# RUB

# ANLEITUNG EINRICHTUNG EINER DIGITALEN SIGNATUR AM BEISPIEL VON OUTLOOK

## ALLGEMEINES

#### Wofür benötige ich eine digitale Signatur?

Bei E-Mails besteht grundsätzlich die Gefahr, dass Unbefugte den Inhalt und/oder die Absenderadresse manipulieren können. Damit könnten kriminelle Hacker in Ihrem Namen schadhafte Inhalte versenden. Nähere Informationen zum sogenannten Phishing bietet die Stabstelle IT-Sicherheit der RUB: <u>https://www.itsb.ruhr-uni-bochum.de/themen/email\_betrug.html</u>.

Sie können dies verhindern, indem Sie dem/der Empfänger\*in eindeutig und fälschungssicher nachweisen, dass die verschickte E-Mail tatsächlich von Ihnen stammt, indem Sie eine digitale Signatur benutzen. Technisch wird dies über ein persönliches Nutzerzertifikat realisiert, das IT.SERVICES allen Mitgliedern und Angehörigen der RUB zur Verfügung stellt.

#### Voraussetzung für die digitale Signatur

Voraussetzung für die Einrichtung einer digitalen Signatur ist ein persönliches Nutzerzertifikat, das Sie bei IT.SERVICES beantragen können. Informationen dazu finden Sie auf unserer <u>Webseite</u>.

#### **HINWEIS**

Wenn es Probleme mit der Authentifizierung oder Überprüfung der Signatur gibt, prüfen Sie, ob alle Zertifikate der Vertrauenskette installiert sind. Diese Zertifikatskette finden Sie <u>hier</u>.

Bei Fragen können Sie unsere Registrierungsstelle per E-Mail an <u>pki@ruhr-uni-bochum.de</u> oder telefonisch im Servicecenter unter 0234/32-24025 erreichen.

### MANUELLER IMPORT

#### Schritt 1

Starten Sie Outlook. Gehen Sie in der oberen Menüleiste auf "Datei" und dann auf "Optionen".



#### Schritt 2

Klicken Sie nun auf "Trust Center" und anschließend auf "Einstellungen für das Trust Center".

Juchen	Microsoft Outlook-Trust Center	
Sprache		
Barrierefreiheit	Das Trust Center enthält Einstellungen für Sicherheit und Datenschutz, um für die Sicherheit des Computers zu sorgen. Es wird davon abgeraten, diese Einstellungen	[
Erweitert	zu ändern.	Einstellungen für das Trust Center
Menüband anpassen		
Symbolleiste für den Schnellzugriff		
Add-Ins	_	
Trust Center		
	4	

#### Schritt 3

Klicken Sie nun auf "E-Mail-Sicherheit" in der linken Menüleiste und anschließend auf "Importieren/Exportieren...".

Irust Center		?	×
Vertrauenswürdige Herausgeber	Verschlüs	selte E-Mail-Nachrichten	
Formularbarierte Anmeldung	$\sim$	Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln	
E Mail Sicherheit	м	<u>Ausgehenden Nachrichten digitale Signatur hinzufügen</u>	
e-mail-sichemen		Signierte Nachrichten als Klartext senden	
Anlagenbehandlung		S/MIME-Bestatigung anfordern, wenn mit S/MIME signiert	
Automatischer Download		verarbeitung von symime-verschlusselten Nachrichten durch bestimmte verbundene Umgebungen blockieren	
Makroeinstellungen		Standardeinstellung: Einstellungen	
Programmgesteuerter Zugriff	Digitale II	Ds (Zertifikate)	
	8	Digitale IDs tow. Zertifikate sind Dokumente, mit denen die ldentität in elektronischen Transaktionen nachgewiesen werden kans. [In GAL veröffentlichen.] [Importieren/Zaportieren.]	
	Als Nur-T	ext lesen	
	🗌 Stan	dardnachrichten im Nur-Text-Format lesen	
		Ngital signierte Nachrichten im Nur-Text-Format Jesen	
	Skript in (	Ordnern	
	Skrip	nt in freigegebenen Ordnern zulassen	
	Skrip	nt in Öffentlichen Ordnern zulassen	

#### Schritt 4

Fügen Sie nun über "Durchsuchen" Ihr Nutzerzertifikat als Importdatei hinzu.

Geben Sie in das Eingabefeld "Kennwort" das Passwort ein, welches Sie bei der Beantragung (im Zertifikatsmanager) festgelegt haben.

Klicken Sie "OK" um das Zertifikat zu Importieren.

