



Jabber/XMPP: 25 Years of Digital Independence

LinuxDays 2026

Daniel Gultsch

✉ daniel@gultsch.de

🏠 gultsch.de

🔗 codeberg.org/iNPUTmice

🐦 [@daniel@guiltsch.social](https://social.gultsch.de/@daniel@guiltsch.social)

About me



- Open standards
 - IETF
 - XMPP Standards Foundation (XSF)
- Android app developer
 - Conversations (Jabber/XMPP client)
 - Ltt.rs (email client)
 - UnifiedPush

Thesis

Open source is necessary, but not sufficient for digital sovereignty.

What Open Source provides

- Protection against spyware
- Verifiable cryptography
- Code that can be inspected and understood

What Open Source does not provide

- Protection against service shutdown
- Protection against sanctions
- Protection against regional blocks
(Signal threatened to withdraw from the EU if chat control is put into law)
- Protection against the operator's arbitrary decisions
(TOS, “rug pull”, ...)

Thesis

Genuine sovereignty requires complete interchangeability.

Sovereignty

- Ability to switch server providers
 - Still able to communicate with others
 - Federated Identities (user@example.com)
- Interchangeability of the software
 - Client
 - Server
- **Any vendor can be replaced at any time**

Thesis

A publicly documented API is not, by itself, an open standard.

Standards Developing Organization (SDO)

- ISO, IETF, W3C, Unicode Consortium
- IETF standards: DNS, HTTP, JSON, TLS 1.3, SSH
- Not a standard: Simple Storage Service (S3)
- **Broad consensus among independent parties**

Extensible Messaging and Presence Protocol (XMPP)

RFC 6120 & RFC 6121



- RFC 3920, RFC 3921 (October 2004)
- RFC 6120, RFC 6121 (March 2011)
- Extensions ⇒ XMPP Standards Foundation (XSF)
- XSF: Members elect Council and Board
- Rules to prevent any company from dominating
- Adaptability
- 518 extensions. 142 Stable, Final, Active

2014 - 2016

Leap into the mobile age

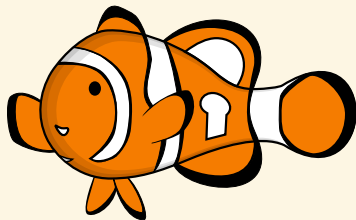
Reliability, network switching, battery saving

- XEP-0198: Stream Management
 - Packets (messages, ...) are individually acknowledged by the server
 - Resumption after a connection change
- XEP-0352: Client State Indication

Support for multiple devices

- Messages to all devices (XEP-0280: Message Carbons)
- Offline messages (XEP-0313: Message Archive Management)
- Sending files to multiple (offline) devices (XEP-0363: HTTP File Upload)
- P2P file transfer remains possible

End-to-end encryption



- XEP-0384: OMEMO Encryption
- “Signal encryption” (WhatsApp, Google Duo, ...)
- Encrypts text and files
- Multiple devices

Status quo

Notable features from recent years

Extensible SASL Profile (SASL2), Bind 2 and FAST

- Direct TLS
- Authenticated and fully connected in one round trip
- Hashed Token instead of SCRAM (IETF Kitten WG)
- Broad adoption across the ecosystem
(Prosody, ejabberd, Openfire, MongooselM, Tigase¹)

¹excluding Hashed Token

Channel Binding

Encrypted traffic interception on Hetzner and Linode targeting the largest Russian XMPP (Jabber) messaging service

WABR22 3rd November 2023 at 9:17pm

TL;DR: we have discovered XMPP (Jabber) instant messaging protocol encrypted TLS connection wrapping (Man-in-the-Middle attack) of jabber.ru (aka.xmpp.ru) service's servers on Hetzner and Linode hosting providers in Germany. The attacker has issued several new TLS certificates using Let's Encrypt service which were used to hijack encrypted STARTTLS connections on port 5222 using transparent MTM proxy. The attack was discovered due to expiration of one of the MTM certificates, which haven't been renewed. There are no indications of the server breach or spoofing attacks on the network segment, quite the contrary: the traffic redirection has been configured on the hosting provider network.

The wiretapping may have lasted for up to 6 months overall (90 days confirmed). We believe this is lawful interception Hetzner and Linode were forced to setup.

