VNG Realisatie

Architectuur GGI-Netwerk

High level design

Versie 1.2
17 juni 2019

Colofon

High Level Design Architectuur GGI-Netwerk
GGI@vng.nl

Inhoud

1. Inleiding

Gemeenten hebben VNG en VNG Realisatie opdracht gegeven in het kader van Samen Organiseren te werken aan meer collectiviteit in ICT-voorzieningen. Hier wordt invulling aan gegeven door het ontwikkelen van de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI). Onderdeel van de GGI is het GGI-Netwerk: een beveiligd datanetwerk speciaal voor gemeenten en gemeentelijke samenwerkingsverbanden.
Het GGI-Netwerk zorgt voor veilige dataconnecties met andere overheden waardoor samenwerken tussen gemeenten onderling en met andere overheden beter, veiliger en gemakkelijker wordt.
GGI-Netwerk wordt gerealiseerd binnen het contract dat met VodafoneZiggo is gesloten bij de aanbesteding GT-Vast. VodafoneZiggo verzorgt de technische inrichting van het datanetwerk in opdracht van VNG Realisatie. Er wordt voor gezorgd dat alle gemeenten en gemeentelijke samenwerkingsverbanden kunnen aansluiten op GGI-Netwerk. Voor gemeenten die niet hebben deelgenomen aan de aanbesteding GT-Vast is daarom een Aansluitvoorziening in Amsterdam beschikbaar. GGI-Netwerk is onderdeel van de diginetwerkinfrastructuur. Hierdoor kunnen gemeenten via GGI-Netwerk dataverbindingen realiseren met ketenpartners die ook op Diginetwerk[1] zijn aangesloten.
Voor commerciële (cloud-)leveranciers wordt het onder voorwaarden ook mogelijk hun diensten te ontsluiten op GGI-Netwerk. Hiermee worden verbindingen met deze leveranciers eenvoudiger en kunnen gemeenten meer grip krijgen op hun aanbod.
De collectieve voorzieningen die in het kader van de aanbestedingen GGI-Veilig (SOC/SIEM-dienst) en GT-Connect (cloud-platform voor telecommunicatiediensten) worden gerealiseerd worden eveneens ontsloten op GGI-Netwerk.

Toolkit GGI-Netwerk
Het document Architectuur GGI-Netwerk maakt onderdeel uit van een pakket ondersteuningsmiddelen: de Toolkit GGI-Netwerk. Deze toolkit wordt door VNG Realisatie en gemeenten[2] in nauwe samenwerking ontwikkeld en ondersteunt verschillende fasen die elke gemeente doorloopt: van een globale oriëntatie tot de afweging deel te nemen, en het daadwerkelijk aansluiten op en gebruiken van het GGI-Netwerk. Dit document ondersteunt de fase waarin u zich oriënteert op de mogelijkheden en het ontwerp van GGI-Netwerk.
Een volledig overzicht van de ondersteuningsmiddelen vindt u op https://www.vngrealisatie.nl/ondersteuningsmiddelen/GGI-netwerk.

[1] Voor meer informatie over Diginetwerk, zie https://www.logius.nl/diensten/diginetwerk
[2] Daar waar gemeenten staat, worden ook gemeentelijke samenwerkingsverbanden bedoeld

2. Vereisten aan GGI-Netwerk

De generieke principes van GGI-Netwerk:

- GGI-Netwerk reduceert vanuit gemeentelijk perspectief de complexiteit van de benodigde netwerkinfrastructuur voor de uitvoering van de gemeentelijke taken.
- De dienstverlening voor de op GGI-Netwerk aan te sluiten partijen is nauwkeurig beschreven en transparant.
- Eén organisatie is verantwoordelijk en aanspreekbaar voor de GGI-Netwerk dienst en -dienstverlening.
- Afspraken zijn vastgelegd.
- GGI-Netwerk is onafhankelijk van het internet.
- GGI-Netwerk staat volledig onder zeggenschap van gemeenten.
- GGI-Netwerk conformeert zich aan de wettelijke standaarden, aan de gangbare en Open Standaarden op de Pas-toe-of-leg-uit-lijst zoals vastgesteld door het Forum en College Standaardisatie en aan landelijk vastgestelde standaarden van gemeenten.
- GGI-Netwerk wordt op basis van het IPv6 overheidsnummerplan ingericht maar ondersteunt ook IPv4. Beide standaarden worden hier vanuit functioneel oogpunt expliciet genoemd vanwege de noodzaak om de toegankelijkheid tussen gemeenten en de buitenwereld te kunnen waarborgen.
- GGI-Netwerk faciliteert de vorming van een gemeentelijke community cloud infrastructuur.

