Virtuelle Poststelle

Mailverschlüsselung (mit S/MIME)

Überblick

E-Mail-Kommunikation ist nicht nur für Unternehmen zu einem wichtig Bestandteil des Tagesgeschäfts geworden. Wobei die herkömmliche E-Mail-Kommunikation alles andere als ein hohes Vertrauen verdient, denn Sie ist vergleichbar mit dem Transport einer Postkarte durch eine unbekannte Personen. E-Mail-Inhalte sind für Fremde nicht nur lesbar sondern auch manipulierbar und der Empfänger der E-Mail kann diese Änderungen nicht einmal erkennen bzw. feststellen.

Erste Schritte zur vertrauenswürdigen E-Mail-Kommunikation ist die elektronische Signatur von E-Mails mit Benutzerzertifikaten. Das dabei verwendete standardisierte S/MIME Verfahren stellt sicher, dass E-Mails unverändert beim Empfänger ankommen. Falls nicht, wird der Empfänger der E-Mail von jedem modernen E-Mail Programm gewarnt.

Der nächste Schritt zu einer vertrauenswürdigen E-Mail-Kommunikation ist die Verschlüsslung von E-Mails. Somit wird aus der "Postkarte" sogar mehr als nur ein verschlossener Brief. Denn nur der vorgesehene Empfänger der E-Mail kann diese lesen.

Vorgang

Zur Verschlüsselung einer E-Mail benötigen Sie ein Zertifikat zur E-Mail-Verschlüsselung. Zu einem Zertifikat gehört ein Schlüsselpaar: Der private Schlüssel ist ausschließlich für Sie gedacht, den öffentliche Schlüssel kann jeder nutzen, der Ihnen eine verschlüsselte Nachricht senden möchte. Der öffentliche Schlüssel ist zudem Bestandteil des Zertifikats.

Mit Hilfe des Zertifikates können Sie E-Mails signieren. Das E-Mail-Programm des Empfängers hat die Möglichkeit anhand der Signatur festzustellen, ob die E-Mail während der Übertragung manipuliert wurde und ob sie von der im Zertifikat angegebenen Absenderadresse stammt. Beim Signieren einer E-Mail erhält der Empfänger zudem Ihr Zertifikat und somit ebenfalls Ihren öffentlichen Schlüssel. Mit diesem Schlüssel kann er in Zukunft E-Mails an Sie verschlüsseln. Nur Sie sind im Stande mit Hilfe Ihres privaten Schlüssels, diese E-Mail zu entschlüsseln. Deshalb ist es besonders wichtig den privaten Schlüssel Ihres Zertifikats vor Diebstahl zu schützen und ihn niemals Anderen zur Verfügung zu stellen.

Durch die Verwendung von Zertifikaten bei beiden Kommunikationspartnern können E-Mails mit dem privaten Schlüssel des Absenders signiert und gleichzeitig mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden. Da die Übermittlung des öffentlichen Schlüssels bei einer signierten Mail Bestandteil des Zertifikates ist, ist der Kommunikationspartner in der Lage, bereits bei einer Antwort auf eine signierte E-Mail, diese sowohl zu signieren als auch zu verschlüsseln.

Vorteile

Die Verschlüsselung durch S/MIME bietet zwei Funktionen:

- Signatur einer zu versendenden E-Mail mit dem privaten Schlüssel des Versenders
- Verschlüsselung einer zu versenden E-Mail mit dem öffentlichen Schlüssel eines Empfängers

Durch die Signatur kann sichergestellt werden, dass die E-Mail während der Übermittlung nicht verändert / manipuliert wurde. Die Verschlüsselung schützt die E-Mail vor der Einsichtnahme unbefugter Dritter.

Zertifikat

Ein Zertifikat ist ein öffentlicher Schlüssel, der von einer Zertifizierungsstelle (Certification Authority) beglaubigt und unterschrieben ist. Ein Zertifikat belegt, dass der Schlüssel wirklich zu derjenigen Person gehört, die in der Benutzerkennung des Schlüssels angegeben ist. Es ist deshalb vergleichbar mit einem elektronischen Ausweis.

