# TOE-R-1 Richtlijn Domeinen en Externe Toegang

## Inleiding

'Compartimentering' van de netwerkinfrastructuur draagt in belangrijke mate bij aan de beveiliging van de informatiesystemen en -verzamelingen die op het netwerk zijn aangesloten.

Dit document beschrijft:

a hoe het Erasmus MC transportnetwerk wordt **onderverdeeld in domeinen** (compartimentering)

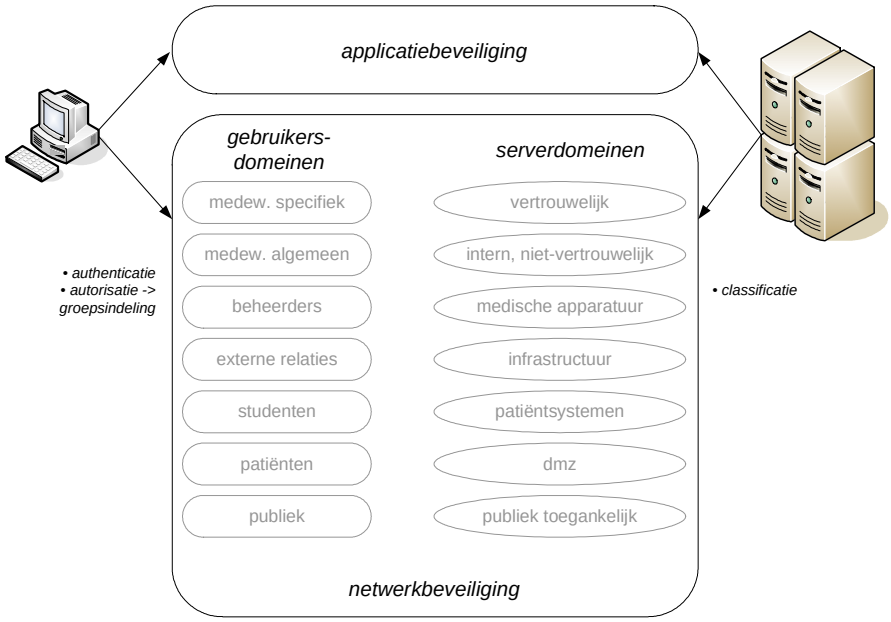
b welke regels gelden voor de **toelating van een computersysteem tot een bepaald domein**, daarbij inbegrepen de **toegang van buitenaf** ('externe toegang')

c welke **standaard toegangsregels** gelden voor 'kruisend' (d.w.z. intern-domein) verkeer, met andere woorden welke informatiestromen op infrastructureel niveau als regel worden toegestaan.

## Definities en uitgangspunten

1 Dit document heeft alleen betrekking op de onderlinge (on)bereikbaarheid van systemen op het niveau van het **transportnetwerk**. Dit staat los van toegangsrechten op **applicatieniveau** (login-accounts, autorisaties).

*Toelichting: als een PC gekoppeld is aan het gebruikersdomein 'medewerkers specifiek', dan kan deze PC op netwerkniveau verbinding maken met het ZIS. Het wil níet zeggen dat de* gebruiker *ook toegang heeft tot de informatie op het ZIS: daarvoor is op applicatieniveau een account op het ZIS vereist.*




2 Een **domein**, zoals het begrip hier wordt gebruikt, bestaat uit een **verzameling toegangsregels op netwerkniveau**. Voor een computersysteem dat is toegelaten tot een bepaald domein geldt (a) dat het op netwerkniveau vrijelijk kan communiceren met andere systemen in het *eigen domein* en (b) dat de communicatie met systemen in *andere domeinen* is onderworpen aan de toegangsregels die in dit document zijn vastgelegd.

Er is geen relatie tussen een domein en een DNS- of Windows-domein.

*De naam van een gebruikersdomein (bv. 'medewerkers specifiek') is bedoeld als indicatie voor het type gebruiker dat een bepaalde verzameling toegangsrechten nodig heeft. Zo kan een arts soms ingedeeld worden in het domein 'medewerkers algemeen' in plaats van 'medewerkers specifiek' – omdat de verbinding niet veilig genoeg wordt geacht om toegang te geven tot de privacygevoelige systemen.*

3 De koppeling aan een netwerk (en dus ook een domein) betreft altijd een **computersysteem**, niet de gebruiker zelf. Vaak worden wel eisen gesteld aan de identificatie en authenticatie van de gebruiker voordat de betreffende computer (PC, etc.) wordt toegelaten tot een bepaald gebruikersdomein.

