

# IBM Sametime 8.5.x / 9.x im Umgang mit IBM Websphere



25. September 2013, Admincamp 2013

Alexander Novak, alexander.novak@edcom.de, Tel.: +49 89 38 40 850

edcom Software & Consulting GmbH, Baierbrunner Straße 39, 81379 München

[www.edcom.de](http://www.edcom.de)

# Agenda

- ▶ **IBM Lotus Sametime 8.5.x Komponenten und deren Zusammenspiel**
- ▶ **Sametime 8.5/9 Installation Best Practices**
- ▶ **Praktische Erfahrungen und Tipps**
  - ▶ Websphere Ports & Portmapping
  - ▶ SSO zwischen Domino & Websphere
  - ▶ Deaktivierung der SSL Verbindung zum Media System (Performance)
  - ▶ Debug Parameter

# IBM Sametime – *Komponenten*

- ST 8.5.x „**Websphere**“ System Console
- ST 8.5.x „**Domino**“ Community Server
- ST 8.5.x „**Websphere**“ Proxy Server (Web/native Clients)
- ST 8.5.x „**Websphere**“ Meeting Server
- ST 8.5.x „**Websphere**“ Advanced Server
- ST 8.5.x „**Websphere**“ Gateway Server
- ST 8.5.x Unified Telephony
- ST 8.5.x „**Websphere**“ Media Manager Server



- ST 8.5.2 TURN Server
- ST 8.5.2 „**Websphere**“ Bandwith Manager
- ST 8.5.2 „**Websphere**“ SIP Edge Proxy
- ST 9.x „**Websphere**“ Video Manager (Linux)
- ST 9.x Video MCU (Linux)



## ➤ Sametime 8.5.x System Console

- ▶ **Zentrale Verwaltungsstelle** für alle ST 8.5 Komponenten (DB2, LDAP)
- ▶ **Richtlinien** für Community, Meeting und Media Server

## ➤ Sametime 8.5.x Community Server

- ▶ **Instant Messaging** (MUX Technik für Lastenverteilung)
- ▶ „Classic“ Meeting (**NICHT MEHR mit Sametime 9**)
- ▶ **Audio/Video** Server für „Classic“ Meeting und ältere ST Clients

## ➤ Sametime 8.5.x Proxy Server (Web Clients)

- ▶ **Chat Client im Browser** (AJAX, Kein Java Download notwendig)
- ▶ **Mobiler** Chat Client für iPhone & Android
- ▶ Anpassbar (CSS), „light“ Client
- ▶ **Audio/Video** erst mit **Sametime 9**



## ➤ Sametime 8.5.x Meeting Server



- ▶ Neuer **Meeting Server** für Browser (AJAX, Kein Java Download notwendig)
- ▶ Meeting Server für ST „rich“ Client (Audio/Video)
- ▶ **MPEG** Aufzeichnung (nur im „rich“ client)
- ▶ Dauerhafte Meetings (**keine Ressource** mehr)

## ➤ Sametime 8.5.x Gateway Server



- ▶ Verbindet Sametime Clients mit **externen CHAT Communities**
- ▶ Öffentlich: Google (AOL frozen!!!), Lycos
- ▶ Privat: OCS (Lynx?), Jabber, Sametime

## ➤ Sametime 8.5.x Unified Telephony



- ▶ **Telefon Integration** für Chat Client oder Meetings (SIP, TCSPi)
- ▶ „click to call“ (SIP Backend Integration), Softphone
- ▶ Telephony Application Server (TAS), Telephony Control Server (TCS)
- ▶ **8.5.2: SUT „light“ Client**



## ➤ Sametime 8.5.x Media Server



- ▶ Verwaltet alle **Audio/Video Verbindungen** von ST „rich“ Clients
- ▶ SIP Proxy/Registrar, Conference Manager, Media Packet Switcher

## ➤ Sametime 8.5.2 TURN Server

- ▶ **Audio/Video** RELAY bei **“NAT“** Netzwerken (TCP/UDP 3478) oder dauerhaft
- ▶ **TURN**: Traversal Using Relay NAT 🌐
- ▶ **STUN**: Session Traversal Utilities for NAT 🌐
- ▶ **ICE**: Interactive Connectivity Establishment 🌐

## ➤ Sametime 8.5.2 Bandwith Manager

- ▶ **Audio/Video Bandbreitenkontrolle** und -überwachung

## ➤ Sametime 8.5.2 SIP Edge Proxy

- ▶ **SIP Vermittlung** über **“NAT“** Netzwerke (TCP 5080/TLS 5081)

# IBM Sametime – “EDGE” Komponenten



## › Community Mux

- › ST Connect „RELAY“

## › HTTP Reverse Proxy

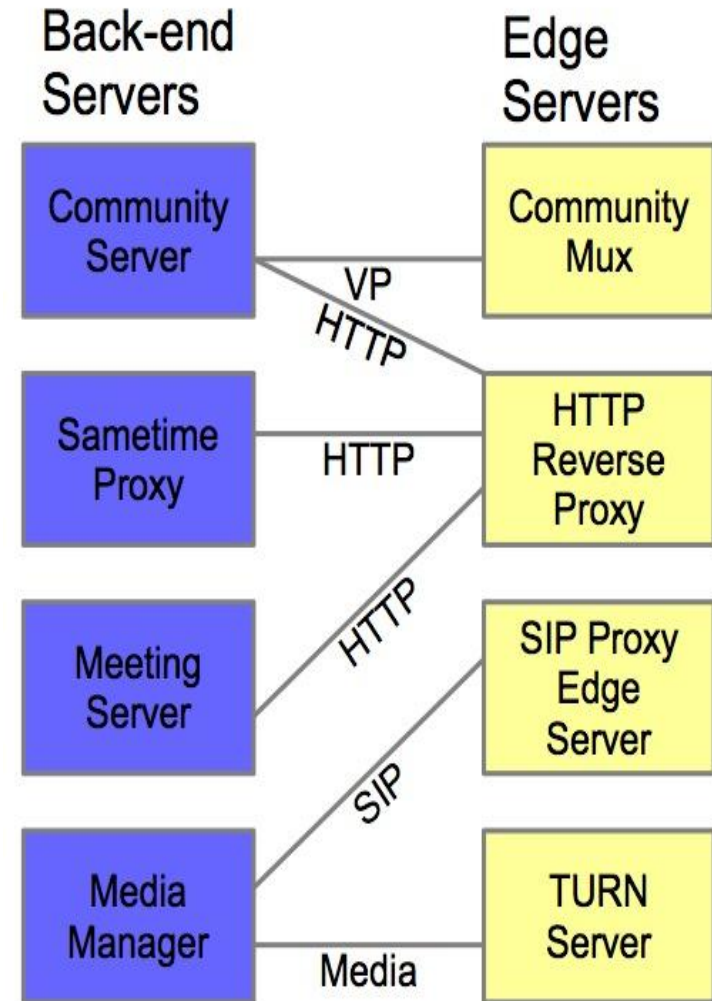
- › Für Webmeeting & ST Chatproxy
- › Für ST Connect Client bei HTTP Verbindung

## › SIP Proxy Edge Server (A/V Clients)

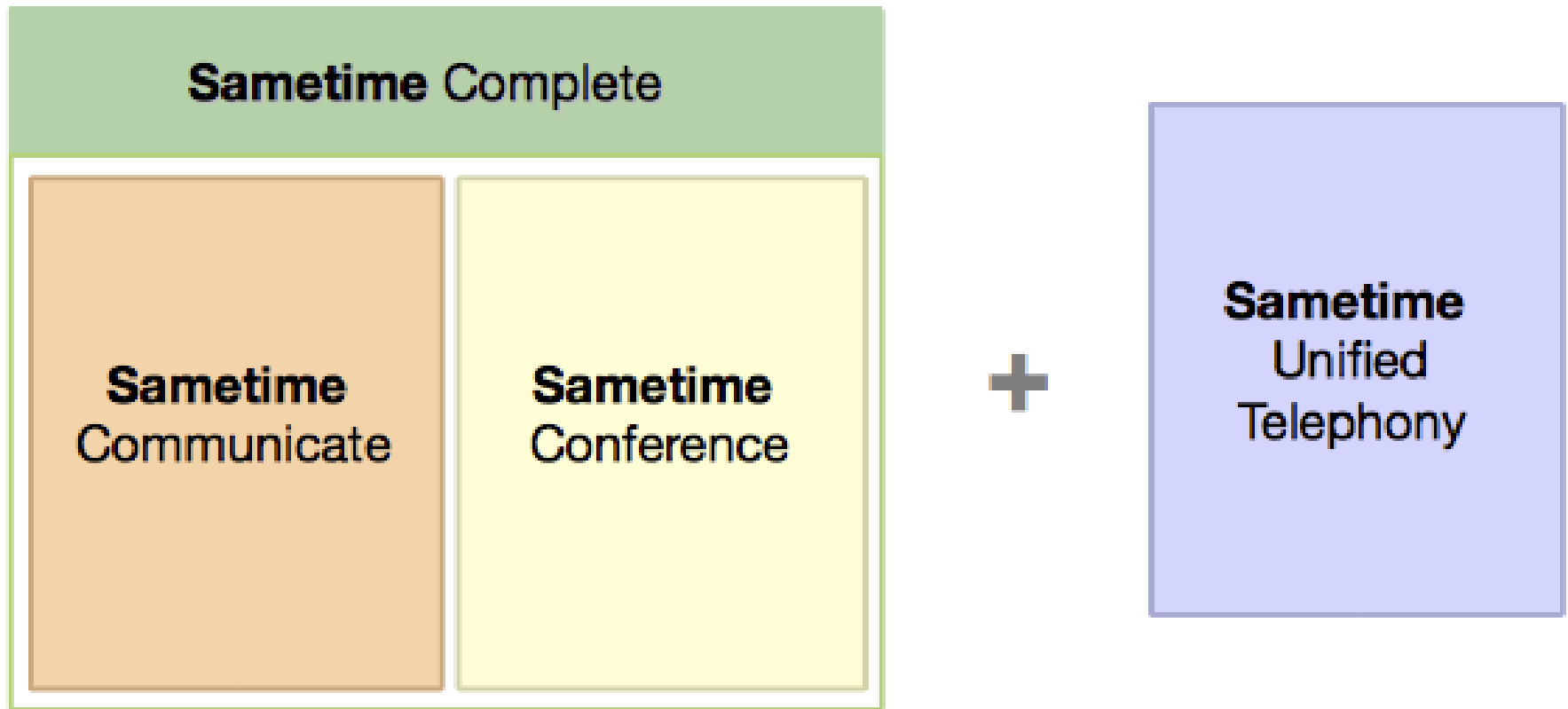
- › Routing von SIP Nachrichten zw. unterschiedlichen Netzen
- › „hält“ eine dauerhafte Verbindung zu den SIP Clients um SIP Nachrichten/Status zu verschicken

## › TURN Server (A/V Clients)

- › Ermittelt die öffentliche „NAT“ Adresse des Clients (ICE)
- › A/V „RELAY“, wenn P2P Verbindung in verschiedenen Netzen nicht möglich ist
- › A/V „RELAY“ auch dauerhaft möglich (P2P wird deaktiviert)



