UNIVERSITÄT HOHENHEIM

Kommunikations-, Informations- und Medienzentrum (KIM)

Zertifikate Adobe Acrobat DC

Certificates Adobe Acrobat DC

Signieren (Unterschreiben, Zertifizieren und Verschlüsseln) von PDF-Dateien in Adobe Acrobat / Sign (Sign, Certify and Encrypt) PDF files in Adobe Acrobat

18.08.2023

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

Inhalt

Allgemeines, Beschreibung und Voraussetzungen / General, description and requirements

Mit einem Nutzerzertifikat, dass Sie ebenfalls auf den KIM-Seiten (https://kim.uni-hohenheim.de/nutzerzertifikat) beantragen können ist es möglich PDF-Dateien in Adobe Acrobat elektronisch zu signieren. Voraussetzung für die Einbindung ist, dass Sie sowohl die Zertifikatsdatei (.p12-Datei) bereits erstellt haben und Sie Zugriff darauf haben, als auch das zugehörige Passwort bekannt ist.

With a user certificate, which you can also apply for on the KIM pages (https://kim.uni-hohenheim.de/en/nutzerzertifikat), it is possible to sign PDF files electronically in Adobe Acrobat. The prerequisite for integration is that both the certificate file (.p12 file) has already been created and you have access to it, and the associated password is known.

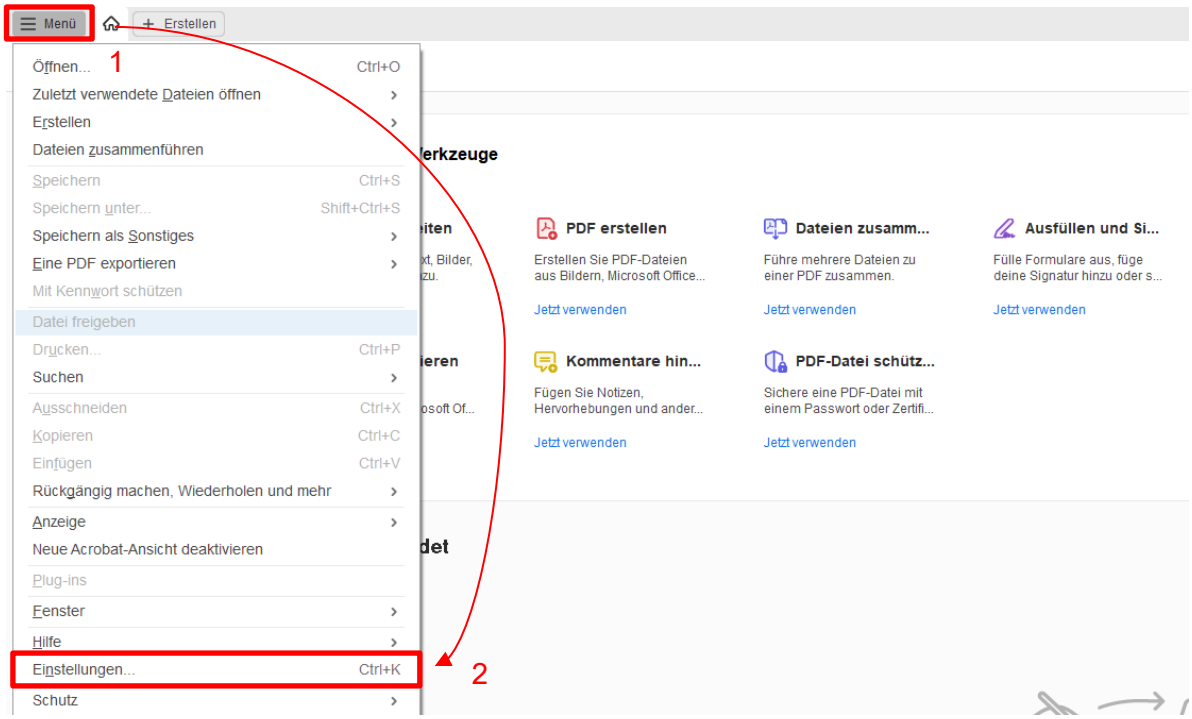
! **Alle folgenden Schritte müssen sowohl vom Ersteller der Signatur, als auch vom Empfänger der PDF-Datei durchgeführt werden. Ansonsten wird ein Fehler beim Empfänger ausgegeben!** !

