



UITVOERING WERKNEMERSVERZEKERINGEN

# **GIV Integratiediensten**

# **Referentie Architectuur**

## **Lite**

Versie 1.1

Datum: 20-01-2023

**Versiebeheer**

Versie	Datum	Status	Korte beschrijving aanleiding / wijziging
0.1	25-10-2022	Concept	Eerste draft
1.0	03-11-2022	Definitief	
1.1	20-01-2023		Opmerking mbt cloud aansluiting MQ en FT toegevoegd.

Opgesteld door:

Mark Verlinden, Jochem IJzermans

Voor vragen opmerkingen:



## Inhoudsopgave

<b>VERSIEBEHEER .....</b>	<b>2</b>
<b>INHOUDSOPGAVE .....</b>	<b>3</b>
<b>1 INLEIDING .....</b>	<b>4</b>
1.1 Doel van het Document .....	4
1.2 Scope .....	4
<b>2 KADERSTELLING .....</b>	<b>5</b>
2.1 Integratiediensten .....	5
2.2 Positionering GIV/ID .....	5
2.3 UWV Service richtlijnen .....	6
2.4 Beveiliging .....	9
2.5 OTAP beleid .....	9
<b>3 TRANSPORT SERVICES .....</b>	<b>10</b>
3.1 Transport Policy Service .....	10
3.2 Transport Message Queue Service .....	10
3.3 Transport File Transfer Service .....	11
<b>4 BIJLAGEN .....</b>	<b>12</b>
4.1 Afkortingen .....	12
4.2 Terms of Service van de Service Provider .....	13
4.3 Service Contract Profielen .....	13

# 1 Inleiding

## 1.1 Doel van het Document

Dit document beschrijft de belangrijkste uitgangspunten voor het gebruik van de Transport Services van UWV GIV Integratiediensten (GIV/ID). Dit document is gebaseerd op de uitgebreid beschreven UWV referentie architectuur voor Transport Services. Het betreft hier de verplicht te gebruiken referentie architectuur voor integratie van interne en externe applicaties en services. Deze referentie architectuur is echter niet voor extern gebruik beschikbaar. Om deze reden is er een lite versie voor externe partijen en aanbestedingstrajecten. Het is een vertaling van de belangrijkste elementen uit de UWV referentie architectuur voor integratie. Het doel van dit document is om partijen bekend te maken met de integratierichtlijnen van UWV voor het koppelen van systemen aan het UWV eco-systeem.

## 1.2 Scope

Dit document richt zich op de integratievraagstukken tussen externe partijen, cloudvoorzieningen en standaardpakketen volgens de wijze waarop UWV kan en wil integreren met andere partijen.

