

Nutzung der Schlüssel/Zertifikate der Volksverschlüsselung

Informationen und Anleitungen für Endanwender

Levona Eckstein Jonathan Leppert Tatjana Rubinstein

1. Juni 2022

Inhaltsverzeichnis

1	1 Einleitung 4						
2 Wozu kann ich meine Schlüssel/Zertifikate der Volksverschlüsselung ver- wenden?							
3	Nut	zung de	er Schlüssel/Zertifikate in S/MIME-fähigen E-Mail-Programmen	5			
	3.1	So fun	ktioniert S/MIME	5			
		3.1.1	Signieren einer E-Mail	5			
		3.1.2	Ende-zu-Ende-Verschlüsseln einer E-Mail	6			
	3.2	Was b	enötigt mein Kommunikationspartner, um mit mir vertraulich				
		komm	unizieren zu können?	6			
	3.3	Wie be	ekomme ich das Verschlüsselungszertifikat des Empfängers?	7			
	3.4	Nutzu	ng in Outlook für Microsoft 365	8			
		3.4.1	Voraussetzungen	8			
		3.4.2	Installation der CA-Zertifikate der Volksverschlüsselung	8			
		0.4.0	Austausch des verschlusselungszeitinkats mittels signierter E-	11			
		3.4.4	Manuelle Konfiguration des Verzeichnisdienstes der Volksver- schlüsselung	11			
		345	Manuelle Konfiguration des Verzeichnisdienstes einer fremden	10			
		0.1.0	Zertifizierungsstelle	16			
		3.4.6	Senden einer verschlüsselten E-Mail	17			
		3.4.7	Empfang einer verschlüsselten E-Mail	18			
		3.4.8	Senden einer signierten E-Mail	19			
		3.4.9	Empfang einer signierten E-Mail	20			
		3.4.10	Senden einer signierten und verschlüsselten E-Mail	22			
		3.4.11	Kontrolle der installierten Zertifikate im Trustcenter	22			

		3.4.12	Nutzung mehrerer E-Mail-Konten	24
		3.4.13	Nutzung eines gesperrten Zertifikats	25
		3.4.14	Zertifikate entfernen	26
	3.5	Nutzu	ng in Thunderbird	29
		3.5.1	Voraussetzungen	29
		3.5.2	Installation der CA-Zertifikate der Volksverschlüsselung	30
		3.5.3	Austausch des Verschlüsselungszertifikats mittels signierter E-	
			Mail	33
		3.5.4	Manuelle Konfiguration des Verzeichnisdienstes der Volksver- schlüsselung	34
		3.5.5	Manuelle Konfiguration des Verzeichnisdienstes einer fremden	
			Zertifizierungsstelle	35
		3.5.6	Senden einer verschlüsselten E-Mail	36
		3.5.7	Empfang einer verschlüsselten E-Mail	37
		3.5.8	Senden einer signierten E-Mail	38
		3.5.9	Empfang einer signierten E-Mail	39
		3.5.10	Senden einer signierten und verschlüsselten E-Mail	39
		3.5.11	Kontrolle der installierten Zertifikate in Einstellungen	40
		3.5.12	Nutzung mehrerer E-Mail-Konten	42
		3.5.13	Nutzung eines gesperrten Zertifikats	43
		3.5.14	Zertifikate entfernen	44
4	Nut	zung de	er Schlüssel/Zertifikate in Browsern	48
5	Nut	zung de	er Schlüssel/Zertifikate auf anderen Rechnern	49
	5.1	Export	t der Schlüssel/Zertifikate aus der Volksverschlüsselungs-Software	49
	5.2	Verteil	ung auf andere Windows-Rechner	51
	5.3	Verteil	ung der Schlüssel auf andere Plattformen, die nicht von der	
		Volksv	erschlüsselungs-Software unterstützt werden	51
		5.3.1	Export für MacOS, Linux und Android	51
		5.3.2	Export für iOS	51

Dokumenthistorie:

Version	Datum	Beschreibung	
1.0	30.12.2016	Initiale Version	
1.1	12.05.2022	Anpassung VV G02	

1 Einleitung

Mit einem persönlichen Zertifikat der Volksverschlüsselung können Sie E-Mails und andere Daten digital signieren und/oder verschlüsseln sowie sich gegenüber Webseiten authentifizieren, die eine zertifikatsbasierte Client-Authentifizierung unterstützen.

In diesem Dokument finden Sie Informationen und Anleitungen, die Sie bei der Nutzung Ihres privaten Schlüssels und persönlichen Zertifikats der Volksverschlüsselung unter Windows in den E-Mail-Programmen und Web-Browsern unterstützen sollen. Außerdem wird beschrieben, wie Sie die Schlüssel/Zertifikate der Volksverschlüsselung auf andere Rechner verteilen können.

Für die Ausführungen in diesem Dokument setzen wir voraus, dass Ihnen ein Windows-System (Vista, Windows 7 oder neuer) zur Nutzung der Volksverschlüsselungs-Software zur Verfügung steht und Sie bereits ein Zertifikat der Volksverschlüsselung für Ihre E-Mail-Adresse besitzen.

Hinweis:

Das Dokument wird kontinuierlich fortgeschrieben. Wenn Sie Anmerkungen oder Verbesserungsvorschläge zum Dokument haben, schicken Sie uns bitte eine E-Mail an **info@volksverschluesselung.de**. Wir sind für jede Anregung dankbar.

2 Wozu kann ich meine Schlüssel/Zertifikate der Volksverschlüsselung verwenden?

Wenn Sie mittels der Volksverschlüsselungs-Software ein Zertifikat beantragen, erhalten Sie technisch gesehen für Ihre E-Mail-Adresse jeweils drei zusammenhängende X.509-Zertifikate für unterschiedliche Anwendungszwecke.

- 1. Mit dem Verschlüsselungszertifikat können Sie mit einem S/MIME-fähigen E-Mail-Programm Ihre E-Mail-Kommunikation oder andere Daten, wie beispielsweise PDF-Dokumente, verschlüsseln.
- 2. Mit dem **Signaturzertifikat** können Sie mit einem S/MIME-fähigen E-Mail-Programm Ihre E-Mails oder andere Daten, wie beispielsweise PDF-Dokumente, digital signieren.
- 3. Das Authentifizierungszertifikat kann in Browsern zur Anmeldung bei Diensten oder Web-Angeboten verwendet werden, sofern der Server nach einem persönlichen Zertifikat zur TLS-Client-Authentifizierung verlangt, zum Beispiel als Ergänzung oder als Ersatz zum herkömmlichen Login mit Benutzername und Passwort.

Im Kapitel Nutzung der Schlüssel/Zertifikate in S/MIME-fähigen E-Mail-Programmen wird das Signieren und Verschlüsseln einer E-Mail in S/MIME-fähigen E-Mail-Programmen beschrieben, die von der Volksverschlüsselungs-Software unterstützt werden. Hier finden Sie auch Informationen, wie Sie die installierten Schlüssel/Zertifikate in Ihrem E-Mail-Programm überprüfen können. Das Kapitel Nutzung der Schlüssel/Zertifikate in Browsern enthält Informationen zur Verwendung der Schlüssel/Zertifikate in Chrome, Internet Explorer und Mozilla Firefox.

3 Nutzung der Schlüssel/Zertifikate in S/MIME-fähigen E-Mail-Programmen

Von der Volksverschlüsselungs-Software werden unter Windows verschiedene S/MIME-fähige E-Mail-Programme automatisch zur Nutzung der Schlüssel/Zertifikate konfiguriert. In diesem Kapitel wird das S/MIME-Verfahren zum Signieren und/oder Verschlüsseln von E-Mails und die Nutzung der Schlüssel/Zertifikate in den E-Mail-Programmen *Microsoft Office Outlook* und *Mozilla Thunderbird* beschrieben sowie Hilfestellungen im Umgang mit den Zertifikaten gegeben.

Da es von Outlook verschiedene Versionen gibt, konzentrieren sich die Ausführungen auf *Microsoft Office Outlook für Microsoft 365*. Anleitungen zu weiteren S/MIMEfähigen E-Mail-Programmen und anderen Outlook-Versionen finden Sie u.a. auf den Seiten der Universität Osnabrück Dort finden Sie auch Informationen zum Signieren und Verschlüsseln von E-Mails in Windows Live Mail.

3.1 So funktioniert S/MIME

Die Volksverschlüsselung stellt X.509 Zertifikate aus, die Sie für die sichere E-Mail-Kommunikation mittels S/MIME nutzen können. Das standardisierte Verfahren S/MIME erlaubt es, E-Mails auf zwei verschiedene Arten kryptographisch zu sichern. Mit S/MIME können E-Mails signiert und/oder Ende-zu-Ende verschlüsselt werden.

3.1.1 Signieren einer E-Mail

Durch das digitale Signieren einer E-Mail kann Ihr Kommunikationspartner überprüfen, ob der Inhalt der E-Mail auch tatsächlich von Ihnen stammt und bei der Übertragung nicht geändert wurde.

Wenn Sie eine E-Mail signieren, dann verwendet Ihr E-Mail-Programm hierfür den privaten Schlüssel zu Ihrem Signaturzertifikat, welcher beispielsweise von der Volksverschlüsselungs-Software in Ihrem E-Mail-Programm installiert wurde. Zunächst wird mittels einer Hashfunktion eine Prüfsumme über den Nachrichteninhalt erstellt. Diese wird dann mit dem privaten Schlüssel verschlüsselt. Die verschlüsselte Prüfsumme bildet dann die Signatur und wird an die E-Mail angehängt. Üblicherweise wird auch das Signaturzertifikat (genauer gesagt die gesamte Zertifizierungskette) an die signierte E-Mail angehängt. Das E-Mail-Programm des Empfängers überprüft mit Hilfe des Signaturzertifikats des Senders die Gültigkeit der Signatur. Konkret bedeutet dies, dass die Signatur mit dem öffentlichen Schlüssel aus dem Signaturzertifikat entschlüsselt wird. Die enthaltene Prüfsumme wird dann mit der Prüfsumme verglichen, die vom Programm des Empfängers gebildet wurde. Die Signatur ist *gültig*, wenn die Prüfsummen übereinstimmen.

Der Empfänger muss zur Gültigkeitsprüfung auch alle zum Signaturzertifikat zugehörigen Zertifikate der übergeordneten Zertifizierungsstellen (CA-Zertifikate) in seinem E-Mail-Programm installiert haben. Anderenfalls wird das Signaturzertifikat als nicht vertrauenswürdig eingestuft und die Signatur als *ungültig* angezeigt. Ist der Empfänger Nutzer der Volksverschlüsselung und hat er sein E-Mail-Programm mit der Volksverschlüsselungs-Software konfiguriert, dann sind alle CA-Zertifikate der Volksverschlüsselung¹ bereits in seinem E-Mail-Programm installiert. Anderenfalls muss er die CA-Zertifikate manuell installieren, wie im Abschnitt *Installation der CA-Zertifikate der Volksverschlüsselung* unter Nutzung in Outlook für Microsoft 365 und Nutzung in Thunderbird beschrieben.

3.1.2 Ende-zu-Ende-Verschlüsseln einer E-Mail

Ende-zu-Ende-Verschlüsselung bedeutet, dass nur Sie und der Empfänger die verschlüsselte E-Mail lesen können und sichert Ihre E-Mail-Kommunikation damit gegen Kenntnisnahme durch unbefugte Dritte. Ende-zu-Ende-Verschlüsselung mittels S/MIME funktioniert nur, wenn sowohl Sender als auch Empfänger ein X.509-Zertifikat für S/MIME besitzen.

Wenn Sie eine E-Mail an einen Empfänger verschlüsselt senden möchten, benötigen Sie das **Verschlüsselungszertifikat des Empfängers**, denn die E-Mail wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und auch nur dieser kann die E-Mail wieder entschlüsseln, da nur er den dazugehörigen privaten Schlüssel besitzt.

Wenn Sie eine E-Mail an mehrere Empfänger verschlüsselt senden möchten, ist es notwendig, dass Sie die Verschlüsselungszertifikate **aller** Empfänger kennen und in Ihrem E-Mail-Programm verfügbar sind.

Wie Sie das Zertifikat Ihres Empfängers erhalten, ist in Abschnitt Wie bekomme ich das Verschlüsselungszertifikat des Empfängers? beschrieben.

3.2 Was benötigt mein Kommunikationspartner, um mit mir vertraulich kommunizieren zu können?

Ihr Kommunikationspartner muss ebenfalls ein X.509-Zertifikat und ein S/MIME-fähiges E-Mail-Programm besitzen, wenn sie miteinander vertraulich kommunizieren möchten.

¹https://volksverschluesselung.de/zertifikate.php

Besitzt ihr Kommunikationspartner ein Zertifikat der Volksverschlüsselung und hat er dieses im Verzeichnis der Volksverschlüsselung veröffentlicht, können Sie mit ihm i.d.R. sofort verschlüsselte E-Mails austauschen, wenn Sie Ihr E-Mail-Programm mit Hilfe der Volksverschlüsselungs-Software konfiguriert haben. Haben Sie oder ihr Kommunikationspartner das Zertifikat nicht veröffentlicht oder besitzt ihr Kommunikationspartner ein Zertifikat von einer anderen Zertifizierungsstelle, müssen zunächst die Zertifikate ausgetauscht werden. Verschiedene Möglichkeiten des Zertifikatsaustauschs sind im Abschnitt Wie bekomme ich das Verschlüsselungszertifikat des Empfängers? beschrieben.

3.3 Wie bekomme ich das Verschlüsselungszertifikat des Empfängers?

Wenn Sie E-Mails verschlüsselt versenden möchten, benötigen Sie, wie in Ende-zu-Ende-Verschlüsseln einer E-Mail beschrieben, das Verschlüsselungszertifikat des jeweiligen Empfängers.

Die Verschlüsselungszertifikate von Kommunikationspartnern, die ein Zertifikat der Volksverschlüsselung verwenden und dieses im Verzeichnisdienst der Volksverschlüsselung veröffentlicht haben, erhalten Sie automatisch, wenn Sie Ihr E-Mail-Programm mit der Volksverschlüsselungs-Software konfiguriert haben. In diesem Fall wird auch der Verzeichnisdienst der Volksverschlüsselung in Ihrem E-Mail-Programm eingerichtet und das E-Mail-Programm holt sich das Zertifikat automatisch aus dem Verzeichnis.

Anderenfalls stehen Ihnen folgende Möglichkeiten zur Verfügung, das Verschlüsselungszertifikat zu erhalten:

1. Zertifikatsaustausch mittels signierter E-Mail

Sie tauschen mit Ihrem Kommunikationspartner eine signierte E-Mail aus, wie im Abschnitt *Austausch des Verschlüsselungszertifikats mittels signierter E-Mail* unter Nutzung in Outlook für Microsoft 365 und Nutzung in Thunderbird beschrieben.

2. Manuelle Konfiguration des Verzeichnisdienstes des Empfängers

Möchten Sie den Verzeichnisdienst der Volksverschlüsselung ohne die Volksverschlüsselungs-Software nutzen oder hat Ihr Kommunikationspartner sein Zertifikat im Verzeichnisdienst einer anderen Zertifizierungsstelle veröffentlicht, können Sie für die automatische Zertifikatssuche in Outlook auch den Verzeichnisdienst manuell einrichten, wie in Manuelle Konfiguration des Verzeichnisdienstes der Volksverschlüsselung und Manuelle Konfiguration des Verzeichnisdienstes einer fremden Zertifizierungsstelle unter Nutzung in Outlook für Microsoft 365 und Nutzung in Thunderbird beschrieben.