# Sametime 9 Produktgruppen / Lizenz

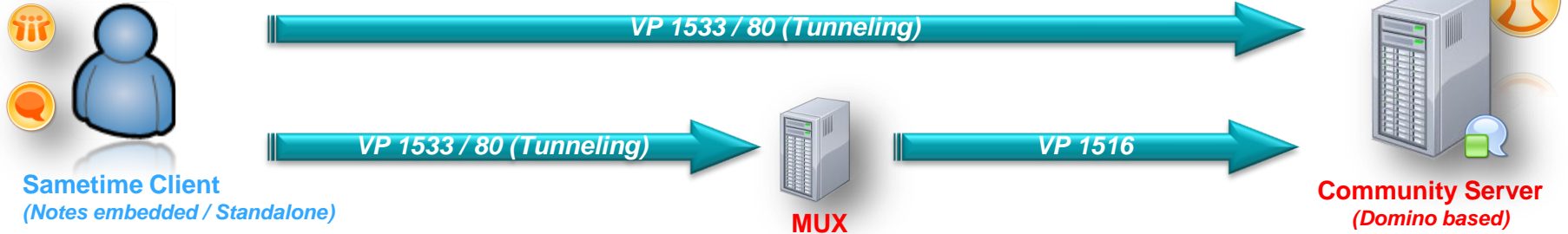




# Sametime 9 Produktgruppen / Lizenz

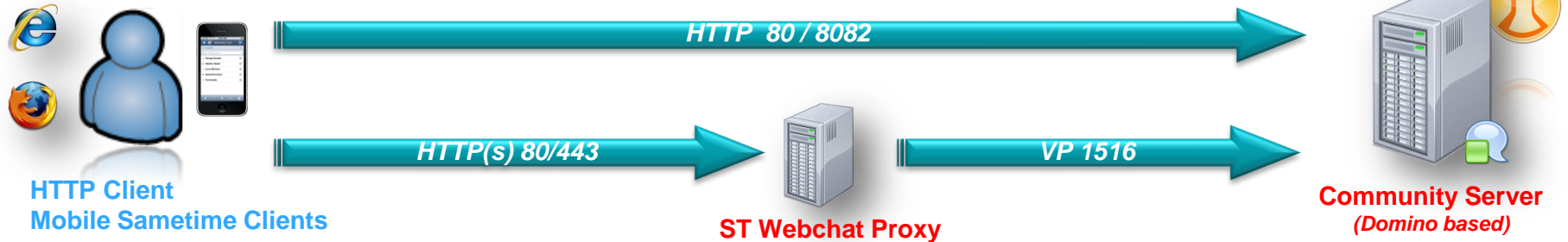
Servers or Services	IBM Notes Entitlement	Sametime Communicate	Sametime Conference	Sametime Complete	Sametime Unified Telephony
Sametime Connect Client	✓	✓	✓	✓	✓
Mobile clients	X	Mobile Chat	Mobile Meetings	Mobile Chat & Mobile Meetings	Mobile Chat can make SUT calls
DB2 Server	X	✓	✓	✓	✓
Sametime System Console	X	✓	✓	✓	✓
Community Server	✓	✓	✓	✓	✓
Sametime Proxy Server	✓ (iNotes)	✓	✓	✓	---
Advanced Server	X	✓	X	✓	---
Media Manager	X	✓	✓	✓	✓
Video Multipoint Control Unit (MCU)	X	X	✓	✓	---
Video Manager	X	X	✓	✓	---
Bandwidth Manager Server	X	✓	✓	✓	---
Meeting Server	X	X	✓	✓	---
Gateway Server	X	✓	X	✓	---
TURN Server	X	✓	✓	✓	---
WebSphere SIP Proxy Server	X	✓	✓	✓	✓
WebSphere HTTP Proxy Server	X	✓	✓	✓	---
Lotus SIP Edge Proxy Server	X	✓	✓	✓	---
Telephony Application Server	---	---	---	---	✓
Telephony Control Server	---	---	---	---	✓

# Sametime – Chat & Awareness



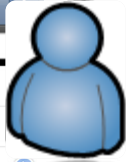
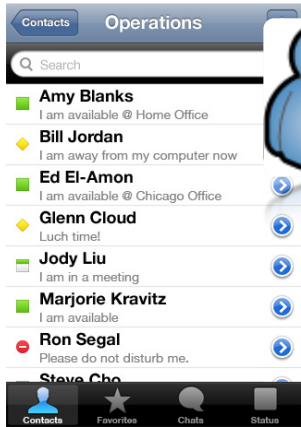
- ST **Community** (Domino) Server
- ST **MUX** Server (Chat Gateway)
- **Lizenz**
  - ST V8.5 Connect Entry / Notes Entitlement
  - ST V8.5 Connect Standard
  - ST V9 Communicate / Conference / Complete

# + Chat via Webclient (Browser) oder mobilen Geräten



- ST **Community** (Domino) Server – mobile Clients
- ST **Proxy** (WAS) Server
- **Lizenz**  
ST V8.5 Connect Standard (nicht im Entry enthalten)  
ST V9 Communicate / Conference / Complete  
Notes Entitlement: Webchat **YES**, Mobile **NO**

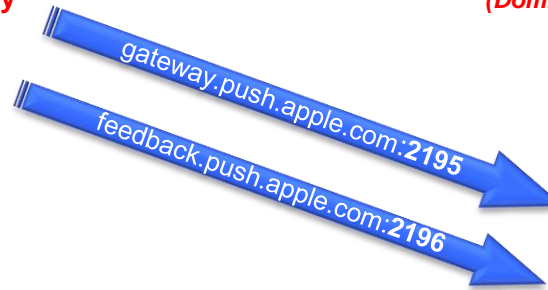
# + Chat via nativer Apple Client (iPad/iPhone)



ST Webchat Proxy



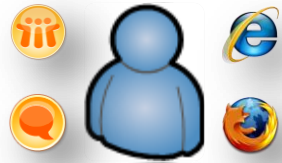
Community Server  
(Domino based)



Apple  
Notification  
Service

- ST **Community** (Domino) Server – mobile Clients
- ST **Proxy** (WAS) Server + DB2
- **Lizenz**  
ST V8.5 Connect Standard (nicht im Entry enthalten)  
ST V9 Communicate / Conference / Complete

# + Meeting Interface



HTTP Client  
Rich/Eclipse Meeting Client



**Community Server**  
(Domino based)



**Meeting Server**  
(Websphere based)

- ST **Community** (Domino) Server – Classic Meeting
- ST **Meeting** (WAS) Server
- **Lizenz**  
ST V8.5 Connect Standard (*nicht im Entry enthalten*)  
ST Concurrent Meeting User  
ST V9 Conference / Complete

# + externe Chat Community *(Google, OCS, Jabber, Sametime)*



Sametime Client  
*(Notes embedded / Standalone)*



Community Server  
*(Domino based)*



Gateway Server  
*(Websphere based)*



**SIP**

- Sametime Gateway
- AOL Instant Messenger
- AOL Clearinghouse (iChat, ICQ, other AOL/ST comm.)
- Office Communications Server

**XMPP**

- Google Talk
- JABBER / Openfire

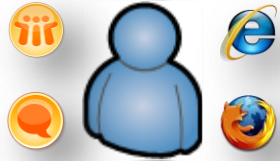


- ST **Gateway** (WAS) Server

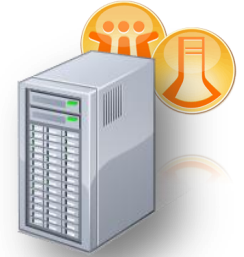
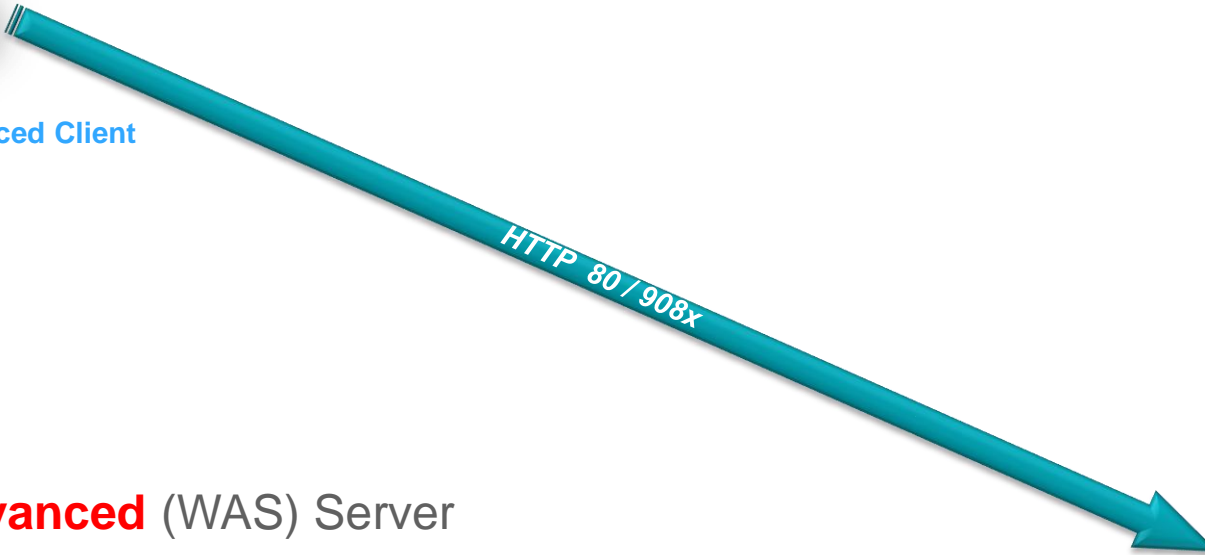
- **Lizenz**  
ST V8.5 Connect Standard *(nicht im Entry enthalten)*  
ST V9 Communicate / Complete

**YAHOO Messenger Service SHUT Down (12/2011)**  
*Interoperability with the Yahoo! Messenger service changes in 2011*

# + dauerhafte Chaträume, Instant Share, erweiterte Chatfunktion



HTTP Client  
Rich/Eclipse Advanced Client



Community Server  
(Domino based)

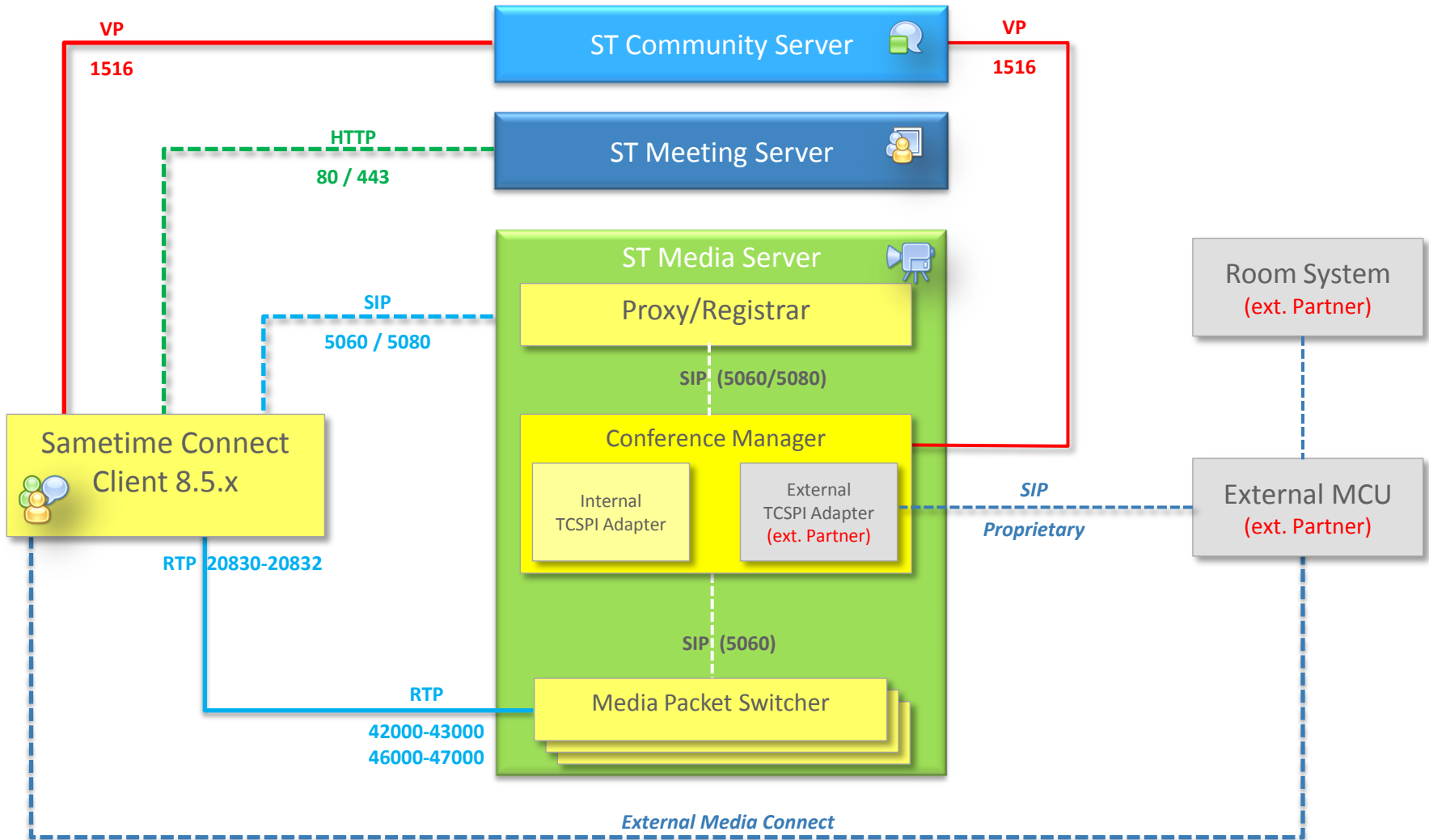


Advanced Server  
(Websphere based)

