cryptorage

Sicherer Austausch vertraulicher Dokumente

BvD Verbandstage 2012

Felix Kronlage <kronlage@bytemine.net>

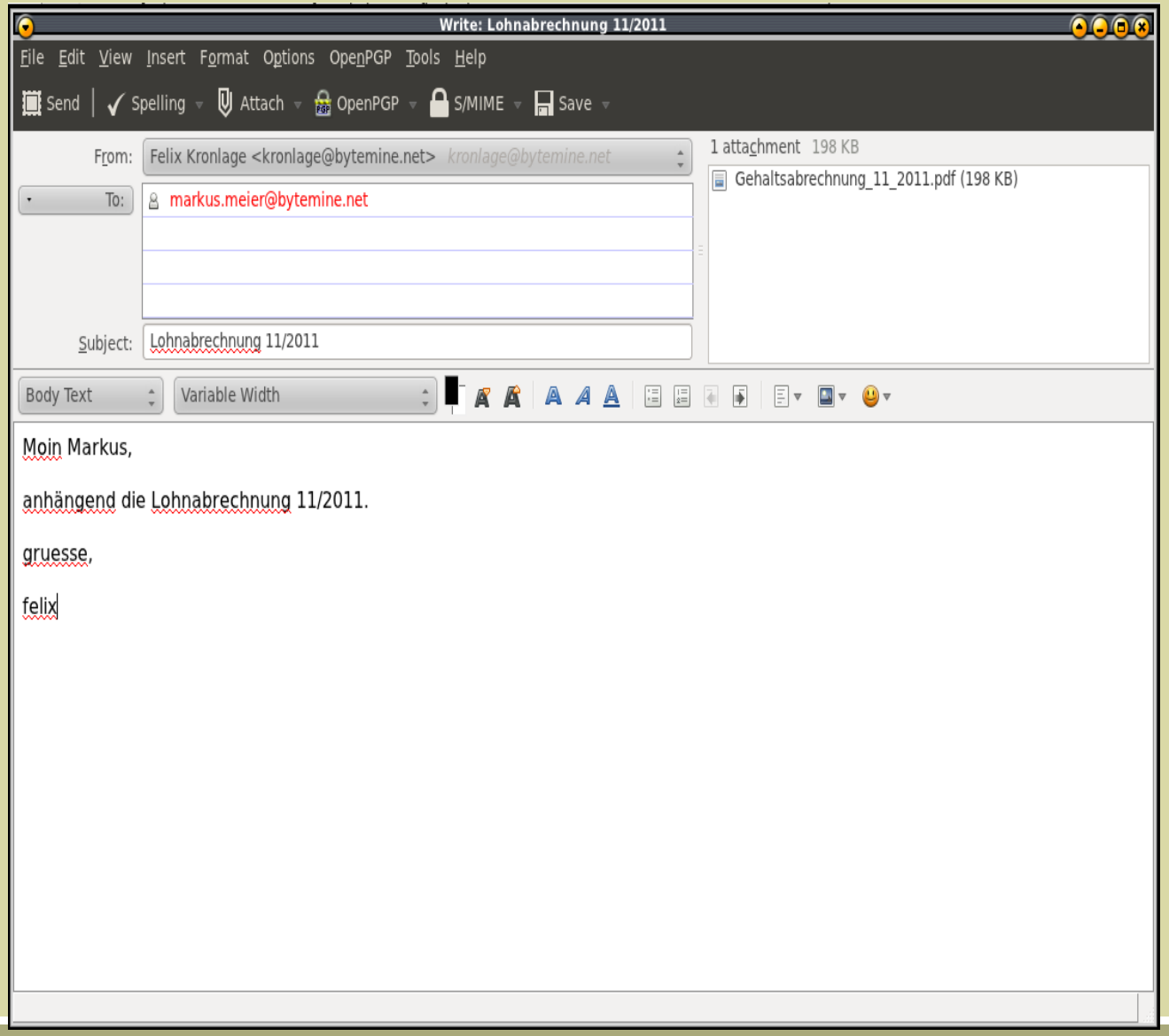
bytemine GmbH

- Unix/Linux Systemhaus / Dienstleister
- Beratung, Konzeption und Wartung
- Produktentwicklung
  - bytemine openbsd appliance
  - cryptorage
- Hosting und Housing
- Sichere und zuverlässige Infrastrukturen

Problem:

Sicherer **und** einfacher Austausch
von Dokumenten

E-Mail?


