



# **Unified Communications-federatie voor Microsoft OCS op basis van XMPP *Implementatiehandleiding***

Project : SURFworks  
Projectjaar : 2010  
Projectmanager : A. van den Hil  
Auteur(s) : E. Dobbelsteijn (NiVo Network Architects)  
Opleverdatum : 31 12 2010  
Versie : 1.0

## **Samenvatting**

SURFnet wil instellingsoverstijgende samenwerking bevorderen door Unified Communications-gebruikers van verschillende instellingen met elkaar, dus domeinoverstijgend, te kunnen laten communiceren. In eerder onderzoek is de open standaard XMPP voor instant messaging en presence gekozen.

Dit document omschrijft hoe XMPP geïmplementeerd wordt in het meest voorkomende Unified Communications-platform in het hoger onderwijs en onderzoek: Microsoft Office Communications Server 2007. Doel is te koppelen met andere XMPP-gebaseerde instant messaging-diensten en -platformen.



Voor deze publicatie geldt de Creative Commons Licentie "Attribution 3.0 Unported".

Meer informatie over deze licentie is te vinden op <http://creativecommons.org/licenses/by/3.0/>

## Colofon

Programmalijn : Stimulering gebruik en support  
Onderdeel : Kennis- en expertisedeling met ICT professionals, Expertisedomein GSO  
Activiteit : Federatieve UC koppelingen  
Deliverable : Handleiding XMPP voor MS Office Communications Server  
Toegangsrechten : publiek  
Externe partij : NiVo Network Architects

Dit project is tot stand gekomen met steun van SURF, de organisatie die ICT vernieuwingen in het hoger onderwijs en onderzoek initieert, regisseert en stimuleert door onder meer het financieren van projecten. Meer informatie over SURF is te vinden op de website ([www.surf.nl](http://www.surf.nl)).



### Versiehistorie:

Ver	Datum	Voortgang	Door	review
0.1	02-10-10	Eerste concept voor kick-off	ED	DA
0.2	04-10-10	Onderzoeksvragen toegevoegd, kleine correcties	ED	DA
0.3	06-10-10	In SURFnet template gegoten	ED	AlHi
0.4	11-11-10	Aangepast n.a.v. ervaringen Windesheim	ED	
0.5	24-12-10	Concept t.b.v. finale review	ED	AlHi, RoSt, DA, HeBe, BaZo
1.0	29-12-10	Finale versie. Review verwerkt, ervaringen SURFdiensten toegevoegd	ED	

## 6 dingen die je moet weten over 'Unified Communications-federatie voor Microsoft OCS op basis van XMPP - Implementatiehandleiding'

Context	<p>SURFnet stimuleert het gebruik van Unified Communications omdat deze trend de communicatiemiddelen bundelt van medewerkers en studenten en samenwerken eenvoudiger maakt. Om dat ook instellingsoverstijgend mogelijk te maken, worden instellingen in dit traject geassisteerd bij de implementatie van XMPP.</p>
Wat is dit document?	<p>Deze handleiding beschrijft hoe Microsoft OCS, het Unified Communications-platform dat het meest gebruikt wordt in hoger onderwijs en onderzoek, kan worden uitgebreid met de mogelijkheid om op basis van XMPP de aanwezigheidsstatus van gebruikers tussen instellingen uit te wisselen en ze elkaar instant messages te kunnen laten sturen.</p>
Voor wie is dit document?	<p>Deze handleiding is bedoeld voor het technisch personeel, beheerders en projectleiders van instellingen die besluiten om XMPP te ondersteunen binnen hun Microsoft OCS implementatie.</p>
Hoe werkt Unified Communications-federatie?	<p>Voor eindgebruikers: een gebruiker van instelling 1 kan een gebruiker van instelling 2 opnemen in zijn contactenlijst. Als instelling 2 daartoe toestemming geeft en vice versa, kunnen zij van elkaar zien of ze online zijn (presence). Ook kunnen zij elkaar korte berichten sturen die meteen aankomen (instant messages).</p> <p>Voor technisch personeel: het Microsoft Office Communications Server platform wordt uitgebreid met een zogenaamde Edge Server en een XMPP-gateway server, beide in de demilitarized zone (DMZ) van het netwerk.</p>
Wat kun je met Unified Communications-federatie?	<p>Gebbruikers van verschillende instellingen kunnen</p> <ul style="list-style-type: none"><li>• elkaar opnemen in hun contactenlijst;</li><li>• elkaars online status zien (na toestemming);</li><li>• elkaar instant messages sturen</li></ul> <p>Datzelfde kunnen deze gebruikers ook doen met gebruikers van Google Talk, Google Apps, Cisco Webex en andere XMPP-gebaseerde publieke diensten.</p>
Extra (Bijlagen, Thema, Gerelateerde thema's)	<p>Naast deze handleiding is er:</p> <ul style="list-style-type: none"><li>• een document met een functionele beschrijving en use cases van Unified Communications-federatie. Dit gaat in op gebruiksmogelijkheden en -beleving.</li><li>• een projectverloopdocument, met conclusies en aanbevelingen.</li></ul>

# Inhoudsopgave

<b>1</b>	<b>Inleiding .....</b>	<b>5</b>
<b>2</b>	<b>Functionele beschrijving .....</b>	<b>7</b>
<b>3</b>	<b>Architectuur.....</b>	<b>9</b>
<b>4</b>	<b>Implementatie .....</b>	<b>19</b>
	<b>Bijlage 1 - Actieplan .....</b>	<b>23</b>
	<b>Bijlage 2 - Afkortingen en begrippen.....</b>	<b>24</b>

# Inleiding

## 1.1 Stand van zaken Unified Communications

SURFnet wil instellingsoverstijgende samenwerking stimuleren door instellingen te faciliteren in het koppelen (federeren) van hun Unified Communications-platformen. De use cases, benodigde functies en standaarden hiervoor zijn omschreven in een eerder traject dat o.a. NiVo uitvoerde voor SURFnet (zie <http://www.ucho.nl>).

