarden. Daardoor kunnen fouten optreden in de implementatie en/of configuratie. Bijvoorbeeld omdat de gebruikte producten niet voldoen aan de betreffende koppelvlakstandaarden, of door een verkeerde interpretatie van de standaarden. In het ergste geval zal er geen berichtenverkeer mogelijk zijn tussen verschillende implementaties bij de overheidsorganisaties. De compliancevoorzieningen zijn er om deze situaties te voorkomen.

3 Belanghebbenden en gebruikers

Met betrekking tot de Compliancevoorzieningen zijn een aantal belanghebbenden en gebruikers geïdentificeerd. Hier beschrijven we alleen de belanghebbenden. Gebruikers hebben namelijk verschillende functies binnen verschillende overheidsorganisaties.

3.1 Rollenoverzicht belanghebbenden en gebruikers

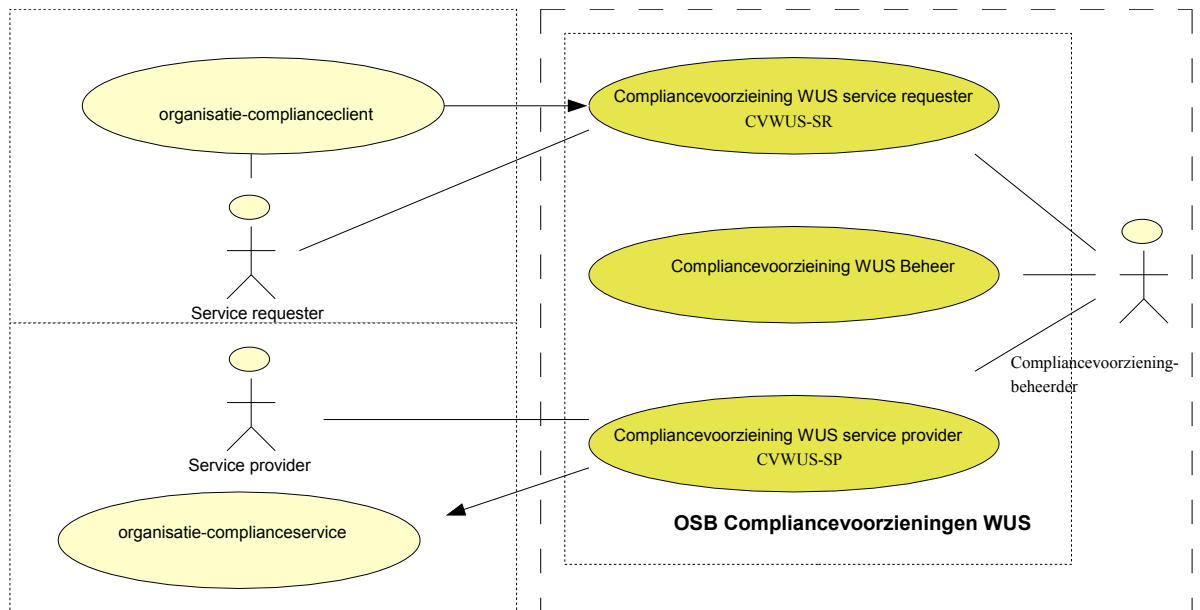
Rol	Beschrijving	Verantwoordelijkheden
Overheids-organisaties	Alle overheidsorganisaties kunnen gebruikmaken van de compliancevoorzieningen. Ze staan aangegeven als service requesters (SR) en service providers (SP).	Gebruikt beschikbare voorzieningen om communicatiestromen in het domein van Digikoppeling vóór productie goed te kunnen testen.
Compliance-voorzieningen-beheerder	Compliancevoorzieningen worden momenteel beheerd door het ICTU programma ODP. Het Digikoppeling project is hier een onderdeel van.	Zorgt ervoor dat het systeem beschikbaar is en levert ondersteuning indien nodig.
Technisch overleg	Vertegenwoordigt de visie van de overheidsorganisaties.	Bepaalt of het concept van de compliancevoorzieningen overeenkomt met de gewenste functionaliteit van de overheidsorganisaties.