All of the following steps must be performed by both the creator of the signature and the recipient of the PDF file. Otherwise an error will be issued to the recipient!

Einstellungen konfigurieren / Configure settings

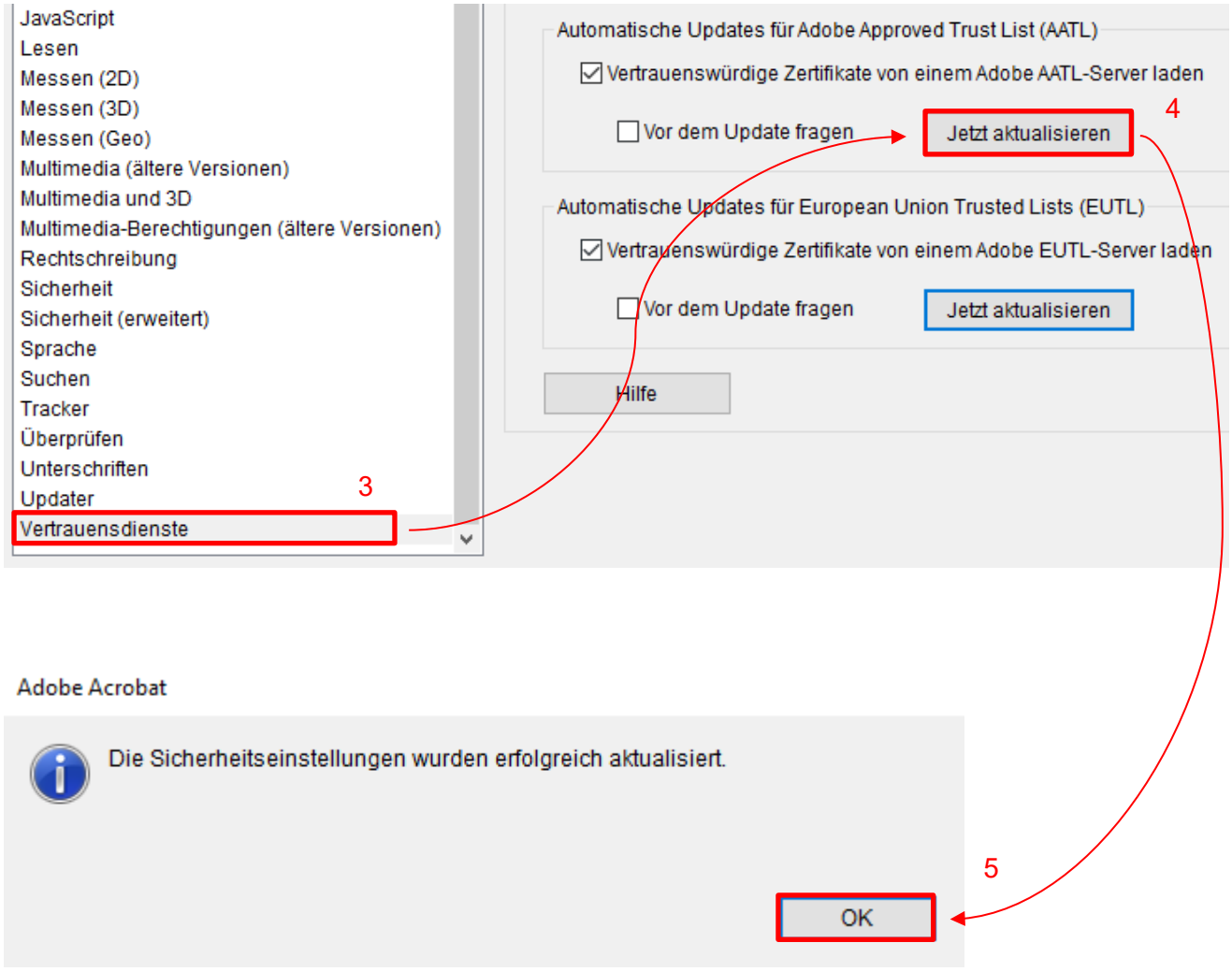
Adobe Acrobat starten. Links oben das Menü (Burgersymbol) öffnen und Einstellungen wählen.