Het blijkt dat de meeste instellingen in de SURFnet-doelgroep gebruik (gaan) maken van Microsoft Office Communications Server (OCS) voor de invulling van Unified Communications-functionaliteit. Dat maakt het koppelen eenvoudig, ware het niet dat deze koppeling een Microsoft-specifieke variant op het SIP-protocol is. Een voordeel is dat het gebruik van versleuteling met TLS wordt afgedwongen. Een nadeel is dat het product niet geheel volgens open standaarden te koppelen is andere SIP-infrastructuren. Ook al zijn er steeds meer fabrikanten die 'Microsoft Certified' te koppelen zijn, SURFnet wil zichzelf en haar instellingen niet beperken tot de (on)mogelijkheden van één leverancier en beoogt een op open standaarden gebaseerde communicatie-infrastructuur.

Dat is in elk geval mogelijk met een deel van de functies die OCS biedt, namelijk presence en instant messaging. OCS maakt het ook mogelijk om presence en instant messages met gebruikers in andere domeinen uit te wisselen, met toevoeging van een gateway die het XMPP-protocol ondersteunt.

## 1.2 Wat vindt u in dit document

Deze handleiding geeft een gedetailleerd stappenplan voor de implementatie van instant messaging en presence op basis van XMPP voor instellingen die reeds een OCS-platform operationeel hebben. Het resultaat is dat gebruikers van verschillende instellingen presence en instant messaging kunnen uitwisselen tussen op basis van het XMPP-protocol, als deze gebruikers elk gebruik maken van Microsoft Communicator op hun desktop of PDA/smartphone.

Vanaf hoofdstuk 3 vindt u invulvelden om ontwerpkeuzes voor uw specifieke instellingsimplementatie voor te bereiden. Deze velden zijn gemarkeerd met teksten als 'vul in', of 'te bepalen'.

## 1.3 Doelgroep

Dit document richt zich met name op technici en projectleiders die verantwoordelijk zijn voor het federeren van Microsoft OCS. Het document bevat veel technische termen en afkortingen die bekend verondersteld worden. Bovendien komt een aantal termen voor die Microsoft hanteert in haar handleidingen. Deze zijn gedefinieerd in de documentatie van Microsoft waar uitvoerig naar verwezen wordt.

Het onderwerp vereist diepgaande kennis van

- IP networking en firewalls
- DNS
- PKI
- Microsoft Windows 2003 of 2008 server
- Microsoft AD
- Microsoft OCS

## **1.4 Gerelateerde documenten**

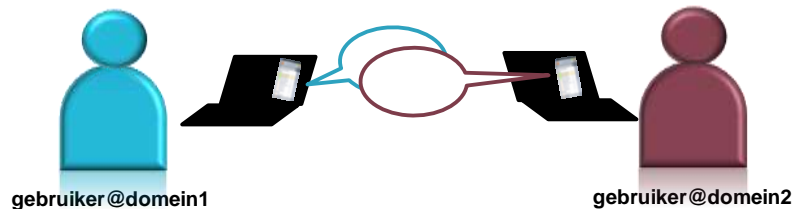
Het doel van het project, de use cases de functionele uitwerking en een beschrijving van best practices is beschreven in het document 'Unified Communications-federatie - Functionele beschrijving en use cases'.

Het document 'Unified Communications-federatie voor Microsoft OCS op basis van XMPP - Projectverloop' beschrijft de projectvoortgang van het project 'XMPP-federatie voor OCS'

## 2 Functionele beschrijving

### 2.1 Communicatie op basis van instant messaging en presence

Een gebruiker van instelling 1 wil communiceren met een gebruiker van instelling 2. Zij willen elkaars online status zien en instant messages uitwisselen. Daarvoor gebruiken zij software op hun PC, laptop of smartphone die een contactenlijst op het scherm toont. Deze software, bekend van diensten als Google Talk, Skype, Live Messenger, Yahoo en vele andere, wordt hierna 'client' genoemd.

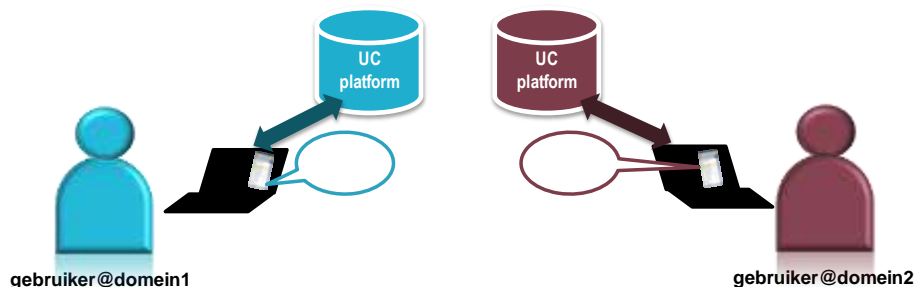


Als de eerste gebruiker in zijn client op zoek gaat naar de andere gebruiker en daarom het contactadres van de andere gebruiker intypt (de URI in de vorm van gebruiker@domein2), dan zoekt de OCS-server van domein1 contact met die van domein2. Als domein2 een white/black list bijhoudt van allowed partners en domein1 is nog niet 'allowed', dan komt gebruiker 1 er niet achter of gebruiker 2 ook OCS gebruikt. Als domein1 wel toegestaan is contact te leggen, dan zal gebruiker1 zien dat gebruiker2 ook OCS gebruikt, maar ziet nog niet zijn presence.

De zendende gebruiker van domein 1 stuurt zijn berichten vanaf één of meerdere clients. De meest gangbare clients hebben een presence roster, een lijst met contactpersonen. Naast elke contactpersoon is zijn status zichtbaar in de vorm van een gekleurd icoontje. Hiernaast is de Microsoft Office Communicator zichtbaar die normaal gesproken gebruikt wordt in combinatie met Microsoft OCS.



Deze clients staan elk in verbinding met hun eigen thuisplatform (OCS), zoals als een e-mailprogramma in contact staat met de e-mailserver van de instelling. De thuisplatformen regelen onderling dat de berichten bij de juiste gebruikers terecht komen.



## **2.2 Privacy**

Het is niet mogelijk om een andere persoon in het contactenlijstje op te nemen totdat deze goedkeuring heeft gegeven. Zo wordt de privacy van de andere partij beschermd.

