JUMBO BLOCK CRYPT

Dateien und Texte verschlüsseln und signieren



Handbuch · Version 1.0.0

Oktober 2026

ZANNI GROUP · Andreas Zanni e.K. · Brauhof 12 · 44866 Bochum · jumboblock.org

Inhalt

1. Überblick
2. Grundbegriffe
3. Arbeitsablauf
4. Schlüsselbund
5. Identitäten
6. Kontakte und Vertrauen
7. Verschlüsseln
8. Entschlüsseln
9. Signieren
10. Signatur prüfen
11. Zusammenspiel mit anderen Programmen
12. Dateien und Formate
13. Sicherheit und Technik
14. Fehlerbehebung

1. Überblick

CRYPT ist das Verschlüsselungswerkzeug im KRITIS-Bereich von JUMBO BLOCK. Es verschlüsselt Dateien und Texte so, dass sie unterwegs niemand lesen oder unbemerkt verändern kann, und weist mit Signaturen nach, von wem ein Inhalt stammt. Gerade im Krisenfall werden Lagebilder, Pläne, Zugangsdaten und Freigaben über ungewohnte Wege ausgetauscht – per USB-Stick, über private Messenger oder ein Ersatz-Postfach. CRYPT macht diese Wege sicher.

Vollständig offline: CRYPT läuft im Browser, auch direkt vom USB-Stick (`file://`). Es gibt keine Server-Verbindung, kein Konto und keine Cloud.

Ohne Fremdcode: Dateiformat, Zertifikatsauswertung und PKCS#12 sind eigener Programmcode. Schlüsselerzeugung, ECDH, ECDSA, RSA, HKDF, PBKDF2 und AES nutzen die eingebaute Web Crypto API des Browsers.

Auch für große Dateien: Dateien werden in Abschnitten von 4 MiB verarbeitet. Mehrere Gigabyte sind möglich; Fortschritt und Abbruch werden angezeigt.

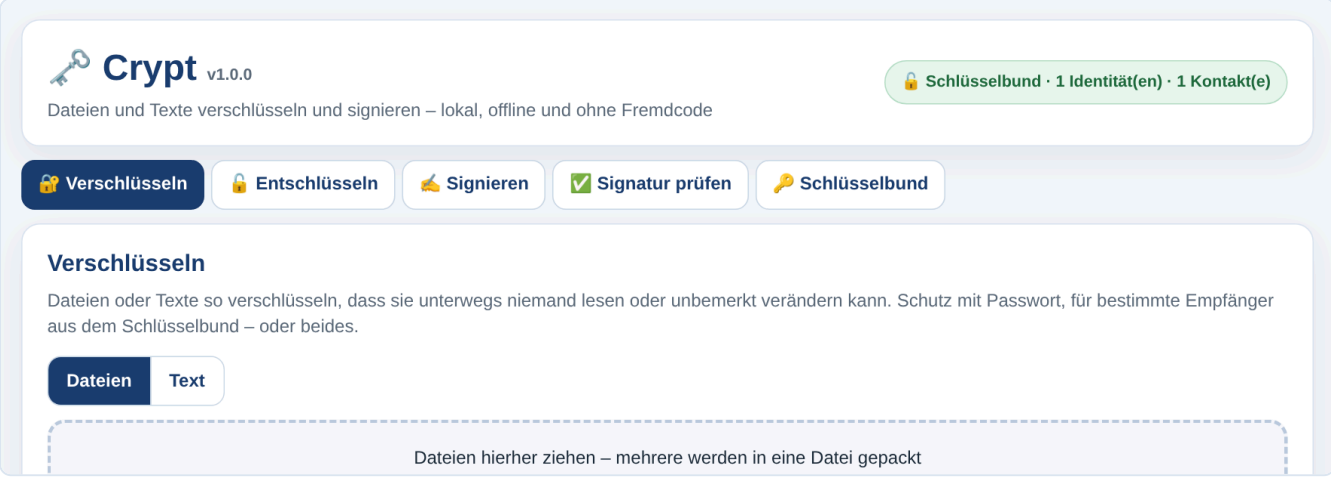


Abb. 1: Die fünf Bereiche von CRYPT

Bereich	Aufgabe
Verschlüsseln	Dateien oder Text mit Passwort, für Empfänger aus dem Schlüsselbund oder beides verschlüsseln, auf Wunsch zusätzlich signieren
Entschlüsseln	Verschlüsselte Dateien (.jbc) oder Textblöcke öffnen; Vollständigkeit und Absender werden geprüft
Signieren	Dateien mit einer Signaturdatei (.jbs) versehen oder Texte zu einem signierten Block machen
Signatur prüfen	Nachweisen, dass eine Datei oder ein Text unverändert ist und von wem er stammt
Schlüsselbund	Eigene Identitäten, Kontakte und vertrauenswürdige Zertifizierungsstellen verwalten

