

Privacy with Cryptomator – End-to-End Cloud Encryption

User-friendly and Open Source



Cryptomator

Markus Kreuzsch & Christian Schmickler

© Skymatic

Privacy & Informational Self-Determination

Turbulent Times for Privacy and Data Security

Political View

Edward Snowden – NSA Spying Scandal 2013

Safe Harbor – 2000-2015

EU-US Privacy Shield – since 2016

Trump: Abolition of Privacy Act for Foreigners



Turbulent Times for Privacy and Data Security

Political & Business View

Governments

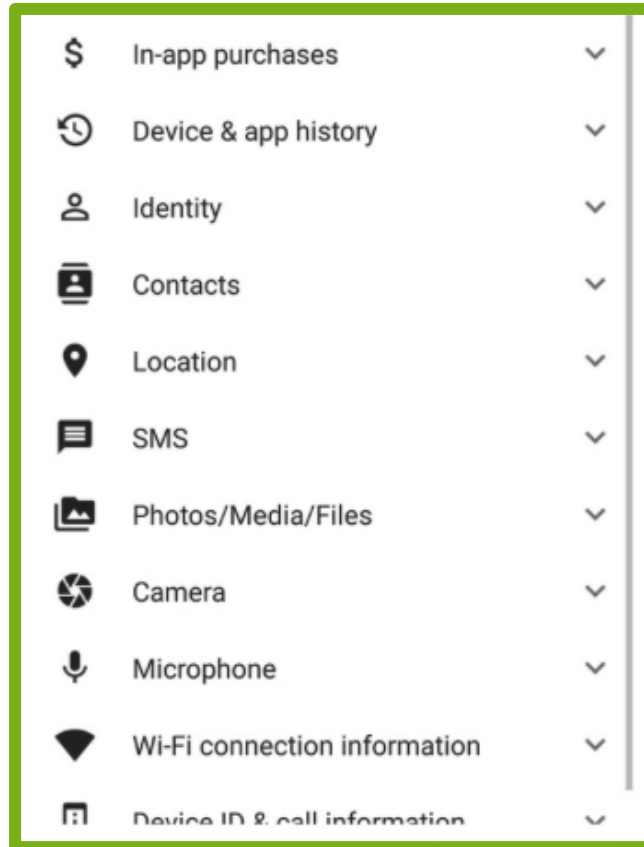
Security

Private Corporations

Business Model

Turbulent Times for Privacy and Data Security

Legal



Turbulent Times for Privacy and Data Security

Legitimate?

Address Book.

*You provide us the phone numbers of WhatsApp users and your other contacts in your mobile phone address book on a regular basis. **You confirm you are authorized to provide us such numbers** to allow us to provide our Services.*

→ Consent by third parties

Turbulent Times for Privacy and Data Security

Illegal



Cryptomator

© Skymatic

Surveillance is Easy & Cheap



Desire for Informational Self-Determination

Highly Pronounced

84%

...say no

„Are you okay if somebody knows something about you or your behavior without your explicit consent?“

