



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

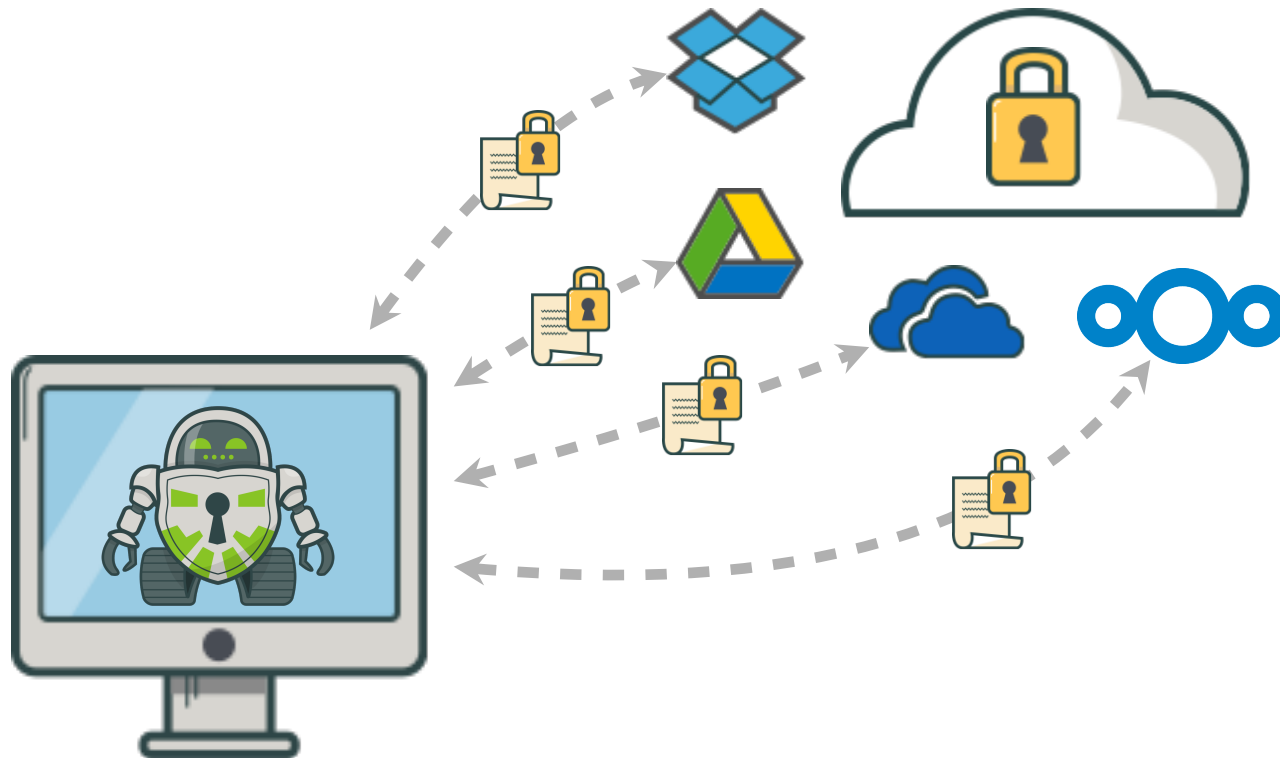


Sebastian Stenzel
Overall Architecture,
Cryptography, Desktop
Development



Christian Schmickler
Marketing, Sales, Finance

Client-Side Encryption for the Cloud



On-the-Fly Encryption

SOBIZSHDC7FO33GTVQ6PYK6UTL2CIV

Suchen

- 4SOQEC7QA...TAEDEIMUW
- B3JSU5CJM...TYY4=====
- D5E7D2EON...ID4FVVNKQ=
- G44OLG4NY...ZRUUTMQC
- LBM2ZJGUJ...QIVZFXVUQ=
- NR6S7SM66...MVCMO===
- NRVNJIDSLX...62BVA=====
- Q7OS5EAC5...VYFVF4JHZR**
- QEBWT6SIW...GR5X7G===
- QFK52VAM5...QLEWBBAVP
- RLUQESELR...KP3T7NNMFP
- W5RU3IS3D...2J5VXLBQ67
- XWKIQAASR...B3NKNP2VO
- XXEV7IMYN...55WA=====

