

Advies

Advies
Federatieve architectuur voor Unified Communications

SURFnet bv

Versie	1.0
Datum	01-04-2010
Documentnaam	SN UC – Federatieve architectuur voor UC 1.0.doc
Auteur	E. Dobbelsteijn
Opdrachtgever	A. Steijaert, R. Staring
Referentienummer	

Versiehistorie:

Ver	Datum	Voortgang	Door	review
0.1	06-01-10	Eerste concept voor SURFnet	ED	ThEs, AnSt, RoSt
0.2	01-02-10	MoSCoW toegepast, samenvattende tabel toegevoegd, praktijkdeel naar bijlagen, versioning aangepast	ED	ThEs, AnSt, RoSt
0.3	19-03-10	Document is in lijn gebracht met kader zoals geschetst in 'Unified Communications implementeren' v.0.1 (15-03-2010)	ED	ThEs, RoSt, HeBe
1.0	01-04-10	Na goedkeuring samenvatting definitief	ED	

Inhoudsopgave

1	INLEIDING	5
1.1	DOEL	5
1.2	DOELGROEP EN LEESWIJZER.....	6
1.3	AANPAK	6
1.4	REFERENTIES	6
2	FEDERATIEVE UNIFIED COMMUNICATIONS ARCHITECTUUR OP BASIS VAN XMPP	7
2.1	UITGANGSPUNTEN VOOR DE ARCHITECTUUR.....	7
2.2	FUNCTIONALITEIT: FUNCTIONELE BESCHRIJVING VAN FEDERATIEVE IM&P	7
2.3	TOPOLOGIE EN MESSAGE FLOW	8
2.3.1	<i>Topologie</i>	8
2.3.2	<i>Koppelvlak</i>	9
2.3.3	<i>Hybride koppelvlak</i>	10
2.3.4	<i>Message flow</i>	10
2.4	SIGNALERING.....	11
2.4.1	<i>Native XMPP versus conversie</i>	12
2.5	ADRESSERING	12
2.6	MIDDLEWARE.....	12
2.6.1	<i>DNS</i>	12
2.7	AUTHENTICATIE EN AUTORISATIE.....	13
2.7.1	<i>Gebruikers</i>	13
2.7.2	<i>Domeinen</i>	13
2.8	IDM & DIRECTORY SERVICES.....	13
2.9	SECURITY.....	14
2.9.1	<i>PKI</i>	14
2.9.2	<i>Preventie</i>	14
2.9.3	<i>Risico's</i>	14
2.9.4	<i>Menselijke factoren</i>	15
2.10	NETWERK	15
2.10.1	<i>Poorten</i>	15
2.10.2	<i>Firewalls</i>	15
2.10.3	<i>NAT</i>	16
2.10.4	<i>Netwerkperformance</i>	16
2.11	DATABEHEER.....	16
2.12	ROBUSTHEID	16
2.12.1	<i>Dubbele uitvoering</i>	16
2.13	BEHEER	16
3	SAMENVATTING.....	19
4	CONCLUSIES EN AANBEVELINGEN	21
BIJLAGE A:	 PRAKTISCHE BEVINDINGEN BIJ HET GEBRUIK VAN XMPP VOOR FEDERATIEVE IM&P	22
A.1.	EIGEN INBRENG VAN LEVERANCIERS	22
A.2.	REFERENTIESERVER.....	22
A.3.	CLIENT	23
A.4.	ANALYSETOOLS	23
A.5.	CONCLUSIES EN AANBEVELINGEN VAN HET TEST BED.....	23
A.6.	AANBEVELINGEN	23
BIJLAGE B:	 AFKORTINGEN EN BEGRIPPEN.....	25

1 Inleiding

In korte tijd maakt SURFnet stappen naar een infrastructuur voor instellingsoverschrijdende elektronische samenwerking in de vorm van een 'federatie voor Unified Communications'. Veel instellingen oriënteren zich op Unified Communications (kortweg UC) en een aantal gebruikt het al in meer of mindere mate.

In oktober 2009 adviseerde NiVo Network Architects in het rapport '[Unified Communications in het Hoger Onderwijs en Onderzoek](#)' een aantal stappen die SURFnet kan ondernemen om grootschalige instellingsoverschrijdende multimediale communicatie te stimuleren.

Op technisch vlak heeft de studie twee ontwikkelingen gedetecteerd die realistische opties bieden om federatie tussen Unified Communications platformen van instellingen mogelijk te maken:

- Veruit de meeste instellingen die actief zijn op het gebied van Unified Communications gebruiken Microsoft Office Communications Server (OCS), dat federatie op basis van een eigen variant op de SIP standaard aan boord heeft
- Leveranciers maken nu grote stappen om federatie te realiseren door hun producten ofwel samen te laten werken met Microsoft OCS en/of de XMPP standaard in hun producten in te bouwen

Het eerder genoemde onderzoek naar 'Unified Communications in het Hoger Onderwijs en Onderzoek' is breed opgezet, en het doel was niet om diepgaand technisch te testen wat de gesteldheid van de functionele en technische interoperabiliteit is. Daarom is dit vervolgonderzoek opgezet, om de conclusies van het voorgaande rapport te toetsen aan de ontwikkelingen binnen standaardisatie en de praktijk, en daaruit de architectuur samen te stellen.

1.1 Doel

In dit project is in korte tijd een beeld gekregen van de manier waarop producten met de XMPP standaard omgaan. Die gegevens leiden tot aanbevelingen over het gebruik van XMPP als federatief protocol binnen de opgestelde architectuur. Op basis van deze blauwdruk kunnen instellingen:

- dezelfde set functies en invulling van de standaarden hanteren in gezamenlijke planvorming
- leveranciers selecteren die gestandaardiseerde federatiemogelijkheden bieden
- Unified Communications implementeren met federatie als uitgangspunt
- hun medewerkers en studenten over de instellingsgrenzen op een eenduidige manier met elkaar laten samenwerken

De architectuur die dit document beschrijft, heeft de volgende uitgangspunten:

- Deze architectuur is een concrete invulling van deelaspecten van 'Unified Communications implementeren' v.0.1 (15-03-2010) dat de algemene uitgangspunten schetst voor implementatie van UC in het HO&O
- Deze architectuur omschrijft uitsluitend inter-instellings communicatie. Het is dus geen 'campus architectuur' die bedoeld is voor het implementeren van UC binnen een instelling
- Op basis van eerder onderzoek concentreert deze architectuur zich op federatie van Instant Messaging en Presence (IM&P)
- Van de beschikbare protocollen die federatieve IM&P mogelijk maken, is in het voorgaande traject de standaard XMPP geselecteerd op basis waarvan inter-instellingsverkeer mogelijk gemaakt kan worden. De alternatieven zijn ofwel nog onvoldoende rijp en ondersteund (SIMPLE) of proprietary (Microsoft Office Communications Server)

1.2 Doelgroep en leeswijzer

Dit is een document met veel technische diepgang. De doelgroep bestaat uit de systeembeheerders en architecten van instellingen die een rol spelen in de besluitvorming rond, of implementatie van Unified Communications. Het document veronderstelt parate kennis van internettechnologieën als DMZ, DNS en PKI.

De terminologie die gehanteerd wordt, is ontleend aan 'Unified Communications implementeren' v.0.1 (15-03-2010). Hierin staan afkortingen en begrippen omschreven zoals een scherpe formulering van het begrip 'Unified Communications', en het kader voor federatie.

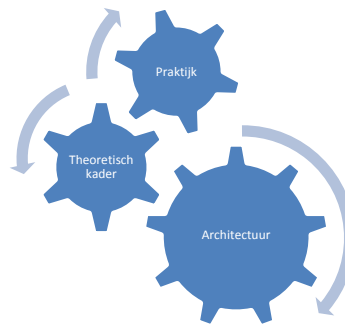
De architectuur rust op een aantal pijlers die per stuk uitgewerkt worden.