4 Een **server** is de hardware en software die samen een combinatie van gegevensverzamelingen, toepassingen, netwerkdiensten en/of informatiesystemen via het netwerk beschikbaar maakt.

5 Domeinen worden onderscheiden in **gebruikers-** en **serverdomeinen**. Een systeem dat is gekoppeld aan een gebruikersdomein kan geen netwerk- of informatiediensten aanbieden die bereikbaar zijn vanaf andere domeinen.

*Dit draagt bij aan de beveiliging van gebruikers-PC's tegen virussen en aan het voorkómen van misbruik van gebruikers-PC's als 'stepping stone'.*

6 Onder de **verkeersrichting** wordt verstaan hoe de rolverdeling tussen client en server is ingericht. Als regel wordt een logische netwerkverbinding geïnitieerd door programmatuur op een client PC in een gebruikersdomein en is het de server die een dergelijke verbinding accepteert. In dat geval is de 'verkeersrichting' van client naar server.

## Serverdomeinen

De volgende serverdomeinen worden onderscheiden:

| *nr* | *naam domein* | *toelichting* |
|---|---|---|
| A | 'vertrouwelijk' | • servers die zijn geclassificeerd als 'intern, vertrouwelijk' worden verplicht opgenomen in dit domein<br>• alleen toegankelijk voor gebruikersdomein 'medewerkers specifiek' (en beheerders) |
| B | intern, niet vertrouwelijk | • default domein voor alle interne toepassingen (huidige server farm)<br>• toegankelijk voor alle medewerkers van het Erasmus MC |
| C | medische apparatuur | • bedoeld voor medische/klinische apparatuur in het huis die niet in de onderverdeling client-PC/server past<br>• vrije communicatie met serverdomein A;<br>standaard is domein C niet bereikbaar vanuit gebruikersdomeinen |
| D | infrastructuur | • (poorten op) systemen die alleen bereikbaar dienen te zijn voor beheerders infrastructuur<br>• alleen bereikbaar voor 'beheerders' |
| E | patiëntsystemen | • systemen die *via het interne netwerk* door patiënten zelf kunnen worden gebruikt worden verplicht in dit domein opgenomen<br>• bereikbaar voor 'patiënten', 'medewerkers specifiek' en beheerders<br>• NB: patiëntsystemen die *via het internet* bereikbaar zijn vallen in F of H |
| F | dmz | • systemen die via het Internet bereikbaar zijn voor het publiek maar die alleen voor gedefinieerde groepen van gebruikers toegang vereisen naar de interne serverdomeinen A/B/C worden verplicht in dit domein opgenomen |
| H | publiek toegankelijk | • systemen die voor het publiek direct benaderbaar zijn, inclusief systemen buiten Erasmus MC (o.a. Internet servers) |

## Classificatie en serverdomeinen

Elk informatiesysteem, -dienst of gegevensverzameling wordt door de verantwoordelijke geclassificeerd, conform de richtlijn “CLA-R-1, Classificatie van bedrijfsprocessen, informatiesystemen en informatie” en de bijbehorende Risicoanalysemethode. Op basis van de uitkomst hiervan kan in een aantal stappen worden bepaald in welk domein een informatiesysteem, -dienst of gegevensverzameling thuishoort:

Stap (1):

In eerste instantie wordt de plaatsing van een informatiesysteem, netwerkdienst of gegevensverzameling in een bepaald domein afgeleid van de classificatie in de dimensie **‘vertrouwelijkheid’**:

| *Uitkomst classificatie van informatiesysteem/dienst/gegevens* | *implementatie op server in domein...* |
|---|---|
| Hoog, ‘Vertrouwelijk’ | A: “intern, vertrouwelijk” |
| Midden, ‘Voor intern gebruik’ | B: “intern, niet vertrouwelijk” |
| Laag, ‘Openbaar’ | B: “intern, niet vertrouwelijk” of<br>F: “dmz” of<br>H: “publiek toegankelijk” |

Stap (2):

Er is een aantal meer **gespecialiseerde serverdomeinen**, waarvoor andere plaatsingsregels gelden:

| *Bijzondere plaatsingsregels* | *te koppelen aan serverdomein* |
|---|---|
| Medische systemen die niet in een MER geplaatst kunnen worden of waarvoor afwijkende toegangsregels nodig zijn (bijv. omkering van client- en server-rol) | C: “medische apparatuur” |
| (Informatie-)systemen die uitsluitend bereikbaar dienen te zijn voor beheerders en/of voor andere servers, niet vanaf enig gebruikersdomein. Ook beheers-‘poorten’ op servers die in andere domeinen zijn geplaatst vallen hieronder. | D: “infrastructuur” |
| Informatiesystemen die via het interne netwerk (dus niet via Internet) bereikbaar moeten zijn door patiënten (en door medewerkers specifiek en beheerders). | E: “patiëntsystemen” |
| Informatiesystemen die (evt. beperkt) bereikbaar moeten zijn vanaf het internet en ook toegang moeten hebben tot domein A, B of C | F: “dmz” |