3. Ontwerpeisen

GGI-Netwerk is onderdeel van de infrastructuur van Diginetwerk. Dit is een van het internet afgesloten netwerk met alleen bekende (trusted) partijen.

GGI-Netwerk fungeert door middel van de aansluiting op het Koppelpunt Publieke Sector (KPS) als koppelvlak tussen Diginetwerk en de gemeentelijke bedrijfsnetwerken. Vanuit de Diginetwerk-architectuur bezien is GGI-Netwerk een koppelnetwerk en moet voldoen aan de eisen die gesteld worden in de Aansluitvoorwaarden Diginetwerk van Logius, de beheerder van Diginetwerk. Met de aansluiting op Diginetwerk via GGI-Netwerk heeft de gemeente connectiviteit naar alle aangesloten (landelijke) voorzieningen, partijen en andere overheden.

Voor de aansluiting van GGI-Netwerk op het KPS stelt Logius de volgende eisen:

- GGI-Netwerk is zonder extra maatregelen geschikt voor Gemeentelijk Vertrouwelijk conform de Baseline Informatiebeveiliging Nederlandse Gemeenten en AVG-risicoklasse II.
- GGI-Netwerk is transparant voor het transport van IP-pakketten.
- Het gebruik van Internet-VPN's binnen Koppelnetwerken Diginetwerk[3] en voor klantaansluitingen is niet toegestaan.
- Er mag vanuit GGI-Netwerk geen communicatie van en naar het internet mogelijk zijn.
- Er mogen tussen GGI-Netwerk en het KPS geen blokkerende firewalls aanwezig zijn voor regulier gebruikersverkeer (HTTP, HTTPS, DNS, SMTP, ICMP, NTP).
- De aangesloten apparatuur van de koppelnetwerkbeheerder op het KPS dient te beschikken over een vaste configuratie van Ethernet-parameters die exact overeenkomt met de door Logius vastgestelde standaard.
- De koppelnetwerkrouters waarmee het Koppelnetwerk op het KPS wordt aangesloten zijn voorzien van een door Logius verstrekt IP-adres.
- Vanuit het Koppelnetwerk worden uitsluitend IP-protocollen op het KPS aangeboden.
- Tussen de koppelnetwerken die aangesloten zijn op het KPS wordt IP-verkeer onderling dynamisch gerouteerd met de door Logius vastgestelde BGP-standaard (BGP-4).
- Voor gebruik van het BGP-protocol dient de beheerder van het koppelnetwerk te beschikken over een Autonomous Sytem Number. Toegestaan zijn:
    - publieke AS-numbers die door het RIPE NCC (of één van de andere RIR's) aan de betreffende organisatie uitgegeven zijn (deze optie heeft de voorkeur), of
    - private AS-numbers die door Logius uitgegeven en geadministreerd worden.
- Apparatuur dient 32-bit (4-byte) AS-numbers te ondersteunen.
- De routers van de koppelnetwerken hebben BGP-verbindingen met de twee routeservers van het KPS.
- Er wordt uitsluitend IP-verkeer gerouteerd afkomstig van die IP-adressen die door Logius zijn verstrekt en geregistreerd.
- ICMP-pakketten van type "Fragmentation Needed and Don't Fragment was Set" (type 3, code 4) dienen waar nodig door routers te worden gegenereerd en niet uitgefilterd.
- Het Ethernetverkeer wordt door de Koppelnetwerkbeheerder op basis van de IEEE 802.3-standaard en RFC 894 aangeboden.
- Koppelnetwerkbeheerders zijn verplicht om van hun koppelnetwerk richting KPS uitgaand verkeer te controleren op source IP-adressen, en pakketten met een source IP-adres dat niet tot hun koppelnetwerk behoort te verwijderen alvorens het aangeboden wordt aan het KPS (anti-spoofing protectie).

[3] Hier wordt bedoeld dat Internet-VPN's geen onderdeel mogen zijn van een Koppelnetwerk, IP-VPN's over Diginetwerk zijn wel toegestaan.

- De Koppelnetwerkbeheerder is binnen zijn netwerk verplicht voor alle IP-interfaces, die deel uitmaken van een routeerbaar pad door Diginetwerk, ICMP/UDP-verkeer zodanig te ondersteunen dat alle andere Koppelnetwerkbeheerders door middel van een Traceroute het volledige routeerbare pad kunnen bepalen.

