PGP4CiviCRM

Plug and play encryption for an open source CRM

Uli Fouquet (ulif) <uli@gnufix.de>
2021-11-23

Who?

Uli (ulif) Fouquet (he/him)

- **Open Source** Developer
- Currently living in **Brunswick**/Germany
- First computer: Sinclair **ZX81**
- **Oldest** available **PGP key**: ~2002

What?

PGP4CiviCRM is (currently) a

- **Milter**
- written in **Python**

useable via a

- **CiviCRM module**
- written in **PHP**
- or **standalone** (as postfix milter)

to **OpenPGP-encrypt** outgoing email where possible and on-the-fly.

Why?

A message from an NGO, **unencrypted** (and with **empty plaintext** alternative MIME part)

```
From: "NGO office" <office@ngo.org>
To:   "Uli" <uli@gnufix.de>
Subject: Your confidential bill
Message-ID: Message-ID: <civicrm_11.22.33@office.ngo>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="=_the_boundary"

--=_the_boundary
Content-Type: text/plain; charset=utf-8

--=_the_boundary
Content-Type: text/html; charset=utf-8

<CONFIDENTIAL DATA HERE>

--=_the_boundary--
```

Why?

A message from an NGO, **unencrypted** (and with **empty plaintext** alternative MIME part)… **although**

- …they had my PGP key already
- …my PGP key was available at keyservers

Their problem:

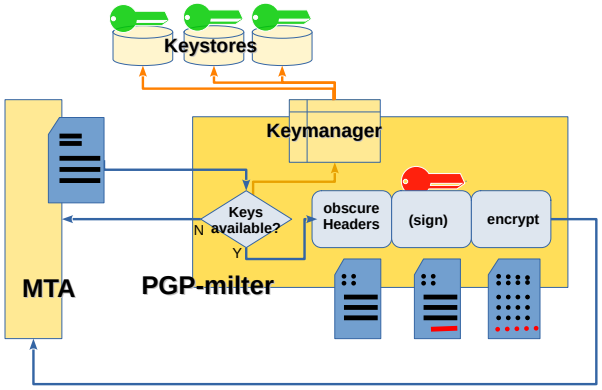
- message was **generated** by a CRM (**automatically**)
- CRM (**CiviCRM**) lacks support for message encryption

Their solution:

- if **you** implement it for us, **we** will use it (and others as well).

Entering NL.NET and NGI ZERO…

pgp-milter: Flow and Components



Features (and anti-features)

Features

- Different Keystores (Memory, local disk, keyservers, [OpenLDAP])
  - Memory
  - Local Disk
  - Keyserver/HKP (Default: keys.openpgp.org)
  - (to come: LDAP, WKD, ...)
- Based on PGPy

Maybe-features

- milter (alternatives: filters, SMTP and non-SMTP)
- Obscured headers (memory hole)

Lessons (about to be) learned

- CiviCRM integration failed a bit (gazillion of email-sending techiques)
- Abstract is better than specialized
- There is at least a usable PGP library for Python available
- hagrid rocks
- (Web Key Directory possibly too)
- PGP UIDs might be overrated, at least when strictly coupled to email addresses
- PGP seems to be a good choice for machine2person encryption.

Thank you!

Sources:
pgp-milter: `https://github.com/ulif/pgp-milter`
pgpy: `https://pgpy.readthedocs.io/`
memory hole: `https://modernpgp.org/memoryhole/`
hagrid: `https://gitlab.com/hagrid-keyserver/hagrid`

Uli Fouquet <uli@gnufix.de>
8173 B77C FE8F D75E 65BC 6FF6 6D93 033F BC9F 6E27