▲ Hochschule Harz

Rechenzentrum

Thunderbird

Signierung und Verschlüsselung von E-Mails im Thunderbird

Stand: 16.10.2017

Inhalt

1.	Import des eigenen Zertifikates im Thunderbird	2
2.	Import von Zertifikaten anderer Personen	2
3.	Signierung einer E-Mail	3
4.	Verschlüsselung einer E-Mail	5

1. Import des eigenen Zertifikates im Thunderbird

Für die Einbindung muss das Zertifikat als *p12* oder *pfx* Datei vorliegen, diese Datei enthält den privaten Schlüssel und das öffentliche Zertifikat.

Für die Einbindung muss das Zertifikat importiert werden, dazu unter *Extras -> Einstellungen -> Erweitert -> Zertifikate* den Zertifikatsspeicher öffnen und im sich öffnenden Fenstert *importieren* drücken.

Einstellungen								×
Allgemein	Ansicht	Verfassen	 Chat	Datenschutz	Sicherheit	Q Anhänge	Kalender	Erweitert
Allgemein Da Wenn eine O Au Ø Aktuell Zertifikate	Ansicht atenübermittlur Website nach d tomatisch eins e <u>G</u> ültigkeit vor	Verfassen ng Netzwerk & S lem persönlicher wählen	Chat Speicherplatz n Sicherheitsze les Mal fragen ch Anfrage be lodule verwalt	Datenschutz Update Zertifika ertifikat verlangt: n ei OCSP-Server be ten	sicherheit	Anhange	Kalender	Erweitert
							ОК	Abbrechen

Durchsuchen Sie den lokalen Dateiträger nach der Zertifikatsdatei und geben Sie dann das Kennwort an. Danach sollte der Import erfolgen.

2. Import von Zertifikaten anderer Personen

Im <u>Webfrontend G2</u> können Zertifikate anderer Personen gedownloadet werden. Für die Installation im Windows am besten gleich den Internet Explorer nehmen. Einfach über den Menüpunkt *"Zertifikat suchen"* den Namen oder die gesuchte E-Mailadresse im Suchfeld eingeben.

Zertifika	te CA-Zei	rtifikate Gesperrte Z	ertifikate Policies Hilf	e Beenden		
Nutzerze	rtifikat	Serverzertifikat	Zertifikat sperren	Zertifikat suchen		
				Zertifikat suchen		
	Bitte geber dem Zertif	n Sie den exakten Nar fikat ein, das Sie suche	men (keine Umlaute) ode en. Es werden maximal 2	er die exakte E-Mail-Adresse aus 0 Zertifikate angezeigt.		
	Name oder E-Mail-Adresse					
			OK Zurücksetzen			

Klicken Sie auf die kleine Grafik links um sich die Detailansicht anzeigen zu lassen. Wenn sie ganz nach unten Scrollen, können Sie das Zertifikat downloaden. Beachten Sie dabei es als *.der* zu speichern.

Klicken Sie auf die Seriennummer eines Zertifikats, um es in Ihren Browser zu importieren.							
0	Seriennummer 908049248716881	Name	E-Mail hs-harz.c	Rolle de User			
Operationen Zertifikat abspeichern DER ✓ Download Zertifikat in den Browser installieren Installieren							

Um das Zertifikat zu importieren, klicken Sie doppelt auf die Datei und befolgen Sie den Assistenten.

3. Signierung einer E-Mail

Mit der Signierung wird nicht nur die Herkunft des Absenders bestätigt, sondern es wird auch weiterhin geprüft, ob eine E-Mail auf Ihrem Weg verändert wurde. Sofern eine geänderte Mail vorliegt, wir der Empfänger durch Thunderbird informiert.

Wenn das eigene Zertifikat eingebunden ist, dann kann unter *"Extras" -> "Einstellungen" -> "Kontoeinstellungen" -> "S/Mime Sicherheit"* das Zertifikat für die Signierung ausgewählt werden.



Wird als Standard "digital unterschreiben" gewählt, werden alle Nachrichten mit dem Zertifikat unterschrieben. Diese Option kann im "Verfassen"- Fenster auch für jede Nachricht einzeln eingestellt werden.

nten-Einstellungen							
∕⊠ <u>@hs-harz.de</u> ^	S/MIME-Sicherheit						
Server-Einstellungen							
Kopien & Ordner	Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben.						
Verfassen & Adressieren							
Junk-Filter	Digitale Unterschrift						
Synchronisation & Speicherplatz	Folgendes Zertifikat verwenden, um Nachrichten digital zu	nterschreiben:					
Empfangsbestätigungen (MDN)	Verein zur Foerderung eines Deutschen Forschungsnetze:	<u>A</u> uswählen	<u>L</u> eeren				
S/MIME-Sicherheit	✓ Nachrichten digital unterschreiben (als Standard)						
🖂 Inetzband@web.de							
Server-Einstellungen	Verschlüsselung						
Kopien & Ordner	Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln:						
Verfassen & Adressieren	Verein zur Foerderung eines Deutschen Forschungsnetze:	Aus <u>w</u> ählen	L <u>e</u> eren				
Junk-Filter	Standard-Verschlüsselungseinstellung beim Senden von Na	chrichten:					
Synchronisation & Speicherplatz	Nie (keine Verschlüsselung verwenden)						
Empfangsbestätigungen (MDN)							
S/MIME-Sicherheit	 Notwendig (Senden nur möglich, wenn alle Empfänger 	ein Zertifikat besi	tzen)				
💆 Lokale Ordner	Zertifikate						
Junk-Filter	Zertifikate verwalten Kryptographie-Module verwalte	en					
Speicherplatz							
🟦 Postausgangs-Server (SMTP) 🛛 🗸							
Konten-Aktionen •							
		ОК	Abbreche				

Der Empfänger erhält mit einer digital unterschriebenen Nachricht das Zertifikat des Absenders. Das Zertifikat des Absenders wird automatisch in den Zertifikatsspeicher importiert.

4. Verschlüsselung einer E-Mail

Durch die Verschlüsselung kann der Absender sicherstellen, dass nur Personen, die auch berechtigt dazu sind, diese E-Mail lesen.

Zertifikate anderer Nutzer werden für die Verschlüsselung von E-Mails benötigt. Um eine E-Mail zu verschlüsseln muss daher das Zertifikat des Gegenübers im Thunderbird bekannt sein. Zum Verschlüsseln im "Verfassen"- Fenster die entsprechende Option auswählen. Thunderbird wählt automatisch anhand der "An"-Liste die entsprechenden Zertifikate aus.

	·		S/MIME 🔻 🕂 Speichern 🔫		
	0		Nachricht <u>v</u> erschlüsseln		
	-	~	Nachricht unterschreiben	63	
	Η		Sicherheitsinformationen anzeigen		
Eventuell	()	_			

🚖 Verfassen: (kein Bet	eff)	_		×				
<u>D</u> atei <u>B</u> earbeiten <u>A</u> ns	<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>E</u> infügen <u>F</u> ormat <u>O</u> ptionen Extras <u>H</u> ilfe							
∰ Senden 🗸 Rechtschr. 🔻 🖲 Anhang 🔻 🖴 S/MIME 👻 III Speichern III								
<u>V</u> on:	Sicherheitseinstellungen ansehen oder ändern			~				
✓ An:								
Bet <u>r</u> eff:								

Der Empfänger sieht seine Mail dann mit dem Schloss-Symbol gekennzeichnet und kann diese nur lesen, wenn Sie mit seinem Zertifikat verschlüsselt wurde.