2. Grundbegriffe

Begriff	Bedeutung
Verschlüsselung mit Passwort	Jeder, der das Passwort kennt, kann öffnen. Einfach, aber das Passwort muss auf einem zweiten, sicheren Weg übermittelt werden.
Verschlüsselung für Empfänger	Nur ausgewählte Personen können öffnen – mit dem privaten Schlüssel aus ihrem Schlüsselbund. Ein gemeinsames Passwort ist nicht nötig.
Schlüsselbund	Mit Passwort verschlüsselte Datei (.dbm) mit Ihren Identitäten, Ihren Kontakten und den Zertifizierungsstellen, denen Sie vertrauen.
Identität	Ihr eigenes Schlüsselpaar: zum Signieren und zum Empfang verschlüsselter Inhalte. Entweder in CRYPT erzeugt oder als Zertifikat aus JUMBO BLOCK CERT übernommen.
Öffentlicher Schlüssel (.jbid)	Der weitergebbare Teil einer Identität mit Name, Stelle und Erreichbarkeit. Andere brauchen ihn, um Ihre Signaturen zu prüfen und Ihnen verschlüsselt zu schreiben.
Fingerabdruck	Kurze Zeichenfolge (z. B. `6C4A-5666-3B11-1D42-89E0-5838`), die einen öffentlichen Schlüssel eindeutig kennzeichnet. Wird beim Austausch telefonisch oder persönlich verglichen.
Kontakt	Öffentlicher Schlüssel einer anderen Person in Ihrem Schlüsselbund – „abgeglichen“, sobald Sie den Fingerabdruck mit der Person verglichen haben.
Zertifizierungsstelle (CA)	Z. B. die eigene CA aus JUMBO BLOCK CERT. Signaturen mit Zertifikaten einer vertrauenswürdigen CA gelten als bestätigt, ohne dass jeder Kontakt einzeln abgeglichen werden muss.
Signatur	Kryptografischer Nachweis, dass ein Inhalt von einer bestimmten Identität stammt und seitdem nicht verändert wurde.

3. Arbeitsablauf

Einmalig einrichten

1. Schlüsselbund anlegen und mit einem starken Passwort schützen (Kapitel 4).
2. Eigene Identität erzeugen oder ein Zertifikat aus CERT übernehmen (Kapitel 5).
3. Eigenen öffentlichen Schlüssel (.jbid) an die Personen geben, mit denen Sie Inhalte austauschen; deren .jbid-Dateien als Kontakte laden.
4. Fingerabdrücke telefonisch oder persönlich abgleichen und Kontakte als abgeglichen markieren – oder die eigene Zertifizierungsstelle als vertrauenswürdig hinterlegen (Kapitel 6).
5. Schlüsselbund speichern und eine Sicherungskopie im Notfallordner ablegen.

Im Einsatz

- **Vertrauliches weitergeben:** Für Empfänger verschlüsseln und signieren (Kapitel 7). Der Empfänger öffnet mit seinem Schlüsselbund und sieht, dass der Inhalt von Ihnen stammt.
- **Ohne Schlüsselbund:** Mit Passwort verschlüsseln und das Passwort auf einem anderen Weg mitteilen, z. B. telefonisch.
- **Freigaben und Anweisungen:** Dateien oder Texte signieren (Kapitel 9). Jeder kann die Signatur prüfen – auch ohne eigenen Schlüsselbund.

4. Schlüsselbund

Der Schlüsselbund wird im Reiter *Schlüsselbund* angelegt oder geöffnet. Zum Verschlüsseln mit Passwort und zum Prüfen von Signaturen ist er nicht nötig.

1. Unter *Neuen Schlüsselbund anlegen* ein Passwort mit mindestens 12 Zeichen zweimal eingeben.
2. *Schlüsselbund anlegen* klicken.
3. Identität erzeugen (Kapitel 5) und im Bereich *Schlüsselbund-Datei* speichern.



Abb. 2: Neuen Schlüsselbund anlegen

> Ohne Passwort lassen sich die privaten Schlüssel nicht mehr nutzen – es gibt keine Wiederherstellung. Passwort getrennt vom Schlüsselbund verwahren.

Öffnen, speichern, sperren

Schlüsselbund öffnen liest eine vorhandene Datei; danach wird das Passwort abgefragt. Der Bereich *Schlüsselbund-Datei* zeigt Datei, Verschlüsselung und ungespeicherte Änderungen.

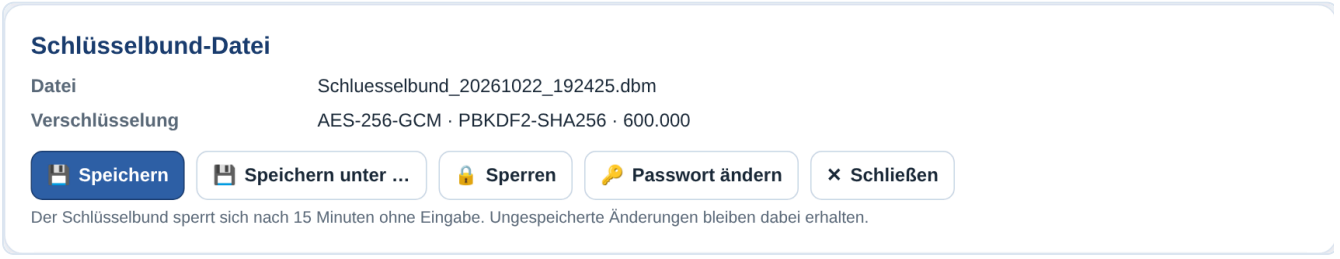


Abb. 3: Schlüsselbund-Datei mit Speichern, Sperren und Passwortänderung

Schaltfläche	Wirkung
Speichern / Speichern unter …	Schreibt den Schlüsselbund verschlüsselt in eine Datei (.dbm). In Chrome und Edge wird beim nächsten Speichern dieselbe Datei überschrieben, in anderen Browsern entsteht ein Download.
Sperren	Entfernt die Schlüssel aus dem Arbeitsspeicher. Zum Weiterarbeiten ist das Passwort nötig; ungespeicherte Änderungen bleiben erhalten.
Passwort ändern	Neues Passwort festlegen, danach speichern
Schließen	Schlüsselbund schließen; bei ungespeicherten Änderungen fragt CRYPT nach

Nach 15 Minuten ohne Eingabe sperrt sich der Schlüsselbund selbstständig.



