# p≡p position paper

W3C Workshop on Privacy and User Centric Controls
20-21 November 2014, Berlin, Germany

## Abstract

p≡p is a family of protocols, concepts and implementation which lead to the situation that privacy can be the default for everyone in written communication in the Internet. This includes concepts for Web-Browser plugins as well as key-management protocols which are cross-device and cross-platform.

## Basic Concept

p≡p isn't a new crypto standard. Instead, it is a standard how to apply existing crypto standards including OTR and OpenPGP to messages sent through anonymizing networks like GNUNet, and fallbacks to support applying such standards to heavily used existing messaging standards including E-Mail, XMPP and SMS.

p≡p is also a reference implementation how to do so. It provides a portable engine with all functionality and adapters to make this engine accessible by managed code, scripting languages and common other application development languages and worlds. p≡p also delivers plugins for messaging applications and browsers, as well as apps for mobile devices where no in-app plugin concept can be realized.

p≡p's whole concept is peer-to-peer. It does not define any own platform but can be used over different platforms itself.

## Targeted platforms

The p≡p concept is truly platform independent. It can be applied on any platform. Platforms already addressed by the project include Microsoft Windows and Windows Mobile, Apple MacOS X, Apple iOS, GNU/Linux, xBSD, Google Android and some more.

The addressed development environments include COM/Windows, Java/JNI, Qt, Python, Ruby and some more.

Plugins for Microsoft Outlook, Mozilla Thunderbird and Apple Mail are planned, as well as Browser plugins for Mozilla Firefox, Google Chrome, Apple Safari and Microsoft Internet Explorer. The Browser plugins allow web-mailers and web-based messaging apps to use a local encryption and key-management solution in a very easy way.

Additionally, full-featured messaging Apps are planned for different mobile OS including Apple iOS, Google Android, Mozilla Firefox OS and some more. These apps primary address convergence of different messaging services and peer-to-peer synchronization of user data including trust, keys, contacts and schedule.

# p≡p Proposals for Standards

p≡p will make proposals for standards in different fields. There will be a proposal for a standard for applying OpenPGP and OTR on messaging channels which don't support own encryption or only weak encryption. There will be a proposal for a standard interface in ECMAScript/HTML, how to access encryption and key-management services of p≡p. There will be proposals for the peer-to-peer synchronization protocols. And there will be proposals for the protocols how to reroute E-Mail and Text messages through anonymizing networks like GNUNet.

# p≡p Communication Strategy

The communication strategy of p≡p includes a fallback concept for reaching people with written communication in the most secure way possible. In the first draft it's like the following:

1. When two p≡p users are communicating
    - a) if online communication available: OTR through GNUnet
    - a) if online communication not available:
        - i) if anonymizing platform available, OpenPGP through anonymizing platform
        - ii) if anonymizing platform not available, fallback to OpenPGP
2. When a p≡p user is communicating with a non-p≡p user then depending on the capabilities of the non-p≡p user
    - a) if anonymizing and forward secrecy is possible, use that (i.e. OTR over GNUnet)
    - b) if anonymizing but no forward secrecy is possible, use that
    - c) if forward secrecy is possible, use that (i.e. OTR)
    - d) if hard cryptography but no forward secrecy is possible, use that (i.e. OpenPGP)
    - e) if only weak cryptography is possible, use that (i.e. S/MIME with commercial CAs)
    - f) send unencrypted

# User Interface

p≡p makes proposals for user interfaces, too. There is a UI prototype (mock-up) for Apps showing how to signal trust and include p≡p in a real world application as well as a preview of a preview (working sample) of a Microsoft Outlook plugin showing how to do the same job inside a messaging application which already exists. p≡p is just developing on an Android preview (working sample) of the p≡p App; this will be available at the end of 2014.

# p≡p is offering a lecture about details

If there is interest, there will be a lecture with samples around the mentioned topics given by Volker Birk, followed by a discussion and workshop.