Stap (3):

Als de uitkomst van de classificatie **in één of meer van de dimensies** (vertrouwelijkheid, integriteit, beschikbaarheid) **‘hoog’** is, dan is de verantwoordelijke verplicht **schriftelijk te toetsen** of de standaard-voorzieningen in de netwerkinfrastructuur in deze dimensie voldoende zijn voor het betreffende object van beveiliging – en zoniet, nadere maatregelen uit te werken.

Stap (4):

Als op deze manier is bepaald in welk serverdomein een informatiesysteem of gegevensverzameling thuishoort, dan zal de **server**-hardware en -software waarop dit wordt geïmplementeerd ook daadwerkelijk in dit domein moeten zijn of worden opgenomen.

## Gebruikersdomeinen

Als een gebruiker toegang wenst tot één van de serverdomeinen, dan dient zijn/haar computer (PC) te zijn opgenomen in een gebruikersdomein:

| *nr* | *naam domein* | *toegang tot welke serverdomeinen?* |
|---|---|---|
| 1 | 'medewerkers specifiek' | A: vertrouwelijk<br>B: intern, niet-vertrouwelijk<br>E: patiëntsystemen<br>H: publiek toegankelijk |
| 2 | 'medewerkers algemeen' | B: intern, niet-vertrouwelijk<br>H: publiek toegankelijk |
| 3 | 'beheerders' | alle domeinen<br>(incl. gebruikersdomeinen) |
| 4 | 'externe relaties' | H: publiek toegankelijk |
| 5 | 'studenten' | B: intern, niet-vertrouwelijk<br>H: publiek toegankelijk |
| 6 | 'patiënten' | E: patiëntsystemen<br>H: publiek toegankelijk |
| 7 | 'publiek' | H: publiek toegankelijk |

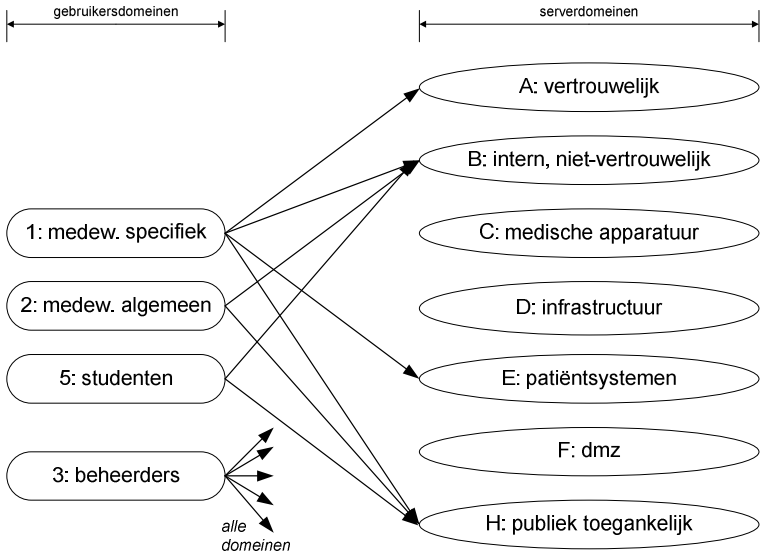
Ad 1: Alle client-PC's die zijn aangesloten op het **interne, draadgebonden LAN** zijn op dit moment opgenomen in het gebruikersdomein '**medewerkers specifiek**'. Geleidelijk zal ook intern meer differentiatie worden geïntroduceerd.

Ad 1/2/3: Voor deze domeinen geldt dat de betrokken gebruiker een **arbeidsovereenkomst** of gastvrijheidsovereenkomst dient te hebben met het Erasmus MC.

