

Tuomas Virtanen

# XMPP-pikaviestinprotokolla

Tietotekniikan  
kandidaatintutkielma  
27. marraskuuta 2010

Jyväskylän yliopisto

Tietotekniikan laitos

Jyväskylä

**Tekijä:** Tuomas Virtanen

**Yhteystiedot:** tuomas.virtanen@jyu.fi

**Työn nimi:** XMPP-pikaviestinprotokolla

**Title in English:** XMPP-Protocol

**Työ:** Tietotekniikan kandidaatintutkielma

**Sivumäärä:** ??

**Tiivistelmä:** XMPP on monipuolinen ja laajennettavissa oleva, avoimiin standardeihin perustuva pikaviestinprotokolla. Sitä voidaan käyttää paitsi puhtaiden tekstiviestien lähettämiseen ja olotilan tarkkailuun, myös esimerkiksi tiedostonsiirtoihin ja VoIP-puheluihin. Tässä tutkielmassa tutustutaan protokollan teknisiin ominaisuuksiin ja tehdään vertailuja muihin pikaviestinprotokolleihin.

**English abstract:** XMPP is a versatile and extensible instant messaging protocol based on open standards. It can be used for eg. sending text messages and presence information, VoIP-calls and file transfers. This thesis examines the technical aspects of the protocol, and makes comparisons to other instant messaging protocols.

**Avainsanat:** XMPP, protokolla, pikaviestintä

**Keywords:** XMPP, Protocol, instant messaging

## Sisältö

# 1 Johdanto

Pikaviestinnästä on tullut osa useiden tietokoneen, ja vähitellen myös erilaisten mobiililaitteiden käyttäjien arkea. Pikaviestintää käytetään niin kotona, koulussa ja töissä. Erilaisia pikaviestin-ohjelmia on useita, ja viestintää voidaan harrastaa joko perinteisesti tekstiviestein, tai monipuolisemmin äänen ja videon avulla. WWW-ohjelmointitekniikoiden edistyessä pikaviestimiä löytyy jopa erilaisilta www-sivuilta, josta hyvänä esimerkkinä toimii mm. Facebook-palvelu.

Erilaisten pikaviestinsovellusten tullessa markkinoille, syntyy myös uusia viestintäprotokollia ja määritelmiä näiden sovellusten käyttöön. Tästä johtuukin nykymallin mukaisen pikaviestinnän suurin ongelma; eri pikaviestinverkkoihin tarvitaan usein eri ohjelmat. Samalla käyttäjällä saattaakin olla käytössä useita ohjelmia, jotka toimivat omissa viestintäverkoissaan. Yrityksiä yhdistää eri pikaviestinverkkoja saman ohjelman käyttöön on olemassa, mutta kaikki näistä ovat eri syistä epätäydellisiä.

Usein ongelmana pikaviestintäprotokollien toteuttamisessa on se, että pikaviestinverkon protokolla on jollain tavalla suljettu. Protokolla voi olla suljettu esimerkiksi lisenssiehdoiltaan, joilla sen käyttöä rajoitetaan muiden kuin sille suunnitellun ohjelman käyttöön. Protokollan määritelmä voi olla suljettu ja itse protokolla voi olla salattu jollain salausalgoritmilla. Esimerkiksi MSN Messenger-ohjelman käyttämän MSNP-protokollan määritelmä ei ole julkinen. Skype-pikaviestinohjelman käyttämä protokolla taas on täysin salattu [?] Rijndael-algoritmilla. Tällaisten ohjelmien käyttämiä protokollia ei voida toteuttaa muihin pikaviestimiin ilman protokollan purkua, joka esimerkiksi Skypen tapauksessa on toistaiseksi ollut menestyksetöntä useista yrityksistä huolimatta.