Voor de aansluiting van gemeentelijke bedrijfsnetwerken (klantaansluiting) op GGI-Netwerk gelden de volgende aanvullende eisen:

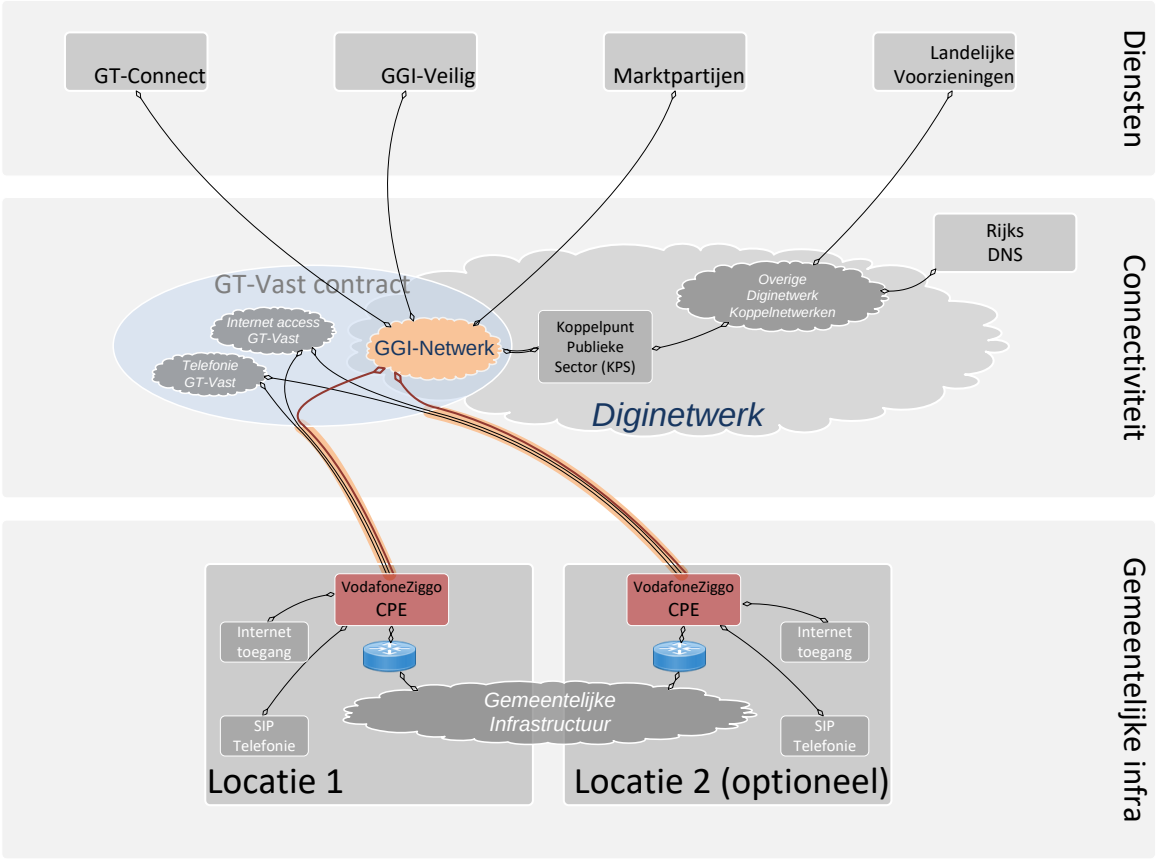
- De te leveren klantaansluitingen en koppelvlakken op laag 1 en laag 2 voor gemeenten die via de access van VodafoneZiggo op basis van de GT-Vast overeenkomst aansluiten zijn:
    - Koper: Ethernet 100 Mbps, 1 Gbps of 10 Gbps; Full duplex, auto negotiate;
    - Glas: Ethernet 100 Mbps, 1 Gbps of 10 Gbps;
- De te leveren klantaansluitingen en koppelvlakken op laag 1 en laag 2 voor gemeenten die via de Aansluitvoorziening in Amsterdam aansluiten zijn:
    - Glas: Ethernet 100 Mbps;
- Naast enkelvoudige aansluitingen worden redundante aansluitingen in de varianten active/active en active/passive geboden. Hiermee wordt een hogere beschikbaarheid bereikt van de dienstverlening. De variant active/active wordt gerealiseerd op basis van het netwerkprotocol BGP en de variant active/passive kan worden gerealiseerd op basis van het netwerkprotocol VRRP of op basis van BGP.
- Een klantaansluiting dient te voldoen aan de randvoorwaarden zoals vastgelegd in de Aansluitvoorwaarden Diginetwerk.
- De klantaansluiting is een overgang van Diginetwerk naar een ander beveiligingsniveau en er dient derhalve een beveiligd koppelvlak gebruikt te worden dat logging en inspectie mogelijk maakt.
- De eindgebruiker (i.e. een gemeente of gemeentelijk samenwerkingsverband) is zelf verantwoordelijk voor de beveiligingsmaatregelen op hun aansluiting op GGI-Netwerk.