Abb. 4: Gesperrter Schlüsselbund

5. Identitäten

Eine Identität ist Ihr eigenes Schlüsselpaar. Mit ihr signieren Sie und empfangen für Sie verschlüsselte Inhalte. Ein Schlüsselbund kann mehrere Identitäten enthalten, z. B. für verschiedene Funktionen; eine davon ist der Standard.

Eigenes Schlüsselpaar erzeugen

Eigenes Schlüsselpaar erzeugen fragt Name, Stelle bzw. Funktion und Erreichbarkeit ab. Name und Stelle erscheinen in Ihren Signaturen und im öffentlichen Schlüssel; die Erreichbarkeit hilft anderen beim Abgleich des Fingerabdrucks.

Zertifikat aus CERT übernehmen

Wer mit JUMBO BLOCK CERT eine eigene Zertifizierungsstelle betreibt, kann Personenzertifikate als Identität verwenden. *Zertifikat aus Cert übernehmen* liest die PKCS#12-Datei (.p12/.pfx, mit deren Passwort) oder Schlüssel (.key) und Zertifikat (.crt) gemeinsam. Unterstützt werden RSA und ECDSA (P-256, P-384, P-521). Das Zertifikat muss zum Signieren vorgesehen und gültig sein. Enthält die Datei auch das CA-Zertifikat, bietet CRYPT an, die Zertifizierungsstelle als vertrauenswürdig zu übernehmen.



Abb. 5: Eigene Identität mit Fingerabdruck und Export des öffentlichen Schlüssels

Öffentlichen Schlüssel weitergeben

Die Schaltfläche *.jbid* neben der Identität speichert den öffentlichen Schlüssel. Diese Datei enthält keinen privaten Schlüssel und darf frei weitergegeben werden – per E-Mail, Messenger oder USB-Stick. CRYPT zeigt dabei den Fingerabdruck an, den Sie mit dem Empfänger abgleichen.

> Eine entfernte Identität lässt sich nicht wiederherstellen. Inhalte, die nur für diese Identität verschlüsselt wurden, sind danach nicht mehr lesbar.

6. Kontakte und Vertrauen

Kontakte sind die öffentlichen Schlüssel anderer Personen. *Kontakt laden (.jbid)* übernimmt eine oder mehrere Dateien. CRYPT prüft dabei, ob die Datei unverändert ist und ob es sich um eine eigene Identität handelt.



Abb. 6: Kontakt, noch nicht abgeglichen

Erst wenn Sie den Fingerabdruck mit der Person selbst verglichen haben – telefonisch über eine bekannte Nummer oder persönlich –, markieren Sie den Kontakt mit *Als abgeglichen markieren*. Damit ist ausgeschlossen, dass Ihnen jemand einen fremden Schlüssel unter falschem Namen untergeschoben hat.

Vertrauenswürdige Zertifizierungsstellen

Bei vielen Beteiligten ist der einzelne Abgleich aufwendig. Betreibt Ihre Organisation eine eigene Zertifizierungsstelle mit JUMBO BLOCK CERT, laden Sie deren CA-Zertifikat mit *CA-Zertifikat laden (.crt, .cer)*. Signaturen mit Zertifikaten dieser Stelle gelten danach als bestätigt.

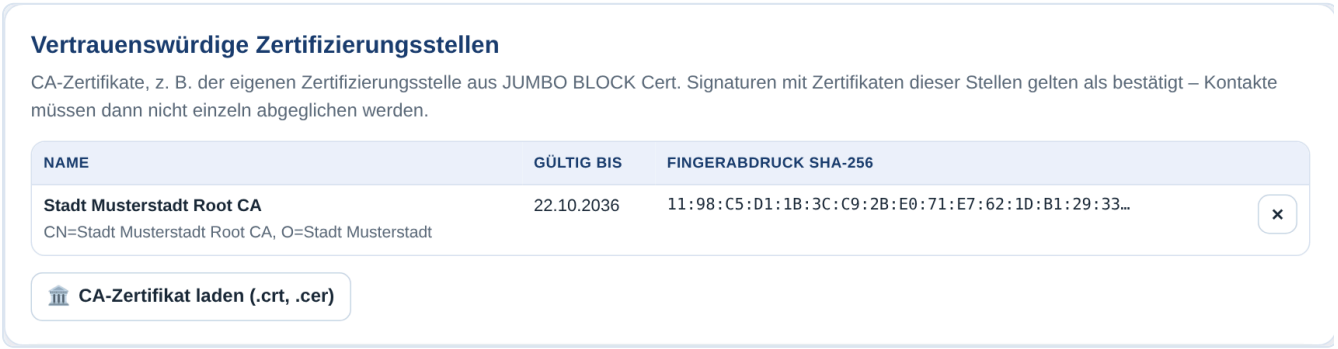


Abb. 7: Eigene Zertifizierungsstelle als vertrauenswürdig hinterlegt

> Nur die eigene oder eine sicher bekannte Zertifizierungsstelle übernehmen. Alle von ihr ausgestellten Zertifikate gelten danach als bestätigt.