Bestehende digitale ID aus eine	er Datei importieren
mportieren Sie die digitale ID au ie das beim Exportieren des Zer cennwort ein.	s der Datei auf Ihren Computer. Geben tifikats in diese Datei verwendete
mportdatei:	Durchsuchen
ennwort:	
lame der digitalen ID:	
Digitale ID in eine Datei export	eren
) Digitale ID in eine Datei export xportieren Sie die Informationer ie ein Kennwort ein, um diese In	ieren n der digitalen ID in eine Datei. Geben formationen besser zu schützen.
) Digitale ID in eine Datei export xportieren Sie die Informationer ie ein Kennwort ein, um diese In Digitale ID:	ieren 1 der digitalen ID in eine Datei. Geben formationen besser zu schützen. Auswählen
Digitale ID in eine Datei exporti xportieren Sie die Informationer ie ein Kennwort ein, um diese In jigitale ID: vateiname:	ieren n der digitalen ID in eine Datei. Geben formationen besser zu schützen. Auswählen Durchsuchen
Digitale ID in eine Datei export: xportieren Sie die Informationer- ie ein Kennwort ein, um diese In bigitale ID: vateiname: ennwort:	ieren n der digitalen ID in eine Datei. Geben formationen besser zu schützen. Auswählen Durchsuchen
Digitale ID in eine Datei export: xportieren Sie die Informationeri ie ein Kennwort ein, um diese In Jigitale ID: ateiname: ennwort: estabigen:	eren n der digitalen ID in eine Datei. Geben formationen Desser zu schützen. Auswählen Durchsuchen
Digitale ID in eine Datei export xportieren Sie die Informationer le ein Kennwort ein, um diese In igitale ID: ateiname: ennwort: estätigen: Microsoft Internet Explorer 4/	eren der digitalen ID in eine Datei. Geben formationen besser zu schützen. Auswählen Durchsuchen 0-kompatibel (niedrige Sicherheitsstufe)

#### Schritt 5

Nun öffnet sich ein Fenster mit dem Titel "Import des privaten Austauschschlüssels".

Wählen Sie hier die gewünschte Sicherheitsstufe aus oder belassen Sie diese auf "mittlere Sicherheitsstufe" und bestätigen Sie mit "OK".

Import des priva	aten Austauschschlüssels X
	Eine Anwendung erstellt ein geschütztes Objekt.
	Privater Schlüssel des CryptoAPI
	Sie haben die mittlere <u>Sicherheitsstufe</u>
	OK Abbrechen Details

#### Schritt 6

Klicken Sie nun auf die Schaltfläche "Einstellungen…".

Anschließend klicken Sie auf "Auswählen…" neben "Signaturzertifikat" und wählen hier Ihr zuletzt importiertes Zertifikat aus. Gehen Sie genauso für "Verschlüsselungszertifikat" vor.

Wählen Sie im aktuellen Einstellungsfenster dann als Hashalgorithmus "SHA256" und als Verschlüsselungsalgorithmus "AES (256bit)". Bestätigen Sie zuletzt alle Einstellungen mit "OK".

omatischer Download	Verarbeitung	tatigung antordern, wenn mit 3 von S/MIME-verschlüsselten l	Nachrichten durch bestimmte verbi	undene Umge <mark>jrungen blockieren.</mark>
kroeinstellungen	<u>S</u> tandardeinstel	lung:		<ul> <li><u>E</u>instellungen</li> </ul>
grammgesteuerter Zugriff	Digitale IDs (Zertifikate)			
	Digitale IDs bzv werden kann. In GAL veröffe	w. Zertifikate sind Dokumente, entlichen	mit denen die Identität in elektron	ischen Transaktionen nachgewies
	Als Nur-Text lesen			
	Standardnachrichten ir	m Nur-Text-Format lesen		
cherheitseinste	llungen ändern			×
vorzugta Sichar	haitcainstallunga	n		
Name der Cicker	rensenistenunge			
Name der Siche	erneitseinstellung	•		
	E Einstallungann (	<u></u>	a sha a sa a sha a sha a sha a sha a sha sh	e) v
Meine S/MIME Kryptografiefor	mat: mat:	S/MIME s Format krypto	ografischer Nachrie	chten
Meine S/MIME Kryptografiefor Standardein Standardsic	mat: mstellung für diese herheitseinstellur	©r S/MIME es Format krypto ng für alle krypto	ografischer Nachrig	chten ichten
Meine S/MIME Kryptografiefor Standardein Standardsic Sicherhei	mat: mat: hstellung für diese herheitseinstellur itskennzeichen	S/MIME es Format krypto ng für alle krypto Neu	ografischer Nachrie ografischen Nachri Löschen	chten
Meine S/MIME Kryptografiefor Standardeir Standardsic Sicherhei Zertifikate und	mat: nstellung für diese herheitseinstellur itskennzeichen Algorithmen —	G/MIME sr Format krypto ng für alle krypto Neu	ografischer Nachrig ografischen Nachrig Löschen	chten
Meine S/MIME Kryptografiefor Standardein Standardsic Sicherhei Zertifikate und Signaturzertifik	rmat: hstellung für diese herheitseinstellur itskennzeichen Algorithmen — cat:	©r S/MIME es Format krypto ng für alle krypto Neu	ografischer Nachrie ografischen Nachrie Löschen	chten ichten Auswählen
Meine S/MIME Kryptografiefor Standardein Standardsic Sicherhei Zertifikate und Signaturzertifik Hashalgorithm	rmat: Instellung für diese herheitseinstellur itskennzeichen Algorithmen cat:	Gring für alle krypte S/MIME ag für alle krypte Neu SHA256	ografischer Nachrie ografischen Nachri Löschen	chten ichten
Meine S/MIME Kryptografiefor Standardeir Standardsic Sicherhei Zertifikate und Signaturzertifik Hashalgorithm Verschlüsselun	rmat: instellung für diese herheitseinstellur itskennzeichen Algorithmen cat: us:	Gring für alle krypte Neu SHA256	ografischer Nachrie ografischen Nachri Löschen	chten ichten Auswählen
Meine S/MIME Kryptografiefor Standardein Standardsic Sicherhei Zertifikate und Signaturzertifik Hashalgorithm Verschlüsselun Verschlüsselun	Einsteilung für diese herheitseinstellur itskennzeichen Algorithmen cat: us: gszertifikat: gsalgorithmus:	S/MIME es Format krypto ng für alle krypto Neu SHA256 AES (256-bit)	ografischer Nachrio ografischen Nachri Löschen	chten ichten Auswählen
Meine S/MIME Kryptografiefor Standardein Standardsic Sicherhei Zertifikate und Signaturzertifik Hashalgorithm Verschlüsselun Verschlüsselun	rmat: instellung für diese herheitseinstellur itskennzeichen Algorithmen cat: us: gszertifikat: gsalgorithmus: lachrichten diese	S/MIME es Format krypto ng für alle krypto Neu SHA256 AES (256-bit) Zertifikate hinzo	ografischer Nachrio ografischen Nachri Löschen v ufügen	chten ichten Auswählen

