XEP-0429: Special Interests Group End to End Encryption

Paul Schaub
mailto:vanitasvitae@riseup.net
xmpp:vanitasvitae@jabberhead.tk

2021-08-10
Version 1.1.0

Status	Type	Short Name
Active	Procedural	SIG-E2EE

This document proposes the formation of a Special Interest Group (SIG) within the XSF devoted to the development of end-to-end encryption within the context of XMPP.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF’s Intellectual Property Rights Policy (a copy of which can be found at <https://xmpp.org/about/xsf/ipr-policy> or obtained by writing to XMPP Standards Foundation, P.O. Box 787, Parker, CO 80134 USA).

Contents

1 Introduction

End-to-end encryption presents a vital tool for users to protect their communications against third parties. To ensure a good user experience it is important to agree on shared standards which are widely rolled out and adopted by implementations.
There already exists a number of encryption protocols with different properties and scopes. It is necessary to coordinate the efforts of further improving those standards to identify and unify common problems and patterns.

2 Scope and Role

The role of the SIG shall be as follows:

- Produce, or coordinate the production and maintenance of relevant XMPP Extension Protocol (XEP) documents as described below under Deliverables.
- Represent the interests and requirements of the XMPP community during the development of end-to-end encryption protocols that are non-exclusive to XMPP. Note: Only elected members of the XSF may act as ambassadors.
- Provide recommendations for implementers.

The SIG-E2EE shall not itself approve XMPP extension protocols (XEPs), which tasks shall remain under the purview of the XMPP Council.
The scope of the SIG is limited to end-to-end encryption in contexts which are useful for instant messaging.

3 Membership

The SIG-E2EE shall be open to the public and shall not be limited to elected members of the XMPP Standards Foundation. Anyone who works with, or is interested in encryption protocols is invited to take part. Only elected members of the XSF however may act as ambassadors.
The following discussion venues have been selected for SIG-E2EE:

- Mailing list: standards@xmpp.org
- MUC: e2ee@muc.xmpp.org

4 Lifetime

The SIG-E2EE shall be a standing SIG, and shall exist as long as the XMPP Council deems it useful.

5 Deliverables

The SIG-E2EE should maintain active existing end-to-end encryption specifications and keep them up to date.
It should also coordinate the production of future end-to-end encryption specifications to keep up with the state of the art.