



**Zertifikate
Thunderbird**

**Einbindung eines Nutzerzertifikates in
Mozilla Thunderbird**

**Certificates
Thunderbird**

**Integration of a user certificate in
Mozilla Thunderbird**

Erstellt und getestet mit Windows 10 Education 22H2 (Build 19045.3208) und Mozilla Thunderbird 115.0 (64-Bit)

Created and tested with Windows 10 Education 22H2 (Build 19045.3208) and Mozilla Thunderbird 115.0 (64-bit)

19.07.2023

kim.uni-hohenheim.de | kim@uni-hohenheim.de

Inhalt

Vorbereitungen / Preparations.....	1
Import des Nutzerzertifikates in Thunderbird / Importing the user certificate into Thunderbird	1
Nachrichten Signieren und/oder Verschlüsseln / Sign and/or encrypt messages	7

Vorbereitungen / Preparations

Bevor Sie mit der Einbindung des Nutzerzertifikates beginnen muss bereits das E-Mail-Konto mit Ihren Hohenheimer Benutzerdaten eingerichtet sein!

Ebenso muss Ihnen die Zertifikatsdatei vorliegen, die mit der E-Mail-Adresse, die in Thunderbird bereits eingerichtet ist, konfiguriert ist bzw. beantragt wurde!

Beides wird bei uns auf kim.uni-hohenheim.de unter „Formulare, Anleitungen & Downloads“ beschrieben.

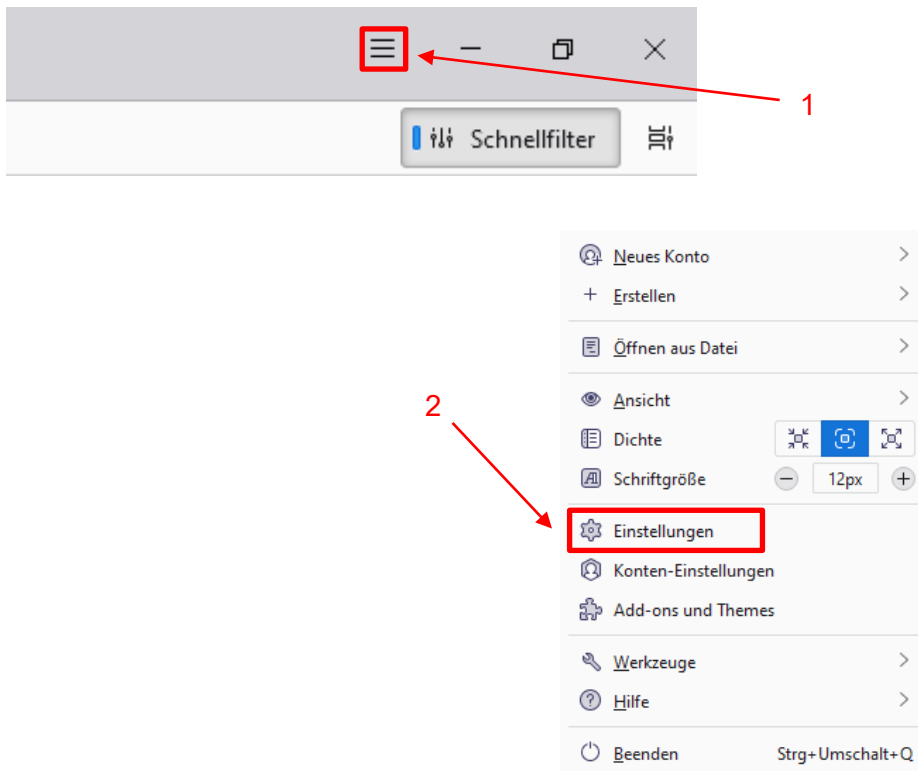
Before you start integrating the user certificate, the e-mail account must already be set up with your Hohenheim user data!

You must also have the certificate file configured or requested with the e-mail address already set up in Thunderbird!