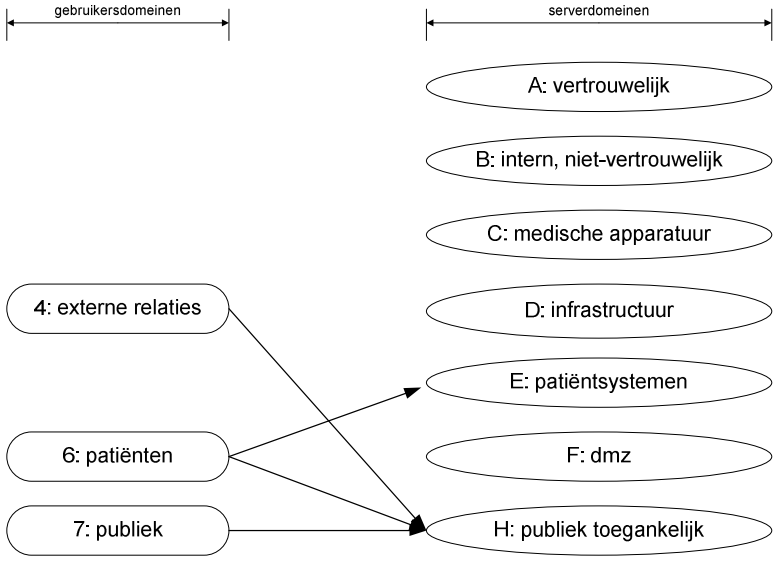
Ad 5: Voor het gebruikersdomein 'studenten' geldt dat de gebruiker als student moet kunnen worden geauthenticeerd tegen de registratie die wordt bijgehouden door de EUR.

## Toegangsregels van gebruikersdomein naar serverdomeinen

De **toegangsregels** vanaf gebruikersdomeinen naar serverdomeinen worden samengevat in de volgende twee afbeeldingen:




*A. Toegangsregels voor 'medewerkers specifiek', 'medewerkers algemeen' en 'beheerders'*




*B. Toegangsregels voor 'externe relaties', 'studenten', 'patiënten' en 'publiek'*

NB: De pijlen geven de toegelaten verkeersrichting aan.

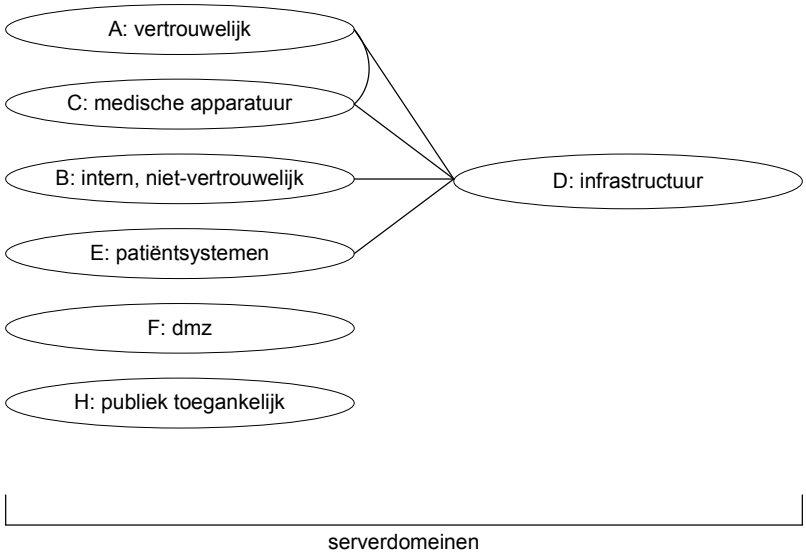
## Toegangsregels tussen serverdomeinen onderling

Communicatie tussen servers onderling kan voor allerlei verschillende toepassingen nodig zijn.
Voorbeelden:

* een applicatieserver die een mail server of database server aanspreekt
* communicatie tussen ZIS en een HL7 communicatieserver
* back-up
* beheersinstrumentatie (HP Openview/Servicedesk).

De volgende toegangsregels gelden tussen **serverdomeinen onderling**:

- het domein 'vertrouwelijk' (A) heeft toegang tot het domein 'medische apparatuur' (C) en vice versa;
- het domein 'infrastructuur' (D) heeft toegang tot de serverdomeinen A/B/C/E/F en vice versa.




Communicatie tussen serverdomeinen is onderworpen aan beperkingen op basis van TCP- of UDP-poortnummer ('netwerkdiensten'). DI / Systemen & Netwerken houdt een lijst bij van poortnummers (c.q. 'netwerkdiensten') die als standaard worden toegelaten op deze overgangen.

Als communicatie vereist is tussen twee serverdomeinen waar dit *niet* is voorzien in de standaard-toegangsregels, dan moet de verantwoordelijke hiervoor een 'aanvraag voor afwijkende toegangsregels' doen, waarin precies wordt aangegeven welke toegang vereist is en waarom.