3.2 Gebruikers en Compliancevoorziening WUS

De Compliancevoorziening is een op zichzelf staand systeem dat toegankelijk is vanuit het Internet. Het bestaat uit een component voor WUS en een component voor ebMS. Elk component heeft zijn eigen interface voor configuratie en beheer. Daarnaast biedt elk component specifieke functionaliteit voor de SP en voor de SR, aangeduid met:

- CVSP: compliancevoorziening voor de service provider;
- CVSR: compliancevoorziening voor de service requester;

Waar nodig wordt de term CVSP en CVSR nader gespecificeerd naar koppelvlakstandaard (bijvoorbeeld CVWUS-SP voor de WUS-specifieke CVSP).



Figuur 1. Gebruikers Compliancevoorzieningen WUS 1.0

De onderstaande use cases zijn onderkend en zullen worden uitgewerkt in afzonderlijke documenten.

De use cases voor de organisatie zijn:

- 01 Test met CVWUS-SR
- 02 Test met CVWUS-SP
- 03 Download WS-I testrapport van CVWUS-SR

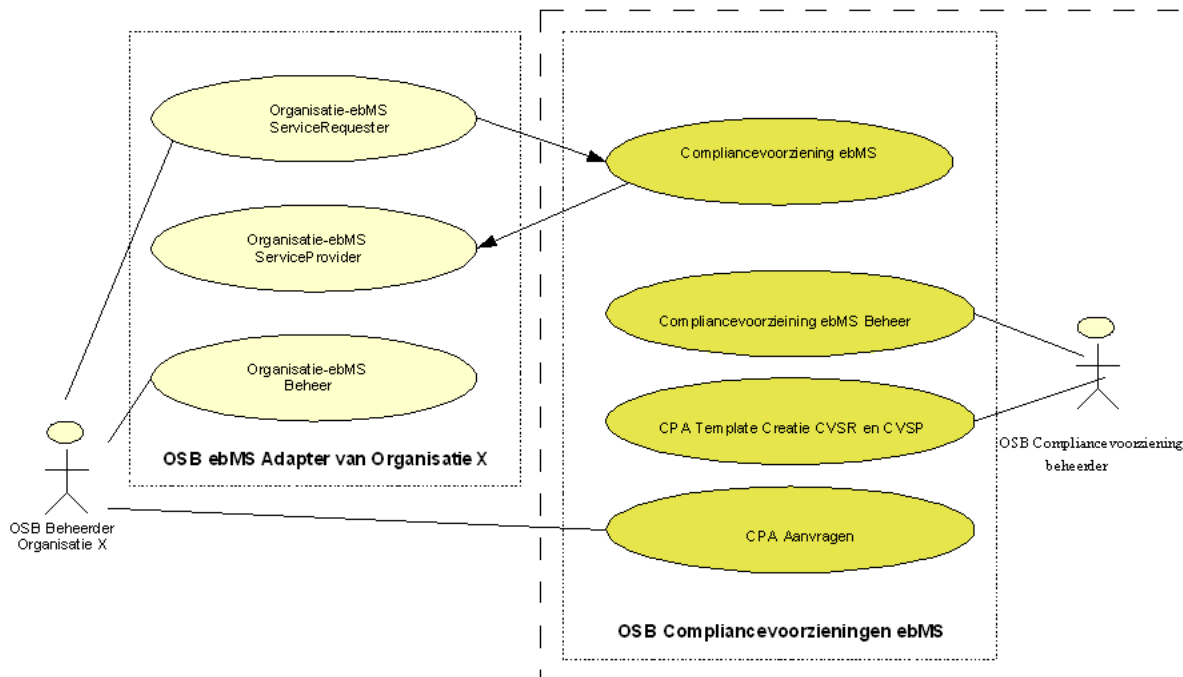
De use cases voor de compliancevoorziening zijn:

- 04 UCS OCVW Validatie PKI Overheid certificaat

De use cases voor de compliancevoorziening-beheerder zijn:

- 05 Inloggen Beheer
- 06 Uitloggen Beheer
- 07 Beheer-Wijzig wachtwoord
- 08 Beheer-Certificaten

3.3 Gebruikers en Compliancevoorziening ebMS



Figuur 2. Gebruikers Compliancevoorzieningen ebMS 1.0

De onderstaande use cases zijn onderkend en zullen worden uitgewerkt in afzonderlijke documenten.