Extensible Messaging and Presence Protocol (XMPP) pyrkii olemaan mahdollisimman avoin ja laajennettavissa oleva, yleiskäyttöinen protokolla kaikkeen pikaviestintään. Se hallitsee laajennuksia käyttäen mm. tekstiviestit, VoIP-puhelut sekä tiedostojen siirron käyttäjien välillä. XMPP-verkko sallii myös esimerkiksi siltaukset muihin pikaviestinverkkoihin, kuten Internet Relay Chat (IRC). XMPP-protokollaa käyttääkin nykyään jo moni tunnettu yritys sovelluksissaan, kuten mm. Nokia (Nokia Ovi), Google (Google Talk, Google Wave) sekä LiveJournal (LJ Talk).

Kandidaatintutkielma tarkastelee lyhyesti pikaviestintää, ja keskittyy erityisesti XMPP-pikaviestinprotokollaan. Luvussa 2 käsitellään pikaviestintää yleisesti, ja esitellään muutamia sen sovelluksia sekä protokollia. Luvussa 3 esitellään XMPP-protokollaa ja sen rakennetta. Luvussa 4 perehdytään XMPP-verkkoihin ja niiden eroihin muihin pikaviestinverkkoihin nähden. Luvussa 5 esitellään XMPP-protokollan pikaviestintään tarjoamia ominaisuuksia, kuten tekstiviestejä ja olotilan hallintaa.

## 2 Pikaviestintä ja sen protokollat

### 2.1 Pikaviestinnän käsitteitä

Pikaviestinnässä on Wikipedian määritelmän [?] mukaan kyse (lähes) reaaliaikaisesta, tekstipohjaisesta viestinnästä kahden tai useamman ihmisen välillä tietokoneiden tai muiden laitteiden välityksellä. Tiedon siirto tapahtuu Internetin tai muun verkon yli. Pikaviestintä voi monipuolisimmillaan olla myös videon tai äänen välityksellä tapahtuvaa viestintää.

### 2.2 Pikaviestinnän sovellukset

## 3 XMPP-Protokolla

Extensible Messaging and Presence Protocol (XMPP) on avoin, reaaliaikaiseen pikaviestintään ja olotilan ilmoittamiseen tarkoitettu XML-pohjainen standardi. Protokollaa kehitettiin alun perin nimellä Jabber, ja se oli tarkoitettu saman nimiseen, vapaaseen lähdekoodiin perustuvaan pikaviestinohjelmaan. Vuonna 2002 perustettiin XMPP työryhmä (XMPP WG), jonka tehtäväksi tuli Jabber-protokollaan perustuvan pikaviestinprotokollan kehitys. Uuden, XMPP-nimisen protokollan tarkoitus oli soveltaa Internet Engineering Task Forcen (IETF) tukemaksi pikaviestintä- ja olotilan hallinta-protokollaksi. Kehitystyön tuloksena oli lopulta dokumentti, jossa määriteltiin protokollan perusominaisuudet ja laajennukset pikaviestintään. Nykyään tätä perustoiminnallisuutta määritellään RFC-dokumenteissa 3920 ja 3921. Myöhemmin protokollaan on luotu laajennuksia esimerkiksi tiedostojen siirtämiseen sekä VoIP-puheluihin.

### 3.1 Versiot ja ydinstandardi

### 3.2 XML-tietovirrat

XMPP-standardissa liikenne kuljetetaan yleensä XML-tietovirrassa. XML-tietovirtaa voidaan ajatella säiliönä, jota käytetään XML-elementtien kuljettamiseen verkkoyhteisöjen välillä. Virran alku ilmoitetaan aina XML-tagilla «stream>», jossa voidaan määritellä attribuutteina myös esimerkiksi käytettävä nimiavaruus ja nerkistö. Virran loppua merkkää vastakkaisesti tagi «/stream>». Niin kauan kuin XML-virta on olemassa, sen luonut entiteetti voi lähettää määrittämättömän määrän XML-elementtejä vastaanottajalle. XML-tietovirta on aina yksisuuntainen; mikäli vastaanottava pää haluaa lähettää viestejä, pitää sen tätä varten erikseen neuvotella erillinen virta (Response Stream).