- ST **Advanced** (WAS) Server
- **Lizenz**  
*ST V8.5 Connect Advanced* (beinhaltet ST Connect Standard)  
*ST V9 Communicate / Complete*

# Sametime Media Server 8.5

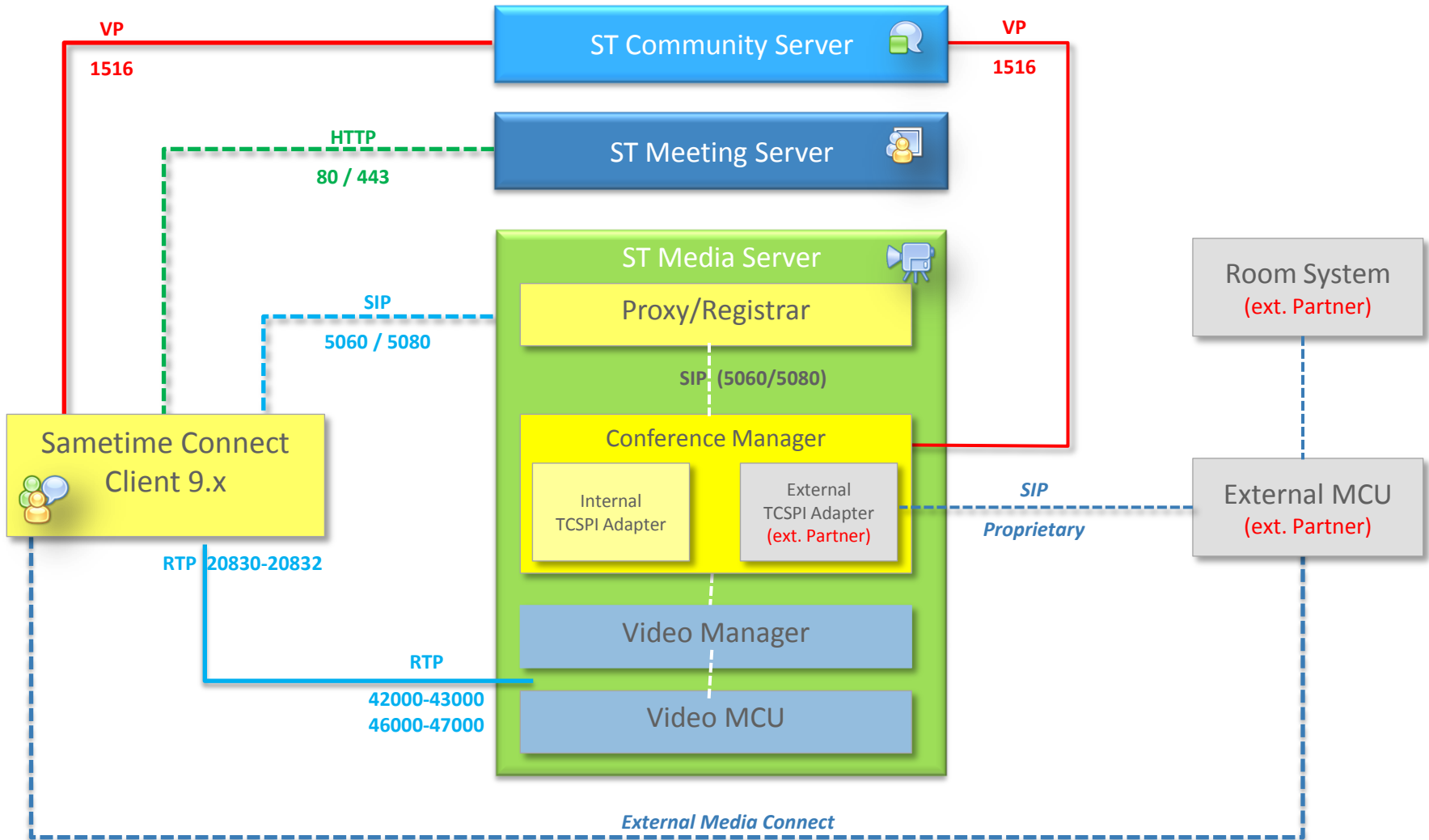
*VP = Virtual Places Protocol*  
*SIP = Session Initiation Protocol*  
*RTP = Real time Transport Protocol (A/V – dyn. UDP)*  
*TCSPI = Telephony Conference Service Provider Interface*



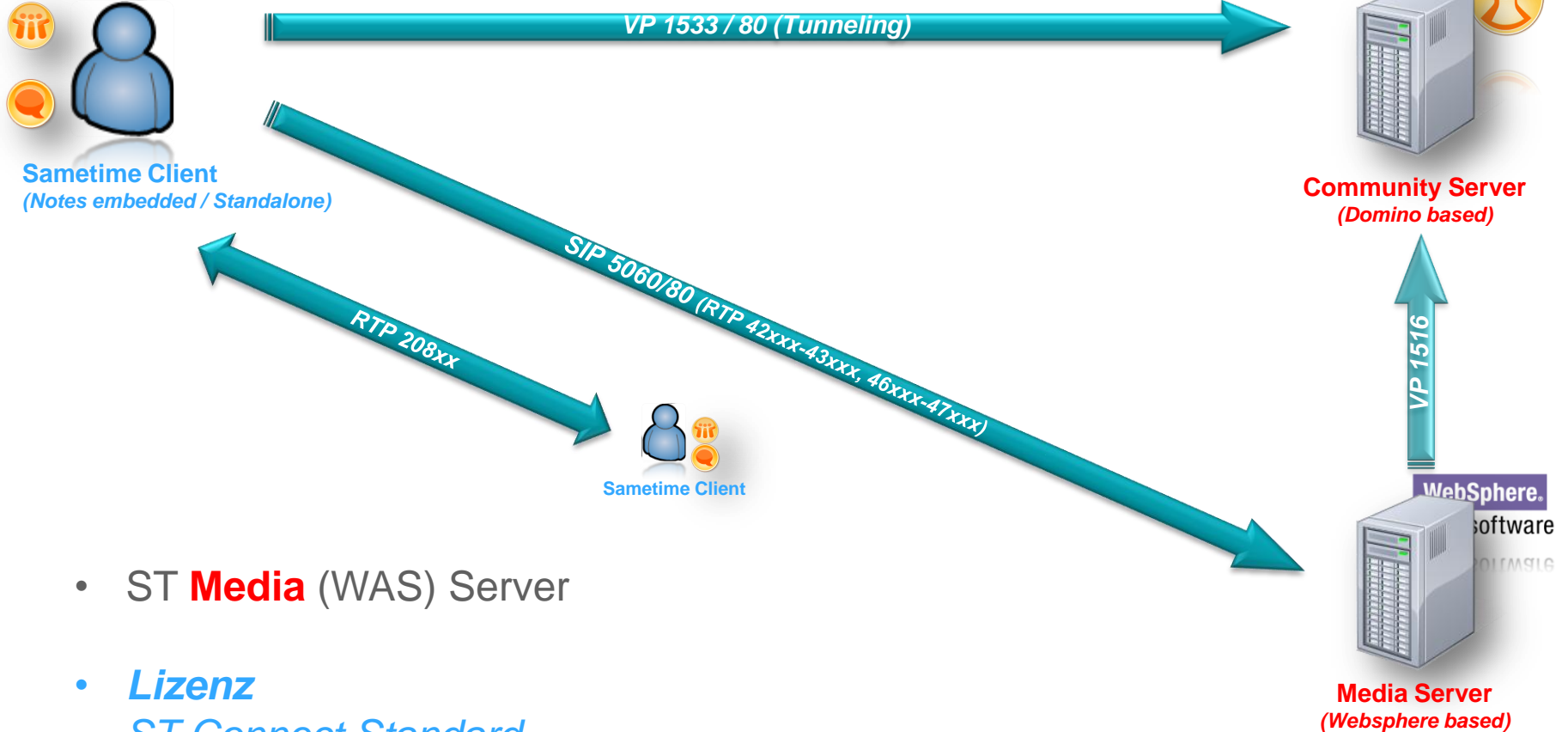


# Sametime Media Server 9

*VP = Virtual Places Protocol*  
*SIP = Session Initiation Protocol*  
*RTP = Real time Transport Protocol (A/V – dyn. UDP)*  
*TCSPI = Telephony Conference Service Provider Interface*



# + Audio/Video – P2P Sametime Connect



Sametime Client  
(Notes embedded / Standalone)

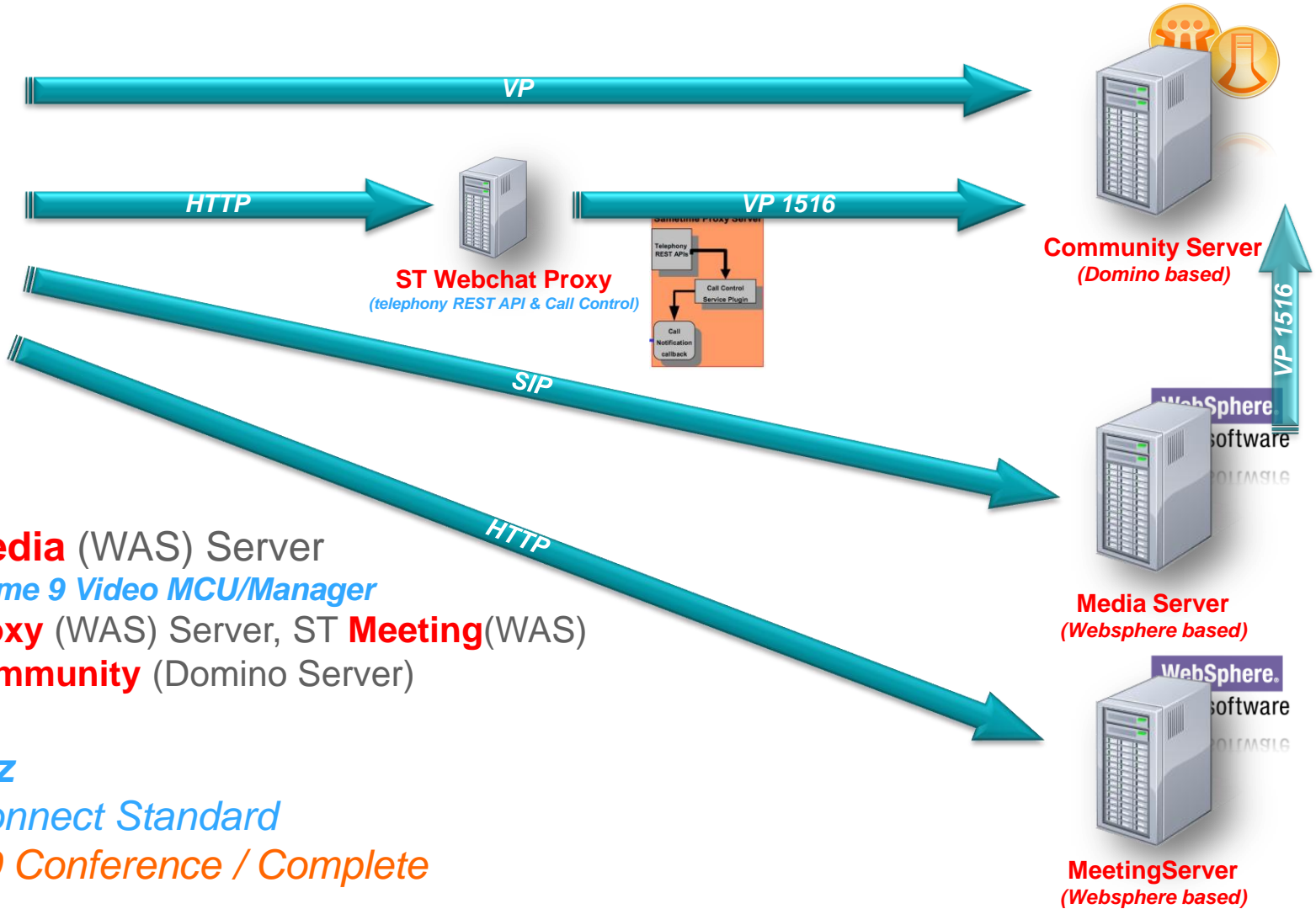
Sametime Client

Community Server  
(Domino based)

Media Server  
(Websphere based)

- ST **Media** (WAS) Server
- **Lizenz**  
ST Connect Standard  
ST V9 Communicate / Conference / Complete