Vertrauensstufen

Stufe	Bedeutung
Ihre eigene Identität	Der Inhalt wurde mit einer Ihrer Identitäten signiert.
Kontakt, Fingerabdruck abgeglichen	Bekannter, persönlich bestätigter Absender
Zertifikat einer vertrauenswürdigen CA	Das Zertifikat stammt nachweislich von einer hinterlegten Zertifizierungsstelle und war zum Signaturzeitpunkt gültig.
Kontakt, noch nicht abgeglichen	Schlüssel bekannt, Herkunft aber nicht bestätigt
unbekannt	Schlüssel nicht im Schlüsselbund – Fingerabdruck mit der Person abgleichen; der Absender lässt sich direkt als Kontakt übernehmen.

7. Verschlüsseln

Im Bereich *Verschlüsseln* wählen Sie zunächst, ob *Dateien* oder ein *Text* verschlüsselt werden sollen.

1. **Inhalt:** Dateien in das Feld ziehen oder über *Dateien wählen* hinzufügen. Mehrere Dateien werden in eine verschlüsselte Datei gepackt; Namen und Änderungsdaten bleiben erhalten. Bei *Text* den Text eingeben.
2. **Schutz:** *Mit Passwort* (mindestens 12 Zeichen) und/oder *Für Empfänger*. Empfänger werden aus Identitäten und Kontakten des Schlüsselbunds ausgewählt; einzelne öffentliche Schlüssel lassen sich auch ohne Schlüsselbund über *Schlüssel eines Empfängers laden (.jbid)* hinzufügen.
3. **Absender:** Mit *Zusätzlich mit meiner Identität signieren* sieht der Empfänger beim Öffnen, dass der Inhalt von Ihnen stammt.
4. *Verschlüsseln* klicken.

