Cryptomator

by Skymatic

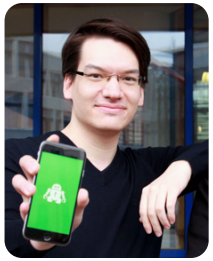
About Us

Figures and Facts

- Founded: 2016
- 4 founders, 2 developers
- 100% self-funded

Our Strengths

- Expertise in the fields of IT, business, and psychology
- Close connections to the open source community with access to broad expert knowledge



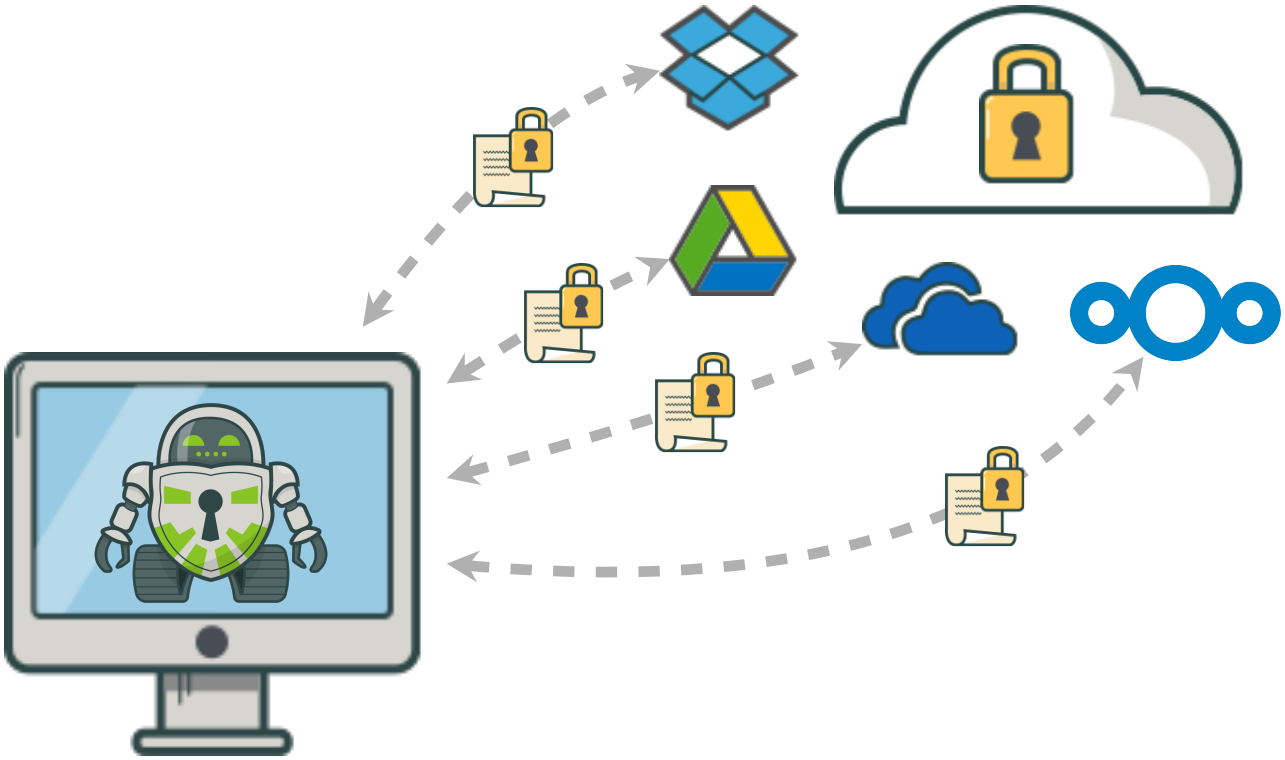
Tobias Hagemann
iOS Development, Project Management, Design