## Externe toegang tot gebruikersdomeinen (individuele gebruikers)

Definities en uitgangspunten:

a Onder een **extern** systeem c.q. een externe gebruiker wordt elk systeem of elke gebruiker verstaan die zich fysiek buiten de muren van het Erasmus MC bevindt.

b Onder **externe toegang** wordt verstaan dat een verbinding tot stand wordt gebracht tussen een extern systeem en de netwerkinfrastructuur van het Erasmus MC, gebruikmakend van een inbelverbinding, huurlijn of Internet.

c Bij **externe toegang door individuele gebruikers** wordt het externe systeem gedurende de levensduur van de verbinding bediend door één persoon. Daarbij is sprake van een logische verbinding tussen client en server, waarbij de client-rol wordt vervuld door het externe systeem.

Bij deze vorm van toegang kan de identiteit van een externe gebruiker worden geverifieerd met **persoonsgebonden authenticatiemiddelen**.

d De eisen die worden gesteld aan externe toegang door individuele gebruikers zijn hetzelfde voor **directe toegang** naar achterliggende serverdomeinen (bijvoorbeeld via IPsec VPN) als voor **indirecte toegang** (bijvoorbeeld via “web-VPN”). Kenmerkend voor al deze scenario’s is dat de server ‘intern’ is en de gebruiker ‘extern’, en dat de gebruiker zijn identiteit kan bewijzen.

*Ter vergelijking: als een gebruiker op een publiek toegankelijke webserver inlogt is geen sprake van een* interne *server die wordt benaderd – en ook geen sprake van externe toegang. Wèl zal in veel gevallen een dergelijke webserver vervolgens informatie willen uitwisselen met interne systemen; dit wordt beschouwd als ‘externe toegang ten behoeve van systeem/systeemkoppeling’ – zie verderop.*

Authenticatie-eisen:

Een externe gebruiker wordt uitsluitend met een bepaald gebruikersdomein geassocieerd als bij het totstandbrengen van de verbinding tussen het externe systeem en de netwerkinfrastructuur van Erasmus MC de identiteit kan worden geverifieerd met behulp van een authenticator – zoals een wachtwoord, token of smartcard.

Hierbij gelden per gebruikersdomein onderstaande eisen:

| | *Gebruikersdomein + toelichting* | *Authenticatie-eisen voor koppeling met gebruikersdomein* |
|---|---|---|
| 1 | ‘medewerkers specifiek’;<br>toegang tot vertrouwelijke systemen | sterke authenticatie |
| 2 | ‘medewerkers algemeen’;<br>toegang tot interne systemen | matige authenticatie |
| 3 | ‘beheerders’;<br>toegang tot alle domeinen | sterke authenticatie of terugbelbeveiliging |
| 4 | ‘externe relaties’;<br>maatwerk-toegang (bijv. leveranciers) | sterke authenticatie |
| 5 | ‘studenten’ | matige authenticatie<br>(met door EUR uitgegeven wachtwoord) |

Deze authenticatie-eisen staan los van de authenticatie-eisen op applicatieniveau.

Onder **matige authenticatie** wordt verstaan: gebruik van gebruikersnaam en wachtwoord.

a Bij indiensttreding wordt de identiteit van een nieuwe medewerker gecontroleerd aan de hand van een identiteitsbewijs. Op basis daarvan wordt de medewerker in de personeelsadministratie opgenomen en wordt een gebruikersnaam (microsectienummer) en wachtwoord toegekend.

   Deze registratie voldoet aan zekerheidsniveau (4) in NEN7512 (paragraaf 7.1): “Directe controle (face-to-face) aan de hand van een document volgens Artikel 3 van de Wet Identificatie bij Dienstverlening (WID)”

b Studenten worden geregistreerd door de EUR. Bij externe toegang naar Erasmus MC wordt door de firewall een controle gedaan op de door EUR uitgereikte gebruikersnaam en wachtwoord.

Voor het wachtwoord gelden onderstaande eisen (o.a. op basis van NEN7512 / EN12251).[1]
Het wachtwoord dient:

a niet gemakkelijk te raden te zijn (zie wachtwoordbeleid)

b nergens, ook niet ter verificatie, in leesbare vorm te worden opgeslagen

c nooit onversleuteld te worden verzonden

d door de houder zelf regelmatig te worden gewijzigd (zie wachtwoord-beleid).

Als **sterke authenticatie** vereist is, dan kan één van de onderstaande middelen worden gebruikt:

a Een cryptografisch token, mits beschermd met een persoonlijke PIN-code

b Een cryptografische smartcard, mits beschermd met een persoonlijke PIN-code

Voor beide authenticatoren geldt dat bij het uitreiken van de authenticator de identiteit van de gebruiker nogmaals moet worden gecontroleerd; bovendien dient (met uitzondering van externe relaties) te worden geverifieerd dat de gebruiker is opgenomen in de personeelsadministratie.