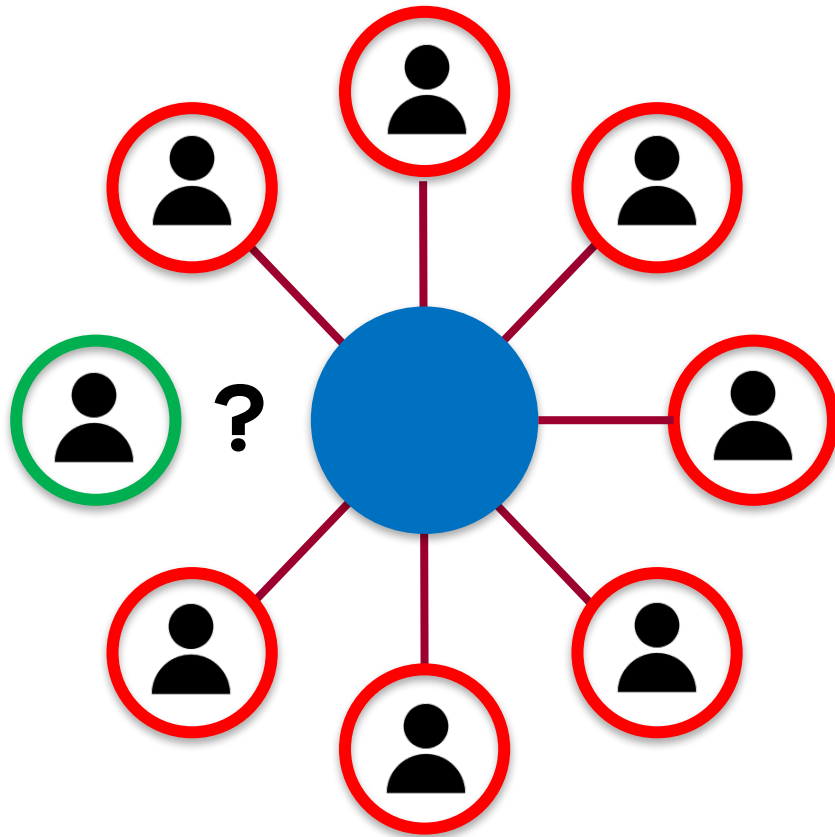






Network Effects

Privacy Paradox – Explanations



Positive Network Effects

Social Coercion

Vocational Necessity

Sharing is Fun

Privacy Paradox – Explanations

Human beings love
to communicate.

Sharing information in
Social Media gives joy.



Atypical form of Interaction

Privacy Paradox – Explanations

Normal reaction to the unfamiliar = Caution
Reaction in the digital realm = Carelessness

1. Cautionary instincts are linked to physical presence
2. Perceived anonymity
3. Familiar device (best friend)
4. No surface feel: Every click feels the same



Swarm Behavior / Herd Instinct

Privacy Paradox – Explanations

Everybody uses it, therefore,
it cannot be (that) harmful.

“I have nothing to hide.”



Abstract Harm

Privacy Paradox – Explanations

...hard to grasp

...will occur in an indefinite future

...will occur only potentially

Consequences of Missing Privacy

Self-Censorship

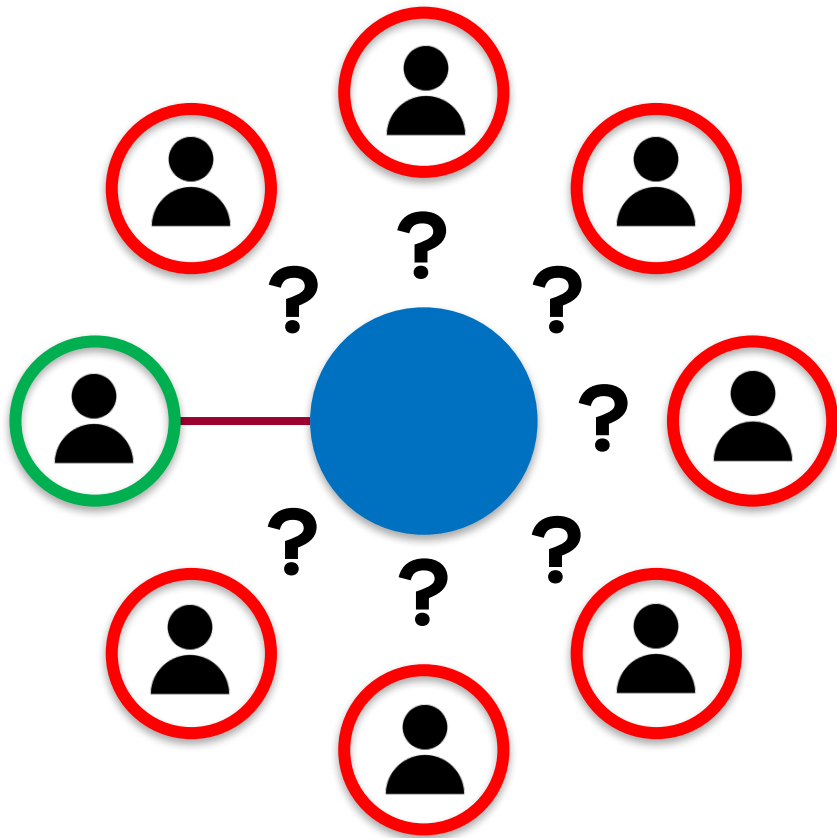
Classification

Manipulability

Presumption of Innocence

Privacy & Data Security – A Collective Challenge

Network Effects



Secure Tools for Everyone

Everyone protects Everyone
(e.g., Email Provider,
App Permissions, “Flagging”)

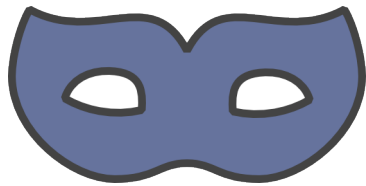




Cryptomator



Cryptomator Represents...