#### Schritt 7

Um zu prüfen, ob Ihre E-Mails signiert werden, erstellen Sie eine neue E-Mail und überprüfen, ob unter "Optionen" das Feld "Signieren" aktiv ist. Möchten Sie eine E-Mail unsigniert versenden, können Sie das Feld "Signieren" manuell deaktivieren.

on 日 り Datei Nachri	Ĉ) î ↓ ≂ Unb	enannt - Nachrich	nt (HTML)	Suchen			-	×
Designs A Scl	rben * Einingen Zeite hriftarten * Seitenfarbe ekte * *	Bcc		Abstimmungsschaltfl. verwenden ~	Zustellungsbestät: anfordern Lesebestät: anfordern	Gesendetes Element Üb speichem unter ~	ermittlung Antworten verzögern richten an	×
D Senden	Von v An Cc	@ruhr-uni-bo	schum.de	<b>4</b>				_
	Betreff							Î

### UMGANG MIT SIGNIERTEN E-MAILS

Sie können Signaturen von empfangenen E-Mails überprüfen, indem Sie auf das Schleifen-Symbol klicken und sich damit weitere Informationen zum Zertifikat anzeigen lassen.

Unter "Details" erhalten Sie weitere Informationen über das Zertifikat. Wir empfehlen, das Häkchen bei "Vor Fehlern [...] warnen" zu setzen. E-Mails mit ungültigen Zertifikaten werden dann nicht direkt geöffnet (siehe nächster Abschnitt "Ungültige Signatur").



# UNGÜLTIGE SIGNATUREN

Ungültige Signaturen erkennen Sie daran, dass in der E-Mail nicht das Schleifensymbol, sondern ein Warndreieck angezeigt wird. Haben Sie, wie auf der vorherigen Seite empfohlen, das Häkchen bei "Vor Fehlern…" gesetzt, werden diese E-Mails nicht direkt geöffnet, sondern zunächst die Informationen zur Signatur. Dies schützt Sie davor E-Mails mit schadhaftem Inhalt (Drive-by-Attacken) zu öffnen.

Prüfen Sie den Fehler genau und klicken erst dann auf "Nachricht anzeigen" oder öffnen Sie die E-Mail gegebenenfalls erst nach Rücksprache mit dem Absender. Möglicherweise ist das Zertifikat lediglich abgelaufen.

		662
KT	< @ruhr-uni-bochum.de>	
gniert von	wrun-un-bochun.de	19.01.2024
		4
		1
Digitale Sign	atur: Ungültig	×
etreff:		
/on:		
igniert von:		
0	Die digitale Signatur dieser Nachrich	t ist ungültig oder
	nicht vertrauenswürdig.	the angulary out
	Klicken Sie auf "Details", um weitere	Informationen zum
	Zertifikat zu erhalten, das für die dig	itale Signatur der
	Nachheite verwendet wurde.	
		Details
Vor Fehler	n in digital signierten Nachrichten vor	dem Öffnen warnen.
		CebliaRan
		Schlieben

#### KONTAKT & HILFE:

Bei Fragen und Problemen wenden Sie sich an unseren Helpdesk unter: its-helpdesk@ruhr-uni-bochum.de

**IT.**SERVICES

STAND: 30. JULI 2024