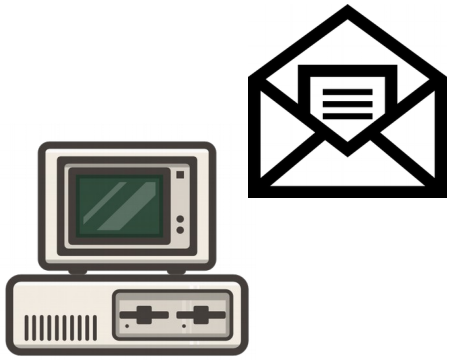
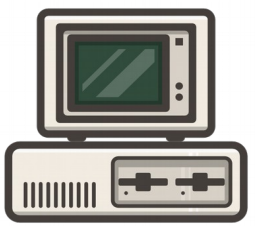
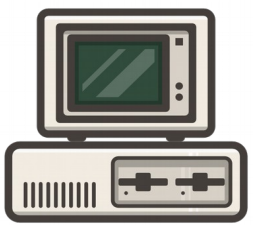
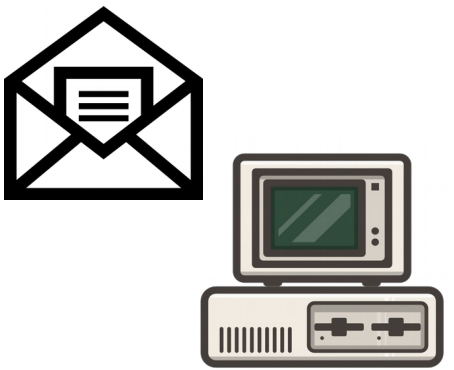
Freie Mailbox Verschlüsselung für Alle