XML-tietovirrassa voidaan lähettää XMPP-standardin mukaan lähettää joko XML-säkeistöjä tai yhteyden neuvottelemiseen tarvittavia XML-elementtejä. Mikäli entiteetti saa vääränmuotoisen paketin, se hylätään. Yhteyden ja virran neuvottelee yleensä asiakas- tai palvelinentiteetti vastaanottavaan entiteettiin, joka on yleensä palvelin. Asiakas-palvelin yhteyksien lisäksi siis palvelin-palvelin yhteydet ovat myös mahdollisia.

### 3.3 Säkeistöt

XMPP-protokollassa säkeistö (Stanza) on itsenäinen tietopaketti, joka voidaan lähettää entiteetiltä toiselle XML-virran yli. Säkeistö kuljetetaan aina suoraan XML-virran stream-juurielementin alla, ja voi olla nimeltään "message", "presence" tai "iq". Säkeistön nimiavaruuden on oltava "jabber:client" tai "jabber:server". Mikä tahansa muu tietovirrassa lähetetty paketti ei ole säkeistö. Säkeistö sisältää yleensä yhden tai useampia lapsielementtejä.

Stanzalla on kolme tyyppiä, joilla määritetään viestintämekanismi. "Push-mekanismi on tarkoitettu yleiseen viestintään, "publish-subscribe" yleiseen palvelimen ja verkon tilan viestittämiseen asiakkaille, ja "request-response" taas tiedon vaihtamiseen entiteettien kesken.

### 3.4 Muita protokollia

XMPP-protokollan lisäksi on olemassa myös muita pikaviestinprotokollia, kuten muunmuassa MSNP, Skype, IRC, SIMPLE ja useita muita. Näistä SIMPLE suunniteltiin myös mahdollisimman yleiskäyttöiseksi ja avoimeksi, ja on käytössä esimerkiksi joissain VoIP-sovelluksissa.

Skype-protokolla on täysin suljettu ja salattu [?]. Protokollasta on onnistuttu selvittämään osia, mutta ainakin toistaiseksi sen toiminta on suurilta osin tuntematon. Skype-verkko on rakenteeltaan hajautettu, mutta verkkoon kirjautuminen pitää tehdä erillisen Skype Limited-yhtiön kirjautumispalvelimen kautta.

MSNP (Microsoft Notification Protocol) on Microsoft-yhtiön protokolla pikaviestintään. Sitä käytetään muunmuassa yhtiön omissa Windows Messenger, MSN Messenger ja Windows Live Messenger-sovelluksissa. Myös esimerkiksi avoimeen lähdekoodiin perustuvat pikaviestinsovellukset Pidgin ja Trillian taitavat viestinnän MSNP-protokollan yli. MSNP-verkko on rakenteeltaan keskitetty [?], ja kirjautumispalvelimet ovat Microsoftin hallinnassa. Microsoft ei julkaise protokollan määritelmää, vaan jokainen protokollan versio on käyttäjien toimesta purettu ja määritelmät julkaistu epävirallisesti. Tällä hetkellä MSNP:n viimeisin julkaistu versio on 19, vaikka kirjautumispalvelimet

tukevatkin kaikkia protokollia versiosta 8 lähtien.

IRC (Internet Relay Chat) on

## 4 Verkko

### 4.1 Palvelin

Vaikka XMPP:n määritelmässä ei varsinaisesti määritellä miten viestejä lähetetään, käytetään protokollaa yleensä asiakas-palvelin-arkkitehtuurilla. Erona useisiin muihin tunnettuihin pikaviestinprotokolliin, kuten OSCAR ja MSNP on kuitenkin se, että XMPP-verkolla ei ole yhtä keskitettyä autentikaatiopalvelinta. Käytännössä siis kuka tahansa voi ajaa omaa palvelintaan, ja liittää sen osaksi suurempaa verkkoa.

Palvelimen tehtävänä XMPP-verkossa on TCP-yhteyksien vastaanotto sekä liikenteen välittäminen muille autentikoiduille käyttäjille, palvelimille ja muille kohteille. Palvelin myös reitittää asiakkaan lähettämät paketit oikeisiin kohteisiin. Palvelimet voivat myös tallentaa käyttäjäkohtaisia tietoja, kuten kontaktilistan, joka voi sisältää muita käyttäjiä mistä tahansa liitetystä XMPP-verkosta.

