Blick auf Jabber

Instant Messaging != „Chat” (1)

Presence

Instant Messaging != „Chat” (2)

/query

Instant Messaging != „Chat” (3)

Viele Erweiterungen

Globale Adressierung (1)

domain

Globale Adressierung (2)

user@domain

(Bare Jabber-ID)

Globale Adressierung (3)

user@domain/resource

(Full Jabber-ID)

Globale Adressierung (4)

domain/resource

Standardisierung

XMPP

- RFC 3920: XML streams, SASL, TLS, stringprep profiles, stanza semantics
- RFC 3921: XMPP extensions for basic instant messaging and presence
- RFC 3922: Mapping XMPP to the IETF's CPIM specifications
- RFC 3923: End-to-end signing and object encryption for XMPP
- RFC 4622: A Uniform Resource Identifier (URI) scheme for XMPP
- RFC 4854: A Uniform Resource Name (URN) tree for use in XMPP extensions
- RFC 4979: IANA registration of an Enumservice for XMPP
- 228 XMPP Enhancement Proposals

SILC

- White Paper
- draft-riikonen-silc-spec-09
- draft-riikonen-silc-pp-09
- draft-riikonen-silc-ke-auth-09
- draft-riikonen-silc-commands-07
- draft-riikonen-silc-flags-payloads-04
- draft-riikonen-silc-multimedia-session-00
- draft-riikonen-presence-attrs-04

Implementationen

Jabber Clients

Adium X, Akeni, BitlBee, Bombus, BuddySpace, centericq, Chatopus, Chatterbox, CJC, Claros Chat, Coccinella, Colibri, dziobber, ekg2, elechat, EntreatCE, Exodus, Eyeball, Fire, Gabber1, Gabber2, Gajim, GCN, Gnome Jabber, GNU Gadu, GOIM, Gossip, gYaber, iChat AV, IM +, imov, IR-Jabber, IRSIM, Jabber, jabber.el, JabberApplet, JabberFoX, JabberMixClient, Jabbernaut, Jabberwocky, Jabberzilla, Jabbin, jaIMy, JAJC, JBother, JClaim, Jeti, JWChat, JWGC, Kava, kf, KomKom, Kopete, Laffer, LinQ, Lluna, M2, mcabber, Meebo, Meetro, MessageMate, MirandaIM, mobber, myJabber, myJabber IM for Pocket PC, neos, NewtonIM, ngIM, Nostromo, OctroTalk, Pandion, Papla Mobile, Papla PC, Pidgin, Piorun, Psi, sendxmpp, SIM-IM, SoapBox, SoapBox Communicator, Spark, Spik, TipicIM, TipicMe, Tkabber, TransactIM, Trillian Pro, Vayusphere XMPP Solution for RIM Blackberry, WannaChat, WhisperIM, wija, Wippien, Wokjab, Wooden Fish Messenger, wpkontakt, xeus messenger, XIFFIAN

Jabber Servers

Antepo OPN, CommuniGate Pro, ejabberd, Jabber XCP, jabberd 1.x, jabberd 2.x, Merak, Openfire, OpenIM, psyced, SoapBox Server, Sun Java System Instant Messaging, Tigase, TIMP.NET, xmppd.py

Jabber Libraries

agsXMPP, ATE Client Library, ATE Component Library, Beep, cl-xmpp, Class.Jabber.PHP, Echomine Feridian, Echomine Muse, gloox, hsxmpp, iksemel, IP*Works, Iris, Jabber Class, Jabber-Net, jabber.py, Jabber4R, Jabber::Connection, Jabber::Lite, JabberBeans, JabberCOM, Jabberlang, JabberLib, jabberoo, Jabberoo WinCE Port, JabberWookie, JabXPCOM, JOPL, JSJaC, JSO, JXA, libstrophe, Loudmouth, micro-jabber, myMatrix XMPP Com Library, Net::Jabber, Net::Jabber::Loudmouth, Net::XMPP, Net::XMPP2, oajabber, PyXMPP, Smack, SoapBox Framework Desktop Edition, SoapBox Framework Mobile Edition, SoapBox Framework Mono Edition, SoapBox Framework Web Service, tweeze, Twisted Words, XIFF, XML::Stream, XMPP Client Daemon, xmpp4moz, XMPP4R, xmpppy, Yaja