# + Audio/Video „Web AV“



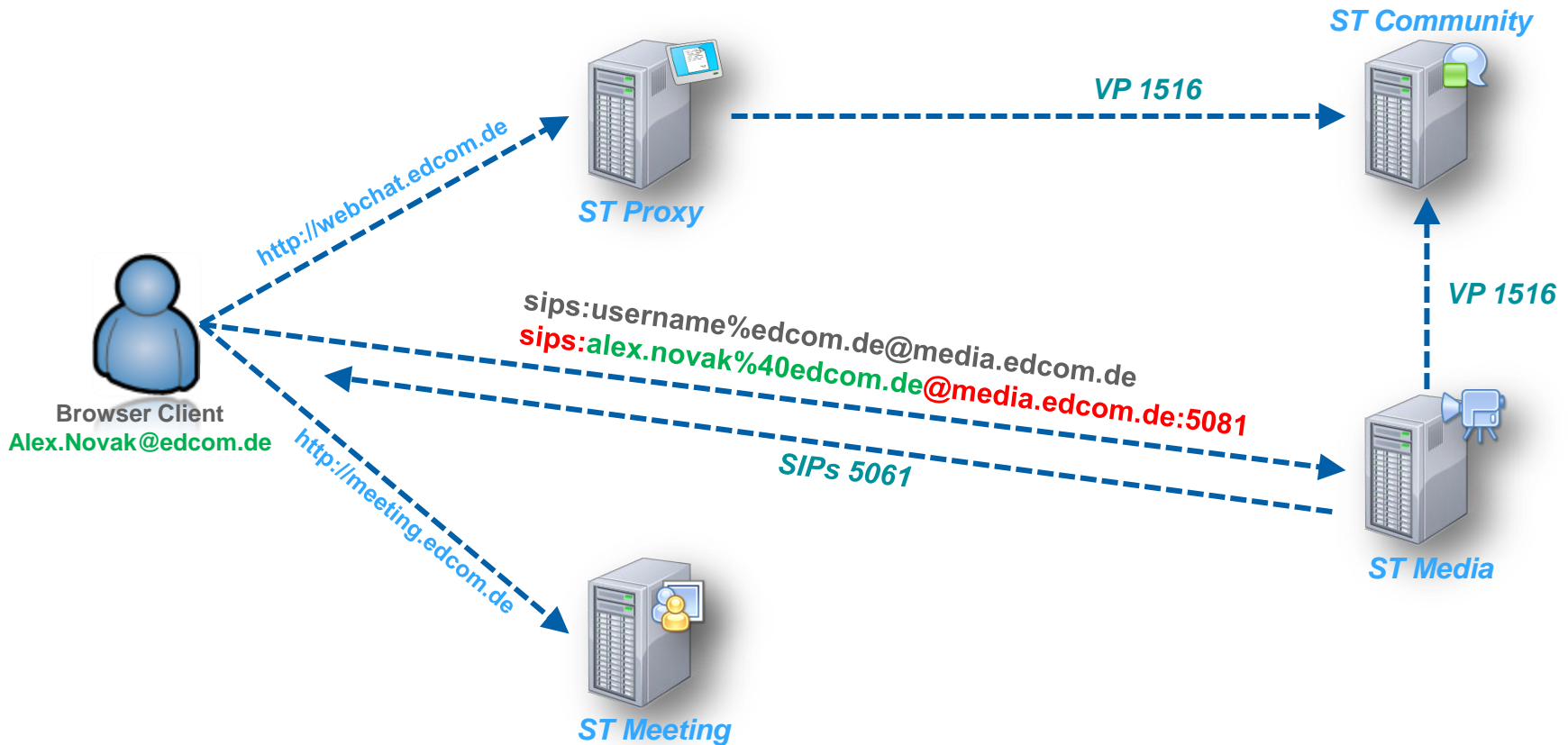
- ST **Media** (WAS) Server  
*Sametime 9 Video MCU/Manager*
- ST **Proxy** (WAS) Server, ST **Meeting**(WAS)  
ST **Community** (Domino Server)

- **Lizenz**  
*ST Connect Standard*  
*ST V9 Conference / Complete*

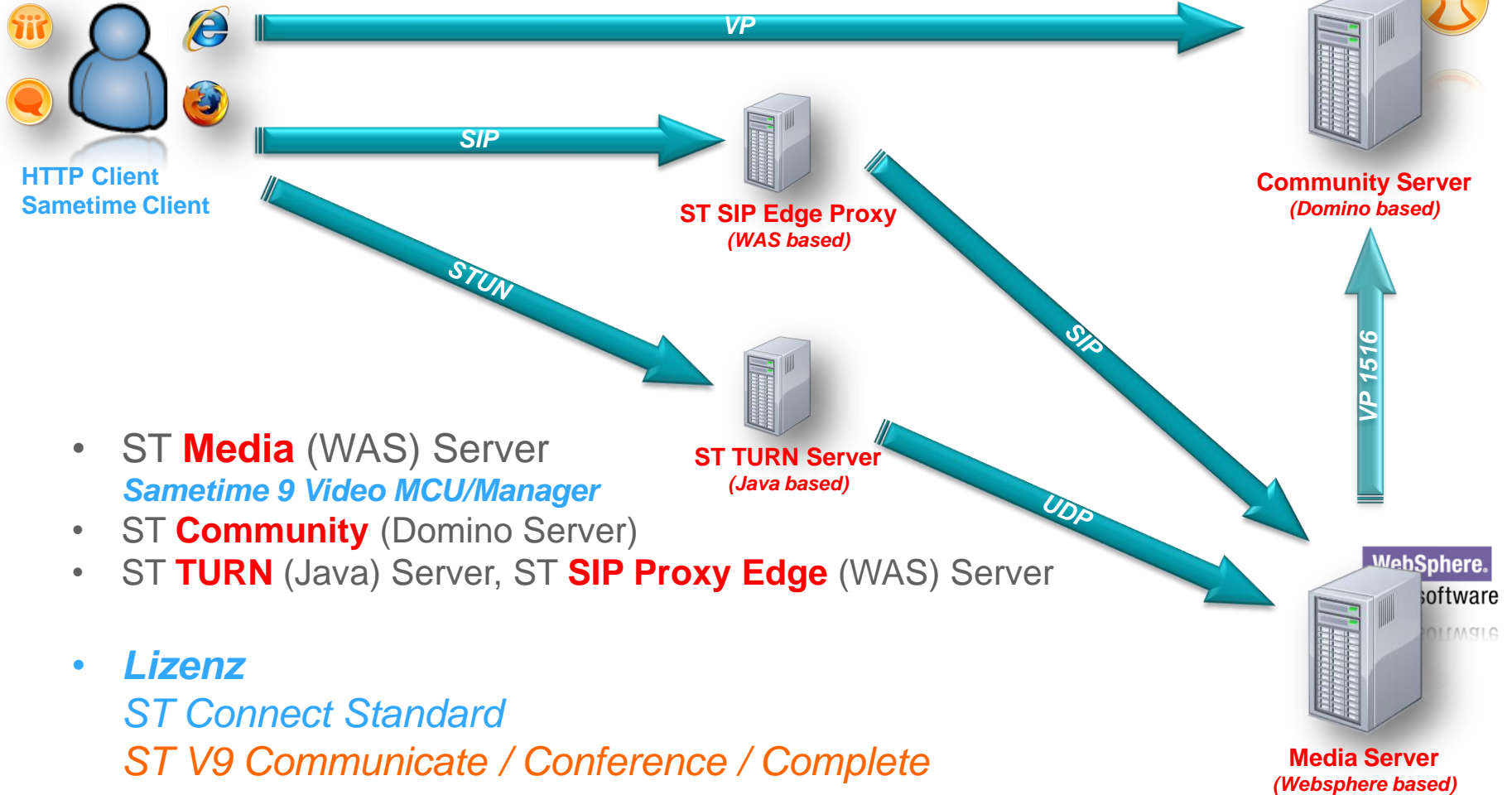
# IBM Sametime - Web A/V



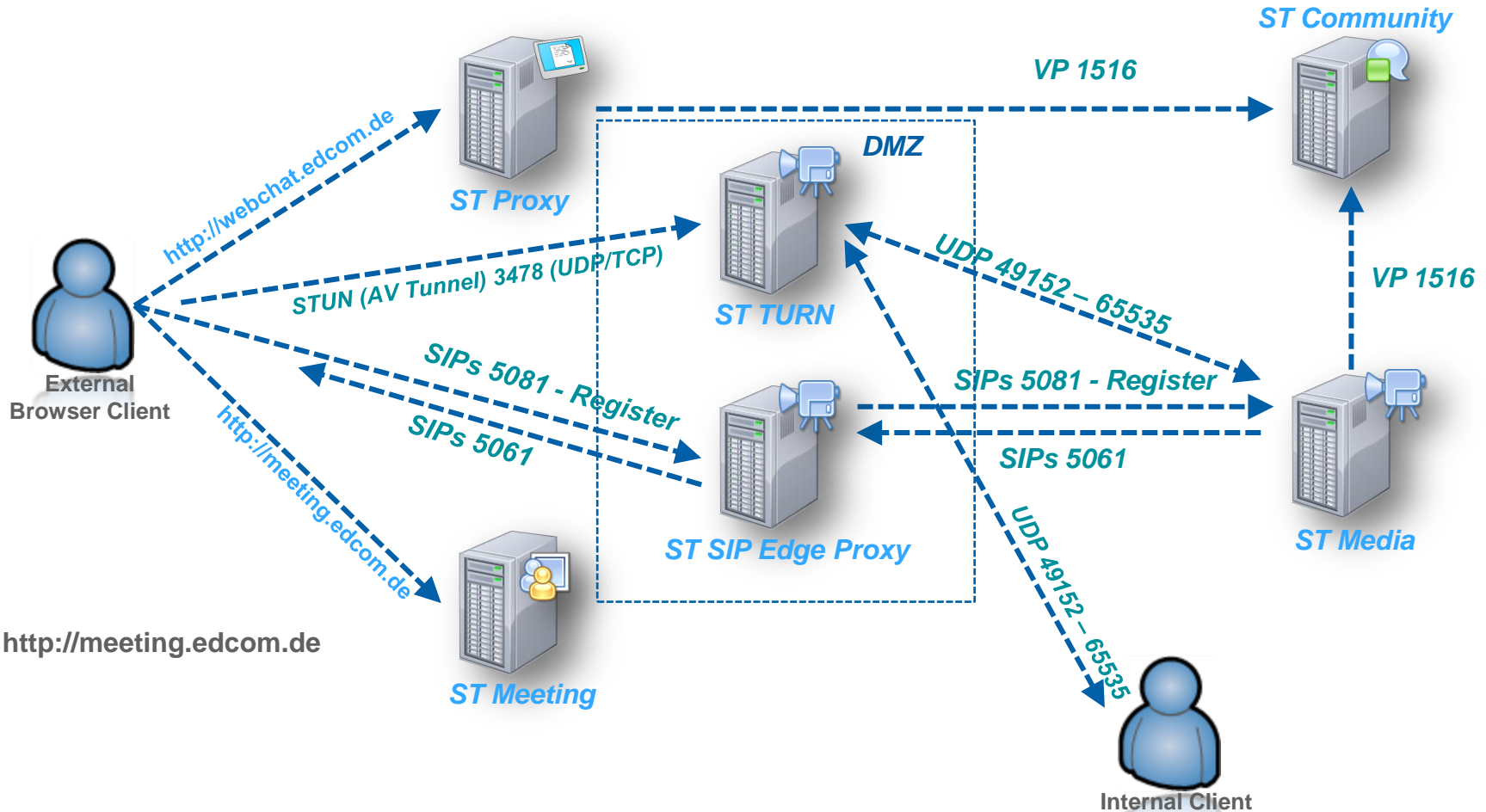
## ST Community, ST Media, ST Meeting, ST Proxy Server(s)



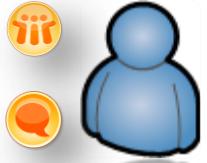
# + Audio/Video „Natting“



# IBM Sametime - Web A/V "NAT"



# + „light“ Telephonie Integration (Softphone)



Sametime Client  
(Notes embedded / Standalone)



Community Server  
(Domino based)



Media Server  
(Websphere based)



SIP TRUNK



- ST **Media** (WAS) Server  
*Modul „Conference Manager“*
- SIP end-points (SIP trunk)
- **Lizenz**  
*ST Unified Telephony „light“ Client*  
*ST V9 Communicate / Complete*