1.3 Aanpak

De uitkomst van dit onderzoek is een architectuur voor federatie van Unified Communications. NiVo Network Architects hecht grote waarde aan de haalbaarheid en realisme van een architectuur. Daarom is de theorie, weergegeven in de standaardisatie, getoetst aan de praktijk. Eerst is een globaal technisch kader opgesteld aan de hand van de standaardisatiedocumenten. De vijf meest in het oog springende producten zijn uitgetest in een test bed. De betrokken leveranciers waren:

- Microsoft Office Communications Server
- IBM LotusLive
- Zimbra (beschikbaar gesteld door Igi)
- Cisco Webex
- Google Talk

Gedurende het test traject heeft het theoretische kader een aantal iteratieslagen ondergaan onder invloed van de praktische bevindingen.



Het resultaat is een ambitieus einddoel met een pragmatisch pad daar naar toe.

1.4 Referenties

De volgende bronnen zijn geraadpleegd:

1. ['Unified Communications in het Hoger Onderwijs en Onderzoek'](#) – NiVo Network Architects 2009
2. 'Unified Communications implementeren' v.0.1 (15-03-2010)
3. [VoIP haalbaarheidsstudie](#) - TNO 2006
4. IETF standaarden (de specifieke RFC's staan in de relevante passages vermeld)
5. Interviews met stakeholders SURFnet
6. Openbare informatie van en navraag bij leveranciers
7. Rapport 'Collaboration Infrastructure' – SURFnet 2009
8. Handboek Unified Communications SURFnet – Altran, versie 1.0, januari 2010

2 Federatieve Unified Communications architectuur op basis van XMPP

Het doel van dit onderzoek is om een realistische *blauwdruk* te geven voor een federatieve Unified Communications infrastructuur. Dit hoofdstuk behandelt de uitgangspunten en functionele werking van de architectuur.

Dit hoofdstuk ontleent zijn aanpak aan zogenaamde 'good practice' documenten die binnen de IETF gangbaar zijn, en is daarmee in lijn met de structuur en inhoud die vanuit standaardisatieorganen zijn gedaan omtrent dit onderwerp.

Voor lezers die geen technische toelichting op de onderwerpen behoeven, volstaat de tabel met vereisten in paragraaf 3.

Het startpunt is de standaardisatie en vervolgens worden de technische componenten van de architectuur uitgediept. De architectuur die hieruit volgt, wordt aangeduid met 'versie 1.0'.

Elk technisch element van de architectuur staat beschreven in een aparte paragraaf, die begint met een onderbouwing van de architectuurkeuze en/of uitleg van het betreffende technisch element. Op die manier staat op eenduidige wijze vast om welk technisch aspect het gaat en waarom het op de aanbevolen wijze geïmplementeerd dient te worden. De aanbevelingen vallen in één van de vier categorieën van de MoSCoW-methode, die in IETF documentatie gebruikt wordt, waarbij de afkorting staat voor:

M	MUST	Dit element MOET op de beschreven wijze geïmplementeerd worden.
S	SHOULD	Dit element ZOU op de beschreven wijze geïmplementeerd MOETEN worden. Daarvan mag slechts worden afgeweken indien er geen reële mogelijkheid is om het element te realiseren zoals voorgeschreven
C	COULD	Dit element ZOU op de beschreven wijze geïmplementeerd KUNNEN worden, en is een suggestie of vrijblijvende aanbeveling
W	WILL NOT	Dit element ZAL NIET op de beschreven wijze geïmplementeerd worden.

Om de terminologie gelijk te houden met de voertaal van de IETF, worden de Engelstalige bewoordingen gebruikt.

2.1 *Uitgangspunten voor de architectuur*

De federatieve architectuur is opgesteld op basis van de uitgangspunten:

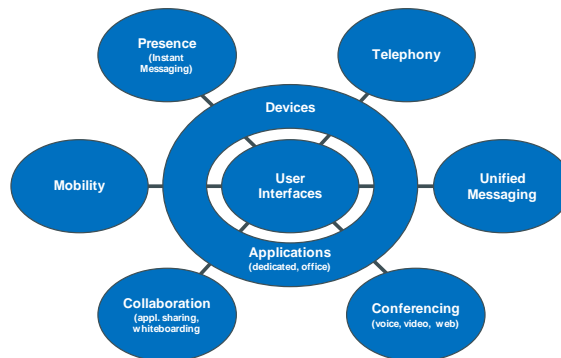
1. een goede uitwisselbaarheid van functionaliteit,
2. eenvoudige onderlinge vindbaarheid,
3. schaalbaarheid van de federatie
4. openheid voor domeinen buiten de federatie
5. verificatie van de gebruikers en
6. beveiliging van de verbindingen.

Elk element van de architectuur is getoetst aan deze uitgangspunten.

2.2 *Functionaliteit: functionele beschrijving van federatieve IM&P*

Samenwerken over de grenzen van instellingen gebeurt door individuele gebruikers. Deze paragraaf beschrijft de technische stappen die bewerkstelligen dat twee medewerkers van verschillende instellingen met elkaar kunnen communiceren. Beiden bevinden zich binnen binnen de context van hun respectievelijke UC omgevingen, elk als volgt generiek weergegeven in 'Unified Communications Implementeren':

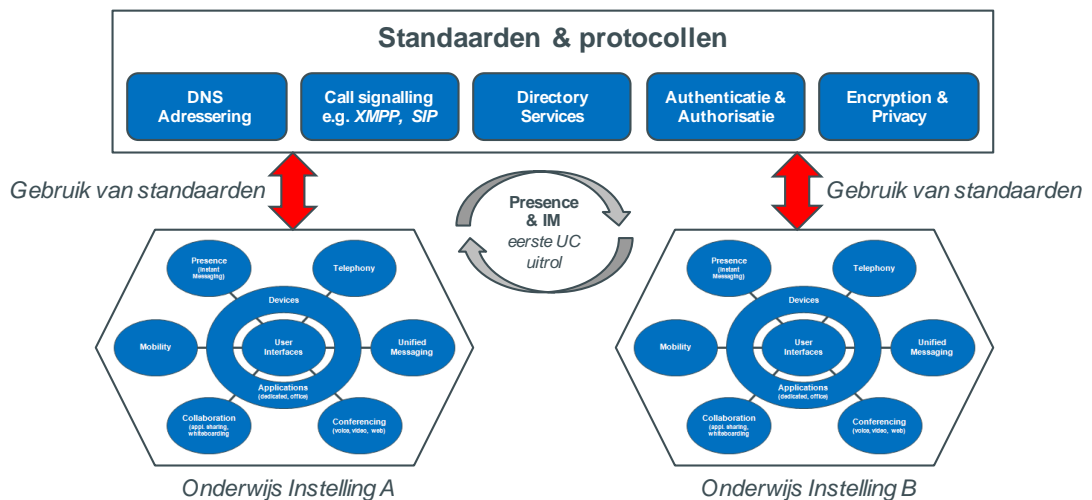
UC Losse Componenten



Het vervolg van dit hoofdstuk concentreert zich op:

- Instant Messaging & Presence
- Op basis van XMPP
- Uitsluitend het federatieve deel van de communicatie
- Organische federatie (dus geen hiërarchie)

Het kader voor de *federatieve* architectuur is als volgt generiek weergegeven in 'Unified Communications Implementeren':



2.3 Topologie en message flow

Voor deze *federatieve* architectuur is het niet van belang welk UC platform verschillende instellingen kiezen, zolang ze

- Gelijkvormige feature sets hebben
- Zich voor wat betreft instellingsoverschrijdende communicatie houden aan de vereisten in dit document

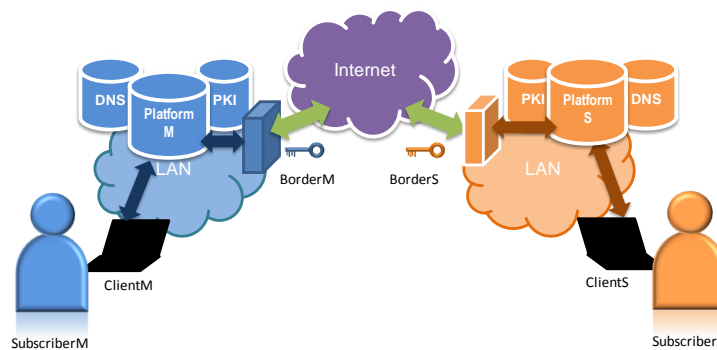
2.3.1 Topologie

Een medewerker van instelling 'M' noemen we 'SubscriberM'. SubscriberM gebruikt software op zijn pc of smartphone ('ClientM') die de online status laat zien van collega's. ClientM staat in verbinding met het platform van instelling 'M', dat dus het thuisplatform van SubscriberM is.