SILC Clients

SILC Client, Silky, Colloquy, GAIM, Kopete, Silsa

SILC Servers

SILC Server

SILC Libraries

SILC Toolkit, Garbledina, Crabadonk

XML-Stream (1)

Client

```
<stream:stream
   to='example.com'
   xmlns='jabber:client'
   xmlns:stream='http://etherx.jabber.org/streams'
   version='1.0'>
```

```
<!-- TLS, Compression, SASL, ..., Binding -->
```

```
<presence>
  <status>I'm on Jabber!</status>
</presence>
```

Server

```
<stream:stream
   from='example.com'
   id='someid'
   xmlns='jabber:client'
   xmlns:stream='http://etherx.jabber.org/streams
   version='1.0'>
```

```
<!-- ... -->
```

```
<presence from='trudy@example.org'>
  <status>I'm online, too!</status>
</presence>

<presence from='eve@example.net'>
  <show>chat</show>
  <status>I am free for chat</status>
</presence>
```

XML-Stream (2)

Client

```
<message to='trudy@example.org'>
  <body>Guten Tag</body>
</message>

<!-- ... -->

</stream:stream>
```

Server

```
<message from='trudy@example.org/Psi'
         to='mallory@example.com/Gajim'>
  <body>Hallo!</body>
</message>

<!-- ... -->


</stream:stream>
```

Stanzas (1)

<message/>

- @id optional
- @from optional
- @to
- @type = # | "normal" | "chat" | "headline" | "groupchat" | "error"
- thread
- subject
- body

Stanzas (2)

<presence/>

- @id optional
- @from optional
- @to optional
- @type = # | "unavailable" | "probe" | "subscribe" | "unsubscribe" | "subscribed" | "unsubscribed" | "error"
- show
- status
- priority

Stanzas (3)