3.4 Nutzung in Outlook für Microsoft 365

Diese Kapitel gibt Hilfestellungen bei der Verwendung der Schlüssel/Zertifikate der Volksverschlüsselung in *Microsoft Office Outlook für Microsoft 365*.

3.4.1 Voraussetzungen

Für die nachfolgenden Ausführungen setzen wir voraus, dass

- 1. Sie Outlook für Microsoft 365 auf Ihrem Rechner installiert und für Ihre E-Mail-Adresse ein Konto eingerichtet haben. Falls Sie beispielsweise ein Konto bei T-Online, GMX oder Web.de haben, so können Sie dieses auch in Outlook konfigurieren und verwenden. Anleitungen für das Einrichten eines E-Mail-Kontos in Outlook finden Sie bei Ihrem E-Mail-Anbieter.
- 2. Sie mit Hilfe der Volksverschlüsselungs-Software für die verwendete E-Mail-Adresse ein Zertifikat beantragt, heruntergeladen und Outlook für Microsoft 365 konfiguriert haben.
- 3. Ihr Kommunikationspartner ebenfalls ein S/MIME-fähiges E-Mail-Programm und ein Zertifikat der Volksverschlüsselung oder eines anderen Anbieters von S/MIME-Zertifikaten besitzt (vgl. Was benötigt mein Kommunikationspartner, um mit mir vertraulich kommunizieren zu können?).

3.4.2 Installation der CA-Zertifikate der Volksverschlüsselung

Um die Gültigkeit eines Zertifikats der Volksverschlüsselung prüfen zu können, muss die gesamte Zertifikatskette in Outlook installiert sein, d.h. das Wurzelzertifikat Volksverschlüsselung Root-CA G02 und das Zertifikat der Private CA Volksverschlüsselung Private-CA G02 müssen Outlook bekannt sein. Wenn Sie die Volksverschlüsselungs-Software zur Konfiguration Ihrer Anwendung verwenden, werden diese Zertifikate automatisch installiert.

Falls Sie die Volksverschlüsselungs-Software nicht verwenden wollen/können, dann müssen Sie die Zertifikate manuell importieren. Laden Sie hierzu die Zertifikate im Binärformat (DER) von der Webseite https://volksverschluesselung.de/ zertifikate.php herunter und binden Sie sie wie folgt in Outlook ein.

Import des Wurzelzertifikats

- 1. Klicken Sie mit der linken Maustaste auf die Zertifikatsdate
iVV-Root-G02-CA.der.
- 2. Es öffnet sich ein Fenster *Datei öffnen Sicherheitswarnung*. Klicken Sie auf Öffnen.
- 3. Es öffnet sich das Fenster Zertifikat. Klicken Sie auf Zertifikat Installieren.
- 4. Es öffnet sich der Zertifikatsimport-Assistent. Klicken Sie auf Weiter.

5. Klicken Sie auf Alle Zertifikate in folgendem Speicher speichern und wählen Sie Vertrauenswürdige Stammzertifizierungsstellen.

Zertifikat	×
Allgemein Details Zertifizierungspfad	← 😺 Zertifikatimport-Assistent
Zertifikatsinformationen	Zertifikatspeicher
Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig. Installieren Sie das Zertifikat in	Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
den Speicher vertrauenswürdiger Stammzertifizierungsstellen, um die Vertrauensstellung zu aktivieren.	Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.
	Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend) Dalle Zertifikate in folgendem Speicher speichern
Ausgestellt für: Volksverschluesselung Root CA G02	Zertifikatspeicher:
Ausgestellt von: Volksverschluesselung Root CA G02	Zertifikatspeicher auswählen X Durchsucher Wählen Sie den Zertifikatspeicher, der verwendet
Gültig ab 26.05.2020 bis 25.05.2036	Werden soll.
Zertifikat installieren	Eigène Zertitikate Greanisationaverbrauen Organisationaverbrauen Zwischenzertifizierungsstellen Arther Directory Berutzerobjekt Viertrauenesitirdine Herausnaher
	Physischen Speicher anzeigen OK Abbrechen Weiter Abbrechen

6. Klicken Sie auf Weiter und dann auf Fertig stellen. Es erscheint eine Sicherheitswarnung, denn Sie legen durch den Import des Wurzelzertifikats fest, dass Sie allen von dieser Zertifizierungsstelle ausgestellten Zertifikaten vertrauen wollen. Sie sollten hier den Fingerabdruck (SHA1 Prüfsumme) mit dem publizierten Fingerabdruck auf unserer Webseite vergleichen. Klicken Sie auf Ja, um das Zertifikat zu importieren.

Sicherh	eitswarnung	\times
	Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:	
	Volksverschluesselung Root CA G02	
	Es wird nicht bestätigt, dass das Zertifikat wirklich von "Volksverschluesselung Root CA G02" stammt. Wenden Sie sich an "Volksverschluesselung Root CA G02", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:	:
	Fingerabdruck (sha1): 65F73FE3 0CE3D293 24B2544F 073B9B00 1B6A4454	
	Warnung: Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf. Möchten Sie dieses Zertifikat installieren?	
	Ja Nein	

Import des Zertifikats der Volksverschluesselung Private CA

- 1. Klicken Sie mit der linken Maustaste auf die Zertifikatsdatei VV-Private-User-G02-CA.der und führen Sie die Schritte 2 bis 4 wie zuvor beschrieben aus.
- 2. Klicken Sie auf Alle Zertifikate in folgendem Speicher speichern und wählen Sie Zwischenzertifizierungsstellen.

Algemein Detals Zertifizierungspfad	
Zertifikatsinformationen Dieses Zertifikat kann nicht bis zu einer Zertifikarismonestelle verefinet werden	Zertifikatspeicher Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
	Windows kann automätisch einen Zertfikatspeicher auswählen, oder Sie können einen Speicherort für die Zertfikate angeben. O Zertfikatspeicher automatisch auswählen (auf dem Zertfikattyp basierend) () Alle Zertfikate in folgendem Speicher speichern
Ausgestellt für: Volksverschluesselung Private CA G02	Zertifikatspeicher auswählen X
Ausgestellt von: Volksverschluesselung Root CA G02	Wählen Sie den Zertifikatspeicher, der verwendet werden soll.
Guitig ab 26.05.2020 bis 25.05.2030	Eigene Zertifikate Organisationsvert haven Organisationsvert haven Vertrauenswürzlichen Active Directory-Benutzerobjekt Vertrauenswürzliche Herausneher Vertrauenswürzliche Herausneher
c	Physischen Speicher anzeigen OK Abbrechen Weiter Abbrechen

3. Klicken Sie auf Weiter und dann auf Fertig stellen.

3.4.3 Austausch des Verschlüsselungszertifikats mittels signierter E-Mail

Eine einfache Möglichkeit sein Verschlüsselungszertifikat verfügbar zu machen, besteht darin, dem Kommunikationspartner eine signierte E-Mail zu senden. Bei einer signierten E-Mail wird i. d. R. auch das Verschlüsselungszertifikat des Absenders mitgesendet und dem E-Mail-Programm auf Empfängerseite bekannt gemacht.

Hinweis: Im E-Mail-Programm des Empfängers der signierten Nachricht muss die Zertifikatskette der Volksverschlüsselung installiert sein, damit die Gültigkeit der Signatur überprüft werden kann. Falls der Empfänger die Volksverschlüsselungs-Software nicht verwendet, muss er die Zertifikate *Volksverschluesselung Root-CA G02* und *Volksverschluesselung Private-CA G02* manuell installieren, wie in Installation der CA-Zertifikate der Volksverschlüsselung beschrieben.

Gehen Sie bei Empfang der signierten E-Mail wie folgt vor:

1. Öffnen Sie die signierte E-Mail von Ihrem Kommunikationspartner und fügen Sie die Adresse des Absenders zu Ihren Outlook-Kontakten hinzu. Gehen Sie hierzu auf die E-Mail-Adresse und drücken Sie die rechte Maustaste. Aus dem Kontextmenü wählen Sie **Outlook-Kontakten hinzufügen**.

Ð	り ▼ P Suchen	(erika.muster@vv.s	sit.fraunh
Posteingang	Start Senden/Empfangen Ordn Alle Ungelesen Nach Datum > Heute erika.muster@vv.sit.fr Englesen Signiere Nachricht 1140 halte, diese Nachricht ist 1140 volksverschlüsselung: Testnac. 1034	er Ansicht Hilfe ↑ Signierte Nach E erika.mu: Signiert von erika.mu Hallo Xavier,	E & □ ≥ ···· X Ausschneiden Kopieren Einfügen & Läschen	✓ → … 11:39 8
∑ ۲ ا∰ ۲ α	noreply@test.volksve ß Volksverschlüsselung Zertifika 10:34 Guten Tag Xavier Muster, ihr	diese Nachricht ist m VG Erika	Alle auswählen Zu Favoriten hinzufügen R∓ Zu Outlook-Kontakten hinzufügen Outlook-Eigenschaften öffnen Visitenkarte öffnen	

2. Der Kontakt wird angezeigt. Klicken Sie auf **Speichern**, um den Kontakt hinzuzufügen. Das Verschlüsselungszertifikat wird dabei automatisch mitgespeichert.

Ш У		↓ v Erika	Muster -	Kontakt	,	ı		• -	0	×
Datei	Kontakt	Einfügen	Text form	atieren	Überprüfen	Hilfe				
×		Ľχ	2	A	P		Q			
Aktionen ~	Anzeigen ~	Kommunizieren ~	Namen ~	Optionen ~	Kategorien ~	Plastischer Reader	Zoom	Einstellung	len	
						Plastisch	Zoom	GpgOL	5	^
Name		Erika Muster					Erika	Muster		
Firma							erika.n	nuster@vv.sit.f	raunhofer.de	
Position										
Speicher	rn unter	Muster, Erika			•	- 11				
Internet										
名 E-N	/ail 🔻	erika.muster@vv.s	it.fraunhofe	r.de						
Anzeiger	n als	erika.muster@vv.s	it.fraunhofe	r.de			tinen			
Webseite	enadresse						Juzen			
Chatadresse										
Telefonnumr	mern									

3. Sie können überprüfen, ob das Zertifikat auch tatsächlich gespeichert wurde. Gehen Sie hierzu auf die E-Mail-Adresse und drücken Sie die rechte Maustaste. Aus dem Kontextmenü wählen Sie **Kontakt bearbeiten**.

Ð	り 、 P Suchen				Erika Mus	ter	o x
Datei	Start Senden/Empfangen	Ordner	Ansicht Hilfe	EM			
, M	Alle Ungelesen Nach Da	tum ∽ ↑	Signierte Nachr		C 🗆 I		✓ ¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬
	erika.muster@vv.sit.fr	Я	E An O xavier	X Ausschnei	iden		11:39
eingang	Signierte Nachricht Hallo Xavier, diese Nachricht ist	11:40	Signiert von erika.must	🕒 Kopieren			R
Post	norenly@test volksve	А		🛅 Einfügen			
	Volksverschlüsselung: Testnac	10:34	Hallo Xavier,	♦ Löschen			
	noreply@test.volksve	ß	diese Nachricht ist mit	Alle ausw	ählen	niert.	
	Volksverschlüsselung: Zertifika Guten Tag Xavier Muster Ibr	10:34	VG	Zu Favori	ten <u>h</u> inzufügen		
	Gateri ragitariei moster, im		Erika	Kontakt <u>b</u>	earbeiten		
				Visitenkar	te öffnen		
⁸⁹							
Ŕ							
••••							

4. Wählen Sie nun **Anzeigen->Zertifikate**. Im Zertifikatsfenster sehen Sie das Zertifikat. Mit einem Doppelklick wird Ihnen das Zertifikat angezeigt.

। ७ ९ ↑	↓ ⊽ Erika	Muster - Kontakt	✓ Suchen			E –	0	×
Datei Kontakt	Einfügen	Text formatieren	Überprüfen	Hilfe				
	Γ <u>λ</u>		P.		Q			
× ×	× ×	v v	v v	Reader	Zoom	Einstellungen		
				Plastisch	Zoom	GpgOL 🗳		^
Name. Firma Position Speicherwomer Internet Maligemeir Aligemeir Aligemeir Aligemeir Aligemeir Aligemeir Anzeigen als Webseitenadresse Chatadresse Telefonnummern Geschäftlich ▼ Fax geschäftl ▼ Adressen Geschäftlich ▼		it.fraunhofer.de it.fraunhofer.de		Notizer	erika.m	Muster Muster@vv.sitfraunl	hofer.de	
Dies ist die Postanschrift			Karte					

3.4.4 Manuelle Konfiguration des Verzeichnisdienstes der Volksverschlüsselung

Die Volksverschlüsselung bietet einen öffentlichen LDAP (Lightweight Directory Access Protocol) Verzeichnisdienst an, in dem die Verschlüsselungszertifikate der Nutzer der Volksverschlüsselung veröffentlicht werden, sofern sie bei der Zertifikatsbeantragung hierzu ihre Einwilligung erteilt haben. Wenn der Verzeichnisdienst in Outlook für Microsoft 365 konfiguriert ist und der Kommunikationspartner sein Zertifikat im

Verzeichnisdienst der Volksverschlüsselung veröffentlicht hat, wird bei Eingabe seiner E-Mail-Adresse automatisch dessen Verschlüsselungszertifikat ausgewählt.

Wenn Sie die Volksverschlüsselungs-Software nicht verwenden, können Sie den Verzeichnisdienst der Volksverschlüsselung auch manuell konfigurieren, indem Sie ein neues Adressbuch einrichten. Hierfür benötigen Sie den Hostname, die Portnummer und den Basis-DN. Die Konfigurationsparameter des Verzeichnisdienstes der Volksverschlüsselung finden Sie auf unserer Webseite.