Uitsluitend ten behoeve van beheer wordt ook **terugbelbeveiliging** toegestaan. In dat geval is het huis-telefoonnummer van de beheerder vastgelegd bij S&N.

Installatie van een zogenaamd certificaat (inclusief het sleutelpaar dat hierbij hoort) op een computersysteem vormt geen erkend middel voor de authenticatie van gebruikers – omdat het computersysteem wordt geauthenticeerd, niet de gebruiker. Een smartcard die wordt gebruikt als drager van sleutelpaar/certificaat, mits beschermd met een persoonlijke PIN-code, wordt wel erkend in die rol, omdat de gebruiker zelf een onmisbare schakel is in de authenticatie (‘something you have’ en ‘something you know’).

**Encryptie**. Voor alle verbindingen die via het Internet worden gemaakt naar bovenstaande domeinen is versleuteling met IPsec of SSL/TLS vereist. Dit komt overeen met versleutelingsniveau (1) in NEN7512: “versleutelde verbinding”.

Voor kieslijnverbindingen (ISDN/modem) direct naar centrale voorzieningen van het Erasmus MC (modempool e.d.) is geen versleuteling vereist.

**Integriteit**. Alle verbindingen die via het Internet worden gemaakt dienen door middel van cryptografische technieken te worden beschermd tegen het wijzigen van de overgedragen informatie. Dit is een automatisch gevolg van het gebruik van IPsec (AH of ESP) of SSL/TLS. Let op: dit veronderstelt nog geen end-to-end integriteit op applicatieniveau!

[1] Op dit moment kan nog niet in alle systemen van Erasmus MC aan al deze eisen worden voldaan. De uitzonderingen worden in kaart gebracht.

## Servers in verschillende domeinen koppelen (systeem/systeem-koppelingen)

Toelichting op systeem/systeem-koppelingen

In veel toepassingen is geen sprake van een gebruiker die kan worden geauthenticeerd bij het totstandkomen van de verbinding, maar is sprake van een **'unattended' communicatie tussen twee computersystemen**. Het onderstaande heeft betrekking op dergelijke communicatie tussen computersystemen in verschillende domeinen, inclusief scenario's waarbij één van de betrokken computersystemen extern is geplaatst.

Bij dergelijke systeem/systeemkoppelingen is gebruikersauthenticatie op netwerkniveau niet aan de orde. Systeemauthenticatie biedt slechts in beperkte mate een bijdrage aan vertrouwelijkheid: allerlei verschillende gebruikers en processen kunnen immers toegang hebben tot het systeem. Daarom worden hogere (en met name: inrichtings-)eisen gesteld aan de beveiliging van de betrokken systemen op toepassings-/systeemniveau.

De rol van de 'verantwoordelijke' voor het informatiesysteem

a Een systeem/systeem-koppeling wordt altijd gerealiseerd ten behoeve van een bepaald **informatiesysteem**. Dit informatiesysteem dient door de verantwoordelijke te worden **geclassificeerd**.

   Als ten behoeve van het informatiesysteem communicatie tussen verschillende domeinen nodig is (en 'externe toegang' is daarvan een voorbeeld) dan moet de verantwoordelijke in kaart (laten) brengen welke beveiligingsmaatregelen op netwerk-, systeem- en applicatieniveau nodig zijn en hoe deze passen in het geheel van de beveiliging van het informatiesysteem.

b De verantwoordelijke voor het informatiesysteem draagt er zorg voor dat de inrichting van alle benodigde systeem/systeem-koppelingen voldoet aan het hier vastgelegde beleid, inclusief alle benodigde middelen – ook al kunnen daarin middelen worden toepast die door de Directie Informatie ter beschikking worden gesteld.

Beleid en architectuur

a Er zijn **twee manieren** waarop een systeem/systeemkoppeling gestalte kan krijgen: rechtstreeks, via een aanpassing van de toegangregels, en indirect, met een tussengeplaatst systeem (een 'applicatie-gateway').

b **Rechtstreekse koppeling, via aanpassing toegangsregels**. Als ten behoeve van een informatiesysteem een systeem/systeemkoppeling nodig is tussen twee systemen die in verschillende serverdomeinen zijn geplaatst, dan kan de verantwoordelijke een 'aanvraag voor afwijkende toegangregels' indienen.

   Op basis van deze procedure wordt dan (na toetsing) ten behoeve van dit specifieke informatiesysteem een directe communicatie tussen twee servers toegelaten.