Privacy



Usability



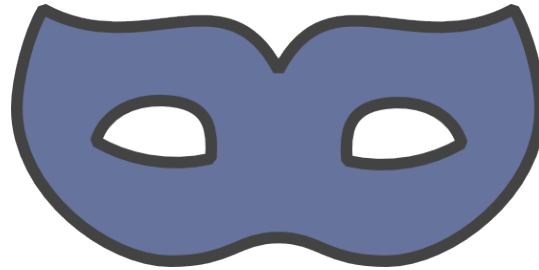
Open Source



for the cloud.



Privacy



End-To-End
Encryption

Zero
Knowledge



Usability



Simple UI

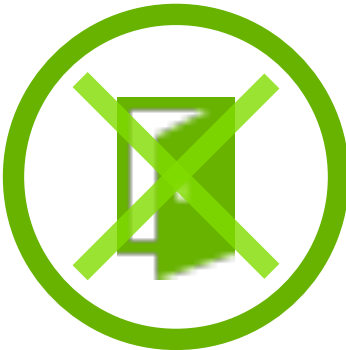
~~Crypto
Knowledge~~

~~Social
Engineering~~

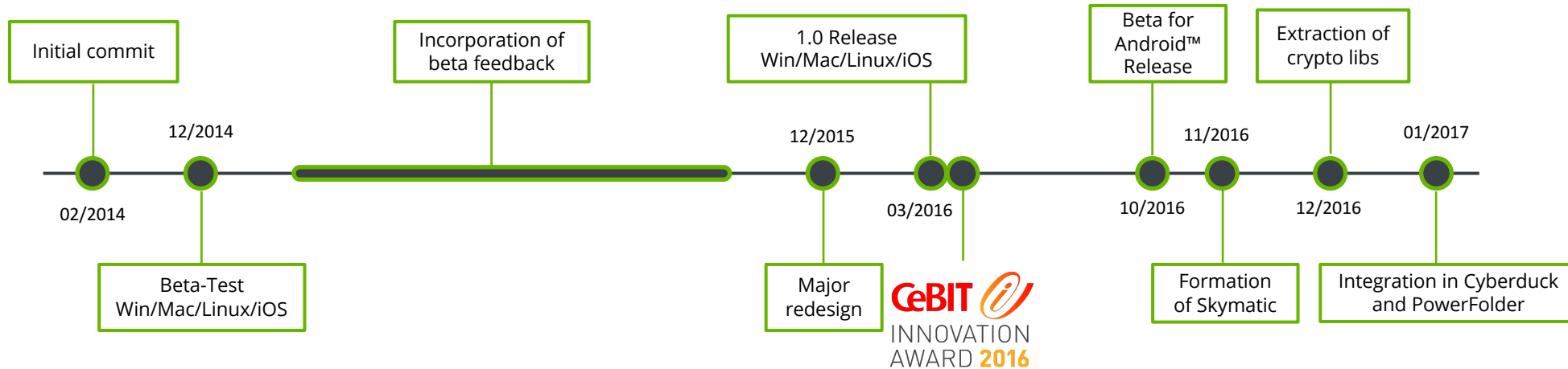