# IBM Sametime



## Classic vs. Websphere Meeting

Funktionen	Classic Meeting	Websphere Meeting
Meeting Erstellung	Zeitbasiert (Kalenderintegration via Mailin)	Dauerhafte Räume
Adhoc Meetings → werden nach Beendigung sofort wieder gelöscht	✓	✓
Löschung von Meetings	Stconf.nsf (Agent)	Nur Ersteller & Admin kann Meetings löschen
Audio & Video	✓	Rich Client oder WebAV & <b>Media Server</b>
Awareness	✓	<b>ST Proxy</b>
Meeting Berechtigungen vergeben	✓	✓ <b>8.5.2</b>
<b>Application sharing remote control</b>	Via Server	8.5 - Nur via Rich Client (Peer-to-peer) ✓ <b>9.0</b>
Presentation files	Nur Präsentation (PDF, PPT, usw.)	Alle Dokumenten Arten (XLS, Doc usw.)
Presentation download	<b>X</b>	✓
Meetingaufzeichnung	Serverseitig (nur online abrufbar)	8.5 - <b>Connect Client</b> 9.0 – <b>Serverseitig</b>
Presenter tools (highlighter, pointer)	✓	✓ <b>8.5.2</b>



# IBM Sametime 8.5/9 – Connect Client



## ▶ Audio / Video Interoperabilität

### ▶ Sametime Client 7.5 – 8.0

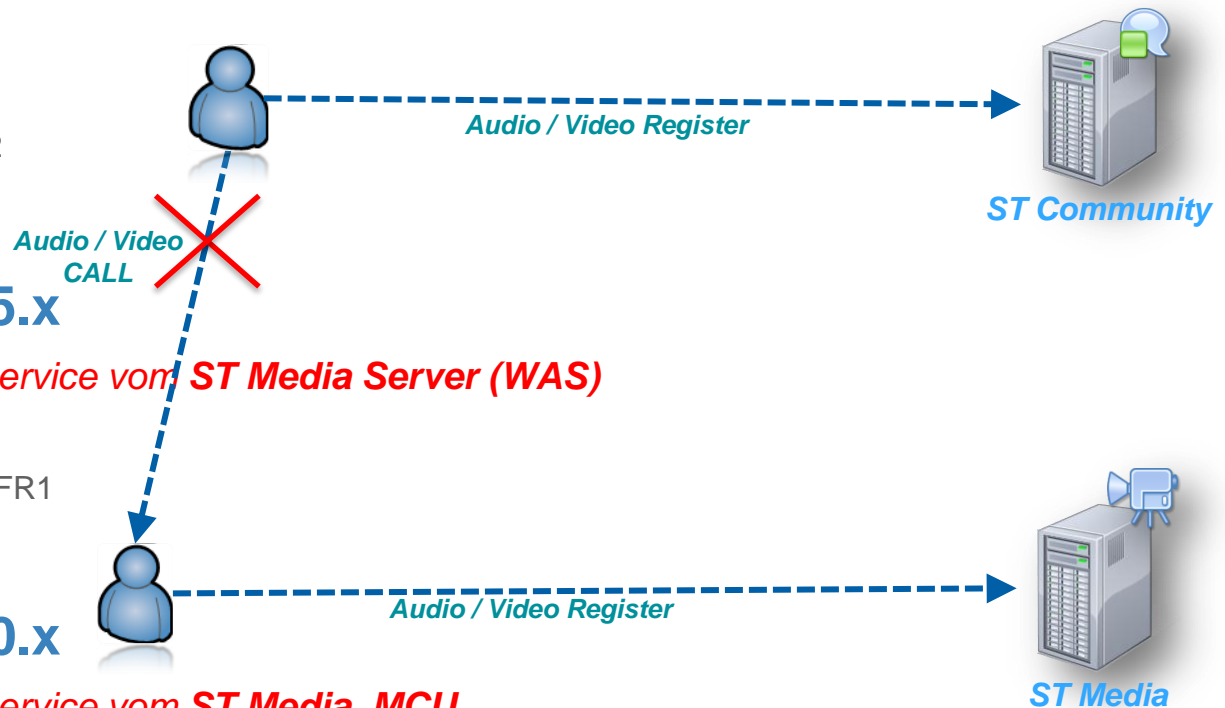
- ▶ *Audio/Video Service vom **ST Community Server (Domino)***
- ▶ Notes 8.0 = Sametime 7.5
- ▶ Notes 8.5.1 = Sametime 8.0.1
- ▶ Notes 8.5.2 = Sametime 8.0.2

### ▶ Sametime Client 8.5.x

- ▶ *verwendet Audio/Video Service vom **ST Media Server (WAS)***
- ▶ Notes 8.5.3 = Sametime 8.5.1
- ▶ Notes 9.0 = Sametime 8.5.2 IFR1

### ▶ Sametime Client 9.0.x

- ▶ *verwendet Audio/Video Service vom **ST Media, MCU***
- ▶ ***Multiple Videos NUR** mit ST 9 Clients oder ST 9 Meetings nutzbar*



# Agenda

- ▶ IBM Lotus Sametime 8.5.x Komponenten und deren Zusammenspiel
- ▶ **Sametime 8.5/9 Installation Best Practices**
- ▶ **Praktische Erfahrungen und Tipps**
  - ▶ Websphere Ports & Portmapping
  - ▶ SSO zwischen Domino & Websphere
  - ▶ Deaktivierung der SSL Verbindung zum Media System (Performance)
  - ▶ Debug Parameter

# Sametime Installation - Vorbereitungen



## ➤ **Hostnamen** und **DNS Einträge** müssen **VOR** der Installation gut überlegt sein

- ▶ IP Adressen können geändert werden
- ▶ Hostnamen und DNS Mappings im Websphere zu ändern ist sehr aufwendig (default\_host)
- ▶ FQHN sollte **=< 32 Zeichen** sein
  - ↳ Probleme mit Media Server & Web Audio/Video (*SIP/2.0 408 Request Timeout*)



## ➤ Verwendung von **Hosts** sofern kein DNS verfügbar ist

## ➤ DB2 User darf **NICHT** der lokale Systemadmin sein (DB2Admin)

## ➤ Websphere Admin (meist **WASADMIN**) darf **NICHT** im LDAP verfügbar sein

## ➤ LDAP Account darf **kein Sonderzeichen** in Kennwort haben

 [Special Characters \(&\) in LDAP Bind Password can cause Installation to fail during Federated Repository Configuration step \(KB #1438995\)](#)

# Sametime Installation - Vorbereitungen



## ➤ **ICMP & SOAP Protokoll** zw. SSC und ST WAS Installation notwendig

 [Troubleshooting the Sametime 8.5 System Console](#)

- ▶ Ping / ICMP kann nach der Installation wieder deaktiviert werden

## ➤ **Eine Migration von Sametime 7.5/8.0.x Servern ist möglich**

- ▶ Einbindung in SSC erfolgt über Registrierungsbatch
- ▶ **Authentifizierung** muss auf **LDAP** umgestellt werden

## ➤ **ST Installation verwendet den Rational Installation Manager**

- ▶ Probleme unter **Win 2003 & 2008 R2** mit dem zugewiesenen Java Heap Speicher - bricht u.U. die Installation mit *Java Heap Memory overflow* ab
  - ▶ *java.io.IOException: Not enough storage is available to process this command.*
- ▶ **IBMIM.ini**
  - ▶ Parameter “**-Xmx1024m**” am Ende hinzufügen
  - ▶ Mit **Version 1.6** nicht mehr notwendig

# “How to” Install IBM Sametime



 [From Zero To Hero \(1\) – Basics](#)

 [From Zero To Hero \(2\) – Edge Components](#)

- Slideshare / PDF
- Frank Altenburg @ IBM

 [Zero to Hero - SUT Lite Client: Configuring SIP trunks to 3<sup>rd</sup> party audio/video](#)

- *IBM Wiki*

 [“Keine Angst vor Sametime 8.5.x”](#)

- Slideshow (Linux based)
- Ulrich Krause @ [www.eknori.de](http://www.eknori.de)

 Redbooks: [Sametime 8.5 Enterprise Scale Deployment](#)

- IBM Wiki / PDF

Installation and Setup of  
IBM Sametime 8.5.2  
“From Zero to Hero”  
Part 1 - Basics

Frank Altenburg | SME for Sametime | IBM  
Volker Juergensen | Senior IT Specialist | IBM  
Social Business

## Keine Angst vor Sametime 8.5.1

Ulrich Krause

20. – 22.09.2010, Maritim Hotel, Gelsenkirchen



### ➤ Sametime 8.5 WAS Installationsablauf

1. Entpacken der WAS Dateien
2. Installation *WAS 7.0.0.3*
3. Erstellung der WAS Profile (*Dmgr, profile, server*)
4. Installation des *WAS Update Installer*
5. Update auf *WAS 7.0.0.15*
6. Installation der *Sametime Anwendung* in WAS
7. Abschließende *Konfigurationen* (*LDAP, DB2 Befüllung, SSC Registrierung*)

### ➤ Instalationsprotokoll (XML) im Browser öffnen

- ▶ Windows 2008: C:\Users\All Users\IBM\Installation Manager\logs



### › Sametime 9 WAS Installationsablauf

1. IBM Rational **Installation Manager V1.6.2** installieren
2. **Websphere V8.5.5** Network Deployment installieren
3. Websphere **Sametime Patches** installieren
4. **Installation** der **Sametime Anwendung** in WAS
  - Erstellt die **WAS Profile** (*Dmgr, profile, server*)
5. Abschließende **Konfigurationen** (*LDAP, DB2 Befüllung, SSC Registrierung*)

### › Instalationsprotokoll (XML) im Browser öffnen

- ▶ Windows 2008: C:\Users\All Users\IBM\Installation Manager\logs

# IBM Sametime

## SSC Installationspläne bereinigen



### ➤ Was passiert mit gelöschten ST WAS Service ?

- ▶ **Implementierungsplan** & ggfls. WAS Dienste in SSC weiter vorhanden

Implementierungsname	Installationstyp	Version	Implementierungsstat
Meeting	Primärknoten	8.5.2	Installiert/Registriert /Eingebunden
<a href="#">STMeetingServer</a>	meetingSTMNode1	meeting.edcomtest.local ND 7.0.0.15	?
<a href="#">nodeagent</a>	meetingSTMNode1	meeting.edcomtest.local	ND 7.0.0.15 ✘

### ➤ Nachträgliche DeRegistrierung mit **updateStaleEntry**

- ▶ [Console.properties](#): Feld „SSCPasswort“ befüllen
- ▶ Erstellt .../Websphere/Cell/console/logs/ConsoleUtility.log



# IBM Sametime

## SSC Installationspläne bereinigen



### ➤ `../SSCCell/console/updateStaleEntry -uninstall`

- ▶ Deployment Parameter vorher notieren !!!
- ▶ *Product type*
- ▶ *Hostname* := `meeting.edcom.local`
- ▶ *Install type* := Zelle oder Primärknoten
- ▶ *Deployment name* := `myMeetingServer`

### ➤ Restart SSC

### ➤ Danach ist der **Plan** in der SSC „löschar“

```
Sametime-Servertyp
[1] Sametime Community Server
[2] Sametime Media Server
[3] Sametime Meeting Server
[4] Sametime Proxy Server
[5] Sametime Gateway Server
Geben Sie Ihre Option an -
3

Installationstyp
[1] Zelle
[2] Primärknoten
[3] Sekundärknoten
[4] Deployment Manager
Geben Sie Ihre Option an -
2

Für Sametime Meeting Server
Geben Sie den Hostnamen an -
meeting.edcomtest.local
Geben Sie den Namen der Implementierung an -
Meeting

Status aktualisiert.
```

🔍 Implementierungsplan löschen

Auswählen	Implementierungsname	Installationstyp	Version	Implementierungssta
<input type="radio"/>	Meeting	Primärknoten	8.5.2	Deinstalliert

# IBM Sametime

## SSC Installationspläne bereinigen



- **Applikationsserver & Nodeagent** müssen manuell entfernt werden

Auswählen	Name	Knoten	Hostname	Version
<input type="checkbox"/>	<a href="#">STConsoleServer</a>	SSCNode	ssc.edcomtest.local	ND 7.0.0.15
<input type="checkbox"/>	<a href="#">STMediaServer</a>	mediaSTMSNode1	media.edcomtest.local	ND 7.0.0.15
<input checked="" type="checkbox"/>	<a href="#">STMeetingServer</a>	meetingSTMNode1	meeting.edcomtest.local	ND 7.0.0.15