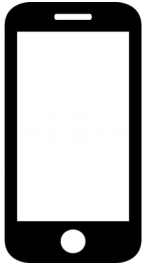
immerda.ch

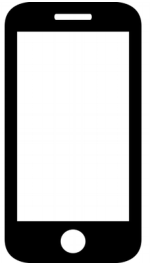


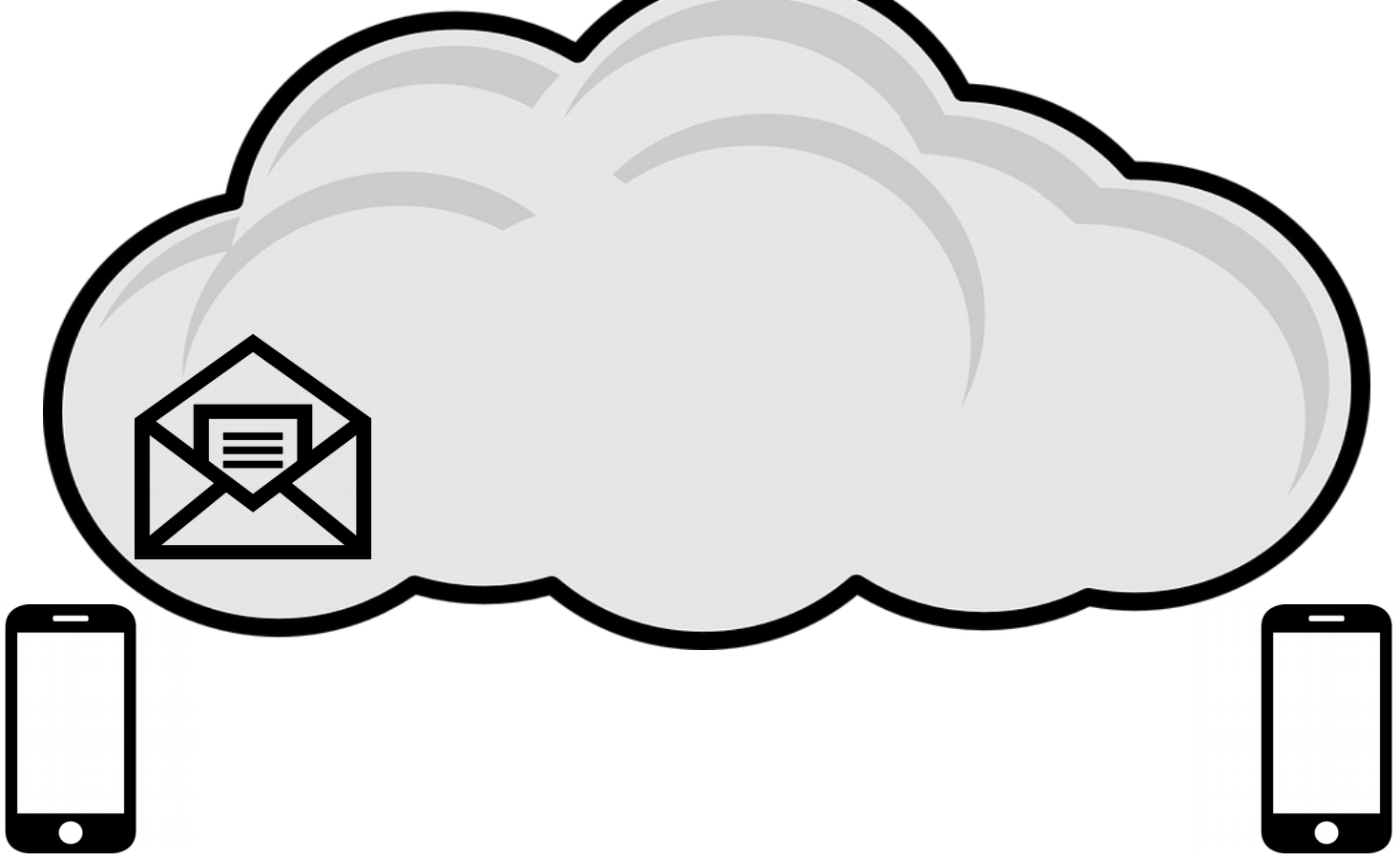


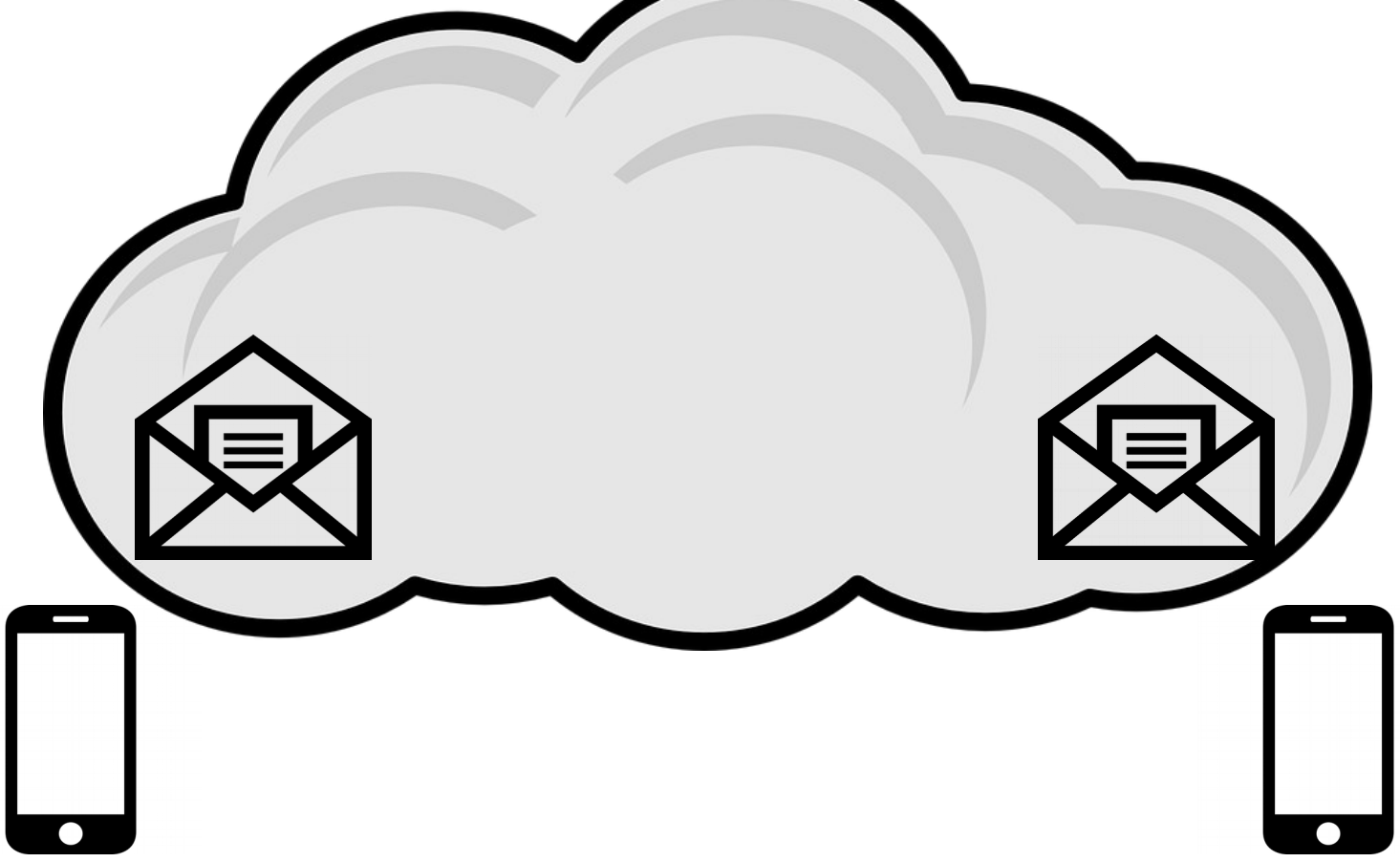




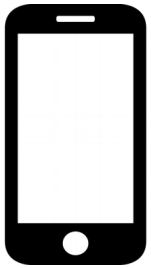




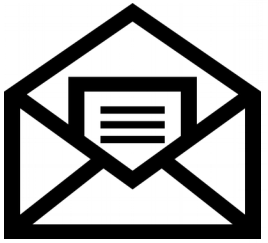




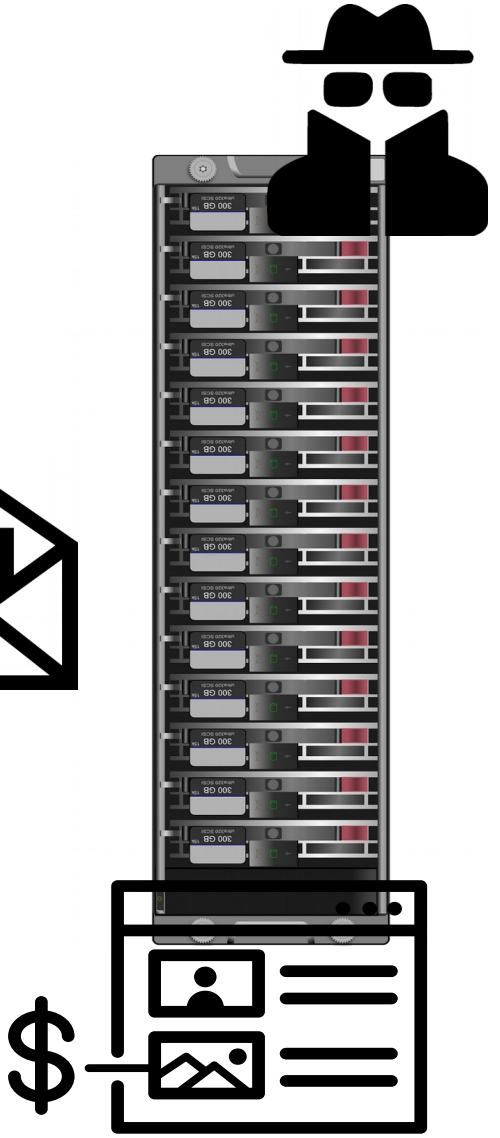

somebody else's machine



dein Gerät



“deine” Daten



Beispiel GMail

Wenn Sie **Inhalte** in oder über unsere Dienste hochladen oder einstellen oder in unseren Diensten oder über unsere Dienste **speichern, senden oder empfangen**, räumen Sie Google (**und denen, mit denen wir zusammenarbeiten**) das Recht ein, diese Inhalte **weltweit zu verwenden, zu hosten, zu speichern, zu vervielfältigen, zu verändern, abgeleitete Werke daraus zu erstellen** […], **zu kommunizieren, zu veröffentlichen, öffentlich aufzuführen, öffentlich anzuzeigen und zu verteilen**.

https://policies.google.com/terms?hl=de#toc-protection

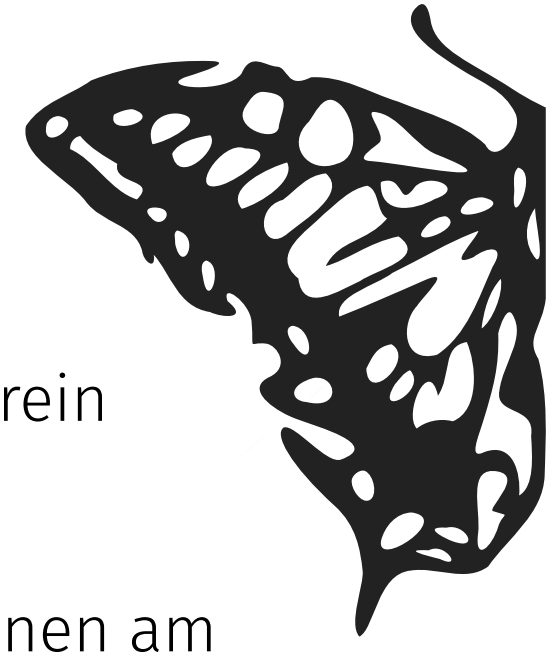
E-Mail?

Daten dritter aufzubewahren ist kein E-Mail spezifisches Problem!

Gegensteuer

strukturell und technisch

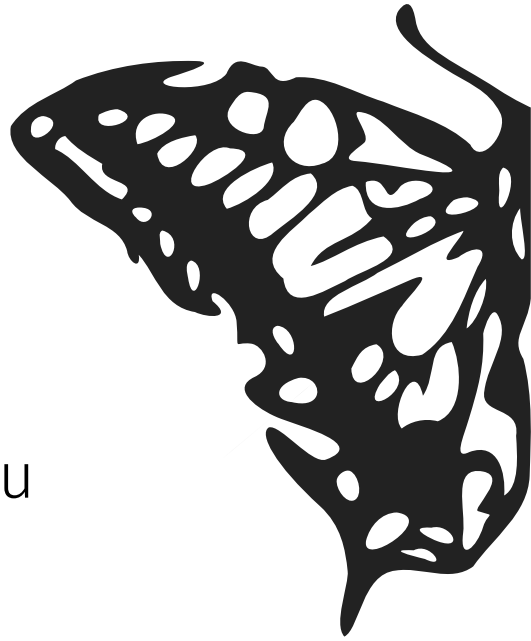
Strukturell



Nicht kommerzieller Provider organisiert als Verein
d.h. kein Datenverkauf-Businessmodel.

Ziel, digitale **Infrastruktur**, die unsere Nutzer*innen am föderierten Internet teilhaben lässt, ohne sich zu verkaufen.

Geschichte



Projekt etabliert vor ca. *20 Jahren* (~2001), um Aktivist*innen eine alternative zu Yahoo-Groups zu ermöglichen.

Weitere Dienste im Lauf der Zeit, gemäss den *Bedürfnissen*.

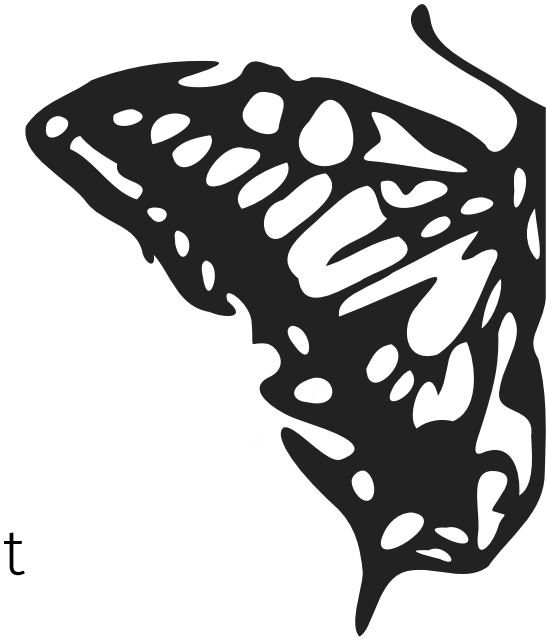
Ansatz: Ein möglicher Provider für deine täglichen Daten

Konzpet

Dienste sind *exklusiv* für unsere Freundinnen und deren Freunde.

Einladungssystem führt zu einem direkten Draht zu unseren User*innen, sowie einem *langsamen* Wachstum.

Konzpet II

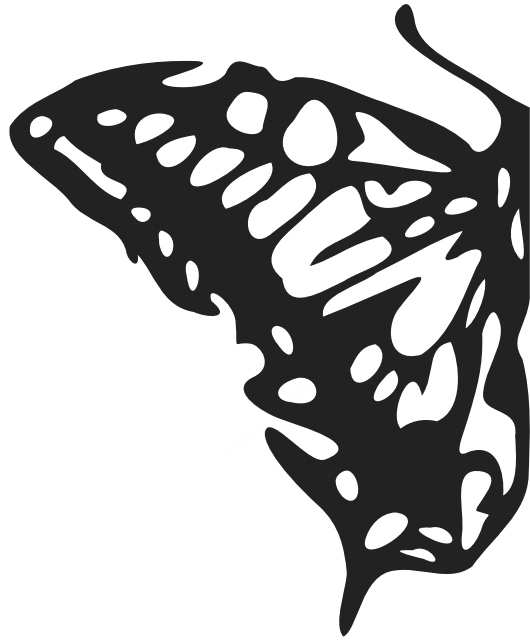


Nutzung *und* Entwicklung von freier Software.

Bewusste und kritische Auseinandersetzung mit Diensten und deren Technologie.

Datensparsamkeit und *Privatsphäre* an erster Stelle.

Dienste



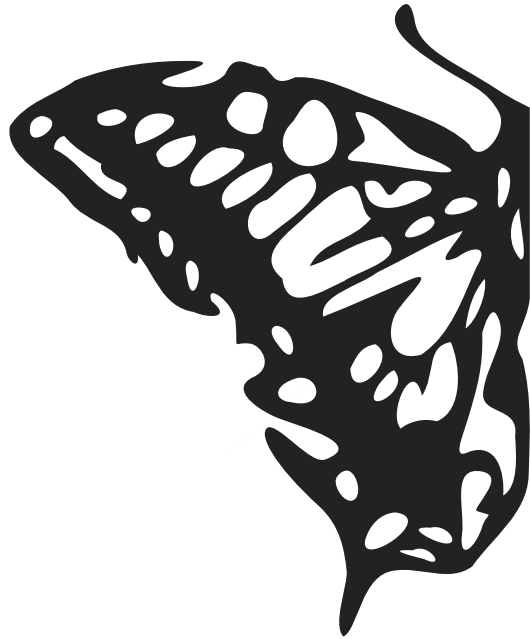
E-Mail
  IMAP, Webmail, ActiveSync, ...

E-Maillisten
  Schleuder, ...

Webhosting
  Wordpress, ...

XMPP, Nextcloud, Schichtplan, Git(Lab), Fileshare, ...