Open Source



AGPLv3



A Short History of Cryptomator



Supported Platforms

Cryptomator supports the following OS

Desktop



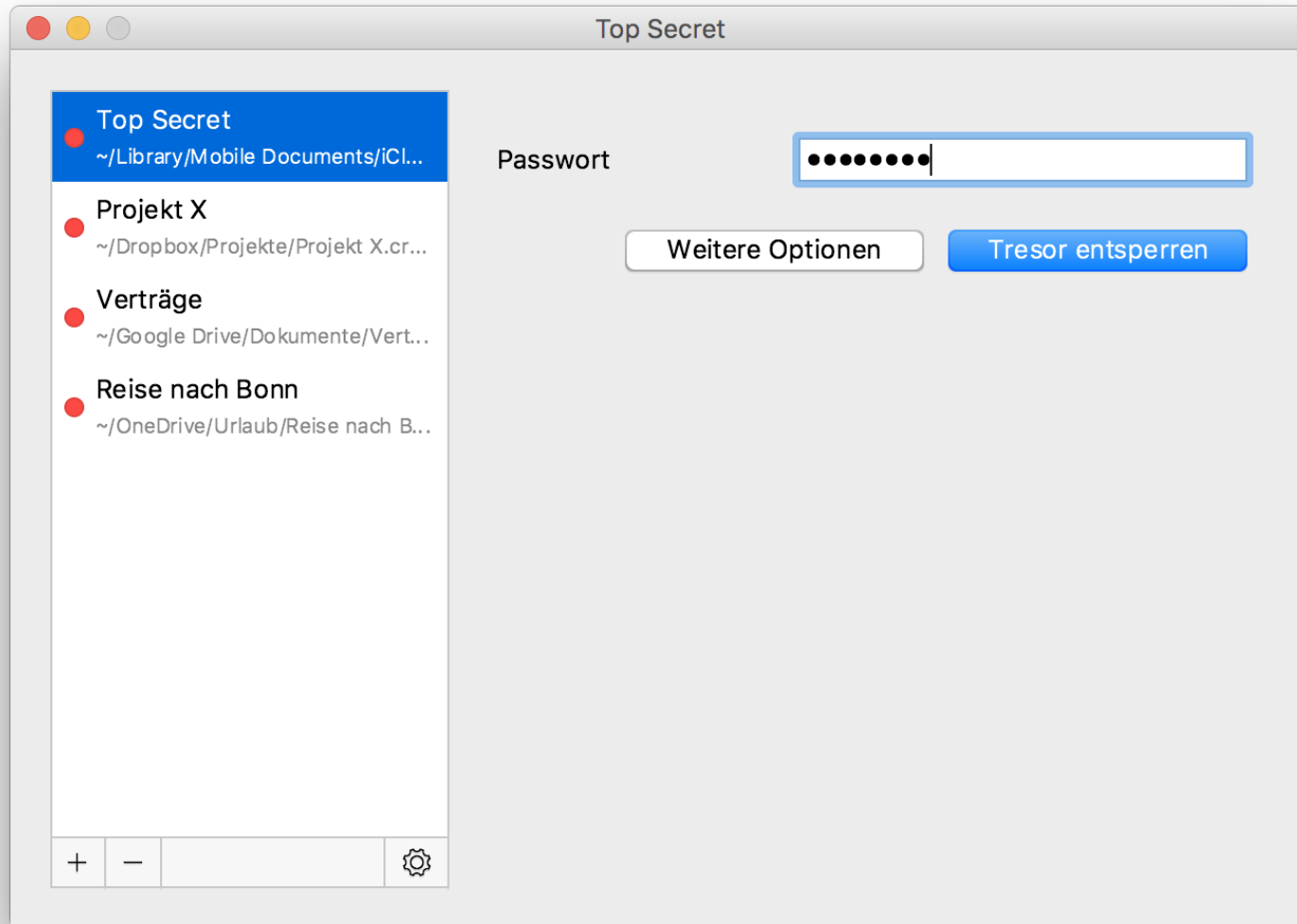
Windows
macOS
Linux

Mobile

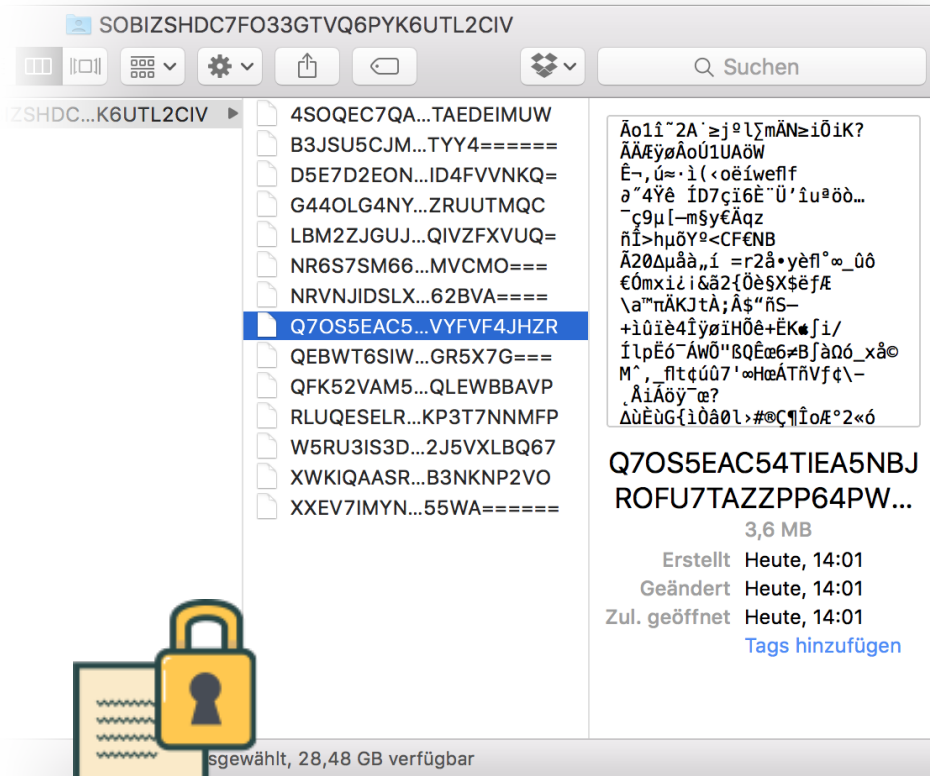


iOS
Android (Beta)