   Deze werkwijze is primair bedoeld voor **interne** inter-domein communicatie tussen systemen, bijvoorbeeld tussen systemen in serverdomein A ('intern, vertrouwelijk') en serverdomein B ('intern, niet-vertrouwelijk). De werkwijze is **niet toelaatbaar** als zich één (of beide) van de volgende condities voordoet:

   1 Als één van de communicerende systemen **extern** is, of **publiek toegankelijk** (op domein F of H).

   2 Als uit de classificatie blijkt dat het informatiesysteem op het aspect vertrouwelijkheid of integriteit in de klasse 'hoog' moet worden geplaatst.

   Vanaf bijvoorbeeld een publieke webserver wordt als regel **geen directe toegang** naar interne domeinen toegelaten (met uitzondering van domein beheer), of de server nu is geplaatst in het DMZ domein of daarbuiten. Als vanaf zo'n webserver toegang nodig is naar interne systemen, databases, etc, dan moet tussen webserver en interne server een applicatie-gateway in het DMZ-domein (F) worden geplaatst.

c **Indirecte koppeling via applicatie-gateway**. Als een rechtstreekse koppeling niet toelaatbaar is of niet voldoende veiligheid biedt, dan moet de systeem/systeem-koppeling worden gerealiseerd met een tussengeplaatst systeem. Dit systeem fungeert als een zgn. applicatie-gateway, die beide systemen op applicatieniveau isoleert en die de benodigde vertrouwelijkheids- en integriteitseisen (zoals gebleken uit de classificatie) waarborgt.

Uit het ontwerp van het betrokken informatiesysteem en de classificatie en risicoanalyse vloeien de inrichtingseisen voort die worden gesteld aan de beide betrokken eindsystemen en aan de tussengeplaatste applicatie-gateway. Deze laatste is dus als maatwerk te beschouwen.

d **Afzonderlijk systeem, afzonderlijk project**. Een applicatie-gateway dient een afzonderlijk systeem te zijn: als één van de te koppelen systemen gecompromitteerd wordt (bijv. toegang als root/administrator) dan mag dat niet betekenen dat ook de applicatie-gateway is gecompromitteerd.

De realisatie van een applicatie-gateway wordt door Directie Informatie uitgevoerd als een zelfstandig project, in opdracht van de 'verantwoordelijke' voor het informatiesysteem ten behoeve waarvan de koppeling moet worden gerealiseerd.

e **Plaatsing van applicatie-gateway**. Als één van de betrokken systemen extern is moet een applicatie-gateway worden geplaatst in het DMZ-domein (F).

Als sprake is van een koppeling tussen twee interne systemen, maar waar om veiligheidsredenen toch een tussenplaatsing nodig is moet voor een dergelijke applicatie-gateway een maatwerk-voorziening worden getroffen (een 'interne DMZ').

Technische voorwaarden

a Middelen die zijn toegelaten voor **gebruikersauthenticatie** (zie elders in dit document) mogen niet worden gebruikt voor geautomatiseerde systeem/systeem-koppelingen, waarbij immers een computersysteem of applicatie wordt geauthenticeerd – geen menselijke gebruiker. Scripts waarin wachtwoorden zijn ingeprogrammeerd zijn soms onvermijdelijk, maar mogen niet worden beschouwd of gebruikt als authenticatiemiddel op netwerkniveau.

b Als een applicatie-gateway gegevens moet uitwisselen met een extern systeem, dan dient dat externe systeem op één of meer van de volgende wijzen te worden geauthenticeerd:

- een op het betrokken systeem geïnstalleerd servercertificaat en bijbehorende private key, waarvan de echtheid bij een door Erasmus MC vertrouwde CA kan worden geverifieerd;
- een aan weerszijden overeengekomen **cryptografische sleutel** – mits in de inrichtingseisen voldoende waarborgen zijn getroffen ten aanzien van sleutelbeheer;
- **'lijn-authenticatie'** (vaste lijn, inclusief huurlijnen) – mits inrichtingseisen worden gesteld aan de fysieke beveiliging van de eindpunten van de lijn;
- als bijzondere vorm van lijn-authenticatie kan ook een **IPsec VPN verbinding** over het Internet worden gebruikt, mits aan de algemene inrichtingseisen voor zo'n verbinding is voldaan en mits gewaarborgd is dat deze verbinding uitsluitend de twee eindsystemen op de gekozen manier met elkaar verbindt; een zgn. 'site-to-site' VPN met routers is alleen toelaatbaar als de connectiviteit wordt beperkt tot de twee eindsystemen.

Ten aanzien van de authenticatie van interne systemen moet een keuze worden gemaakt op basis van de bredere beveiligingsanalyse van het betrokken informatiesysteem.

c De gegevensuitwisseling tussen eindsystemen via de applicatie-gateway dient **geminimaliseerd** te worden tot die informatie die voor de **onderhavige toepassing** benodigd is; de applicatie-gateway dient zo te worden ingericht dat het niet mogelijk is om zonder expliciete herziening van de inrichting andere informatie uit te wisselen.