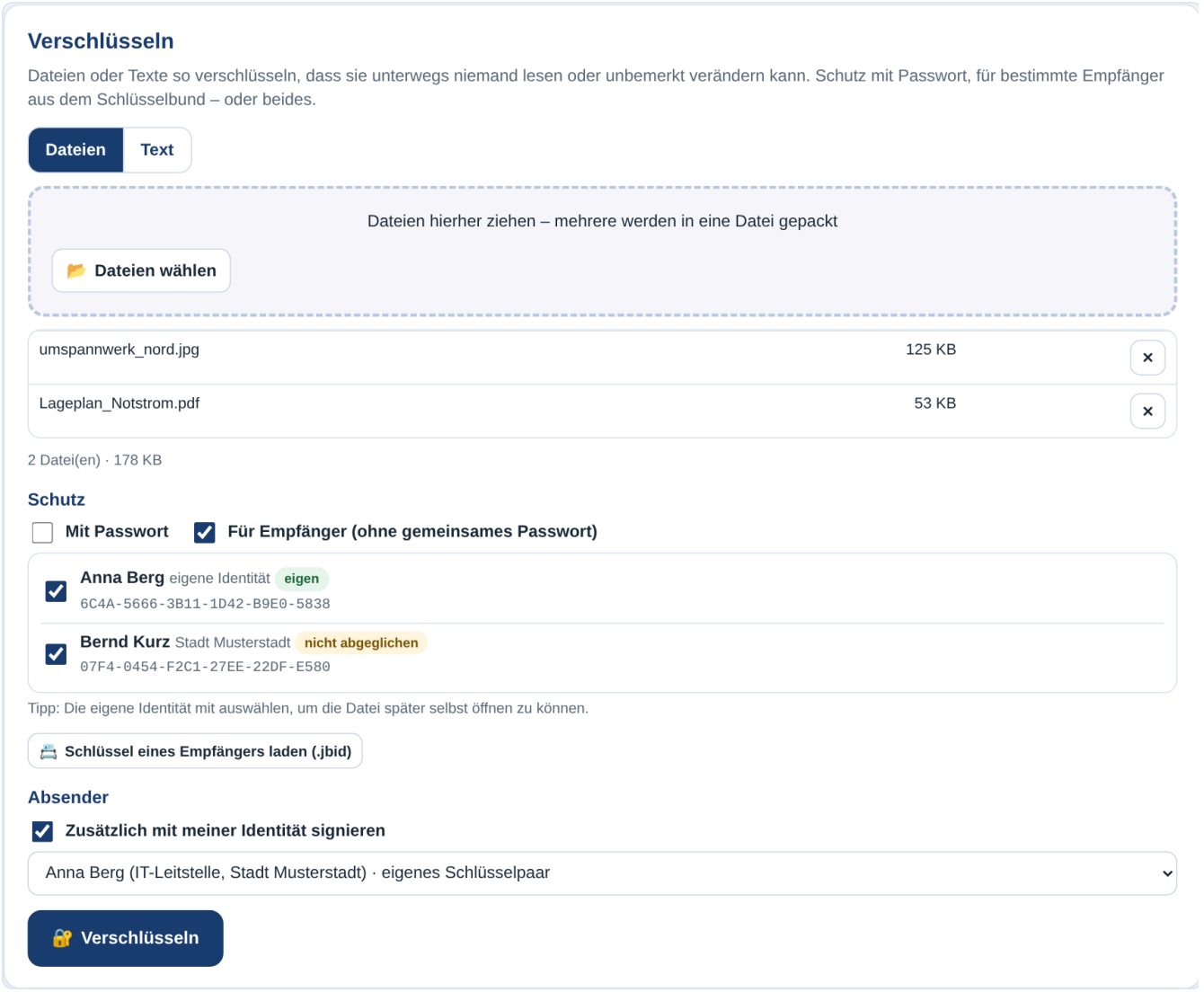


Abb. 8: Zwei Dateien für zwei Empfänger verschlüsseln und signieren

Tipp: Die eigene Identität mit auswählen, um die Datei später selbst wieder öffnen zu können. CRYPT wählt sie standardmäßig vor.

Dateien werden als `.jbc` gespeichert. Bei Texten erscheint ein Textblock, der vollständig einschließlich Kopf- und Fußzeile in E-Mail oder Messenger eingefügt wird.



Abb. 9: Ergebnis: verschlüsselte Datei für zwei Empfänger, signiert



Abb. 10: Verschlüsselter Textblock mit Passwort

> Das Passwort niemals auf demselben Weg wie die verschlüsselte Datei übermitteln – besser telefonisch oder persönlich.

8. Entschlüsseln

1. Im Bereich *Entschlüsseln* die Datei (.jbc) wählen oder in das Feld ziehen – oder einen verschlüsselten Textblock einfügen und *Lesen* klicken. Umgebender Text wie eine Anrede in der E-Mail stört nicht.
2. CRYPT zeigt, womit der Inhalt geschützt ist: Passwort und/oder Empfänger. Bei Empfänger-Verschlüsselung erkennt CRYPT mit geöffnetem Schlüsselbund, ob eine Ihrer Identitäten dazugehört.
3. Gegebenenfalls das Passwort eingeben und *Entschlüsseln* klicken.