So richten Sie den Verzeichnisdienst der Volksverschlüsselung in Outlook für Microsoft 365 ein :

1. Öffnen Sie ihre Kontoeinstellungen, indem Sie in Outlook auf **Datei-**>Kontoeinstellungen->Kontoeinstellungen klicken



2. Es erscheint das Fenster *Kontoeinstellungen*. Wählen Sie **Adressbücher** und dann **Neu**.

ail Datendateien R	SS-Feeds SharePoir	t-Listen Internetkale	nder Veröffentlichte Ka	lender Adressbücher	
Neu 🚰 Ändern	🗙 Entfernen				
ime		Тур			
tlook-Adressbuch		MAP			

14

3. Wählen Sie Internetverzeichnis (LDAP).

Konto hinzufügen	22
Verzeichnis- oder Adressbuchtyp Sie können wählen, welchen Verzeichnis- oder Adressbuchtyp Sie hinzufügen möchten.	×
Thermetverzeichnisdienst (LDAP) Verbindung zu einem LDAP-Server herstellen, um E-Mail-Adressen und weitere Informationen zu suchen und zu überprüfen. Usacliche Adressbucher Verbindung zu einem Adressbucher	
verbindung zu einem Adressbuch nerstellen, um E-Mali-Adressen und weitere Informationen zu suchen und zu überprüfen.	
< Zurück	Weiter > Abbrechen

4. Geben Sie als Servername ldap.volksverschluesselung.de ein und gehen Sie auf Weitere Einstellungen....

Konto hinzufügen		×
Einstellungen für Geben Sie die E	den Verzeichnisdienst (LDAP) instellungen ein, die für den Zugriff auf Informationen eines Verzeichnisdiensts erforderlich sind.	***
Serverinformatione	n	
Geben Sie den Nam Internetdienstanbie	en des Verzeichnisservers ein, den Sie von Ihrem eter oder Systemadministrator erhalten haben.	
Servername:	ldap.volksverschluesselung.de	
Anmeldeinformatio	nen	
Server erfordert	Anmeldung	
Benutzername:		
Kennwort:		
Gesicherte K	ennwortauthentifizierung (SPA) erforderlich	
	Weitere Einstellungen	
	< Zurück	Weiter > Abbrechen

- 5. Tragen Sie die Konfigurationsdaten wie folgt in die Felder ein:
 - Anzeigename: Verzeichnis der Volksverschlüsselung (frei wählbar)
 - Anschluss: 636
 - Setzen Sie ein Häkchen bei Secure Sockets Layer verwenden

Conto ändern		
Einstellungen für den Verzeichnisdienst (LDAP) Geben Sie die Einstellungen ein, die für den Zugriff auf Inform	ationen eines Verzeichnisdiensts erford	erlich sind.
Serverinformationen		
Get Microsoft LDAP-Verzeichnis	×	
Inte Ser Verbindung Suche		
Anzeigename		
Anzeigename, wie er im Adressbuch erscheint.		
Verzeichnis der Volksverschlüsselung		
	_	
Verbindungsdetails		
Anschluss: 636		
Sacura Sacketr		
Layer verwenden		
OK Abbrechen	Übernehmen	< Zurück Weiter > Abbreche
OK Abbrechen	Obernenmen	< Zurück Weiter > Abbreche

- 6. Wechseln Sie auf den Karteireiter Suche
 - Wählen Sie Suchbasis Benutzerdefiniert und geben Sie folgenden Wert ein ou=Certificates,o=Volksverschluesselung,c=de
 - Bestätigen Sie mit **OK**

Verinformationen Microsoft LDAP-Verzeichnis	×		
Verbindung Suche			
Servereinstellungen]	
Timeout der Suche in Sekunden:	60		
Geben Sie die maximale Anzahl der E die bei einer erfolgreichen Suche an werden sollen:	inträge an, 100 gezeigt		
Suchbasis			
Standard verwenden			
Benutzerdefiniert: kates, o=Volk	csverschluesselung, c= de		

3.4.5 Manuelle Konfiguration des Verzeichnisdienstes einer fremden Zertifizierungsstelle

Hat Ihr Kommunikationspartner sein Zertifikat in einem Verzeichnisdienst eines anderen Zertifizierungsanbieters veröffentlich, dann bitten Sie ihn, Ihnen die Konfigurationsdaten zu nennen: Hostname, Portnummer (mit/ohne SSL/TLS) und Basis-DN. Wenn Ihnen die Konfigurationsdaten bekannt sind, können Sie den Verzeichnisdienst, wie im vorherigen Abschnitt beschrieben, in Outlook für Microsoft 365 einrichten.

3.4.6 Senden einer verschlüsselten E-Mail

Im Folgenden wird eine Möglichkeit beschrieben, wie Sie eine E-Mail für Ihren Kommunikationspartner in Outlook für Microsoft 365 verschlüsseln können.

Im folgenden Beispiel wird davon ausgegangen, dass Ihr Kommunikationspartner ebenfalls ein Zertifikat der Volksverschlüsselung besitzt und dieses im Verzeichnis der Volksverschlüsselung veröffentlicht hat. In diesem Fall holt sich Outlook das Zertifikat *automatisch* aus dem konfigurierten Verzeichnisdienst der Volksverschlüsselung.

Für die Kommunikation mit einem Kommunikationspartner, dessen Zertifikat Sie noch nicht kennen, müssen Sie zuerst sein Zertifikat in Ihrem E-Mail-Programm verfügbar machen, wie in den vorhergehenden Abschnitten beschrieben.

In Ihrem Ordner, in dem Ihre gesendeten E-Mails abgespeichert werden, können Sie eine verschlüsselte Nachricht an dem "Schloss-Symbol" erkennen. Jede verschlüsselte E-Mail wird auch mit Ihrem **Verschlüsselungszertifikat** verschlüsselt und in diesem Ordner abgelegt. Wenn Sie auf das Schloss-Symbol klicken, dann auf **Verschlüsselungsschicht->Details** anzeigen und dann auf **Zertifikat anzeigen**, sehen Sie Ihr Verschlüsselungszertifikat.

- 1. Suchen Sie die E-Mail-Adresse Ihres Kommunikationspartners im Verzeichnis der Volksverschlüsselung:
 - Wählen Sie **Neue Nachricht** und klicken Sie auf **An...**; es erscheint das Fenster *Namen auswählen.*
 - Wählen Sie unter Adressbuch das Verzeichnis der Volksverschlüsselung.
 - Geben Sie im Feld **Suche** die **vollständige E-Mail-Adresse** ein, klicken Sie auf **OK** und wählen Sie die Adresse mit einem **Doppelklick** aus.

⊒ਜ਼ਿਤਟੇ≜∳∓	Unbenannt - Nachricht (HTML) ?
DATEI NACHRICHT EINF	ÜGEN OPTIONEN TEXT FORMATIEREN ÜBERPRÜFEN
Einfügen	Image: A for the second sec
Zwischenablage	Suchen: Nur Name Mehr Spalten Adressbuch
An	erika.muster@vv.sit.fraunhofer.de OK Verzeichnis der Volksverschlüsselung - Weitere V
	Name E-Mail-Adresse E Telefon gesch Büro Position Firma
Betreff	
	An -> Erika Muster
	(c->
	Bcc ->
	OK Abbrechen

2. Nachdem Sie Ihre E-Mail verfasst haben, klicken Sie auf **Optionen**, dann auf das Icon mit der Beschriftung **Verschlüsseln** und schicken Sie anschließend Ihre E-Mail ab.

891	↓ ₹	Unbenannt - Nachrich	nt (HTML) 🔎 Suc	hen		Ŧ	-	×
Datei Na	chricht Ein	fügen Optionen	Text formatieren	Überprüfen	Hilfe			
Designs	Bcc Von Verso	chlüsseln Signieren	Verlauf verlauf	er ×	ng verzögern richten an			
Felde	r anzeigen	Verschlüsseln		Weitere Optionen	L2			^
Senden	An	erika.muster@vv.sit.f	fraunhofer.de					
benden								
	Bcc							
	Betreff							

3.4.7 Empfang einer verschlüsselten E-Mail

Wenn Sie eine verschlüsselte E-Mail empfangen, wird diese automatisch beim Öffnen entschlüsselt, vorausgesetzt der private Schlüssel ist in Outlook für Microsoft 365 konfiguriert. Andernfalls erhalten Sie die Meldung: ""**Das Element kann im Lesebereich nicht angezeigt werden. Öffnen Sie das Element, um den Inhalt zu lesen**"". Das Schloss-Symbol zeigt an, dass die E-Mail vom Absender (hier: Erika Muster) verschlüsselt wurde.

ଅ୨୯↑↓	~	Ein	e vertrauliche N	achricht - Nachr	icht (Nur-Text)		ר ק	<u>ه</u>		×
Datei Nachricht H	Hilfe									
Image: Constraint of the second se	Antworten	QuickSteps	Verschieben V	Markierungen	D Bearbeiten	Plastisch	Übersetzer	Q Zoom	? Unsicher	
Löschen		QuickSteps					Sprache	Zoom	GpgOL IS	_
Eine vertrauliche Nachricht										
erika.muster@vv.sit.fraunhofer.de \bigcirc Antworten \bigcirc Allen antworten \rightarrow Weiterleiten \dotsb							•			
An Oxavier.m	uster@vv.sit.fr	raunhofer.de						Mo 23.	.05.2022 15:	53
									â]

3.4.8 Senden einer signierten E-Mail

Für das Signieren Ihrer E-Mail wird Ihr privater Schlüssel zu Ihrem Signaturzertifikat verwendet, welcher von der Volksverschlüsselungs-Software bereits in Ihrem Outlook installiert wurde.

In Ihrem Ordner, in dem Ihre gesendeten E-Mails abgespeichert werden, können Sie eine signierte Nachricht an dem **Siegel-Symbol** erkennen.

Nachdem Sie Ihre E-Mail verfasst haben, klicken Sie unter **Optionen** auf das Icon mit der Beschriftung **Signieren** und schicken anschließend über **Senden** Ihre E-Mail ab.

	> ↑	• •	~			Diese I	Nachricht ist signiert	- Nachricht (Nur	r-Text)	Q
Datei	Nac	hricht:	Einf	ügen	Optione	en Te	ext formatieren	Überprüfen	Hilfe	
Designs V	Felder	Bcc Von	(Versch	hlüsseln Verschlüs	G Signieren	& Verlauf v	Gesendetes Elem speichern unter	ent Antworte	ung verzögern n richten an	Ā
	relaci	unzeigen		versenius	Jen 1		•	enere optionen		-
\triangleright		An		<u>erika.m</u>	nuster@vv.s	it.fraunhc	fer.de			
Sende	n	Cc								
		Всс								
		Betre	ff	Diese I	Nachricht ist	signiert				

Hallo Erika, diese Nachricht ist signiert.

Hinweise: Sie können Outlook für Microsoft 365 so konfigurieren, dass jede neue E-Mail standardmäßig signiert wird. Außerdem sollten Sie signierte Nachrichten immer im Klartext versenden, damit auch Empfänger ohne S/MIME-Sicherheit die Nachricht lesen können. In Outlook ist dieses Kontrollkästchen standardmäßig aktiviert. Sie können die Einstellungen wie folgt vornehmen:

- 1. Wählen Sie **Datei** und dann **Optionen**.
- 2. Gehen Sie auf **Trust Center**.

- 3. Klicken Sie auf Einstellungen für das Trust Center.
- 4. Klicken Sie auf den Karteireiter E-Mail-Sicherheit und setzen Sie bei Ausgehende Nachrichten digitale Signatur hinzufügen ein Häkchen.

Trust Center	8 23
Vertrauenswürdige Herausgeber Datenschutzoptionen E-Mail-Sicherheit Anlagenbehandlung Automatischer Download Makroeinstellungen Programmgesteuerter Zugriff	Verschlüsselte E-Mail-Nachrichten Impalt und Anlagen für ausgehende Nachrichten verschlüsseln Impalt und Anlagen für ausgehende Nachrichten verschlüsseln Impalt und Anlagen für ausgehende Nachrichten verschlüsseln Impalt und Anlagen für ausgehende Nachrichten digitale Signatur hinzufügen Impalt und Anlagen für ausgehende Nachrichten verschlüsseln Impalt und Anlagen für ausgehende Nachrichten signatur hinzufügen Impalt und Anlagen für ausgehende Nachrichten signatur Standardeinstellung: Impalt und Kalmeter Digitale IDs (Zertifikate Importieren/Exportieren Impalt veröffentlichen Importieren/Exportieren Impalt alignierte Nachrichten im Nur-Text-Format lesen Digitale iljagineite Nachrichten im Nur-Text-Format lesen Skript in Ordnern Skript in Offentlichen Ordnern zulassen Skript in Öffentlichen Ordnern zulassen Skript in Öffentlichen Ordnern zulassen
	OK Abbrechen

3.4.9 Empfang einer signierten E-Mail

Eine signierte E-Mail erkennen Sie an dem **Siegel-Symbol**. Wenn Sie eine signierte E-Mail empfangen, prüft Outlook für Microsoft 365 die Gültigkeit der Signatur. Kann die Signatur nicht geprüft werden, da beispielsweise die CA-Zertifikate noch nicht importiert sind oder das Zertifikat zwischenzeitlich gesperrt wurde, erscheint eine Fehlermeldung. Wenn Sie auf das **Siegel-Symbol** klicken, erhalten Sie Informationen zum Signaturzertifikat des Senders:



Wurde die Signatur auf dem Transportweg manipuliert oder ist das Zertifikat des Senders gesperrt, wird dies anhand eines **gelben Warndreiecks** sichtbar:

Q. Activatoria Q. Allina rationation: Q. Weiterleiten Do 3411.2016 59:11 Dis 39:11 Erika Muster erika.muster@vv.sit.fraunhofer.de> Signierte Nachricht Signierten activiter.de Signierten metter@vv.sit.menter.de Signierten activiter.de	
Eine signierte Nachricht von Erika Muster!!	<u>_</u>

Wenn Sie auf das **Warndreieck** und auf **Details** klicken, erhalten Sie weitere Informationen, z.B. ob das Zertifikat auf einer Sperrliste steht.

Eigenschaften der Nachrichtensicherheit	x
Betreff: Signierte Nachricht	
Nachrichten enthalten u. U. Ebenen für Verschlüsselung oder digitale Signat Ebene für digitale Signaturen kann mehrere Signaturen enthalten.	turen. Jede
Sicherheitsschichten	
Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen.	
Betreff: Signierte Nachricht	
Digitalsignaturschicht	
Signierer: erika.muster@vv.sit.fraunhofer.de	
Beschreibung:	
Fehler:	
Das Zertifikat, das zum Erstellen dieser Signatur verwendet wurde, ist auf ein	ner
Signiert von erika muster///ww.cit.traunhoter de unter Verwendung von PSA/	SHA756
Klicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten	
Signaturschicht zu erhalten oder um sie zu bearbeiten:	
Vertrauen Details anzeigen Zertifizierungsstelle v	ertrauen
🔲 Bei Fehlern in digital signierten Nachrichten Warnhinweis anzeigen.	Schließen

3.4.10 Senden einer signierten und verschlüsselten E-Mail

Wenn Sie eine signierte und verschlüsselte E-Mail versenden möchten, gehen Sie vor wie in den vorherigen Abschnitten beschrieben. In diesem Fall müssen vor dem Versand der E-Mail unter **Optionen** das Icon für die **Verschlüsselung** und für das **Signieren** ausgewählt werden.

3.4.11 Kontrolle der installierten Zertifikate im Trustcenter

Wenn Sie überprüfen möchten, ob Ihre Zertifikate im Trustcenter von Outlook für Microsoft 365 installiert sind, dann können Sie wie folgt vorgehen:

1. Wählen Sie Datei, dann Optionen und klicken Sie auf Trust Center und Einstellungen für das Trust Center.



2. Gehen Sie auf den Karteireiter E-Mail Sicherheit und klicken Sie auf Einstellungen....

Trust Center		?	×
Vertrauenswürdige Herausgeber	Verschlüsselte E-Mail-Nachrichten		
Datenschutzoptionen	🗣 🔄 Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln		
E-Mail-Sicherheit	Ausgehenden Nachrichten digitale Signatur hinzufügen		
Anlagenbehandlung	Signierte Nachrichten als <u>K</u> lartext senden		
Automatischer Download	S/MIME-Bestätigung anfordern, wenn mit S/MIME signiert		
Makroeinstellungen	Standardeinstellung: VV-PKI VI Einstellungen		
Programmgesteuerter Zugriff	Digitale IDs (Zertifikate)		
	Digitale IDs bzw. Zertifikate sind Dokumente, mit denen die Identität in elektronischen Transaktionen nachgewies kann.	en werd	en
	Importieren/Exportieren Digitale ID anfordern		
	Als Nur-Text lesen		
	Standardnachrichten im <u>N</u> ur-Text-Format lesen		
	Digital signierte Nachrichten im Nur-Text-Format lesen		
	Skript in Ordnern		
	Skript in <u>f</u> reigegebenen Ordnern zulassen		
	Skrip <u>t</u> in Öffentlichen Ordnern zulassen		
·] [.	OK	Abbre	echen

3. Im Fenster Sicherheitseinstellungen ändern können Sie überprüfen, ob Ihr Signaturzertifikat und Verschlüsselungszertifikat konfiguriert ist. Wird Ihr Zertifikat nicht angezeigt, können Sie durch einen Klick auf **Auswählen** die Liste der vorhandenen Zertifikate anzeigen lassen. Das Zertifikat der Volksverschlüsselung muss auf jeden Fall in der Liste erscheinen, auch wenn es nicht direkt ausgewählt ist. Outlook für Microsoft 365 wählt automatisch beim Signieren und Entschlüsseln von E-Mails das passende Zertifikat zur E-Mail-Adresse aus.