Voorbeeld: een HL7 applicatie-gateway zou alleen die specifieke HL7 berichten moeten vertalen en doorsturen die voor het betreffende informatiesysteem vereist zijn, dit in plaats van een generieke HL7 gateway die *elk* HL7 bericht aankan – en die dus zonder aanpassing in beleid of inrichting (en mogelijk onbedoeld) veel breder kan worden gebruikt.

## Aanpassingen en uitzonderingen

1 De Raad van Bestuur en het MT Directie Informatie moeten kunnen vertrouwen dat domeinindeling en toegangsregels worden gehandhaafd en dat gevallen waar dat níet het geval is, bekend en zichtbaar zijn.

2 **Aanpassingen**. Het MT van de Directie Informatie kan besluiten tot een aanpassing van deze richtlijn (indeling en toegangsregels). De richtlijn wordt beheerd door de Security Officer van Erasmus MC.

3 **Afwijkende toegangsregels**. Het staat de 'verantwoordelijke' voor een informatiesysteem vrij om te komen tot een verdere inperking van de hier vastgelegde toegangsregels mits de hieronder geschetste consequenties ten aanzien van de infrastructuur in aanmerking worden genomen. Hiervoor is geen goedkeuring van de Security Officer benodigd.

   Als echter voor de communicatie tussen twee systemen een **uitbreiding** van de toegangsregels nodig is, dan moet hiervoor een **'aanvraag voor afwijkende toegangsregels'** worden gedaan. Deze aanvraag wordt aan gericht aan het Hoofd Systemen & Netwerken, door de Security Officer beoordeeld en uiteindelijk door het Hoofd Systemen & Netwerken goedgekeurd of afgewezen.

   Zowel een inperking als uitbreiding van de toegangsregels kan gevolgen hebben voor de inrichting van de infrastructuur (server, netwerk, inrichting gebruikers-PC's, authenticatiemiddelen). Deze gevolgen worden door de verantwoordelijke in overleg met S&N in kaart gebracht; vervolgens is het aan de verantwoordelijke om deze gevolgen te adresseren voordat een systeem in productie wordt genomen.

4 **Overige uitzonderingen**. Als het nodig wordt geacht om af te wijken van de beleidsregels in dit document en die afwijking gaat verder dan alleen de toegangsregels, dan wordt een gemotiveerde aanvraag gericht aan het Hoofd Systemen & Netwerken. Op basis van advies door de Security Officer en het Hoofd Systemen & Netwerken besluit het MT van de Directie Informatie tot goedkeuring of afwijzing.

5 Elk van bovenstaande aanpassingen van de toegangsregels (uitbreidingen, inperkingen, en uitzonderingen) wordt doorgegeven aan en geregistreerd door **technisch beveiligingsbeheer**, belegd bij de afdeling Systemen & Netwerken.

   De taak van technisch beveiligingsbeheer is om een registratie bij te houden die op elk gewenst moment inzicht geeft in de geldende *normatieve* toegangsregels ('Soll') – los van de *implementatie* van deze toegangsregels in individuele producten (firewalls, routers, etc; de 'Ist'). Desgewenst kan door de afdeling Systemen & Netwerken of door derden worden geverifieerd dat de 'Soll' en 'Ist' posities met elkaar corresponderen.

### Huidige uitzonderingen en verbijzonderingen

Er zijn op dit moment reeds een aantal 'verbijzonderingen' aangebracht in het netwerk, die een aanscherping vormen ten opzichte van de in dit document vastgelegde toegangsregels – en waarvoor om die reden geen aparte goedkeuring of registratie is vereist:

a Het serverdomein '**acceptatie- en test**' is een verbijzondering van het serverdomein 'vertrouwelijk' (A). Vanuit de gebruikersdomeinen wordt echter alleen verkeer vanaf het domein 'beheerders' (3) toegelaten.

b Het gebruikersdomein **'applicatiebeheer'** is een verbijzondering van het gebruikersdomein 'beheerders', maar zonder toegang naar serverdomein 'infrastructuur' (D).

c Het gebruikersdomein **'PDMS clients'** is een verbijzondering van het gebruikersdomein 'medewerkers specifiek', maar zonder toegang naar publiek toegankelijke systemen (H).

d Voor de toegang tot interne systemen door leveranciers zoals Vosko en iSOFT wordt een uitzondering aangevraagd. Zij worden ingedeeld in het gebruikersdomein '**externe relaties**'.