Technisch



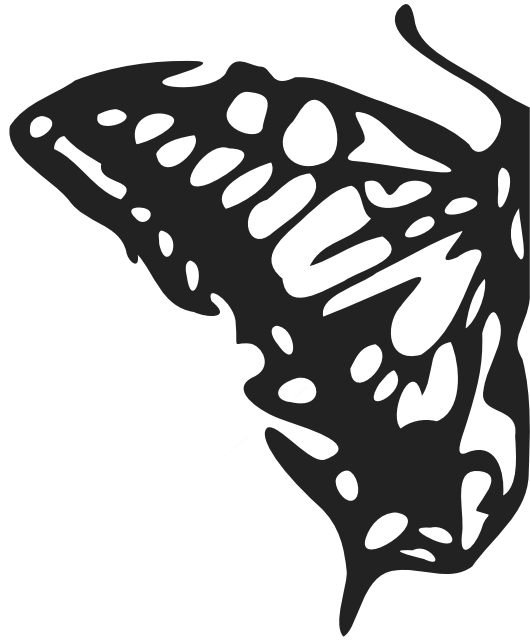
Best practices seit 2001

Sicherheit und Schutz hat viele Schichten

Konfigurationen und Lösungen sind public

u.a. https://code.immerda.ch/immerda/ibox

Datensparsamkeit



Verwendung ohne persönliche Angaben

Anonymisierte oder keine Logs

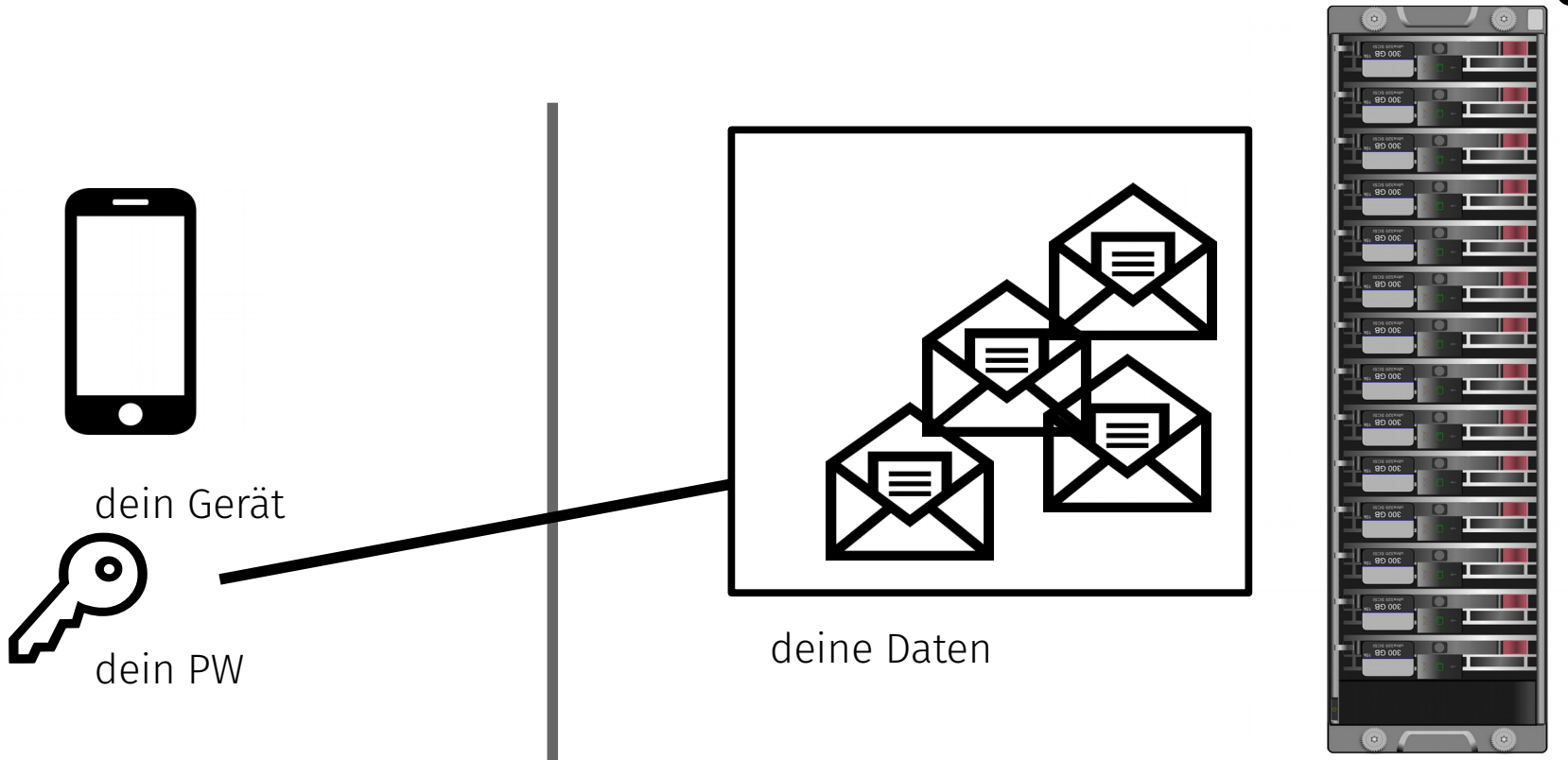
Kurze Aufbewahrungsfristen

Wir bewahren die Daten auf, die uns anvertraut werden

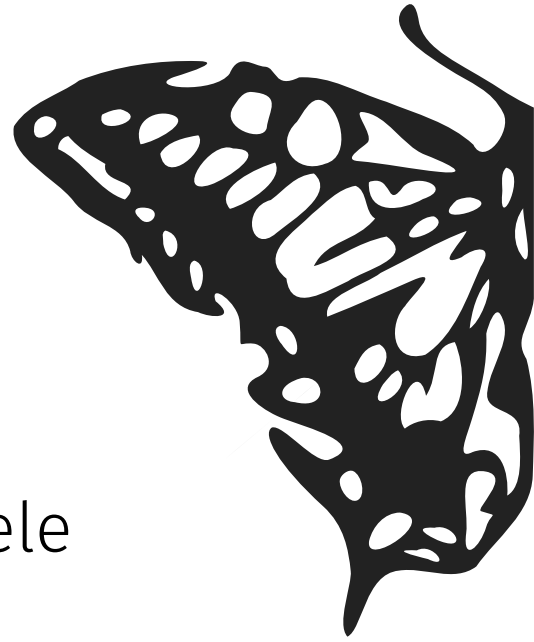
Persönlich verschlüsselte Datenablage

Verschlüsselte Datenablage, bei der die Schlüssel nur der Benutzer*in bekannt sind.

Persönliche Mailboxverschlüsselung



Eine Teillösung

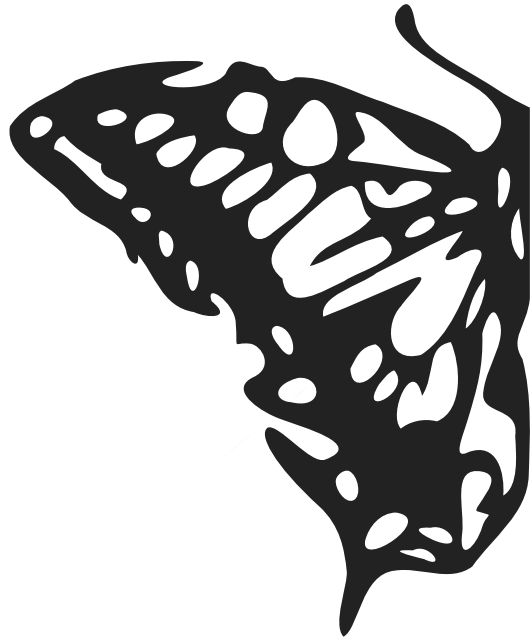


Keine Einzellösung

Schutz und Sicherheit hat viele Ebenen

Andere Mechanismen nach wie vor notwendig

E2E Encryption



Problem: Metadaten…

Beispiel: PGP verschlüsselte E-Mail auf dem Server

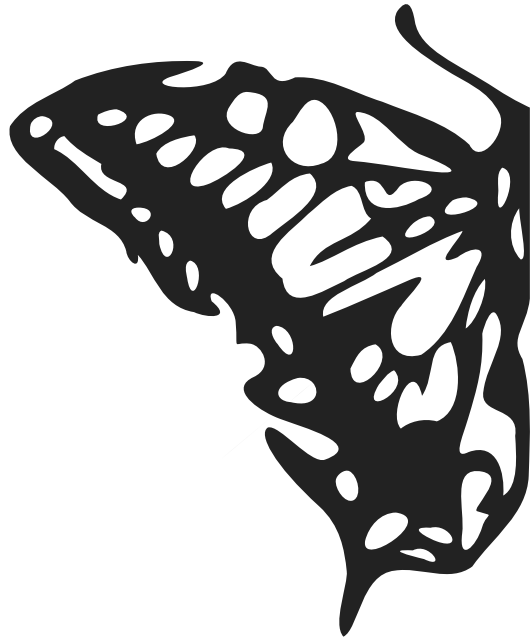
Festplatten-verschlüsselung

Problem: 24/7 offen

Eigentlich die Lösung bei physikalischem Diebstahl

Nebenbei:
https://code.immerda.ch/immerda/apps/arver/

Weitere Punkte



Datensparsamkeit
Inhalte!

Zugriffskontrolle
Immer verbunden

mail-crypt mit Dovecot

https://doc.dovecot.org/plugin-settings/mail-crypt-plugin/

Persönliche Mailboxverschlüsselung

Benjamin Fichtner: Untersuchung von Techniken zur persönlichen E-Mail-Postfachverschlüsselung
https://gitlab.com/bifi/mailboxencryption_thesis

	Scrambler	(Posteo)
	TREES	(Riseup Labs)
1.	mail-crypt	(Dovecot)