Trust Center							? ×
Vertrauenswürdige Herausgeber	Verschlüsse	lte E-Mail-Nachrichten					
Datenschutzoptionen	<u></u>] Inhalt und Anlagen für ausg	ehende Nachrichte	n verschlüsseln			
E-Mail-Sicherheit	- Te F		Italian I. Chanadana Ista			1	
Anlagenbehandlung		Sicherheitseinstellungen ände	rn		×		
Automatischer Download	1	Bevorzugte Sicherheitseinstellung	en				
Makroeinstellungen		Name der Sicherheitseinstellur	19:				
Programmgesteuerter Zugriff	Digitale II	Kryptografieformat:	S/MIME		~		
	D I	Standardeinstellung für die	ses Format kryptogra	fischer Nachrichten		n Transaktionen nachgewie	esen werden
	🖳 🥵 🖌	Standardsicherheitseinstell	ung für alle kryptogra	fischen Nachrichten			
		Sicherheitskennzeichen.	Neu	Löschen			
	Als Nur-T	Zertifikate und Algorithmen					
	Stand	Signaturzertifikat:	Xavier Muster <xavi< td=""><td>ier.muster@vv.sit.f</td><td>Auswählen</td><td></td><td></td></xavi<>	ier.muster@vv.sit.f	Auswählen		
	🗌 Diç	Hashalgorithmus:	SHA256	~			
	Skript in C	Verschlüsselungszertifikat:	Xavier Muster <xavi< td=""><td>ier.muster@vv.sit.f</td><td>Auswählen</td><td></td><td></td></xavi<>	ier.muster@vv.sit.f	Auswählen		
	Skript	Verschlüsselungsalgorithmus:	AES (256-bit)	~			
	Skript	Signierten Nachrichten dies	e Zertifikate hinzufüg	jen			
				ОК	Abbrechen		
	L					1	
						ОК	Abbrechen

3.4.12 Nutzung mehrerer E-Mail-Konten

In Outlook können Sie mehrere E-Mail-Konten einrichten und für jede E-Mail-Adresse ein eigenes Zertifikat besitzen. Die verschlüsselte Kommunikation zwischen zwei installierten E-Mail-Konten findet genauso statt, wie die Kommunikation mit einem externen Kommunikationspartner, d.h. die Zertifikate müssen ggf. noch ausgetauscht werden (vgl. Wie bekomme ich das Verschlüsselungszertifikat des Empfängers?).

Wenn Sie für mehrere E-Mail-Konten in Outlook jeweils ein Zertifikat von der Volksverschlüsselung verwenden und diese mit Hilfe der Volksverschlüsselungs-Software in Outlook installieren, können Sie sofort die E-Mail-Konten in Outlook für eine vertrauliche und sichere Kommunikation verwenden. Jedes E-Mail-Konto wird mit dem eigenen persönlichen Zertifikat konfiguriert. Falls Sie für eine E-Mail-Adresse ein Zertifikat von einer anderen Zertifizierungsstelle verwenden möchten, müssen Sie dieses manuell in Outlook einrichten.

Welche Zertifikate in Outlook konfiguriert sind, können Sie gemäß Abschnitt Kontrolle der installierten Zertifikate im Trustcenter im Trust Center kontrollieren, wie folgendes Beispiel zeigt:

Trust Center					? ×
Vertrauenswürdige Herausgeber	Verschlüsse	elte E-Mail-Na	achrichten		
Datenschutzoptionen	<u>Q_</u>	Inhalt und	Anlagen für ausgehende Nachrichten verschlüsseln		
Formularbasierte Anmeldung	A	Windows-S	icherheit	×	
E-Mail-Sicherheit					
Anlagenbehandlung		2=	Xavier Muster		
Automatischer Download			Aussteller: Volksverschluesselung Private CA		de) 💌 <u>E</u> instellungen
Makroeinstellungen	Distals		G02 TEST		
Programmgesteuerter Zugriff	Digitale I		Gültig ab: 19.05.2022 bis 17.05.2025		
	Als Nur-T	22	Erika Muster <erika muster@vv.sit.fraunhofer.de=""> [VV] Aussteller. Volksverschluesselung Private CA G02 TEST Gültig ab: 19.05.2022 bis 17.05.2025</erika>		ransaktionen nachgewiesen werden

3.4.13 Nutzung eines gesperrten Zertifikats

Sie können jederzeit Ihr Zertifikat vor Ablauf der Gültigkeit mit Hilfe der Volksverschlüsselungs-Software sperren lassen, beispielsweise wenn es fehlerhaft ist oder kompromittiert wurde. Hierbei ist zu beachten, dass immer alle drei Zertifikate gesperrt werden.

Erstellen Sie immer auch eine Sicherungskopie von Ihren gesperrten Zertifikaten und entfernen Sie diese nicht aus dem Windows Zertifikatsspeicher, da Sie ansonsten alte Nachrichten nicht mehr entschlüsseln können. Sollten gesperrte Zertifikate nicht mehr im Windows Zertifikatsspeicher vorliegen, können Sie diese mit Hilfe der Sicherungskopie und der Volksverschlüsselungs-Software wieder installieren.

Nach der Sperrung können Sie keine signierten und/oder verschlüsselte E-Mails mehr senden. Sie erhalten folgende Fehlermeldung:



Wenn Sie in den *Sicherheitseinstellung* die Häkchen entfernen, wird die Nachricht unsigniert bzw. unverschlüsselt versendet.

_					
S	icherheitseigenschafter	ı			\times
	Nachrichten und Anlage	n verschlüsseln			
	Diese Nachricht digital s	ignieren			
	Signatur und Klarte	ext senden			
	S (MIME-Rostätigur	a anfordern			
		ig anordern			
Si	cherheitseinstellungen				
	Sichemen:				
	<automatisch></automatisch>			Einst	ellungen ändern
	Sicherheitskennzeichen				
	Richtlinienmodul:	<keines></keines>		\sim	Konfigurioron
		(Kentes)		_	Koniiguneren
	Klassifikation:			\sim	
	Vertraulichkeitsstufe:				
				ОК	Abbrechen
S	icherheitseigenschafter	า			×
S	icherheitseigenschafter	1			×
S	icherheitseigenschafter	n en verschlüsseln			×
s L	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s —	n en verschlüsseln ignieren			×
s L	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte	n en verschlüsseln signieren ext senden			×
s L	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte	n en verschlüsseln ignieren ext senden ng anfordern			×
s Si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen	n en verschlüsseln ignieren ext senden ng anfordern			×
s Si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit:	n en verschlüsseln ignieren ext senden ng anfordern			×
S Si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit: < Automatisch>	n en verschlüsseln ignieren ext senden ng anfordern	~	Einst	×
S Si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit: <automatisch></automatisch>	n en verschlüsseln ignieren ext senden ng anfordern	v	Einst	×
S Si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit: <automatisch> Sicherheitskennzeichen</automatisch>	n en verschlüsseln ignieren ext senden ng anfordern	×	Einst	×
s Si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit: <automatisch> Sicherheitskennzeichen Richtlinienmodul:</automatisch>	n en verschlüsseln ignieren ext senden ng anfordern <keines></keines>	~	Einst	Konfigurieren
S S Si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit: <automatisch> Sicherheitskennzeichen Richtlinienmodul: Klassifikation:</automatisch>	n en verschlüsseln ignieren ext senden ng anfordern 	×	Einst	Konfigurieren
S Si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit: <automatisch> Sicherheitskennzeichen Richtlinienmodul: Klassifikation: Vertraulichkeitsetufer</automatisch>	n en verschlüsseln ignieren ext senden ng anfordern <keines></keines>	×	Einst	Konfigurieren
s S si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte Sicherheitseinstellungen Sicherheit: <automatisch> Sicherheitskennzeichen Richtlinienmodul: Klassifikation: Vertraulichkeitsstufe:</automatisch>	n verschlüsseln iignieren ext senden ng anfordern 	×	Einst ~	Konfigurieren
S S Si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit: <automatisch> Sicherheitskennzeichen Richtlinienmodul: Klassifikation: Vertraulichkeitsstufe:</automatisch>	n verschlüsseln signieren ext senden ng anfordern	×]	Einst ~	Konfigurieren
si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit: <automatisch> Sicherheitskennzeichen Richtlinienmodul: Klassifikation: Vertraulichkeitsstufe:</automatisch>	n verschlüsseln ignieren ext senden ng anfordern <keines></keines>	×	Einst ~	ellungen ändern
s si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S S/MIME-Bestätigur cherheitseinstellungen Sicherheit: <automatisch> Sicherheitskennzeichen Richtlinienmodul: Klassifikation: Vertraulichkeitsstufe:</automatisch>	n verschlüsseln ignieren ext senden ng anfordern 	×	Einst	Konfigurieren
si	icherheitseigenschafter Nachrichten und Anlage Diese Nachricht digital s Signatur und Klarte S/MIME-Bestätigur cherheitseinstellungen Sicherheit: <automatisch> Sicherheitskennzeichen Richtlinienmodul: Klassifikation: Vertraulichkeitsstufe:</automatisch>	n verschlüsseln iignieren ext senden ng anfordern 	×	Einst	Konfigurieren

3.4.14 Zertifikate entfernen

Wenn Ihre Schlüssel/Zertifikate aus dem Trustcenter von Outlook und dem Windows Zertifikatsspeicher entfernt sind, können Sie für Sie verschlüsselte Nachrich-

ten nicht mehr lesen. Sie können aber nachträglich die Schlüssel/Zertifikate mit der Volksverschlüsselungs-Software beispielsweise aus der Sicherungskopie wieder installieren.

Wenn Sie Ihre Schlüssel/Zertifikate in Outlook für Microsoft 365 entfernen möchten, gehen Sie wie folgt vor:

1. Wählen Sie Datei, dann Optionen und klicken Sie auf Trust Center und Einstellungen für das Trust Center

Outlook-Optionen	?	×
Allgemein E-Mail	Sorgen Sie für die Sicherheit Ihrer Dokumente und des Computers.	
Kalender	Datenschutz	
Personen Aufgaben Suchen	Microsoft nimmt den Datenschutz ernst. Weitere Informationen, wie Microsoft Outlook für den Datenschutz sorgt, finden Sie i den Datenschutzbestimmungen Datenschutzbestimmungen für Microsoft Outlook anzeigen	n
Sorache	Sicherheit & mehr	
Erweitert	Besuchen Sie Office.com, um weitere Informationen zum Datenschutz und zur Sicherheit zu erhalten.	
Menüband anpassen	Microsoft Trustworthy Computing	
Symbolleiste für den Schnellzugriff	Microsoft Outlook-Trust Center	
Add-Ins	Das Trust Center enthält Einstellungen für Sicherheit und Datenschutz, um für die	_
Trust Center	Sicherheit des Computers zu sorgen. Es wird davon abgeraten, diese Einstellungen zu ändern.	9 r
	OK Abbre	chen

2. Gehen Sie auf den Karteireiter **E-Mail Sicherheit** und klicken Sie auf **Einstellungen...**.

Trust Center		7	×
Vertrauenswürdige Herausgeber Verschlüss	elte E-Mail-Nachrichten		
Datenschutzoptionen	Inbalt und Anlagen für ausgehende Nachrichten verschlüsseln		
E-Mail-Sicherheit	Ausgehenden Nachrichten digitale Signatur hinzufügen		
Anlagenbehandlung	Signierte Nachrichten als Klartext senden		
Automatischer Download	S/MIME-Bestätigung anfordern, wenn mit S/MIME signiert		
Makroeinstellungen	tandardeinstellung: VV-PKI v Einstellungen		
Programmgesteuerter Zugriff Digitale ID	s (Zertifikate)		
Skript in O	Igliele Ds bzw. Zertifikate sind Dokumente, mit denen die Identität in elektronischen Transaktionen nachgewies nn. mportleren/Exportieren. Digitale ID anfordern xt lesen findachrichten im Nur-Text-Format lesen ital signierte Nachrichten im Nur-Text-Format jesen rdnern in freigegebenen Ordnern zulassen in Offentlichen Ordnern zulassen	en werde	an
	ОК	Abbree	chen

3. Wählen Sie im Fenster *Sicherheitseinstellungen ändern* Ihre Sicherheitseinstellung aus (in diesem Beispiel VV_PKI). Es werden Ihnen das Signatur- und Verschlüsselungszertifikat angezeigt. Klicken Sie auf Löschen.

Sicherheitseinstellungen ände	rn	\times
Bevorzugte Sicherheitseinstellung	en 🦳	
Name der Sicherheitseinstellur	ng:	
VV-PKI		×
Kryptografieformat:	S/MIME	\sim
🗹 Standardeinstellung für die	ses Format kryptografischer Nachrichten	
✓ Standardsicherheitseinstell	ung für alle kryptografischen Nachrichten	
Sicherheitskennzeichen.	Neu Löschen	
Zertifikate und Algorithmen		
Signaturzertifikat:	Xavier Muster <xavier.muster@vv.sit.f< td=""><td>Auswählen</td></xavier.muster@vv.sit.f<>	Auswählen
Hashalgorithmus:	SHA256 V	
Verschlüsselungszertifikat:	Xavier Muster <xavier.muster@vv.sit.f< td=""><td>Auswählen</td></xavier.muster@vv.sit.f<>	Auswählen
Verschlüsselungsalgorithmus:	AES (256-bit) \checkmark	
Signierten Nachrichten die	e Zertifikate hinzufügen	
	ОК	Abbrechen

Hinweis: Wenn Sie Ihre Schlüssel/Zertifikate in Microsoft Anwendungen generell nicht mehr nutzen möchten, reicht es nicht aus, wenn Sie nur die Konfiguration im Trust Center löschen. Die Zertifikate müssen noch aus dem Windows Zertifikatspeicher gelöscht werden. Dazu gehe Sie wie folgt vor:

1. Klicken Sie z.B. im Microsoft Edge oben rechts auf das Zeichen "…" und weiter auf "Einstellungen".

G Google × +		Neuer Tab	STRG+T	×
← → C A C https://www.google.de/?gws_rd=ssl		Neues Fenster	STRG+N	•
Platzieren Sie für den Schnellzugriff Ihre Favoriten in der Favoritenleiste. Jetzt Favoriten verv	walten	Reues InPrivate-Fenster	STRG+UMSCHALTTASTE+N	
Über Google Store		Zoomen	- 100 % + 2	
	• • •	ζ≟ Favoriten	STRG+UMSCHALTTASTE+O	•
		G Sammlungen	STRG+UMSCHALTTASTE+Y	
	Juge	🕙 Verlauf	STRG+H	
	•	⊥ Downloads	STRG+J	
		🗄 Apps	>	
4		C Erweiterungen		
		😵 Leistung		
	Google Suche Auf gut Glück!	Drucken	STRG+P	
		🚱 Webaufnahme	STRG+UMSCHALTTASTE+S	
		🖻 Teilen		
		8 Auf Seite suchen	STRG+F	
		A [®] Laut vorlesen	STRG+UMSCHALTTASTE+U	
		Weitere Tools	>	
Deutschland		Einstellungen		
	CO:-neutral seit 2007	⑦ Hilfe und Feedback	>	
Werbeprogramme Unternehmen Wie funktioniert die Google Suche?		Microsoft Edge schließen	30	

