

Geneva, 9 October 2017

To: ISOC-CH members and Swiss residents

Request for expressions of interest

ISOC-CH is hereby requesting any interested member to propose to carry out the work described in the terms of reference below.

ISOC-CH will select a party, or decide not to select any party, and will not be required to provide reasons for its selection or decision.

ISOC-CH reserves its right to modify the terms of reference below, including with respect to the price and the volume of work. Any modifications will be agreed by email between ISOC-CH and the party doing the work.

Payment will be made after the work has been delivered and checked for accuracy by the project implementation team.

Proposals should take the form of an email to board@isoc.ch stating that the party is willing to do the work in accordance with the terms of reference, together with an explanation of why the party is qualified to do the work. The explanation should include:

- the experience the candidate has in working with IETF Internet-Drafts (I-Ds) and possibly achieved Request For Comments (RFCs)
- the experience the candidate has with the IETF (participation, roles)

Proposals must be submitted by 30 October 2017.

Terms of Reference

*ISOC-CH & pEp Foundation
Beyond the Net Project on Implementing Privacy via Mass Encryption - Standardising Pretty
Easy Privacy protocols (July 2017 - June 2019)*

Objective: Professionalizing and readying for submission Internet Drafts (I-Ds) implementing the pretty Easy privacy (pEp / p≡p) protocols

Professionalize each existing and newly created I-Ds concerning the p≡p protocols and make them ready for submission: we assume each I-D (as it becomes available content-wise by the p≡p foundation) to take half a day (=4hrs) to two working days (=16hrs) for it to become ready for discussion across the Internet community.

Tasks for the first year of the project:

- Professionalize and polish „pep“ I-D (cf. version already submitted to the IETF: <https://tools.ietf.org/html/draft-birk-pep-00>)
- Professionalize and polish „pep-email“ I-D (cf. not yet submission-ready version: <https://letsencrypt.pep.foundation/dev/repos/internet-drafts/file/tip/pep-email/draft-birk-pep-email-NN.txt>)
- Professionalize and polish „pep-keysync“ I-D (cf. not yet submission-ready version: <https://letsencrypt.pep.foundation/dev/repos/internet-drafts/file/tip/pep-keysync/draft-birk-pep-keysync-NN.txt>)
- Professionalize and polish „pep-rating“ I-D (cf. not yet submission-ready version: <https://letsencrypt.pep.foundation/dev/repos/internet-drafts/file/tip/pep-rating/draft-birk-pep-rating-NN.txt>)
- Professionalize and polish „pep-trustwords“ I-D (cf. not yet submission-ready version: <https://letsencrypt.pep.foundation/dev/repos/internet-drafts/file/tip/pep-trustwords/draft-birk-pep-trustwords-NN.txt>)
- Add as many „pep-trustwords“-¹ I-Ds as possible (Trustwords in different languages, reviewed by native language speakers; cf. not yet submission-ready English version: <https://letsencrypt.pep.foundation/dev/repos/internet-drafts/file/tip/pep-trustwords-en/draft-birk-pep-trustwords-NN.txt>)

Tasks for the second year of the project:

Throughout the second year, more I-Ds will be created in consultation with the experts involved in the process. Eight of these should be professionalised and polished. Among the planned I-Ds are the following (non-exhaustive list):

- I-D on „pep-message-format-1“ (for email almost identic to existing formats, but with an easy approach for subject line encryption)
- I-D on „pep-message-format-2“ (for email: full message enclosed by outer message in the MIME tree, such as to hide the most possible amount of metadata)
- I-D on „pEp-smime“ (specifying S/MIME handling and interoperability with other encryption standards with pEp)
- I-D on „pep-xmpp“ (specifying how pEp will be bridged to / support the XMPP chat protocols)
- I-D on „pep-tox“ (specifying how pEp will be bridged to / support the Tox chat protocols (cf. <https://tox.chat>))
- I-D on „pep-sync“ (specification of pEp’s peer-to-peer protocol in the most general form)
- I-D on „pep-sync-events“ (specification of how pEp can synchronize calendar data across devices in a peer-to-peer fashion)
- I-D on „pep-sync-contacts“ (specification of how pEp can synchronize contact data across devices in a peer-to-peer fashion)
- I-D on „pep-email-onionrouting“ (specification proposing changes to the Simple Mail Transfer Protocol (SMTP) such as to support onion routing with email servers for email messages)
- I-D on „pep-dime“ (specification for pEp bridging to / supporting the DIME specification, cf. <https://dime.info>)
- I-D on „pep-gnunet“ (specification on how all message traffic can be routed through the GNUnet, cf. <https://gnunet.org>)

¹ Note: in what concerns the Trustwords concept, it is not yet clear if there will be an I-D for every language or just a well-known URL, which is part of the more general pep-trustwords I-D. This will emerge out of discussions at IETF meetings.

Project timeframe (October 2017-June 2019)

Dates of work: November 2017-May 2019

Payment: a total of 7,000 CHF is allocated to turning the 7 I-Ds into professional submissions for the IETF during year 1 of the project. During year 2 of the project, a total of 8,000 CHF is allocated for the professionalisation of 8 I-Ds.

The work on each I-D can be completed individually or as part of the expert group. If the latter is preferred, the total amount of 15,000 CHF will be shared between the active members of the group.

Procedure: individual delivery or as part of an expert group

Delivery: RTF or plain text format, via email.

(optional): Follow the progress of the I-Ds in the IETF tracker, working groups until the next IETF meeting(s).

Respondents should be based in Switzerland and should know about IETF work and have specific knowledge in the privacy and security areas -- the more, the better. That is, respondents should have knowledge of cryptography, security formats and protocols involved in these areas.

Your work on the I-Ds will be acknowledged, by stating your name and the funding source (i.e. ISOC's Beyond the Net programme supporting the standardization process of p≡p) as part of the corresponding I-D.

Feel free to forward this call to any party in Switzerland who might be interested.