Eerst stuurt gebruiker 1 daarom een verzoek aan gebruiker 2 om gebruiker 2 in zijn contactenlijst op te kunnen nemen (subscribe). Na goedkeuring door gebruiker 2 kan deze omgekeerd gebruiker 1 in zijn lijst opnemen. Daarvoor moet gebruiker 1 dan weer toestemming verlenen. Als één van beiden in een later stadium niet meer zichtbaar wil zijn voor de ander, kan hij de contactpersoon verwijderen uit de lijst.

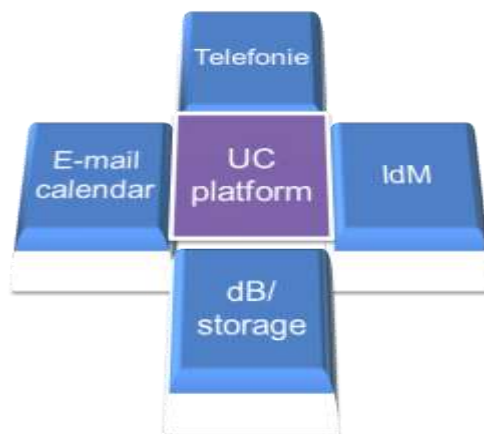
## 3 Architectuur

### 3.1 Kern van het systeem

Om federatie mogelijk te maken, moet eerst een werkend OCS-platform succesvol geïnstalleerd zijn binnen de instelling. Dat kan op vele manieren, omdat er veel scenario's zijn voor het inrichten van OCS zijn. Zaak is dat de validation wizard, een installatiehulpmiddel dat meegeleverd wordt met OCS, geen fouten ontdekt in de bestaande configuratie.

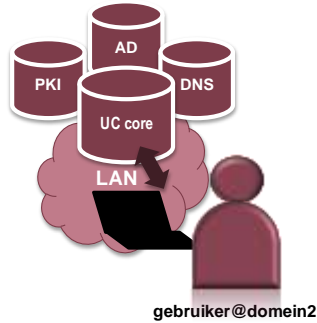
Het is met het bestaande platform al mogelijk om binnen de instelling te chatten tussen interne gebruikers onderling.

In het algemeen wordt het interne Unified Communications-platform omringd door een groot aantal andere systemen en vervult het een integratierol:



Omdat er verschillende architecturen mogelijk zijn voor de interne implementatie van OCS, wordt dit verder het 'coreplatform' genoemd. Dat platform staat nooit op zichzelf maar is sterk afhankelijk van onder andere:

- de Active Directory voor gebruikersbeheer en authenticatie;
- DNS voor het vinden en gevonden worden van andere delen van het systeem;
- PKI voor beveiliging op basis van X.509 certificaten;
- storage voor opslag van gebruikers- en gebruiksgegevens.



De Unified Communications-core kan zowel een standard edition- als een enterprise edition-platform zijn, al dan niet met load balancers en additionele directors. De verschillende core-componenten zijn uitgevoerd als services die bovenop het besturingssysteem draaien. Denk aan services als Front End Server, A/V server, IM MCU server, web conferencing server. Ze kunnen colocated op één server draaien of verdeeld zijn over (ge-loadbalancete) servers. Er bestaat één resource pool waaraan de Edge Server gekoppeld zal worden.

**Noteer het domein dat in dit project ontsloten wordt:**

---

**Noteer de naam van de resource pool:**

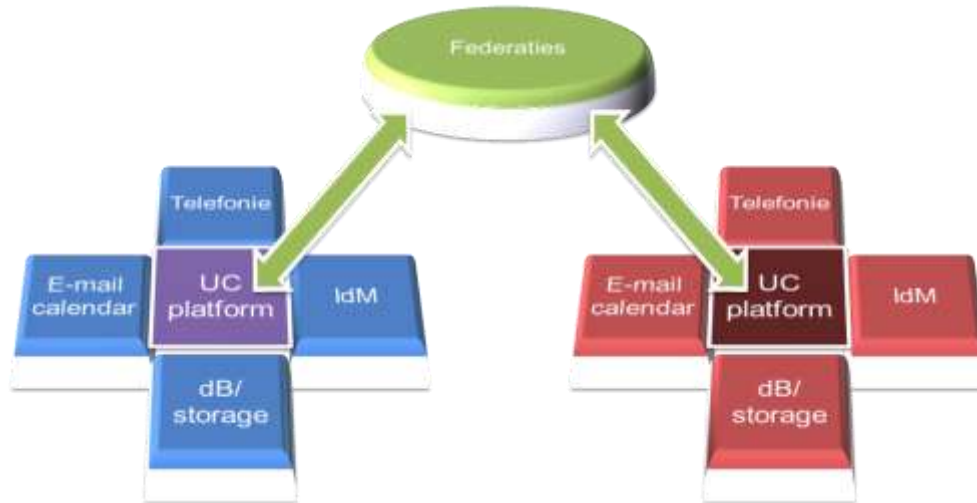
---

**Noteer hier de architectuur van het core systeem (Standard edition, Consolidated Enterprise architectuur, load balancing, inzet van directors etc.):**

---

### **3.2 Toevoeging van federatie**

In eerdere onderzoeken werd instellingsoverschrijdende communicatie functioneel voorgesteld door de Unified Communications-platformen te koppelen:

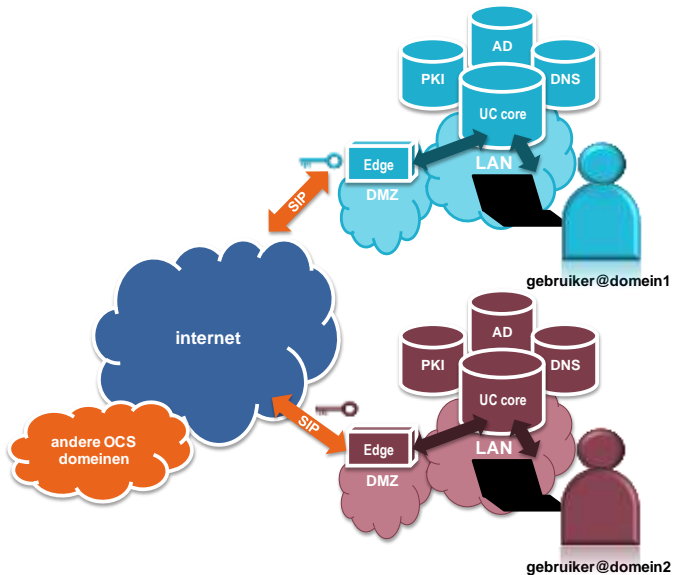


Het principe van organische federatie (zie het rapport '[Federatieve architectuur voor UC in het HO&O](#)') betekent dat er geen centrale componenten nodig zijn om verschillende domeinen te koppelen, zoals dat bij de andere optie (hiërarchie) wel het geval is. Een alternatieve architectuur is mogelijk op basis van Distributed Hash Tables (DHT) zoals Skype die gebruikt, maar die is voor XMPP niet beschikbaar en is voor SIP in de maak, maar nog niet wijdverbreid. DHT houdt in dat elke deelnemer in het netwerk een tabel heeft met adressen van enkele andere deelnemers zodanig dat ze samen een dynamisch geheel vormen en voor elkaar berichten routeren naar andere deelnemers (nodes).

In de praktijk is een nadere uitwerking van het Unified Communications-platform nodig. Het is bijvoorbeeld niet wenselijk om het kernsysteem bloot te stellen aan het open internet zoals in het bovenstaande diagram lijkt. Het Unified Communications-platform in het bovenstaande diagram bestaat uit een aantal componenten. De kern van het systeem bestaat uit alle componenten die nodig zijn voor *intern* gebruik van Unified Communications. De ontsluiting naar buiten vindt plaats via een bastion dat in een demilitarized zone (DMZ) van het netwerk wordt geplaatst. In termen van standaardisatie wordt zo'n bastion ook wel een 'gateway' of SIP Border Controller genoemd (SBC).

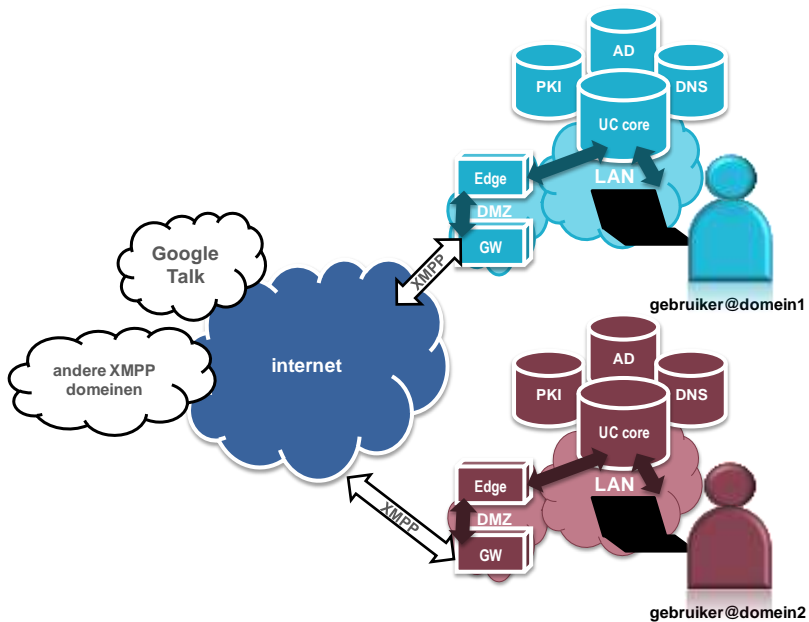
### **Federatie op basis van SIP over TLS (Microsoft-specifiek)**

Microsoft noemt deze component van zijn OCS-infrastructuur de Edge Server. Contact tussen domeinen wordt gelegd tussen Edge Servers onderling, die SIP over TLS gebruiken voor de communicatie. Hieronder is deze 'native' federatie van OCS-implementaties schematisch weergegeven:



### Federatie op basis van XMPP

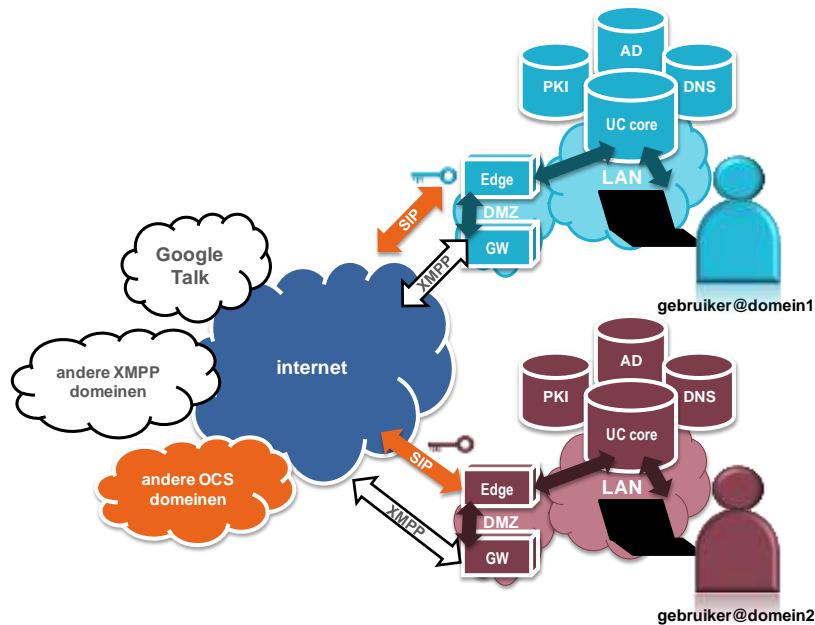
Omdat dit project focust op het gebruik van open standaarden, wordt voor presence en instant messaging de additionele OCS XMPP-gateway ingezet. De XMPP-gateway vertaalt SIP over TLS naar XMPP en vice versa, en legt de relatie tussen de buitenwereld en de core via de Edge Server:



Federatie op deze wijze gebruikt het XMPP-protocol voor instant messaging en presence, zonder encryptie en zonder aanvullende media zoals audio, video, desktopdelen enzovoort.