2. Geben Sie im Suchfeld links oben "Zertifikate" ein und klicken Sie auf "Zertifikate verwalten" im rechten Fenster.

Ein	stellungen	Sicherheit	
୍ର	^{Zertifikate} ×	Verwalten der Sicherheitseinstellungen für Microsoft Edge	
8	Profile	Zertifikate verwalten	Ø
6	Datenschutz, Suche und Dienste	HTTPS-VSSI-Zertifikate und -Einstallungen verwalten	
~)	Darstellung	Microsoft Defender SmartScreen	ō 💼
E	Start, Startseite und neue	Mein Gerät mit Microsoft Defender SmartScreen vor schädlichen Websites und Downloads schützen	
ß	Registerkarten Teilen, kopieren und einfügen	Potenziell unerwünschte Apps blockieren Blockiert Downleads von nicht vertrauenswürdigen Apps, die unerwarteter Verhalten verursachen können	۵ 💽

3. Wählen Sie **Eigene Zertifikate**. Markieren Sie die zu entfernenden Zertifikate und klicken Sie auf **Entfernen**.

Zertifikate	×
Beabsichtigter Zweck: <alle></alle>	Y
Eigene Zertifikate Andere Personen Zwischenzertifizierungsstellen Vertrau	ienswürdige Stamn 🔹 🕨
WU-PKI Clien. V-PKI Client. 18.11. W-PKI Cli WU-PKI Clien. 24.11 Xavier Muster Volksverschlu 24.11 Xavier Mus WAavier Muster Volksverschlu 24.11 Xavier Mus WARK Muster WAavier Muster Volksverschlu 24.11 Xavier Mus WARK Muster	
Zertifikate Sie können die Daten, die nicht entschlüsseln. Soll d	mit dem Zertifikat verschlüsselt wurden, as Zertifikat gelöscht werden?
Importieren Exportieren Beabsichtigte Zwecke des Zertifika	Ja Nein
	Anzeigen
	Schließen

3.5 Nutzung in Thunderbird

Dieser Abschnitt gibt Hilfestellungen bei der Verwendung der Schlüssel/Zertifikate der Volksverschlüsselung in *Thunderbird*.

3.5.1 Voraussetzungen

Für die nachfolgenden Ausführungen setzen wir voraus, dass

- 1. Sie Thunderbird auf Ihrem Rechner installiert und für Ihre E-Mail-Adresse ein Konto eingerichtet haben. Falls Sie beispielsweise ein Konto bei T-Online, GMX oder Web.de haben, so können Sie dieses auch in Thunderbird konfigurieren und verwenden. Anleitungen für das Einrichten eines E-Mail-Kontos in Thunderbird finden Sie bei Ihrem E-Mail-Anbieter.
- 2. Sie mit Hilfe der Volksverschlüsselungs-Software für die verwendete E-Mail-Adresse ein Zertifikat beantragt, heruntergeladen und Thunderbird konfiguriert haben.
- 3. Ihr Kommunikationspartner ebenfalls ein S/MIME-fähiges E-Mail-Programm und ein Zertifikat der Volksverschlüsselung oder eines anderen Anbieters von

S/MIME-Zertifikaten besitzt (vgl. Was benötigt mein Kommunikationspartner, um mit mir vertraulich kommunizieren zu können?).

3.5.2 Installation der CA-Zertifikate der Volksverschlüsselung

Um die Gültigkeit eines Zertifikats der Volksverschlüsselung prüfen zu können, muss die gesamte Zertifikatskette in Thunderbird installiert sein, d.h. das Wurzelzertifikat Volksverschlüsselung Root-CA G02 und das Zertifikat der Private CA Volksverschlüsselung Private-CA G02 müssen Thunderbird bekannt sein. Wenn Sie die Volksverschlüsselungs-Software zur Konfiguration Ihrer Anwendung verwenden, werden diese Zertifikate automatisch installiert.

Falls Sie die Volksverschlüsselungs-Software nicht verwenden wollen/können, dann müssen Sie die Zertifikate manuell importieren. Laden Sie hierzu die Zertifikate im Binärformat (DER) von der Webseite https://volksverschluesselung.de/ zertifikate.php herunter und binden Sie sie wie folgt in Thunderbird ein.

Import des Wurzelzertifikats

1. Gehen Sie auf Hamburger-Menü (drei Striche oben rechts) -> Erweitert und geben Sie Zertifikate im Suchfeld ein. Klicken Sie auf Zertifikate verwalten:

Posteingang	🔅 Einstellungen X	₩ 9 - σ × <mark>8</mark>
		✓ Zertifikat ②
Allgemein	Suchergebnisse	L. L
🖋 Verfassen	Zertifikate	
Datenschutz & Sicherheit	Wenn eine Website nach dem persönlichen Sicherheits <mark>zertifikat</mark> verlangt: Automatisch eins wählen • Jedes Mal fragen	
C hat	Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen	zertifikat Zertifikate verwalten Kryptographie-Module verwalten

2. Gehen Sie auf den Karteireiter Zertifizierungsstellen und klicken Sie auf Importieren. Suchen Sie den Pfad, in dem Sie die zuvor heruntergeladenen Zertifikate abgelegt haben, und wählen Sie die Datei VV-Root-G02-CA.cer aus.

Zertifikat-Manager			-	- 🗆	×
Ihre Zertifikate Personen Server	Zertifizierungsstellen	Andere			
Sie haben Zertifikate gespeichert	, die diese Zertifizieru	ngsstellen identifizieren:			
Zertifikatsname		Kryptographie-Modul			EŞ.
∨AC Camerfirma S.A.					^
Chambers of Commerce Ro	ot - 2008	Builtin Object Token			
Global Chambersign Root - 2	2008	Builtin Object Token			
✓AC Camerfirma SA CIF A82743	287				
Chambers of Commerce Ro	ot	Builtin Object Token			
Global Chambersign Root		Builtin Object Token			
~ACCV					
ACCVRAIZ1		Builtin Object Token			
✓ Actalis S n A /03358520967					~
<u>A</u> nsehen Vertrauen <u>b</u> earb	beiten Importier	Exportieren	Lösche <u>n</u> oder Vertraue	n entziehe	en
					ОК

3. Setzen Sie in allen Feldern ein Häkchen und klicken Sie auf OK.

Ihre Zerti	Herunterladen des Zertifikats X	ngsstellen
ie haben <mark>Ze</mark> i	Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.	
Zertifikatsna	Soll "Volksverschluesselung Root CA G02" für die folgenden Zwecke vertraut werden?	Ę
✓ GlobalSig	Dieser CA vertrauen, um Websites zu identifizieren.	^
Global:	Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.	
Global	Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien	
Global	und Prozeduren (wenn vorhanden) überprüfen.	
Global	Ansicht CA-Zertifikat überprüfen	
Global	OK Abbrechen	

Import des Zertifikats der Volksverschluesselung Private CA

1. Gehen Sie auf den Karteireiter Zertifizierungsstellen und klicken Sie auf Importieren. Suchen Sie den Pfad, unter dem Sie die zuvor heruntergeladenen Zertifikate abgelegt haben und wählen Sie die Datei VV-Private-User-G02-CA.cer aus.

Zertifikat-Manager	- 0	
hre Zertifikate Personen Server Zertifizieru	gsstellen Andere	
Sie haben Zertifikate gespeichert, die diese	ertifizierungsstellen identifizieren:	
Zertifikatsname	Kryptographie-Modul	₽₽
∽AC Camerfirma S.A.		^
Chambers of Commerce Root - 2008	Builtin Object Token	
Global Chambersign Root - 2008	Builtin Object Token	
∨AC Camerfirma SA CIF A82743287		
Chambers of Commerce Root	Builtin Object Token	
Global Chambersign Root	Builtin Object Token	
~ACCV		
ACCVRAIZ1	Builtin Object Token	
×Actalis S.n.A./03358520967		۷
Ansehen Vertrauen <u>b</u> earbeiten	Importieren Exportieren Lösche <u>n</u> oder Vertrauen entziehen.	
	ОК	(

2. Setzen Sie in keinem Feld ein Häkchen und klicken Sie auf OK.

Ihre Zerti	Herunterladen des Zertifikats X	ngsstellen
Sie haben <mark>Ze</mark> l	Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.	
Zertifikatsna	Soll "Volksverschluesselung Private CA G02" für die folgenden Zwecke vertraut werden?	E
✓ GlobalSig	Dieser CA vertrauen, um Websites zu identifizieren.	^
Global	Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.	
Global	Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien	
Global	und Prozeduren (wenn vorhanden) überprüfen.	
Global	Ansicht CA-Zertifikat überprüfen	
Clabel		

3.5.3 Austausch des Verschlüsselungszertifikats mittels signierter E-Mail

Eine Möglichkeit sein Verschlüsselungszertifikat verfügbar zu machen, besteht darin, dem Kommunikationspartner eine signierte E-Mail zu senden. Bei einer signierten E-Mail werden alle Zertifikate des Absenders mitgesendet und dem E-Mail-Programm auf Empfängerseite bekannt gemacht.

Hinweis: Im E-Mail-Programm des Empfängers der signierten Nachricht muss die Zertifikatskette der Volksverschlüsselung installiert sein, damit die Gültigkeit der Signatur überprüft werden kann. Falls der Empfänger die Volksverschlüsselungs-Software nicht verwendet, muss er die Zertifikate *Volksverschluesselung Root-CA G02* und *Volksverschluesselung Private-CA G02* manuell zu installieren, wie in Installation der CA-Zertifikate der Volksverschlüsselung beschrieben.

 Ihr Kommunikationspartner sendet eine signierte Mail an Sie, die Sie an dem S/MIME mit schwarzem Siegel erkennen. Durch das Öffnen der signierten E-Mail wird der öffentliche Schlüssel aus dem Verschlüsselungszertifikat des Senders automatisch in den Zertifikatsspeicher von Thunderbird übernommen.



2. Sie können den öffentlichen Schlüssel Ihres Kommunikationspartners sofort nutzen, um verschlüsselt mit ihm zu kommunizieren.



3.5.4 Manuelle Konfiguration des Verzeichnisdienstes der Volksverschlüsselung

Die Volksverschlüsselung bietet einen öffentlichen LDAP (Lightweight Directory Access Protocol) Verzeichnisdienst an, in dem alle Verschlüsselungszertifikate der Nutzer der Volksverschlüsselung zu finden sind, sofern sie bei der Zertifikatsbeantragung hierzu ihre Einwilligung erteilt haben.

Wenn Sie die Volksverschlüsselungs-Software nicht verwenden, aber den Verzeichnisdienst der Volksverschlüsselung installieren wollen, um Personen zu finden, denen Sie eine verschlüsselte E-Mail schicken möchten, müssen Sie ein neues Adressbuch einrichten. Hierfür benötigen Sie den Hostname, den Basis-DN und die Portnummer. Die Konfigurationsparameter des Verzeichnisdienstes der Volksverschlüsselung finden Sie auf unserer Webseite.

So richten Sie den Verzeichnisdienst der Volksverschlüsslung in Thunderbird ein:

🙀 xavier.mustermann@vv.sit.fra				1	-	×							
📩 Abrufen 🔻 🖉 Verfassen 🔻 🗭 Chae	Adressbuch	🗣 Schlagwörter 👻 🝸 Schnellfilter	Suchen <strg+k></strg+k>		م	=							
a xavier.mustermann@vv.sit.fraunhofer.de a Posteingang (2)	Thun	Thunderbird E-Mail - xavier.mustermann@vv.sit.fraunhofer.de											
Gesendet	E-M	ail											
m Papierkorb		lachrichten lesen											
a Maine Ordner	M 1	leue Nachricht verfassen											
	Kon	ten											
		onten-Einstellungen bearbeiten											
	🚗 N	leues Konto erstellen:											
	Ð	🛛 E-Mail 🛛 🖳 Chat 🖓 Newsgruppen 🗎	Feeds										
	E	inen neuen Kalender erstellen											
	Erwe	eiterte Funktionen											
	Q 1	lachrichten suchen											
	- ≪∳≫ - F	ilter erstellen											
9				2	agesplan	^							

1. Öffnen Sie in Thunderbird das Adressbuch.

2. Erstellen Sie ein neues LDAP-Verzeichnis, indem Sie auf **Datei->Neu-**>**LDAP-Verzeichnis** klicken.

🗊 Ad	Iressbuch												-	٥	×			
<u>D</u> atei	<u>B</u> earbeiten	Ansicht	Extras	Hilfe														
	<u>N</u> eu		>		Kontakt	Strg+N	assen	🛇 Löschen		Na	me oder E-Mail-Adresse				Q			
	Druckvorschau: Kontakt			Verteiler-Lis	te	K	Kontakte externer Adressbücher werden erst nach einer Suche angezeigt.											
	Kontakt dr <u>u</u> ci	ikt dr <u>u</u> cken		Adressbuch			dresse		Chatname		Organisation	Tel. dienst	lich		E			
	Seite einrichten			LDAP-Verze	ichnis	unt_020	nt_02@vv.sit.fraunhof											
				<u>N</u> achricht	Strg+M	unt_03(⊉vv.sit.fraunhof											
	Adressbuch d	ruc <u>k</u> en																
	S <u>c</u> hließen	S	trg+W															
_				_														

- 3. Tragen Sie folgende Konfigurationsdaten in die Felder ein und bestätigen Sie dann alles mit **OK**.
 - Name: Verzeichnis der Volksverschlüsselung (Name frei wählbar)
 - Serveradresse: ldap.volksverschluesselung.de
 - Basis-DN: ou=Certificates,o=Volksverschluesselung,c=de
 - Port-Nummer: 636
 - Bei Verschlüsselte Verbindung (SSL) verwenden: ein Häkchen setzen

LDAP-Verzeichnisserv	rer bearbeiten		×
Allgemein Offline	Erweitert		
<u>N</u> ame:	Verzeichnis der Volksverschlüsselung		
Server <u>a</u> dresse:	ldap.volksverschluesselung.de		
<u>B</u> asis-DN:	ertificates, o= Volksverschluesselung, c= de	<u>S</u> uchen	
<u>P</u> ort-Nummer: Bind-DN:	636		
- <u></u>			
Verschlüssel	te Verbindung (SS <u>L</u>) verwenden		
	ОК	Abbrecher	n

3.5.5 Manuelle Konfiguration des Verzeichnisdienstes einer fremden Zertifizierungsstelle

Hat Ihr Kommunikationspartner sein Zertifikat in einem Verzeichnisdienst eines anderen Zertifizierungsanbieters veröffentlich, dann bitten Sie ihn, Ihnen die Konfigurationsdaten zu nennen: Hostname, Portnummer (mit/ohne SSL/TLS) und Basis-DN. Wenn Ihnen die Konfigurationsdaten bekannt sind, können Sie den Verzeichnisdienst, wie im vorherigen Abschnitt beschrieben, in Thunderbird einrichten.

3.5.6 Senden einer verschlüsselten E-Mail

Im Folgenden wird eine Möglichkeit beschrieben, wie Sie in Thunderbird eine verschlüsselte E-Mail für Ihren Kommunikationspartner erzeugen können.