## 2 KADERSTELLING

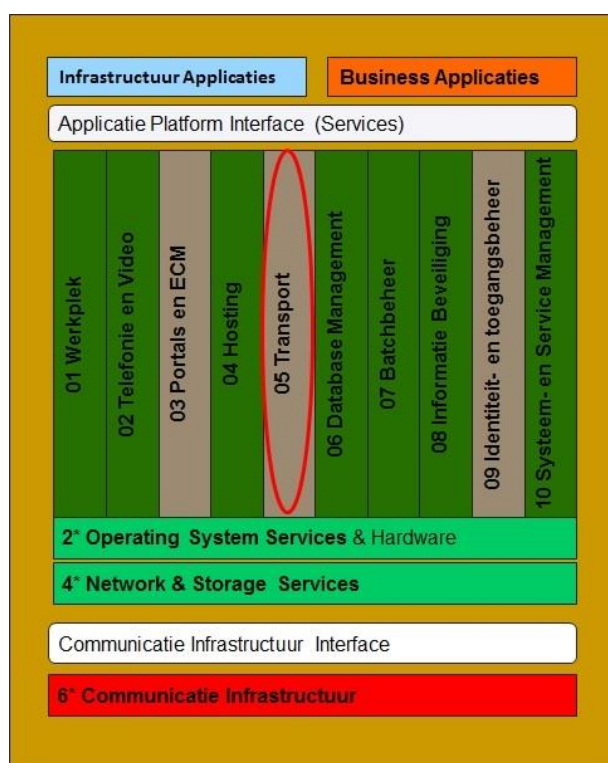
### 2.1 Integratiediensten

GIV/ID biedt gestandaardiseerde transport services aan om applicaties c.q. services met elkaar te verbinden. Voor het koppelen met UWV is inhoudelijke berichttransformatie (van de payload) niet gewenst, omdat er een ontwikkeltraject voor nodig is. Er zal daarom te allen tijde worden gestuurd op de bestaande standaard transport services beschreven in dit document. Dit betekent dat transformaties plaatsvinden aan de te koppelen systemen en niet in de Service Proxies van GIV/ID.

*Indien sprake is van service ontsluiting over divisie grenzen heen of ontsluiting naar externe partijen moet altijd worden voldaan aan de UWV Referentiearchitectuur voor integratie van GIV/ID.*

### 2.2 Positionering GIV/ID

UWV heeft op basis van het TOGAF Technical Reference Model raamwerk haar eigen UWV Technical Reference Model (UTRM) uitgewerkt.



Figuur 1: Het UTRM

De services die Integratiediensten levert vallen binnen de services groep Transport. Figuur 2 geeft hiervan een overzicht. De implementatie van deze transport services worden zogenaamde 'Service Proxies' genoemd. Een Service Proxy bevat alle technische aspecten voor het managed ontsluiten van Services. Een Service Proxy bevat nooit bedrijfsregels of bedrijfslogica. Daarnaast is de ontvangende partij altijd de eindverantwoordelijke voor de validatie van de berichten.

## 2.3 UWV Service richtlijnen

In dit hoofdstuk zijn de service richtlijnen in hoofdlijnen beschreven. Deze richtlijnen hebben betrekking op de wijze van ontwerpen, registreren en implementeren van services. Veelal gelden deze richtlijnen ook voor partijen anders dan UWV, wanneer gekoppeld moeten worden met UWV services en applicaties. In hoofdstuk 4 wordt per beschikbare Transport Services beschreven wat de belangrijkste uitgangspunten zijn.

Voor de uitwerking van de Service Richtlijnen is ervoor gekozen om de Archimate definitie als basis te nemen:

**Application Service:** *“An application service represents an explicitly defined exposed application behavior.”*

**Application Component:** *An application component represents an encapsulation of application functionality aligned to implementation structure, which is modular and replaceable.*

Hierbij is een service equivalent is aan de applicatie service en een application component equivalent aan een applicatie.

#REF <sup>1</sup>	Richtlijn	Beschrijving en rationale
REF000	Een service heeft altijd een eigenaar	Er moet altijd een eindverantwoordelijke zijn voor het beheer van een service. De verantwoordelijkheid kan gedelegeerd worden over verschillende teams, maar er is altijd 1 eindverantwoordelijke noodzakelijk.  <i>De contactgegevens zijn verplicht en worden bij UWV voor externe partijen opgeslagen in de UWV Servicebibliotheek.</i>
REF001	Een service moet een duidelijk maar eenvoudig doel dienen	Indien een service klein en eenvoudig genoeg is (veelal gerelateerd aan een business capability), dan wordt de aanpasbaarheid van een service groter en de onderhoudbaarheid beter. Als een service te rijk aan functionaliteit wordt, zullen kwaliteitsattributen als onderhoudbaarheid, wendbaarheid, veranderbaarheid in het gedrang komen. De interne cohesie van een service dient hoog te zijn. Veelal betekent dit dat veranderingen in het datamodel binnen de service context vallen. Dit vermindert de communicatie met andere services aanzienlijk en wordt de afhankelijkheid sterk verlaagd. Het duidelijke doel uit zich ook vaak in een eenduidige naam.  <i>De naamgeving van service dient helder en eenduidig te zijn voor de correcte registratie in de UWV Servicebibliotheek.</i>
REF002	Een service is bij voorkeur stateless	Dit betekent dat een service geen state/informatie mag bijhouden gerelateerd aan service requests uit het verleden. In principe zal de service een binnenkomend request ongeacht de instantie hetzelfde moeten verwerken. Dit is een essentieel uitgangspunt om schaalbaarheid mogelijk te maken. Dit betekent ook dat 'consumers' van services de state moeten bijhouden van het proces dat is gekoppeld aan de bedrijfsfunctie.

