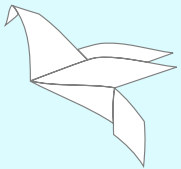
Trust-Management in Gruppen mit OpenPGP CA

https://openpgp-ca.org

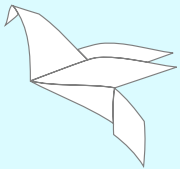
Heiko Schäfer <heiko@schaefer.name>

03. Februar 2022



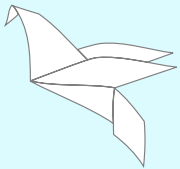
Kontext: (Open)PGP

- Standardisiertes System für kryptographische Operationen [RFC 4880]
- Erste Version: 1991, seither fortlaufend weiter entwickelt [IETF crypto-refresh]
- “PGP basiert dabei auf dem sogenannten Web of Trust, bei dem es keine zentrale Zertifizierungsinstanz gibt, sondern Vertrauen von den Benutzern selbst verwaltet wird.” [Wikipedia]



Kontext: Sequoia PGP

- Moderne OpenPGP Implementierung: https://sequoia-pgp.org/
- Rust; “Library first”
- OpenPGP CA nutzt Sequoia PGP

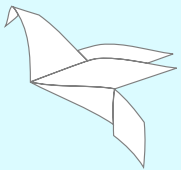


OpenPGP CA

"OpenPGP certification authority"

- Ansatz für die Nutzung von OpenPGP in Organisationen:
  Modellierung von Authentifikation durch standardisierte, maschinenlesbare OpenPGP Artefakte (digitale Zertifikate; "Trust Signatures")
- Tooling um diesen Ansatz praktisch umzusetzen

Ziel: PGP wird für Anwender gleichzeitig einfacher und sicherer



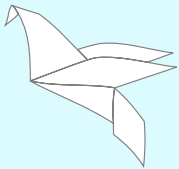
Authentifikation, oder: Sicher den ‘richtigen Schlüssel’ verwenden.

Alice
(prüft nicht besonders gerne Fingerprints)

Bob
0x12345678

Carol
0x87654321

Dave
0xABCDEF01



Authentifikation: verbreitete Herangehensweisen

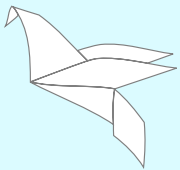
Zentrale, obligatorische Vertrauensanker (z.B. TLS)

- Gut: Authentifikation, maschinenlesbare Artefakte, transparent für Nutzer
- Schlecht: zentrale Autorität, potentiell nicht im Sinne der Nutzer

Variationen von TOFU oder YOLO (z.B.: ssh, e2ee Messenger)

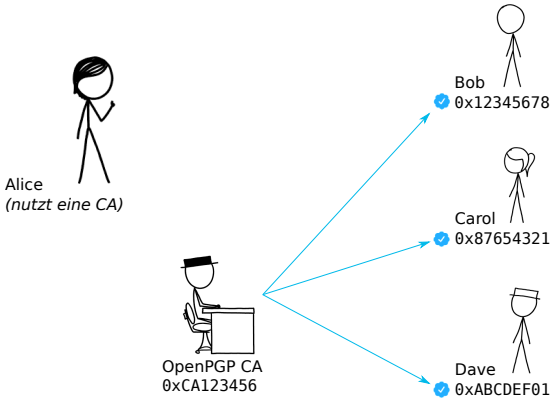
- Gut: Einfach bis transparent für Nutzer
- Schlecht: schwache oder keine Authentifikation

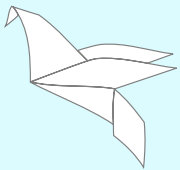
Unser Ziel: Starke Authentifikation + dezentral + einfach für Nutzer



Authentifikation mit Hilfe von OpenPGP CA

CA Admin prüft und beglaubigt Schlüssel, Alice nutzt Zertifikate der CA.



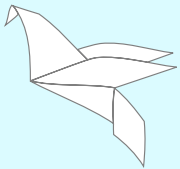


Authentifikation mit Hilfe von OpenPGP CA

Starke Authentifikation + dezentral + für Nutzer weitgehend transparent.

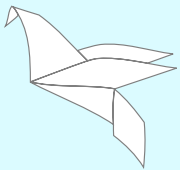
- CA Nutzer: authentifiziert und nutzt CA als Vertrauensanker [O(1)].
- CA Admin: manuelle Authentifikation aller Gruppenmitglieder [O(n)].
  (Auch: Schlüssel-Tausch und neue Gruppen-Mitglieder)

CA Nutzer können Gruppen-intern oder -extern sein.



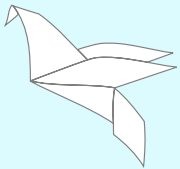
Weitere Aspekte von OpenPGP CA

- Publikation von Schlüsseln (insbesondere per WKD).
- Vertrauen in CAs kann per Domainname eingegrenzt werden.
- Föderation (*"bridging"*) zwischen Organisationen.
- Integration in existierende Infrastruktur (z.B. per REST API an LDAP).



Vorteile aus Nutzer-Sicht

- Starke Authentifikation ohne fortlaufenden Aufwand.
  - Vereinfacht auch key discovery und Schlüssel-Tausch.
- Nutzer können explizit CAs vertrauen, deren Ziele zu ihren passen.
- Keine zusätzliche Software nötig (OpenPGP CA Instanzen erstellen standard-konforme Zertifikate im “Web of Trust”).



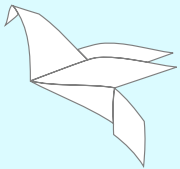
Links

OpenPGP CA ist Freie Software (GPLv3)

https://gitlab.com/openpgp-ca/openpgp-ca

Ausführliche Dokumentation auf https://openpgp-ca.org

- Technische Sicht auf die Konzepte
- Betrieb einer CA Instanz
- Nutzung einer CA (z.B. mit GnuPG)



Danke!

Eine OpenPGP CA Instanz in Ihrer Organisation betreiben?
Sprechen Sie uns gerne an!

- Matrix Space: #sequoia-pgp:matrix.org
- IRC: OFTC #openpgp-ca oder #sequoia

Danke an NLnet und pep foundation für finanzielle Unterstützung des Projekts