De use cases voor de organisatie zijn:

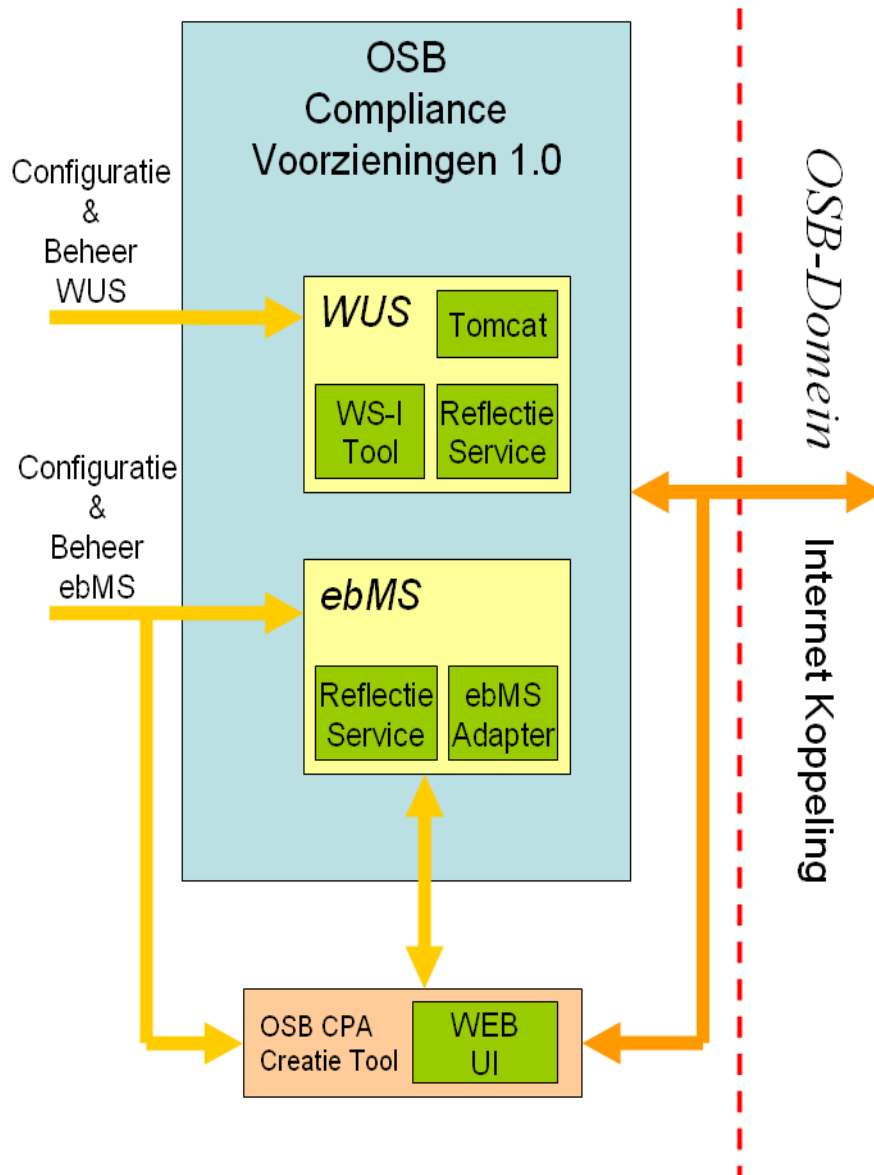
- [UC-E-01] Use Case Organisatie ebMS service requester
- [UC-E-02] Organisatie ebMS service provider
- [UC-E-03] Organisatie ebMS beheer

De use cases voor de compliancevoorziening zijn:

- [UC-E-04] Compliancevoorziening ebMS (CVebMS)
- [UC-E-05] Compliancevoorziening ebMS beheer
- [UC-E-06] CPA template creatie CVebMS-SR en CVebMS-SP
- [UC-E-07] CPA aanvragen

3.4 **Systeemperspectief**

In het systeemperspectief staan de verschillende systeemcomponenten met de daarin gebruikte modules.