4. High level design GGI-Netwerk

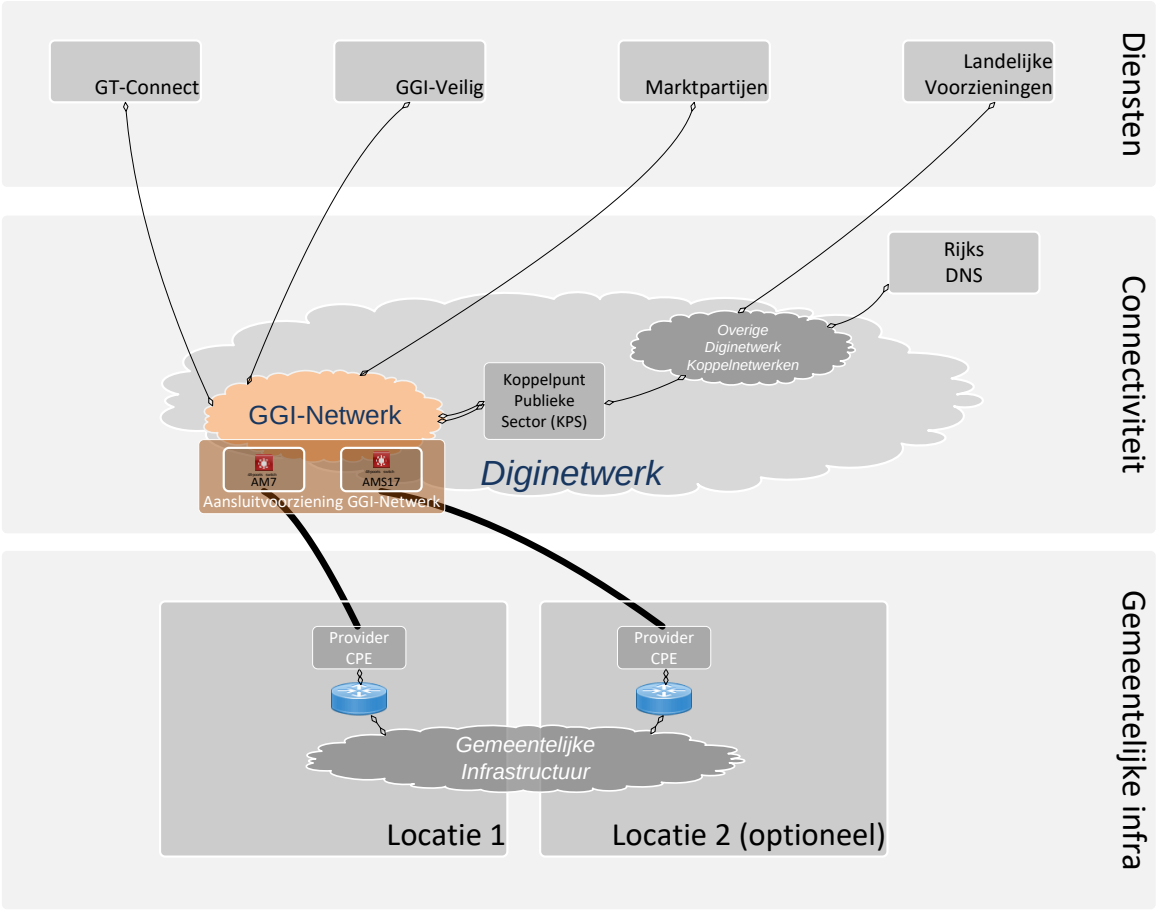
4.1. Beschrijving GGI-Netwerk

GGI-Netwerk is een IP-VPN dat door VodafoneZiggo wordt beheerd in opdracht van VNG Realisatie op basis van het GT-Vast contract. Dit IP-VPN is aangesloten op het Koppelpunt Publieke Sector (KPS) en is daarmee een Koppelnetwerk binnen Diginetwerk. Gemeenten met een GT-Vast overeenkomst krijgen “access” van VodafoneZiggo ten behoeve van hun Internet-verbinding en ten behoeve van hun SIP-trunks (telefoonverkeer). De hierbij gebruikte apparatuur (Customer Premises Equipment) wordt ook gebruikt voor toegang tot GGI-Netwerk. Eén van de vrije poorten wordt dan voor deze toepassing geconfigureerd. Indien gewenst kan ook op een tweede locatie access aangelegd worden, waarna een redundante aansluiting op GGI-Netwerk gerealiseerd kan worden. Voor gemeenten zonder GT-Vast overeenkomst is een Aansluitvoorziening aangelegd in twee datacenters in Amsterdam. Deze gemeenten kunnen een eigen provider opdracht geven een verbinding te realiseren tussen hun eigen locatie(s) en genoemde Aansluitvoorziening (al dan niet redundant). Gemeenten kunnen ook via een andere gemeente aansluiten; de verbinding tussen de gemeenten is dan wel de eigen verantwoordelijkheid. Via de aansluiting op GGI-Netwerk krijgen gemeenten toegang tot diensten van Landelijke Voorzieningen, Marktpartijen, andere overheden en collectieve gemeentelijke voorzieningen.

In de onderstaande figuren is de opbouw van GGI-Netwerk schematisch weergegeven, vanuit het perspectief van een gemeente die aansluit via access van VodafoneZiggo op basis van de GT-Vast overeenkomst respectievelijk vanuit het perspectief van een aangesloten gemeente die aansluit via de Aansluitvoorziening in Amsterdam.



Figuur 1: Aansluiting op GGI-Netwerk via access van VodafoneZiggo op basis van de GT-Vast overeenkomst



Figuur 2: Aansluiting op GGI-Netwerk via de Aansluitvoorziening in Amsterdam

4.2. Beschikbaarheid

De beschikbaarheid van de dienstverlening wordt bepaald door de beschikbaarheid van de centrale en lokale componenten.

Centrale inrichting

- GGI-Netwerk is 7 x 24 uur beschikbaar met een beschikbaarheidseis van >99,9%.
- GGI-Netwerk is opgebouwd met redundante aansluitingen met een automatische herroutering.