Zertifikatsketten

Um Zertifikate überprüfen zu können, enthält jedes Zertifikat einen Verweis auf das Zertifikat der Zertifizierungsstelle, welche das Zertifikat ausgestellt hat. Technisch gesprochen handelt es sich bei diesem Verweis um eine digitale Unterschrift (Signatur) der Zertifizierungsstelle. Anwendungsprogramme können mit Hilfe des Zertifikats der Zertifizierungsstelle die Gültigkeit eines Zertifikats überprüfen.

Aus technischen oder organisatorischen Gründen, kann es sein, dass das Zertifikat einer Zertifizierungsinstanz seinerseits wieder einen Verweis auf ein Zertifikat einer übergeordneten Zertifizierungsinstanz enthält.

Daraus ergibt sich eine Kette oder eine Hierarchie von Zertifikaten, die überprüft werden müssen, um die Gültigkeit eines Zertifikats zu prüfen.

Zertifikatskette der Poststelle KRZ Lemgo (poststelle@vps.krz.de)



Zertifikatskette eines kostenlosen Zertifikats für max@mustermann.de von COMODO



Wurzelzertifikat

Am Anfang der Kette/Hierarchie von Zertifikaten steht das Wurzelzertifikat (top-level certificate). Die Wurzelzertifikate werden von keiner anderen Zertifizierungsinstanz ausgestellt und enthalten somit keinen nachprüfbaren Verweis auf ein anderes Zertifikat. Die Zertifizierungsinstanz "unterschreibt" vielmehr ihr eigenes Zertifikat (selbst-signiert).

Wurzelzertifikate müssen in den Anwendungsprogrammen installiert sein, damit die Anwendungsprogramme die Hierarchie/Kette von Zertifikaten überprüfen können.

Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Der Absender muss im Besitz eines gültigen X.509-Zertifikates sein und dieses auch installiert haben.
- Für die Empfänger müssen ebenfalls gültige Zertifikate installiert sein.
- Es müssen die Zertifikate der herausgebenden Zertifizierungsstellen installiert sein.
- Den Zertifikaten der Empfänger und der Herausgeber ist das Vertrauen ausgesprochen.

Zuordnung der Zertifikate

Zuordnung der Zertifikate in die jeweiligen Zertifikatsspeicher



Installation des X.509-Zertifikates

Installation der erforderlichen Ausstellerzertifikate

Thunderbird

Während eine Vielzahl von Ausstellerzertifikaten bereits im Zertifikatsspeicher des Thunderbird installiert sind, müssen Sie gegebenenfalls Ihre Ausstellerzertifikate (Wurzelzertifikat, Zwischenzertifikate) nachträglich installieren:

Einstellungen... > Einstellungen... > Zertifikate > Zertifikate... > Zertifizierungsstellen

👔 max.mustermann@example.com				
🛃 Abrufen 🔹 🖋 Verfassen 🔲 Chat 💡	🚨 Adressbuch 🛛 🗞 Schlagwörter - 🔍 Schnellfilter 🛛 Suchen <strg+k> 🔎</strg+k>			
max.mustermann@example.com Posteingang Lokale Ordner	Thunderbird E-Mail - max.mustermann@example.com	Neue Nachricht Anhänge Bearbeiten	Aktivitäten Filter •	
Papierkorb	E-Mail	Suchen	Einstellungen 🕨	Einstellungen Konten-Einstellungen
	Nachrichten lesen Neue Nachricht verfassen	Speichern als Ordner Papierkorb leeren	Datei Ansicht Navigation Nachricht Extras	Hauptsymbolleiste <u>M</u> enüleiste Schnellfilterleiste Statusleiste
	Konten	Beenden	Hilfe •	Symbolleisten anpassen
	Konten-Einstellungen bearbeiten			Fensterlayout
	Neues Konto erstellen			
	Erweiterte Funktionen			
	Nachrichten suchen			
Fertig				





Klicken Sie auf "Importieren" und wählen Sie das Ausstellerzertifikat aus. Danach ist diesem importierten Zertifikat durch "Bearbeiten" der Vertrauensstatus einzustellen. Hier ist zumindest das Vertrauen für die Identifikation von Mail-Benutzern erforderlich.

Outlook 2010

Während eine Vielzahl von Ausstellerzertifikaten bereits im Zertifikatsspeicher von Windows installiert sind, müssen Sie gegebenenfalls Ihre Ausstellerzertifikate (Wurzelzertifikat, Zwischenzertifikate) nachträglich installieren. Hierzu gehen Sie im Internet Explorer über Extras > Internetoptionen > Inhalte



und klicken auf "Zertifikate".