Figuur 3. Systeem perspectief van de Compliancevoorzieningen 1.0

4 Functionele en niet-functionele requirements

In dit hoofdstuk staan de vereisten waaraan de compliancevoorzieningen moeten voldoen. De prioriteitsaanduiding 'M' geeft aan dat het onderdeel zal uitmaken van de Compliance Voorziening 1.0.

ID	Omschrijving requirement	Prioriteit
OCV-R1	Communicatie met de compliancevoorzieningen ten behoeve van de validatie van berichten dient op basis van HTTPS (tweezijdige SSLv3/TLS 1.0) en HTTP mogelijk te zijn. Afhankelijk van de gekozen instelling of endpoint moet hierop ook getoetst kunnen worden.	M
OCV-R2	De organisatie als WUS service provider krijgt een webinterface geboden (CVSP) vanwaar hun organisatie-complianceservice aangeroepen kan worden. De berichten voldoen zoals opgesteld in de Compliancevoorziening WUS WSDL.	M
OCV-R3	De compliancevoorziening stuurt (als Service Requester) een melding naar de organisatie (die zich als Service Provider geconfigureerd heeft). De berichten voldoen aan de vereisten als opgesteld in de Compliancevoorziening ebMS CPA. Hier is één operatie in gedefinieerd (CVSP-Melding).	M
OCV-R4	De CVWUS-SR biedt de organisatie als service requester de mogelijkheid om via hun organisatie-compliancecliënt de CVSR aan te roepen conform Koppelvlakstandaard WUS. Hierin zijn twee operaties gedefinieerd (ping en toUppercase). De pingfunctie retourneert exact dezelfde string als binnengekomen bij het request. De toUppercase-functie zet alle karakters (a-z, A-Z) om in hoofdletters.	M
OCV-R5	De CVebMS-SR biedt de organisatie als service requester de mogelijkheid om via hun organisatie-compliance ebMS adapter de CVSR aan te roepen conform de Koppelvlakstandaard ebMS. Hier is één operatie in gedefinieerd (Digikoppeling-SR-Melding).	M
OCV-R6	Er worden duidelijke foutmeldingen gegeven. Dit helpt de gebruiker bij zowel het analyseren van de fouten als bij het verbeteren van de implementatie en/of configuratie.	M
OCV-R7	Het systeem is in staat om een aantal systeemactiviteiten te registreren en op te slaan. Na inloggen kunnen deze worden ingekeken. Alle loggegevens, voor zowel CVSP als CVSR, kunnen middels een interface ingekeken worden. Er is een filter mogelijkheid om zowel functionele meldingen en foutmeldingen te kunnen selecteren. Een aantal belangrijke activiteiten die gelogd moeten kunnen worden zijn: <ol style="list-style-type: none"> 1. Berichtenverkeer tussen OCVSP en Organisatie-compliance SP. (M) 2. Berichtenverkeer tussen OCVSR en Organisatie-compliance SR. (M) 3. Inloggen/uitloggen door de compliancevoorziening-beheerder. (S) 4. Installeren PKI certificaat hiërarchie door de compliancevoorziening-beheerder. (S) 5. Verwijderen WS-I rapportage door de compliancevoorziening-beheerder. (S) 6. Foutmeldingen en excepties. (M) 	M/S