<sup>1</sup> Alleen de richtlijnen van toepassing op externe partijen, cloudvoorzieningen en standaard pakketen zijn opgenomen in deze lijst. Hierdoor is de nummering niet opeenvolgend.

		<p><i>Wanneer niet kan worden voldaan aan de bovenstaande richtlijn, dan moet dit tijdig kenbaar gemaakt worden aan UWV om te komen toch een goede integratie.</i></p>
REF003	Een service heeft altijd een contract	<p>Een service heeft een duidelijk contract (met zowel business als technische contracten) met de buitenwereld waarin precies staat wat verwacht mag worden van de service. Best practice om het contract eerst op te stellen alvorens te beginnen met realiseren.</p> <p><i>Technische Service Contracten zijn verplicht en worden gezamenlijk opgesteld en vastgelegd in de UWV Servicebibliotheek. Voor service provider zijn zogenaamde Terms of Service tevens noodzakelijk.</i></p>
REF004	Een service is altijd gedocumenteerd	<p>Een service heeft een goede beschrijving omtrent het gebruik ervan en bij voorkeur een developer portal of een zelf beschrijvende interface, waartegen gebruikers van de service kunnen ontwikkelen en testen.</p> <p><i>Elk te koppelen service provider is verplicht een beschrijving op te leveren die voldoende informatie bevat om te kunnen koppelen. Er zijn verschillende vormen van documentatie mogelijk als: WSDL, Swagger, openAPI etc. Maar denk ook aan infrastructuur en security documentatie.</i></p>
REF007	Een service heeft een standaard wijze van logging	<p>Wanneer services het log aggregation pattern implementeren, wordt trouble shooten vele malen makkelijker. De logstandaard beschrijft welke elementen minimaal lokaal gelogd moeten worden, zodat deze eenvoudig geconsolideerd kunnen worden in een centrale omgeving voor analysedoeleinden. Inzicht en overzicht van met betrekking tot gebruik van services wordt hiermee mogelijk.</p> <p><i>UWV heeft een aantal solutions beschikbaar voor het aggregeren van logging informatie.</i></p>
REF008	Een service moet fouten correct kunnen afhandelen	<p>Een service moet ontworpen zijn met de gedachte dat fouten in infrastructuur optreden. De software dient adequaat hierop te kunnen reageren. Vaak worden de software fouten nog wel mee ontworpen, maar de infrastructuurfouten niet. Denk aan vollopen queues, netwerk problemen etc. REF007 is hiervoor randvoorwaardelijk om integrale inzicht te hebben!</p> <p><i>Uiteraard geldt dit voor alle services en applicaties.</i></p>
REF010	Een service moet waar nodig in staat zijn meerdere instanties van zichzelf te kunnen draaien.	<p>Een service is een geheel van functionaliteit, techniek en gegevens. Een service heeft controle over alle (runtime) onderdelen die nodig zijn voor een goede autonome werking.</p> <p><i>Deze richtlijn is vooral van belang als er grote aantallen request worden verwacht. In het technische Service Contract wordt dit by design vastgelegd.</i></p>
REF013	Een service communiceert volgens standaard protocollen	<p>(s)FTP, HTTP(s), Websphere MQ, SOAP, REST.</p>
REF015	Een service kent voor service requests altijd een correlatie identificatie	<p>Om traceerbaarheid te verwezenlijken zal een service alle communicatie moeten identificeren.</p> <p><i>In de berichtenstructuur moet plek zijn voor een correlatie identificatie.</i></p>