https://gitlab.com/bifi/mailboxencryption_thesis

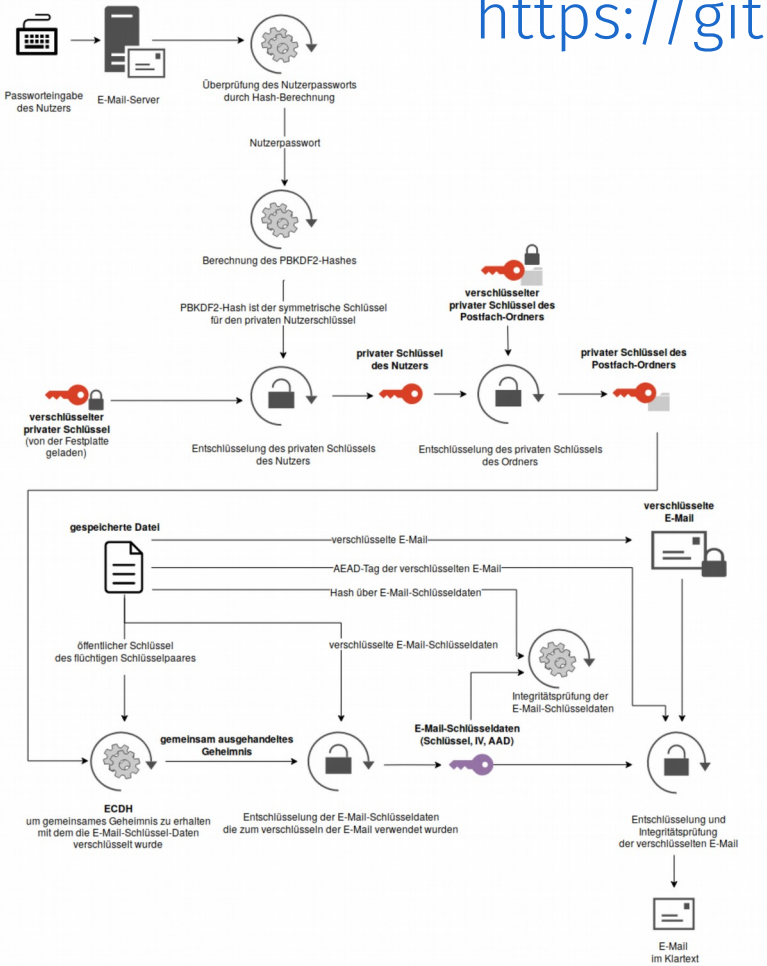


Abbildung 5: E-Mail-Entschlüsselungsprozess beim E-Mail-Abruf mit MailCrypt

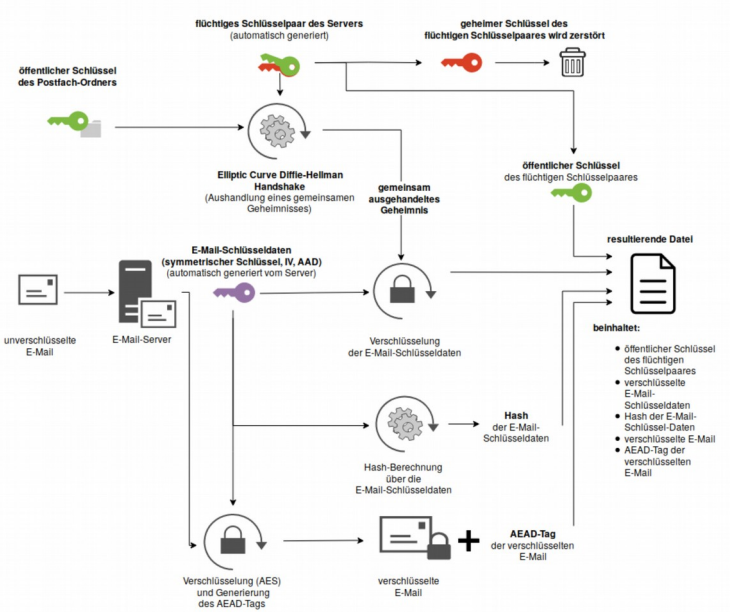
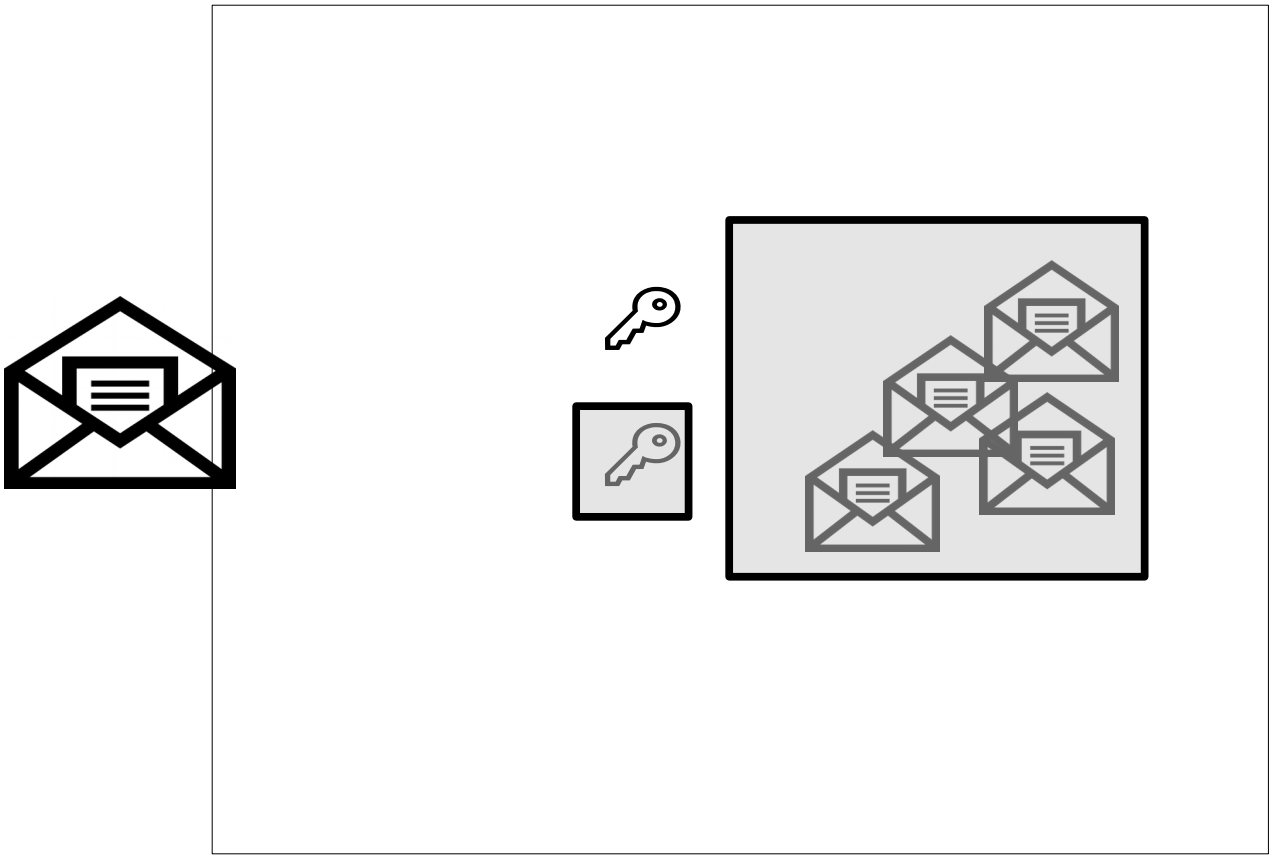
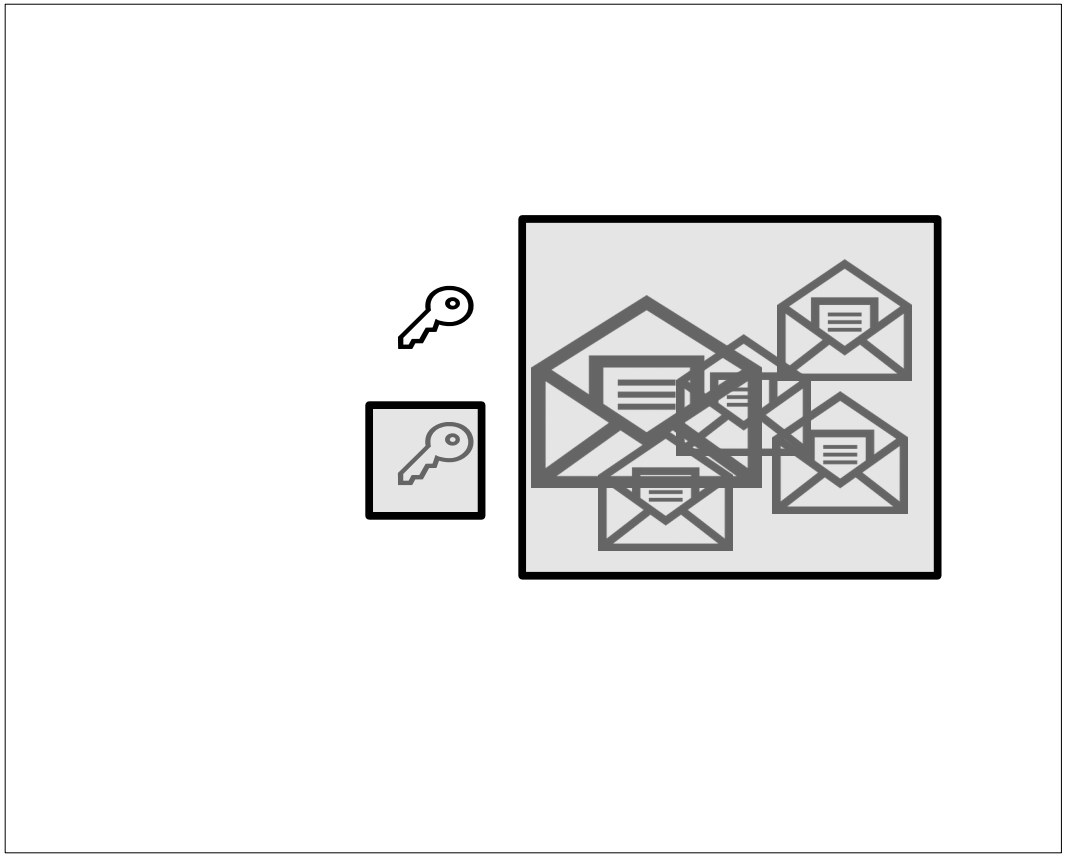