- **Meeting Server**

- ▶ **Meeting Bus Eintrag** muss manuell aus der ISC gelöscht werden, da ansonsten die **NEUInstallation fehlschlägt**

- **Deinstallation** via **IBM Installation Manager** bereinigt die „meisten“ Einträge (Ausnahme Meeting BUS)

# Sametime

## *Installation/Migrationsprobleme „FAIL“*

### ► Updating Installation Manager if the admin name or password has changed

#### ► Backup

- C:\ProgramData\IBM\Installation Manager\installRegistry.xml
- C:\ProgramData\IBM\Installation Manager\installed.xml

#### ► Prüfung der Einträge `user.was.adminid/user.was.password`

```
<property name='user.com.ibm.lotus.sametime.systemconsoleserver.IsFederat  
<property name='user.was.password' value='His07dANmcIkCioT1t3b3g==' />  
<property name='user.nonWin.temp' value='D:/IBM/WebSphere/STtemp' />
```

- Vergleich Passworhashes (Encode Tool „generateEncodedPassword“)

```
D:\install\ST852Meetingsrv\generateEncodedPassword>generateEncodedPassword.bat p  
assword  
fufgZbY47EfxLYarBAIxeQ==
```

### ► Bereinigungscript von IBM (`iscmod_uninstall.py`)

- `<WebSphere install root>/STSCServerCell/iscmod_uninstall.py` ersetzen
- `<WebSphere install root>/AppServer/deploytool/scripts/install/ejbdeploy-clear-cache`

# Agenda

- ▶ IBM Lotus Sametime 8.5.x Komponenten und deren Zusammenspiel
- ▶ Sametime 8.5/9 Installation Best Practices
- ▶ **Praktische Erfahrungen und Tipps**
  - ▶ Websphere Ports & Portmapping
  - ▶ SSO zwischen Domino & Websphere
  - ▶ Deaktivierung der SSL Verbindung zum Media System (Performance)
  - ▶ Debug Parameter

# Sametime WAS Umgebung

## Verwendung mehrere Websphere Zellenprofile

### SSC Websphere Zelle

#### SSC Dmgr

- LDAP Konfiguration
  - Benutzer
  - Gruppen
- Schlüsselverwaltung
  - SSL, Truststore
- Security Konfiguration
  - SSO
  - LTPA
  - SPNEGO



Nodeagent  
SSC



#### STConsoleServer

- Sync bzw. Zugriff auf die Sametime Konfiguration
- Sameitme Policy



### Meeting Websphere Zelle

#### Meeting Dmgr

- LDAP Konfiguration
  - Benutzer
  - Gruppen
- Schlüsselverwaltung
  - SSL, Truststore
- Security Konfiguration
  - SSO
  - LTPA
  - SPNEGO



Nodeagent  
STMeeting



- Sametime Konfiguration
- Policy
- STMeetingServer



### Nachteil

- SSL Zertifikate (TRUST)
- Mehrfache Websphere Konfiguration
  - SSO
  - SSL
  - LDAP
  - etc.

### Media Websphere Zelle

#### Media Dmgr

- LDAP Konfiguration
  - Benutzer
  - Gruppen
- Schlüsselverwaltung
  - SSL, Truststore
- Security Konfiguration
  - SSO
  - LTPA
  - SPNEGO



Nodeagent  
STMedia



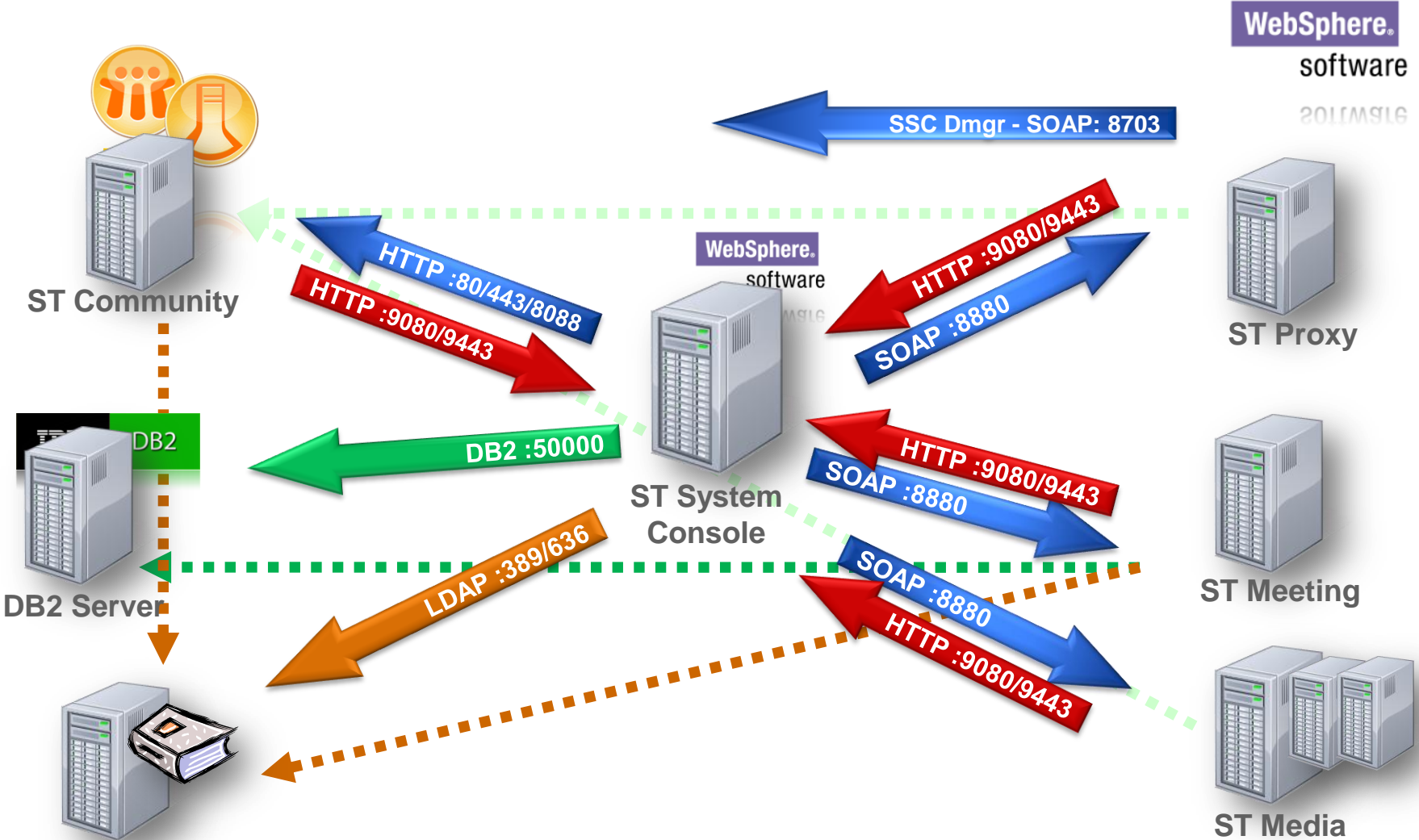
- Sametime Konfiguration
- Policy
- STAVconfig.xml



# Sametime System Console (SSC) - Ports



SOAP = **Simple Object Access Protocol** / Austausch von XML-Basierter Nachrichten  
 SOAP → Adminrequest  
 HTTP → Console notification



# Sametime/WebSphere Server Ports

Source → Destination

	DB2	LDAP	Deployment Manager	System Console	Community	Mux	Sametime Proxy	Sametime Meeting	Media Manager
Deployment Mgr	50000	389	---	---	---	---	SOAP 8878 (node) SOAP 8880	SOAP 8878 (node) SOAP 8880	SOAP 8878 (node) SOAP 8880
System Console	50000	389	SOAP 8703	---	80/443	---	---	---	---
LDAP (Comm Srv)		---							
Community Server		389		ST: 9080/9443	---	---	---	---	---
Mux	---			---	VP 1516	---	---	---	---
Sametime Proxy	50000	389	SOAP 8703	ST: 9080/9443	VP 1516	---	---	---	---
Sametime Meeting	50000	389	SOAP 8703	ST: 9080/9443	---	---	---	---	---
Media Manager	---	389	SOAP 8703	ST: 9080/9443	VP 1516	---	---	---	---

# Sametime – *Port/Hostmapping*



- ▶ Websphere Application Server binden Ihren HTTP Dienst **NICHT** auf den Port **80** oder **443**
- ▶ Möglichkeit den Vorgabepport 908x bzw. 944x „umzubiegen“

- ▶ WAS Console > Anwendungsserver > STProxyServer > Ports

- ▶ **WC\_Defaulthost: 80**

- ▶ **WC\_Defaultlhost\_secure: 443**



<a href="#">WC_defaulthost</a>	chat.edcom.de	80
<a href="#">WC_defaulthost_secure</a>	*	9443

- ▶ **Hostmapping** notwendig wenn mehrere Anwendungen auf einer Maschine laufen (z.B. Meeting und Proxy)
  - ▶ Proxy = „chat.edcom.de“
  - ▶ Meeting = meeting.edcom.de



# Sametime – *Port/Hostmapping*

- ▶ Sametime Proxy und Sametime Meeting sollten nicht auf der gleichen Maschine installiert sein
    - ▶ **HTTP Konflikte**, da beide 80/443 verwenden sollen
    - ▶ **JSessionID** Probleme, wenn beide gleichen Hostnamen verwenden
    - ▶ Wenn allerdings unumgänglich – Verwendung der Websphere Portmappings und Zuweisung eines HostAlias (eigene IP)
-  [Deploying ST Proxy and ST Meeting Server on the same machine](#)

Auswählen	Hostname 	Port 
Sie können die folgenden Ressourcen verwalten:		
<input type="checkbox"/>	*	9080
<input type="checkbox"/>	*	80
<input type="checkbox"/>	*	9443
<input type="checkbox"/>	*	5060
<input type="checkbox"/>	*	5061

# Sametime – Integration SSO



## ➤ Web SSO Dokument in Websphere DNS Token eintragen

- ▶ [.edcom.local;.timetoact.de](#)
- ▶ Interoperabilitätsmodus
  - ▶ Domino 7 oder älter

**Globale Sicherheit > Single Sign-on (SSO)**  
Gibt die Konfigurationswerte für Single Sign-on an.

**Allgemeine Eigenschaften**

- Aktiviert
- Erfordert SSL
- Interoperabilitätsmodus
- Weitergabe der Sicherheitseinstellungen für eingehende Verbindungen

Domänenname

## ➤ Zuweisung LTPA

- ▶ **Timeout** (sollte identisch mit Domino sein)
- ▶ „*Export LTPA Token*“ to Filesystem
  - ▶ Domino
  - ▶ Andere Websphere Zellen

**Globale Sicherheit > LTPA**  
Verschlüsselt die Authentifizierungsinformationen so, dass der Anwendung...  
Authentifizierungsinformationen, die zwischen Servern ausgetauscht werden...

**Schlüsselgenerierung**  
Authentifizierungsdaten werden mit Schlüsseln, die in einem oder mehreren...  
Schlüsselsatzgruppe

**LTPA-Zeitlimit**  
LTPA-Zeitlimit für zwischen Servern weitergeleitete Berechtigungsna...  
 Minuten

**Zellenübergreifendes Single Sign-on**  
Zellenübergreifendes Single Sign-on (SSO, Einzelanmeldung) kann d...  
Schlüssel und das Kennwort gemeinsam nutzen möchten, melden Sie...  
exportieren. Melden Sie sich anschließend an der anderen Zelle an, g...

\* Kennwort

\* Kennwort bestätigen

Vollständig qualifizierter Name der Schlüsseldatei

# Sametime – Integration SSO



## › Domino LTPA

- › LTPA Dokument erstellen
- › Sametime Server zuweisen
- › Websphere LTPA einlesen

## › Sametime.ini Anpassungen

- › ST\_TOKEN\_TYPE=LTPATokenEdcom
- › Internet Sites !!!
  - › ST\_ORG\_NAME=Organization

## › Debug

- › Notes.ini := debug\_sso\_trace\_level=2
- › Token Überprüfung := JavaScript: alert(document.cookie)

The screenshot shows the 'Web SSO Configuration for : LtpaToken' dialog box. The 'Token Configuration' section includes fields for Configuration Name (LtpaToken), Organization, DNS Domain (.corp.intl), Map names in LTPA tokens (Disabled), Require SSL protected communication (HTTPS) (Disabled), and Restrict use of the SSO token to HTTP/HTTPS (Disabled). The 'Token Expiration' section shows Expiration (minutes) set to 720. The 'Participating Servers' section includes Domino Server Names (dom/educ) and Windows single sign-on integration (Disabled). The 'WebSphere Information' section includes Token Format (LtpaToken2), LDAP Realm (defaultWIMFileBasedRealm), and LTPA Version (1.0). A 'Enter Import File Name' dialog box is overlaid, showing the path d:\stmltpakey\.