REF017	Een service moet geregistreerd worden in een centrale servicebibliotheek	Een service moet vindbaar zijn.  <i>Elke service provider en service consumer wordt vastgelegd in de UWV Servicebibliotheek. UWV doet dit voor externe partijen.</i>
REF018	Een service dient een health check interface te hebben	Het moet mogelijk zijn om services die in productie draaien te kunnen controleren op hun toestand. Dit is veelal een beheerinterface die bij voorkeur een standaard vorm heeft.
REF019	Een service dient alleen de strikt noodzakelijk elementen in de service interface op te nemen.	In relatie tot REF001 heeft een service een duidelijk doel en contract en mag niet zomaar worden uitgebreid met subdoelen. Bij voorkeur contract first!  <i>Dit leidt veelal tot meerdere API's/service interfaces.</i>
REF020	Een service kent een beperkt aantal interface versies	Een service kent naast de huidige versie maximaal 2 versies in het verleden (eventueel toekomst) in de productieomgeving. Voor OTA kan hiervan afgeweken worden.  Indien dit niet mogelijk is kan een open/closed principe <sup>2</sup> worden gehateerd.
REF021	Een service valideert invoer	Een service zal naar gelang de noodzaak op basis van een (minimale) invoervalidatie (inhoudelijk, sematisch, functioneel en technisch) bepalen of een aanvraag verwerkt kan worden of niet.

### 2.3.1 Service registratie: Servicebibliotheek

GIV/ID heeft in haar portfolio de UWV Servicebibliotheek. In deze applicatie worden alle interfaces (API's: Application Programming Interfaces) als services geregistreerd. Daarnaast regelt de UWV Servicebibliotheek ook de Service Life Cycle Management. Voor externe partijen regelt UWV deze registratie.

### 2.3.2 Service Contracten

Tevens dient in de UWV Servicebibliotheek gewerkt te worden met zogenaamde technische service contracten in relatie tot de 'terms of service' van de service provider, waarin het gebruik van een interface wordt vastgelegd op voorhand.

---

<sup>2</sup> Open-closed Principle (OCP) states: Objects or entities should be open for extension but closed for modification.

## 2.4 Beveiliging

### 2.4.1 Informatiebeveiliging

GIV/ID volgt de UWV IB&P Security richtlijnen en zullen in dit document niet verder worden toegelicht. Dit onderdeel valt onder '08 Informatie beveiliging', zie ook: Figuur 1: Het UTRM. Dit geldt ook voor Identity & Access Management (IAM). In dit document wordt met name beantwoord hoe UWV dit toepast voor verbindingen met externe partijen en standaardpakketten.

### 2.4.2 Confidentiality Class

Hieronder zijn de UWV risicoklassen (confidentiality classes) beschreven en gemapt op de functionele- en technische beveiligingsinrichtingen.

Klasse	Omschrijving	Functioneel niveau	Toegepast op Technisch niveau
<b>0</b> <u>Openbaar</u>	Niet vertrouwelijke gegevens die publiekelijk beschikbaar kunnen worden gesteld.	<u>Niet beveiligd</u> Betekent dat hackers vrij gemakkelijk bij de data kunnen komen.	<u>Transportbeveiliging</u> 1-way TLS <u>Authenticatiemechanisme</u> Geen
<b>1</b> <u>Interne informatie</u>	Reguliere persoonsgegevens zolang deze niet kunnen worden gerekend tot de bijzondere persoonsgegevens conform WPB art.16.	<u>Minimale beveiliging</u> Betekent dat met een beetje proberen het niet mogelijk is bij de data te komen.	<u>Transportbeveiliging</u> 1-way TLS
<b>2</b> <u>Vertrouwelijk</u>	Defaultklasse voor UWV. Vertrouwelijke gegevens die niet voor brede kennisgeving zijn bedoeld. Gegevens die vallen onder WPB art.16	<u>Gemiddelde beveiliging</u> Betekent dat voor een professionele hacker met een beetje proberen het niet mogelijk is bij de data te komen.	<u>Transportbeveiliging</u> 2-way TLS HTTPs sFTP
<b>2+</b> <u>Vertrouwelijk</u>	Klasse 2+ geldt voor bijzondere persoonsgegevens.	<u>Zie klasse 2</u>	<u>Zie klasse 2</u>
<b>3</b> <u>Strikt vertrouwelijk.</u> <u>Geheim</u>	Gegevens die vallen onder WPB art 9 lid 4.	<u>Maximale beveiliging</u> Betekent dat het voor professionele hackers moeilijk is om bij de data te komen.	<u>Zie klasse 2</u>