In diesem Beispiel wird vorausgesetzt, dass Ihr Kommunikationspartner ebenfalls ein Zertifikat der Volksverschlüsselung besitzt und sein Zertifikat im Verzeichnis veröffentlicht hat.

Für die Kommunikation mit einem Kommunikationspartner, dessen Zertifikat Sie noch nicht kennen, müssen Sie zuerst sein Zertifikat in Ihrem E-Mail-Programm verfügbar machen, wie in den vorhergehenden Abschnitten beschrieben wurde.

In dem Ordner, in dem Ihre gesendeten E-Mails abgespeichert werden, können Sie eine verschlüsselte Nachricht an dem "Schloss-Symbol" erkennen. Jede verschlüsselte E-Mail wird auch mit Ihrem **Verschlüsselungszertifikat** verschlüsselt und in diesem Ordner abgelegt.

1. Öffnen Sie das Adressbuch.

🙀 xavier.mustermann@vv.sit.fra		
🛃 Abrufen 🔻 📝 Verfassen 🔻 🗭 Cha: 👤 A	ressbuch Schlagwörter - TSchnellfilter Suchen <strg+k></strg+k>	۹ =
a xavier.mustermann@vv.sit.fraunhofer.de a Posteingang (2)	Thunderbird E-Mail - xavier.mustermann@vv.sit.fraunhofer.de	e
Entwürfe	E-Mail	
Papierkorb	Rachrichten lesen	
A M Lokale Ordner	Veue Nachricht verfassen	
a Postausgang	Konten	
	Konten-Einstellungen bearbeiten	
	Neues Konto erstellen: Chat O Neurographia D Foods	
	Einen neuen Kalender erstellen	
	Envitante Evalutionen	
	Nachrichten suchen	
	🐳 Filter erstellen	
種		🐯 Tagesplan 🔺

- 2. Suchen Sie die E-Mail-Adresse Ihres Kommunikationspartners:
 - Gehen Sie unter Alle Adressbücher auf das Verzeichnis der Volksverschlüsselung.
 - Geben Sie in der Suche die vollständige E-Mail-Adresse ein.
 - Klicken Sie auf die E-Mail-Adresse und dann im Fenster *Kontakte* erneut auf die E-Mail-Adresse, um eine E-Mail zu schreiben.

Adressbuch					- 0	×
Datei Bearbeiten Ansicht Extras Hilfe						
& Neuer Kontakt & Neue Liste 🖨 Bear	peiten 🖋 Verfasse	en 🗎 🛍 Kontakt löschen			unhofer.de	⊗
→ 🖪 Alle Adressbücher	Name	 E-Mail-Adresse 	Chatnam	e Organisation	Tel. dienstlich	E.
Persönliches Adressbuch	A xavier.muste	er xavier.muster@vv.sit.f				
Gesammelte Adressen						
	xavier.must	er				
		ontakt <u>E-Mail-Adresse:</u> <u>xavier.muster@vv.sit.frau</u>	<u>nhofer.de</u>]		

- 3. Geben Sie Ihre Nachricht ein und verschlüsseln Sie diese wie folgt:
 - Gehen Sie auf **Sicherheit**.
 - Wählen Sie die Option **Nur mit Verschlüsselung senden** aus und senden Sie Ihre E-Mail.

🖋 Verfassen: meine Zertifikate - Thunderbird	- 🗆 X
Datei Bearbeiten Ansicht Einfügen Format Optionen Extras Hilfe	
📣 Senden 🛛 🔥 Rechtschr. 👻 🚨 Sicherheit 💌 🖬 Speichern 💌	🖉 Anhängen 🗸
Verschlüsselungs- <u>T</u> echnologie	
<u>v</u> on Erika M <u>N</u> icht verschlüsseln	a.muster@vv.sit.jraannojer.ae V Kopie (CC) Biinakopie (BCC)
An xavier.n Vur mit Verschlüsselung senden	
Nachricht unterschreiben	
Betreff meine Z Sicherheitsinformationen anzeigen	
Absatz Variable Breite V T T- T- B	Ґ⊻∣&│≔ः⊈ःॡः हः ∣≣▾⊠▾☺ݖ
Hallo Xavier.	
,	
diese Nachricht ist verschlüsselt.	
VG	
vo	
Erika Muster	

Hinweis: Nach einer einmaligen erfolgreichen vertraulichen Kommunikation können Sie die E-Mail-Adresse Ihres Kommunikationspartner direkt aus einer E-Mail oder aus Ihrer Kontaktliste entnehmen. Seine Zertifikate sind dann schon dem Thunderbird bekannt.

3.5.7 Empfang einer verschlüsselten E-Mail

Wenn Sie eine verschlüsselte E-Mail empfangen, können Sie diese sofort lesen, wenn Sie Ihren privaten Schlüssel in Thunderbird beispielsweise mit Hilfe der Volksverschlüsselungs-Software konfiguriert haben. Das **Schloss-Symbol** zeigt an, dass die E-Mail vom Absender verschlüsselt wurde.

3 Nutzung der Schlüssel/Zertifikate in S/MIME-fähigen E-Mail-Programmen

Posteingang										Ē	¥1		- 0	×
🖵 Abrufen 🗸 🖋 Verfassen 🛛	↓ Chat		Adressbuch	Schlagwörter	✓ ♥ Schne	ellfilter	ſ	₽ Suchen <strg< th=""><th>+K></th><th>_</th><th>-</th><th></th><th></th><th>≡</th></strg<>	+K>	_	-			≡
Ordner •••	农	۵	Ungelesen	🟠 Gekennzeichnet	Kontakt	Sch	lagwörter	🛛 Anhang	₽ Die	se Nachrichten d	urchsu	chen ·	<strg+ums< th=""><th>chalt+K></th></strg+ums<>	chalt+K>
 avier.musteaunhofer.de Posteingung Posteingung Entwärde Entwärde Junk-E-Mail Colale Ordner Postausgang 		0	Betreff Volksve Volksve Signiert Eine ver Signiert meine Z	rschlüsselung: Zertifik rschlüsselung: Testna e Nachricht trauliche Nachricht e Nachricht e Nachricht lertifikate	at wurde aus <u>c</u> chricht [versch	jestellt lüsselt]	000 0 0 0 0 0	Beteiligte noreply@test. erika.muster@ erika.muster@ erika.muster@ Erika Muster	volksvers volksvers vv.sit.fra vv.sit.fra	chluesselung.de chluesselung.de unhofer.de unhofer.de unhofer.de	 ・ ・	Datum 9.05.2 9.05.2 9.05.2 3.05.2 3.05.2 1:06	022, 10:33 022, 10:34 022, 11:39 022, 15:52 022, 16:18	~ 10
	Vor Betref Ar Hall dies VG Erik	n Erik f me i n Mic o Xa e Na a Mu	a Muster <e ine Zertifik h û avier, achricht uster</e 	rikamuster@vv.sit.fra ate ist verschlüss	uunhofer.de> 1	\$	∮ Ant	worten 🥻 🏕 Weit	erleiten	Archivieren	ەر ھ	nk	کر Löschen	Mehr V 11:06 MIME

3.5.8 Senden einer signierten E-Mail

Für das Signieren Ihrer E-Mail wird Ihr gültiges Signaturzertifikat verwendet. Wenn Sie Thunderbird mit Hilfe der Volksverschlüsselungs-Software konfiguriert haben, ist dieses bereits installiert.

In dem Ordner, in dem Ihre gesendeten E-Mails abgespeichert werden, können Sie eine signierte Nachricht an dem S/MIME mit einem schwarzen Siegel erkennen.

Wenn Sie Ihre E-Mail verfasst haben, gehen Sie auf **Sicherheit**, wählen die Option **Nachricht unterschreiben** aus und senden dann ihre E-Mail.

🖋 Verfassen: signi	🖍 Verfassen: signierte Nachricht - Thunderbird													-		\times						
<u>D</u> atei <u>B</u> earbeiten	<u>A</u> nsic	:ht <u>E</u> infüg	gen	<u>F</u> ormat <u>O</u>	ptione	n E <u>x</u>	tras <u>I</u>	<u>H</u> ilfe														
📣 Senden 🛛 🔥 F	Rechts	chr. 🗸	🔒 S	icherheit 🔹	- 🖬	Speid	hern	~												0	Anhäng	en 🗸 🗸
	<u>V</u> on An	Erika M xavier.n	~	Verschlüsse <u>N</u> icht verso Nur mit <u>V</u> e	/erschlüsselungs- <u>T</u> echnologie > 4							vv.sit.f	frauni	hofer.d	e 🗸	•	Кор	ie (CC)) Bl	lindkoj	oie (BCC)	»
Be	Bet <u>r</u> eff signierte		~	Nachricht	intersc inform	hreib atione	en en anze	eigen														
Absatz 🗸	Vari	iable Breite	e	~	-	، ⊤ ٦	r, T	B	I	U	₽⊗	ŧ≡	12 —	₹≡ ₹	3 3	≣~		⊙•				
Hallo Xavier,	at will	rde sign	iert																			
		rue sign	iere.																			
VG																						
Erika Muster																						

3.5.9 Empfang einer signierten E-Mail

Eine signierte E-Mail erkennen Sie an dem **S/MIME mit einem schwarzen Siegel**. Wenn Sie eine signierte E-Mail empfangen, prüft Thunderbird automatisch die Gültigkeit der Signatur.

Wenn Sie auf das Signatur-Symbol klicken, erhalten Sie Informationen zum Signaturzertifikat des Senders.

Posteingang	🖸 Eine vertrauliche Nachricht - 🗙	8	- 0	×
🛛 🖓 Abrufen 🗸 🖋 Verfassen 🛛	Chat Adressbuch Schlagwörter ➤ Schnellfilter O Suchen <strg+k></strg+k>			Ξ
Ordner •••	🛠 🛛 Ungelesen 🏠 Gekennzeichnet 🖪 Kontakt 🗞 Schlagwörter 🕅 Anhang 🔎 Diese Nachrichter	durchsu	chen <strg+um< th=""><th>schalt+K></th></strg+um<>	schalt+K>
Caverage and the second s	• • Betreff • • Volksverschlüsselung: Zertifikat wurde ausgestellt • norep/y@test.volksverschlüsselung: • Volksverschlüsselung: Testmachricht (verschlüsselt] • norep/y@test.volksverschlüsselung: • > Signierte Nachricht • erika.muste@vvsit.fraunhofer.de • > Signierte Nachricht • erika.muste@vvsit.fraunhofer.de • > meine Zertifikate • Erika Muster	● C de ∂ 1 de ∂ 1 2 2 ∂ 2 ∂ 2 ∂ 1	Datum 9.05.2022, 10:33 9.05.2022, 10:34 9.05.2022, 11:39 3.05.2022, 15:52 3.05.2022, 16:18 6.05.2022, 11:06 5:56	A 6
	Von Erika Muster <erika.muster@vvsit.fraunhofer.de>☆ Antworten → Weiterleiten @ Archiviere Betreff signierte Nachricht An Mich☆ Hallo Xavier, diese Nachricht wurde signiert. VG Erika Muster</erika.muster@vvsit.fraunhofer.de>	n 🕑 Jun	nk 🗍 Löschen	Mehr V 15:56

Wurde die Signatur auf dem Transportweg manipuliert oder ist das Zertifikat des Senders gesperrt, wird es anhand eines **Siegel mit einem roten Warndreieck** sichtbar:

Posteingang	🖸 Eine vertrauliche Nachricht - 🗙 🛗 🖻 — 🗆 🗙
🖵 Abrufen 🔽 🖋 Verfassen 🛛	Chat 🖪 Adressbuch 🛇 Schlagwörter 🗸 🍞 Schnellfilter 🔎 Suchen <strg+k> 🗧</strg+k>
Ordner •••	★ □ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ <
 ✓ Savier.musteaunhofer.de ✓ Posteingang □ Papierkorb □ Entwürfe □ Gesendet □ Junk-E-Mail ✓ Gesendet ✓ Iokale Ordner □ Papierkorb ※ Postausgang 	 ★ ● Betreff ● Betreff ● Datum ▲ E ★ Signierte Nachricht ● erika.muster@vv.sit ● 19.05.2022, 1 ★ Eine vertrauliche Nachricht ● erika.muster@vv.sit ● 23.05.2022, 1 ★ \$ signierte Nachricht ● Erika Muster ● 27.05.2022, 1 ★ Yon Erika Muster <erika.muster@vv.sit.fraunhofer.de> ★ > → ○ ● ● ●</erika.muster@vv.sit.fraunhofer.de> ♥ → ○ ● ● ● ♥ → ○ ● ● ♥ → ○ ●
((•))	Ungelesen: 0 Gesamt: 5

3.5.10 Senden einer signierten und verschlüsselten E-Mail

Wenn Sie eine signierte und verschlüsselte E-Mail versenden möchten, gehen Sie vor, wie in den vorherigen Abschnitten beschrieben. In diesem Fall müssen vor dem Versand der Nachricht die Optionen **Nur mit Verschlüsselung senden** und **Nachricht unterschreiben** ausgewählt werden.

🖋 Verfassen: signierte und versch	lüsselte Nachricht - Thunderbird		- 🗆	×
Datei Bearbeiten Ansicht Einf	ügen <u>F</u> ormat <u>O</u> ptionen E <u>x</u> tras <u>H</u> ilfe			
🛦 Senden 🔥 Rechtschr. 🗸	🔒 Sicherheit 💌 🗈 Speichern 🗸		🛛 Anhänge	en 🗸
N 51 N	Verschlüsselungs- <u>T</u> echnologie			
Von Erika iv	<u>N</u> icht verschlüsseln	a.muster@vv.sit.jraunnojer.ae 🗸 Kopie (CC)	Blindkopie (BCC)	"
An xavier.r	 Nur mit Verschlüsselung senden 			
	✓ Nachricht unterschreiben			
Betreff signiert	Sicherheitsinformationen anzeigen	·		
Absatz 🗸 Variable Bre	ite 🗸 🗖 नी T+ TA B 1	ݱ⊻∣⊗∣≔指理理≣ヾ⊠ヾ☺ヾ		
Hallo Xavier,				
diese Nachricht wurde sig	niert und verschlüsselt.			
VG				
Erika				

3.5.11 Kontrolle der installierten Zertifikate in Einstellungen

In Thunderbird können Sie sich unter **Einstellungen** alle Details zu den installierten Zertifikaten ansehen.

1. Gehen Sie im Anwendungsmenü zu Einstellungen.



2. Geben Sie im Suchfeld links oben "Zertifikate" ein und klicken Sie auf "Zertifikate verwalten" im rechten Fenster.

						۶z	ertifikat	(0]	
🌣 All	gemein	Suchergebnisse									
🖋 Ver	rfassen	<mark>Zertifikat</mark> e									
A Da Sic	itenschutz & :herheit	Wenn eine Website nac	h dem persönlichen wählen O J <u>e</u> des	Sicherheits <mark>zertifika</mark> Mal fragen	<mark>it</mark> verlangt:						
Ch	at	Aktuelle <u>G</u> ültigkeit v bestätigen lassen	on <mark>Zertifikat</mark> en durc	h Anfrage bei OCSF	P-Server	Z <u>K</u> ryptog	zertifikat ertifikat <mark>e verw</mark> graphie-Modul	alten e verwalten.			

