

ECRIT
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2012

H. Tschofenig
Nokia Siemens Networks
March 5, 2012

Emergency Services Functionality with the Extensible Messaging and
Presence Protocol (XMPP)
draft-tschofenig-ecrit-xmpp-es-00.txt

Abstract

The Extensible Messaging and Presence Protocol (XMPP) is a technology that enjoys widespread deployment in the instant messaging application domain. While many features for XMPP had been standardized in the IETF as well as in the XMPP Standards Foundation emergency services functionality was not part of it.

This document aims to initiate a discussion about the necessary emergency services functionality for XMPP.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 6, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	Interoperability Need	5
4.	Functionality	7
4.1.	Emergency Call Marking	7
4.2.	Location	7
4.3.	Routing	9
4.4.	Voice and Video	9
4.5.	Real-Time Text	9
4.6.	PSAP Callback	9
4.7.	Additional Data	10
4.8.	Data Only Emergency Calls	10
5.	Security Considerations	11
6.	Acknowledgements	12
7.	References	13
7.1.	Normative References	13
7.2.	Informational References	15
	Author's Address	17

1. Introduction

The Extensible Messaging and Presence Protocol (XMPP) is a technology for real-time communication over the Internet that uses the Extensible Markup Language (XML) as the base format for exchanging information. XMPP provides a way to send small snippets of XML from one communication entity to another one. XMPP has found usage in a variety of protocols, but most people use it primarily for instant messaging.

With the widespread usage of XMPP on the Internet for instant messaging and the desire to offer multi-media emergency services support, i.e., any form of emergency support that goes beyond voice calling, a frequently asked question is those applications that utilize XMPP today are able to offer emergency services support similar to what had been standardized for the Session Initiation Protocol (SIP) over the last 10 years.

XMPP has found widespread usage for instant messaging on the Internet. At the same time there is an increasing interest to add multi-media support to the emergency services portfolio. Consequently, a frequently asked question by emergency services professionals is whether applications utilizing XMPP today will be able to offer emergency services support in the future as well. Standardization activities have so far exclusively focused on the Session Initiation Protocol (SIP).

The author believes that it is time to have a discussion about the desired level of interoperability between XMPP and the standardized, implemented and even deployed IP-based emergency services infrastructure that is based on SIP. This document provides a first discussion input. The main part of the document focuses on the various components of the emergency services functionality.

[2.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

This document uses the terminology defined in [[RFC5012](#)].

[3.](#) Interoperability Need

When deciding about the required emergency services functionality in XMPP a decision has to be made about where to put the burden for interoperability. There only seem to be two main options, which are graphically shown in Figure 1 and Figure 2.

In Figure 1 the XMPP is used between the XMPP client and a XMPP server run by some provider. Whenever the interaction with the emergency services authorities are needed a gateway translates XMPP to SIP very similar to how legacy protocols or proprietary protocols are translated. While the exact placement of the XMPP-to-SIP gateway does not matter from a protocol point of view deployment-wise it does. Here we assume that the emergency services infrastructure only supports a single protocol internally, namely SIP. This is also inline with the current standardization situation.