SubscriberM kan zich overigens binnen het instellingsnetwerk (LAN) bevinden, of via een VPN verbinding toegang tot PlatformM hebben verkregen.

PlatformM handelt de communicatie af voor iedereen in het domein 'domainM.edu', want subscriber M is bereikbaar via zijn adres SubscriberM@DomainM.edu. Hij wil communicatie opzetten met SubscriberS die bereikbaar is onder het adres SubscriberS@DomainS.edu. Deze SubscriberS gebruikt ook software ('ClientS') waarmee hij is ingelogd op het Unified Communications platform ('ServerS') dat alle verkeer afhandelt voor het domein DomeinS.edu.

De componenten die betrokken zijn in dit scenario, staan in onderlinge samenhang in het volgende schema:



In de figuur staan ook de DNS en PKI infrastructuur getekend, die in de technische uitwerking verderop van belang zijn. De groene pijlen laten zien wat het koppelvlak is van het platform van de instelling met de buitenwereld. In dit schematisch overzicht is het UC platform van de instellingen niet uitgesplitst in afzonderlijke functionele componenten en redundante componenten. Leveranciers hanteren verschillende architecturen met andere nomenclatuur waardoor het complete platform lastig generiek weer te geven is. Voor de eenvoud is het platform in de vorm van één server geschetst. Er is altijd sprake van minstens één *core* server die het hart van het UC platform vormt.

Wel is het goed om zich te realiseren dat het koppelvlak met de buitenwereld meestal geïmplementeerd wordt door een grenselement dat als veiligheidsbuffer dient tussen de kern van het platform en de buitenwereld. Deze component bevindt zich in de DMZ van het instellingsnetwerk en wordt vaak 'border controller', 'gateway' of 'edge' genoemd. Net als een web proxy, bundelt deze component het verkeer van en naar de buitenwereld en is het eerste aanspreekpunt voor communicatie van buitenaf.

De sleutels bij de verbindingspijlen symboliseren het feit dat de verbindingen bij voorkeur versleuteld worden door middel van encryptietechnologie in samenhang met PKI.

2.3.2 Koppelvlak

Voor een veilig en gecontroleerd koppelvlak tussen de *core* van het instellingsplatform en de buitenwereld heeft elke UC-productlijn een proxy-component die vaak *edge*, *border controller* of *gateway* heet, vergelijkbaar met de rol van een webproxy voor web servers. Het is 'common practice' om deze in te zetten, al ondersteunen sommige producten ook een rechtstreekse verbinding via een 'gat' in de firewall. Omdat de proxy-component in de DMZ staat, zal de impact van een inbreuk beperkt blijven tot deze component en geen invloed hebben op de kern van het platform. Tevens is het mogelijk om het netwerkverkeer te concentreren, dimensioneren en controleren. Wanneer in een later stadium real-time media als audio en video ingezet worden, zullen die in eerste instantie via een zo rechtstreeks mogelijk pad tussen de clients willen stromen. Een grenselement zorgt ervoor dat die media alleen op dat punt het instellingsnetwerk in- of uit mag. SURFnet en haar klanten hebben hier inmiddels steeds meer ervaring in binnen de [SURFcontact](#) dienst. Het grenselement dient geoptimaliseerd te zijn



voor real-time performance. Op dit moment houdt dat in dat het (nog) niet gevirtualiseerd wordt.

SHOULD:

Instellingen brengen een buffer aan tussen het SURFnet netwerk en de core van hun instellingsplatform in de vorm van een grenselement in de DMZ.

SHOULD:

Het grenselement is geoptimaliseerd voor real-time performance en is derhalve niet gevirtualiseerd uitgevoerd.

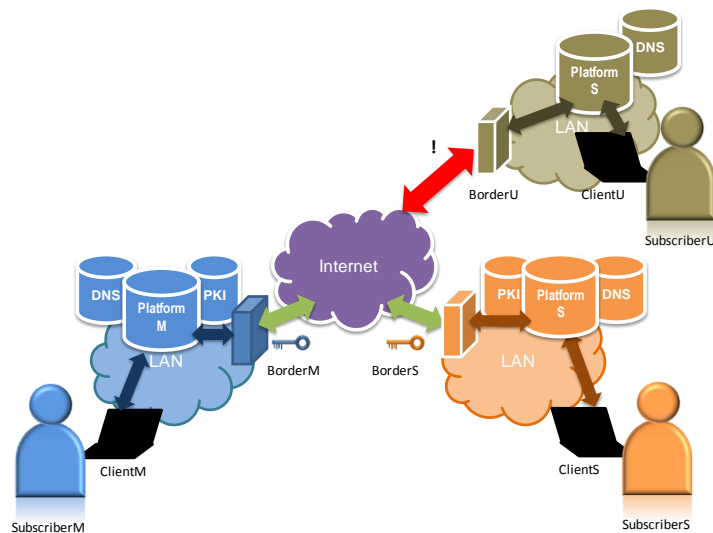
2.3.3 Hybride koppelvlak

Encryptie is een optioneel element in de XMPP standaard. SURFnet moet instellingen dringend aanbevelen om wel encryptie te gebruiken.

Aangezien in het test bed bleek dat encryptie niet gebruikt wordt in de meeste XMPP-gebaseerde diensten, is het voor instellingen praktisch als de koppeling met de buitenwereld ook communicatie met niet versleutelde domeinen ondersteunt. In het begin zal de UC federatie dat om praktische redenen moeten doen. Dat betekent dat het federatieve XMPP koppelvlak hybride moet zijn: het moet zowel versleutelde als niet versleutelde verbindingen ondersteunen.

Een nadeel van een hybride koppelvlak is dat de eindgebruiker geen onderscheid kan maken tussen geverifieerde en niet-geverifieerde contactpersonen en tussen beveiligde verbindingen en niet beveiligde verbindingen. De XMPP standaard verplicht de bouwers van servers om in de logging van de server weer te geven welke verbindingen versleuteld waren en welke niet. Dat geeft enige houvast wanneer de oorsprong van misbruik of SPIM achterhaald moet worden.

Hieronder is een situatie weergegeven waarin binnen de UC federatie versleuteld contact is tussen domain 'M' en 'S', en niet versleuteld contact tussen 'M' en 'U'.



2.3.4 Message flow

Wanneer de twee gebruikers in het scenario contact met elkaar leggen, worden de volgende stappen doorlopen:

- 1 SubscriberM logt in op ServerM, en SubscriberS

- 2 (optioneel): door middel van ENUM bepaalt SubscriberM wat de technologie is die door SubscriberS gebruikt wordt. Deze UC federatiearchitectuur heeft XMPP als uitgangspunt, dus deze stap kan overgeslagen worden. ENUM bewijst vooral zijn nut als slechts het telefoonnummer van SubscriberS bekend is. ServerM kan in DNS het ENUM record van het telefoonnummer opzoeken, en vertalen naar een XMPP of SIP adres.
- 3 ServerM zoekt in DNS op wat het adres is van (het koppelvlak van) ServerS. Met DNS wordt het domein in het adres van SubscriberS vertaald naar een IP adres.
- 4 ServerM legt contact met ServerS via het SURFnet netwerk door middel van het XMPP protocol. ServerS kijkt of ServerM in een whitelist of blacklist voorkomt. Dan wordt de versleuteling uitonderhandeld, waarna berichten kunnen worden uitgewisseld
- 5 Afhankelijk van het type bericht attendeert ServerS SubscriberS, bijvoorbeeld door aan te geven dat SubscriberM een abonnement (*subscription*) op dienst presence informatie wil, of dat er een binnenkomend bericht is
- 6 Voor de volledigheid, maar buiten de scope van deze architectuur: als één van de gebruikers rijkere media zoals audio en video wil bijschakelen, verstuurt zijn client de uitnodiging hiervoor via zijn eigen server naar de server van de andere, en zo komt het bij de andere gebruiker aan. Na acceptatie van de uitnodiging wisselen de clients (via de servers) informatie uit over het type media (codec, resolutie, bitrate etcetera) waarna de media gaan stromen tussen beide clients.