Write: Lohnabrechnung 11/2011
File Edit View Insert Format Options OpenPGP Tools Help
Send Spelling Attach OpenPGP S/MIME Save
From: Felix Kronlage <kronlage@bytemine.net> kronlage@bytemine.net
To: markus.meier@bytemine.net
Subject: Lohnabrechnung 11/2011
1 attachment 198 KB
Gehaltsabrechnung_11_2011.pdf (198 KB)
Body Text
Variable Width
Moin Markus,
anhängend die Lohnabrechnung 11/2011.
gruesse,
felix

E-Mail?

from Mail Delivery System <Mailer-Daemon@bytemine.net>
subject **Mail delivery failed: returning message to sender**
reply-to bytemine Postmaster <postmaster@bytemine.net>
to Kronlage, Felix

```
This message was created automatically by mail delivery s

A message that you sent could not be delivered to one or
recipients. This is a permanent error. The following addr

  markus.meier@bytemine.net
    SMTP error from remote mail server after RCPT TO:<mar
    host uzarafa.fra.bytemine.net [91.212.95.65]:
    550 Unknown user
```

```
This is a multi-part message in MIME format.
--------------000609090204080007080500
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 8bit

Moin Markus,

anhängend die Lohnabrechnung 11/2011.

gruesse,

felix

--------------000609090204080007080500
Content-Type: application/pdf;
 name="Gehaltsabrechnung_11_2011.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="Gehaltsabrechnung_11_2011.pdf"

JVBERi0xLjMNJeLjz9MNCjE2OCAwIG9iag08PCANL0xpbmVhcml6ZWQgMSANL08gMTcwIA0v
SCBbIDEyODEgNDI0IF0gDS9MIDIwMjMzNyANL0UgNjMwMDMgDS9OIDkgDS9UIDE5ODg1OCAN
Pj4gDWVuZG9iag0gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgICAgICAgICB4cmVmDTE2OCA0MSANMDAwMDAwMDAxNiAwMDAwMCBuDQowMDAwMDAxMTcx
IDAwMDAwIG4NCjAwMDAwMDE3MDUgMDAwMDAgbg0KMDAwMDAwMTkyMyAwMDAwMCBuDQowMDAw
MDAyMjI1IDAwMDAwIG4NCjAwMDAwMDIyNjYgMDAwMDAgbg0KMDAwMDAwMzAlMSAwMDAwMCBu
DQowMDAwMDAzMjY3IDAwMDAwIG4NCjAwMDAwMDQwMjUgMDAwMDAgbg0KMDAwMDAwNDI0OSAw
```

Lösungsansätze

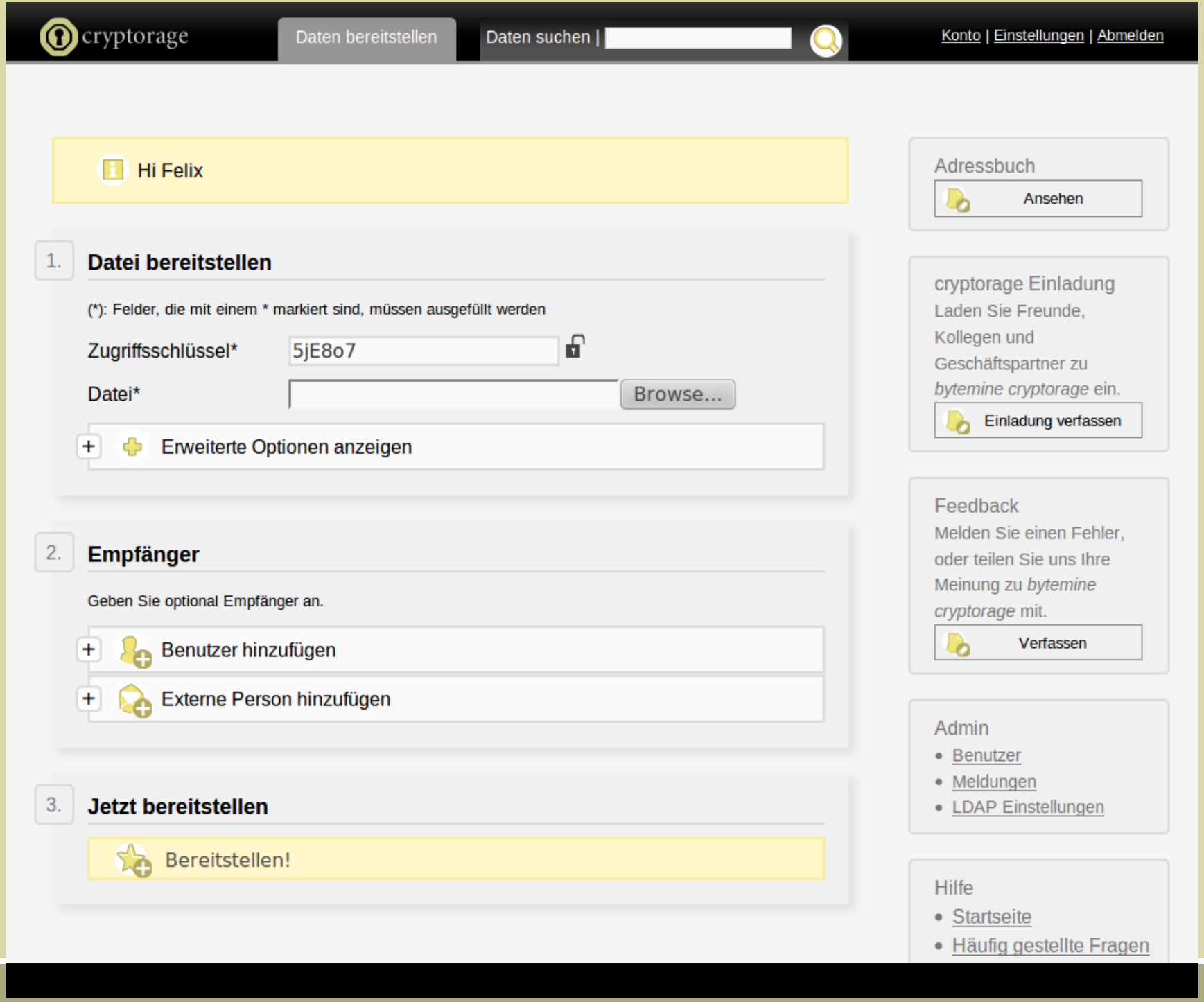
- PGP - Pretty Good Privacy
  - GNU Privacy Guard
  - PGP/GPG Mailgateways
- S/MIME
- TrueCrypt Container
- Steed