Ceere Seite - Windows Internet Explor	er			_O×
G 🕞 🗢 🧟 about:blank	ه 🕂 🔍 ۹	Leere Seite	×	în ☆ 🔅
Datei Bearbeiten Internetoptionen			?×	
Zertifikate				×
Beabsichtigter Zweck: <alle< td=""><td>></td><td></td><td>•</td><td>न ।</td></alle<>	>		•	न ।
Zwischenzertifizierungsstelle	n Vertrauenswürdige Sta	mmzertifizierun	asstellen Vertrauen 4	- FI
				1
Ausgestellt für	Ausgestellt von	Ablaufda	Anzeigename 🔺	
AAA Certificate Ser	AAA Certificate Services	01.01.2029	соморо —	
ABA.ECOM Root CA	ABA.ECOM Root CA	09.07.2009	DST (ABA.ECOM	
AC Raíz Certicámar	AC Raíz Certicámara	02.04.2030	AC Raíz Certicá	
AC RAIZ DNIE	AC RAIZ DNIE	09.02.2036	DIRECCION GEN	
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	01.01.2030	AC RAIZ FNMT	
AC1 RAIZ MTIN	AC1 RAIZ MTIN	03.11.2019	AC1 RAIZ MTIN	
ACEDICOM Root	ACEDICOM Root	13.04.2028	EDICOM	
A-CERT ADVANCED	A-CERT ADVANCED	23.10.2011	A-CERT ADVANC	
ACNLB	ACNLB	15.05.2023	NLB Nova Ljublja 🖵	
Importieren Exportiere	n Entfernen		Erweitert	
				ʻ
Beabsichtigte Zwecke des Z	ertifikats			
			Anzeigen	
				·
Weitere Informationen über	Zertifikate		California	
	<u>eer enneree</u>		Schlieben	

Im folgenden Dialogfenster "Zertifikate" wählen wir den Reiter "Zwischenzertifizierungsstellen" aus und klicken auf "Importieren". Falls Sie ein Wurzelzertifikat installieren müssen, wählen Sie stattdessen den Reiter "Vertrauenswürdige Stammzertifizierungsstellen" und klicken auf "Importieren".

Leere Seite -	Windows Internet Explo	er		1	
Datei Bearbei	iten Internetoptionen		Leere Seite	×	<u> </u>
Ze	ertifikate				×
-	Beabsichtigter Zweck: <a>Alle	>			3
	Eigene Zertifikate Andere	Personen Zwischenzertifiz	tierungsstellen	Vertrauenswürdige	빅
	Ausgestellt für	Ausgestellt von	Ablaufda	Anzeigename	
	Microsoft Internet	GTE CyberTrust Globa	14.04.2018	<keine></keine>	
	Microsoft Secure S	Microsoft Internet Au	20.05.2014	<keine></keine>	
	Boot Agency	Root Agency	31,12,2002	<keine></keine>	
	TC TrustCenter Cla	TC TrustCenter Class	01.01.2026	<keine></keine>	
	TC TrustCenter Cla	TC TrustCenter Class	01.01.2026	<keine></keine>	
	TeleSec ServerPass	Baltimore CyberTrust	30.11.2017	<keine></keine>	
	USERTrust Legacy	Entrust.net Secure Se	01.11.2015	<keine></keine>	
	En www.vensign.com/	Class 5 Public Primary	25.10.2016	<keine></keine>	
	Exportieren Exportiere Beabsichtigte Zwecke des Z	n Entfernen		Erweitert	
				Anzeigen	
	Weitere Informationen über	Zertifikate		Schließen	

Wählen Sie das Ausstellerzertifikat und bestätigen mit OK.

