Artikel 12, Erklärung der Menschenrechte:
Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.
http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=ger

Ein großer Teil unserer Kommunikation online ist einsehbar wie eine Postkarte. Seit Snowden 2013 wissen wir, dass es Massenüberwachung gibt. p≡p versucht eine nachhaltigen Lösung: Zunächst Massenverschlüsselung, später Massenanonymisierung (Schutz von Metadaten).

Wir kommen aus der Cypherpunkbewegung und möchten mit Massenverschlüsselung die Kosten der Massenüberwachung "optimieren"! Wir wollen die Wurzel packen, statt immer wieder nur an den Symptomen zu arbeiten! Wir haben jahrzehntelang allen, die es hören wollten, erklärt, wie Verschlüsselung funktioniert und wie man sie benutzt – irgendwann hatten wir es satt: Anstatt immer mehr Anleitungen zu schreiben, schreiben wir nun die Erwartungen in Software und Standards, um die Schritte zu automatisieren, die normalerweise ausgeführt werden sollten: Die "Crypto Needs" sollen aus der Nutzerperspektive verschwinden; Crypto benutzen wird pretty easy und hoffentlich der default Standard - mit Hilfe von p≡p-Sync auch flexibel auf verschiedenen Geräten. Um das hinzukriegen haben wir zusammen mit der ISOC einen Internet-Draft geschrieben. https://datatracker.ietf.org/doc/draft-birk-p≡p/ (wird zu RFC).

Wir wollen Crypto nicht nur für Nutzende pretty easy machen: **Die Architektur von p≡p** ist so aufgebaut, dass es auch für Entwickelnde pretty easy ist, p≡p einzubinden und damit die eigene (Kommunikations-)Software um Verschlüsselung zu erweitern. Es gibt drei Komponenten: Ganz unten liegt die Engine, die verschiedene Verschlüsselungsstandards und Transportprotokolle kennt und mittels Adaptern in Anwendungen eingebunden werden kann: Es gibt einen COM Server Adapter für C#, einen JNI Adapter für Java, einen für JSON, ObjC (und Swift), Python und einen für C++/ Qt. Ein Adapter ist ein Sprachen-/ Umgebungsspezifisches Interface zwischen der Engine API und einer Anwendungsentwicklungsumgebung. Dies sind quasi Bindings um die Engine anzusprechen, und gibt deren Resultate wieder. Die Engine kümmert sich um Details wie Ver- und Entschlüsselung bzw. MIME de- und encoding, Trustrating und Keymanagement.

Selbstverständlich sind Adapter und Engine Free Software und unterliegen regelmässigen, externen Code Audits – die Anwendung dagegen kann alle möglichen Lizenzen haben, da sie ja weiterhin den Anwendungsentwicklenden gehört. Diese müssen sich nur noch um die Schnittstelle zwischen Adapter und eigener Software kümmern – statt sich aufwendig in Verschlüsselungsmethoden einzuarbeiten. Auch brauchen sie sich keine Sorge mehr um die Aktualiät der verwendeten Methoden zu machen - wenn sich etwas verändert, wird dies direkt in der Engine abgebildet.

p≡p ist kompatibel zu verschiedenen Cryptostandards, Transportprotokollen, Sprachen und Platformen. Unterstützt werden momentan OpenPGP, GnuPG, netGPG, S/MIME (passiv); geplant sind: OTR, OMEMO, Axolotl, etc und bei den Transportprotkollen entsprechend momentan: SMTP, IMAP, POP3, Exchange; geplant sind: XMPP, SMS, aber auch non-open Standards wie zb Twitter-DMs. Daneben kommt es in der Zukunft zum Schutz von Metadaten mittels Routing über GNUnet – ein Set von Protokollen für Ende-zu-Ende verschlüsselte, anonymisierte Datenübertragung, die eines Tages unsere derzeitigen Internetprotokolle ersetzen sollen.

Repositories: https://p≡p.foundation/p≡p-software

Die p≡p Stiftung verteidigt die Privatsphäre. p≡p steht für pretty Easy privacy (p≡p oder pEp) und für die radikale Vereinfachung der Nutzung von Ende-zu-Ende-Kryptografie-Tools für schriftliche digitale Kommunikationskanäle. Mit der Integration des sicheren peer-to-peer Frameworks GNUnet wird zudem am effektiven Schutz der Metadaten gearbeitet. Letztlich will p≡p realisieren, dass eine verschlüsselte, verifizierte und anonymisierte schriftliche digitale Kommunikation zum Standard wird ("Privacy by Default").

Die p≡p Stiftung ist gemeinnützig und steuerbefreit mit Sitz in der Schweiz. Ihr gehört die Kernsoftware des p≡p-Projekts (p≡p-Engine und Adapter). Ihre Aktivitäten umfassen unabhängige Codeentwicklung, Arbeit im Rahmen der IETF, um die Interoperabilität von p≡p-Software zu wahren, die Unterstützung von FOSS-Projekten, Organisation von Code-Audits sowie politische Arbeit.

p≡p