Die Idee

Anforderungen

- Nur ein Internet Browser wird benötigt
- Schlüsselaustausch möglichst einfach
- Einfache Benutzung
  - So einfach wie Webmail!
- Darf den Arbeitsfluß nicht behindern


Sender
1. Anmelden
3. Empfänger wählen
2. Daten bereitstellen
bytemine
cryptorage
1. Schlüssel
1. Download-Link
2. Daten abrufen
Empfänger


cryptorage
Daten bereitstellen
Daten suchen |
Konto | Einstellungen | Abmelden
Hi Felix
1. Datei bereitstellen
(*): Felder, die mit einem * markiert sind, müssen ausgefüllt werden
Zugriffsschlüssel* 5jE8o7
Datei* Browse...
Erweiterte Optionen anzeigen
2. Empfänger
Geben Sie optional Empfänger an.
Benutzer hinzufügen
Externe Person hinzufügen
3. Jetzt bereitstellen
Bereitstellen!
Adressbuch
Ansehen
cryptorage Einladung
Laden Sie Freunde, Kollegen und Geschäftspartner zu bytemine cryptorage ein.
Einladung verfassen
Feedback
Melden Sie einen Fehler, oder teilen Sie uns Ihre Meinung zu bytemine cryptorage mit.
Verfassen
Admin
Benutzer
Meldungen
LDAP Einstellungen
Hilfe
Startseite
Häufig gestellte Fragen

Fakten

- Alle gängigen Internet Browser unterstützt
- Mehr als Transfer-Sicherheit
  - Mehr als nur ein verschlüsseltes Dateisystem
- Symmetrische Verschlüsselung
  - **KEIN** eigenes Cryptosystem entworfen
  - BouncyCastle Cryptobibliothek
  - AES-Kandidat *Twofish*

Bereitstellung

- Upload erfolg via Secure Socket Layer
- Direkte Verschlüsselung beim Upload
- Speicherung der Datei erfolgt verschlüsselt
- Datei wird Ablaufdatum versehen

Abrufen

- Eingabe des Schlüssels über SSL-Verbindung
- Direkte Entschlüsselung beim Abrufen
- Versender wird ggf. benachrichtigt
- Datei läuft auf dem Server ab

Vertrauen in den Anbieter?

- Verschlüsselung in den Client verlagern
  - Cryptosystem muss als OSS vorliegen
- Offenes REST-API für Drittanbieter
  - Offenes Produkt
  - http://doc.cryptorage.com/
- JavaScript Client

Vertrauen in den Anbieter?

