Import des Nutzerzertifikats

Das beantragte Nutzerzertifikat wird Ihnen zeitnah zip-komprimiert per E-Mail zugestellt. Sie erhalten eine E-Mail mit angehängtem ZIP-Ordner, in welchem sich das Zertifikat befindet. Zertifikate - Gauß-IT-Zentrum BDD: Ihr Nutzerzertifikat Wir haben zusätzliche Zeilenumbrüche aus dieser Nachricht entfernt.

Guten Tag,

im Anhang erhalten Sie das über den BDD beantragte Nutzerzertifikat in einer .zip-Datei. Nach dem Entpacken der Datei können Sie das Zertifikat wie gewohnt verwenden.

Bitte leiten Sie diese Email nicht weiter und antworten Sie nicht auf diese Email, sie enthält eine vertrauliche Datei.

Weitere Informationen finden Sie im Anleitungs-Wiki des Gauß-IT-Zentrums: <u>https://doku.rz.tu-bs.de/doku.php?</u> <u>id=zertifikate:zertifikate</u>

Diese Email wurde automatisch erstellt. Bei Rückfragen stehen wir Ihnen gerne zur Verfügung.

Viele Grüße

Abteilung Netze

Dieses zip-Archiv enthält eine **pkcs#12 (.p12) Zertifikatsdatei**. Diese muss entpackt und im Trust-Center von Outlook eingebunden werden.

Zum Hinzufügen des Nutzerzertifikats öffnen Sie die Oulook **[Optionen]** (Datei < Optionen).

$ \in $	Posteingang - @tu-braunschweig.de - Outlook
Informationen Öffnen und Exportieren	Kontoinformationen
Speichern unter Anlagen speichern	Microsoft Exchange Konto hinzufügen
Office- Konto Optionen	Kontoeinstellungen Ändern der Einstellungen für dieses Konto oder Einrichten weiterer Verbindungen. Zugriff auf dieses Konto im Internet. <u>https://mail.tu-braunschweig.de/owa/</u> Die Outlook-App für iPhone, iPad, Android oder Windows 10 Mobile herunterladen.
Beenden	Ändern Automatische Antworten Automatische Antworten Sie auf E-Mail-Nachrichten nicht antworten können.

Wählen Sie in den Optionen unter dem Reiter [Trust Center] die [Einstellungen für das Trust Center] aus.

	Outlook-Optionen	\times
Allgemein E-Mail	Sorgen Sie für die Sicherheit Ihrer Dokumente und des Computers.	
Kalender	Sicherheit & mehr	
Personen	Besuchen Sie Office.com, um weitere Informationen zum Datenschutz und zur Sicherheit zu erhalten.	
Aufgaben	Microsoft Trustworthy Computing	
Suchen	Microsoft Outlook-Trust Center	
Sprache	Das Trust Center enthält Einstellungen für Sicherheit und Datenschutz, um für die Sicherheit	_
Erleichterte Bedienung	des Computers zu sorgen. Es wird davon abgeraten, diese Einstellungen zu ändern.	iter
Erweitert		
Menüband anpassen		
Symbolleiste für den Schnellzugriff		
Add-Ins		

Wählen Sie die Kategorie **[E-Mail-Sicherheit]** aus und klicken Sie unter dem Aspekt Digitale IDs auf **[Importieren/Exportieren]**.

Trust Center

Vertrauenswürdige Herausgeber	Verschlüsselte E-Mail-Nachrichten	
Datenschutzoptionen	In <u>h</u> alt 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- <u>B</u> estätigung anfordern, wenn mit S/MIME signiert	
Makroeinstellungen	Standardeinstellung:	
Programmgesteuerter Zugriff	Digitale IDs (Zertifikate)	
	Digitale IDs bzw. Zertifikate sind Dokumente, mit denen die Identität in elektronischen Transaktionen nachgewiesen werden kann. In <u>G</u> AL veröffentlichen	
	Als Nur-Text lesen	
	Standardnachrichton im Nur-Toxt-Format lecon	

In dem sich geöffneten Fenster müssen Sie nun die Zertifikatsdatei auswählen. Klicken Sie auf **[Durchsuchen]**.

Digitale ID importieren/exportieren X				×	
O Bestehende digitale ID a	O Bestehende digitale ID aus einer Datei importieren				
Importieren Sie die digitale ID aus der Datei auf Ihren Computer. Geben Sie das beim Exportieren des Zertifikats in diese Datei verwendete Kennwort ein.					
Importdatei:				Durchruchen	
Kennwort:				13	
Name der digitalen ID:					
O Digitale ID in eine Datei exportieren					
Exportieren Sie die Informationen der digitalen ID in eine Datei. Geben Sie ein Kennwort ein, um diese Informationen besser zu schützen.					
Digitale ID:				Auswählen	
Dateiname:				Durchsuchen	
Kennwort:					
Bestätigen:					
Microsoft Internet Explorer 4.0-kompatibel (niedrige Sicherheitsstufe)					
Digitale ID vom Syster	n löschen				
			ОК	Abbrecher	n

Wählen Sie die passende Datei aus und geben Sie das Transportpasswort ein, welches Sie beim Beantragen des Nutzerzertifikates (s.o.) im BDD eingegeben haben.