# Sametime – Integration SSO



➤ „**Base DN**“ ist nicht notwendig – ABER ...

➤ „**LDAP Deployment name**“ wird via Sametime Wizard in die Webshere Konfiguration übernommen

Deployment name	Host name	Port
LDAP on mail02-tta	mail02.timetoact.de	389

## General Properties

\* Repository  
LDAP on mail02-tta

\* Distinguished name of a base entry that uniquely identifies this set  
LDAPDeployname

Distinguished name of a base entry in this repository  
LDAPDeployname

Username BaseDN  
Gruppen BaseDN

- ▶ Macht später Probleme mit **SSO** zwischen Domino & Websphere Servern (Meeting, Proxy, Advanced)
- ▶ **Falsche Username** im Websphere  
➔ cn=Alexander Novak, o=edcom, o=LDAPDeployname

# Sametime – Integration SSO



## ➤ Lösung = Deploymentname durch Base DN Eintrag ersetzen

- ▶ Zweites Feld ist für Gruppensuche zuständig
- ▶ Problematisch bei mehreren Organisationen (z.B. O=edcom, O=tta)

General Properties

\* Repository: LDAP on mail02-tta [Add Repository...]

\* Distinguished name of a base entry that uniquely identifies this set: LDAPDeployname (Username BaseDN)

Distinguished name of a base entry in this repository: LDAPDeployname (Gruppen BaseDN)

## ➤ BEST PRACTICE = Eintrag „root“ setzen

- ▶ BaseDN Eintrag in der `profile_root/config/cells/cell_name/wim/config/wimconfig.xml` wird gelöscht

\* Repository: LDAP on mail02-tta [Add Repository...]

\* Distinguished name of a base entry that uniquely identifies this set: root (Username BaseDN = \*)

Distinguished name of a base entry in this repository: "Flache" Gruppen (Notes)

- ▶ WAS 7.0.0.21 notwendig (Fehler beim Aufruf der WAS Repository)
- ▶ Prüfung der Namen WAS > Manage Users/Groups

1 users matched the search criteria.

Create... Delete Select an action...

Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	<a href="#">anovak</a>	Alexander Novak	Novak	alexander.novak@edcom.de	CN=Alexander Novak,O=edcom,C=DE

Richtiger Lookup

# Websphere – SSL Zertifikate

- ▶ Websphere generiert ein „**self-signed**“ SSL Zertifikat
  - ▶ Ein Jahr gültig
  - ▶ Erneuert sich selbstständig
- ▶ **Extranet** und **mobile Access** benötigen **offizielle SSL Zertifikate** (Verisign, Cybertrust, Trustcenter, etc.)
  - ▶ SSL Request erstellen & empfangen
  - ▶ Import Privat Key Format \*.p12 (z.B. Wilcard Zertifikate)
  - ▶ Zuweisung des SSL Schlüssel an den WAS Server
- ▶ **Import der SSL Zertifikate in WAS Zellen (Trust)**
  - ▶ z.B. Media Server TLS

# Websphere – SSL Zertifikate

## ➤ SSL Verwaltung

### ▶ Zellen **Key** & **Truststore**

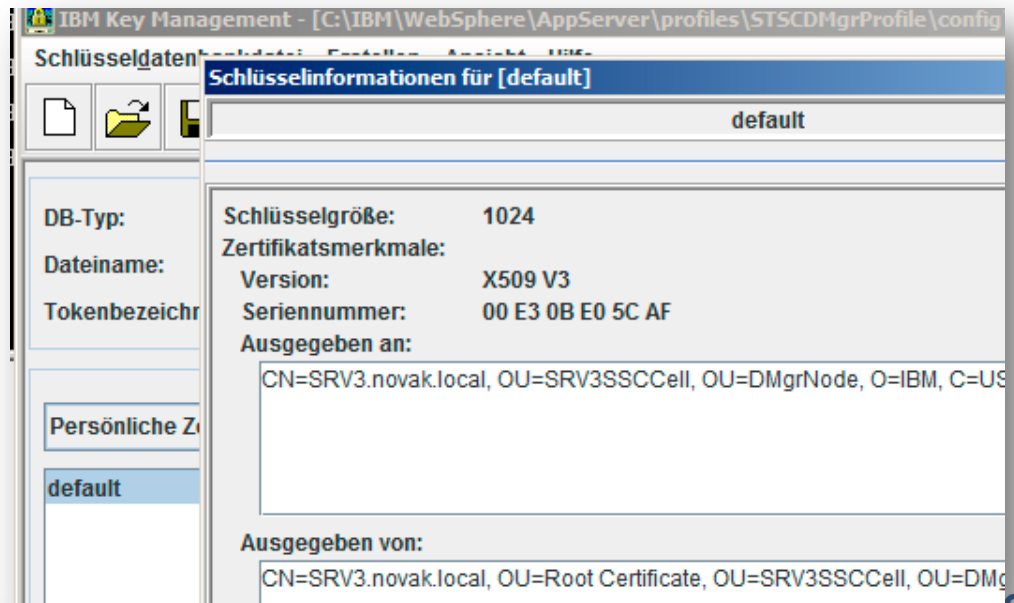
- ▶ ... \websphere\appserver\profiles\STSCDMgrProfile\config\cells\<cellname>\trust.p12
- ▶ ... \websphere\appserver\profiles\STSCDMgrProfile\config\cells\<cellname>\key.p12

### ▶ Websphere **ISC**

- ▶ SSL certificate and key management > Key stores and certificates > CellDefaultKeyStore

### ▶ **ikeyman**

- ▶ Password „WebAS“



# Websphere – SSL Zertifikate

## ➤ SSL Request erstellen & empfangen

### ▶ Websphere **ISC**

#### ▶ **Request erstellen**

SSL certificate and key management > Key stores and certificates > CellDefaultKeyStore > **Personal certificate requests** > **NEW**

#### ▶ **Request wieder importieren** (zurück von der CA)

SSL certificate and key management > Key stores and certificates > CellDefaultKeyStore > **Personal certificates** > **Receive certificate from CA**

### ▶ **keyman** (Zellen Keystore öffnen – key.p12)

Request erstellen: **Personal certificate requests** > **NEW**

Request wieder importieren: **Personal certificates** > **Receive**

Dateiname: C:\IBM\WebSphere\AppServer\profiles\STSCDMgrProfile\config\cells\SRV3SSCCell\key.p12

Tokenbezeichnung:

Schlüsseldatenbankinhalt

Persönliche Zertifikatsanforderungen

Neu...

Löschen

Anzeigen

Extrahieren...

Neuen Schlüssel und neue Zertifikatsanforderung erstellen

Geben Sie folgende Informationen an:

Schlüsselkennsatz

Schlüsselgröße 1024



# Websphere – SSL Zertifikate

## ➤ SSL „private Key“ importieren / SSL Verlängerung

- ▶ Ist der „personal request“ nicht mehr vorhanden (z.B. bei Verlängerungen) kann ein „Renewal“ nicht mehr eingelesen werden (ISC Fehlermeldungen)
  - ▶ **keyman** nutzen (Zellen Keystore öffnen – key.p12)
    - ▶ Request erstellen: Personal certificate requests > *Receive*
  - ▶ P12 „private“ Key verwenden (z.B. bei **Wildcard** Zertifikaten)
    - ▶ SSL certificate and key management > Key stores and certificates > CellDefaultKeyStore > Personal certificates > *Import certificates from a key file or key store*

The screenshot shows the WebSphere Administration Console interface. On the left is a navigation tree with categories like 'Anzeigen', 'Sicherheit', 'Umgebung', 'Systemverwaltung', 'Benutzer und Gruppen', 'Überwachung und Optimierung', 'Fehlerbehebung', 'Serviceintegration', and 'UDDI'. The main content area is titled 'Zelle srv-stproSTPCell1, Profil srv-stproSTPDMProfile1' and 'Seite schließen'. The breadcrumb path is: 'Verwaltung von SSL-Zertifikaten und Schlüsseln > Keystores und Zertifikate > CellDefaultKeyStore > Persönliche Zertifikate > Zertifikate aus einer Schlüsseldatei oder einem Keystore importieren'. The dialog box contains the following fields and options:

- Allgemeine Eigenschaften**
- Verwalteter Keystore**
  - Keystore: CellDefaultKeyStore ((cell):srv-stproSTPCell1)
  - Keystore-Alias-abrufen: [button]
  - Kennwort für Keystore: [input]
- Keystore-Datei**
  - Name der Schlüsseldatei: d:\zertifikat\\*.com.p12
  - Typ: PKCS12
  - Kennwort der Schlüsseldatei: [input] Schlüsseldateialias abrufen: [button]
- Zu importierender Zertifikatsalias: 78920552047042902818938441355328619659cn=\*,... c=de, cn=thawte ssl ca, o="thawte, inc.", c=us
- Importierter Zertifikatsalias: GlobalKey
- Buttons: Anwenden, OK, Zurücksetzen, Abbrechen

# Websphere – SSL Zertifikate

## ➤ SSL Zertifikate können **NUR** in der Websphere Console (ISC) **zugewiesen** werden

- ▶ SSL certificate and key management > Manage endpoint security configurations > **Inbound** > **WebsphereServer** (z.B. STProxyServer)
- ▶ SSL certificate and key management > Manage endpoint security configurations > **Outbound** > **WebsphereServer** (z.B. STProxyServer)

**SSL certificate and key management > Manage endpoint security configurations**  
Displays Secure Sockets Layer (SSL) configurations for selected scopes, such as a cell.

Local Topology

- Inbound
  - SRV3SSCell(CellDefaultSSLSettings)
    - nodes
      - DMqrNode
      - SRV3SSNode(NodeDefaultSSLSettings)
      - srv4STMSNode1(NodeDefaultSSLSettings)
      - IHS\_Node
      - srv4STPNode1(NodeDefaultSSLSettings)
      - servers
        - STProxyServer**
        - nodeagent
      - srv3STMNode1(NodeDefaultSSLSettings)
    - clusters
    - nodegroups
      - DefaultNodeGroup
    - meeting\_service\_bus
- Outbound

**Specific SSL configuration for this endpoint**

Override inherited values

SSL configuration  
CellDefaultSSLSettings

Certificate alias in key store  
default  and then select New Alias from List

# Sametime Media Server – A/V TLS



- ▶ Der Media Server verwendet automatisch **TLS** für die **SIP Registrierung**
- ▶ **Probleme** bei der SIP Registrierung via TLS

*„Unable to initialize Computer, and it can't be used at this time. com.ibm.collaboration.realtime.telephony.softphone.SIPPhoneException: Processed unsuccessful response: SIP/2.0 500 Server Internal Error.....“*

- ▶ Probleme mit SSL Schlüsseln (WAS Multi Zellen Konfiguration)
- ▶ Performance Probleme (Anmeldung) an „Leitungsschwachen“ Standorten (z.B. China)
- ▶ Performance Probleme bei Sametime Clients 8.5.0 und 8.5.1
  - ▶ [Technote Enabling interoperability of A/V functionality with 8.5.0 / 8.5.1 Sametime client](#)
- ▶ Probleme bei der SUT „light“ Anbindung an SIP „trunk“ (reactivate after config)
  - ▶ [Sametime Client Deployment: Audio / Video Considerations](#)

## ▶ Workaround – Deaktivierung TLS

- ▶ [Disabling SIP security](#)

# Sametime Media Server – A/V TLS disable



- ▶ ISC > Applications > WebSphere enterprise applications > IBM Lotus SIP Registrar > **Security Role mapping**
  - ▶ Security role „AllAuthenticatedUsers“ auf EVERYONE ändern



# Sametime Media Server – A/V TLS disable



## ➤ Media Server Konfiguration von TLS auf TCP ändern

- ▶ ISC oder direkt in der StAVconfig.xml
- ▶ SIP\_ProxyReg\_Secure > SIP\_ProxyRegHost (notieren)
  - ▶ Port 5081 auf 5080

<a href="#">SIP_ProxyRegHOST</a>	*	5080
<a href="#">SIP_ProxyReg_SECURE</a>	*	5081

- ▶ SIP\_DEFAULTHOST\_SECURE > SIP\_DEFAULTHOST (notieren)
  - ▶ Conference Manager Port

<a href="#">SIP_DEFAULTHOST</a>	*	5063
<a href="#">SIP_DEFAULTHOST_SECURE</a>	*	5062

- ▶ SRTP deaktivieren
  - ▶ TLS > TCP
  - ▶ Port 5081 > 5080

SIP-Proxy-Registrar

\*Hostname: w28-an-sttest.edcomtest.local

\*Port: 5080

\*Übertragungsprotokoll: TCP

Ablauf der Sitzung: 150

Wird verwendet, um zu steuern, wie oft Nachrichten an d  
überprüfen (30 bis 300 s).