3. Wählen Sie den Karteireiter **Ihre Zertifikate**. Suchen Sie nach Ihren drei Volksverschlüsselungs-Zertifikaten. Sie finden Ihre Zertifikate der Volksverschlüsselung unter **Fraunhofer SIT**

	<mark>Zert</mark> ifikatverw	valtung	
Ihre Zertifikate	Authentifizierungs-Entscheidungen Person	en Server Zertifizierur	ngsstellen
ie haben <mark>Zert</mark> ifikate dies	er Organisationen, die Sie identifizieren:		
Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis
✓ Fraunhofer SIT			
Erika Muster	das Software-Sicherheitsmodul	41:FA:A7:88:2E:B0:BE:33	Samstag, 17. Mai 2025
Erika Muster	das Software-Sicherheitsmodul	0C:CA:93:F9:46:14:4B:54	Samstag, 17. Mai 2025
Erika Muster	das Software-Sicherheitsmodul	47:D6:DE:38:C0:48:3B:6F	Samstag, 17. Mai 2025
<u>A</u> nsehen <u>S</u> icherr	<u>Alle sichern</u> <u>Importieren</u> Lösch	hen	
			ок

4. Um überprüfen zu können, ob das Zertifikat erfolgreich installiert und verifiziert wurde, klicken Sie auf ein Zertifikat und auf Button "Ansehen". In den Feldern *Schlüsselverwendung* und *Erweiterte Schlüsselverwendung* sehen Sie, ob es sich um das Verschlüsselungs-, Signatur- oder Authentifizierungszertifikat handelt.

ndet	🔅 Einstellungen 🛛 🗙 🖪	Zertifikat für Erika Muster 🛛 🗙	ė	-	σ	×
	Schlüsselverwendung Verwendungen	Digital Signature, Non-Repudiation				
	Erweitere Schlüsselverwendung Verwendungen	E-mail Protection				
	ID für verwendeten Schlüssel des Zertifikatinhabers (Subject Key ID) Schlüssel-ID	72:E3:E60A:75:FD:419D:85:34:864A:89:F9:F7:39:78:2E:3C:C2				
	ID für verwendeten Schlüssel der Zertifizierungsstelle (Authority Key ID)					
	Schlüssel-ID	F6:A0:01:C1:74:01:82:F1:6C:F3:2A:A6:D3:A7:B1:A4:45:A2:B2:D1				

🖈 Gese

Wenn Sie die Zertifikate der Volksverschluesselung Root-CA G02 und Volksverschluesselung Private-CA G02 kontrollieren möchten, gehen Sie zum Karteireiter Zertifizierungsstellen.

		Zei	r <mark>t</mark> ifikatverwaltur	g		
Ihre Zertifikate	Authentifizierungs	-Entscheidungen	Personen	Server	Zertifizierungsstellen	
e haben <mark>Zert</mark> ifikate	gespeichert, die diese	<mark>Zert</mark> ifizierungsstelle	n identifizieren:			
Zertifikatsname			Kryptogr	aphie-Modul		E
AC RAIZ FNMT-RCM		Builtin Obj	ect Token		^	
AC RAIZ FNMT	-RCM SERVIDORES SE	GUROS	Builtin Obj	ect Token		
 Fraunhofer SIT 						
Volksverschlue	sselung Root CA G02_	TEST	das Softwa	re-Sicherheit	smodul	
Volksverschlue	sselung Private CA G0	2 TEST	das Softwa	re-Sicherheit	smodul	
 GlobalSign 						
GlobalSign Roo	ot CA - R2		Builtin Obj	ect Token		~
Ansehen Ver	trauen <u>b</u> earbeiten	Importieren	Exportieren	Lösche <u>n</u> od	der Vertrauen entziehen	
						ОК

3.5.12 Nutzung mehrerer E-Mail-Konten

In Thunderbird können Sie mehrere E-Mail-Konten einrichten und für jede E-Mail-Adresse ein eigenes Zertifikat besitzen. Die verschlüsselte Kommunikation zwischen zwei installierten E-Mail-Konten findet genauso statt, wie die Kommunikation mit einem externen Kommunikationspartner, d.h. die Zertifikate müssen ggf. noch ausgetauscht werden (vgl. Wie bekomme ich das Verschlüsselungszertifikat des Empfängers?).

Wenn Sie für mehrere E-Mail-Konten in Thunderbird jeweils ein Zertifikat von der Volksverschlüsselung verwenden und diese mit Hilfe der Volksverschlüsselungs-Software in Thunderbird installieren, können Sie sofort die E-Mail-Konten in Thunderbird für eine vertrauliche und sichere Kommunikation verwenden. Falls Sie für eine E-Mail-Adresse ein Zertifikat von einer anderen Zertifizierungsstelle verwenden möchten, müssen Sie dieses manuell in Thunderbird einrichten.

Jedes E-Mail-Konto wird mit dem eigenen persönlichen Zertifikat konfiguriert. Sie können es wie folgt kontrollieren:

1. Klicken Sie mit der rechten Maustaste auf das entsprechende E-Mail-Konto und klicken Sie auf **Einstellungen**.

😭 erika.muster@vv.sit.f	fraunhofer.d 🖪 Konten-Einstellungen	×	Ŵ	2	-	٥	×
🖵 Abrufen 🖌 🖋 Ver	rfassen 📮 Chat 🖪 Adressbuch 🛇	Schlagwörter 👻 🎖 Schnellfilter 🖉 Suchen <strg+k></strg+k>					Ξ
Ordner ∲ C⊉ erika.muster⊗vv	erika.mu	ter@vv.sit.fraunhofer.de		🔅 Kor	ntoeinste	llungen	î
 ✓ IPosteingang Entwürfe ✓ Gesendet IPapierkorb ✓ Entwürfe 	Nagninchen abruten In neuem Tab öffnen In neuem Fenster öffnen Nachrichten guchen Abonnieren	sen 🖋 Neue Nachricht verfassen 🔍 Nachrichten suchen 🗑 Filter für Nachrichten verwalten 🗝 Ende	-zu-Ende-W	erschlüsse	elung		
 Junk-E-Mail Yavier.muster@v Posteingang 	Neuer Ordner Alle Ordner als gelesen markieren	> hinzufügen					
✓ □ Lokale Ordner □ Papierkorb ② Postausgang	Einstellungen	🕼 Kalender 🚺 Adressbuch 🖓 Chat 🍫 Fileink		Fee	d		
	Aus anderen	Programm importieren et den import von E-Mall-Nachrichten, Adressbuchenträgen, Feed Abonnements					

2. Gehen Sie zum Menüpunkt **Ende-zu-Ende-Verschlüsselung** und kontrollieren im rechten Fenster, welche Zertifikate für das Konto konfiguriert sind.

ika.muster@vv.sit.fraunhofer.c 🕥 Konten-Einstellunge	×		ė	8	-	٥	
r ⊡erika.muster@vv.sit.fraunhofer.de ^ Server-Einstellungen	Thunderbird verfügt über keinen persönlichen OpenPGP-Schlüssel für erika.muster@vv.sit.fraunhofer.de.	A Schlüssel	hinzufügen				
Kopien & Ordner Verfassen & Adressieren Junk-Filter	Mit der OpenPGP-Schlüsselverwaltung können Sie die Schlüssel Ihrer Kontakte un aufgeführte Schlüssel anzeigen und verwalten.	nd andere oben r	nicht				
Synchronisation & Speicherplatz Ende-zu-Ende-Verschlüsselung	OpenPGP-Schlüssel verwalten						
Emprangsbestattgungen (MDN)	S/MIME Persönliches Zertifikat für digitale Unterschrift: Erika Muster (IOC:CA:93:F9:46:14:48:54)	Auswählen	Leeren				
Kopien & Ordner Verfassen & Adressieren Junk-Filter	Persönliches Zertifikat für Verschlüsselung: Erika Muster [41:FA:A7:88:2E:80:8E:33]	Aus <u>w</u> ählen	Leeren				
Synchronisation & Speicherplatz	S/ <u>M</u> IME-Zertifikate verwalten S/MIME-Kryptographie-Module verwalten						
Konten-Aktionen V	Senden von Nachrichten - Standardeinstellungen Ohne Ende-zu-Ende-Verschlüsselung ist der Inhalt Ihrer Nachrichten für Ihren E-M und kann auch Bestandteil einer Massenüberwachung werden.	/lail-Anbieter leic	ht zugänglich				
Add-ons und Themes	 Verschlüsselung standardmäßig nicht aktivieren Verschlüsselung standardmäßig verlangen 						

3.5.13 Nutzung eines gesperrten Zertifikats

Sie können jederzeit Ihr Zertifikat vor Ablauf der Gültigkeit mit Hilfe der Volksverschlüsselungs-Software sperren lassen, beispielsweise wenn es fehlerhaft ist oder kompromittiert wurde. Hierbei ist zu beachten, dass immer alle drei Zertifikate gesperrt werden.

Erstellen Sie immer auch eine Sicherungskopie von Ihren gesperrten Zertifikaten und entfernen Sie diese nicht aus dem Zertifikatsspeicher von Thunderbird, da Sie ansonsten alte Nachrichten nicht mehr entschlüsseln können. Sollten gesperrte Zertifikate nicht mehr im Zertifikatsspeicher vorliegen, können Sie diese mit Hilfe der Sicherungskopie und der Volksverschlüsselungs-Software wieder installieren.

Sie können keine *signierte* oder *verschlüsselte* Nachrichten mit einem gesperrten Zertifikat weiter versenden. Ihre Kommunikationspartner können Ihnen keine *verschlüsselten* Nachrichten mehr senden, da Ihr Zertifikat nicht mehr gültig ist. Beim Versenden erscheint folgende Fehlermeldung:

Verfassen: Verschlüssel Datei Bearbeiten Ansich	n nach Sperrung - Thunderbird 11 Finfügen Format Ontionen Extras Hilfe	- 🗆	×
A Senden	hr. Y 🚔 Sicherheit Y 📑 Speichern Y	🛛 Anhänger	~
<u>V</u> on	Erika Muster <erika.muster@vv.sit.fraunhofer.de> erika.muster@vv.sit.fraunhofer.de 💙 🛛 Kopie (CC)</erika.muster@vv.sit.fraunhofer.de>	Blindkopie (BCC)	»
An	xavier.muster@vv.sit.fraunhofer.de		
Betreff	Verschlüsseln nach Sperrung		
Normaler Text 🗸 🛛 Varia	שלא שלים שלים שלים שלים שלים שלים שלים שלים		
Hallo, diese Nachricht wird Mein Zertifikat wurd VG Erika	I nicht vers Senden der Nachricht ist fehlgeschlagen Senden der Nachricht fehlgeschlagen. Sie haben ausgewählt, diese Nachricht zu verschlüsseln, aber die Anwendung konnt Verschlüsselungszerlicht acht icht nicht finden, das Sie in Ihren Konten-Einstellungen angege oder das Zertifikat ist abgelaufen.	× e das ben haben, OK	
Nachricht wird erstellt		S/MIME	-

3.5.14 Zertifikate entfernen

Wenn Ihre Schlüssel/Zertifikate aus dem Zertifikatsspeicher von Thunderbird entfernt sind, können Sie für Sie verschlüsselte Nachrichten nicht mehr lesen. Sie können aber nachträglich die Schlüssel/Zertifikate mit der Volksverschlüsselungs-Software beispielsweise aus der Sicherungskopie wieder installieren.

Wenn Sie in Thunderbird Ihre Schlüssel/Zertifikate aus Ihrem E-Mail-Konto und aus dem Zertifikatsspeicher entfernen wollen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das E-Mail-Konto und klicken Sie auf **Einstellungen**.

😭 erika.muster@vv.sit.fra	aunhofer.c 🔲 Konten-Einstellungen	×				ė	2	-	٥	×
🖵 Abrufen 🖌 🖋 Verfa	assen 🖵 Chat 🖪 Adressbuch 🕔	Schlagwörter 👻 🍟 Schnellfilter		₽ Suchen <strg+k></strg+k>						Ξ
Ordner C die erika.muster@vr 4 C erika.muster@vr 4 C traktingsong E trakufe G forsudef D pajekobb E trakufe D taktefogang to savier.muster@vr to taktefogang Postanogang Postanogang	Reproduced and the second and t	uster@vvsit.fraunhofer.de em Pieur Nochride verfasem hinzufügen iir Kalender noppe	Q Nachrichten suchen	Filter für Nachric	hten verwalten 🔹 🕫 Ende-zu	-Ende-V	☆ Ko /erschilüss	ntoeinste selung	llungen	
	Aus andere	n Programm importieren								
	Thunderbird b	ietet den Import von E-Mail-Nachrichten, Ad	ressbucheinträgen, Feed-Ab	onnements						

2. Gehen Sie zum Menüpunkt **Ende-zu-Ende-Verschlüsselung** und klicken Sie im rechten Fenster auf **Leeren**, sowohl für die *Digitale Unterschrift* als auch für die *Verschlüsselung*.

ka.muster@vv.sit.fraunhofer.c	n X	E	a -	٥
Server-Einstellungen	Thunderbird verfügt über keinen persönlichen OpenPGP-Schlüssel für erika.muster@vv.sit.fraunhofer.de.	A Schlüssel hinzufügen		
Kopien & Ordner				
Verfassen & Adressieren	Mit der OpenPGP-Schlüsselverwaltung können Sie die Schlüssel Ihrer Kontakte	und andere oben nicht		
Junk-Filter	aufgeführte Schlüssel anzeigen und verwalten.			
Synchronisation & Speicherplatz	OpenPGP-Schlüssel verwalten			
Ende-zu-Ende-Verschlüsselung				
Empfangsbestätigungen (MDN)	S/MIME			
⊠xavier.muster@vv.sit.fraunhofer.de	Persönliches Zertifikat für digitale Unterschrift:		_	
Server-Einstellungen	Erika Muster [0C:CA:93:F9:46:14:4B:54]	Auswählen Leeren	1	
Kopien & Ordner	Den Vellah en Zentificat (De Venach/Zenacher en		1	
Verfassen & Adressieren	Personiicnes Zertinikat für Verschlusselung:		1	
Junk-Filter	Erika Muster [41:FA:A7:88:2E:B0:BE:33]	Auswählen Leeren		
Synchronisation & Speicherplatz	S/MIME-Zertifikate verwalten S/MIME-Kryptographie-Module verwalten			
Enda.711.Enda.Varechlüccalung				
Konten-Aktionen 🗸				
	Senden von Nachrichten - Standardeinstellungen			
Thunderbird - Einstellungen	Ohne Ende-zu-Ende-Verschlüsselung ist der Inhalt Ihrer Nachrichten für Ihren E	-Mail-Anbieter leicht zugänglich		
	und kann auch Bestandteil einer Massenüberwachung werden.			
Add-ons und Themes	Verschlüsselung standardmäßig nicht aktivieren			
	 Verschlüsselung standardmäßig verlangen 			