Cryptomator for Desktop



Cryptomator for Desktop



SOBIZSHDC7FO33GTVQ6PYK6UTL2CIV

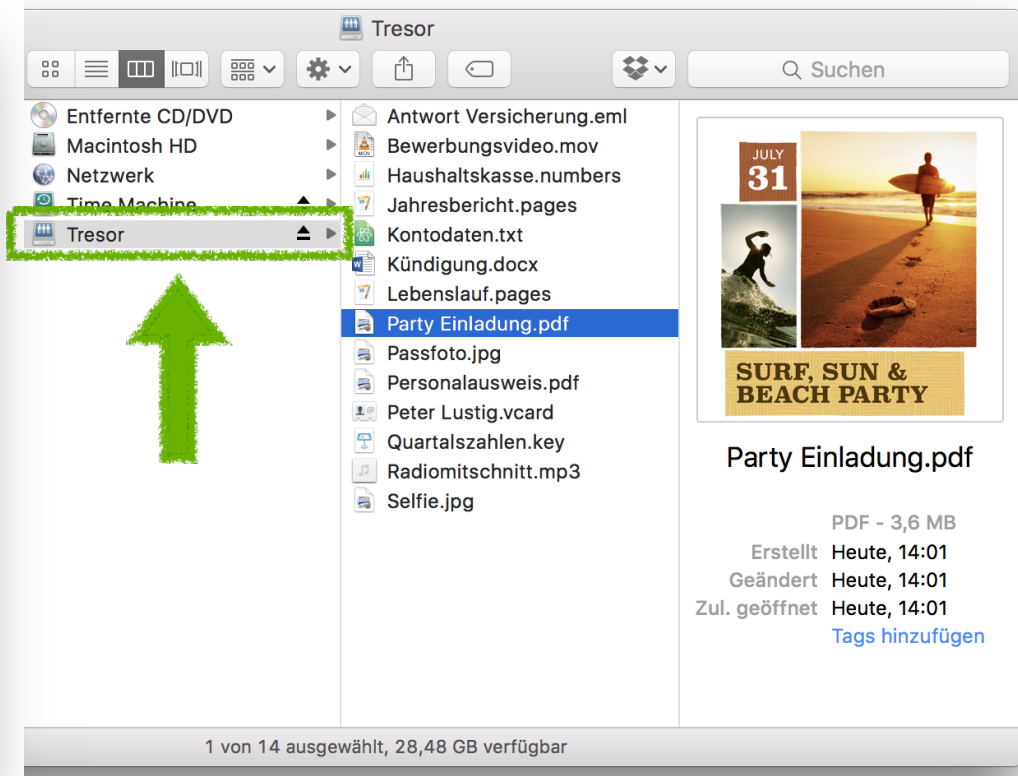

Suchen

ZSHDC...K6UTL2CIV

- 4SOQEC7QA...TAEDEIMUW
- B3JSU5CJM...TTY4=====
- D5E7D2EON...ID4FVVKQ=
- G44OLG4NY...ZRUUTMQC
- LBM2ZJGUJ...QIVZFXVUQ=
- NR6S7SM66...MVCMO===
- NRVNJIDSLX...62BVA=====
- Q7OS5EAC5...VYFVF4JHZR**
- QEBWT6SIW...GR5X7G===
- QFK52VAM5...QLEWBBAVP
- RLUQESLR...KP3T7NNMFP
- W5RU3IS3D...2J5VXLBQ67
- XWKIQAASR...B3NKNP2VO
- XXEV7IMYN...55WA=====

Q7OS5EAC54TIEA5NBJ
ROFU7TAZZPP64PW...
3,6 MB
Erstellt Heute, 14:01
Geändert Heute, 14:01
Zul. geöffnet Heute, 14:01
[Tags hinzufügen](#)

sgewählt, 28,48 GB verfügbar



Tresor

Suchen

- Entfernte CD/DVD
- Macintosh HD
- Netzwerk
- Time Machine
- Tresor**

- Antwort Versicherung.eml
- Bewerbungsvideo.mov
- Haushaltskasse.numbers
- Jahresbericht.pages
- Kontodaten.txt
- Kündigung.docx
- Lebenslauf.pages
- Party Einladung.pdf**
- Passfoto.jpg
- Personalausweis.pdf
- Peter Lustig.vcard
- Quartalszahlen.key
- Radiomitschnitt.mp3
- Selfie.jpg