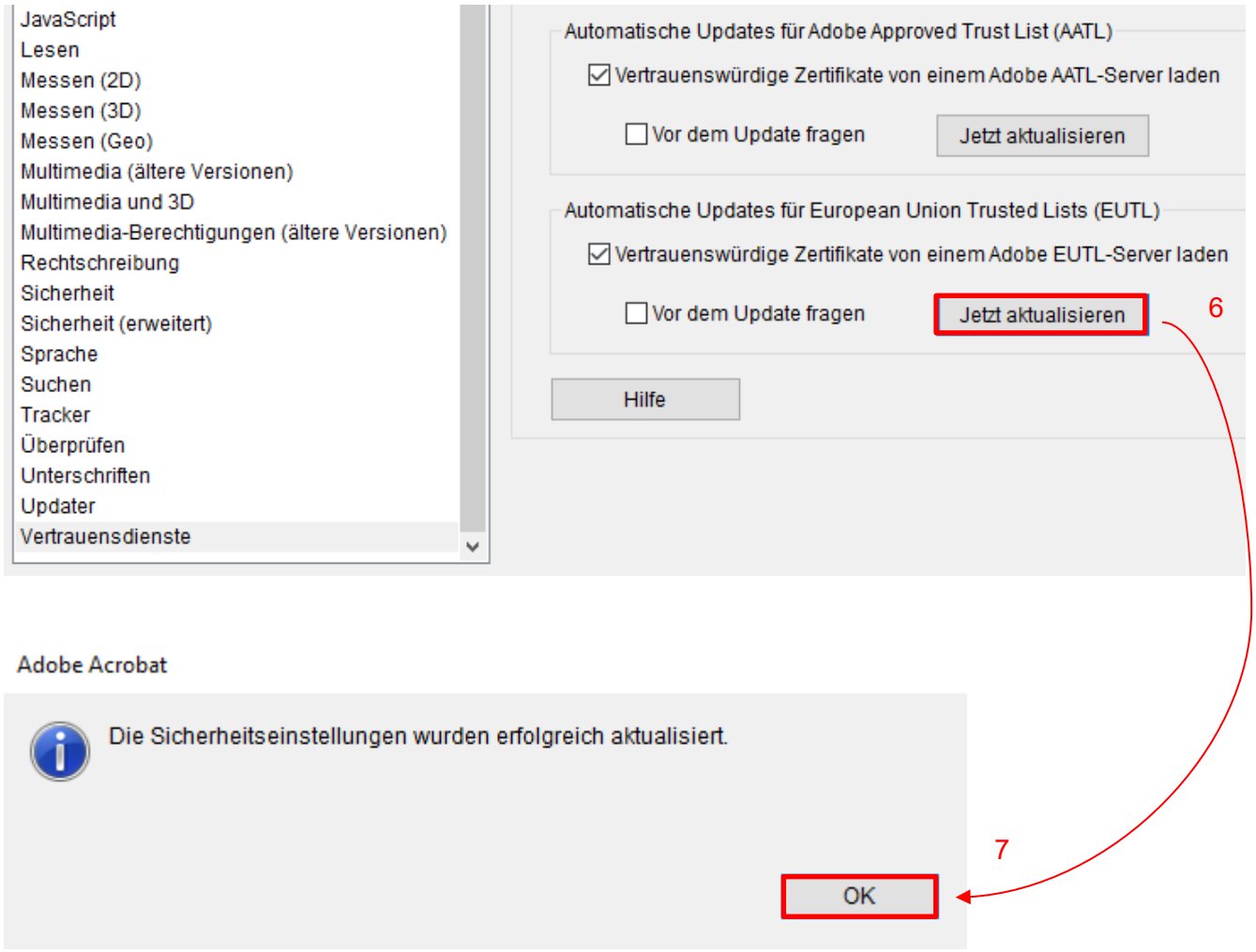
Start Adobe Acrobat. In the upper left corner, open the menu (burger icon) and select Settings.