Äo1i~2A'≥j°lÿmÄN≥i0iK?
ÄÄËÿøÄoú1UAöw
É-,ú≈·i(·oëiweff
ä~4Yè ID7çï6È"ú'iu°öð...
-ç9u[-m\$y€Äqz
ñI>hµøY°<CFENB
Ä2ØΔµää,,i =r2ää·yèñ°∞_úð
€0mxiz i&ä2{0è\$X\$ëfÆ
\\a"nÄKJtÄ;Ä\$"ñS-
+iüie4IÿøiH0è+EK*f/i/
ÍlpÉó~Äw0"ßQÈæ6#BjãQó_xää°
M',_fltdúú7'∞HæÁTñVfç\~
.ÄiÄöÿ~æ?
ΔüÈüG{i0ää0l>#@Ç¶iøÆ°2<ó

**Q7OS5EAC54TIEA5NBJ
ROFU7TAZZPP64PW...**

3,6 MB

Erstellt Heute, 14:01
Geändert Heute, 14:01
Zul. geöffnet Heute, 14:01
[Tags hinzufügen](#)

1 ausgewählt, 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

Runs on These Operating Systems



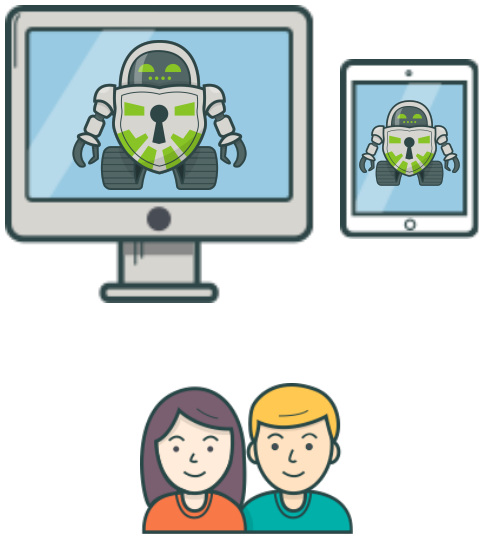
beta

Open Source → Transparency



Fields of Application

Cryptomator for Consumer



App White Labeling

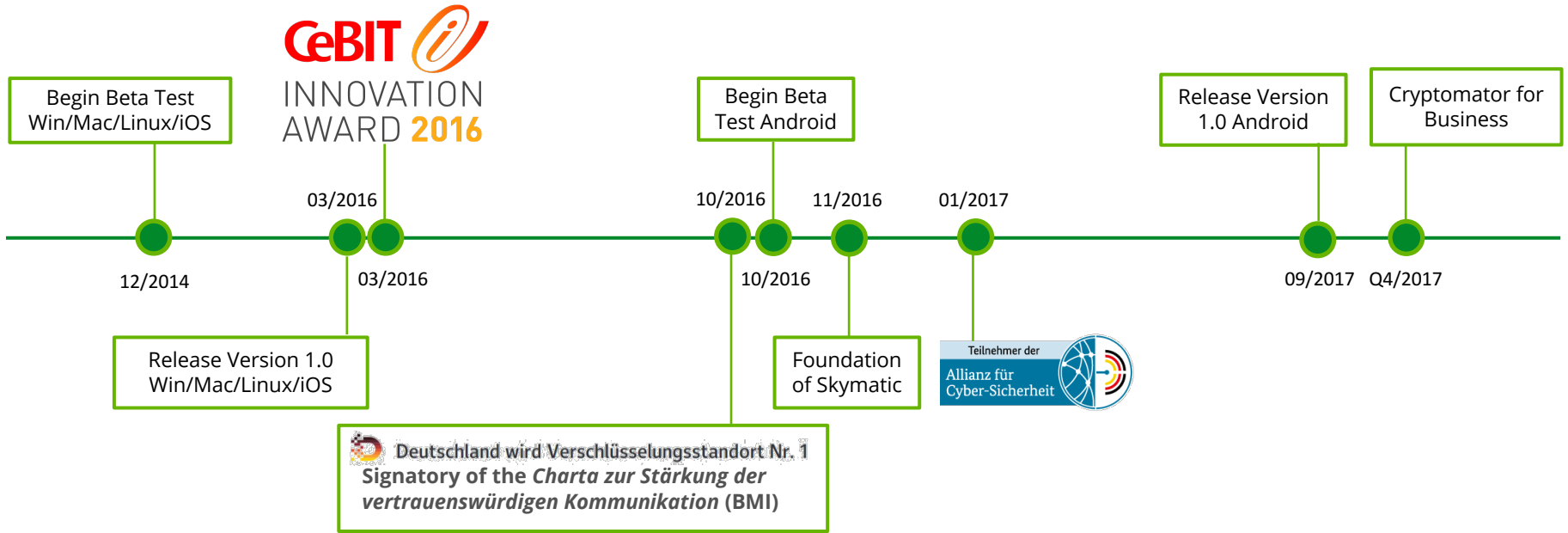
**YOUR
BRAND**



Cryptographic Libraries



Milestones



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/C7W3TUOWYVQ

- 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