### 4.2 Asiakas

Asiakas luo yhteyden palvelimeen TCP-protokollan yli tiettyyn palvelimen porttiin. Internet Assigned Numbers Authority (IANA) on määritellyt XMPP-protokollan käyttöön portin 5222, mutta muitakin saattaa olla käytössä. Asiakkaan tehtävänä on lähettää viestejä ja tilatietoja palvelimelle, sekä vastaanottaa niitä palvelimelta. Asiakkaan on osattava vähintään avata yhteys XML-viestien lähettämistä ja vastaanottamista varten.

XMPP-verkossa jokaista asiakasta tai päätepistettä kutsutaan entiteetiksi, jolla on aina oma tunnisteensa nimeltään JID. Tunniste on kolmiosainen, esimerkiksi muotoa «solmu@toimialue/resurssi>». Tunnisteessa toimialue-kenttä määrittelee käytetyn palvelimen osoitteen, »solmu-kenttä käyttäjän nimen ja »resurssi-kenttä käyttäjälle kuuluvan toisen asiakaslaitteen. Protokolla sallii useampien asiakasohjelmien kirjautumisen samalle palvelimelle samalla käyttäjätunnuksella, kunhan eri ohjelmille määritellään oma kotiosoitteensa.

Entiteeteille voidaan määrittää myös tärkeystasoja, jolloin esimerkiksi osoitteeseen «solmu@toimialue/matkapuhelin>» lähetetty viesti menee käyttäjän matkapuhelimeen, mutta osoitteeseen «solmu@toimialue>» lähetetty viesti ohjautuu tärkeimmäksi määritettyyn asiakasohjelmaan tai laitteeseen.

### 4.3 Välipalvelin

Koska XMPP-sallii useampien palvelinten toimimisen yhdessä, voidaan XMPP-verkkoa laajentaa niinsanotuilla välipalvelimilla (Gateway). Välipalvelimen tehtävänä on muuntaa XMPP-viestejä sopivaksi välipalvelimen toisella puolella toimivaan pikaviestinverkkoon, ja toisaalta toisesta verkosta tulevia viestejä XMPP-verkkoon sopiviksi. Tunnettuja välipalvelimia on olemassa esimerkiksi SMTP, Internet Relay Chat, SIMPLE sekä SMS -verkkoja varten.

Suurimpana ongelmana välipalvelinten käytössä on se, että protokollat eivät aina ole täysin yhteensopivia. Tästä seuraa, että osa viesteissä välitetystä tiedosta ei välttämättä ole esitettävissä toisella protokollalla. Ongelmia tulee myös turvallisuuden kanssa, sillä lähetettyjen viestien tai muun tiedon siirtyessä toiseen pikaviestinverkkoon, ei sen turvallisuutta voida enää taata.

### 4.4 Autentikaatio

- Miten käyttäjä autentikoituu palvelimelle - Miten varmistetaan muille palvelimille ?

## 5 Laajennukset pikaviestintään

### 5.1 Session aloitus

### 5.2 Tekstiviestien välitys

### 5.3 Ystävälistan hallinta

### 5.4 Tilatiedot

### 5.5 VoIP

## 6 Yhteenveto

Tämän voisi kirjoittaa uudelleen!

Vaikka XMPP ei varsinaisesti vielä ole standardi, on sillä jo laaja tukijapohja. Protokollaa käytetään jo esimerkiksi Google Talk -pikaviestinohjelmassa, kuten myös linux-käyttäjien tuntemassa pidgin-ohjelmassa. Vaikka toistaiseksi yksikään suurista pikaviestinverkkoja ylläpitävistä yhtiöistä, kuten Microsoft ja Yahoo, eivät ole XMPP:tä käyttöön ottaneet, ovat nekin jo raottaneet pikaviestinohjelmiaan muille protokollille [?]. Suurempaa muutosta odotellessa on XMPP:aa käyttävien pikaviestimien silti helppo jutella näihin verkkoihin siltapalvelimien avulla. Koska XMPP on myös yksin-



kertaisesti laajennettavissa, on se helppo saada toimimaan tulevisuudenkin pikavies-tinnän luomien vaatimusten kanssa.