Installation des eigenen Zertifikates

Thunderbird

Dazu ist hier die aus dem Browser exportierte .pfx- oder .p12-Datei mit dem geheimen Schlüssel auszuwählen:

Einstellungen... > Einstellungen... > Zertifikate > Zertifikate... > Ihre Zertifikate > Importieren

					_	
ax.musterma	nn@example.com				-	
					0	
🚨 Abrufen 🔹 🖉 Vi	erfassen 🖤 Chat 📕 Adre	ssbuch 👒 Schlagwörter 🛀 🔍	Schnellfilter Suchen <	Strg+K>	ر	=
⊿a max.musterma	ann@example.com	underbird E-Mail	- max mucto	rmann@ova	mple con	. A
Posteingang	111		- maximuste	ппапп@еха	inple.com	
Papierkorb	Einstellu	ngen				×
🛕 Postausgang	Zertifikat-Manager					
	Ihre Zertifikate	Server Zertifizierungsstellen	Andere			
	Sie behan Zortifikete dier	ren Organisationan, die Sie identifini			1	
	Sie haben zertinkate dies	er Organisationen, die bie identitizi	eren:	1		
	Zertifikatsname	Kryptographie-Modul	Seriennummer	Läuft ab am	<u>E</u>	
	Anathen Coltan	- Alle state on Transaction	t Sector			
Fertig	Ansenen Sicher		Loschen			1
					or 1	

Hierbei werden Sie zuerst nach dem Masterpasswort des "Software-Sicherheitsmoduls" und danach nach dem "Transportpasswort" der .pfx- bzw. .p12-Datei gefragt.

ax.mustermann@example.com		
초 Abrufen 🔹 🖋 Verfassen 🔍 Chat	Adressbuch Schlagwörter Schnellfilter Suchen <strg+k></strg+k>	≡ ۹
max.mustermann@example.co	^m Thunderbird E-Mail - max.mustermann@exan	nple.com
Papierkorb	Einstellungen	×
🚵 Postausoano 🎯 Zertifikat-Manager		Erweitert
Ihre Zertifikate Persone	n Server Zertifizierungsstellen Andere	
Sie haben Zertifikate die	ser Organisationen, die Sie identifizieren:	
Zertifikatsname	Kryptographie-Modul Seriennummer Läuft ab am 🛱	
	Passworteingabe-Dialog X Bitte geben Sie das Passwort ein, das verwendet wurde, um dieses Zertifikats-Backup zu verschlüsseln. Passwort: Passwort:	_
Ansehen Siche	m Alle sicherm Importieren	
	OK	

Voraussetzung für einen erfolgreichen Import ist das Vorhandensein der Herausgeberzertifikate (unter "Zertifizierungsstellen") sowie das ausgesprochene Vertrauen in diese Zertifikate (=> "Bearbeiten").

🛛 max.mu	stermann@example.com	D. Schlagujärter - O. School Kätzer - States IV.	
Abduer	stermann@example.com ang rdner rb Zertifikat-Manager	erbird E-Mail - max.mustermann@examp	le.com
	Sie haben Zertifikate gespeichert, die diese Zr Zertifikatsname Equifax Secure eBusiness CA-1 a Example Inc. C a Example	ertifizierungsstellen identifizieren: Kryptographie-Modul Builtin Object Token	
	▲ Generalitat Valenciana Root CA Generalitat Valenciana ▲ GeoTrust Inc. GeoTrust Extended Validation SSL CA GeoTrust Global CA 2 GeoTrust Global CA	CA-Zertifikat-Vertrauenseinstellungen bearbeiten X Das Zertifikat "CA-Example" repräsentiert eine Zertifizierungsstelle. Vertrauenseinstellungen bearbeiten Dieses Zertifikat kann Websites identifizieren.	
<u>s</u>	GeoTrust Primary Certification Authorit:	Dieses Zertifikat kann Mail-Benutzer identifizieren. Dieses Zertifikat kann Software-Hersteller identifizieren. OK Abbrechen	

Nach dem erfolgreichen Import des eigenen Zertifikates übernimmt das Software-Sicherheitsmodul des Thunderbird durch die Verschlüsselung mit dem Masterpasswort den Schutz des eigenen privaten Schlüssels.

Outlook 2010

Im Internet Explorer wählen Sie *Extras > Internetoptionen > Inhalte* und klicken auf "Zertifikate". Im folgenden Dialogfenster "Zertifikate" wählen Sie den Reiter "Eigene Zertifikate" aus und klicken auf "Importieren".