Both are described on our website kim.uni-hohenheim.de under "Forms, Instructions & Downloads".

Import des Nutzerzertifikates in Thunderbird / Importing the user certificate into Thunderbird

Wählen Sie in Thunderbird oben rechts das „Burger-Menü“. Anschließend wählen Sie „Einstellungen“.
In Thunderbird, select the "Burger" menu at the top right. Then select "Settings".



Kommunikations-, Informations- und Medienzentrum (KIM)

Wählen Sie „Datenschutz & Sicherheit“ und scrollen zum Bereich „Zertifikate“. Wählen Sie dort den Button „Zertifikate verwalten...“.

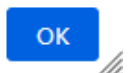
Select "Privacy & Security" and scroll to the "Certificates" section. There, select the button "Manage certificates...".

The screenshot shows the Thunderbird settings window. On the left sidebar, the 'Datenschutz & Sicherheit' (Privacy & Security) option is highlighted with a red box and labeled '3'. The main content area shows the 'Zertifikate' (Certificates) section. The 'Zertifikate verwalten...' (Manage certificates...) button is highlighted with a red box and labeled '4'. Other visible options include 'Antivirus' and 'Kryptographie-Module verwalten...' (Manage cryptographic modules...).

Wählen Sie den Reiter „Ihre Zertifikate“ und klicken Sie auf den Button „Importieren...“.

Select the tab "Your certificates" and click on the button "Import...".

The screenshot shows the 'Zertifikatverwaltung' (Certificate Management) window. The 'Ihre Zertifikate' (Your certificates) tab is highlighted with a red box and labeled '5'. Below the tabs, there is a table with columns: 'Zertifikatsname', 'Kryptographie-Modul', 'Seriennummer', and 'Gültig bis'. Below the table, the 'Importieren...' (Import...) button is highlighted with a red box and labeled '6'. Other buttons include 'Ansehen...', 'Sichern...', 'Alle sichern...', and 'Löschen...'.



Kommunikations-, Informations- und Medienzentrum (KIM)

Geben Sie nun den Speicherort für die Zertifikatsdatei (.p12) an und geben Sie unter „Kennwort“ das Passwort ein, das Sie im Zuge des Zertifikatbezugs selbst gesetzt haben.

Bestätigen Sie mit „Anmelden“.

Now enter the storage location for the certificate file (.p12) and enter the password you set yourself in the course of obtaining the certificate under "Password".

Confirm with "Log in".

Passwort erforderlich - Mozilla Thunderbird



Bitte geben Sie das Passwort ein, das zur Verschlüsselung dieses Zertifikatbackups verwendet wurde:

7

8

Schließen Sie das Fenster „Zertifikatverwaltung“ mit „OK“.

Close the "Certificate Management" window with "OK".

Zertifikatverwaltung

Ihre Zertifikate

Authentifizierungs-Entscheidungen

Personen

Server

Zertifizierungsstellen

Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:

Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis	
GEANT Vereniging				
██████████	das Software-Sicherheits...	██████████	Samstag, 4. Juli 2026	

Ansehen...

Sichern...

Alle sichern...

Importieren...

Löschen...

OK

9

Kommunikations-, Informations- und Medienzentrum (KIM)

Scrollen Sie nun weiter in den Absatz „Ende-zu-Ende-Verschlüsselung für E-Mails“, einen Absatz weiter wie den zuvor verwendeten Absatz „Zertifikate“. Klicken Sie den Button „Konten-Einstellungen“.

Now scroll further into the paragraph "End-to-end encryption for e-mails", one paragraph further like the previously used paragraph "Certificates". Click the button "Account settings".

zu löschen), bevor diese im Posteingang gespeichert werden. Dies kann bei POP-Konten vor Datenverlust schützen, benötigt aber mehr Zeit.

Antivirus-Software ermöglichen, eingehende Nachrichten unter Quarantäne zu stellen

Zertifikate

Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:

Automatisch eins wählen Jedes Mal fragen

Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen

Zertifikate verwalten...
Kryptographie-Module verwalten...