Last update: 03 Nov 2023

Introduction

`@rpa`, experienced UNIX administrator who is in charge for the oldest Russian XMPP service `jabber.ru` established in year 2000, was puzzled by "Certificate has expired" message upon connecting to the service on 16 October 2023. All the certificates seemed to be up-to-date on the server, but the connection to port 5222 (XMPP STARTTLS) was presenting an outdated certificate to the client.

During all kinds of software, network and configuration checks with the help of other professionals and `ejabberd` software author, it was discovered that:

- The software serves proper, non-expired certificate in the network traffic
- The expired certificate is not present on the server
- It is based on other private key and was never issued by the server's `acme.sh` certificate issuing script
- Incoming TCP connections to port 5222 are altered: they have different source port, SEQ/ACK numbers, and appear to arrive without any intermediate routing hops (TTL=64).
- This behavior is not observed on other, non-5222 ports, such as 5223 XMPP TLS port

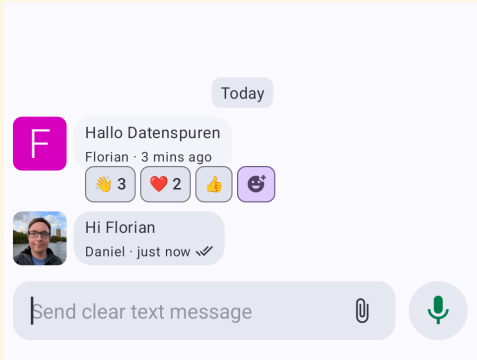
The affected machines are dedicated server on Hetzner and two virtual servers on Linode, all hosted in Germany.

Source	Destination	Protocol	Length	Info
172.184.234.182	172.184.234.182	TCP	60	40808 -> 5222 [RST] Seq= 952154533
172.184.234.182	172.184.234.182	TCP	60	5222 -> 40808 [RST] Seq= 172184234
172.184.234.182	172.184.234.182	TCP	60	40808 -> 5222 [ACK] Seq= 172184234

Source	Destination	Protocol	Length	Info
95.215.45.33	172.184.234.182	TCP	60	40808 -> 5222 [RST] Seq= 952154533
172.184.234.182	95.215.45.33	TCP	60	5222 -> 40808 [RST] Seq= 172184234
172.184.234.182	95.215.45.33	TCP	60	40808 -> 5222 [ACK] Seq= 172184234

- Provider-level MitM
- ACME request intercepted. Valid Let's Encrypt certificates
- SCRAM- $\star$ -PLUS $\Rightarrow$ Same TLS session at both ends

Emoji Reactions



- XEP-0444: Message Reactions
- Conversations, converse.js, Gajim, Dino, Movim, poezio, Psi

Moderation

- XEP-0425: Moderated Message Retraction
- Combating spam in “public channels”
- Requires server support
- Ban + delete all messages in one step (client-side)

Hats



ralphm

Owner

XSF member

Board



Ge0rG

Admin

XSF member

Mod



jonas'

Admin



singpolyma

Admin

Council

XSF member

Mod



alexkurisu

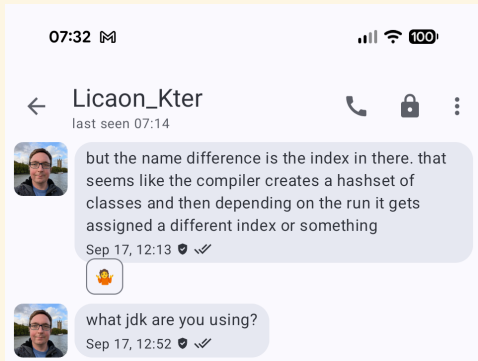
Member

- XEP-0317: Hats
- Organisational roles, not technical roles

Multi-device synchronisation of read status

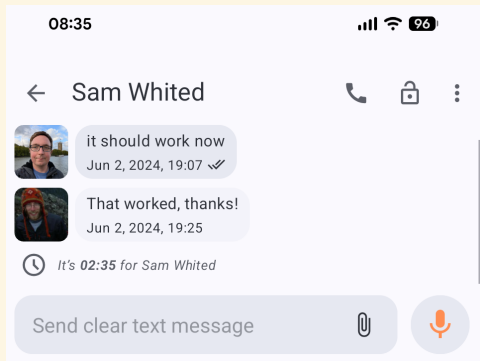
- XEP-0333: Displayed Markers
 - Lets contact(s) know that a message has been read
 - Can be turned off (for privacy reasons)
 - Often disabled in large groups
- XEP-0490: Message Displayed Synchronization