.-----.
,-----.
, 'IP-based`.
/ Emergency \

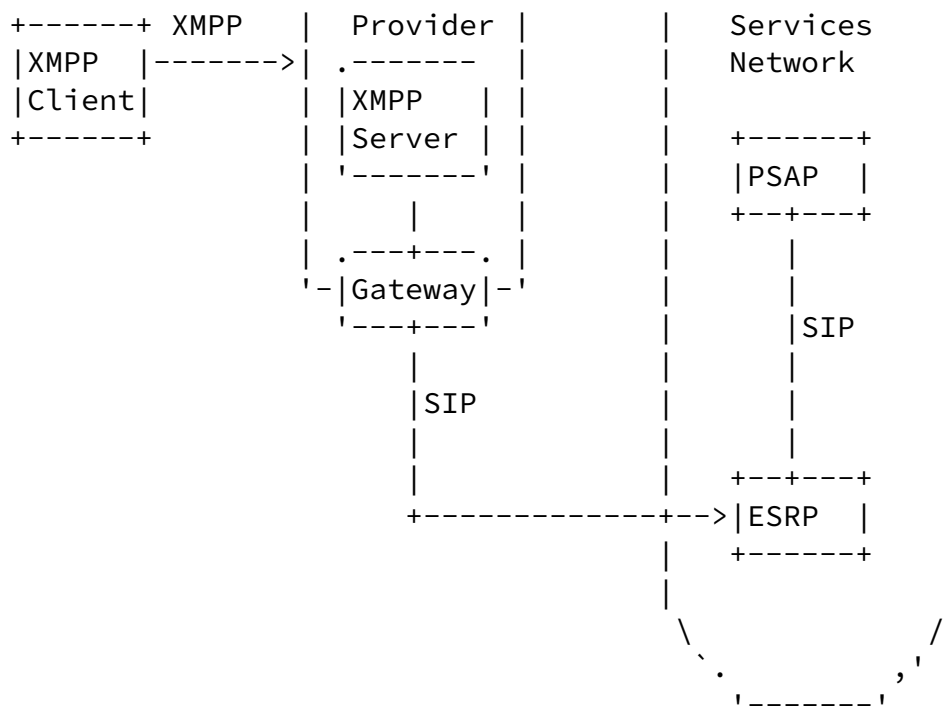
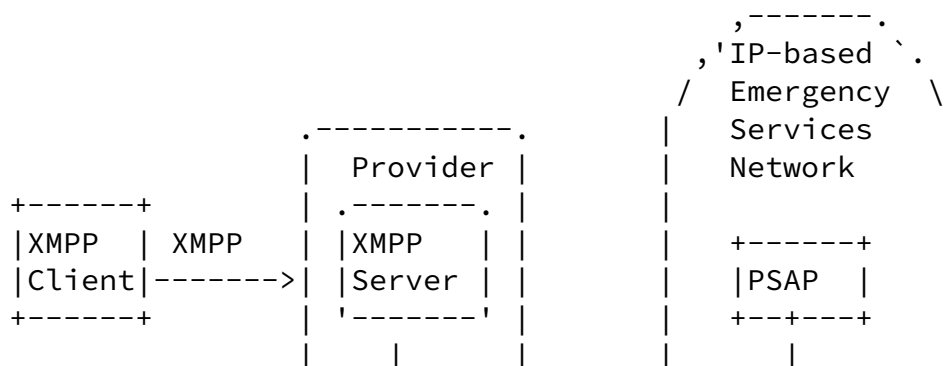


Figure 1: Backend Interoperability

The interworking between SIP and XMPP had been subject to earlier investigations, as described in [[I-D.saintandre-sip-xmpp-core](#)], [[I-D.saintandre-sip-xmpp-media](#)], and [[I-D.saintandre-sip-xmpp-im](#)].

In Figure 2 we show a deployment where XMPP is used end-to-end and the emergency services supports XMPP in addition to SIP.



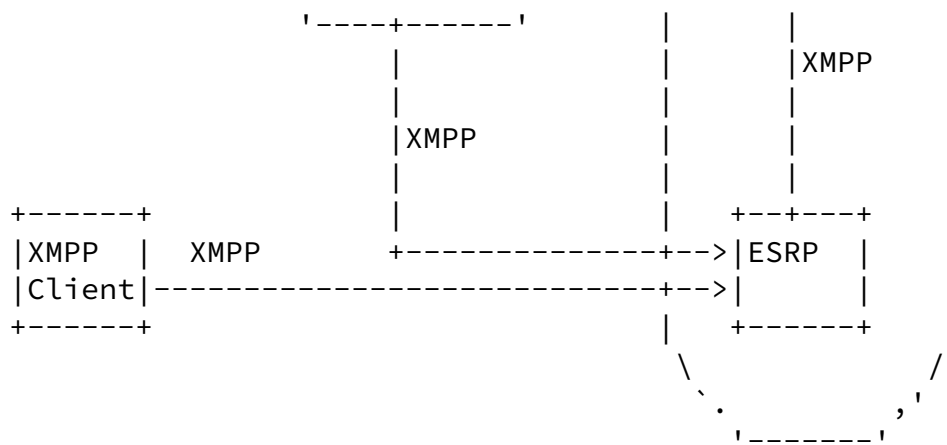


Figure 2: End-to-End Interoperability

Not shown in the figures above is the ability for combined SIP and XMPP usage. Requirements for such interworking are described in [\[I-D.veikkolainen-sip-xmpp-coex-reqs\]](#) and guidance is provided in [\[I-D.veikkolainen-sip-voip-xmpp-im\]](#).

4. Functionality

An important aspect in the support of emergency services in XMPP is how far current XMPP features are equivalent to those offered by SIP. For SIP [\[I-D.ietf-ecrit-phonebcp\]](#) describes the necessary functionality for emergency calling on the Internet. A similar specification is needed for XMPP. [\[I-D.ietf-ecrit-phonebcp\]](#), however, relies on already defined functionality and 'glues' these

available building blocks together. The sub-sections below discuss some of the most important building blocks.