Lokale inrichting

- Gemeenten kunnen bij hun aansluiting op GGI-Netwerk de keuze maken tussen een enkelvoudige en een redundante configuratie. Bij een aansluiting via access van VodafoneZiggo op basis van de GT-Vast overeenkomst is de benaming hiervoor Premium (beschikbaarheid 99,90%) respectievelijk Verhoogde Beschikbaarheid (99,95%). Voor een redundante aansluiting dienen twee gescheiden accessen te zijn aangelegd. Bij een aansluiting via de Aansluitvoorziening in Amsterdam kan er ook enkelvoudig (via één datacenter) of redundant (via twee datacenters) worden aangesloten.
- Een redundante aansluiting kan op basis van *active/passive* of op basis van *active/active* aangelegd worden.
- Bij een *active/passive* configuratie zorgen netwerkprotocollen er bij uitval van de actieve verbinding voor dat het verkeer automatisch zal overschakelen naar de passieve verbinding. Nadat is

overgeschakeld is de volledige afgenomen bandbreedte weer beschikbaar. Dit verloopt zonder performanceverlies.

- Bij een *active/active* configuratie zorgen netwerkprotocollen er bij uitval van één van de verbindingen voor dat al het verkeer toegevoegd zal worden op de andere verbinding. Bij *active/active* kunnen de IP-subnetten verdeeld worden over de beide verbindingen. Voor elk IP-subnet dient één van de twee verbindingen als actieve verbinding gedefinieerd te worden. Typisch zullen de IP-subnetten zodanig over de verbindingen worden gerouteerd, dat beide in normaal bedrijf ongeveer evenveel data-verkeer te verwerken krijgen. Dit zorgt tevens voor een efficiënter gebruik van de beschikbare bandbreedte. Mocht de primaire verbinding uitvallen dan wordt het dataverkeer omgeleid naar de secundaire verbinding. Dat kan leiden tot een merkbaar performanceverlies, aangezien er reeds verkeer op deze secundaire verbinding actief is.
- In het *active/passive* scenario kan zowel VRRP als BGP als netwerkprotocol worden toegepast. In het active/active scenario kan alleen BGP als netwerkprotocol worden toegepast. BGP is complexer dan VRRP qua implementatie en bij het oplossen van storingen en vergt een hoger kennisniveau van het betrokken personeel.
- De ingezette apparatuur dient uiteraard het betreffende protocol te ondersteunen.