## Hybride federatie

Zodra de XMPP-gateway is geïnstalleerd, kan de instelling kiezen welk protocol gebruikt wordt om een ander domein te bereiken. Standaard probeert OCS op de 'native' OCS-manier (SIP over TLS) het andere domein te bereiken. Als in de Edge Server en op de XMPP-gateway ingesteld wordt dat het domein via de XMPP-gateway bereikt moet worden, wordt automatisch het XMPP-protocol ingezet naar buiten toe:



## 3.3 Virtualisatie

Vaak wordt virtualisatie van de serverrollen toegepast. Microsoft biedt alleen ondersteuning voor (kort samengevat) 'niet-real-time rollen' van OCS, dus instant messaging en presence. Voor audio, video, webconferencing en telefoniefuncties wordt virtualisatie dus niet ondersteund. De website van Microsoft biedt meer informatie over [virtualisatie in combinatie met OCS](#).

Virtualisatie van de gebruikersdesktop is mogelijk zolang de functionaliteit beperkt blijft tot instant messaging en presence. Zodra audio en video benodigd zijn, voldoet de client-serverarchitectuur van gevirtualiseerde desktops niet om realtime de audio- en videostreamen heen en weer te sturen. Dat vereist encoding-kracht dichtbij de bron (de geluidskaart, de webcam en de processor) en decoding-kracht dichtbij het doel (wederom de videokaart, processor en de display driver). Thin clients zijn daar niet op berekend en het communicatieprotocol tussen de clients en de servers is niet ingericht op het op en neer sturen van realtime verkeer.

## 3.4 Ontwerpkeuzes

Een aantal ontwerpkeuzes is gemaakt tijdens de start van het project:

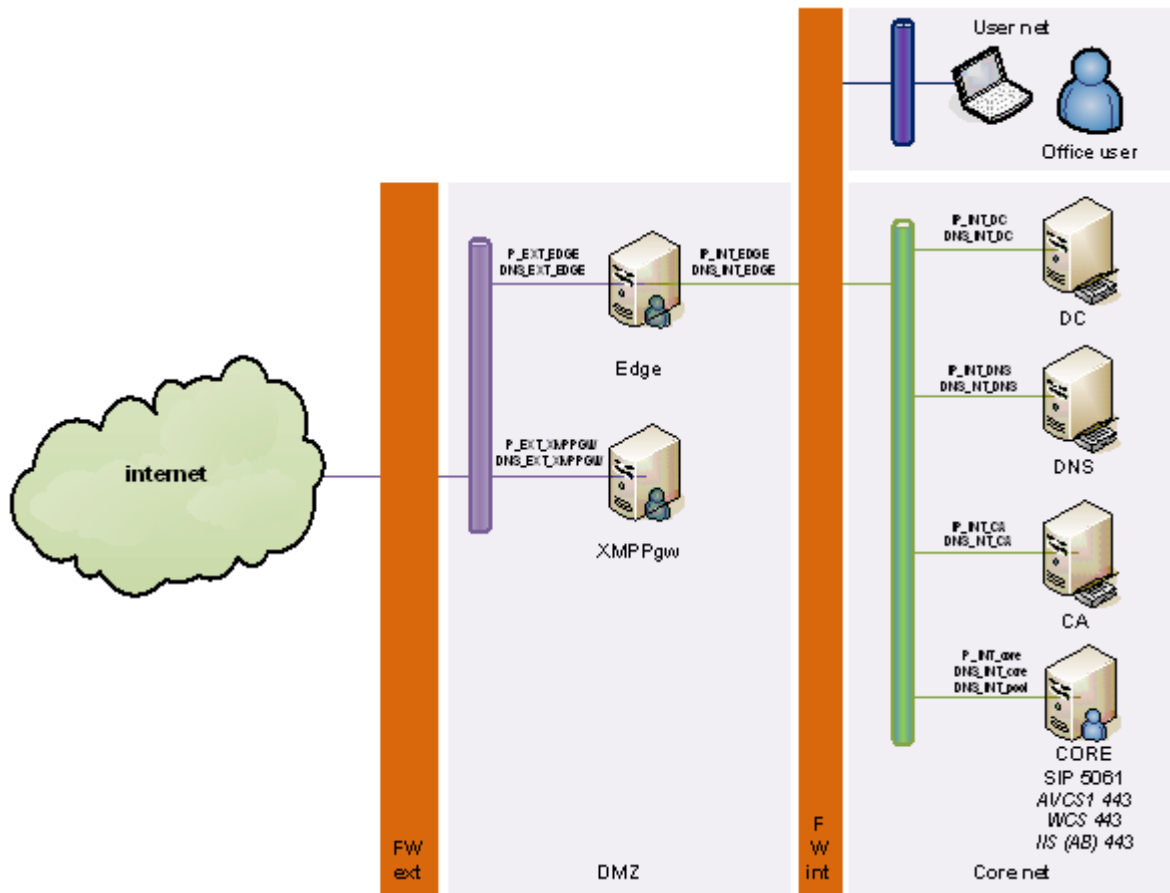
- Gereedmaken van federatie voor OCS behelst in elk geval de installatie van een Edge Server. Er zijn verschillende manieren om deze te implementeren. Deze handleiding hanteert het zogenaamde 'consolidated Edge' deployment scenario, waarbij alle software services waaruit de Edge Server

bestaat, op één machine samen actief zijn. Services die bij de Edge Server-rol horen zijn bijvoorbeeld de Remote Access Service en de AV service.