Abbildung 4: E-Mail-Verschlüsselungsprozess beim E-Mail-Empfang mit MailCrypt

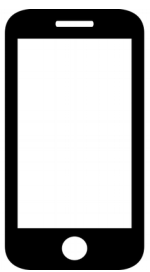
Empfangen



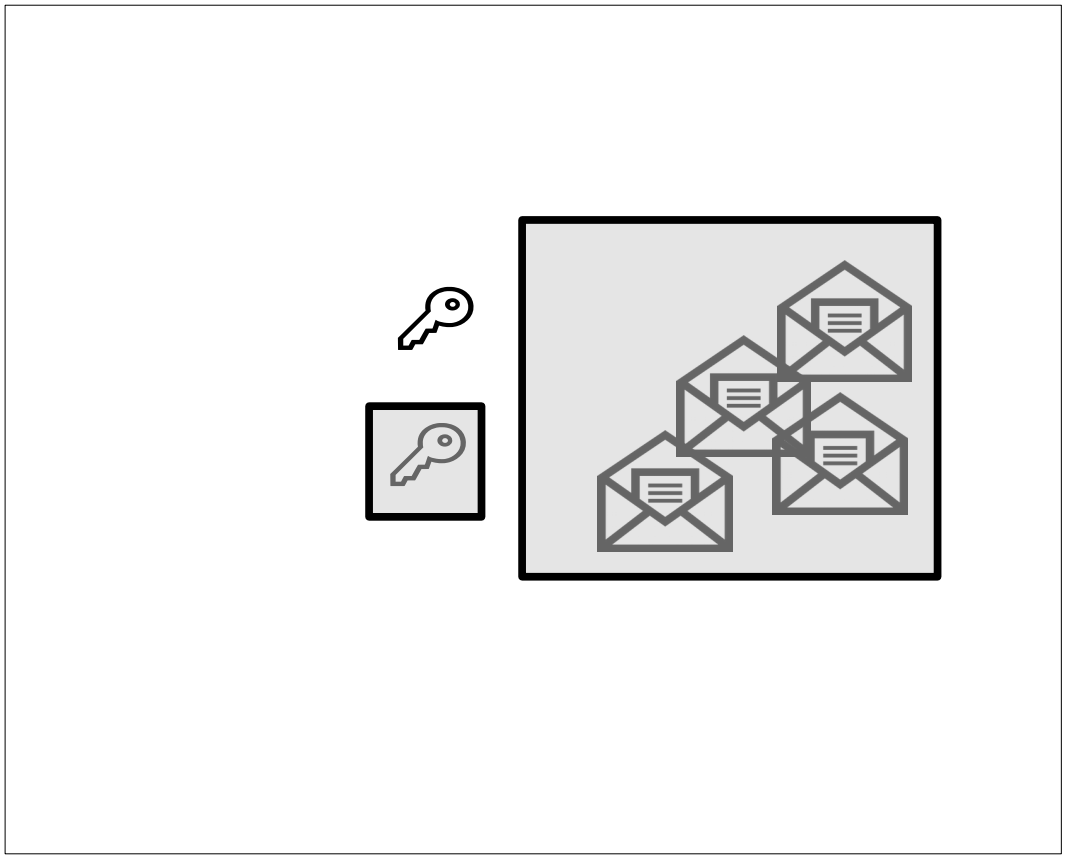
Empfangen



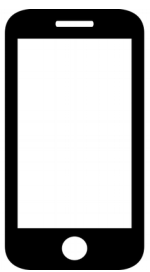
Abrufen

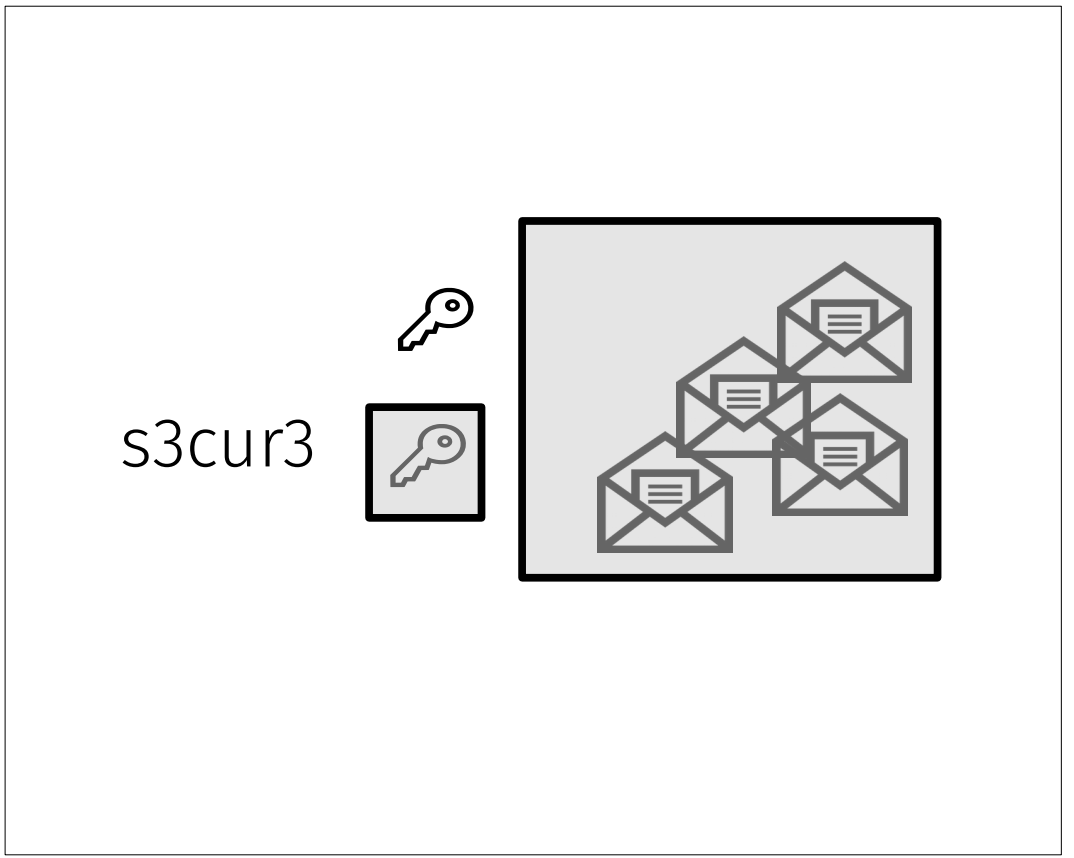


s3cur3

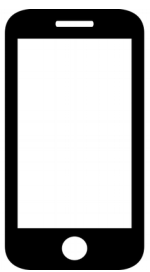


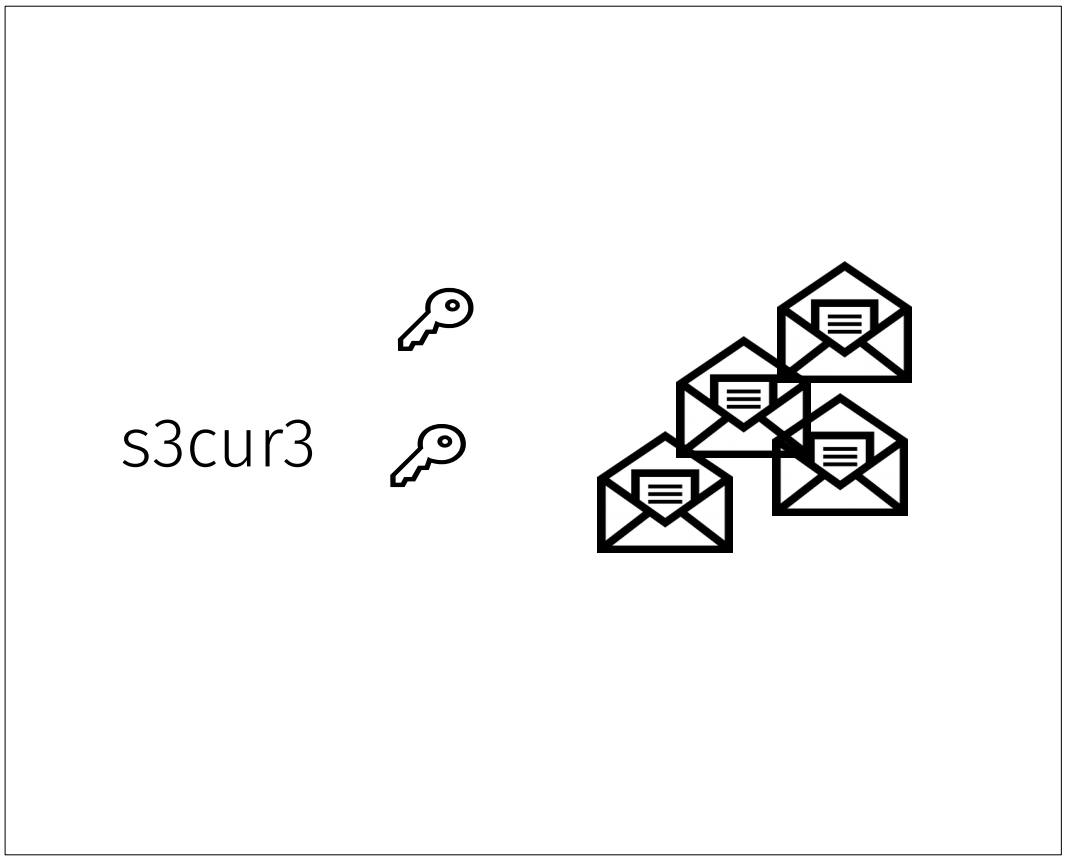
Abrufen



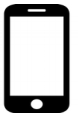
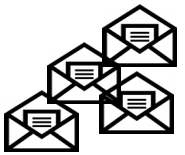
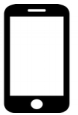
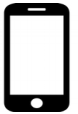
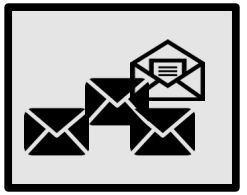


Abrufen





E2E?

	Benutzer*in	Anbieterin
		
PGP		
PGP+mail-crypt		

mail-crypt

Dovecot IMAP Server Plugin.

Mails werden verschlüsselt geschrieben und beim lesen entschlüsselt.

mail-crypt in 10 Sekunden

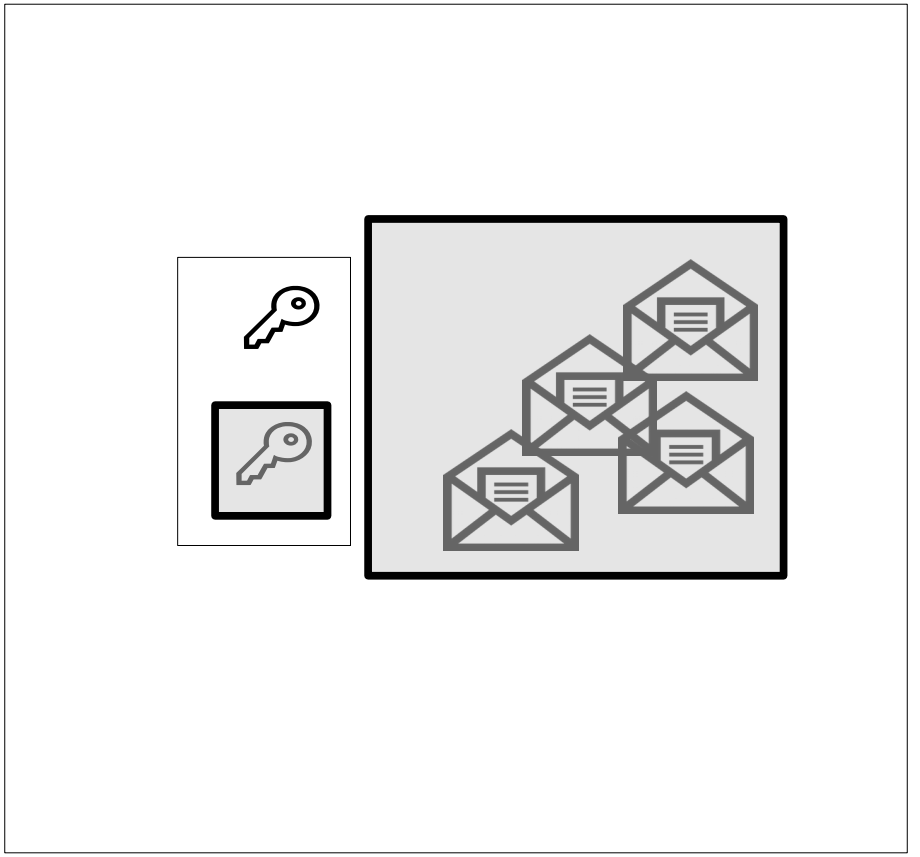
```
mail_attribute_dict = file:%h/Maildir/dovecot-attributes
mail_plugins = $mail_plugins mail_crypt

plugin {
  mail_crypt_curve = secp521r1
  mail_crypt_save_version = 2
  mail_crypt_require_encrypted_user_key = yes
}
```

Authentication muss zusätzliches Feld liefern: `userdb_mail_crypt_private_password`

Schlüsselverwaltung

In Dovecot

Probleme:
PW ändern,
wiederherstellen



mail-crypt bei immerda.ch

1. mail-crypt Settings
2. Schlüsselverwaltung
3. Wiederherstellung

mail-crypt bei immerda.ch

```
mail_plugins = $mail_plugins mail_crypt

Plugin { mail_crypt_save_version = 0 }
```

Ausgeschaltet per default.
Zur Migration bestehender Mailboxen!

Global Key

User Keys: Dovecot verwaltet Keys.