Ende-zu-Ende-Verschlüsselung für E-Mails

Richten Sie E-Mail-Konten und Identitäten für die Ende-zu-Ende-Verschlüsselung in den Konten-Einstellungen ein.

Konten-Einstellungen

Automatische Verwendung der Verschlüsselung

Thunderbird kann Sie dabei unterstützen, indem es die Verschlüsselung während des Verfassens einer E-Mail automatisch aktiviert oder deaktiviert. Die automatische Aktivierung/Deaktivierung basiert auf der Verfügbarkeit von gültigen und akzeptierten Schlüsseln oder Zertifikaten der Korrespondenten.

Verschlüsselung automatisch aktivieren, wenn möglich
 Verschlüsselung automatisch deaktivieren, wenn sich die Empfänger ändern und eine Verschlüsselung nicht mehr möglich ist
 Eine Benachrichtigung anzeigen, wenn die Verschlüsselung automatisch deaktiviert wird

Automatische Entscheidungen können durch manuelles Aktivieren oder Deaktivieren der Verschlüsselung beim Verfassen einer Nachricht außer Kraft gesetzt werden. Hinweis: Die Verschlüsselung wird immer automatisch aktiviert, wenn auf eine verschlüsselte Nachricht geantwortet wird.

Nun wechseln Sie in die „Ende-zu-Ende-Verschlüsselung“ und klicken im Absatz „S/MIME“ auf den ersten „Auswählen...“-Button.

S/MIME

Persönliches Zertifikat für digitale Unterschrift:

Auswählen... Leeren

Persönliches Zertifikat für Verschlüsselung:

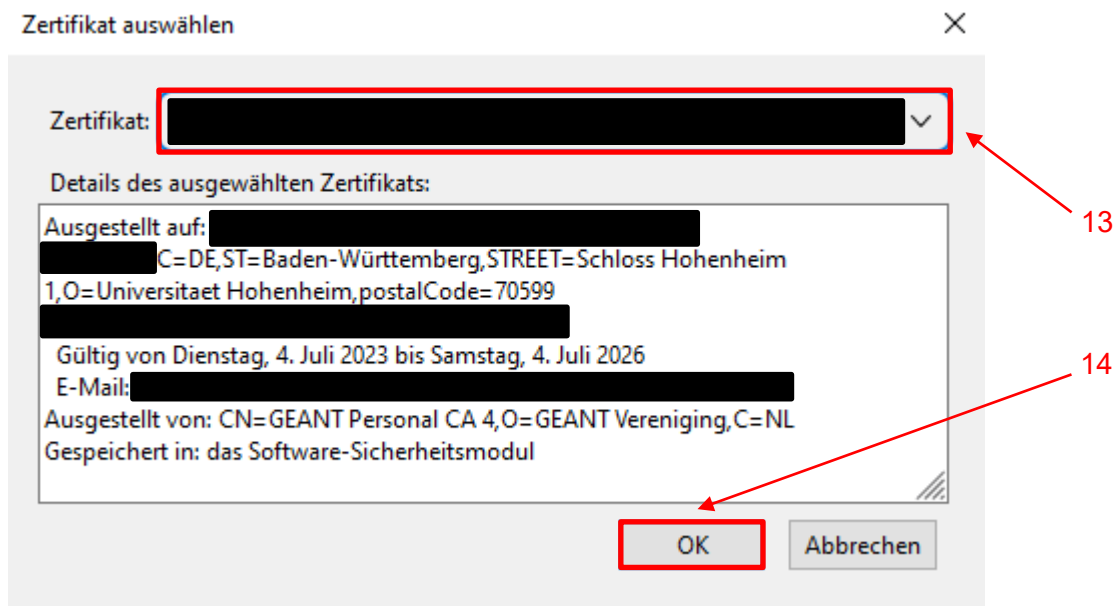
Auswählen... Leeren

S/MIME-Zertifikate verwalten S/MIME-Kryptographie-Module verwalten

Kommunikations-, Informations- und Medienzentrum (KIM)