Wählen Sie in den „Einstellungen“ unter den „Kategorien:“ „Vertrauensdienste“. Klicken Sie auf „Jetzt aktualisieren“ bei „Automatische Updates für Adobe Approved Trust List (AATL)“ und „Automatische Updates für European Union Trusted Lists (EUTL) und bestätigen Sie diese jeweils mit „OK“.

Select "Trust Services" in the "Settings" under the "Categories:". Click "Update now" for "Automatic updates for Adobe Approved Trust List (AATL)" and "Automatic updates for European Union Trusted Lists (EUTL)" and confirm each with "OK".

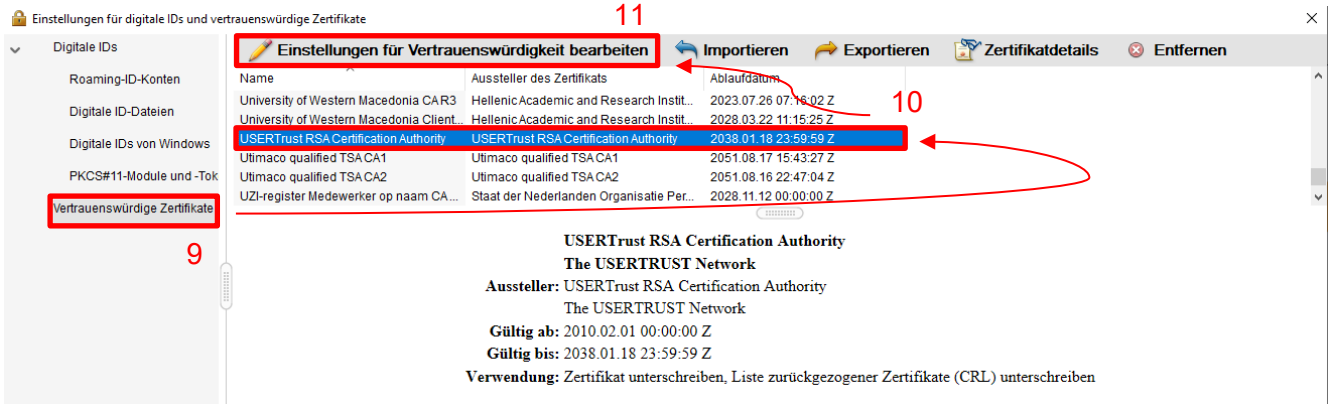


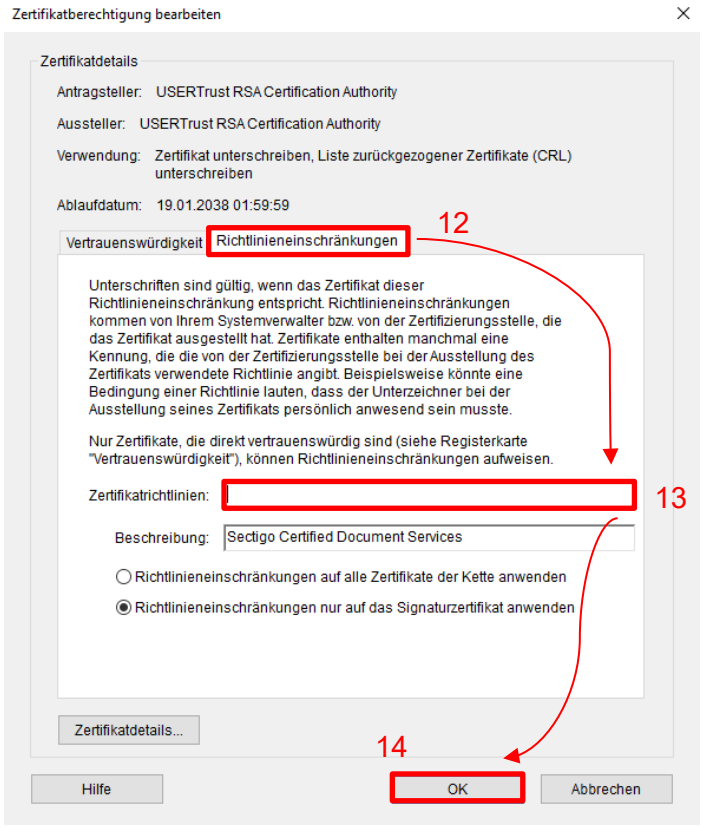


Löschen Sie nun die Richtlinieneinstellungen der USERTrust RSA Certification Authority über die “Einstellungen” → “Unterschriften” → “Identitäten und Vertrauenswürdige Zertifikate” über den Button “Weitere…” und im sich nun öffnenden Fenster unter “Vertrauenswürdige Zertifikate” und Scrollen bis zum o.g. Eintrag. Klicken Sie nun auf “Einstellungen für Vertrauenswürdigkeit bearbeiten” und wählen Sie den Karteireiter “Richtlinienbeschränkungen”. Löschen Sie alle vorhandenen Richtlinienbeschränkungen aus dem Feld “Zertifikatrichtlinien und bestätigen Sie mit “OK”.

Now delete the policy settings of the USERTrust RSA Certification Authority via the "Settings" → "Signatures" → "Identities and Trusted Certificates" via the button "More..." and in the window that now opens under "Trusted Certificates" and scroll down to the entry mentioned above. Now click on "Edit trust settings" and select the "Policy restrictions" tab. Delete all existing policy restrictions from the "Certificate policies" field and confirm with "OK".