Global Keys: Key extern, global pro Prozess, aber kann pro User beim Login konfiguriert werden.

mail-crypt bei immerda.ch

```
mail_plugins = $mail_plugins mail_crypt

Plugin { mail_crypt_save_version = 0 }
```

Pro Account:

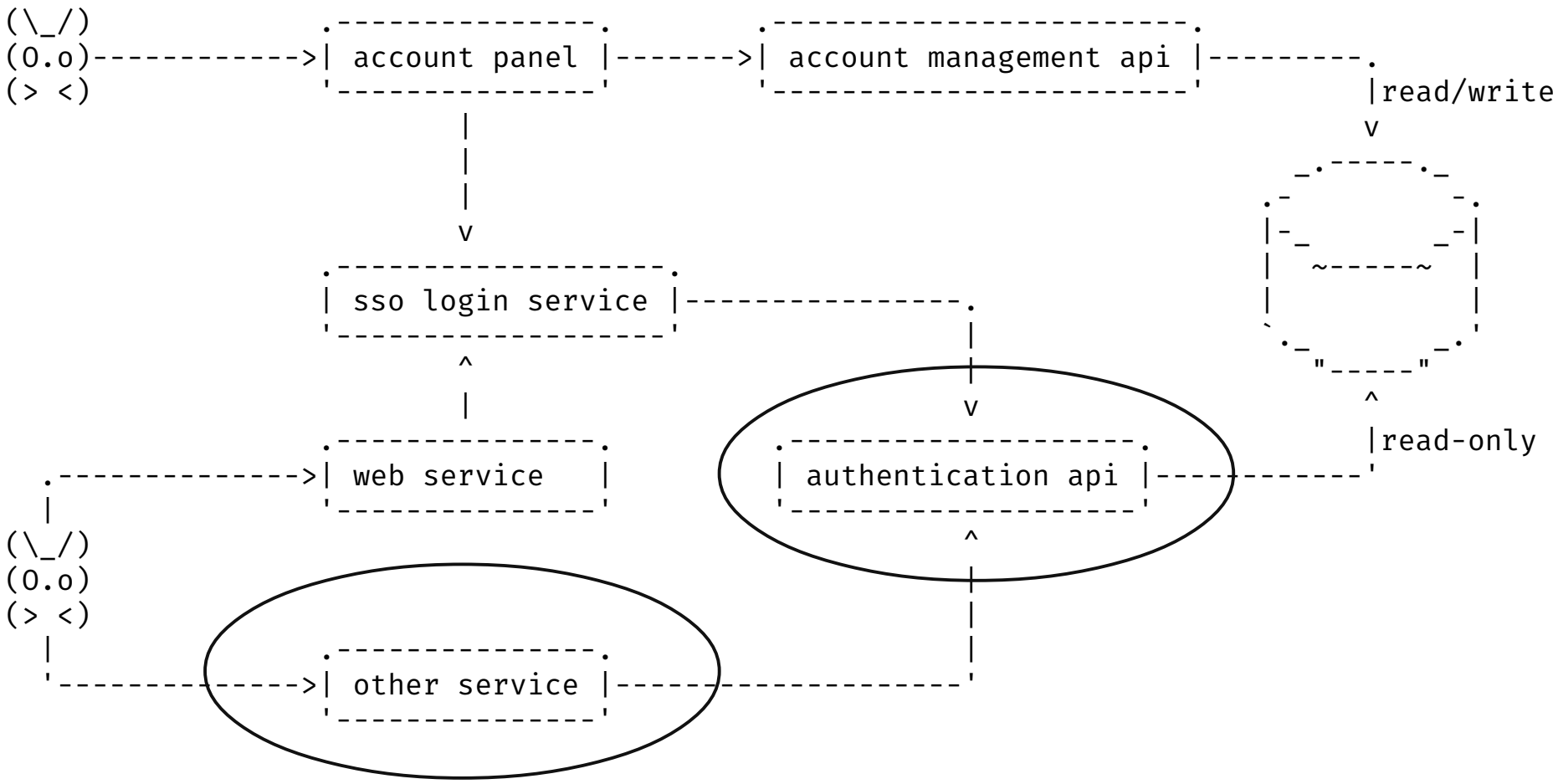
```
userdb_mail_crypt_save_version = 2
userdb_mail_crypt_global_public_key = …
userdb_mail_crypt_global_private_key = …
```

mail-crypt bei immerda.ch

IAPI ist unsere interne Schnitstelle
zur Ressourcen und
Benutzer*innen verwaltung.

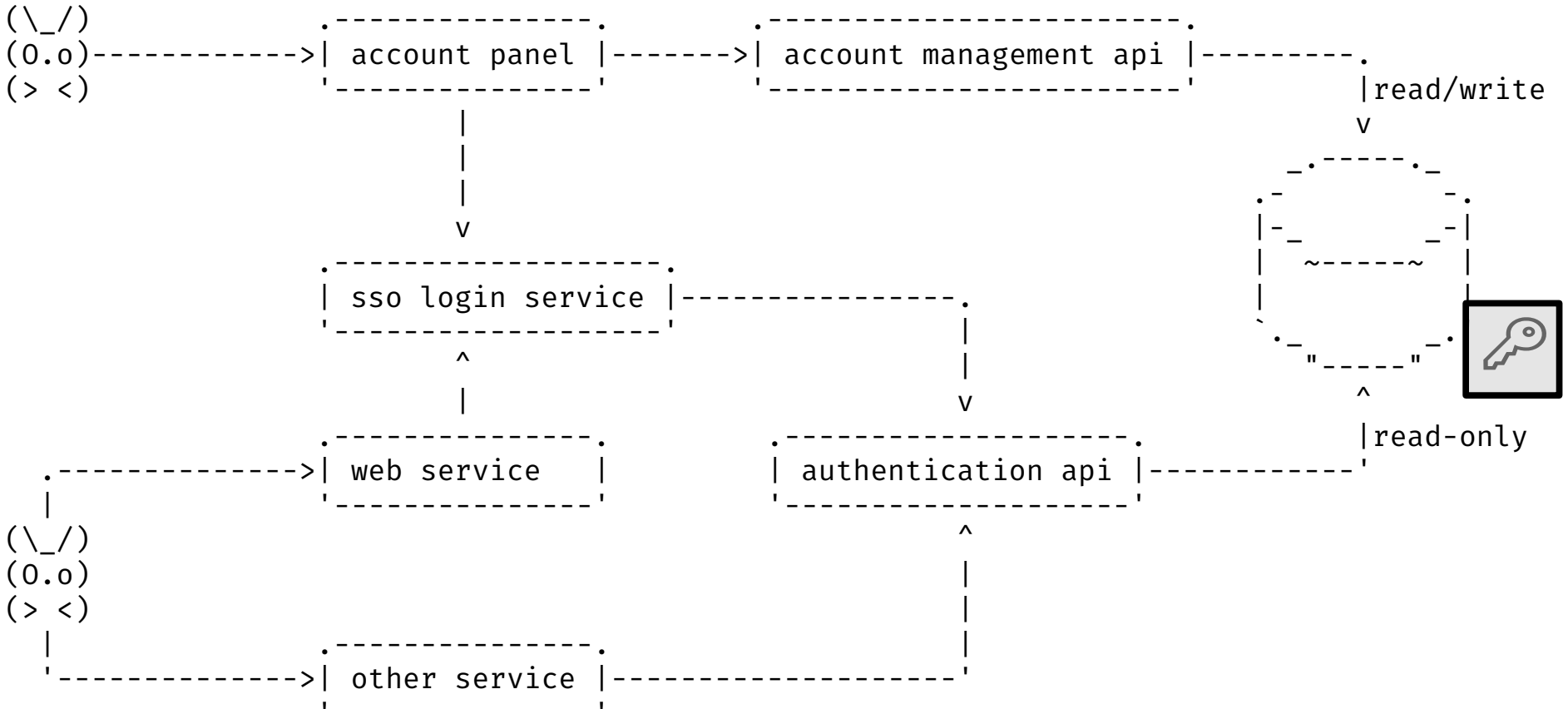
Login Endpunkt für Dovecot liefert
den Schlüssel.

https://code.immerda.ch/immerda/apps/iapi-hack


(_/)
(O.o)
(> <)
account panel
account management api
read/write
sso login service
read-only
web service
authentication api
(_/)
(O.o)
(> <)
other service

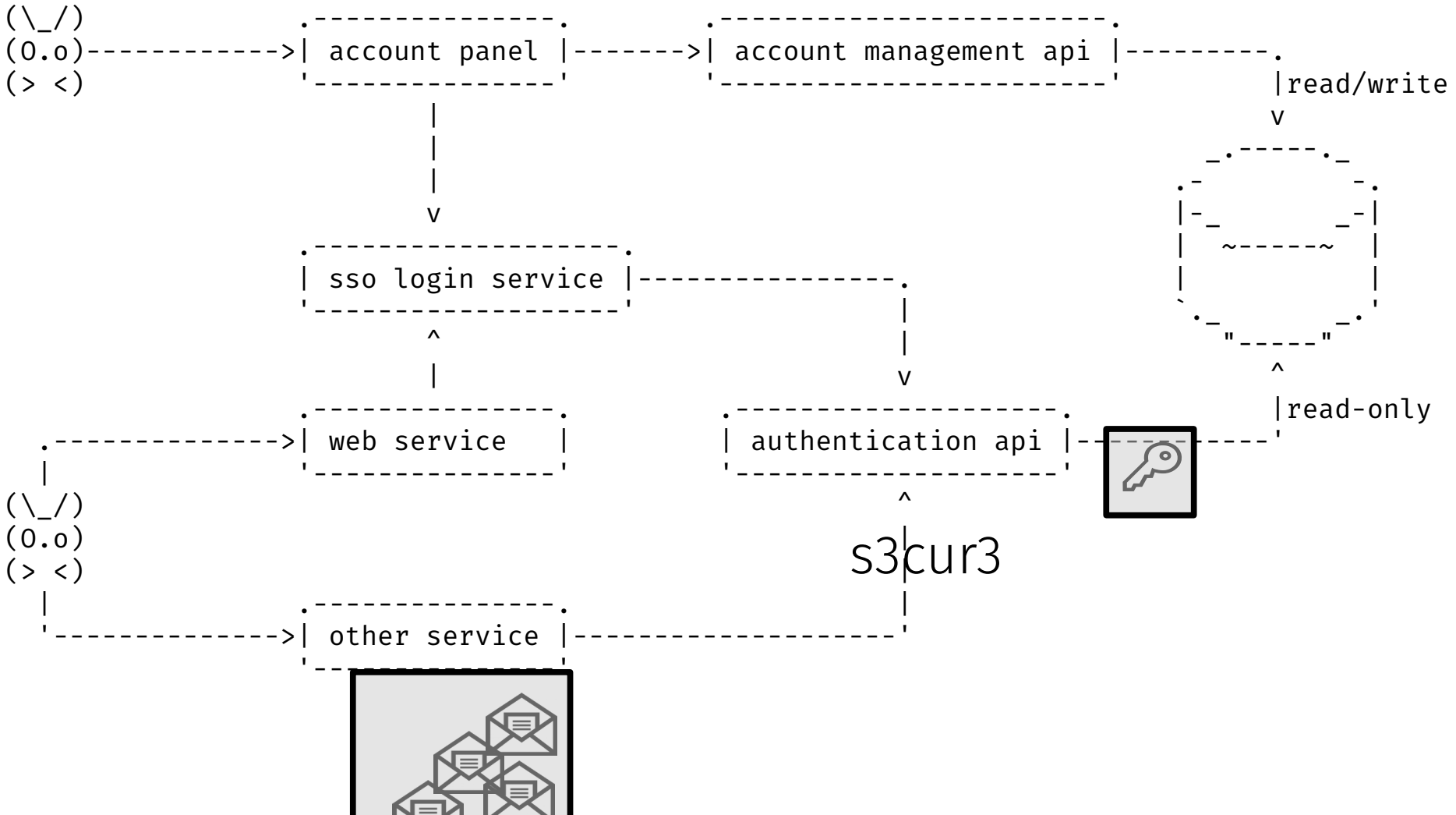
```
dovecot$ echo -n 'auth:user@imr.ch#s3cur3'
                 | nc -U /var/run/iapi/dovecot
{
  "result":"success",
  "login":{
    "USER":"user@imr.ch",
    …,
    "userdb_mail_crypt_save_version":"2",
    "userdb_mail_crypt_global_public_key":"...",
    "userdb_mail_crypt_global_private_key":"...",
    …,
    "EXTRA":"userdb_mail_crypt_save_version
                  userdb_mail_crypt_global_public_key
                  userdb_mail_crypt_global_private_key"}
}
```