De onderliggende techniek van al deze stappen komt aan bod in de paragrafen hierna.

2.4 Signalering

De basis voor de communicatie in de UC federatie en met domeinen daarbuiten is de XMPP standaard. Overigens beveelt NiVo Network Architects in het voorgaande onderzoek aan om zeker ook SIMPLE te ondersteunen. Dit document concentreert zich op XMPP omdat dat een grotere adaptatie kent van bedrijven die het nauwkeurig implementeren.

Beide standaarden zijn geabstraheerd door de IETF, omdat de IETF geen van beiden wilde verheffen tot 'de' standaard, ten koste van de andere. Deze generalisatie is samengevat in zogenaamde 'Common Profiles':

Common Profile for Presence (CPP), RFC 3859, J. Peterson, IETF, August 2004,
<http://tools.ietf.org/html/rfc3859>

Common Profile for Instant Messaging (CPIM), RFC3860, J. Peterson, IETF, August 2004,
<http://tools.ietf.org/html/rfc3860>

Beide delen de manier waarop domeinservers elkaar vinden via DNS:
Address Resolution for Instant Messaging and Presence, RFC 3861, Peterson, J., IETF,
August 2004, <http://tools.ietf.org/html/rfc3861>

Bovendien delen ze het dataformaat waarin presence wordt uitgewisseld:
Presence Information Data Format (PIDF), RFC3863, Sugano, H., Fujimoto, S., Klyne, G.,
Bateman, A., Carr, W., J. Peterson, IETF, August 2004, <http://tools.ietf.org/html/rfc3863>

De kern van de XMPP standaard (Core) is omschreven in:
<http://www.ietf.org/rfc/rfc3920.txt>

De opzet van de architectuur in dit hoofdstuk heeft het Common Profile als uitgangspunt. Voor SIMPLE is een specifieke draft opgesteld die beschrijft hoe inter-domain (dus federatieve) communicatie plaats moet vinden, die de uitgangspunten van de federatieve UC architectuur grotendeels invult. Dit is een uitstekend voorbeeld van een good practice.
<http://tools.ietf.org/html/draft-aoki-simple-interdomain-bcp-02.txt>

MUST:

Instellingen implementeren XMPP als protocol voor uitwisseling van IM&P met andere domeinen in de federatieve SURFnet UC architectuur.

Om de invulling van deze voorwaarde eenduidig te definiëren, gaan de volgende paragrafen in op details die in de standaardisatie keuzevrijheid bieden.

COULD:

Naast XMPP kan de instelling andere protocollen gebruiken voor uitwisseling van IM&P met de buitenwereld.

2.4.1 Native XMPP versus conversie

De koppeling tussen de instelling en de federatie kan op verschillende wijzen gerealiseerd worden. Een meerderheid van de UC platformen van leveranciers gebruikt 'native' XMPP, ofwel XMPP in de kern van het systeem. Veel echter niet. In het vooronderzoek zijn drie manieren omschreven om ook XMPP te ondersteunen als de kern van het systeem op een andere technologie gebaseerd is.

1. Adapters of plugins op het platform: aan de serverzijde kan door middel van softwaremodules een relatie gelegd worden met andere producten of diensten. Steeds meer leveranciers ondersteunen dit model, voor steeds meer verschillende producten en diensten.
2. Gateways: zelfstandige elementen (mogelijkerwijs van derden zoals van NextPlane) die koppelingen en conversie verzorgen
3. De client is 'multistack', ofwel ondersteunt meerdere protocollen. Voorbeelden hiervan zijn Gizmo en Nimbuzz. Bijbehorend nadeel is, dat het afhangt van de software client welke platformfuncties voor de gebruiker bereikbaar zijn. Een client die uitgeleverd wordt met een serverplatform, zal de volledige functionaliteit van dat platform ondersteunen.

In de markt zijn alle drie de opties verkrijgbaar. Drie van de producten in het test bed zijn opgebouwd rondom XMPP, de twee andere implementeren XMPP als adapter.

MUST:

Instellingen ondersteunen de XMPP standaard als koppelvlak met de UC federatie door middel van een adapter of plugin in hun platform of een gateway die gekoppeld is aan hun platform.

2.5 Adressering

Gebruikers vinden elkaar op basis van een URI die gelijk is aan het e-mailadres, dus in de vorm Subscribers@DomainS.edu. Dit wordt ook de JabberID of JID genoemd.

MUST:

Elke instelling kent JID's toe aan haar gebruikers die gelijk zijn aan het e-mailadres.

2.6 Middleware

2.6.1 DNS

De essentie van de organische vorm van federatie waarop deze architectuur is gebaseerd, is het feit dat domeinen elkaar kunnen vinden via DNS. In DNS zorgen SRV records voor de juiste verwijzing naar de server(s) of grenselementen die UC voor het domein afhandelen. Voor 'backward compatibility' worden de oude jabber records aanbevolen.

MUST:

Elke instelling implementeert de volgende DNS records:

Entry	TTL	Type	Prio	Port	Address
_xmpp-server._tcp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.
_xmpp-client._tcp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.

COULD:

Elke instelling implementeert optioneel de volgende DNS records:

_jabber._tcp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.
_xmpp-server._udp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.
_xmpp-client._udp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.
_jabber._udp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.
_jabber-client._tcp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.
_jabber-client._udp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.

COULD:

Zodra een instelling een redundant koppelvlak heeft (zie 2.12.1), moet per grenselement een DNS SRV record worden gemaakt waarvan de prioriteit is ingesteld.

(tip: records kunnen gecheckt worden met, naast de gebruikelijke tools als *dig*, de URL: http://dopeman.org/xmpp_srv_test/)

2.7 Authenticatie en Autorisatie

2.7.1 Gebruikers

Op federatief nivo vindt geen gebruikersauthenticatie en autorisatie plaats en is dus niet van toepassing

2.7.2 Domeinen

Het enige mechanisme dat op dit moment realistisch is om domeinen expliciet te autoriseren (vertrouwen) of uit te sluiten zijn zogenaamde white lists en black lists. Er zijn nog geen mechanismen om deze automatisch uit te wisselen. SURFnet kan een rol spelen in het uitwisselen ervan.

Op den duur zullen SAML-achtige verificatievormen door XMPP (en SIMPLE) gebruikt kunnen gaan worden, die eventueel gebruik kunnen maken van de SURFFederatie-dienst om de identiteit van gebruikers te verifiëren.

COULD:

Instellingen kunnen SURFnet op de hoogte stellen van (vermoedde) malefide UC-domeinen.

COULD:

Door SURFnet aangereikte white lists en black lists van domeinen hanteren in het eigen UC platform.

2.8 IDM & Directory services

Gebruikersprofielen worden volledig decentraal beheerd, binnen de instellingen. Op federatief nivo is IDM derhalve niet relevant.

Directory services kunnen optioneel op federatief nivo geboden worden. Dat is echter een dienstverlening met een eigen architectuur, die op clientnivo interacteert met de UC federatie. Indien centrale directory services gewenst zijn, kan hiervoor een aparte functionele omschrijving en architectuur voor worden opgesteld.

2.9 Security

2.9.1 PKI

Wanneer elke instelling een goede identiteitverificatie tussen hun gebruikers en het thuisplatform realiseert, en binnen de federatie de verificatie van de UC platformen goed is ingericht, is in voldoende mate de identiteit van contactpersonen gegarandeerd (op *hop by hop* basis).

Datzelfde geldt voor de versleuteling van berichtenverkeer. Elke node in het pad (ClientM, ServerM, ServerS, ClientS) moet het verkeer versleutelen en ontsleutelen.

De XMPP RFC zegt dat encryptie optioneel is voor client-to-server communicatie. In deze federatie moet versleuteling zo snel mogelijk verplicht worden. Ook versleuteling van server-to-server communicatie is in de RFC optioneel.

In de praktijk stuit dat op compatibiliteitsproblemen. Daarom kan encryptie gefaseerd ingevoerd worden. De server mag daarom ook niet-versleutelde berichten verwerken. De standaard dwingt af dat hiervan melding wordt gemaakt in de logging. Bij voorkeur ziet de gebruiker dat de identiteit van de contactpersoon waarmee hij communiceert niet geverifieerd kan worden en dat de verbinding niet versleuteld is. Op dit moment bieden clients deze waarschuwing nog niet. SURFnet kan bij de betrokkenen in de standaardisatie actief de discussie voeren hoe dit in te voeren is.