Markus Kreusch
Desktop & Android Development

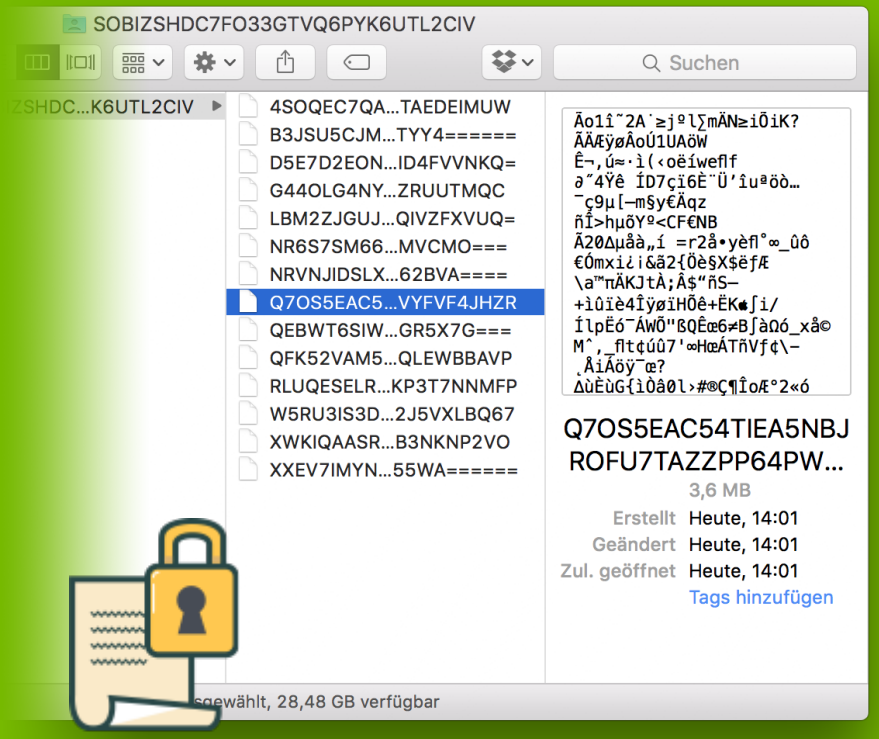
Sebastian Stenzel
Overall Architecture, Cryptography, Desktop Development

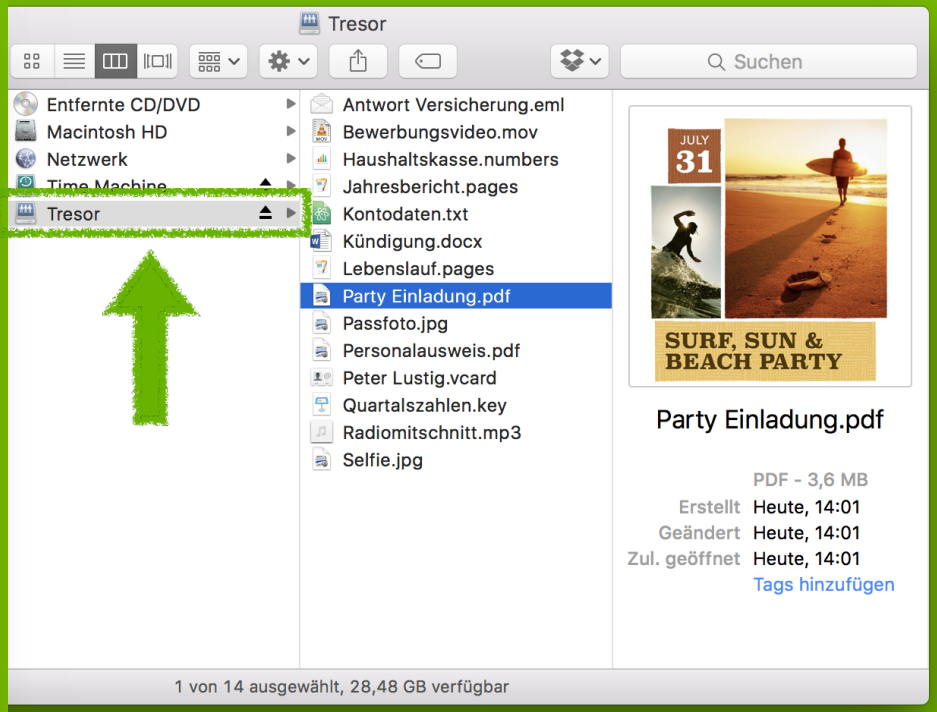
Christian Schmickler
Marketing, Sales, Finance