IMAP login

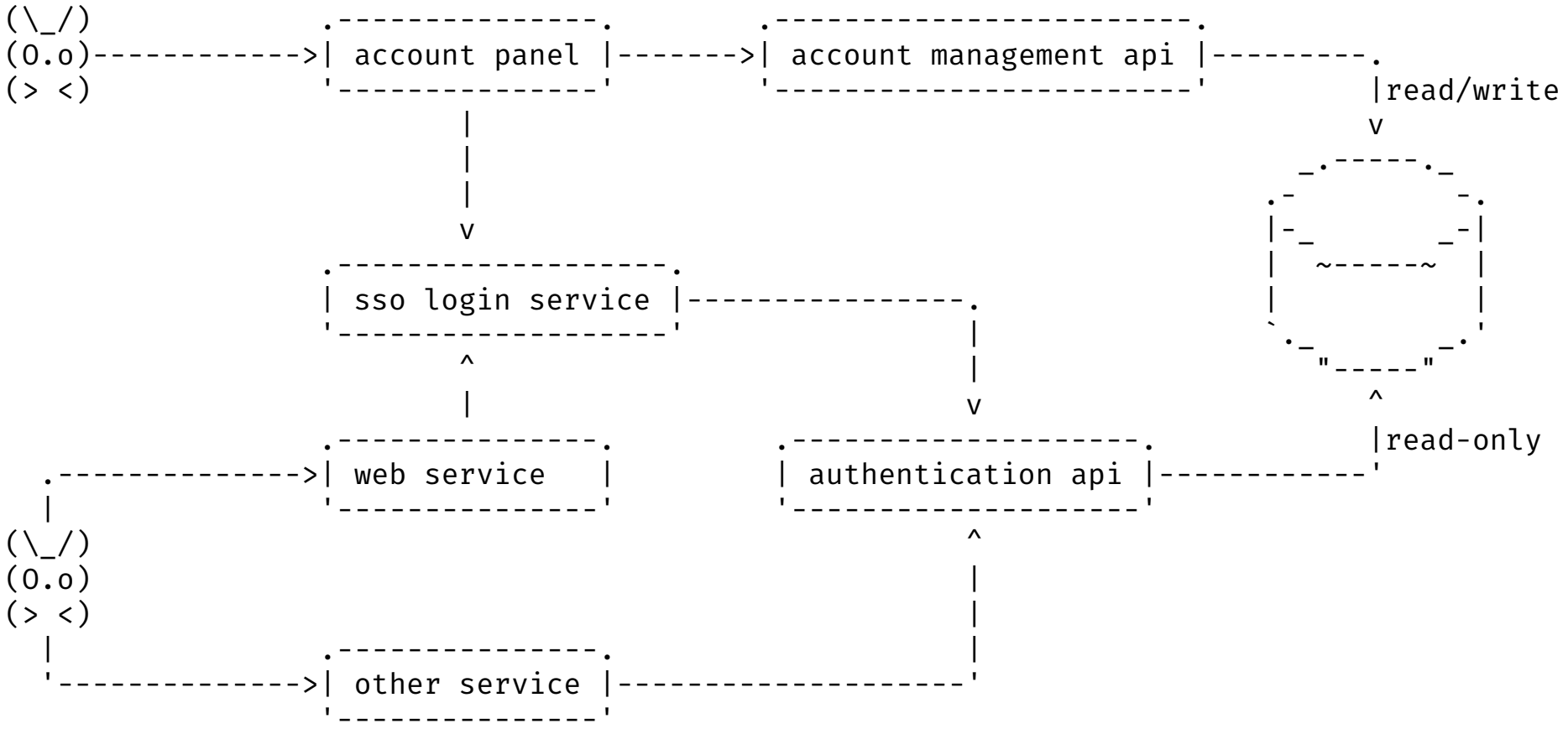


s3cur3

IMAP login

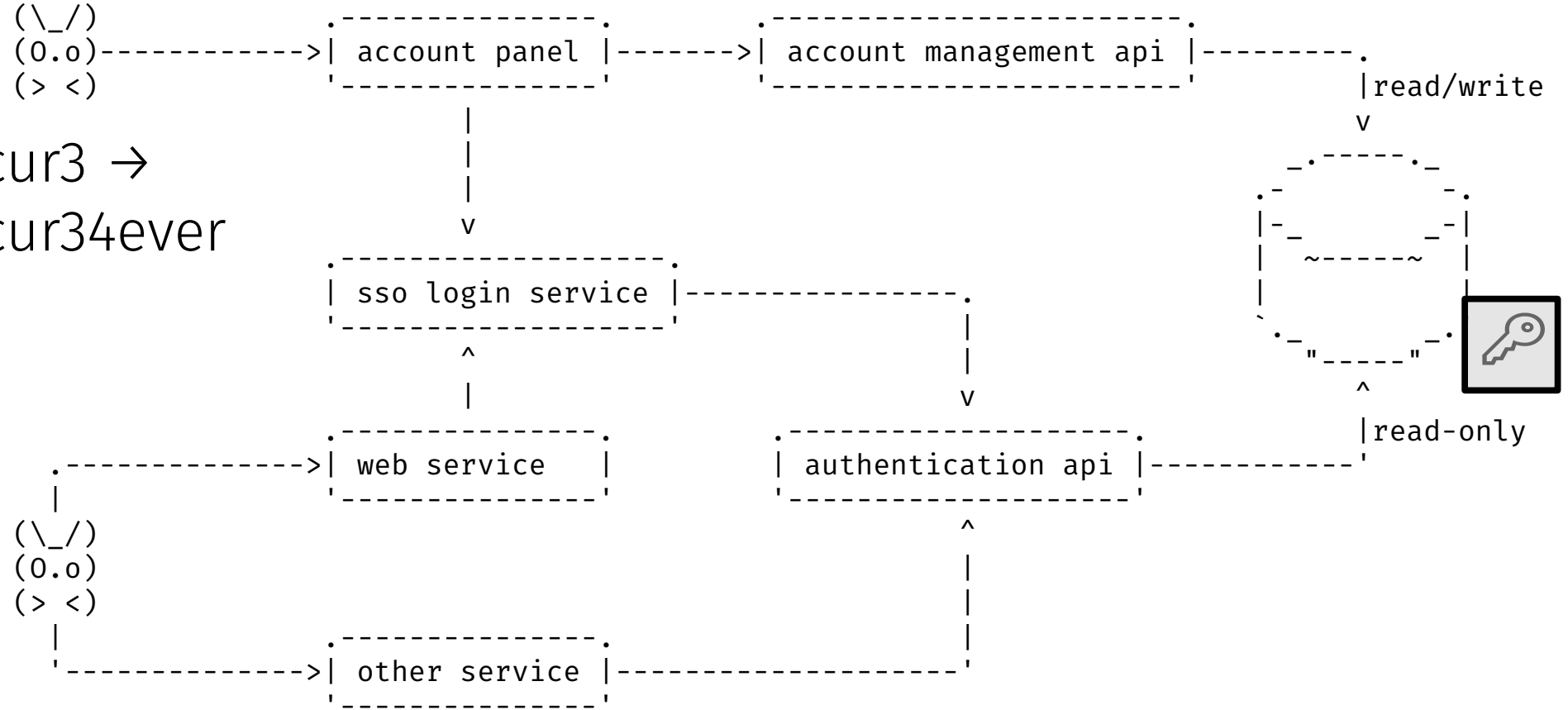

(_/)
(O.o)
(> <)
account panel
account management api
read/write
read-only
sso login service
web service
authentication api
(_/)
(O.o)
(> <)
s3cur3
other service