SHOULD:

Instellingen gebruiken TLS versleuteling van de communicatie tussen clients en de *core* van het UC platform

SHOULD:

Instellingen gebruiken TLS versleuteling tussen de *core* van het UC platform en de federatieve UC architectuur.

SURFnet moet uitsluitend geven of de certificatservice van TERENA het juiste formaat certificaten kan bieden.

MUST:

Indien certificaten worden toegepast, moeten deze geïmplementeerd worden volgens <http://xmpp.org/rfcs/rfc3920.html> paragraaf 5.1

- RSA moet ondersteund worden
- Het CommonName veld moet de domeinnaam bevatten. Dat kan gevolgen hebben voor de naamgeving van de hostnaam van het kernplatform of het borderelement.
- Er moet een SubjectAlternativeName veld zijn dat de domeinnaam bevat
- Een additioneel SubjectAlternativeName kan alternatieve domeinnamen of subdomeinnamen bevatten, of een wildcard voor subdomeinen.

2.9.2 Preventie

Een aantal mechanismen is genoemd om veiligheidsrisico's te beperken. Geen oplossing is waterdicht. De zwakste schakel bepaalt het netto veiligheidsniveau.

Een account dat gereed is voor Unified Communications, en met name telefoniegebruik, is geld waard. Als dit account wordt misbruikt, kan op kosten van de gedupeerde gebruiker gebeld worden. Deze kosten zijn eenduidig traceerbaar tot bij de gebruiker, die zich van geen kwaad bewust is. Ook misbruik in de vorm van lastigvallen van gebruikers (SPIM) moet zoveel mogelijk traceerbaar zijn.

2.9.3 Risico's

De bekendste risico's op een rijtje:

- Onderschepping van het verkeer

- Stelen van identiteiten

2.9.3.1 Stelen van identiteiten

Deze vorm van misbruik heet in het Engels 'Identity theft' en komt er op neer dat een kwaadwillende de inloggegevens van gebruikers achterhaalt.

2.9.3.2 Onderschepping van het netwerkverkeer

Dit is mogelijk kan op een aantal manieren. De twee belangrijkste zijn:

- ARP poisoning
- DNS poisoning

De kwaadwillende fungeert als 'Man in the Middle' zonder dat de eindgebruikers in de gaten hebben dat hun verkeer wordt afgeluisterd. Om dit te voorkomen en andere mechanismen om de identiteit van een gebruiker te misbruiken is <http://www.xmpp.org/extensions/xep-0165.html> opgesteld: 'Best practice to discourage JID mimicing'. Het document is door IETF nog niet geratificeerd maar bevat uiterst nuttige tips voor het beperken van risico's.

SHOULD:

Instellingen volgen de best practice volgens XEP-0165 zoveel als mogelijk.

2.9.4 Menselijke factoren

Meestal is de zwakste schakel de gebruiker zelf, die zwakke wachtwoorden gebruikt, wachtwoorden niet geheim houdt of computervirussen een kans geeft die de pc af luisteren. SURFnet besteedt hier aandacht aan in haar campagne '[Cybersave yourself](#)'.



MUST:

Instellingen moeten hun gebruikers bewust maken van het feit dat ze op een veilige manier met hun inloggegevens om moeten gaan.

SHOULD:

Instellingen moeten beleid voeren op het gebied van het gebruik van sterke wachtwoorden die regelmatig veranderd worden.

2.10 Netwerk

2.10.1 Poorten

Volgens RFC3920, zal TCP poort 5269 gebruikt worden voor server-to-server communicatie. Detectie van het gebruik van TLS gebeurt door het (grenselement van) UC platform, niet op basis van een aparte TCP poort.

MUST:

Alle UC platformen luisteren op TCP poort 5269 naar XMPP communicatie

Van latere zorg is de veelheid aan poorten die bij real-time media benodigd zijn. De hoeveelheid poorten kan gereduceerd worden door gebruik te maken van een grenselement.

2.10.2 Firewalls

Binnen de federatieve UC architectuur is geen sprake van firewalls. Wel op de grensvlakken. Firewalls dienen zodanig ingericht te zijn dat het bovenstaand poortgebruik toegestaan wordt.

2.10.3 NAT

Op federatief nivo is NAT niet van toepassing.

2.10.4 Netwerkperformance

De architectuur concentreert zich op presence en Instant Messaging, beide synchrone communicatievormen met een semi-realtime karakter. In een latere fase ondersteunt de architectuur het transport van real-time media. Toch is het goed om al rekening te houden met de real-time performance van het netwerk en het platform: lage vertraging en geringe packet loss geven een betere real-time 'feel' voor de gebruikers. Later is ook voldoende bandbreedte van belang voor audio en video.

Zoals TNO reeds in 2006 concludeerde levert de architectuur van de SURFnet backbone de garantie dat [real-time verkeer met de hoogste kwaliteit wordt afgewikkeld](#). Het is zaak dat ook het instellingsnetwerk ingericht is met een goede real-time performance als uitgangspunt.

SHOULD:

Het instellingsnetwerk is zodanig gedimensioneerd dat in het pad tussen eindgebruikers in een UC-sessie en SURFnet sprake is van:

- Meer dan 2Mbps bidirectioneel
- Minder dan 1% packet loss
- Minder dan 5ms delay
- Minder dan 5ms jitter

2.11 Databeheer

In de organische opzet van federatieve UC is geen sprake van dataopslag in de federatie.

2.12 Robustheid

2.12.1 Dubbele uitvoering

Instellingen worden geacht hun core systeem en grens elementen dubbel uit te voeren. Door middel van L4 load balancing en DNS kan het verkeer verdeeld worden over de elementen en terugvallen naar werkende elementen als er één uitvalt. Het is aannemelijk dat het redundant uitvoeren van het grenselement aan de orde is als het externe verkeer toeneemt.

SHOULD:

Instellingen voeren de *core* van hun platform dubbel uit, verspreid over twee geografisch gescheiden locaties

SHOULD:

Instellingen voeren het grenselement van hun platform dubbel uit, verspreid over twee geografisch gescheiden locaties en met inachtneming van dubbele DNS records (zie 2.6)

Op federatief nivo biedt het gebruik van DNS in combinatie met dubbel uitgevoerde koppelvlakken een hoge mate van robuustheid. Het tussenliggende netwerk –SURFnet- biedt met haar gezonde dimensioneringsbeleid voldoende schalingsmogelijkheden. De behoeftes voor een robuuste federatie van UC platformen zal dus vooral afhangen van de robuustheid van de instellingsplatformen (buiten de scope van dit document).

2.13 Beheer

Uiteraard moet het beheer met de hoogste mate van beveiliging worden uitgevoerd.

MUST:

Het beheer van het UC platform dient zodanig ingericht zijn dat

- toegang tot de systemen voor buitenstaanders verregaand afgeschermd wordt, door bijvoorbeeld meertraps toegang van systemen (dus via andere systemen)
- niet méér beheerders toegang hebben dan strikt noodzakelijk, en uitsluitend vanaf relevante lokaties
- beheerders niet méér instellingen in het platform kunnen beïnvloeden dan waartoe zij gerechtigd zijn
- alle configuratieveranderingen traceerbaar zijn tot op beheerdersniveau, wat bekend staat onder de term 'auditing'
- het risico van identity theft van een beheerder maximaal gereduceerd wordt, door bijvoorbeeld gebruik te maken van sterke authenticatievormen, bij voorkeur meerdere.

Dit document kan onmogelijk een sluitend beveiligingsadvies te geven. Beveiliging is een cruciaal element van een gezonde federatie en dus moet elke instelling de hoogste mate van beveiliging in acht nemen bij de implementatie van UC, en ontsluiten van de federatieve mogelijkheden van UC.

3 Samenvatting

Alle elementen van de architectuur staan in onderstaande tabel, met de vermelding in welke categorie ze vallen van de MoSCoW methodiek.