Party Einladung.pdf
PDF - 3,6 MB
Erstellt Heute, 14:01
Geändert Heute, 14:01
Zul. geöffnet Heute, 14:01
[Tags hinzufügen](#)

1 von 14 ausgewählt, 28,48 GB verfügbar

Challenges when Targeting the Cloud

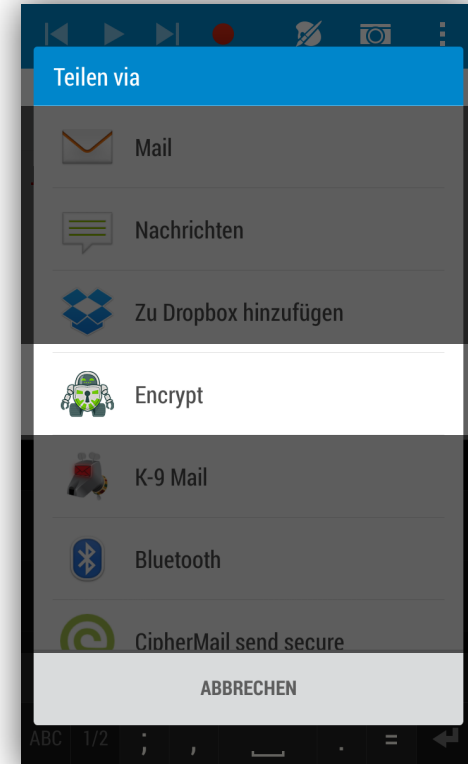
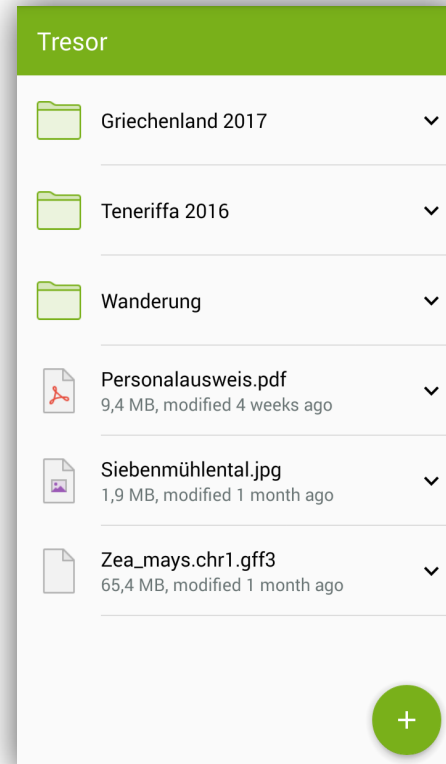
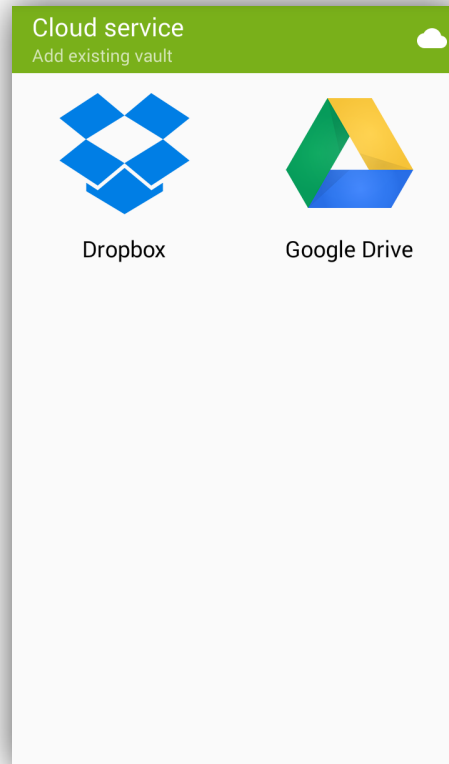
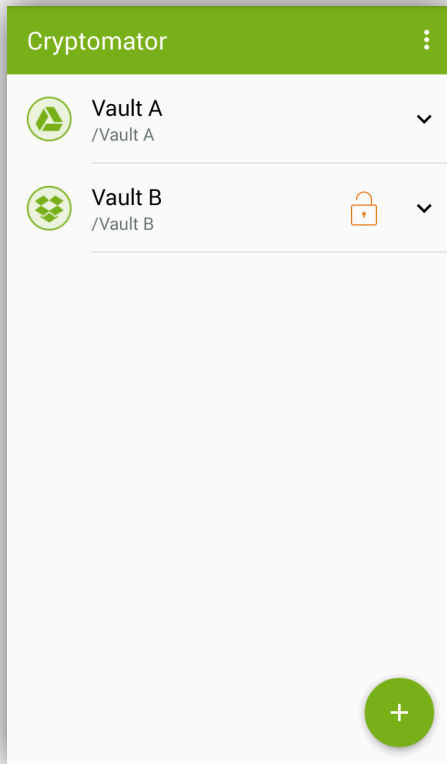
Efficient
syncing