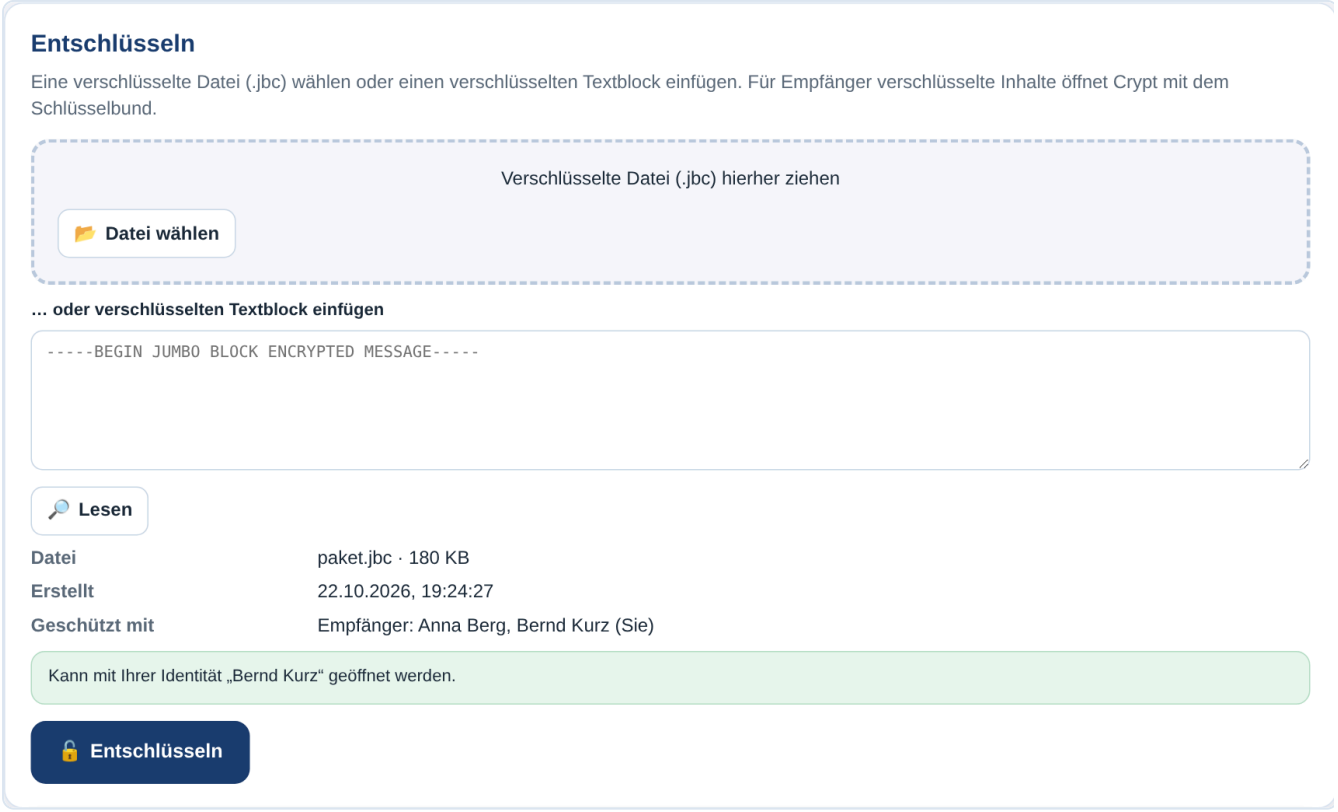


Abb. 11: Datei für Empfänger – kann mit der eigenen Identität geöffnet werden

Beim Entschlüsseln prüft CRYPT jeden Abschnitt und am Ende die Prüfsumme des gesamten Inhalts. Nur wenn alles stimmt, erscheint *Entschlüsselt und unverändert*. Eine enthaltene Signatur wird mit Vertrauensstufe angezeigt.



Abb. 12: Entschlüsselt und unverändert, signiert von einem abgeglichenen Kontakt

Die enthaltenen Dateien lassen sich einzeln oder mit *Alle speichern* sichern. Texte erscheinen in einem Feld zum Kopieren.

Meldet CRYPT einen Fehler beim Entschlüsseln, wurde die Datei beschädigt, gekürzt oder verändert. Teilergebnisse werden nicht ausgegeben.

9. Signieren

Eine Signatur weist nach, dass eine Datei oder ein Text von Ihnen stammt und seitdem unverändert ist. Zum Signieren muss der Schlüsselbund geöffnet sein.

Dateien signieren

1. Unter *Signieren als* die Identität wählen.
2. Dateien hinzufügen. Optional einen *Vermerk* eintragen, z. B. „freigegeben für den Wiederanlauf“ – der Vermerk ist Teil der Signatur.
3. *Signieren* klicken. Für jede Datei entsteht eine Signaturdatei `datei.endung.jbs`.