## Lähteet

- [1] P. Saint-Andre, *"Extensible Messaging and Presence Protocol (XMPP): Core"*, Saatavilla osoitteesta <URL: <http://www.xmpp.org/rfcs/rfc3920.html>>, lokakuu 2004, RFC-3920.
- [2] P. Saint-Andre, *"Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence"*, Saatavilla osoitteesta <URL: <http://www.xmpp.org/rfcs/rfc3921.html>>, lokakuu 2004, RFC-3921.
- [3] P. Saint-Andre, *"Mapping the Extensible Messaging and Presence Protocol (XMPP) to Common Presence and Instant Messaging (CPIM)"*, Saatavilla osoitteesta <URL: <http://tools.ietf.org/html/rfc3922>>, lokakuu 2004, RFC-3922.
- [4] Mikko Laukkanen, *"Extensible Messaging and Presence Protocol (XMPP)"*, Saatavilla osoitteesta <URL: <http://www.cs.helsinki.fi/u/kraatika/Courses/IPsem04s/xmpp.pdf>>, Helsingin yliopisto, viitattu 15.3.2008.
- [5] Scott Ludwig, Joe Beda, Peter Saint-Andre, Robert McQueen, Sean Egan ja Joe hildebrand, *"XEP-0166: Jingle"*, Saatavilla osoitteesta <URL: <http://www.xmpp.org/extensions/xep-0166.html>>, 29.2.2008.
- [6] Thomas Muldowney, Matther Miller, Ryan Eatmon, *"XEP-0096: File Transfer"*, Saatavilla osoitteesta <URL: <http://www.xmpp.org/extensions/xep-0096.html>>, 13.4.2004.
- [7] Peter Salin, *"Mobile Instant Messaging Systems - A Comparative Study and Implementation"*, Saatavilla osoitteesta <URL: <http://www.tml.tkk.fi/~anttiyj/Salin-IMPS.pdf>>, Teknillinen korkeakoulu, 21.9.2004.
- [8] Laurence Goasduff, Carina Forsling, *"Gartner Predicts Instant Messaging Will Be De Facto Tool for Voice, Video and Text Chat by The End of 2011"*, Saatavilla osoitteesta <URL: <http://www.gartner.com/it/page.jsp?id=507731>>, Gartner, Egham, Iso-Britannia, 21.6.2007.

- [9] *"Yahoo! and Microsoft Bridge Global Instant Messaging Communities"*, Saatavilla osoitteesta <URL: <http://www.microsoft.com/presspass/press/2006/jul06/07-12IMInteropPR.msp>>, Microsoft, 12.7.2006, Redmond, Yhdysvallat.
- [10] *"Jabber Software Foundation Renamed to XMPP Standards Foundation"*, Saatavilla osoitteesta <URL: <http://www.xmpp.org/xsf/press/2007-01-16.shtml>>, XMPP standards foundation, 16.1.2007, Denver, Yhdysvallat.
- [11] Wikipedia, *"Instant messaging"*, Saatavilla osoitteesta <URL: [http://en.wikipedia.org/wiki/Instant\\_messaging](http://en.wikipedia.org/wiki/Instant_messaging)>, viitattu 27.11.2010.
- [12] Salman A. Baset, Henning Schulzrinne, *"An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol"*, Saatavilla osoitteesta <URL: <http://arxiv.org/pdf/cs/0412017>>, Columbia University, New York, Yhdysvallat, 15.9.2004.
- [13] MSNPiki, *"MSN Protocol Version 8"*, Saatavilla osoitteesta <URL: [http://msnpiki.msnfanatic.com/index.php/Main\\_page](http://msnpiki.msnfanatic.com/index.php/Main_page)>, viitattu 10.1.2011.