## 2.5 OTAP beleid

Voor software deployments binnen het rekencentrum van UWV (on premise) geldt een OTAP beleid. OTAP staat voor Ontwikkeling, Testen, Acceptatie en Productie. De bedoeling is dat elke wijziging of vernieuwing op automatisering deze stappen opeenvolgend moet doorlopen. In het UWV beleid is tevens vastgelegd dat voor elke stap een eigen gescheiden omgeving gebruikt moet worden. Voor externe deployments, bijvoorbeeld cloudoplossingen, is er alleen een Acceptatie- en Productieomgeving beschikbaar.

### 3 TRANSPORT SERVICES

Dit hoofdstuk beschrijft Transport Services voor externe partijen, cloudvoorzieningen en standaardpakketten en de bijbehorende uitgangspunten:

#### 3.1 Transport Policy Service

De Transport Policy Service is de primaire transportdienst voor synchroon verkeer met interne, externe en overheidspartijen.

Aspect	Invulling
Protocol en formaat	REST/JSON, SOAP/XML, UvwML, SAML, WUS, ebMS, HTTP(s)
UWV standaarden	UWV Gegevensstandaard voor het maken van datamodellen, berichten en interfaces. Cloud- en standaardpakketten moeten kunnen aansluiten volgens de UWV Standaard.
DigiKoppeling	<p>Voor ontsluiten van en naar overheidspartijen volgt UWV de DigiKoppeling 2.0 standaard. Tevens is het ook de voorkeur voor andere partijen.</p> <p><b>Beleid</b>  <i>UWV hanteert WUS voor synchroon raadplegen en</i>  <i>UWV hanteert ebMS 2.0 voor asynchroon leveren en muteren</i></p> <p>Het DigiKoppeling REST API wordt nog niet ondersteund. Hiervoor is nog geen security standaard vastgelegd op Europees niveau.</p> <p>Profielen DK WUS: DigiKoppeling 2W-be, DigiKoppeling 2W-be-S, DigiKoppeling 2W-be-SE</p>
Logging en monitoring	Cloudpartijen moeten kunnen aansluiten op Security Information & Event Management (SIEM). Dit onderdeel valt onder '08 Informatie beveiliging', zie ook: Figuur 1: Het UTRM.
Bericht grootte	Deze transportdienst wordt gebruikt voor enkelvoudige berichten met de profielen MSP1, MSP2 (zie Service Contract Profielen) middels standaard HTTP. Wanneer er sprake is van MSP3 en MSP4, dan zal altijd HTTP streaming worden toegepast.
Frequentie van berichten	Deze transportdienst kan de RRP1 t/m RRP7 ondersteunen (zie Service Contract Profielen).
Foutafhandeling	De transportdienst hanteert het 'fail fast rather than block' principe. Dit betekent dat wanneer fouten ontstaan, het niet wacht op een time-out maar zo snel mogelijk een foutmeldingen zal teruggeven om de resources weer vrij te spelen. Belangrijk is dat de transportdienst niet persistent is, de verzendende partij dient te zorgen voor een retry-mechanisme.
Standaard extra latency	Minimaal 100 ms voor de transportdienst.
Cloud aansluiting	Indien er gebruik gemaakt wordt van statische IP adressen, dan kan UWV de partij als trusted partner worden gekenmerkt. Bij dynamische IP zal gebruik gemaakt moeten worden van een forward reverse proxy. Dit heeft niet de voorkeur. Dynamische IP adressen via de reverse proxy worden niet toegestaan.