- Alleen de federatiefunctie van de Edge Server wordt geconfigureerd, dus geen Public IM Connectivity, web conferencing en remote access.
- De XMPP-gateway bouwt verder op de Edge Server. Om op basis van XMPP te federeren is het niet nodig dat de Edge Server van buiten te benaderen is. Als de Edge Server echter ook rechtstreeks benaderbaar is, en niet alleen via de XMPP-gateway, dan kunnen OCS-platformen ook andere media uitwisselen zoals audio en video. De vraag is echter: welk protocol krijgt voorrang bij het federeren tussen domeinen? Dat is nog onbekend. Tot dat bekend is, zal ook de Edge Server van buitenaf bereikbaar worden gemaakt. In feite is dan federatie mogelijk zowel op de 'OCS native' manier (SIP over TLS) en via XMPP. Zie paragraaf 3.2.
- Alleen de Edge Server wordt geïnstalleerd, niet de reverse proxy (die benodigd is voor het kunnen inzien van het adresboek als gebruik wordt gemaakt van remote access, en voor web conferencing).
- Deze handleiding gaat ervan uit dat er één resource pool is van OCS en één domein (instelling.nl).
- Microsoft raadt een director aan in de pool als een Edge wordt toegevoegd maar deze is niet verplicht. Een director laten we buiten beschouwing.
- Er zullen alleen enkelvoudige servers geïnstalleerd worden (dus geen load balancing van Edge Server en XMPP-gateway, ofwel het 'high availability scenario' zoals Microsoft het noemt).
- De instelling moet bepalen of externen van willekeurige organisaties contact mogen leggen met haar gebruikers. Het alternatief betekent dat de instelling kiest voor het hanteren van white lists en black lists. In dat geval zullen in elk geval de domeinen van de deelnemende instellingen worden toegelaten.
- Dimensionering van het platform hangt af van veel verschillende parameters. Microsoft hanteert de vuistregel dat tot 5000 client-connecties mogelijk zijn op één Edge Server met de verderop vermelde dimensies.

### **3.5 Netwerk**

De Edge Server en XMPP-gateway zullen in een DMZ geplaatst worden. Toegang van buiten wordt gecontroleerd door de externe firewall, en de communicatie tussen de Edge Server en het core-systeem wordt gecontroleerd door de interne firewall. De generieke opzet hiervan is in het onderstaande diagram weergegeven. De nummering en benaming van de servers is geabstraheerd, zodat elke instelling deze variabelen zelf kan invullen.



Voor elke interface is een IP-adres (intern of extern/publiek) en een DNS-record (A-record) nodig, en het is praktisch om de IP-adressen en DNS-namen van de core-systemen bij de hand te hebben:

Variabele	Omschrijving	waarde
IP_EXT_EDGE	extern IP-adres van Edge Server (public)	Bepaal: .....
DNS_EXT_EDGE	externe DNS-naam van Edge Server	Bepaal: .....
IP_INT_EDGE	intern IP-adres van Edge Server (private of public)	Bepaal: .....
DNS_EXT_EDGE	interne DNS-naam van Edge Server	Bepaal: .....
IP_EXT_XMPPGW	extern IP-adres van XMPP-gateway (public)	Bepaal: .....
DNS_EXT_XMPPGW	externe DNS-naam van XMPP-gateway	Bepaal: .....
IP_INT_CORE	intern IP-adres van OCS front end server(cluster)	..... (vul in)
DNS_INT_CORE	interne DNS-naam van OCS Front End server (cluster)	..... (vul in)
DNS_INT_POOL	interne DNS-naam van de OCS resource pool	..... (vul in)
IP_INT_DC	Intern IP-adres van Domein Controller (cluster)	..... (vul in)
DNS_INT_DC	Interne DNS-naam van Domein Controller (cluster)	..... (vul in)

IP_INT_CA	intern IP-adres van Certificate Authority	..... (vul in)
DNS_INT_CA	interne DNS-naam van Certificate Authority	..... (vul in)
IP_INT_DNS	IP-adres van intern DNS-server(cluster)	..... (vul in)
DNS_INT_DNS	DNS-naam van intern DNS-server(cluster)	..... (vul in)
IP_EXT_DNS	IP-adres van externe DNS-server(cluster)	..... (vul in)
DNS_EXT_DNS	DNS-naam van externe DNS-server(cluster)	..... (vul in)

TIP: kies voor DNS\_EXT\_EDGE de naam sip.< domein> om in een later stadium remote access mogelijk te maken.

Verder moeten SRV-records in DNS opgenomen worden:

Record	Type	TCP poort	A-record
_sipfederationtls._tcp.<domein>	SRV	5061	DNS_EXT_EDGE
_sipexternaltls._tcp.<domein>	SRV	5061	DNS_EXT_EDGE
_xmpp-server._tcp.<domein>	SRV	5269	DNS_EXT_XMPPWG

De externe firewall moet de volgende poorten open laten:

Firewall extern	Type	Poort	Van	Naar
XMPP	TCP	5269	Extern	IP_EXT_XMPPGW
			IP_EXT_XMPPGW	Extern
SIP	TCP	5061	Extern	IP_EXT_EDGE
			IP_EXT_EDGE	Extern

De interne firewall moet de volgende poorten open laten:

Firewall extern	Type	Poort	Van	Naar
SIP	TCP	5061	IP_INT_EDGE	IP_INT_CORE
			IP_INT_CORE	IP_INT_EDGE

De interne firewall moet nog meer poorten open zetten als ook audio en video gebruikt worden (zie ook de paragraaf 'Default Ports' in de Edge Deployment guide welke poorten optioneel opengezet moeten worden t.b.v. real-time media (OCS-to-OCS) en andere Edge-rollen, zoals remote access).

Optioneel is een additionele netwerkinterface mogelijk voor beheer en remote toegang en dergelijke. De routing hiervan mag niet in de weg zitten van de externe en interne routing van de machines.

## 3.6 Machines, software en besturingssysteem

### Edge Server

Voor de Edge Server geeft Microsoft een capaciteit van 5000 gelijktijdige sessies bij de volgende specificaties:

- 2.3 GHz CPU
- 8.0 GB memory
- 8 processors
- Kernel SSL disabled
- ASP NET 1.5 request queue limit of  $1.5 * \text{the number of concurrent users of the server}$
- HTTPS connection
- no collocation with other virtual server or Office Communications Server
- 16 GB virtual memory
- Communicator Web Access logging (retail tracing) set to off.