OCV-R8	De CVWUS-SR en CVWUS-SP bieden de SR of SP de mogelijkheid om de berichten die hun implementatie verstuurt te valideren op WS-I B.P. conformance. De berichten worden verstuurd op basis van communicatie conform Koppelvlakstandaard WUS (SSL/TLS). Omdat de WS-I validatie tegelijkertijd plaatsvindt met validatie van Digikoppeling WUS compliance, is er een optie om WS-I validatie uit te schakelen. Zo komen in het resultaatsscherm allen zaken met betrekking op Digikoppeling WUS validatie. Voor de CVSR komt een scherm waar alle gegenereerde rapporten te downloaden zijn. Deze kunnen door de beheerder van de compliancevoorziening opgeschoond worden.	M
OCV-R9	De verificatie is eenmalig. Door het uitvoeren van de verificatie zal de betreffende overheidsorganisatie inzicht krijgen in de betekenis, werking en implementatieaspecten van de koppelvlakstandaarden. Digikoppeling verwacht dat de betreffende overheidsorganisatie deze vaardigheden zal gebruiken bij het ontwikkelen van services voor het domein van Digikoppeling.	M
OCV-R10	Digikoppeling definieert de service. Digikoppeling bepaalt de specificatie van de service waarmee zowel een service provider als een service requester de verificatie kan uitvoeren. Er vindt geen verificatie plaats van een service die door de betreffende overheidsorganisatie wordt of is gebouwd.	M
OCV-R11	De testen kunnen tegelijkertijd uitgevoerd worden. Het uitvoeren van de testen met de compliancevoorzieningen kan niet door meerdere overheidsorganisaties tegelijkertijd gedaan worden.	S
OCV-R12	Uitvoeren van de compliancetest gebeurt zonder inzet van de beheerder van de compliancevoorzieningen.	M
OCV-R13	Bij de CVSR krijgt de SR de mogelijkheid om verschillende end points te gebruiken, zodat bepaalde fouten optreden op HTTP of SOAP niveau. De CVSP kan ook diverse aanroepen doen die een voorgedefinieerde fout bevatten. Zo wordt getest hoe de webservice daarop reageert. Overzicht van in te stellen fouten: 1. Invalide opbouw van het bericht (bijvoorbeeld ontbreken van een element) 2. Communicatie op basis van een verlopen certificaat 3. Communicatie op basis van een niet valide certificaat (geen test certificaat op basis van vereiste hiërarchie). In geval van Digikoppeling WUS: 1 Test met het ontbreken van verplichte WS-addressing headers 2 Er is een endpoint waarmee over http mee gecommuniceerd kan worden.	C
OCV-R14	De CV test alleen de logistieke functionaliteit.	M
OCV-R15	De CV valideert, naast de logistieke functionaliteit, ook de payload functional middels een xsd.	S
OCV-R16	De compliancevoorziening heeft een beschikbaarheid van 24x7 waarbij de ondersteuning in het geval van problemen 10x5 is ("kantooruren").	M
OCV-R17	De responsetijden van de compliancevoorzieningen liggen in de orde van grootte van seconden.	M

OCV-R18	De compliancevoorziening kan een belasting aan van ongeveer 5 concurrent "gebruikers" (interactief of computer-computer).	M
OCV-R19	De user-interfaces van de verschillende componenten van de compliancevoorziening hebben dezelfde look-and-feel en dezelfde opbouw.	S
OCV-R20	Alle user interfaces moeten via internet (met een web browser) benaderbaar zijn. Ze moeten allemaal voldoen aan de webrichtlijnen van overheid.nl (http://www.webrichtlijnen.nl/).	M
OCV-R21	Op elk scherm waar invoervelden staan, heeft de GUI een knop/link naar een scherm met helpteksten	S
OCV-R22	Attachments die ontvangen zijn moeten teruggestuurd worden in het response bericht. (Conform Digikoppeling 2.0)	M
OCV-R23	Als een bericht ontvangen is dat ondertekend is, zal het responsebericht ook ondertekend moeten zijn. (Conform Digikoppeling 2.0)	M
OCV-R24	Als een bericht ontvangen is dat versleuteld (en ondertekend) is, zal het responsebericht ook versleuteld (en ondertekend) moeten zijn. (Conform Digikoppeling 2.0)	