E Leere Seite - Windows Internet Explorer	
Co v C about:blank	☆ ☆ 🕸
Datei Bearbeiten Internetoptionen	
Zertifikate	
Beabsichtigter Zweck: <alle></alle>	
Eigene Zertifikate Andere Personen Zwischenzertifizierungsstellen Vertrauenswürdige :	
Ausgestellt für Ausgestellt von Ablaufda Anzeigename	
Transitianan Fonderson Frusitant	
Beabsichtigte Zwecke des Zertifikats	
Anzeigen	
Weitere Informationen über Zertifikate Schließen	

Wählen Sie Ihr Zertifikat aus und bestätigen, anschließend werden Sie nach dem "Transportpasswort" der .pfx- bzw. .p12-Datei gefragt.



Einstellen der S/MIME-Sicherheit des Mailkontos

Thunderbird

Jetzt ist die Verknüpfung des Zertifikates mit dem Mailkonto herzustellen. Dazu ist hier das richtige Zertifikat auszuwählen:

Einstellungen... > Konten-Einstellungen... > %Kontenname% > S/MIME-Sicherheit

ax.mustermann@example.com				
🛃 Abrufen 🔹 🖋 Verfassen 🔲 Chat	🚨 Adressbuch 🛛 🗞 Schlagwörter - 🔍 Schnellfilter 🛛 Suchen <strg+k> 🔎</strg+k>			
max.mustermann@example.com Posteingang Jokale Ordner	Thunderbird E-Mail - max.mustermann@example.cor	Neue Nachricht Anhänge Bearbeiten	Aktivitäten Filter •	
 Papierkorb Postausgang 	E-Mail	Suchen	Einstellungen 🕨	Einstellungen Konten-Einstellungen
	Rachrichten lesen	Speichern als Ordner	Datei Ansicht Navigation	 ✓ Hauptsymbolleiste Menüleiste
,	Neue Nachricht verfassen	Papierkorb leeren	Nachricht Extras Hilfe	Schnellfilterleiste ✓ Statusleiste
	Konten			Symbolleisten anpassen
	🌼 Konten-Einstellungen bearbeiten			Pensteriayout
	Neues Konto erstellen			
	Erweiterte Funktionen			
	Q Nachrichten suchen			
Fertig		li.		

max.mustermann@example.com		
Konten-Einstellungen	X	
 max.mustermann@example.com Server-Einstellungen Kopien & Ordner Verfassen & Adressieren Junk-Filter Synchronisation & Speicherplatz Empfangsbestätigungen (MDN) S/MIME-Sicherheit Lokale Ordner Junk-Filter Speicherplatz Postausgang-Server (SMTP) 	S/MIME-Sicherheit Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben. Digitale Unterschrift Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiben: Auswählen Leeren Nachrichten gigital unterschreiben (als Standard) Verschlüsselung Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln: Auswählen Leeren Standard-Verschlüsselungseinstellung beim Senden von Nachrichten: © Igie (keine Verschlüsselung verwenden) © In getwendig (Senden nur möglich, wenn alle Empfänger ein Zertifikat besitzen) Zertifikate Zertifikate verwalten Kryptographie-Module verwalten	mple.com
Konten-Aktionen •		
	OK Abbrechen	

Das Zertifikat ist sowohl für die "Digitale Unterschrift" (Signatur) als auch für die "Verschlüsselung" auszuwählen. Die standardmäßige Anwendung der digitalen Unterschrift bei allen Nachrichten ist empfohlen, die standardmäßige Anwendung der Verschlüsselung nur dann, wenn von allen Adressaten ein Zertifikat vorhanden ist.

Outlook 2010

In Outlook klicken Sie auf den orangen "Datei" Reiter oben links. Klicken Sie anschließend linker Hand auf "Optionen".



Das Dialog-Fenster "Outlook-Optionen" öffnet sich. Klicken Sie linker Hand auf "Sicherheitscenter". Danach klicken Sie rechter Hand auf "Einstellungen für das Sicherheitscenter".