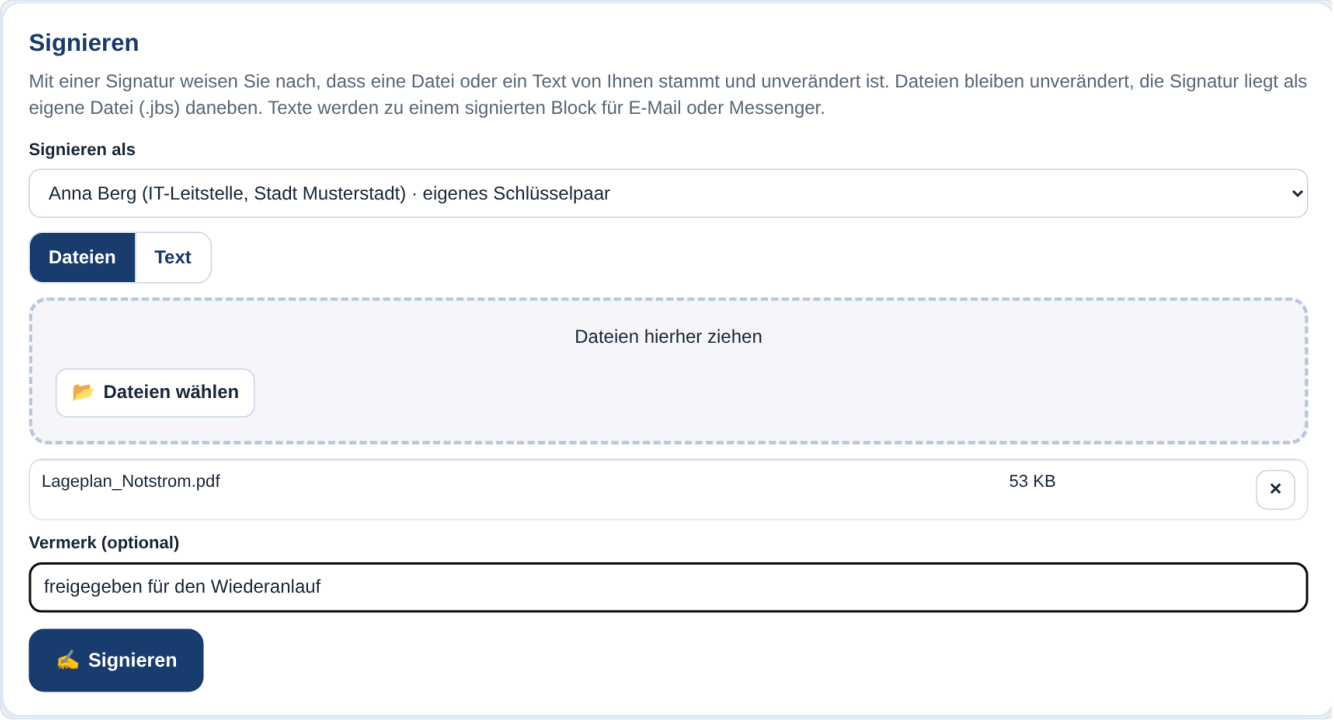


Abb. 13: Datei mit Vermerk signieren

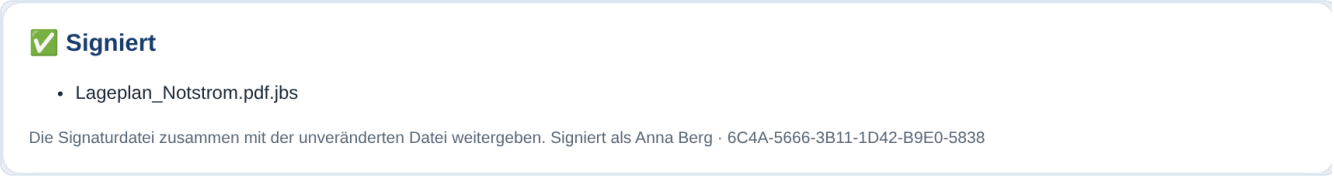


Abb. 14: Ergebnis: Signaturdatei

Die Datei selbst bleibt unverändert. Geben Sie Datei und Signaturdatei gemeinsam weiter.

Text signieren

Bei *Text* entsteht ein signierter Textblock aus dem lesbaren Text und einem Signaturteil. Der Block wird vollständig weitergegeben. Zeilenenden und Leerzeichen am Zeilenende werden vereinheitlicht, damit die Signatur auch nach dem Weg durch E-Mail-Programme gültig bleibt; jede inhaltliche Änderung macht sie ungültig.

Signierter Text

```
-----BEGIN JUMBO BLOCK SIGNED MESSAGE-----
Freigabe: Pumpwerk Süd darf wieder ans Netz.
Anna Berg, IT-Leitstelle
-----BEGIN JUMBO BLOCK SIGNATURE-----
eyJvYmoiOnsidHlwIjoidGV4dCIsInRleHRfc2hhMjU2IjoiMzgwYTQxN2U0MWQw
ZTJkMDAwMjlhMmUzMmE3NmUyNGE2NzQyZWVkMDI4NDU4ZWM4ZjgzMmI5ZDlkYWNi
YjI0MSIsInplaXQiOiIyMDI2LTEwLTIyVDE3OjI0OjMyLjA1OVoiLCJzaWduaWVy
ZXIiOiI2QzRBLTU2NjYtM0IxMS0xRDQyLUI5RTAtNTgzOCJ9LCJhbGciOiIxLjIu
ODQwLjEwMDQ1LjQuMy4yIiwid2VydCI6Ik1FUUNJRnZKek1GV040K3h2MnJTVlZP
SExLclJhVmtQQ3FXU3Nhemx1cDd6L0VBeUFpQVptSHlYYzFsQUxTNStUYW1CNVV0
RlhRQURNSDhNckJDc2pERyt2ZGVxcFE9PSIsImthcnRlIjp7ImthcnRlIjp7InYi
OjEsImlkIjoiODE0OWM4ZmMwZGMwYmQ4MDY3MDVkOGFmYjcyMWYzM2MiLCJhcnQi
```

Kopieren

Den Block vollständig weitergeben. Empfänger prüfen ihn in Crypt unter „Signatur prüfen“. Jede Änderung am Text macht die Signatur ungültig.

Abb. 15: Signierter Textblock

10. Signatur prüfen

Signaturen lassen sich von jedem prüfen – auch ohne eigenen Schlüsselbund. Mit geöffnetem Schlüsselbund erkennt CRYPT zusätzlich Kontakte und Zertifikate der eigenen Zertifizierungsstelle.

1. Im Bereich *Signatur prüfen* die Datei und ihre Signaturdatei (.jbs) gemeinsam wählen oder in das Feld ziehen – oder bei *Text* den signierten Block einfügen.
2. *Prüfen* klicken.



Abb. 16: Echt und unverändert – Absender ist ein abgeglichener Kontakt



Abb. 17: Datei verändert – nicht verwenden

Ergebnis	Bedeutung
Echt und unverändert	Inhalt unverändert, Absender bestätigt (eigene Identität, abgeglichener Kontakt oder vertrauenswürdige CA)
Unverändert – Absender noch nicht bestätigt	Inhalt unverändert, der Schlüssel ist aber nicht bestätigt. Fingerabdruck mit der Person abgleichen.
Datei verändert / Text verändert	Der Inhalt weicht vom signierten Inhalt ab – nicht verwenden.
Signatur ungültig	Die Signatur gehört nicht zu diesem Inhalt oder wurde verändert.
Zertifikat gefälscht	Das Zertifikat gibt vor, von einer vertrauenswürdigen CA zu stammen, ist aber nicht von ihr signiert. Inhalt nicht verwenden.

Zusätzlich zeigt CRYPT Signaturzeit, Vermerk, Name und Prüfsumme der signierten Datei. Bei Zertifikaten wird geprüft, ob das Zertifikat zum Signaturzeitpunkt gültig und zum Signieren vorgesehen war. Ein inzwischen abgelaufenes Zertifikat wird nur als Hinweis angezeigt, wenn es zum Signaturzeitpunkt gültig war.

11. Zusammenspiel mit anderen Programmen

Programm	Verwendung von CRYPT
JUMBO BLOCK CERT	Personenzertifikate der eigenen CA als Identität; CA-Zertifikat als vertrauenswürdige Zertifizierungsstelle
JUMBO BLOCK REPORT	Signiert den Stand einer Vorfallakte mit einer Identität aus dem Schlüsselbund. Die dabei entstehende Signaturdatei (.jbs) wird in CRYPT unter *Signatur prüfen* zusammen mit der Prüfdatei geprüft.
JUMBO BLOCK INVENTORY	Verschlüsselt und signiert Lieferungen zwischen Stellen und Zentrale mit dem Schlüsselbund; Stellen und Zentrale tauschen dazu ihre öffentlichen Schlüssel (.jbid) aus.