### XMPP-gateway

Twee (virtuele) machines met de volgende hardwarespecificaties moeten worden voorbereid (zie ook de handleiding):

System component	Minimum requirement
CPU	Dual processor, quad-core 2.0 gigahertz (GHz) + 4-way processor, dual-core 2.0 GHz +
Disk	2x 72 GB, 15K or 10K RPM, RAID 0 (striped) or equivalent
Memory	4 gigabyte(GB) of RAM
Install Space	15 MB
Cache	2 MB L2 per core
Network	1x gigabit network adapter
Bandwidth Requirements	128 kbps if deployed on Internet

De softwarespecificaties:

System component	Minimum requirement
.NET Framework	3.5
Operating System	The Windows Server 2003 Standard x64 Edition operating system with Service Pack 2 or Windows Server 2003 Enterprise x64 Edition with Service Pack 2

The 64-bit editions of Windows Server 2008	
Microsoft Management Console	3.0
Microsoft Visual C ++® 2005 Redistributable or Visual C++ 2008 Redistributable	

## 4 Implementatie

### 4.1 Inleiding

Dit hoofdstuk beschrijft de stappen die nodig zijn om federatie op basis van XMPP mogelijk te maken. De met 'voorbereiding' gemarkeerde zaken vergen doorgaans enige doorlooptijd (zoals certificaataanvragen) en zijn handig om in de voorbereidende fase uit te voeren.

In bijlage 1 op pagina 23 vindt u een actieplan voor de implementatie

### 4.2 Randvoorwaarden

- Het core-systeem op basis van OCS 2007 of OCS 2007 R2 is correct geïnstalleerd en werkend. Dit is te verifiëren met behulp van de Validation Wizard die bij de installatiesoftware meegeleverd wordt.
- Er is een DMZ beschikbaar met firewall tussen het publieke internet en de DMZ (de externe firewall), en een firewall tussen de DMZ en het coresysteem (de interne firewall).
- Bevoegden met administratieve toegang tot Active Directory, DNS, interne CA, firewalls zijn ten tijde van de implementatie beschikbaar.
- Fysieke toegang tot serverruimtes om apparatuur te installeren is nodig als gekozen is voor fysieke hardware.

Zie verder de 'Prerequisites' in de handleiding ([Planning Deploying and Administering OCS R2 XMPP-gateway](#)).

De IP- en DNS-gegevens en informatie over de topologie zijn ingevuld in hoofdstuk 3.

### 4.3 Hulpmiddelen

- Tijdens de installatie moet de Windows Server DVD (of ISO) beschikbaar zijn, evenals de OCS DVD (of ISO).
- Diepgaande technische informatie over OCS 2007 R2 is te vinden via de [Microsoft Technet site](#); op de Microsoft site staan ook [downloadbare handleidingen](#). De [OCS Planning guide](#) geeft meer informatie over de voorbereidingen, benodigde hardware en software.
- De [OCS resource tools](#) bestaan uit o.a. de MMC snap-ins en handige scripts en de debugginghulpmiddelen die de logging van de OCS-componenten kunnen analyseren en visualiseren.
- Een packetsniffer (zoals [Wireshark](#)) geeft inzicht in het netwerkverkeer zoals dat op een netwerkinterface binnenkomt en is handig om op alle machines beschikbaar te hebben.
- Eventueel kan een security assessment worden uitgevoerd met een tool als [OCS Assessment Tool](#).
- Download de [Edge Server Deployment Guide](#).
- De [Edge Planning tool](#) is een wizard die helpt om op een gestructureerde manier de benodigde informatie voor de implementatie van de Edge Server te verzamelen.
- Naast de validation wizard die in de OCS setup DVD inbegrepen is, is de online test <https://www.testocsconnectivity.com/> ook een praktisch hulpmiddel bij het debuggen van mogelijke Edge Server-problemen.

- [Download de gateway software](#) van de Microsoft website en tevens de laatste [hotfixes](#). Op de download pagina is ook de handleiding te vinden (Planning Deploying and Administering OCS R2 XMPP-gateway).

## 4.4 Installatiestappen

In het algemeen bestaat de installatie uit:

- Installatie van het OS
- Installatie van de software
- Configuratie van de rol
- Activering van de rol (daadwerkelijk starten van de services)
- Validatie van de rol

### Edge Server

VOORBEREIDING: voor de vereisten met betrekking tot hardware en software, zie de [OCS Planning guide](#).

VOORBEREIDING: Het interne certificaat kan eenvoudig via de interne CA worden aangevraagd, tenzij deze een interne doorlooptijd nodig heeft. Het externe certificaat wordt bij een publieke CA aangevraagd en zal zeker een doorlooptijd vergen. Het is handig om hiervoor de certificate wizard te gebruiken die meegeleverd wordt bij de installer. Microsoft biedt informatie over [leveranciers van certificaten](#), en daarnaast levert TERENA dergelijke certificaten. De gegevens:

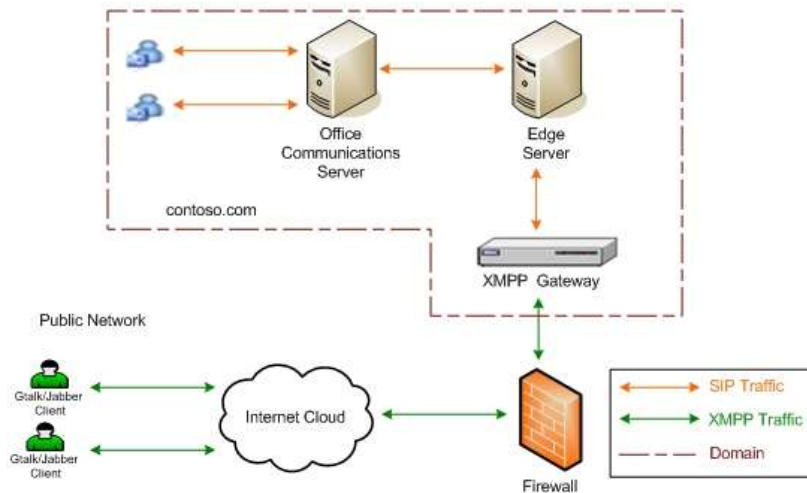
Extern certificaat (aan te vragen bij een publieke/commerciële CA)	
SN	DNS_EXT_EDGE of sip.<domein> (om later remote access mogelijk te maken)
SAN	sip.<domein>,DNS_EXT_EDGE
Attributen	MTLS

Intern certificaat (aan te vragen bij de interne CA)	
SN	DNS_INT_EDGE
Attributen	MTLS

Volg de Microsoft installatiehandleiding en met name het gedeelte 'Configure Federation' op pagina 33.