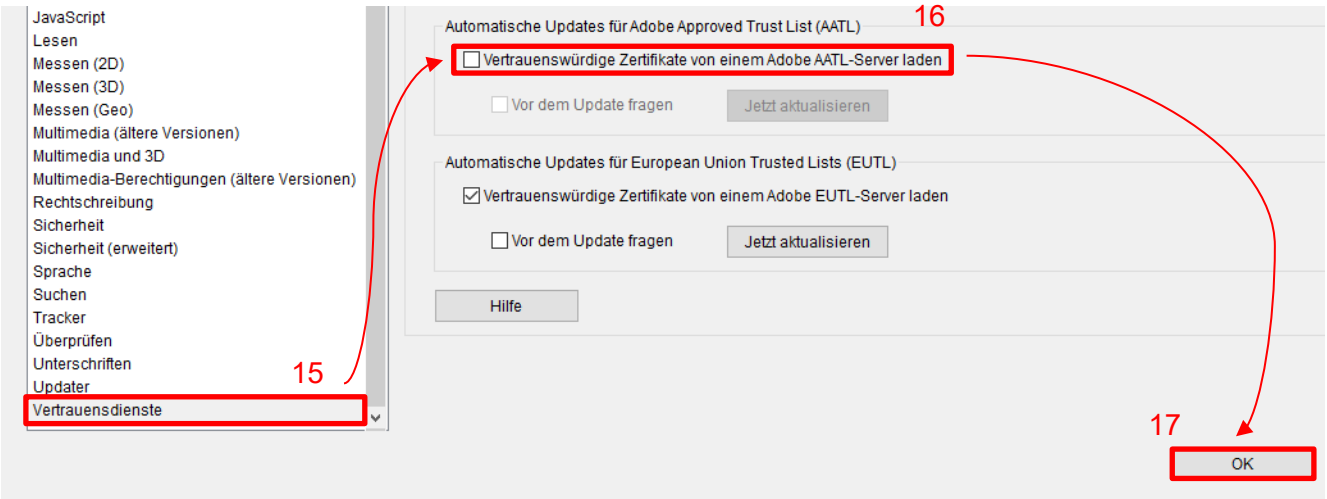

Inhaltsbearbeitung
Internet
JavaScript
Lesen
Messen (2D)
Messen (3D)
Messen (Geo)
Multimedia (ältere Versionen)
Multimedia und 3D
Multimedia-Berechtigungen (ältere Versionen)
Rechtschreibung
Sicherheit
Sicherheit (erweitert)
Sprache
Suchen
Tracker
Überprüfen
Unterschriften
Updater
7
Identitäten und vertrauenswürdige Zertifikate
• Erstellen und Verwalten von Identitäten für die Unterzeichnung
• Verwalten von Anmeldeinformationen für die Vertrauenswürdigkeit von Dokumenten
Weitere...
8
Zeitstempel für Dokumente
• Konfigurierung der Servereinstellungen für Zeitstempel
Weitere...


Einstellungen für digitale IDs und vertrauenswürdige Zertifikate
11
Digitale IDs
Roaming-ID-Konten
Digitale ID-Dateien
Digitale IDs von Windows
PKCS#11-Module und -Tok
Vertrauenswürdige Zertifikate
9
Einstellungen für Vertrauenswürdigkeit bearbeiten
Importieren
Exportieren
Zertifikatdetails
Entfernen
Name
Aussteller des Zertifikats
Ablaufdatum
University of Western Macedonia CAR3
Hellenic Academic and Research Instit...
2023.07.26 07:16:02 Z
University of Western Macedonia Client...
Hellenic Academic and Research Instit...
2028.03.22 11:15:25 Z
USERTrust RSA Certification Authority
USERTrust RSA Certification Authority
2038.01.18 23:59:59 Z
Utimaco qualified TSA CA1
Utimaco qualified TSA CA1
2051.08.17 15:43:27 Z
Utimaco qualified TSA CA2
Utimaco qualified TSA CA2
2051.08.16 22:47:04 Z
UZI-register Medewerker op naam CA...
Staat der Nederlanden Organisatie Per...
2028.11.12 00:00:00 Z
10
USERTrust RSA Certification Authority