Audio-/Video-Medien

Anmerkung: Der TLS-Transport empfiehlt sich bei der Verwendung der Datenträger

SRTP-Verschlüsselung (SRTP, Secure Real-time Transport Protocol) sichern:

Inaktivieren

Aktivieren: Anrufe zwischen dem Verbindungsclient und jedem anderen Endp  
Verbindungsclients oder einer Partnerkonferenzbrücke) werden verschlüsselt. Te  
die den Media Manager Packet-Switcher oder den SUT Media Server verwenden,

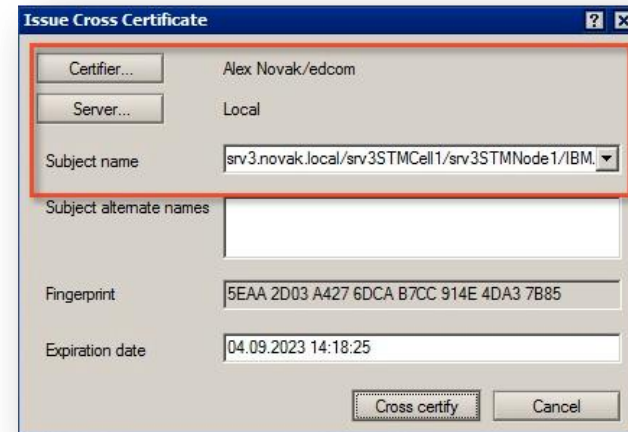
## ➤ Alle Media Server Komponenten neu starten

# Sametime Meeting Server

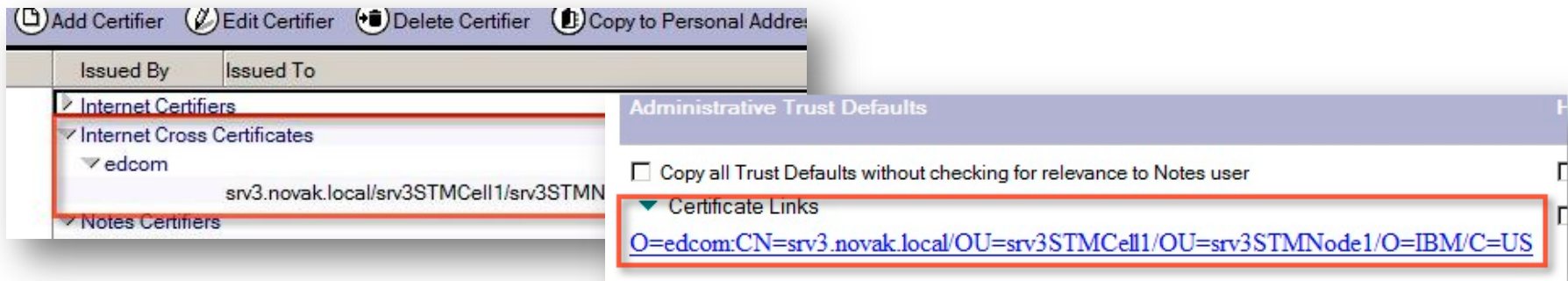
## SSL Zugriffe im Notes Client

- Öffnet ein Notes „**embedded**“ Sametime **Client** per **SSL** auf den **Meeting Server** zu erscheint beim allersten Zugriff ein **Querzulassungsfenster**

- ▶ TRUST Meeting SSL Cert



- Zertifikat per Notes Policy (Security Setting) verteilen



# Sametime

## Websphere Logs/Debug

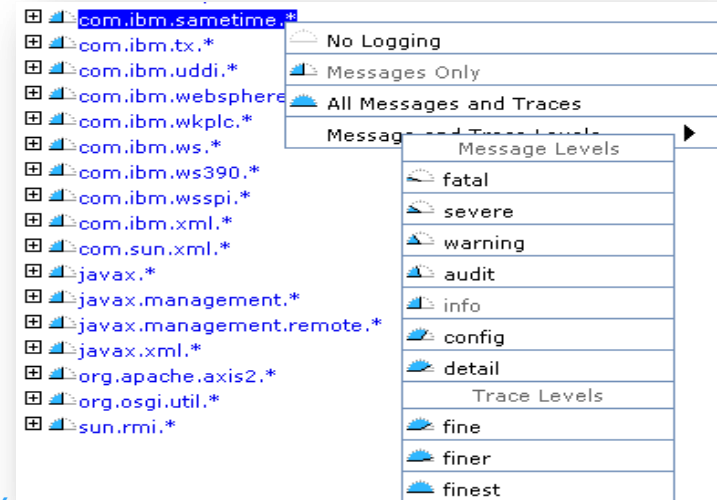


### ➤ Server Protokolle

- ▶ ...\- Startserver.log / Stopserver.log
- Systemout.log / Systemerr.log
- Trace.log (Bei aktiviertem debugging)

### ➤ Debug erweitern

- ▶ ISC > Troubleshooting
  - > Logs & Trace > Change log detail levels
    - ▶ **Configuration** → wird **dauerhaft** nach Neustart aktiv
    - ▶ **Runtime** → nur für **Laufzeit** /nach dem Neustart inaktiv



### ➤ Protokoll Sprache ist OS Sprache

- ▶ OS Sprache oder WAS Sprache ändern
- ▶ ISC > dmgr/node/server > Process definition > JVM > Generic JVM-Argumente
  - ▶ Parameter hinzufügen **-Duser.language=en -Duser.region=GB**

```
Generische JVM-Argumente  
-Dclient.encoding.override=UTF-8 -Duser.language=en -Duser.region=GB
```





- ▶ Bei Anmeldeproblemen empfiehlt es sich ein **SEHR detailliertes Debugging** für die Fehlersuche zu aktivieren

- ▶ ISC > Troubleshooting > Logs & Trace > Change log detail levels

- ▶ **Configuration** → wird **dauerhaft** nach Neustart aktiv
- ▶ **Runtime** → nur für **Laufzeit** /nach dem Neustart inaktiv

- ▶ *\*=info:*

- com.ibm.websphere.security.\*=finest:*

- com.ibm.ws.security.\*=finest:*

- com.ibm.ws.wim.\*=finest:*

- com.ibm.wsspi.wim.\*=finest:*

- com.ibm.websphere.wim.\*=finest:*

- SASRas=finest*





# Sametime „speed geeking“

## ▶ Meeting Server URL (*Meeting Fix Mai 2013*)

- ▶ `meetingroomcenter.useUUIDBasedURL = TRUE`

## ▶ Sametime Mobile Access

- ▶ Fehlermeldung „**Username oder Password falsch**“
- ▶ Prüfung ob „**Allow mobile Client**“ in der ST Policy aktiviert ist !!

## ▶ HTTP auf HTTPS umleiten (Websphere)

- ▶ *Redirect kann nur im Websphere Proxy eingerichtet werden*
- ▶ URI (/\*) Dokument und „virtual host“ (port 80 mapping) erstellen
- ▶ Port 80 mapping in den „klassischen“ hosts löschen
- ▶ Websphere Proxy und Routing Rules erstellen

## ▶ Sametime 8.5.2 Websphere Performance Tuning

- ▶ [Sametime Tuning Guide](#)

## ▶ Windows 2008 & Windows 7 ignorieren RoundRobin DNS

- ▶ Default = RFC 3484 (Erreichbarkeit der „nächsten“ IP laut Priorität)

talk nerdy to me.



**General Properties**

- \* Name: nonSSL2SSL
- Enable this rule
- \* Name of the Virtual Host: proxy\_https\_host
- \* URI group: https\_uri\_group

**Routing action**

- Generic Server Cluster (none)
- Failure Status Code
- Redirect URL: \*.com:443/stmeetings

# Sametime Resources



› [Noviblog.net](#)

› [Lotus Sametime Wiki](#)

› [Lotus Sametime 8.5 Information Center](#)

› [Lotus Sametime Forum](#)

› [Sametime BLOG](#)





**Alexander Novak**  
Senior Consultant  
Germany  
Floor: 4 | Office: +49-89-384085-0  
+49-89-384085-0  
alexander.novak@edcom.de

**Beurteilung bitte nicht vergessen!**

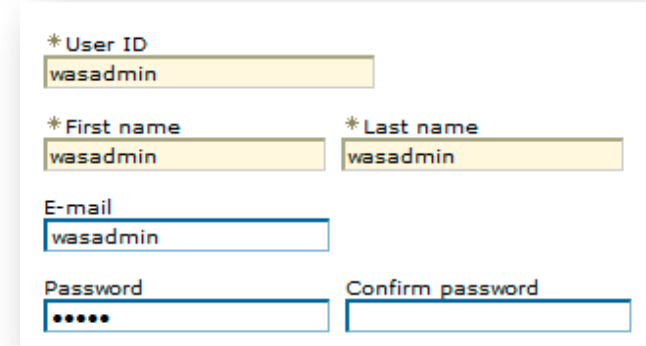
**IBM Sametime 8.5.x / 9.x  
im Umgang mit IBM Websphere**

# Appendix

## Change Websphere Admin (wasadmin) Password

### ➤ Websphere Admin Password

- ▶ ISC > Users & Groups -> [Manage Users](#)
- ▶ wasadmin suchen in editieren
- ▶ Password ändern



\* User ID  
wasadmin

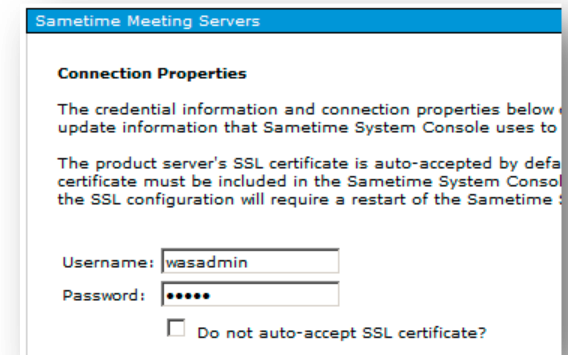
\* First name wasadmin \* Last name wasadmin

E-mail  
wasadmin

Password Confirm password  
.....

### ➤ Sametime „deployment“ Password (SSC)

- ▶ ISC > Sametime System Console > Sametime Servers > Deployment name > [Connection Properties/Edit](#)
- ▶ Password ändern



Sametime Meeting Servers

**Connection Properties**

The credential information and connection properties below update information that Sametime System Console uses to

The product server's SSL certificate is auto-accepted by default. If a custom certificate must be included in the Sametime System Console, the SSL configuration will require a restart of the Sametime

Username: wasadmin

Password: .....

Do not auto-accept SSL certificate?

### ➤ Installation Manager Password

- ▶ C:\ProgramData\IBM\Installation Manager\installRegistry.xml
- ▶ C:\ProgramData\IBM\Installation Manager\installed.xml
- ▶ Hashwert direkt eintragen
  - ▶ Passworthashes Encode Tool „generateEncodedPassword“

# Appendix

## *Change Websphere Admin (wasadmin) Password*

- ▶ Damit die „nodes“ weiterhin sich mit der Zelle verbinden muss zusätzlich des WASAdmin Kennwort in der security.xml geändert werden...
  - ▶ .../WASroot/profiles/dmgr/config/cells/<cellname>/security.xml
  - ▶ `<userRegistries xmi:type="security:WIMUserRegistry" xmi:id="WIMUserRegistry_1" serverId="sscadmin" serverPassword="{xor}MTArOiw=" realm="defaultWIMFileBasedRealm" ignoreCase="true" useRegistryServerId="false" primaryAdminId="sscadmin" registryClassName="com.ibm.ws.wim.registry.WIMUserRegistry"/>`
- ▶ und manuell mit dem Deployment Manager (dmgr) verbinden
  - ▶ `../WASroot/profiles/node/bin/syncnode ssc.novitest.local 8703`