No single
source of truth

Mobile access
scenarios



Cryptomator Beta for Android



Current and Planned Features

Backlog

Done

Background
up- &
download

Document
Provider

Basic file
browser

Vault
encryption &
decryption

Auto lock

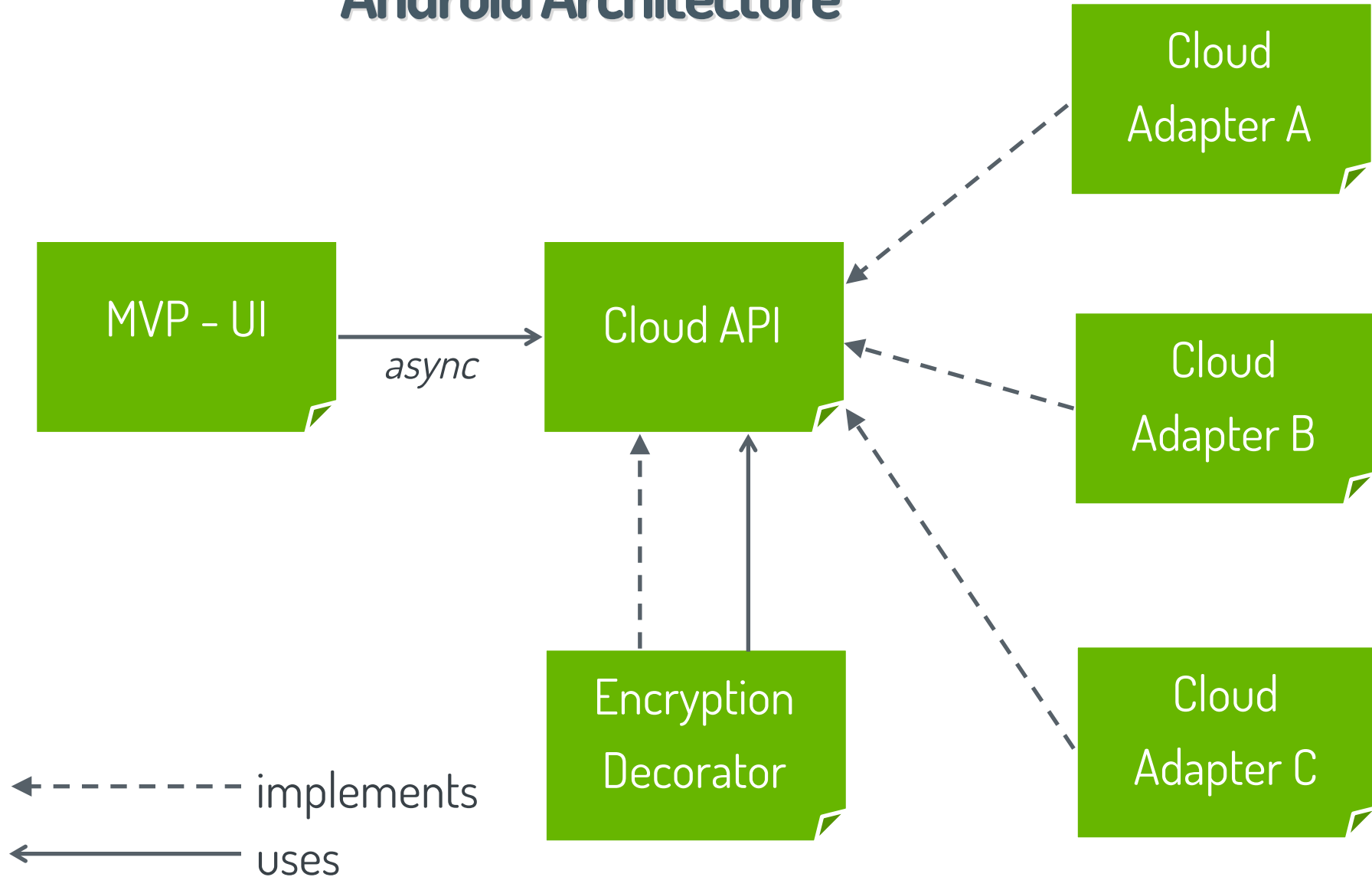
More
cloud services

Dropbox
support

Google Drive
support



Android Architecture



Encryption Scheme

Overview

Key-derivation



- 256-bit keys (enc + MAC)
- Passphrase per vault
- Key derivation using scrypt
- RFC 3394 AES key wrapping of generated keys