In allen Fällen öffnen die Programme den Schlüsselbund nur lesend und nur für die Dauer der Sitzung. Die Datei des Schlüsselbunds wird dabei nicht verändert.

12. Dateien und Formate

Datei	Inhalt	Weitergabe
Schlüsselbund (.dbm)	Identitäten mit privaten Schlüsseln, Kontakte, Zertifizierungsstellen – mit Passwort verschlüsselt	Nur eigene Sicherungskopien
Öffentlicher Schlüssel (.jbid)	Name, Stelle, Erreichbarkeit, öffentliche Schlüssel, ggf. Zertifikat	Frei weitergeben, Fingerabdruck abgleichen
Verschlüsselte Datei (.jbc)	Eine oder mehrere Dateien bzw. ein Text, verschlüsselt, optional signiert	Beliebiger Weg
Signaturdatei (.jbs)	Signatur, Signaturzeit, Vermerk, Prüfsumme und Name der Datei, öffentlicher Schlüssel des Absenders	Zusammen mit der Datei
Textblöcke	`-----BEGIN JUMBO BLOCK ENCRYPTED MESSAGE-----` bzw. `SIGNED MESSAGE` mit `SIGNATURE`	E-Mail, Messenger, Textdatei

13. Sicherheit und Technik

Bereich	Umsetzung
Inhaltsverschlüsselung	AES-256-GCM mit zufälligem Inhaltsschlüssel, Abschnitte von 4 MiB mit eigener Authentisierung, abschließende SHA-256-Prüfsumme des Gesamtinhalts
Passwort	PBKDF2-SHA-256 mit 600 000 Durchläufen, mindestens 12 Zeichen
Empfänger	ECDH P-256 mit kurzlebigem Schlüssel je Empfänger und HKDF-SHA-256; Inhaltsschlüssel je Empfänger eingepackt
Signatur	ECDSA P-256 für eigene Schlüsselpaare; RSA oder ECDSA für Zertifikate aus CERT
Fingerabdruck	SHA-256 über den öffentlichen Signaturschlüssel, die ersten 96 Bit in Vierergruppen
Schlüsselbund	AES-256-GCM, PBKDF2-SHA-256 mit 600 000 Durchläufen, automatisches Sperren nach 15 Minuten
Datenschutz	Keine Netzwerkverbindung, keine Telemetrie, keine Speicherung von Schlüsseln im Browser

Grenzen

- Der Schutz hängt am Passwort und am Gerät: Auf einem kompromittierten Rechner können Eingaben mitgelesen werden.
- Eine Signatur weist die Identität nach, nicht die Person dahinter. Deshalb Fingerabdrücke abgleichen oder eine eigene CA verwenden.
- Ein Widerruf von Schlüsseln wird nicht automatisch verteilt. Bei Verlust eines Schlüsselbunds die Kontakte informieren und eine neue Identität erzeugen.
- Bei Aufruf über das Netzwerk stellt der Browser die Web Crypto API nur über HTTPS bereit. Vom USB-Stick (`file://`) und über jumboblock.org funktioniert CRYPT uneingeschränkt.

14. Fehlerbehebung

Problem	Ursache und Lösung
„Keine Ihrer Identitäten gehört zu den Empfängern“	Die Datei wurde für andere Personen verschlüsselt oder mit einer älteren Identität. Absender bitten, mit Ihrem aktuellen öffentlichen Schlüssel neu zu verschlüsseln.
„Das Passwort ist falsch“	Groß-/Kleinschreibung und Tastaturbelegung prüfen. Ohne richtiges Passwort lässt sich der Inhalt nicht öffnen.
„Die verschlüsselten Daten sind unvollständig“	Datei beim Kopieren oder Herunterladen abgeschnitten. Neu übertragen lassen.
„Kein verschlüsselter Textblock gefunden“	Block nicht vollständig eingefügt. Kopf- und Fußzeile mitkopieren.
Signatur „Unverändert – Absender noch nicht bestätigt“	Fingerabdruck mit der Person abgleichen und Kontakt als abgeglichen markieren oder CA hinterlegen.
„Datei verändert“	Falsche Version oder Datei nach dem Signieren bearbeitet. Originaldatei verwenden.
PKCS#12-Datei wird nicht unterstützt	Ältere Verschlüsselungsverfahren in der .p12-Datei. In CERT neu exportieren oder Schlüssel (.key) und Zertifikat (.crt) verwenden.
„Das Zertifikat ist nicht zum Signieren vorgesehen“	Server-Zertifikat statt Personenzertifikat. In CERT ein Zertifikat mit Client-/Signaturverwendung ausstellen.
Prüfsumme des Schlüsselbunds stimmt nicht	Datei außerhalb von CRYPT verändert. Inhalt wird dennoch durch die Verschlüsselung bestätigt; neu speichern.
Web Crypto API nicht verfügbar	Aktuellen Browser verwenden; bei Aufruf über das Netzwerk HTTPS nutzen.