Last seen



- XEP-0319: Last User Interaction in Presence
- Gajim, converse.js, Monal, Conversations, Movim, poezio
- „off by default“ in Conversations

Time zone display for contacts



- XEP-0202: Entity Time, March 2007
- Responding to requests is widely supported.
- New way of displaying time zones since 2025

Implementation tracking

Software Specifications Community Getting Started News Jobs

no event found

New XEPs

[XEP-0318](#) Payment Required
[XEP-0317](#) Angle Synchronized Real-Time Text
[XEP-0316](#) XMPP Decentralized ID (XID)
[XEP-0315](#) TLS Channel-Binding Downgrade Protection
[XEP-0314](#) Error Markup

Recently Updated XEPs

[XEP-0315](#) TLS Channel-Binding Downgrade Protection
[XEP-0318](#) Payment Required
[XEP-0034](#) User Avatar
[XEP-0040](#) Message Displayed Synchronization
[XEP-0066](#) Out of Band Data

The whole list

The XMPP Standards Foundation develops extensions to XMPP in its XEP series. This page lists Stable and Final XEPs as well as experimental proposals that are currently under consideration.

XEP series data can be explored using [data.xmpp.net/explore](#).

Good places for developers to start are the [compliance suites](#), as well as the [technology overview](#) pages. For further reading, we suggest the independent [Modern XMPP project](#) which attempts to improve the quality of user-to-user messaging applications that use XMPP.

The following table is sortable, just click on the headers (click twice to reverse the sort order).
You can show/hide the various types of XEPs by applying filters via the Filter button below.

Search by number, name, short name or tag...

Filter XEPs

Filter XEPs

Only checked types will be shown

☐ Proposed ☒ Stable ☒ Final ☐ Active

☐ Deprecated ☐ Obsolete ☐ Rejected ☐ Retracted

☐ Experimental ☐ Deferred ☒ Dormant

☒ Dormant XEPs in Experimental/Deferred are hidden. Check Dormant to show all Experimental/Deferred XEPs.

Showing 91 of 518 XEPs (2 filters active)

Number	Name	Type	Status	Date	Tags	Implementations
XEP-0004	Data Forms (x-data)	Standards Track	Final	2004-08-20		46
XEP-0009	Jabber-RPC (xm-rpc)	Standards Track	Final	2007-09-04		6
XEP-0012	Last Activity (x-last)	Standards Track	Final	2008-11-26		20
XEP-0030	Service Discovery (x-service)	Standards Track	Final	2004-04-30		93
XEP-0032	Extended Stanza Addressing (x-addr)	Standards Track	Stable	2007-05-15		10
XEP-0045	Multi-User Chat (x-muc)	Standards Track	Stable	2006-06-05		93

XEP-0030: Service Discovery

Last XEP revision: Version 2.5.0 (2024-04-30)

Name	Status	Since Version	XEP Version
Artalk.Xmpp	✓	2.0.0	2.5.0
AstraChat XMPP Client	-	-	-
AstraChat XMPP Server	-	-	-
afalk	✓	0.5.8	2.5.0
Beagle IM	✓	-	2.5x3
Brute	✓	-	2.5x3
Cheogram Android	✓	-	2.5x3
Conversations	✓	-	2.5x3
Converse.js	✓	0.6.2	-
CoyIM	✓	-	-
cz-xmpp	✓	-	-
Dino	✓	0.1	-
egabberd	✓	0.10	2.5.0
ElangElkor XMPP	-	-	2.5.0
Ethara	✓	-	-
Fluxus Messenger	✓	-	-
Gajim	✓	-	2.4
Hatizen	✓	-	2.5x3
Jabber.al	✓	-	2.5.0
JaxXMPP	✓	-	2.5x3
Kalden	✓	0.2	2.4
Likewise	✓	-	2.5.0
Martin	✓	-	2.5x3
Metronome IM	✓	-	2.4
Moranda NG	-	-	-
Murai IM	✓	4.6	2.5.0
MongooseIM	✓	-	2.5.0
monocles chat	✓	-	2.5x3
Movim	✓	-	2.5
moxxmpp	✓	-	2.5x3
Moxy	✓	-	2.5x3