Name encryption

abc

- AES-SIV
- Base32 encoding of encrypted names

Content encryption

010010

- AES-CTR
- 256-bit key per file
- Usage of 32 KiB chunks
- HMACs authentication

Path shortening

.{1,255}

- Shortening of paths to less than 256 chars
- No security feature but only to provide compatibility

Structure obfuscation

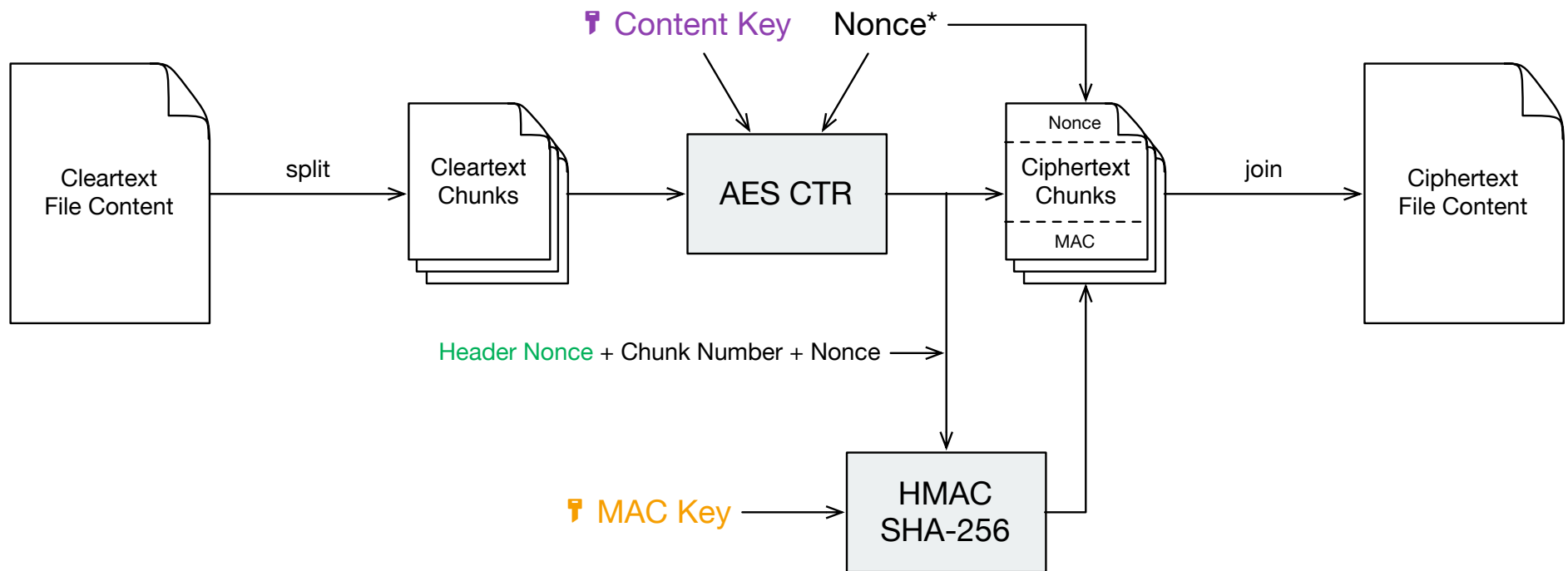
/d/NF/C7W3TUOVVYVQ

- UUID per directory
- Encrypted directories are placed next to each other
- No security feature but only to provide compatibility



Encryption Scheme

File Contents



full scheme described at <https://cryptomator.org/architecture/>

Future plans

Cryptomator for Business



- Cryptomator including key and user management
- Available as „On-Premise“ software and Software-as-a-Service
- License per user and month

FUSE and Dokany

- Alternative filesystem provision
- FUSE for Linux and macOS
- Dokany for Windows

Clouds for mobile apps



- Long term plan
- Not yet decided
- Document provider integration
- Open sourcing the cloud API and integrating third party implementations



Contact

Questions & Ideas? – Tell us!



info@skymatic.de



Skymatic UG (haftungsbeschränkt)
Grantham-Allee 2-8
53757 Sankt Augustin
Germany



Homepage
<https://cryptomator.org/>



Facebook
<https://facebook.com/Cryptomator>



Blog
<https://cryptomator.org/blog/>



Twitter
<https://twitter.com/Cryptomator>



GitHub
<https://github.com/cryptomator/cryptomator>