1.1	Instellingen brengen een buffer aan tussen het SURFnet netwerk en de core van hun instellingsplatform in de vorm van een grenselement in de DMZ.	S																																				
1.2	Het grenselement is geoptimaliseerd voor real-time performance en is derhalve niet gevirtualiseerd uitgevoerd	S																																				
2.1	Instellingen implementeren XMPP als protocol voor uitwisseling van IM&P met andere domeinen in de federatieve SURFnet UC architectuur.	M																																				
2.2	Naast XMPP kan de instelling andere protocollen gebruiken voor uitwisseling van IM&P met de buitenwereld.	C																																				
2.3	Instellingen ondersteunen de XMPP standaard als koppelvlak met de UC federatie door middel van een adapter of plugin in hun platform of een gateway die gekoppeld is aan hun platform.	M																																				
3.1	Elke instelling kent JID's toe aan haar gebruikers die gelijk zijn aan het e-mailadres.	M																																				
3.2	Elke instelling implementeert de volgende DNS records:	M																																				
<table border="1"> <thead> <tr> <th>Entry</th> <th>TTL</th> <th>Type</th> <th>Prio</th> <th>Port</th> <th>Address</th> </tr> </thead> <tbody> <tr> <td>_xmpp-server._tcp</td> <td>3600</td> <td>IN SRV</td> <td>10 0</td> <td>5269</td> <td>ServerS.DomainS.edu.</td> </tr> <tr> <td>_xmpp-client._tcp</td> <td>3600</td> <td>IN SRV</td> <td>10 0</td> <td>5222</td> <td>ServerS.DomainS.edu.</td> </tr> </tbody> </table>			Entry	TTL	Type	Prio	Port	Address	_xmpp-server._tcp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.	_xmpp-client._tcp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.																		
Entry	TTL	Type	Prio	Port	Address																																	
_xmpp-server._tcp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.																																	
_xmpp-client._tcp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.																																	
3.3	Elke instelling implementeert optioneel de volgende DNS records:	C																																				
<table border="1"> <tbody> <tr> <td>_jabber._tcp</td> <td>3600</td> <td>IN SRV</td> <td>10 0</td> <td>5269</td> <td>ServerS.DomainS.edu.</td> </tr> <tr> <td>_xmpp-server._udp</td> <td>3600</td> <td>IN SRV</td> <td>10 0</td> <td>5269</td> <td>ServerS.DomainS.edu.</td> </tr> <tr> <td>_xmpp-client._udp</td> <td>3600</td> <td>IN SRV</td> <td>10 0</td> <td>5222</td> <td>ServerS.DomainS.edu.</td> </tr> <tr> <td>_jabber._udp</td> <td>3600</td> <td>IN SRV</td> <td>10 0</td> <td>5269</td> <td>ServerS.DomainS.edu.</td> </tr> <tr> <td>_jabber-client._tcp</td> <td>3600</td> <td>IN SRV</td> <td>10 0</td> <td>5222</td> <td>ServerS.DomainS.edu.</td> </tr> <tr> <td>_jabber-client._udp</td> <td>3600</td> <td>IN SRV</td> <td>10 0</td> <td>5222</td> <td>ServerS.DomainS.edu.</td> </tr> </tbody> </table>			_jabber._tcp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.	_xmpp-server._udp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.	_xmpp-client._udp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.	_jabber._udp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.	_jabber-client._tcp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.	_jabber-client._udp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.
_jabber._tcp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.																																	
_xmpp-server._udp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.																																	
_xmpp-client._udp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.																																	
_jabber._udp	3600	IN SRV	10 0	5269	ServerS.DomainS.edu.																																	
_jabber-client._tcp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.																																	
_jabber-client._udp	3600	IN SRV	10 0	5222	ServerS.DomainS.edu.																																	
3.3	Zodra een instelling een redundant koppelvlak heeft, moet per grenselement een DNS SRV record worden gemaakt waarvan de prioriteit is ingesteld.	M																																				
4.1	Instellingen kunnen SURFnet op de hoogte stellen van (vermoedde) malefide UC-domeinen.	C																																				
4.2	Door SURFnet aangereikte white lists en black lists van domeinen hanteren in het eigen UC platform.	C																																				
5.1	Instellingen gebruiken TLS versleuteling van de communicatie tussen clients en de core van het UC platform	S																																				
5.2	Instellingen gebruiken TLS versleuteling tussen de core van het UC platform en de federatieve UC architectuur.	S																																				
5.3	Indien certificaten worden toegepast, moeten deze geïmplementeerd worden volgens http://xmpp.org/rfcs/rfc3920.html paragraaf 5.1 <ul style="list-style-type: none"> - RSA moet ondersteund worden - Het CommonName veld moet de domeinnaam bevatten. Dat kan gevolgen hebben voor de naamgeving van de hostnaam van het kernplatform of het borderelement. - Er moet een SubjectAlternativeName veld zijn dat de domeinnaam bevat - Een additioneel SubjectAlternativeName kan alternatieve domeinnamen of subdomeinnamen bevatten, of een wildcard voor subdomeinen. 	M																																				
6.1	Instellingen volgen de best practice volgens XEP-0165 zoveel als mogelijk	S																																				

6.2	Instellingen moeten hun gebruikers bewust maken van het feit dat ze op een veilige manier met hun inloggegevens om moeten gaan.	M
6.3	Instellingen moeten beleid voeren op het gebied van het gebruik van sterke wachtwoorden die regelmatig veranderd worden.	S
7.1	Alle (grenselementen van) instellings-UC platformen luisteren op TCP poort 5269 naar XMPP communicatie	M
7.2	Het instellingsnetwerk is zodanig gedimensioneerd dat in het pad tussen eindgebruikers in een UC-sessie en SURFnet sprake is van: <ul style="list-style-type: none"> - Meer dan 2Mbps bidirectioneel - Minder dan 1% packet loss - Minder dan 5ms delay - Minder dan 5ms jitter 	S
8.1	Instellingen voeren de <i>core</i> van hun platform dubbel uit, verspreid over twee geografisch gescheiden locaties	S
8.2	Instellingen voeren het grenselement van hun platform dubbel uit, verspreid over twee geografisch gescheiden locaties en met inachtneming van dubbele DNS records (zie 2.6)	S
9.1	Het beheer van het UC platform dient zodanig ingericht zijn dat <ul style="list-style-type: none"> - toegang tot de systemen voor buitenstaanders verregaand afgeschermd wordt, door bijvoorbeeld meertraps toegang van systemen (dus via andere systemen) - niet méér beheerders toegang hebben dan strikt noodzakelijk, en uitsluitend vanaf relevante lokaties - beheerders niet méér instellingen in het platform kunnen beïnvloeden dan waartoe zij gerechtigd zijn - alle configuratieveranderingen traceerbaar zijn tot op beheerdersnivo, wat bekend staat onder de term 'auditing' - het risico van identity theft van een beheerder maximaal gereduceerd wordt, door bijvoorbeeld gebruik te maken van sterke authenticatievormen, bij voorkeur meerdere. 	M

4 Conclusies en aanbevelingen

Instellingen die grensoverschrijdende communicatie willen faciliteren voor studenten en medewerkers hebben groeiende keus in producten. Dit rapport geeft vorm aan de technische invulling van deze inter-domein communicatie.

De architectuur die dit document beschrijft, vult de gestelde randvoorwaarden in van schaalbaarheid en beveiliging. Alle technische aspecten zijn stap voor stap beschreven, van adressering, netwerkeigenschappen, encryptie en beveiliging tot de omschrijving van functionele pakketten (capability sets) op basis van standaardisatiedocumenten en praktische invulling daar waar deze onduidelijk zijn of waar keuzes gemaakt moeten worden.

