Operating PGP keyservers and Ensuring GDPR Compliance

A Practical Approach

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL *TLP:WHITE*

7th May 2018

OpenPGP and PGP Keyservers

- OpenPGP (RFC 4880) is an **encryption standard** widely used in the CSIRT and security community.
- OpenPGP actively relies on **a network of distributed PGP keyservers** to publish and search for keys (including revocations, signatures, uid and alike).
- The keyservers are often running SKS software and are operated by volunteers. Keyservers **are synchronised and automatically share OpenPGP keys** including updates.
- The goal is to easily find users having encryption keys in order to send **encrypted messages** to, but also to find revoked keys, new keys or signatures to build a network of local trust.

OpenPGP format - what's inside a PGP key?

- The OpenPGP format is composed of packets which can include (in addition to cryptographic packets):
- User ID packet, which is an UTF-8 text, intended to represent **a user with his/her name along with their email address(es)**.
- An Image Attribute subpacket, which encodes an image and often **a picture of the owner**.
- Signature packets signing the OpenPGP keys and also specific Keys (User ID) signing the key (e.g. web-of-trust of the signatures).

Legal ground and lawfulness of a PGP Keyserver

- *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller* 6(1e).
- A task carried out in the public interest: **RFC 2350 3.5.2. Proactive Activities - Security Tools**.
- In addition, PGP encryption mechanisms and its security rely on the availability of PGP Keyservers **GDPR Recital 49 - ensuring network and information security**.

Privacy notice on PGP Keyserver

```
1   CIRCL provides an OpenPGP key server to promote, in the public interest,
    the use of encryption, for example in email communication. Once uploaded, PGP
    keys and aforementioned packets are publicly accessible.
    Before submitting a public PGP key to the server, the submitter is obliged
    to check that any personal data inside the public PGP key are meant to be made
     public and the submitter is allowed to upload it. Once uploaded, due to the
    distributed and resilient nature of the PGP network and to the security
    concern of PGP key deletion, **it would involve a disproportionate technical
    effort to delete or modify your PGP key on the server**.
3   The submitter should specifically verify that the name and surname in the
    PGP key, the physical address and pictures (if any) are allowed and intended
    to be made public. Any personal data you do not want to be made public, should
     be removed. Please note that the email address is the only mandatory field
    when uploading a PGP key.
```

- The privacy notice is included on `https://pgp.circl.lu`.

Synchronisation

- But what about *right of erasure, right of restriction and righ of rectification*.
- The PKS interface is open to everyone to lookup, add or update a key.
- By design, data is synchronised to allow easy lookup of information to validate a key.
- Introducing **OpenPGP key filtering** would allow data subject the right of erasure/restriction on a specific key.
- How do you verify the identity? Email validation? Or more? Is it a disproportionate effort?

OpenPGP key filtering

- CIRCL introduced a list of public filters[1] for PGP keys which can be used to support requests of data subject.
- The lists only contain the fingerprint of a PGP key and is separated in three categories formatted in JSON format:
  - **Trusted list**: a list of PGP key ultimately trusted by the maintainer (CIRCL in this case).
  - **Blacklist**: known bad PGP key, e.g. if someone is spoofing a data subject and uploads fake keys.
  - **Privacy list**: validated privacy concern, e.g. if a data subject wants to have his/key key hidden from public interface.
- Then it's up to OpenPGP key server operators, software developers or CSIRTs to implement/use those public filters.

[1] `https://github.com/CIRCL/openpgp-keys-filterlists`

- Contact: info@circl.lu
- https://www.circl.lu/
- https://github.com/CIRCL/compliance
- https://github.com/CIRCL/openpgp-keys-filterlists