IMAP login

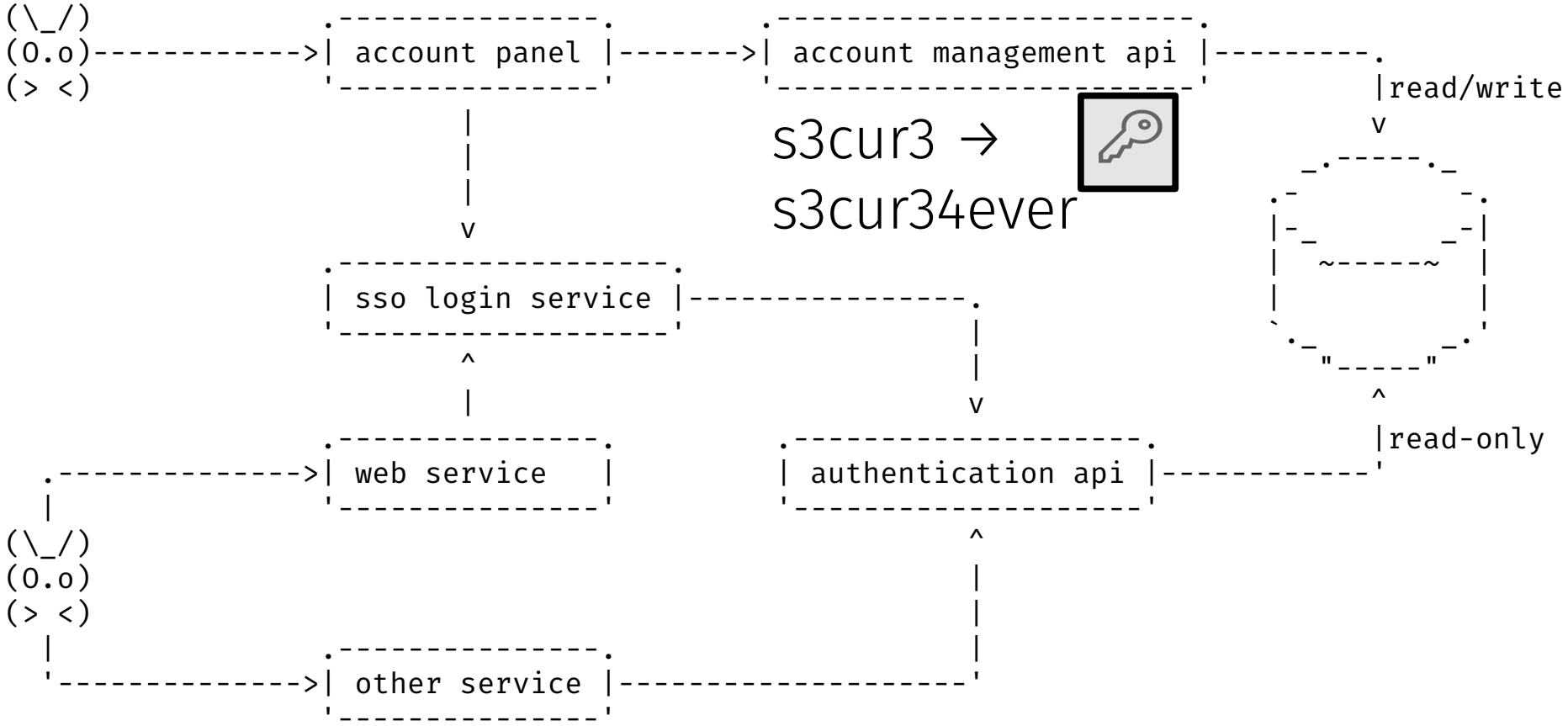

(_/)
(O.o)
(> <)
account panel
account management api
read/write
sso login service
web service
authentication api
read-only
(_/)
(O.o)
(> <)
other service

PW ändern

s3cur3 →
s3cur34ever



PW ändern


(_/)
(O.o)
(> <)
account panel
account management api
s3cur3 →
s3cur34ever
read/write
read-only
sso login service
web service
authentication api
other service

Wiederherstellungscode

Wiederherstellungscode, den die Benutzer*innen selber aufbewahren müssen.

Dieser beinhaltet den persönlichen mail-crypt Key, verschlüsselt mit einem offline Key von uns.

UX

Vor allem: trade-offs

Kein merklicher Unterschied

Knackpunkt: Passwortverlust

Schwierig zu erklären

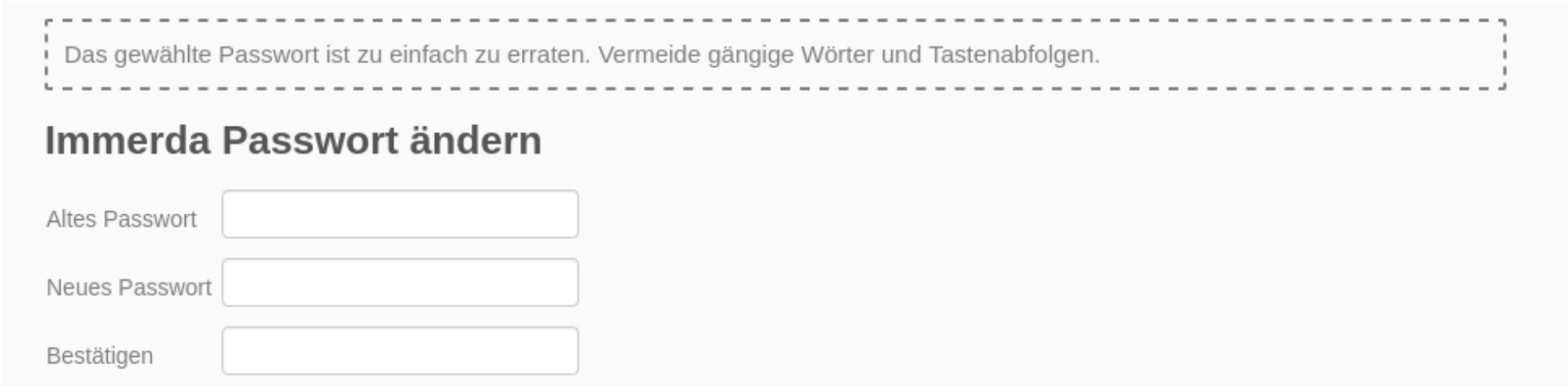
Auf unserem Server sind deine Mails kryptographisch mit deinem Passwort geschützt. Im Unterschied zu anderen Anbietern können wir deine Nachrichten nicht einsehen. Wenn du dein Passwort vergisst, musst du uns einen Wiederherstellungscode schicken. Ohne diesen Code, gehen deine alten Nachrichten verloren, wenn wir dein Passwort zurücksetzen müssen. Bewahre den Code sicher auf.

◯ Sende mir einen Wiederherstellungscode an meine Wiederherstellungs Email Adresse.

◯ Ich kann den Wiederherstellungscode jetzt sicher aufbewahren. (DATENVERLUST beim Verlust von Passwort und Code)

◯ Ich kann den Wiederherstellungscode jetzt gerade nicht aufbewahren und werde ihn später generieren.

Die meistgehasste Fehlermeldung



Konto

Konzept: User*innenpasswörter sind schwach

Die Zeiten ändern sich..

vs.

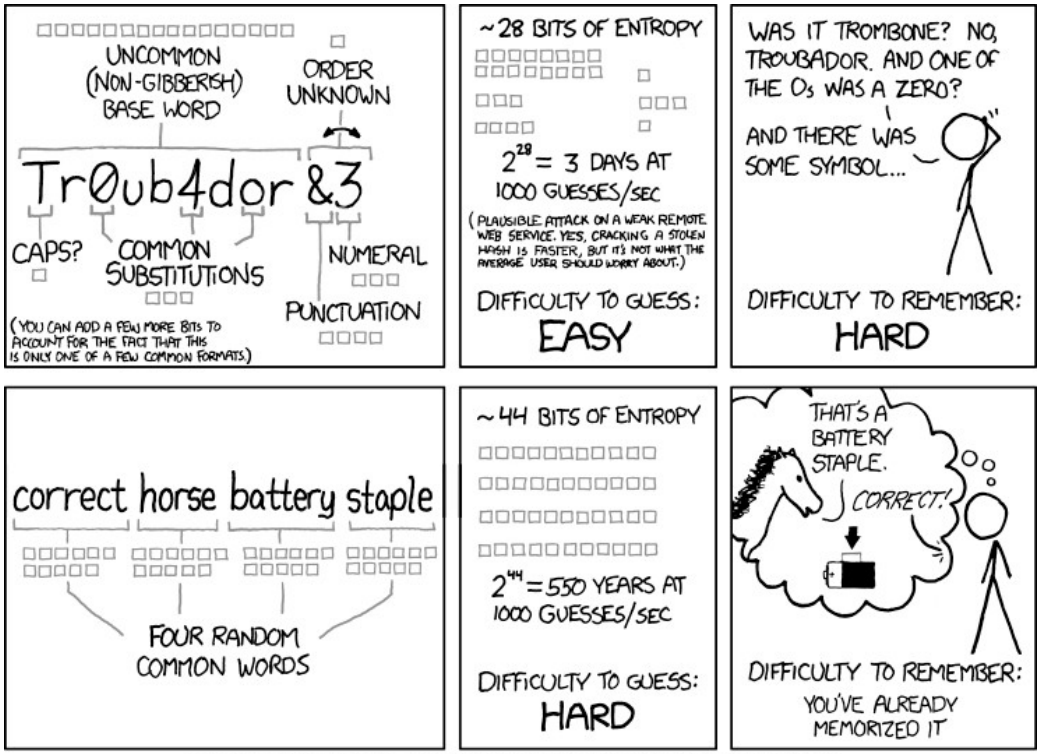
Konto und Daten

ein Konto für eine vielzahl von Diensten
und damit eine Vielzahl von Daten

unterschiedliche Daten auf unterschiedlichen Geräten

Zugang zu einem Teil deiner Daten muss nicht Zugang zu deinem Konto bedeuten

Die Sicherheit ist nur so stark, wie das schwächste Glied in der Kette



https://www.xkcd.com/936/

Applikationspasswörter

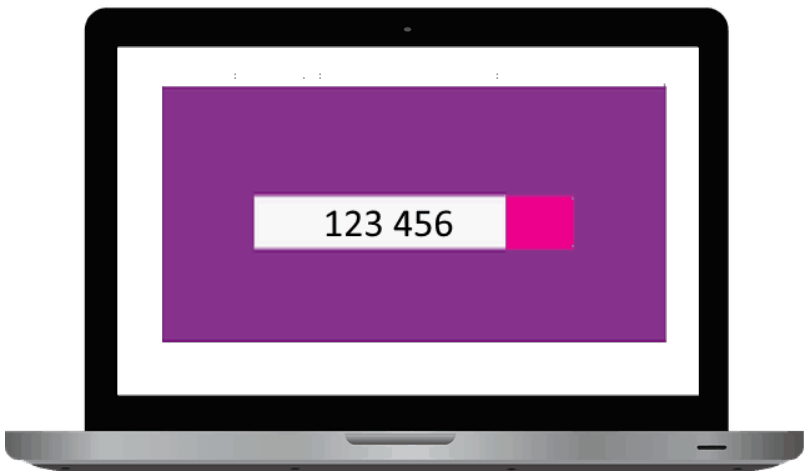
generierte zufällige Passwörter

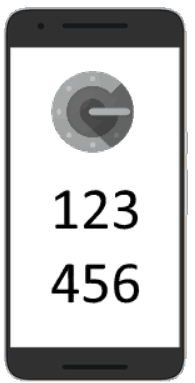
Kein Zugang zum Konto

Zum Teil in Dienste integriert (bspw. Nextcloud)

Ermöglicht die Sicherung deines Hauptpasswortes mit einem zweiten Faktor

zweiter Faktor





Fazit

Gründet community Provider! Es öffnet neue Perspektiven.

mail-crypt funktioniert, verwendet es!

Passwortwechsel, Passwort recovery und die UX muss gut überlegt werden.

E-Mail ist nur eine von vielen Datenablagen.
Es gibt noch viel zu tun!

slides.immerda.ch/winterkongress20.pdf