Digitale ID importieren/exportieren X			
• Bestehende digitale ID aus einer Datei importieren Importieren Sie die digitale ID aus der Datei auf Ihren Computer. Geben Sie das beim Exportieren des Zertifikats in diese Datei verwendete Kennwort ein.			
Importdatei:	tu-bs.de_p12\21	5114 p12	Durchsuchen
Kennwort:	•••••		
Name der digitalen II):		5
Digitale ID in eine I	Datei exportieren		
Exportieren Sie die Informationen der digitalen ID in eine Datei. Geben Sie ein Kennwort ein, um diese Informationen besser zu schützen.			
Digitale ID:			Auswählen
Dateiname:			Durchsuchen
Kennwort:			
Bestätigen:			
Microsoft Internet Explorer 4.0-kompatibel (niedrige Sicherheitsstufe)			
Digitale ID vom System löschen			
		ОК	Abbrechen

Klicken Sie nun auf **[OK]**. Anschließend erscheint das Modul zum Import und Verwaltung des Zertifikats und des enthaltenen Schlüssels. Klicken Sie auf **[Sicherheitsstufe]**.

Import des priv	aten Austauschschlüssels	\times
	Eine Anwendung erstellt ein geschütztes Objekt.	
	Privater Schlüssel des CryptoAPI	
	Sie haben die mittlere Sicherheitsstufe gewählt.	
	OK Abbrechen Details	

Der Autor empfiehlt die Sicherheitsstufe Hoch, diese hat zur Folge, dass beim Signieren oder Verschlüsseln der Zugriff auf das Zertifikat und den enthaltenen Schlüssel nur über eine Passwortabfrage möglich ist. Wählen Sie die für Ihre Sicherheit notwendige Sicherheitsstufe aus.

Nach Klick auf **[Weiter]** und Abschluss des Imports können nun die eigentlichen Einstellungen zur Verwendung des Nutzerzertifikats zum Signieren und Verschlüsseln vorgenommen werden; Punkte 1 bis 3 ist das von uns empfohlene Alltagsverhalten.



In den Einstellungen müssen anschließend noch folgende Parameter angepasst werden:

(1) Es darf bzw. sollte kein Haken bei [Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln] gesetzt werden.

Hintergrund: es handelt sich primär um Signaturzertifikate.

(2) Es muss ein Haken bei [Ausgehenden Nachrichten digitale Signatur hinzufügen] gesetzt werden.

(3) Es muss ein Haken bei [Signierte Nachricht als Klartext senden] gesetzt werden.

Klicken Sie anschließend auf [Einstellungen].

Vertrauenswürdige Herausgeber Verschlüss Datenschutzoptionen Image: State	elte E-Mail-Nachrichten Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln Ausgehenden Nachrichten digitale Signatur hinzufügen Signierte Nachrichten als Klartext senden S/MIME-Bestätigung anfordern, wenn mit S/MIME signiert Einstellungen	
Programmgesteuerter Zugriff Digitale ID Logical ID Logi	s (Zertifikate) gitale IDs bzw. Zertifikate sind Dokumente, mit denen die Identität in elektronischen Transaktionen nachgewiesen werden nn. n GAL veröffentlichen Importieren/Exportieren xt lesen rdnachrichten im Nur-Text-Format lesen ital signierte Nachrichten im Nur-Text-Format lesen in freigegebenen Ordnern zulassen in Öffentlichen Ordnern zulassen	

Vergeben Sie in dem neuen Fenster einen Namen für diese Sicherheitseinstellung (wenn noch nicht automatisch erzeugt). Setzen Sie die entsprechenden Häkchen wie im folgenden Bild und wählen Sie das Signaturzertifikat. Bestätigen Sie mit **[OK]**.

Wichtig: Ändern Sie nach Hinzufügen den Hashalgorithmus von SHA-1 auf mindestens SHA-256 und vergewissern Sie sich bitte, dass der Verschlüsselungsalgorithmus auf AES 256-bit eingestellt ist.

Sicherheitseinstellungen ändern	×	in
Schemeisensteilungen andern		♥ Windows-Sicherheit 🖓 🗙
Bevorzugte Sicherheitseinstellungen		
Name der Sicherheitseinstellung:		Zentifiket heetikinen
S/MIME-TUBS	~	Zertifikat bestatigen
Kryptografieformat: S/MIME	~	Bestätigen Sie dieses Zertifikat, indem Sie auf "OK" klicken. Wenn
Standardeinstellung für dieses Format kryptografischer Nachrichten		es sich nicht um das richtige Zertifikat handelt, klicken Sie auf
Standardsicherheitseinstellung für alle kryntografischen Nachrichten	,	"Abbrechen".
Sicherheitskennzeichen Neu Löschen		21 114
Zertifikate und Algorithmen		
Signaturzertifikat: 21 114	Auswählen	Aussteller: GEANT Personal CA 4
Hashalgorithmus: SHA512 ~		Gültig ab: 16.04.2024 bis 17.04.2026
		Zertifikateigenschaften anzeigen
	Auswahlen	
Verschlüsselungsalgorithmus: AES (256-bit)		
signierten Nachrichten diese Zertifikate hinzufügen		OK Abbrechen
ОК	Abbrechen	

Wurde nun mit **[OK]** bestätigt, wird nun im Trust-Center das aktive S/MIME Profil angezeigt.

Sie können nun das Trust-Center und die Einstellungen schließen.



Revision #12 Created 16 April 2024 14:23:23 by Marius Kannicht Updated 16 August 2024 10:52:17 by Sandra Ulbrich