0	utlook-Optionen	2 💌
	Allgemein E-Mail	Sorgen Sie für die Sicherheit Ihrer Dokumente und des Computers.
	Kalender	Datenschutz
	Kontakte	Microsoft nimmt den Datenschutz ernst. Weitere Informationen, wie Microsoft Outlook für den Datenschutz sorgt, finden Sie in den Datenschutzbestimmungen.
	Aufgaben	Datenschutzbestimmungen für Microsoft Outlook anzeigen
	Notizen und Journal	Datenschutzbestimmungen für Office.com
	Durchsuchen	Programmi zur Verbesserung der benützenreunonchkeit
	Mobiltelefon	Sicherheit & mehr
	Sprache	In Office.com finden Sie weitere Informationen zum Datenschutz und zur Sicherheit.
	Erweitert	Microsoft Trustworthy Computing
	Menüband anpassen	Microsoft Outlook-Sicherheitscenter
	Symbolleiste für den Schnellzugriff	Das Sicherheitscenter enthält Einstellungen für Sicherheit und Datenschutz, um für
	Add-Ins	die Sicherheit des Computers zu sorgen. Es wird davon abgeraten, diese Einstellungen für das Sicherheitscenter…
	Sicherheitscenter	
Ľ		OK Abbrechen

Das Fenster "Sicherheitscenter" öffnet sich. Wählen Sie links in der Liste den Punkt "E-Mail-Sicherheit". Um die Standardeinstellungen festzulegen, klicken Sie auf "Einstellungen".

Sicherheitscenter	? **
Sicherheitscenter Vertrauenswürdige Herausgeber DEP-Einstellungen Datenschutzoptionen Inglat und Anlagen für ausg. Anlagenbehandlung Automatischer Download Inglat EDS (Zertifikate) Einstellungen für Makros Programmgesteuerter Zugriff Digitale IDS zw. Zertifikate sind Dr. werden kann. In GAL veröffentlichen Makros Digital signierte Nachrichten im Nur- Skript in Ordnern Skript in Öffentlichen Ordnern zulasser	ehende Nachrichten verschlüsseln gitale Signatur hinzufügen text senden rn, wenn mit S/MUME signiert skumente, mit denen die Identität in elektronischen Transaktionen nachgewiesen ortieren/Exportieren Digitale ID anfordern et lesen -Text-Format Jesen
	OK Abbrechen

Das Fenster "Sicherheitseinstellungen ändern" öffnet sich. Im Feld "Name der Sicherheitseinstellung" tragen Sie nun einen beliebigen Namen ein. Als nächstes wählen Sie das Signaturzertifikat aus, klicken Sie dazu auf "Auswählen" in der Zeile Signaturzertifikat. Wählen Sie nun Ihr Zertifikat aus und bestätigen mit ok. Wiederholen Sie nun den Vorgang für das Verschlüsselungszertifikat. Klicken Sie danach auf "OK" um die Konfiguration abzuschließen.

Sicherheitseinstellungen änder	n		— X—
Bevorzugte Sicherheitseinstellung Na <u>m</u> e der Sicherheitseinstellun	en g:		
1			•
Kryptografieformat:	S/MIME		-
🔲 Standardeinstellung für die	ses <u>F</u> ormat kryptograf	fischer Nachricht	en
Stan <u>d</u> ardsicherheitseinstellu	ung für alle kryptograf	fischen Nachricht	en
Sicherheitskennzeichen	Neu	Löschen	Kennwort
Zertifikate und Algorithmen			
Signaturzertifikat:			Auswählen
Hashalgorithmus:		v	
Verschlüsselungszertifikat:			Auswählen
Verschlüsselungsalgorithmus:		Ŧ	
📝 Signierten Nachrichten dies	e <u>Z</u> ertifikate hinzufüge	en	
		ОК	Abbrechen

Installation der Zertifikate der Adressaten

Um Nachrichten an einen Adressaten verschlüsseln zu können, ist die Installation seines Zertifikates erforderlich. Beim Öffnen einer vom diesem Adressaten signierten E-Mail erfolgt die Installation automatisch, aber auch hier ist das Aussprechen des Vertrauens notwendig.

Analog zu dem eigenen Zertifikat, ist auch hier zu nächst die Installation der Ausstellerzertifikate von Nöten (siehe "Installation der erforderlichen Ausstellerzertifikate").