4.1. Emergency Call Marking

In existing telecommunications systems, there are many well-known communication and information services that are characterized by long-term stability of user- visible identifiers, decentralized administration of the underlying service, and a well-defined resolution or mapping mechanism. [[RFC5031](#)] defines a URN namespace that, together with resolution protocols, allows us to define global, well-known services, while distributing the actual implementation across a large number of service-providing entities.

[RFC5031] is not only used for marking SIP communication but it is also used by various emergency components, such as the Location-to-Service Translation (LoST) protocol. [[RFC5031](#)] also has to be integrated into XMPP.

Part of the emergency call marking is also the ability to indicate a test emergency call, as described in Section 15 of [[I-D.ietf-ecrit-phonebc](#)]. An equivalent feature is highly likely to be useful for XMPP.

4.2. Location

The IETF has produced a fairly extensive set of location specifications that are re-used for emergency services. The work falls into various categories, as described in [[RFC6280](#)] and in [Section 6 of \[RFC6443\]](#). The requirements for obtaining high accuracy location information are more complex for emergency services than with commercial location applications due to the life critical nature of the service.

Location Formats:

There are two main formats standardized for location information, namely civic and geodetic location information. The core civic location standard can be found in [[RFC5139](#)] and the profile for geodetic information is available with [[RFC5491](#)]. [[RFC5491](#)]

supports a large set of location shapes. Various additional

extensions have been developed, such as the support for relative location [[I-D.ietf-geopriv-relative-location](#)] and location civic addresses [[I-D.ietf-geopriv-local-civic](#)]. It is also important to mention that there have been efforts ongoing to map the civic addresses in various countries to the PIDF-LO civic location tokens, based on the recommendations in [[RFC5774](#)].

Location Encoding:

There are mainly two encodings of location information, namely a binary encoding, as for example used by DHCP location extensions, and an XML-based encoding based on PIDF-LO [[RFC4119](#)]. Note that the PIDF-LO element contains more than pure location data but also provides information about the entity that constructed the location object (based on the 'provided-by' element) and supplementary data about the utilized location determination technique (based on values from the 'method' token IANA registry).

Location Configuration Protocols:

A Location Configuration Protocol (LCP) [[RFC5687](#)] is one mechanism that can be used by a device to discover its own location from a LIS. Several LCPs have been developed within Geopriv, such as [[RFC5985](#)]. LCPs obtain location information from location servers and are therefore indirectly relevant for location conveyed within XMPP.

Location Derefencing:

For location derefencing two protocols have been defined, namely one based on HTTP [[I-D.ietf-geopriv-deref-protocol](#)] and another one based on SIP which may use filters to reduce the number of asynchronous notifications [[RFC6447](#)]. A session setup protocol has to support the ability to convey these references.

Location Conveyance:

The ability to convey a PIDF-LO and a location by reference in SIP had been defined by [[RFC6442](#)]. For a single call there may be more than one location object in a call.

While there is a location extensions available in XMPP with XEP-0080 [[XEP-0080](#)] it is not equivalent to the functionality listed above. XEP-0080 offers a different civic location format and geodetic location based on a reduced set of location shapes. It uses an XML encoding and allows this information to be conveyed in XMPP. A table

with a mapping to the PIDF-LO semantic is provided in XEP-0080 but unfortunately since the functionality is not equivalent to the list presented above there will be a loss of information during the lifecycle of location handling in most of the scenarios.

[4.3.](#) Routing

The LoST protocol [[RFC5222](#)] offers the ability to discover service contact URIs based on provided service identifiers and location information. In particular, it can be used to determine the location-appropriate Public Safety Answering Point (PSAP) for emergency services. During the design of LoST it was already anticipated that service contact URIs based on a variety of different protocols (not only SIP) will be needed. As such, XMPP is seamlessly supported by LoST.

[4.4.](#) Voice and Video

With XEP-0166 [[XEP-0166](#)] the ability to initiate and manage peer-to-peer media sessions between two XMPP entities in a way that is interoperable with existing Internet standards had been defined. The protocol enables the core session management semantics (compatible with SIP) to be used for a wide variety of application types (e.g., voice chat, video chat).

The ability for voice and video conference bridge as needed by persons with disabilities for sign-language interpretation is, however, not offered by Jingle.