NiVo Network Architects beveelt SURFnet aan om:

- White- en blacklists van domeinen te onderhouden voor instellingen op de korte termijn
- De federatieve mogelijkheden van instellingen te verifiëren d.m.v. een certificering zoals ook binnen de SURFcontact dienst gebruikelijk is
- Instellingen te wijzen op de invulling van randvoorwaarden *binnen* de instelling om een veilige en schaalbare UC-federatie te realiseren
- Met instellingen te onderzoeken hoe de voorlopers reeds kunnen federeren op basis van de producten die reeds in gebruik zijn, los van het gebruik van XMPP
- Met instellingen en leveranciers te onderzoeken hoe een hogere mate van beveiliging kan worden gerealiseerd, door
 - o Gebruik van encryptie verplicht te stellen
 - o Het beveiligingsnivo van individuele contactpersonen van een gebruiker te tonen
- Te onderzoeken of de huidige certificatedienst voldoet voor gebruik binnen de XMPP federatie (reeds gestart)
- Meer producten te testen op het gebruik van XMPP, die relevant zijn voor het HO&O veld
- Te onderzoeken hoe de SURFFederatie-dienst identiteiten van gebruikers kan verifiëren binnen de UC-federatie op de lange termijn
- dit document consequent als referentie te gebruiken in onderlinge communicatie over technische aspecten van federatieve Instant Messaging & Presence
- er bij instellingen op aan te dringen in een vroeg stadium rekening houden met deze *good practices* in de besluitvorming, leverancierselectie en implementatie van Unified Communications
- op basis van voortschrijdende inzichten als gevolg van bovenstaande aanbevelingen, nieuwe opeenvolgende versies van de architectuur uitgewerkt worden

Het gebrek aan versleuteling vereist een handreiking aan instellingen en leveranciers die versleuteling nog niet of onvoldoende ondersteunen. De standaard laat hiervoor ruimte, met als gevolg dat de implementatie ervan achterloopt. Om de voortgang van de UC federatie niet in gevaar te laten komen, is versleuteling uitgesteld tot een volgende versie van de architectuur.

De praktijk toont aan dat het adviesrapport '[Unified Communications in het Hoger Onderwijs en Onderzoek](#)' een goede functionele basis vormt voor federatie van Unified Communications. Enkele knelpunten zijn geïdentificeerd en oplossingen voorgesteld, waarmee instellingen op korte termijn reeds aan de slag kunnen. Naarmate de federatie groeit en de behoefte aan meer mogelijkheden ontstaat, biedt dit advies aanknopingspunten om op te schalen in functionaliteit en omvang.

Bijlage A: Praktische bevindingen bij het gebruik van XMPP voor federatieve IM&P

Om het theoretische kader voor federatieve IM&P te testen, is een beperkt aantal leveranciers gevraagd in een kortdurend test bed deel te nemen. Het test bed was niet bedoeld om een compleet beeld van de markt en de mogelijkheden te krijgen, maar om op een snelle en eenvoudige wijze inzicht te krijgen in de meest realistische wijze waarop XMPP op dit moment ingezet kan worden.

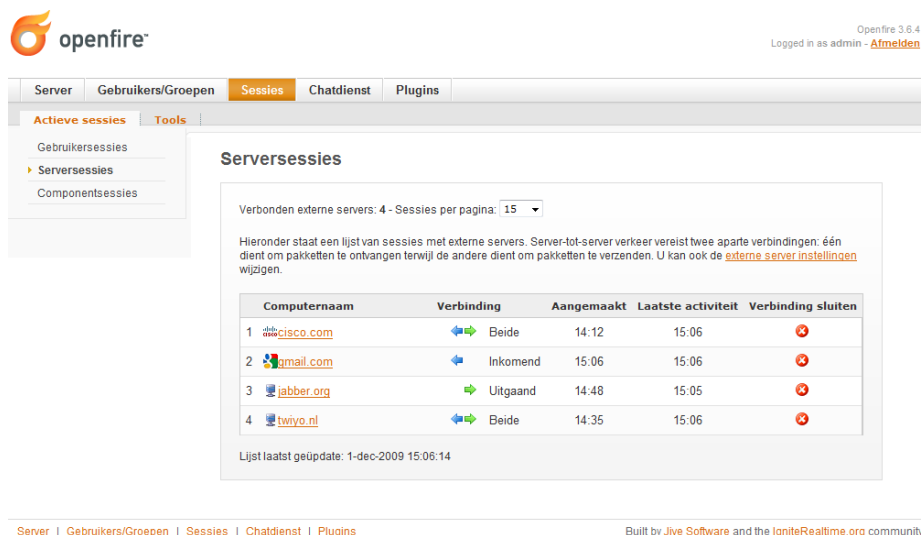
Dit hoofdstuk is een samenvatting van het test rapport, ter onderbouwing van de theorie en ontwerpkeuzes van de federatieve UC architectuur in het volgende hoofdstuk.

A.1. Eigen inbreng van leveranciers










Een vijftal leveranciers bood zelf, via internet, hun product of dienst aan om ze uit te testen. Deze aanpak heeft als voordeel dat geen kostbare tijd verloren ging met het opbouwen van alle individuele producten op één locatie, en dat ze aangeleverd werden zoals de leveranciers zelf dachten dat ze geconfigureerd dienden te zijn. Een mogelijk nadeel was, dat minder goed inzichtelijk kon worden gemaakt waar mogelijke verstoringen optreden. Dat probleem is ondervangen door het server-to-server verkeer te monitoren.

A.2. Referentieserver

Het zou teveel tijd vergen om elk product tegen elk product te testen. Leveranciers geven zelf in hun specificaties aan met welke andere producten hun product kan samenwerken, en het gaat binnen dit kader te ver om de details van deze interoperabiliteit te verifiëren. Daarom is gekozen voor een centraal opgestelde referentie testserver. Voor de volledigheid: deze heeft niet de rol van een centraal punt in een hiërarchie op zich genomen, maar gold als een voorbeeld van een XMPP implementatie waar leveranciers tegenaan konden testen. De server is uitgerust met OpenFire, een Open Source XMPP implementatie. Zowel OpenFire als Jabberd zijn open source servers die XMPP op een goede manier ondersteunen. Open Source biedt de mogelijkheid om problemen te onderzoeken door in de broncode van de server te kijken. OpenFire is gekozen omdat die snel beschikbaar was op Amazon Elastic Cloud. Daarnaast is Jabberd overgenomen door Cisco. Door voor OpenFire te kiezen is een potentiële discussie over de inbreng van een commerciële partij in het test bed voorkomen. Verder werkt een actieve community aan OpenFire met goede informatieuitwisseling.



The screenshot shows the OpenFire web interface. At the top left is the OpenFire logo. At the top right, it says "Openfire 3.6.4" and "Logged in as admin - Afmelden". Below the logo is a navigation menu with tabs: "Server", "Gebruikers/Groepen", "Sessies", "Chatdienst", and "Plugins". The "Sessies" tab is selected. Underneath, there are sub-tabs: "Actieve sessies" and "Tools". The "Actieve sessies" sub-tab is selected, and a sidebar menu shows "Gebruikerssessies", "Serversessies", and "Componentsessies". The main content area is titled "Serversessies" and contains a table of active sessions. Above the table, it says "Verbonden externe servers: 4 - Sessies per pagina: 15". Below the table, there is a paragraph of text explaining that the list shows sessions with external servers and that server-to-server traffic requires two separate connections. The table has five columns: "Computernaam", "Verbinding", "Aangemaakt", "Laatste activiteit", and "Verbinding sluiten".

Computernaam	Verbinding	Aangemaakt	Laatste activiteit	Verbinding sluiten
1  cisco.com	 Beide	14:12	15:06	
2  gmail.com	 Inkomend	15:06	15:06	
3  jabber.org	 Uitgaand	14:48	15:05	
4  twilio.nl	 Beide	14:35	15:06	

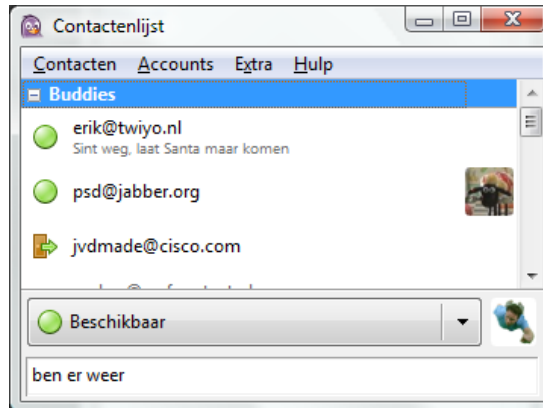
Lijst laatst geüpdate: 1-dec-2009 15:06:14

Server | Gebruikers/Groepen | Sessies | Chatdienst | Plugins

Built by [Jive Software](#) and the [IgniteRealtime.org](#) community

A.3. Client

De keuze voor de software voor de testgebruikers is ruimer. De keuze is gevallen op de open source client Pidgin vanwege de goede XMPP interoperabiliteit en analysemogelijkheden.