### XMPP-gateway

Van de Microsoft-installatiehandleiding ([Planning Deploying and Administering OCS R2 XMPP-gateway](#)) volgen we het scenario voor 'Public Federation':



Let op: in de documentatie wordt niet duidelijk gemaakt in welk scenario zowel een interne als een externe netwerkkaart nodig is in de XMPP-server. Voor het type deployment in deze installatiehandleiding is uitsluitend een *externe* interface nodig. Daarmee samenhangend is het van groot belang dat **de machinenaam (Netbios-naam) samen met de Primary DNS suffix gelijk is aan de FQDN.**

#### Belangrijke tips:

- Zorg dat de prerequisites ingevuld zijn; .net framework 3.5 en de Unified Communications API.
- De installer installeert niet de gatewaysoftware, maar een andere installer die in c:\program files\Microsoft Office Communications Server 2007 R2\XMPP-gateway installer\ komt te staan. Hierna moet dus de feitelijke setup uitgevoerd worden die in die directory staat.
- Installeer ook de hotfix.
- De XMPP-gateway kan alleen aan een domeincontroller verbonden worden als deze in de DMZ staat en het externe domein van de instelling bedient (bijv. 'instelling.nl'). Als de DC niet het externe domein ondersteunt, worden de primary DNS-suffix en de machinenaam verkeerd door de DC afgedwongen.
- De XMPP-gateway moet gebruik maken van externe DNS-resolvers, dus geen interne. Dat geldt overigens ook voor de Edge Server.
- De Common Name van het X.509-certificaat moet gelijk zijn aan de FQDN van de server (servernaam.instelling.nl). Ook is de 'Enhanced Key Usage' voor client authentication ('Client EKU') nodig. Het is het handigst om de Certificate Wizard te gebruiken op een Front End server. Andere wizards zijn hiervoor niet geschikt (de wizard op de Edge Server en de ingebouwde wizard in de 'Certificate MMC' van Windows 2008 Server). Genereer het request, dien het in bij een publieke CA en voltooi de wizard met het ontvangen getekende certificaat. Sla meteen het certificaat met private key op de front end server en verplaats het naar de XMPP-gateway.
- Vergeet niet de .config-file aan te vullen met het IP-adres van de server (deze stap is duidelijk vermeld in het stappenplan).

- Gebruik nslookup om te controleren of de Edge Server en XMPP-gateway voor elkaar te vinden zijn.
- Gebruik telnet om te controleren of poort 5269 en 5061 bereikbaar zijn op de XMPP-gateway en 5061 op de Edge Server.
- Gebruik een packet sniffer als Wireshark (zie 'hulpmiddelen') met filters als 'tcp.port==5269' om te zien of XMPP-gateway van en naar andere domeinen stroomt, en 'tcp.port==5061' om de communicatie tussen XMPP-gateway en Edge Server te controleren.

Onafhankelijk van het feit of Open Federation gebruikt wordt of niet, moet in de allowed list op de Edge Server (de white list voor andere domeinen) ingegeven worden welke domeinen via de XMPP-gateway te bereiken zijn.

## 4.5 Test & acceptatie

De validation wizard aan het einde van de installatie- en configuratieprocedure van de Edge Server deployment wizard laat zien of de installatie gelukt is.

Controleer of het mogelijk is om:

- een uitnodiging te versturen naar [erik@twiyo.nl](mailto:erik@twiyo.nl) en [erik.dobbelsteijn@gmail.com](mailto:erik.dobbelsteijn@gmail.com) via XMPP;
- presencestatus te wijzigen;
- instant messages uit te wisselen.

De gebruikers die toegestaan zijn om externe contacten te onderhouden, moeten (batchgewijs) worden *enabled for federation*.

## Bijlage 1 - Actieplan

Onderstaand overzicht van actiepunten geeft de concrete stappen weer die nodig zijn om federatie van OCS op basis van de XMPP-gateway in te richten, gegeven de randvoorwaarden. De fasering is als volgt gecodeerd:

- V Voorbereiding
- I Implementatie
- T Test
- O Oplevering

Actiepunt	Fase	Houder	deadline	Status
Randvoorwaarden controleren	V			
Software en licenties bestellen	V			
Hardware bestellen of dimensionering virtualisatieplatform aanpassen	V			
Reservering IP-adressen (intern, extern)	V			
Bepalen DNS namen en invoering in DNS	V			
Externe certificaten bestellen	V			
Creëren (virtuele) machines	V			
Installatie Operating Systems	V			
Installatie <i>prerequisites</i> en hulpmiddelen	V			
Installatie Edge Server	I			
Configuratie Edge Server	I			
Installatie XMPP-gateway	I			
Configuratie XMPP-gateway	I			
Testgebruikers <i>enablen</i> voor federatie	T			
Externe testgebruikers/testaccounts online	T			
Functionele test (subscription, presence change, IM)	T			
Gebruikers enablen voor federatie	O			

## Bijlage 2 - Afkortingen en begrippen

AD	Active Directory
CA	Certificate Authority
CRM	Customer Relationship Management
DC	Domain Controller
DMZ	Demilitarized Zone
DNS	Domain Name System
IM	Instant Message
IM&P	Instant Messaging & Presence
LDAP	Lightweight Directory Access Protocol
P(A)BX	Private (Automatic) Branch Exchange, ofwel huiscentrale
PKI	Public Key Infrastructure, waarin digitale certificaten gebruikt worden om identiteiten te verifiëren
Presence Roster	Software op PC of smartphone die een lijst met contactpersonen toont en hun 'presence' informatie (beschikbaarheidsinformatie) met symbolen en kleuren
SMART	Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdgebonden
SRV	Service record in DNS
SSO	Single Sign On
TCO	Total Cost of Ownership
URI	Universal Resource Identifier
VoIP	Voice over IP