[4.5.](#) Real-Time Text

[RFC 5194](#) [[RFC5194](#)] defines the framework for Real-Time Text over IP. All required functionality is based on SIP and the Real-Time Transport Protocol (RTP).

XEP-0301 [[XEP-0301](#)] seems to offer functionality that is similar to what had been defined by [RFC 5194](#).

[4.6.](#) PSAP Callback

After an emergency call is completed it is possible that the call-taker feels the need for further communication. For example, the call may have been dropped by accident without the call-taker having sufficient information about the current situation of a wounded person. A call-taker may trigger a callback towards the emergency caller using the contact information provided with the initial

emergency call, which includes the GRUU as well as the Address-of-Record. This callback would be treated like any other call and as a

consequence it may get blocked by authorization policies or may get forwarded to an answering machine.

The work on PSAP callback [[I-D.ietf-ecrit-psap-callback](#)] is an ongoing effort to give these calls preferential treatment so that the callback has a higher success in reaching the original emergency call.

This functionality does not exist for XMPP yet.

[4.7.](#) Additional Data

The Internet Protocol suite offers a rich information exchange and thereby better situational awareness for call takers and first responders. The richness comes in various forms, including the multi-media communication capabilities (via voice, video, instant messaging, and real-time text), but also via more additional data made available by various actors of the emergency signaling chain. Sharing information between various actors will enable more intelligent decision making and therefore better response in case of an emergency.

In the SIP environment additional data had been provided in various ways, as described in [[I-D.ietf-ecrit-additional-data](#)], and the same capabilities will have to be provided in XMPP as well.

[4.8.](#) Data Only Emergency Calls

Data-only emergency calls are similar to regular emergency calls in the sense that they require emergency call routing functionality and may even have the same location requirements. On the other hand, the communication interaction occurs without establishment of a voice or video channel.

As a technical mechanism a Common Alert Protocol (CAP) payload is pushed by the SIP User Agent towards the PSAP, as described in [[I-D.ietf-ecrit-data-only-ea](#)]. The ability to push CAP payloads is also available in XMPP with XEP-0127 [[XEP-0127](#)].

5. Security Considerations

This document focuses on the integration of emergency services functionality into XMPP. Offering security features for emergency calls is both important but also challenging as security failures (such as expired certificates) may have fatal effects. SIP offers a secure identity mechanism as well as media security. Functionality for these two areas are specified in [[I-D.ietf-ecrit-phonebcp](#)]. Offering a solid mechanisms for identification of the persons seeking help is important for the overall security of the emergency services system, as described in [[I-D.ietf-ecrit-trustworthy-location](#)].

[6.](#) Acknowledgements

The author would like to thank the members of the European Emergency Number Association (EENA) Next Generation 112 technical committee and the National Emergency Number Association (NENA) Long-Term Definition working group for their discussions around XMPP emergency services support.

[7.](#) References

[7.1.](#) Normative References

[I-D.ietf-ecrit-additional-data]

Rosen, B., Tschofenig, H., and R. Marshall, "Additional Data related to an Emergency Call", [draft-ietf-ecrit-additional-data-02](#) (work in progress), October 2011.

[I-D.ietf-ecrit-data-only-ea]

Rosen, B., Schulzrinne, H., and H. Tschofenig, "Common Alerting Protocol (CAP) based Emergency Alerts using the Session Initiation Protocol (SIP)", [draft-ietf-ecrit-data-only-ea-02](#) (work in progress), July 2011.

[I-D.ietf-ecrit-phonebcg]

Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling", [draft-ietf-ecrit-phonebc-20](#) (work in progress), September 2011.

[I-D.ietf-ecrit-psap-callback]

Holmberg, C., Tschofenig, H., Schulzrinne, H., and M. Patel, "Public Safety Answering Point (PSAP) Callback", [draft-ietf-ecrit-psap-callback-03](#) (work in progress), October 2011.

[I-D.ietf-geopriv-deref-protocol]

Thomson, M., Dawson, M., Winterbottom, J., Tschofenig, H., and H. Schulzrinne, "A Location Dereferencing Protocol Using HELD", [draft-ietf-geopriv-deref-protocol-04](#) (work in progress), October 2011.

[I-D.ietf-geopriv-local-civic]

Winterbottom, J., Thomson, M., Barnes, R., Rosen, B., and R. George, "Specifying Civic Address Extensions in PIDF-LO", [draft-ietf-geopriv-local-civic-03](#) (work in progress), February 2012.