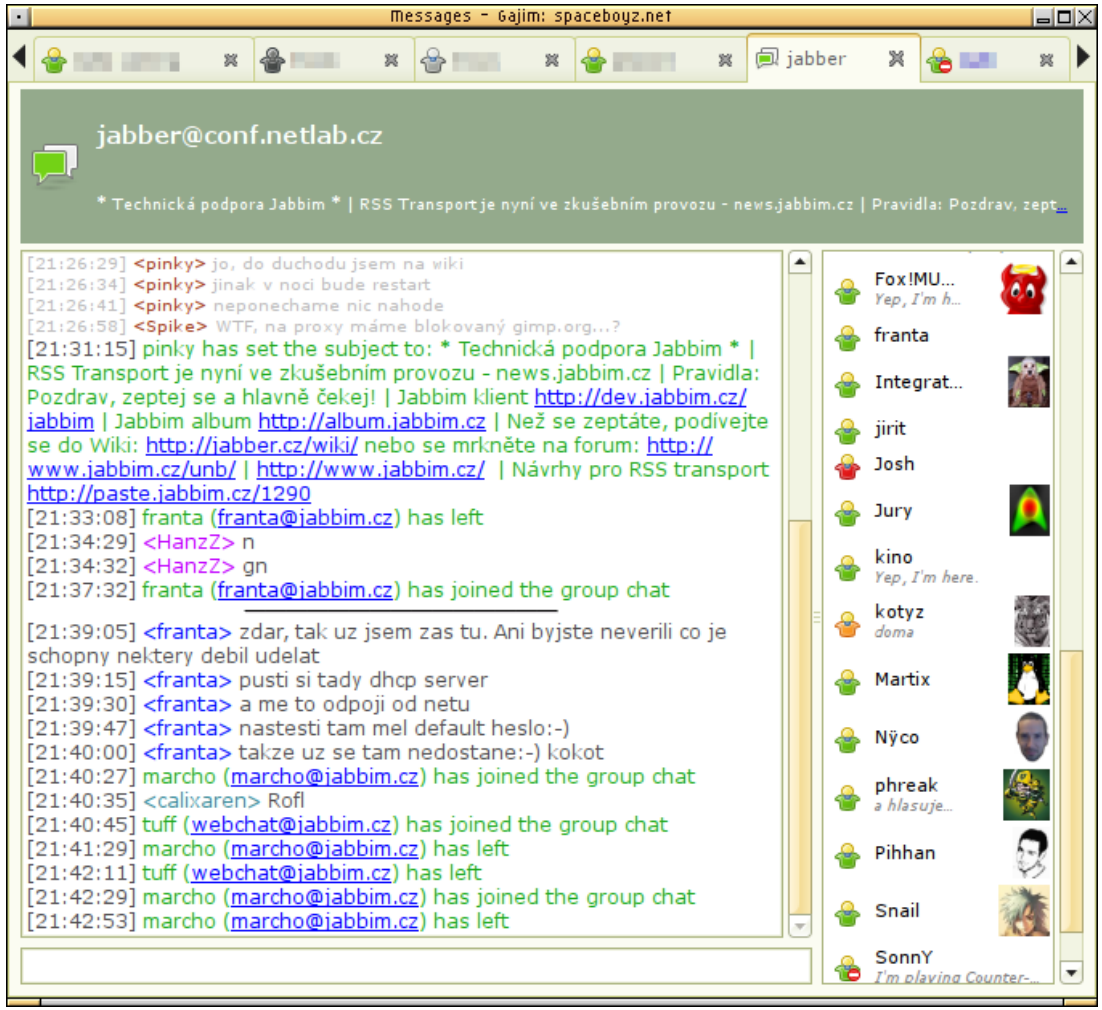
<iq/>

- @id optional
- @from optional
- @to
- @type = "get" | "set" | "result" | "error"

Erweiterbarkeit heisst...

```
<presence from='mallory@example.net/BlacBook'
          to='astro@spaceboyz.net/saturn/gajim'
          id='408'>
  <show>dnd</show>
  <status>Hacking</status>
  <priority>50</priority>
  <x xmlns='vcard-temp:x:update'>
    <photo>
      488cb365e50bc0a126e8cc572e3c5ee0642da024
    </photo>
  </x>
  <c xmlns='http://jabber.org/protocol/caps'
     node='http://gajim.org/caps'
     ext='xhtml cstates' ver='0.11.2'/>
  <x xmlns='jabber:x:signed'>
    hQQNAzw8w3WdMoZBEBAAr0zcttXSJm6nZiD28DB2CFesA/5uLpIZ9pWAaODNuZNk
    fhGtyzO+jiQiod+8E7Nucx2Jd6SvEWviSQCC2Y69CRO0w19/m0HT7dklUQ4lUSOR
    ...
  </x>
</presence>
```

Multi-User Chat (1)



Multi-User Chat (2)

XEP-0045: Multi-User Chat

„No end-to-end message or session encryption method is specified herein. Users SHOULD NOT trust a service to keep secret any text sent through a room.”

Kryptographie in der Praxis

```
Date: Thu, 25 Oct 2007 15:10:39 +0200
From: Frank Benkstein <frank@benkstein.net>
To: c3d2@mail.skyhub.de
Subject: [c3d2] Beamer für SILC-TA
Message-ID: <472095CF.6030202@benkstein.net>


Hallo,

kann sich jemand um einen Beamer für morgen kümmern?  In der BA wird es
wahrscheinlich keinen geben.

Danke
Frank.

--
GPG (Mail): 7093 7A43 CC40 463A 5564  599B 88F6 D625 BE63 866F
GPG (XMPP): 2243 DBBA F234 7C5A 6D71  3983 9F28 4D03 7110 6D51
```

Transport channel encryption

- SSL über Port 5553 (deprecated)
- STARTTLS im XML-Stream auf Port 5552

PGP-Integration (1)

XEP-0027: Current Jabber OpenPGP Usage

```
<presence from='trent@example.net/Psi'>
  <status>Online</status>
  <x xmlns='jabber:x:signed'>
    iQA/AwUBOjU5dnol3d88qZ77EQI2JACfRngLJ045brNnaCX78ykKNUZa...
    2uJxPMGR73EBIvEpcv0LRSy+
    =45f8
  </x>
</presence>
```

PGP-Integration (2)

XEP-0027: Current Jabber OpenPGP Usage

```
<message to='eve@example.net/home' from='trent@example.net/Psi'>
  <body>This message is encrypted.</body>
  <x xmlns='jabber:x:encrypted'>
    qANQR1DBwU4DX7jmYZnncmUQB/9KuKBddzQH+tZ1ZywKK0yHKnq57kW...
    WpdWpR0uQsuJe7+vh3NWn59/gTc5MDlX8dS9p0ovStmNcyLhxVgmqS8...
    ...
    Oin0vDOhW7aC
    =CvnG
  </x>
</message>
```