Thunderbird

Zur Installation des Zertifikats des Adressaten wählen Sie:

🛃 max.i	mustermann@example.com				_ _ _ ×
🚨 Abrufen	🔹 🖉 Verfassen 🔍 Chat 🔒 Adressbur	:h 🔊 Schlagwörter 🔹 🔍 Schne	lfilter Suchen <strg+k></strg+k>		₽ ≡
⊿ <mark>≧⊠ max.m</mark> Å Postei	nustermann@example.com Ingang Thun	derbird E-Mail - m	ax.mustermanı	ı@example	e.com 🗎
🛛 🖳 Lokale	Ordner			-	
🔯 Papier			0	O.	A A A A A A A A A A A A A A A A A A A
i rostat	avana 🖉				202
		un la l			Erweitert
	Ihre Zertifikate Personen Server Zer	tifizierungsstellen Andere			
	Sie haben Zertifikate gespeichert, die die	se Personen identifizieren:			
	Zertifikatsname	Läuft ab am	E-Mail-Adresse	E	
	Ansehen Vertrauen bearbeiten	Importieren Exportieren	Löschen		
				ок	

Einstellungen... > Einstellungen... > Zertifikate > Zertifikate > Personen

Klicken Sie auf "Importieren" und wählen Sie das Zertifikat des Adressaten aus.

Outlook 2010

Erstellen Sie einen neuen "Kontakt" in Outlook indem Sie den Reiter "Start" auswählen und auf "Neue Elementen" klicken und dabei "Kontakt" wählen. Im folgenden Dialogfenster "Kontakt" klicken Sie auf "Anzeigen" und wählen "Zertifikate".

토 및 의 (Y 수 가 I국 🖬	Unbenannt -	Kontakt			
Datei Kontakt Einfügen Text formatier	n Überprüfen				~ ?
Speichern und neuer Kontakt Speichern & schließen Aktionen	▼ Anzeigen	Adressbuch Namen überprüfen Namen	Visitenkarte Bild Optionen	 Kategorisieren * Nachverfolgung * Privat Kategorien 	Zoom Zoom
Name Firma: Position: Speichern unter: Internet Internet Anzeigen als: Webseite:	Allgemein Allgemein Allge Alle Felde Anzeigen	n r Notizen			
Telefonnumern Geschäftlich Fax geschäftl Fax geschäftlich Adressen Geschäftlich Dies ist die Potsanschrift					4
	Zuordnen				•

Klicken Sie nun auf "Importieren" und wählen anschließend das Zertifikat des Adressaten aus und bestätigen mit "OK".

도 ↓ <) (5 ★ → =	📕 🤊 🕑 🍲 🕴 🗧 Unbenannt - Kontakt							
Datei Kontakt Einfügen Text formatieren	Überprüfen				~ ?			
Speichern und neuer Kontakt * Speichern Löschen & schließen	Anzeigen	Adressbuch Namen überprüfen	Visitenkarte Bild	 Kategorisieren * Nachverfolgung * Privat 	Zoom			
Aktionen kategorien zoom kategorien zoom kategorien zoom kategorien zoom optionen kategorien zoom Outlook verwendet eines dieser Zertifikate, um verschlüsselte E-Mail-Nachrichten an diesen Kontakt zu senden. Sie können ein Zertifikat erhalten, indem Sie eine digital signierte Nachricht von diesem Kontakt empfangen oder eine Zertifikatdatei für diesen Kontakt importieren.								
Zertifikate (digitale IDs): Eigenschaften								
	Als Sta	Als Standard festl.						
				En	tfernen			
					^			

Klicken Sie anschließend wieder auf "Anzeigen" und wählen dann "Allgemein" aus. Vervollständigen Sie nun die Angaben zu Ihrem E-Mail Kontakt (Name, E-Mail, usw.).

X.509-Zertifikat

X.509

X.509 ist ein Standardformat der ITU-T (International Telecommunication Union-Telecommunication) für Zertifikate. Es beinhaltet den Namen des Ausstellers, üblicherweise eine Certification Authortity, Informationen über die Identität des Inhabers sowie die digitale Signatur des Ausstellers und den Gültigkeitszeitraum des Zertifikates. Auf dem X.509-Format basieren z. B. SSL und S/MIME.

X.509-Zertifikate für Einzelpersonen werden in folgenden Klassen herausgegeben:

Class 0

Class 0-Zertifikate (Demo-Zertifikate) sind für Testzwecke gedacht und mit beschränkter Gültigkeitsdauer.