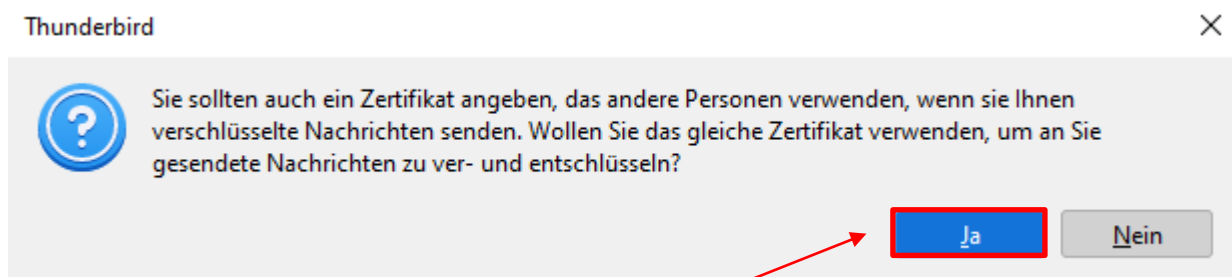
Wählen Sie (vor allem, falls Sie mehrere Zertifikate importiert haben) das passende Zertifikat aus. Hinweise für das passende Zertifikat finden Sie unter „Details des ausgewählten Zertifikats.“. Bestätigen Sie mit „OK“.

Select the appropriate certificate (especially if you have imported several certificates). You will find instructions for the appropriate certificate under "Details of the selected certificate:". Confirm with "OK".



Nun Wichtig! Wählen Sie im folgenden Fenster „Ja“ aus, um das Zertifikat auch für die evtl. notwendige Verschlüsselung zu hinterlegen.

Now Important! In the following window, select "Yes" to also store the certificate for any necessary encryption.





Kommunikations-, Informations- und Medienzentrum (KIM)

Um Standardmäßig jede E-Mail zu signieren (empfohlen), setzen Sie bitte noch den Haken im Absatz „Senden von Nachrichten – Standardeinstellungen“ bei „Unverschlüsselte Nachrichten digital unterschreiben“.

To sign every e-mail by default (recommended), please tick the box "Digitally sign unencrypted messages" in the paragraph "Sending messages - default settings".

Senden von Nachrichten - Standardeinstellungen

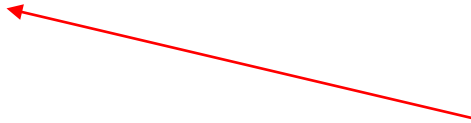
Ohne Ende-zu-Ende-Verschlüsselung ist der Inhalt Ihrer Nachrichten für Ihren E-Mail-Anbieter leicht zugänglich und kann auch Bestandteil einer Massenüberwachung werden.

- Verschlüsselung für neue Nachrichten nicht verwenden
- Verschlüsselung für neue Nachrichten verwenden

Die Verschlüsselung kann für einzelne Nachrichten deaktiviert werden.

Eine digitale Unterschrift ermöglicht den Empfängern zu verifizieren, dass die Nachricht von Ihnen gesendet und der Inhalt nicht verändert wurde. Verschlüsselte Nachrichten sind standardmäßig immer signiert.