Off The Record

Plugins für Adium, Pidgin, Kopete

Ciphertext als Base64 im <body/>

E2E Encryption

RFC 3923: End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol

- S/MIME
- Für Interoperabilität mit nicht-XMPP-Systemen: CPIM Message Format (RFC 3862)

Example 9: Sender generates XMPP presence stanza:

```
|   <presence to='romeo@example.net/orchard'>
|     <e2e xmlns='urn:ietf:params:xml:ns:xmpp-e2e'>
|   <![CDATA[
|   Content-Type: multipart/signed; boundary=next;
|                 micalg=sha1;
|                 protocol=application/pkcs7-signature
|
|   --next
|   Content-type: application/pidf+xml
|   Content-ID: <2345678901@example.com>
|
|   <xml version="1.0" encoding="UTF-8"?>
|   <presence xmlns="urn:ietf:params:xml:ns:pidf"
|             xmlns:im="urn:ietf:params:xml:ns:pidf:im"
|             entity="pres:juliet@example.com">
|     <tuple id="hr0zny">
|       <status>
|         <basic>open</basic>
|         <im:im>away</im:im>
|       </status>
|       <note xml:lang="en">retired to the chamber</note>
|       <timestamp>2003-12-09T23:53:11.31Z</timestamp>
|     </tuple>
|   </presence>
|   --next
|   Content-Type: application/pkcs7-signature
|   Content-Disposition: attachment;handling=required;\
|                                   filename=smime.p7s
|
|   [signed body part]
|
|   --next--
|   ]]>
|     </e2e>
|   </presence>
```

ESessions (1)

XEP-0210: Requirements for Encrypted Sessions

- Security Requirements: Confidentiality, Integrity, Replay Protection, Perfect Forward Secrecy, PKI Independence, Authentication, Identity Protection, Repudiability, Robustness, Upgradability
- Application Requirements: Generality, Implementability, Usability, Efficiency, Flexibility, Offline Sessions, Interoperability, Object Encryption
- However, both many-to-many sessions and one-to-many broadcast are deemed out-of-scope for this document.

ESessions (2)

XEP-0116: Encrypted Session Negotiation

SIGMA: the 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and its Use in the IKE Protocols

ESessions (3)

XEP-0188: Cryptographic Design of Encrypted Sessions

The conceptual model for the approach specified in this document was inspired by "off-the-record" (OTR) communication [...]

ESessions (4)

XEP-0200: Stanza Encryption

```
<presence from='alice@example.org/pda'
          to='bob@example.com/laptop'
          type='available'>
  <c xmlns='http://www.xmpp.org/extensions/xep-0200.html#ns'>
    <data> ** Base64 encoded m_final ** </data>
    <mac> ** Base64 encoded a_mac ** </mac>
  </c>
</presence>
```

ESessions (5)

XEP-0217: Simplified Encrypted Session Negotiation

The cut-down protocol described here is a 4-message key exchange (see useful summary of 4-message negotiation) with short-authentication-string (SAS), hash commitment and optional retained secrets. It avoids using public keys - thus protecting the identity of both participants against active attacks from third parties.

ESessions (6)

XEP-0218: Bootstrapping Implementation of Encrypted Sessions

Approach:

- XEP-0218: Best Practices for Message Threads
- XEP-0155: Stanza Session Negotiation
- XEP-0200: Stanza Encryption
- XEP-0217: Simplified Encrypted Session Negotiation
- XEP-0116: Encrypted Session Negotiation
- XEP-0188: Cryptographic Design of Encrypted Sessions
- (XEP-0189: Public Key Publishing)
- (XEP-0187: Offline Encrypted Sessions)
- (XEP-0136: Message Archiving)

ESessions (7)

XEP-0219: Hop Check

```
<iq type='result' from='capulet.lit'
    to='juliet@capulet.lit/balcony' id='check1'>
  <hopcheck xmlns='http://www.xmpp.org/extensions/xep-0219.html#ns'
            from='juliet@capulet.lit/balcony'
            to='romeo@montague.lit/orchard'>
    <hop from='juliet@capulet.lit/balcony' to='capulet.lit'
         auth='DIGEST-MD5' encrypted='true'/>
    <hop from='capulet.lit' to='montague.lit'
         ip='192.0.2.1' delay='11.602'
         auth='EXTERNAL' encrypted='true'/>
    <hop from='montague.lit' to='romeo@montague.lit/orchard'
         delay='15.734' auth='PLAIN'
         encrypted='true'/>
  </hopcheck>
</iq>
```