Client-Side Encryption for the Cloud



On-the-Fly Encryption





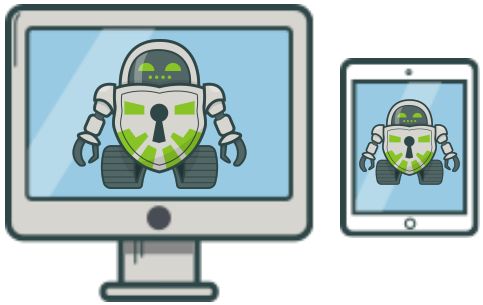
Runs on These Operating Systems

beta

Open Source → Transparency

Fields of Application

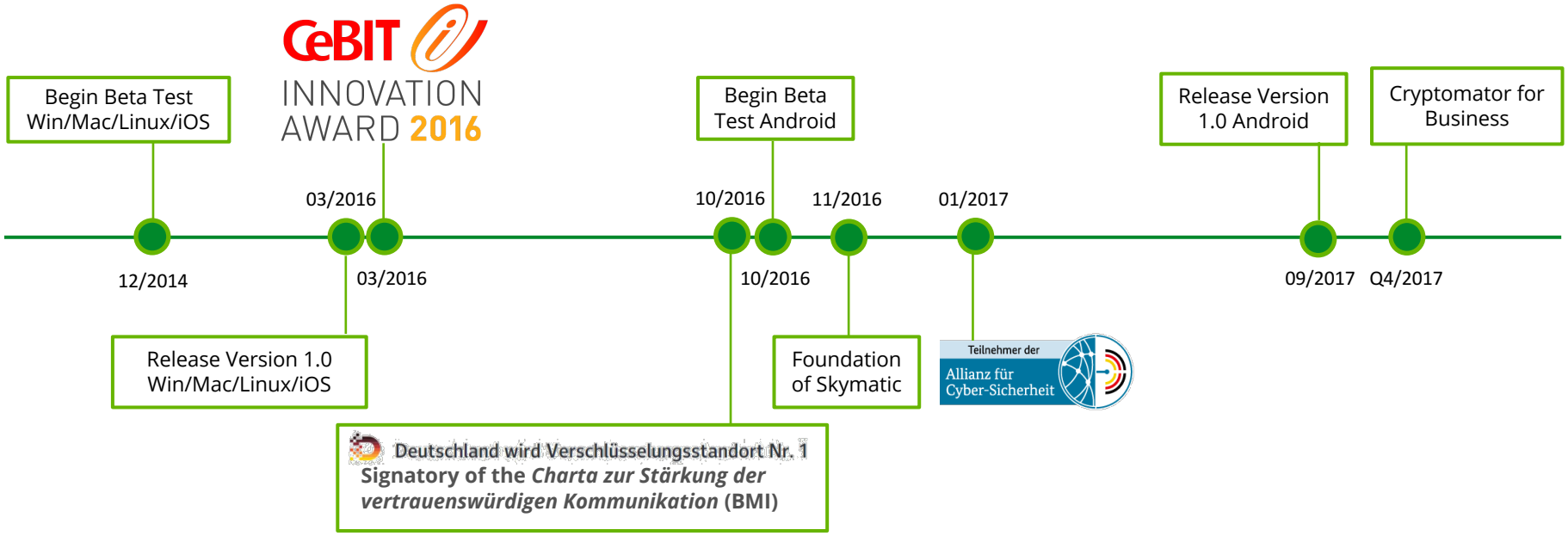
Cryptomator for Consumer



App White Labeling

Cryptographic Libraries

Milestones


Begin Beta Test Win/Mac/Linux/iOS
CeBIT INNOVATION AWARD 2016
Begin Beta Test Android
Release Version 1.0 Android
Cryptomator for Business
03/2016
10/2016
11/2016
01/2017
12/2014
03/2016
10/2016
09/2017
Q4/2017
Release Version 1.0 Win/Mac/Linux/iOS
Foundation of Skymatic
Teilnehmer der Allianz für Cyber-Sicherheit
Deutschland wird Verschlüsselungsstandort Nr. 1
Signatory of the Charta zur Stärkung der vertrauenswürdigen Kommunikation (BMI)

Encryption Scheme

Key Derivation

- 256 bit keys (Enc + MAC)
- Password for each vault
- Derivation with scrypt
- RFC 3394 AES key wrapping of generated master key

Name Encryption

abc

- AES-SIV
- UUID per directory
  → obfuscation of hierarchy
- Base32 encoding of encrypted names

Content Encryption

010010

- AES-CTR
- Utilization of 32 KiB blocks
- 256 bit key per file
- HMACs for authentication

Path Shortening

.{1,255}

- Shortening of paths to keep them below 256 characters
- No security functionality but important for compatibility

Obfuscation of Hierarchy

/d/NF/C7W3TUOVVYVQ

- All encrypted directories are paralleled
- Structure of directory is obfuscated

Cryptographic Libraries

CryptoFS (Java)

- NIO filesystem implementation
- Applications can write encrypted data on filesystem with conventional I/O methods
- After CryptoFS initialization, no code adjustment is necessary

CryptoLib (Java)

- High-level API for file name and file content encryption as well as integrity protection

WebDAV Servlet (Java)

- In JEE environments, access to cleartext data is possible via WebDAV
- Physical storage of data in combination with CryptoFS only encrypted

iOS (C, ObjC)

- C-based library similar to CryptoLib
- Linked to Apple Common Crypto and OpenSSL
- Porting and deployment in pure C projects possible

Web Browser (Javascript)

?

Workshop & Contact

Main Room, 4:30 PM

for Nextcloud (App) Developers with Storage Focus, Javascript Developers with Crypto Knowledge, Security/Privacy Enthusiasts

---

Homepage
https://cryptomator.org

Facebook
https://facebook.com/Cryptomator

Email
info@cryptomator.org

Twitter
https://twitter.com/Cryptomator

Cryptomator