3. Klicken Sie auf Zertifikate verwalten.

😭 erika.muster@vv.sit.fraunhofer.c 🔳 Konten-Einstellunge	×		ŵ	2	-	٥	×
✓ ♡ <u>erika.muster@vv.sit.fraunhofer.de</u> ^ Server-Einstellungen	Thunderbird verfügt über keinen persönlichen OpenPGP-Schlüssel für erka.muster@vv.sit.fraunhofer.de.	A Schlüssel	hinzufügen				,
Kopien & Ordner Verfassen & Adressieren Junk-Filter Synchronisation & Speicherplatz	Mit der OpenPGP-Schlüsselverwaltung können Sie die Schlüssel ihrer Kontakte aufgeführte Schlüssel anzeigen und verwalten.	und andere oben r	nicht				
Ende-zu-Ende-Verschlüsselung Empfangsbestätigungen (MDN) ~ 🖸 xavier.muster@vv.sit.fraunhofer.de	S/MIME Persönliches Zertifikat für digitale Unterschrift:						
Server-Einstellungen Kopien & Ordner	Erika Muster [OC:CA:93:F9:46:14:48:54] Percönliches Zertifiket für Verschlüsselung:	Auswählen	Leeren				
Verfassen & Adressieren Junk-Filter	Erika Muster [41:FA:A7:88:2E:B0:BE:33]	Aus <u>w</u> ählen	Leeren				1
Synchronisation & Speicherplatz	S/MIME-Zertifikate verwalten S/MIME-Kryptographie-Module verwalten						
Thunderbird - Einstellungen	Senden von Nachrichten - Standardeinstellungen Ohne Ende-zu-Ende-Verschlüsselung ist der Inhalt Ihrer Nachrichten für Ihren E- und kann auch Bestandteil einer Massenüberwachung werden. O Verschlüsselung standardmäßig nicht aktivieren O Verschlüsselung standardmäßig nicht aktivieren	-Mail-Anbieter leic	cht zugänglich				
Nachrichten f ür xavier.muster@vv.sit.fraunhofer.de@mail.v	sitfraunhofer.de: Verbinden mit mail.vv.sit.fraunhofer.de						

4. Wählen Sie den Karteireiter Ihre Zertifikate.

	<mark>Zert</mark> ifikatverv	waltung		
Ihre Zertifikate Aut	hentifizierungs-Entscheidungen Persor	nen Server Zertifizierur	ngsstellen	
iie haben <mark>Zert</mark> ifikate dieser C	Organisationen, die Sie identifizieren:			
Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis	EQ.
✓ Fraunhofer SIT				
Erika Muster	das Software-Sicherheitsmodul	41:FA:A7:88:2E:B0:BE:33	Samstag, 17. Mai 2025	
Erika Muster	das Software-Sicherheitsmodul	0C:CA:93:F9:46:14:4B:54	Samstag, 17. Mai 2025	
Erika Muster	das Software-Sicherheitsmodul	47:D6:DE:38:C0:48:3B:6F	Samstag, 17. Mai 2025	
<u>A</u> nsehen <u>S</u> ichern	Alle sichern Importieren	chen		
				OK
				OK

5. Suchen Sie nach Ihren drei Volksverschlüsselungs-Zertifikaten, markieren Sie diese und klicken Sie auf Löschen.

	Zertifikatverwaltu	ng		×
Ihre Zertifikate	Authentifizierungs-Entscheidungen	Personen Server	Zertifizierungsstellen	
ie haben Zertifikate c	lieser Organisationen, die Sie identifizierer	ו:		
Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis	E\$
✓ Fraunhofer SIT				
Erika Muster	das Software-Sicherheitsmodul	41:FA:A7:88:2E:B0:BE:33	Samstag, 17. Mai 2025	
Erika Muster	das Software-Sicherheitsmodul	0C:CA:93:F9:46:14:4B:54	Samstag, 17. Mai 2025	
Erika Muster	das Software-Sicherheitsmodul	47:D6:DE:38:C0:48:3B:6F	Samstag, 17. Mai 2025	
<u>A</u> nsehen <u>S</u> ich	nern <u>A</u> lle sichern <u>I</u> mportieren.	<u>L</u> öschen		

Wenn keiner Ihrer Kommunikationspartner ein Zertifikat der Volksverschlüsselung besitzt, können Sie auch die Zertifikate der Volksverschluesselung Root-CA G02 und Volksverschluesselung Private-CA G02 löschen.

1. Gehen Sie zum Karteireiter Zertifizierungsstellen. Suchen Sie nach den Zertifikaten der Volksverschluesselung Root-CA G02 und Volksverschluesselung Private-CA G02, markieren Sie diese und klicken Sie auf Löschen oder Vertrauen entziehen.

		Zertif	ikatverwa	ltung			×
Ihre Zertifik	ate Authentifizie	rungs-Entscheid	lungen	Personen	Server	Zertifizierungsstellen	
Sie haben Zerti	fikate gespeichert, die o	diese Zertifizieru	ingsstell	en identifizieren:			
Zertifikatsnan	ne		Kryp	otographie-Modul			E.
AC RAIZ	FNMT-RCM		Builtin Object Token				^
AC RAIZ FNMT-RCM SERVIDORES SEGUROS			Builti	n Object Token			
✓ Fraunhofer	SIT						
Volksver	Volksverschluesselung Root CA G02_TEST das Software-Sicherheitsmodul						
Volksver	schluesselung Private C	A G02 TEST	das S	oftware-Sicherheit	smodul		
✓ GlobalSign							~
<u>A</u> nsehen	Vertrauen <u>b</u> earbeite	n Importie	eren	Exportieren	Lösche <u>n</u> o	der Vertrauen entziehen	
						O	K

2. Bestätigen Sie die Meldung CA-Zertifikat löschen oder Vertrauen entziehen mit OK.

_	-	
Ihre Ze	CA-Zertifikate löschen oder Vertrauen entziehen	< gsstellen
e haben Z	Sie haben um ein Löschen dieser CA-Zertifikate angefragt. Für eingebaute Zertifikate wird alles Vertrauen entzogen, was den gleichen Effekt hat. Sollen diese CA-Zertifikate wirklich gelöscht oder ihr Vertrauen entzogen werden?	
Zertifikats	Volksverschluesselung Root CA G02 TEST	E
AC R	Volksverschluesselung Private CA G02 TEST	^
AC R		
Y Fraunho		
Volks		
Volk		
VOIK:	Wenn Sie ein Zertifizierungsstellen(CA)-Zertifikat löschen oder sein Vertrauen entziehen, vertraut die Anwendung keinen Zertifikaten mehr, die von dieser CA ausgestellt wurden	
✓ GlobalS		~
Ansehen	OK Abbrechen	utziehen
<u></u>		criticite for the second

4 Nutzung der Schlüssel/Zertifikate in Browsern

Die Volksverschlüsselungs-Software importiert alle drei Zertifikate der Volksverschlüsselung sowie das Zertifikat der *Volksverschluesselung Root-CA G02* und der *Volksverschluesselung Private-CA G02* in den Zertifikatsspeicher, der von dem jeweiligen Browser verwendet wird. Die Zertifikate stehen somit allen Anwendungen zur Verfügung, die diesen Zertifikatsspeicher nutzen.

Das Authentifizierungs-Zertifikat der Volksverschlüsselung kann für die Anmeldung an Diensten bzw. Web-Portalen verwendet werden, die eine SSL/TLS-Client-Authentifizierung verlangen.

Der folgende Link ermöglicht Ihnen, die erfolgreiche Einrichtung Ihres Browser und die Authentifizierung mittels Ihrem Authentifizierungs-Zertifikat zu testen:

https://volksverschluesselung.de/portal/

Konnte die Authentifizierung erfolgreich durchgeführt werden, wird Ihnen folgende Seite angezeigt:



5 Nutzung der Schlüssel/Zertifikate auf anderen Rechnern

5.1 Export der Schlüssel/Zertifikate aus der Volksverschlüsselungs-Software

Um die Zertifikate auf anderen Rechnern nutzen zu können, müssen sie zunächst aus der Volksverschlüsselungs-Software in eine Datei exportiert werden. Um möglichst viele Zielsysteme zu unterstützen, werden drei unterschiedliche Formate zum Export bereitgestellt:

- .vv-backup: Die Datei enthält sowohl alle Ihre Schlüsselpaare, als auch Ihr Sperrpasswort. Dieses Exportformat sollten Sie wählen, wenn Sie Ihre Schlüssel/Zertifikate in Ihre Anwendungen auf einem anderen Windows-Rechner mit Hilfe der Volksverschlüsselungs-Software automatisch importieren möchten.
- .zip: Die Datei enthält alle Ihre Schlüsselpaare je eine **p12**-Datei pro Schlüsselpaar (s. nächster Punkt). Das Sperrpasswort wird nicht mitexportiert. Dieses Exportformat sollten Sie wählen, wenn Sie Ihre Schlüssel/Zertifikate auf einem iOS, Android oder Mac-Gerät verwenden möchten.
- .p12: Die Datei enthält alle Ihre Schlüsselpaare. Wenn Sie Ihre Schlüssel/Zertifikate in einen Schlüssel-Container im PKCS#12-Format exportieren, können Sie Ihre Schlüssel/Zertifikate auf einer anderen Betriebssystemplattform, wie beispielsweise Linux, in Ihre E-Mail-Programme und Browser manuell importieren.
- 1. Gehen Sie im Hauptmenü auf den Menüpunkt Zertifikatsverwaltung und wählen Sie Zertifikat exportieren.

🕜 Vol	ksverschlüsselung		- 🗆	×
Volksverschlüsselung [®]		Zertifikate verwalten Sie können jetzt eine Zertifikats-Datei in die lokale Datenbank importieren oder ein Ze Jokalen Datenbank als Datei exportieren (Backup). Widerrufen Sie ein Zertifikat, z.B. nar des geheimen Schlüssels, um dieses Zertifikat dauerhaft für ungültig erklären zu lassen.	ManageC rtifikat au: ch dem Ve	erts/Menu s der erlust
	Zertifikate verwalten	Bitte die gewünschte Aktion auswählen:		
<u>↓</u>	 Operation wählen Verwaltungs-Operation Abschließen 	Zertifikat exportieren Ein Zertifikat aus der lokalen Datenbank in eine Datei exportieren (Backup)	~	
-		Zertifikat importieren Eine existierende Zertifikats-Datei in die lokale Datenbank importieren		
?		Zertifikat widerrufen Eines Ihrer existierenden Zertifikate dauerhaft für ungultig erklären lassen		
С				
i				
😹 Fr	aunhofer T	© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie	eiter	-

2. Sie erhalten die Möglichkeit, ein oder mehrere Schlüssel/Zertifikate auszuwählen.

5 Nutzung der Schlüssel/Zertifikate auf anderen Rechnern

Volksverschlüsselung	>
Volksverschlüsselung®	Zertifikate exportieren Die folgende Liste enthält Ihre verfügbaren Zertifikate. Bitte wählen Sie jetzt die gewünschten
Zertifikatsverwaltung	Zertritikat aus, welche im Anschluss als Sicherheitskopie exportiert werden sollen.
Image: Second	Veringen date 2 Zeit dirikelen brite denten Sie jetze finie Wallit Murtad Cheng-Taul Testaccourt.01@wxait.fnaurholer.de Gillig ab: 2016-08-08 1532 Martad Cheng-Taul (GESPERT) testaccourt.01@wxait.fnaurholer.de Gillig ab: 2016-08-01 1606
?	
С	
€ Fraunhofer	vije auswanien į keinė auswanien 1/2 Zertifikatė gewahit © 2015-2016 Franchefer-Institut für Schere Informationstechnologie Weiter

3. Wählen Sie das Zielverzeichnis aus und geben Sie einen Namen ein. Alternativ können Sie den voreingestellten Namen übernehmen. Wählen Sie das Export-Format aus:

Volksverschlüsselung	-		×	×		
	ManageCert	s/ExportCert,	Directory	~ 🕐		
Volksverschlüsselung®	Ziel-Verzeichnis auswählen			Q		
	Bitte wählen Sie jetzt das Ziel-Laufwerk/-Verzeichnis aus, um die Sicherheitskopie Ihrer abzulegen. Es wird empfohlen, hierfür einen Wechseldatenträger (z.B. USB-Stick) zu verw	Zertifik enden.	ate			
Zertifikatsverwaltung						
	Ziel-Verzeichnis auswählen:		8			
Zertifikate verwalten	C:\Users\cheng\Desktop					
Operation wählen	A 🔝 cheng		^			
 Verwaltungs-Operation 	Desktop					
Abschließen	Downloads					
	Links					
	OneDrive					
	Saved Games		~			
2	Gehe zu Desktop Gehe zu Dokumente Neuer Ordner		_			
С	Dateiname eingeben:					
	Zertifikat von cheng (2016-08-23)	.p12	~	1		
()		.p12		1		
Translater T						
st 1	© 2015-2016 Fraunholer-Institut für Sichere Informationstechnologie		_	1		
1 Element 1 Element ausgewählt (66,3 KB)						

4. Geben Sie ein sicheres Passwort ein.

🔮 Vol	ksverschlüsselung	- 🗆 ×
		ManageCerts/ExportCert/Password
Volksverschlüsselung®		Passwort auswählen
†	Zertifikatsverwaltung	Bitte vergeben Sie jetzt ein Passwort, um Ihre exportierten Zertifikate gegen unberechtigten Zugriff zu schützen. Wenn Sie kein Passwort vergeben, werden die Zertifikate unverschlüsselt gespeichert!
	Zertifikate verwalten	✓ Private Schlüssel mit Passwort-Schutz exportieren – EMPFOHLEN
$\overline{1}$	 Operation wählen Verwaltungs-Operation 	Passwort eingeben:
٥	Abschließen	Passwort erneut eingeben:
		••••••
?		Hinweis: Das Passwort muss min. acht Zeichen lang sein und Groß-/Kleinbuchstaben sowie Ziffern enthalten. Erlaubt sind außerdem folgende Sonderzeicher: !*#§≋&`() *+,/: :<>>8 {\]^_` () >>
С		
(i)		
🗟 Fr	aunhofer 🕂	© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie

50

5.2 Verteilung auf andere Windows-Rechner

Übertragen Sie die Datei im Format **.vv-backup** auf Ihr Windows-Zielsystem. Installieren Sie die Volksverschlüsselungs-Software auf dem Zielsystem. Gehen Sie im Hauptmenü auf den Menüpunkt **Zertifikatsverwaltung** und wählen Sie **Zertifikat importieren**. Wählen Sie die Datei aus und geben Sie das beim Export ausgewählte Passwort ein.

Jetzt können Sie mit Hilfe der Volksverschlüsselungs-Software Ihre Schlüssel/Zertifikate wieder in den E-Mail-Programmen und Browsern automatisch installieren.

5.3 Verteilung der Schlüssel auf andere Plattformen, die nicht von der Volksverschlüsselungs-Software unterstützt werden

Wenn Sie normalerweise kein Windows-System nutzen, dann können Sie in einer Windows-Systemumgebung Ihre Zertifikate beantragen, diese exportieren und dann auf eine beliebige Plattform übertragen. Die Konfiguration Ihrer Anwendungen auf dem Zielsystem müssen Sie dann allerdings manuell durchführen.

5.3.1 Export für MacOS, Linux und Android

Sie können Ihre Zertifikate in eine **zip**- oder **p12**-Datei exportieren, wie in Export der Zertifikate aus der Volksverschlüsselungs-Software beschrieben. Übertragen Sie diese Datei auf Ihr Zielsystem. Die Konfiguration Ihrer Anwendungen auf dem Zielsystem müssen Sie dann allerdings manuell durchführen. Es existieren zahlreiche Anleitungen im Internet, die den Import einer P12-Datei in eine Anwendung beschreiben.

Beispielsweise für **Apple Mail** und die Android-App **R2Mail2** (Android App), finden Sie Anleitungen u.a. auf den Seiten der Universität Osnabrück. Nähere Informationen zur Nutzung der Schlüssel und Zertifikate unter Android, erhalten Sie auf Nachfrage. Senden Sie hierzu eine Mail an info@volksverschluesselung.de.

5.3.2 Export für iOS

Eine Anleitung zur Nutzung von Schlüsseln der Volksverschlüsselung unter iOS erhalten Sie auf Nachfrage. Senden Sie hierzu eine Mail an info@volksverschluesselung.de.