[I-D.ietf-geopriv-relative-location]

Thomson, M., Stanley, D., Rosen, B., Thomson, A., and G. Bajko, "Relative Location Representation", [draft-ietf-geopriv-relative-location-02](#) (work in progress), October 2011.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Tschofenig

Expires September 6, 2012

[Page 13]

Internet-Draft

XMPP Emergency Services

March 2012

Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", [RFC 4119](#), December 2005.

[RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", [RFC 5012](#), January 2008.

[RFC5031] Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", [RFC 5031](#),

January 2008.

- [RFC5139] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", [RFC 5139](#), February 2008.
- [RFC5194] van Wijk, A. and G. Gybels, "Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)", [RFC 5194](#), June 2008.
- [RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", [RFC 5222](#), August 2008.
- [RFC5491] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", [RFC 5491](#), March 2009.
- [RFC5687] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements", [RFC 5687](#), March 2010.
- [RFC5774] Wolf, K. and A. Mayrhofer, "Considerations for Civic Addresses in the Presence Information Data Format Location Object (PIDF-LO): Guidelines and IANA Registry Definition", [BCP 154](#), [RFC 5774](#), March 2010.
- [RFC5985] Barnes, M., "HTTP-Enabled Location Delivery (HELD)", [RFC 5985](#), September 2010.
- [RFC6280] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", [BCP 160](#), [RFC 6280](#), July 2011.
- [RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance

Tschofenig

Expires September 6, 2012

[Page 14]

Internet-Draft

XMPP Emergency Services

March 2012

for the Session Initiation Protocol", [RFC 6442](#),
December 2011.

- [RFC6443] Rosen, B., Schulzrinne, H., Polk, J., and A. Newton,

"Framework for Emergency Calling Using Internet Multimedia", [RFC 6443](#), December 2011.

- [RFC6447] Mahy, R., Rosen, B., and H. Tschofenig, "Filtering Location Notifications in the Session Initiation Protocol (SIP)", [RFC 6447](#), January 2012.

7.2. Informational References

- [I-D.ietf-ecrit-trustworthy-location]
Tschofenig, H., Schulzrinne, H., and B. Aboba,
"Trustworthy Location Information",
[draft-ietf-ecrit-trustworthy-location-02](#) (work in progress), May 2011.
- [I-D.saintandre-sip-xmpp-core]
Saint-Andre, P., Houri, A., and J. Hildebrand,
"Interworking between the Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP): Core", [draft-saintandre-sip-xmpp-core-01](#) (work in progress), March 2009.
- [I-D.saintandre-sip-xmpp-im]
Saint-Andre, P., Houri, A., and J. Hildebrand,
"Interworking between the Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP): Instant Messaging",
[draft-saintandre-sip-xmpp-im-01](#) (work in progress), March 2009.
- [I-D.saintandre-sip-xmpp-media]
Saint-Andre, P., "Interworking between the Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP): Media Sessions",
[draft-saintandre-sip-xmpp-media-01](#) (work in progress), March 2009.
- [I-D.veikkolainen-sip-voip-xmpp-im]
Veikkolainen, S. and M. Isomaki, "Guidelines and Protocol Extensions for Combining SIP Based Real-time Media Sessions With XMPP Based Instant Messaging and Presence Service.", [draft-veikkolainen-sip-voip-xmpp-im-01](#) (work in progress), July 2009.

[I-D.veikkolainen-sip-xmpp-coex-reqs]

Veikkolainen, S. and M. Isomaki, "Requirements and Use Cases for Combining SIP Based Real-time Media Sessions With XMPP Based Instant Messaging and Presence Service.", [draft-veikkolainen-sip-xmpp-coex-reqs-02](#) (work in progress), January 2011.

[XEP-0080]

Hildebrand, J. and P. Saint-Andre, "User Location", XSF XEP 0080, September 2009.

[XEP-0127]

Saint-Andre, P. and B. Fletcher, "Common Alerting Protocol (CAP) Over XMPP", XSF XEP 0127, December 2004.

[XEP-0166]

Ludwig, S., Beda, J., Saint-Andre, P., McQueen, R., Egan, S., and J. Hildebrand, "Jingle", XSF XEP 0166, December 2009.

[XEP-0301]

Rejhon, M., "In-Band Real Time Text", XSF XEP 0301, June 2011.

Internet-Draft

XMPP Emergency Services

March 2012

Author's Address

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445

Email: Hannes.Tschofenig@gmx.net

URI: <http://www.tschofenig.priv.at>

Tschofenig

Expires September 6, 2012

[Page 17]