- Unverschlüsselte Nachrichten digital unterschreiben



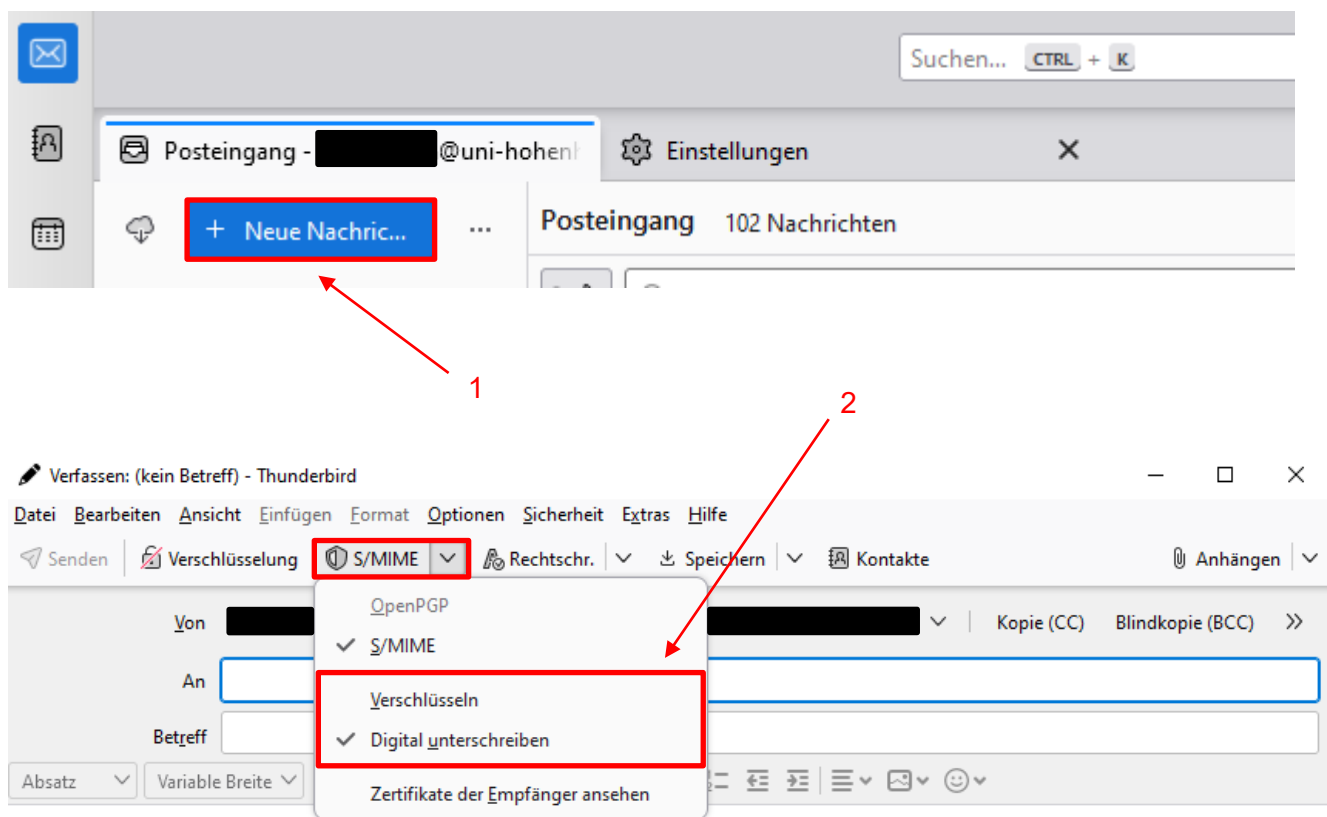
Nachrichten Signieren und/oder Verschlüsseln / Sign and/or encrypt messages

Wenn Sie eine „Neue Nachricht“ verfassen, haben Sie nun im Menüreiter „S/MIME“ die Möglichkeit zu „Signieren“ und/oder zu „Verschlüsseln“.

Ebenso verhält es sich beim Antworten oder Weiterleiten von E-Mails.

When you compose a "New Message", you now have the option to "Sign" and/or "Encrypt" in the "S/MIME" menu tab.

The same applies when replying to or forwarding e-mails.





Sollten unerwartete Probleme auftreten stehen wir Ihnen gerne am
KIM IT-Service-Desk
Biogebäude 1, Garbenstraße 30, 1. UG
per E-Mail unter
kim-it@uni-hohenheim.de
zur Verfügung

Should unexpected problems arise, we will be happy to help you at the
KIM IT-Service-Desk
Biogebäude 1, Garbenstraße 30, 1. Basement
email us at
kim-it@uni-hohenheim.de