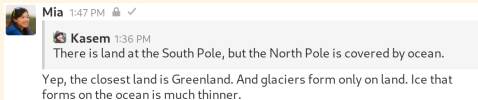
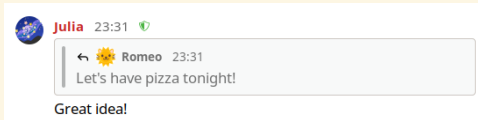
xmpp.org/extensions

Looking ahead

Upcoming protocol developments

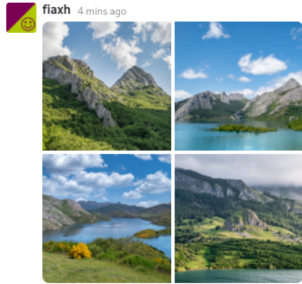
- XEP-0420: Stanza Content Encryption
- Specified Double Ratchet (previously: use libsignal-protocol)
- More robust. 10 years of experience OMEMO

Message Replies



- XEP-0461: Message Replies
- Gajim, Dino, Movim, converse.js

Galerie / Multi-Image-Sharing



- XEP-0447: Stateless file sharing
- With thumbnails
- Requires OMEMO 2

OAuth integration



- Web client sign-in
- Central user management (Keycloak)
- XMPP Sprint London, November 2026

XMPP 2.0

Back to the IETF



- Update the core RFC
(Setting up the connection looks completely different)
- Combine popular XEPs
- Side Meeting IETF 126 Vienna
- BoF IETF 128 Kuala Lumpur
(non-working group forming?)

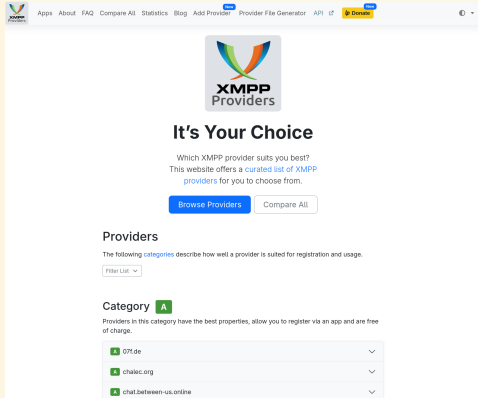
Giving it a try

Clients, provider, self hosting

Clients

- Linux ⇒ Dino (oder Gajim)
- Windows ⇒ Gajim
- Android ⇒ Conversations
- iPhone ⇒ Monal

Provider



The screenshot shows the homepage of the XMPP Providers website. The navigation bar at the top includes links for Apps, About, FAQ, Compare All, Statistics, Blog, Add Provider, Provider File Generator, API, and a Compare button. The main heading is "It's Your Choice", followed by a subheading "Which XMPP provider suits you best?". Below this, a paragraph states: "This website offers a [curated list of XMPP providers](#) for you to choose from." There are two buttons: "Browse Providers" (highlighted in blue) and "Compare All". Under the "Providers" section, a note says: "The following [categories](#) describe how well a provider is suited for registration and usage." Below this is a "Filter List" dropdown menu. The "Category A" section lists providers with the best properties, allowing registration via an app and being free of charge. The listed providers are: 071.de, chalc.org, and chat.between-us.online.

Apps About FAQ Compare All Statistics Blog Add Provider Provider File Generator API [Compare](#)



It's Your Choice

Which XMPP provider suits you best?
This website offers a [curated list of XMPP providers](#) for you to choose from.

[Browse Providers](#) [Compare All](#)

Providers

The following [categories](#) describe how well a provider is suited for registration and usage.

[Filter List](#) ▾

Category **A**

Providers in this category have the best properties, allow you to register via an app and are free of charge.

 071.de	▾
 chalc.org	▾
 chat.between-us.online	▾

- conversations.im (in band registration)
- providers.xmpp.net
- Hackspace

- Prosody
- ejabberd

Questions?

joinjabber.org · xmpp.org