4.3. Capaciteit

Aansluiting op GGI-Netwerk via access van VodafoneZiggo op basis van de GT-Vast overeenkomst is mogelijk met een bandbreedte van veelvouden van 100 Mb/s tot maximaal 1 Gb/s. Aansluiting op GGI-Netwerk via de Aansluitvoorziening in Amsterdam is mogelijk met een bandbreedte van 100 Mb/s.

4.4. Beveiliging

Vanuit het oogpunt van beveiliging zijn de Baseline Informatiebeveiliging Gemeenten (BIG) en de Baseline Informatiebeveiliging Rijksdienst (BIR) van belang. De BIG omdat gemeenten daaraan moeten kunnen voldoen bij gebruik van GGI-Netwerk. En de BIR omdat Logius dit voorschrijft vanuit de eisen aan Diginetwerk. GGI-Netwerk is een beveiligingsmaatregel op zich. Het netwerk kent een besloten karakter. Er is geen directe (d.w.z. zonder beveiligde ontkoppeling) koppeling met openbare netwerken zoals internet mogelijk of aanwezig.
GGI-Netwerk is een infrastructuur voor datatransport. Encryptie, identificatie en authenticatie kunnen op applicatieniveau ingeregeld worden.

Afsprakenstelsel Diginetwerk
GGI-Netwerk is onderdeel van het afsprakenstelsel Diginetwerk en voldoet dus aan de beveiligingseisen van Diginetwerk. VNG Realisatie heeft GGI-Netwerk ingericht conform de door Logius aan Diginetwerk Koppelnetwerken gestelde beveiligingseisen. Bij oplevering van GGI-Netwerk is hierop een controle gedaan door Logius.

Aansluitende partijen
Partijen die aansluiten op GGI-Netwerk moeten voldoen aan de Aansluitvoorwaarden Diginetwerk en de daarin gestelde voorwaarden aan de beveiliging van de aansluiting. Er wordt gekoppeld middels beveiligde koppelvlakken: op Diginetwerk kunnen besloten netwerken aangesloten worden met een ander (zowel hoger als lager) beveiligingsniveau. Hiervoor geldt de verplichting dat er op het koppelvlak en aan de klantzijde een beveiligingsfunctie actief is (beveiligd koppelvlak).
Conform het afsprakenstelsel Diginetwerk is de eindgebruiker zelf verantwoordelijk voor de beveiligingsmaatregelen op hun aansluiting op GGI-Netwerk.
Een gemeente zal zijn elektronische communicatienetwerk en zijn aansluiting op GGI-Netwerk (en daarmee Diginetwerk) moeten beveiligen conform de informatiebeveiligingstandaarden NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002 om te voldoen aan de Aansluitvoorwaarden Diginetwerk.

Penetratietesten en Security-monitoring
VNG Realisatie heeft aan een externe gespecialiseerde partij opdracht gegeven om penetratietesten uit te voeren op GGI-Netwerk om de conformiteit met de beveiligingseisen te controleren.
Conform de BIG en de BIR (o.a actieve netwerkmonitoring) zal in 2019 GGI-Veilig gekoppeld worden aan het GGI-Netwerk waardoor er gebruik gemaakt zal worden van de SOC/SIEM-dienst voor actieve security-monitoring voor het bewaken van dataverkeer over het GGI-Netwerk.

4.5. DNS

Aangesloten organisaties op GGI-Netwerk kunnen gebruikmaken van het RijksDNS voor het resolven van domeinnamen die eindigen op diginetwerk.net en diginetwerk.nl. Van services die aangesloten partijen op GGI-Netwerk aan de gebruikers van Diginetwerk ter beschikking willen stellen kunnen de domeinnamen (onder diginetwerk.net of diginetwerk.nl) eveneens in het RijksDNS geregistreerd worden.

4.6. Positionering binnen de GEMMA Architectuur

Het onderstaande schema met een overzicht van het GGI-Netwerk en diensten binnen de GEMMA Architectuur vindt u op Gemma online. De beschrijving van begrippen en elementen zijn ook op deze website te vinden.