- Verschlüsselung in den Client verlagern
  - Cryptosystem muss als OSS vorliegen
- Offenes REST-API für Drittanbieter
  - Offenes Produkt
  - http://doc.cryptorage.com/
- JavaScript Client

Vertrauen in den Anbieter?

- *Nullcipher* Option in der API
- Client kann die Verschlüsselung bestimmen
- Interoperabilität zu anderen Produkten
  - OpenPGP Standard
- Lösung vs. Plattform

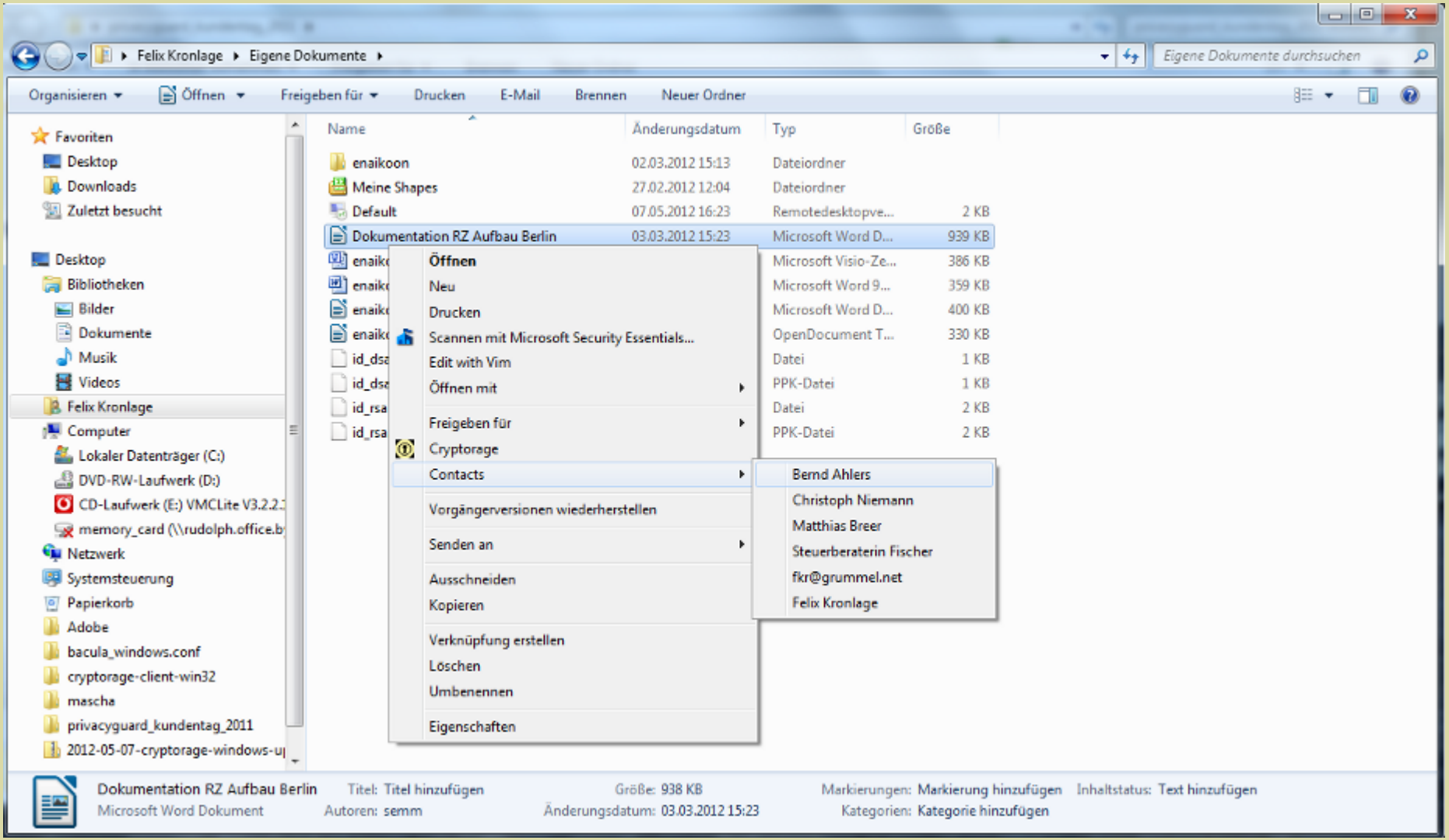
Microsoft Windows Client

- Kooperation mit KO GmbH aus Magdeburg

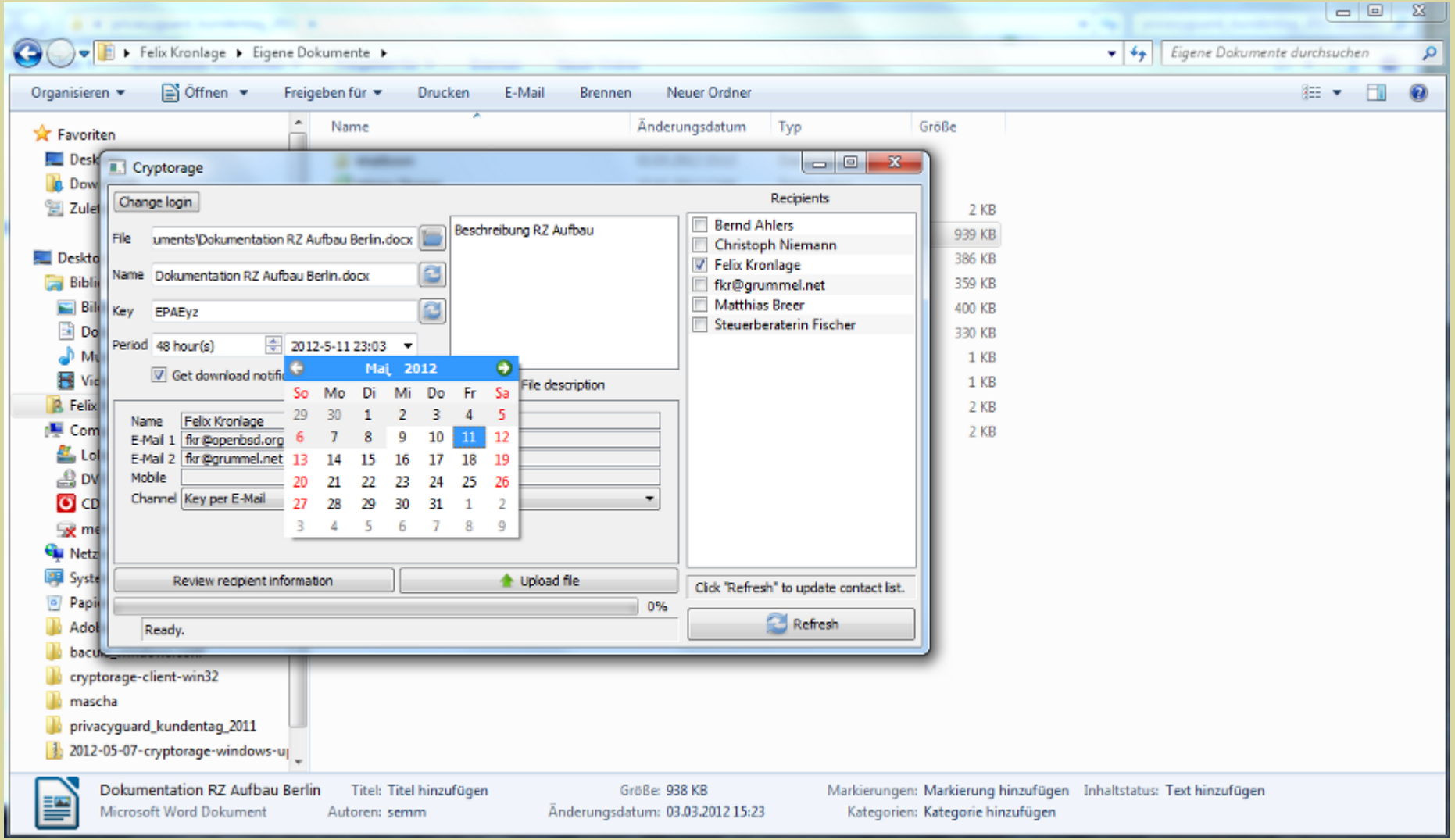
- Native Windows 32/64 Bit Shell Extension
- Nativer UI-Client
- Einbindung in das Explorer Kontextmenü

- Erste Implementierung der cryptorage API

Microsoft Windows Client



Microsoft Windows Client



Weitere Erweiterungen

- Clientseitige Verschlüsselung: 2. Hälfte 2012
- Bibliothek zur Einbindung in Produkte
- iOS / Android App
- SOAP-API

Variationen

- cryptorage hosted Edition
  - portal.cryptorage.com
  - dediziert
- Boxed Produkte
  - Hardware Appliance
  - Software Appliance

Alternativen?

Vielen Dank für die Aufmerksamkeit

bytemine GmbH

Marie-Curie-Str. 1
26129 Oldenburg

info@bytemine.net
http://www.bytemine.net
http://blog.bytemine.net/
+49-441-3091970