Class 1

Class 1-Zertifikate bestätigen, dass die angegebene E-Mail-Adresse existiert und der Besitzer des zugehörigen öffentlichen Schlüssels Zugriff auf diese E-Mail-Adresse hat. Sie stellen damit nur einen sehr geringen Nachweis der Identität dar. Da keine Überprüfung anhand von Unterlagen stattfindet, können Class 1-Zertifikate (Express-Zertifikat) binnen weniger Minuten ausgestellt und an den Kunden ausgeliefert werden. Sie sind ideal für private Nutzer, die erste Schritte auf dem Weg zur sicheren Internet-Kommunikation gehen wollen und den Umgang mit verschlüsselter E-Mail ausprobieren möchten, und sie werden von den meisten Trustcentern kostenlos herausgegeben.

Class 2

Bei Class 2-Zertifikaten für Unternehmen wird auf eine persönliche Identitätsfeststellung verzichtet. Eine einfache Kopie des Handelsregisterauszuges zur Feststellung der zeichnungsberechtigten Person und ein schriftlicher Auftrag sind ausreichend. Diese Zertifikate sind hauptsächlich für die gesicherte Kommunikation zwischen einander bereits außerhalb des Internets bekannten Partnern gedacht.

Class 3

Class 3 beinhaltet neben der E-Mail-Überprüfung eine persönliche Identitätsprüfung der Person. Mit der Ausstellung eines Class 3-Zertifikats bestätigt das Trustcenter, dass diese Person anhand ihres Personalausweises oder Reisepasses identifiziert worden ist und die im Zertifikat enthaltenen Angaben zur Person mit den Angaben im Ausweis übereinstimmen. Diese Zertifikate sind vor allem für Anwendungen im E-Commerce gedacht, wie beispielsweise Internet Banking und Online Shopping. Sie werden aber auch zunehmend für die elektronische Kommunikation mit Behörden eingesetzt (Übermittlung Steuerdaten und zukünftig elektronische Antragstellung).

Certificate Authority (CA)?

Eine Zertifizierungsstelle (engl. Certificate Authority, kurz CA) ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist gewissermaßen das Cyberspace-Äquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie diese mit ihrer eigenen digitalen Unterschrift versieht. Die Zertifikate enthalten "Schlüssel" und Zusatzinformationen, die zur Authentifizierung sowie zur Verschlüsselung und Entschlüsselung sensitiver oder vertraulicher Daten dienen, die über das Internet und andere Netze verbreitet werden. Als Zusatzinformationen sind zum Beispiel Lebensdauer, Verweise auf Sperrlisten etc. enthalten, die durch die CA mit in das Zertifikat eingebracht werden.

Zunehmend bieten auch Banken und Sparkassen ihren Kunden qualifizierte Zertifikate auf Chipkarten an. Zertifikate werden durch die CA je nach Anforderung als Hardwaretoken (auf Chipkarte) oder als Softwarezertifikat herausgegeben. Für die außerordentlich hohen Anforderungen der so genannten "qualifizierten Signatur" (Class 3) sind ausschließlich Hardwaretoken und die entsprechenden Kartenleser zugelassen.

Die für private Nutzung meist ausreichenden Class 1-Zertifikate werden dem Antragsteller als Softwaretoken übergeben. Beispiele für Trustcenter sind: <u>http://www.trustcenter.de/</u>, <u>https://www.startssl.com</u>

Selbstverständlich gibt es auch die Möglichkeit, X.509-Zertifikate speziell für geschlossene Nutzergruppen (Familie, Freunde, Forum, Firmen ...) selbst zu produzieren.

Ein ausgezeichnetes Werkzeug dafür ist das als Linux- und auch als Windowsversion erhältliche Freewareprogramm "XCA". <u>http://xca.sourceforge.net/</u> Dieses Programm besticht nicht nur durch ein logisches Bedienkonzept, sondern auch durch die Möglichkeit, für alle gängigen Anwendungsfälle Vorlagen zu erstellen. Selbstverständlich ist auch die Erstellung von Sperrlisten möglich und die produzierten Zertifikate lassen sich in allen gängigen Formaten exportieren.

kostenloses X.509-Zertifikat (Class 1)?

Beispielsweise hier: trustcenter.de, StartSSL Free, Free Secure Email Certificate (Comodo)

Qualifizierte elektronische Signatur

Voraussetzungen

- Komfort Kartenlesegerät
- elektronische Signaturkarte
- Prüfsystem-/software
- Archiv