*Tabel 1 Aansluitvoorwaarden Transport Policy Service.*

#### 3.2 Transport Message Queue Service

De Transport Message Queue Service is de primaire transportdienst voor asynchroon verkeer met interne partijen en standaardpakketten.

Aspect	Invulling
Protocol en formaat	IBM MQ, SOAP/XML, UwwML
Uwv standaarden	Uwv Gegevensstandaard voor het maken van datamodellen, berichten en interfaces. Cloud- en standaardpakketten moeten kunnen aansluiten volgens de UWV Standaard.  Het inrichten van IBM MQ gaat volgens UWV IBM MQ Richtlijnen.
Logging en monitoring	Cloudpartijen moeten kunnen aansluiten op Security Information & Event Management (SIEM). Dit onderdeel valt onder '08 Informatie beveiliging', zie ook: Figuur 1: Het UTRM.
Bericht grootte	Deze transportdienst wordt gebruikt voor enkelvoudige en meervoudige berichten met de profielen MSP1, MSP2 (zie Service Contract Profielen).
Frequentie van berichten	Deze transportdienst kan de RRP1 t/m RRP7 ondersteunen (zie Service Contract Profielen).
Cloud aansluiting	Indien er gebruik gemaakt wordt van statische IP adressen, dan kan UWV de partij als trusted partner worden gekenmerkt. Bij dynamische IP zal gebruik gemaakt moeten worden van een forward reverse proxy. Dit heeft niet de voorkeur. Dynamische IP adressen via de reverse proxy worden niet toegestaan.

Tabel 2 Aansluitvoorwaarden Transport Message Queue Service

### 3.3 Transport File Transfer Service

De Transport File Transfer Service is de primaire transportdienst voor het zowel intern als extern van grote bestanden.

Aspect	Invulling
Protocol en formaat	sFTP, FTPs
Uwv standaarden	Uwv Gegevensstandaard voor het maken van datamodellen, berichten en interfaces. Cloud- en standaardpakketten moeten kunnen aansluiten volgens de UWV Standaard.
DigiKoppeling	Voor ontsluiten van en naar overheidspartijen volgt UWV de DigiKoppeling 2.0 standaard. Tevens is het ook de voorkeur voor andere partijen.  Het DigiKoppeling REST API wordt nog niet ondersteund. Hiervoor is nog geen security standaard vastgelegd op Europees niveau.
Logging en monitoring	Cloudpartijen moeten kunnen aansluiten op Security Information & Event Management (SIEM). Dit onderdeel valt onder '08 Informatie beveiliging', zie ook: Figuur 1: Het UTRM.
Bericht grootte	Deze transportdienst wordt gebruikt voor meervoudige berichten met de profielen MSP3 en MSP4 (zie Service Contract Profielen).
Frequentie van berichten	Deze transportdienst kan voor meervoudige berichten de RRP1 t/m RRP4 ondersteunen (zie Service Contract Profielen).
Cloud aansluiting	Indien er gebruik gemaakt wordt van statische IP adressen, dan kan UWV de partij als trusted partner worden gekenmerkt. Bij dynamische IP zal gebruik gemaakt moeten worden van een forward reverse proxy. Dit heeft niet de voorkeur. Dynamische IP adressen via de reverse proxy worden niet toegestaan.

Tabel 3 Aansluitvoorwaarden Transport File Transfer Service.

## 4 Bijlagen

### 4.1 Afkortingen

Overzicht van gebruikte afkortingen in dit document.