The USERTRUST Network
Aussteller: USERTrust RSA Certification Authority
The USERTRUST Network
Gültig ab: 2010.02.01 00:00:00 Z
Gültig bis: 2038.01.18 23:59:59 Z
Verwendung: Zertifikat unterschreiben, Liste zurückgezogener Zertifikate (CRL) unterschreiben


Zertifikatberechtigung bearbeiten
Zertifikatdetails
Antragsteller: USERTrust RSA Certification Authority
Aussteller: USERTrust RSA Certification Authority
Verwendung: Zertifikat unterschreiben, Liste zurückgezogener Zertifikate (CRL) unterschreiben
Ablaufdatum: 19.01.2038 01:59:59
Vertrauenswürdigkeit
Richtlinieneinschränkungen
12
Unterschriften sind gültig, wenn das Zertifikat dieser Richtlinieneinschränkung entspricht. Richtlinieneinschränkungen kommen von Ihrem Systemverwalter bzw. von der Zertifizierungsstelle, die das Zertifikat ausgestellt hat. Zertifikate enthalten manchmal eine Kennung, die die von der Zertifizierungsstelle bei der Ausstellung des Zertifikats verwendete Richtlinie angibt. Beispielsweise könnte eine Bedingung einer Richtlinie lauten, dass der Unterzeichner bei der Ausstellung seines Zertifikats persönlich anwesend sein musste.
Nur Zertifikate, die direkt vertrauenswürdig sind (siehe Registerkarte "Vertrauenswürdigkeit"), können Richtlinieneinschränkungen aufweisen.
Zertifikatrichtlinien:
13
Beschreibung:
Sectigo Certified Document Services
Richtlinieneinschränkungen auf alle Zertifikate der Kette anwenden
Richtlinieneinschränkungen nur auf das Signaturzertifikat anwenden
Zertifikatdetails...
14
Hilfe
OK
Abbrechen

Deaktivieren Sie nun noch die Updates für die AATL.