Een voordeel van een open source client is dat mogelijke problemen op het gebied van XMPP die het gevolg zijn van een verschillende interpretatie van de standaard, in de broncode van de software kunnen worden nagekeken.

A.4. Analysetools

Op de client computers (Windows Vista Ultimate 64bit, Windows 7 Ultimate 32bit, Windows XP Home Premium 32bit en Ubuntu 9.10 32bit) is Wireshark gebruikt om het netwerkverkeer te analyseren. Ook de logging van Pidgin is gebruikt om gegevens te achterhalen. Op de server toonde 'ngrep' het netwerkverkeer, en is de logging geanalyseerd die bijvoorbeeld aangaf welke actieve server-to-server connecties open stonden. Het test bed is in korte tijd opgezet en heeft inzet van enthousiaste leveranciers goede inzichten gegeven in het gebruik van XMPP als techniek om Unified Communications platformen in het Hoger Onderwijs en Onderzoeksveld met elkaar te laten samenwerken.

A.5. Conclusies en aanbevelingen van het test bed

- De XMPP standaard als communicatiemiddel tussen domeinen die Instant Messaging en Presence gebruiken, bewijst zichzelf als geschikt protocol in deze tests
- Drie producten bieden basisfunctionaliteit met goede samenwerking met OpenFire.
- Geavanceerdere functies zoals meer grafische tekstmogelijkheden en multipartychat werken nog niet optimaal onderling samen
- Sommige leveranciers bieden hun XMPP implementatie uitsluitend aan voor ontsluiting van geselecteerde producten zoals Google Talk, als terugvaloptie als het niet mogelijk is om het 'native' protocol te gebruiken van het product dat doorgaans 'rijkere' functionaliteit (zoals telefonie-integratie) biedt.
- Encryptie van server-to-serververbindingen is optioneel in de standaard. Deze optie wordt amper ondersteund, of afgedwongen, in de geteste producten.

A.6. Aanbevelingen

- Onderzoek hoe rijkere samenwerking mogelijk is door de kritieke massa die ontstaat van instellingen die Microsoft Office Communications gebruiken. Deze samenwerking is weliswaar op een Microsoft-specifieke implementatie van de SIP standaard gebaseerd, maar OCS kan ook al (beperkt) XMPP-verbindingen leggen. De deur naar een op open standaarden gebaseerde toekomst is daarmee niet dichtgeslagen. Het wordt een de-facto standaard, gezien het aantal leveranciers dat er compatibel mee

claimt te zijn en het massale gebruik ervan, en biedt vooralsnog meer functionaliteit dan XMPP.

- Test meer producten
- Stimuleer instellingen en leveranciers die aangeven op basis van XMPP te willen werken, door hun te faciliteren met soortgelijke interoperabiliteitstests tussen producten die voor hen van belang zijn. Daarvoor zou het huidige testbed steviger aangezet kunnen worden.
- Stimuleer het gebruik van encryptie bij leveranciers en instellingen door met ze in conclaaf te gaan over productontwikkelingen en ze te certificeren.

De architectuur voor federatieve Unified Communications is mede op basis van deze constatering uitgewerkt in hoofdstuk 2.

Bijlage B: Afkortingen en begrippen

AD	Active Directory	De gebruikersdatabase voor Microsoft-omgevingen op basis van LDAP
AMI	Amazon Machine Instance	Naam die Amazon geeft aan virtuele machines die draaien in haar Elastic Cloud dienst
API	Application Programming Interface	Een interface naar een systeem waarmee het systeem commando's kan ontvangen van andere systemen en gegevens kan teruggeven
ATA	Analog Telephony Adapter	Een omvormer van klassieke telefonie naar VoIP
CDR	Call Detail Record	Vastlegging van gespreksgegevens door een telefooncentrale
CRM	Customer Relationship Management	Systeem waarin contactgegevens en contactmomenten van klanten worden opgeslagen
DECT	Digital Enhanced Cordless	Standaard voor draadloze telefonie binnenshuis
DLO	Digitale Leeromgeving	Webgebaseerde omgeving waarin docenten en studenten educatieve content uitwisselen
DMZ	DeMilitarized Zone	Buffernetwerk tussen het kantoor netwerk en de buitenwereld voor beveiliging
DNS	Domain Name System	Opzoeksysteem dat internet domeinnamen (zoals www.google.nl) vertaalt in een IP-adres
ENUM	Electronic NUMbers	Techniek om via DNS een telefoonnummer te vertalen naar een VoIP- of videoconferencingadres
GSM	Global System for Mobile Communications	Standaard voor draadloze telefonie buitenshuis
HO&O	Hoger Onderwijs & Onderzoek	Doelgroep van SURFnet
HR	Human Resource	Afdeling die zich bezighoudt met personeelszaken
IM&P	Instant Messaging & Presence	Korte berichten sturen en elkaars online status zien zoals bij MSN en Skype
IP	Internet Protocol	Computertaal die binnen bedrijven en op het internet gebruikt wordt om systemen met elkaar te laten communiceren. Elk systeem heeft een IP-adres. Drager voor e-mail, webbrowsing en alle andere internetapplicaties
iPABX	IP-gebaseerde PABX	Bedrijfstelefooncentrale op basis van VoIP
ISDN2_ ISDN30	Integrated Services Digital Network	Digitale telefoonverbinding met het telefoonnetwerk met 2 of 30 kanalen
Jabber	Zie XMPP	Zie XMPP
JID	Jabber ID	Het Jabber ofwel XMPP adres van een persoon
LDAP	Lightweight Directory Access Protocol	Opslag van gebruikersgegevens zoals namen, accountnaam en wachtwoord
LinkedIn	n.v.t.	Website met profielen van personen die hun carrière weergeven en die zich aan elkaar kunnen verbinden aan de hand van

		gemeenschappelijke factoren als dezelfde (voormalige) werkgever
P(A)BX	Private (Automatic) Branch Exchange	Bedrijfstelefooncentrale
PKI	Public Key Infrastructure	Systeem van digitale certificaten die identiteiten van personen en websites op internet te verifiëren
Presence Roster		Software op PC of smartphone die een lijst met contactpersonen toont en hun 'presence' informatie (beschikbaarheidsinformatie) met symbolen en kleuren
S2C	Server to Client	Communicatie tussen client (de software van de gebruiker) en de server
S2S	Server to Server	Communicatie tussen servers onderling
SIP	Session Initiation Protocol	Standaard voor het opzetten van telefoon- en videogesprekken via internettechnologie
SMART	Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdgebonden	(Management) methodiek om doelen scherp te formuleren.
SMS	Short Message Service	Techniek om berichten tot 160 tekens te versturen naar en van mobiele GSM telefoons
SOAP	Simple Object Access Protocol	Commando's die systemen onderling kunnen uitwisselen via hun API, gebaseerd op de XML talengroep
SSO	Single Sign On	Het principe dat een gebruiker slechts 1x hoeft in te loggen op de PC en daarmee toegang heeft tot alle systemen waarvan hij gebruik mag maken.
TCO	Total Cost of Ownership	Accountantbegrip voor de totale kosten van een dienst of product
TLS	Transport Layer Security	Versleuteling van gegevens over een dataverbinding zodat ze niet ontcijferd kunnen worden indien onderschept
UC	Unified Communications	Combinatie van telefonie, videoconferencing en kantoorautomatisering die telecommunicatie eenvoudiger en rijker maakt
URI	Universal resource identifier	Adres van een systeem of een persoon, bijvoorbeeld e-mailadres
VoIP	Voice over IP	Transport van spraak (telefonie) via internet technologie
Wifi	Wireless Fidelity	Certificering voor draadloze datanetwerken voor de thuis- en professionele markt
XML	eXtensible Markup Language	Computertaal die systemen gebruiken om commando's en gegevens uit te wisselen.
XMPP	eXtensible Messaging & Presence Protocol	Protocol voor uitwisseling van presence informatie en instant messages, ook 'Jabber' genoemd.