<b>Afkorting</b>	<b>Verklaring, eventueel met toelichting</b>
AMG	API Management Gateway
API	Application Programming Interface
DK	Logius DigiKoppeling
ebMS	ebXML Messaging Service
FT	File Transfer
GIV/ID	GIV Integratiediensten
HTTPS	Hypertext Transfer Protocol Secure
ICAP	Internet Content Adaptation Protocol
JSON	JavaScript Object Notation
LCM	Life cycle management
MQ	Message Queue
RA	Referentie Architectuur
REST	Representational state transfer
SAML	Security Assertion Markup Language
SIEM	Security Information & Event Management
SOAP	Simple Object Access Protocol
TLS	Transport Layer Security
UTRM	UWV Technical Reference Model
WUS	WSDL, UDDI en SOAP
XML	Extensible Markup Language

## 4.2 Terms of Service van de Service Provider

De Terms of Service is een registratie onderdeel van de service provider en geeft aan wat de grenzen voor het gebruik van de service in kwestie. In de Terms of Service staan de eisen waaraan alle service consumers gezamenlijk minimaal moeten voldoen, waarbij de service provider haar functie nog steeds correct kan aanbieden.

### 4.2.1 Interface Performance

#### **Maximum Message Size**

What is the maximum message size that will be allowed to send to the service (Example maximum message size is 4MB per request)

#### **Average Service Requests Rate**

Fill in the average rate limiting per minute (Example the service can handle an average of 500 transactions per minute per customer).

#### **Maximum Service Requests Rate**

Fill in the rate limiting per minute (Example the service can handle a maximum of 10 transactions per minute per customer)

#### **Maximum Concurrent Service Requests**

How many concurrent service calls can the service handle per second (Example 100 per second)

### 4.2.2 Interface Usage

#### **Utilisation Period**

Use of service during which hours (Example only from 08:00 till 17:00 or 24/7)

#### **Network Type**

Which network type is being used (Example Internet, Intranet, Diginet, Private Network)

#### **Data Exchange Format Type**

Data exchange format used: UwwML, SuwiML, JSON, XML, SubML

#### **Communication Standard**

This is the communication standard used: Digikoppeling, SAML, SUWI Transactie standaard

#### **Confidentiality Class**

Confidential Class within UWV 0-3 (Example 0 is very low risk like public information and 3 is very high like medical information of a person)

## 4.3 Service Contract Profielen

De service contracten maken gebruik van profielen om snel te komen tot een inschatting.

#### **Request Rate Profile (RRP) en Message Size Profile (MSP)**

Om de request rate en message size in makkelijker hanteerbare staffels te verdelen zijn voor beide rubrieken voor gedefinieerde profielen gemaakt. Daarbij is er over verschillende assen onderscheid gemaakt: Enkelvoudig of bulk berichten en per rubriek het maximale en gemiddelde aantal per profiel.

#### **Voor meervoudige berichten (bulk)**

Meervoudige berichten kunnen met een maximum van 1x per 15 minuten gestuurd worden en hebben een minimale berichtgrootte van 4 MB. Er is geen minimaal aantal keren dat een bericht gestuurd kan worden. De maximale berichtgrootte is 1500 MB.

Request Rate Profile (RRP)	Max	Average	Unit
RRP1: <1x per month	1	0.5	per month
RRP2: 1x per month to 1x per week	4	2	per month
RRP3: 1x per week to 1x per day	7	3.5	per week
RRP4: 1x per day to 1x per 15 minutes	96	48	per day

Message Size Profile (MSP)	Max (MB)	Average (MB)
MSP3: 4 MB and 20 MB	20	12
MSP4: 20 MB and bigger	1500	750

#### Voor enkelvoudige berichten

Enkelvoudige berichten kunnen met een maximum van 1000 berichten per minuut gestuurd worden en met een maximale berichtgrootte van 4 MB. Er is geen minimaal aantal keren dat een bericht gestuurd kan worden, noch een minimale berichtgrootte.

Request Rate Profile (RRP)	Max	Average	Unit
RRP5: <100 per minute	100	50	per minute
RRP6: 100 to 500 per minute	500	250	per minute
RRP7: >500 per minute	1000	500	per minute

Message Size Profile (MSP)	Max (MB)	Average (MB)
MSP1: Up to 5 KB	5 KB	2.5 KB
MSP2: Between 5 KB and 4 MB	4 MB	2 MB