Now deactivate the updates for the AATL.



Einrichtung der digitalen Signatur (Unterschrift) / Digital signature setup (signature)

In den “Einstellungen” wählen Sie “Unterschriften” und klicken auf den Button “Weitere…” bei “Identitäten und vertrauenswürdige Zertifikate”.

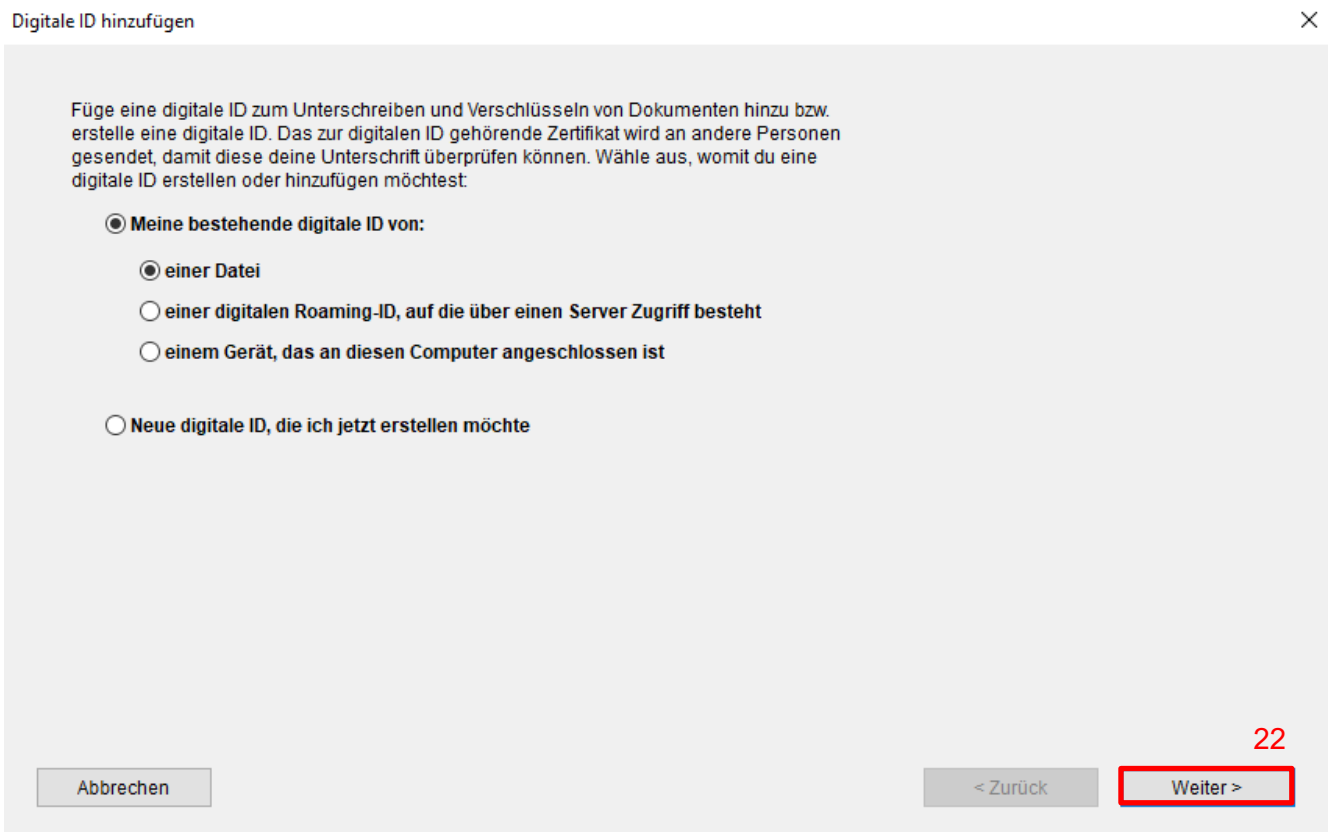
In the "Settings" select "Signatures" and click on the "More..." button at "Identities and trusted certificates".

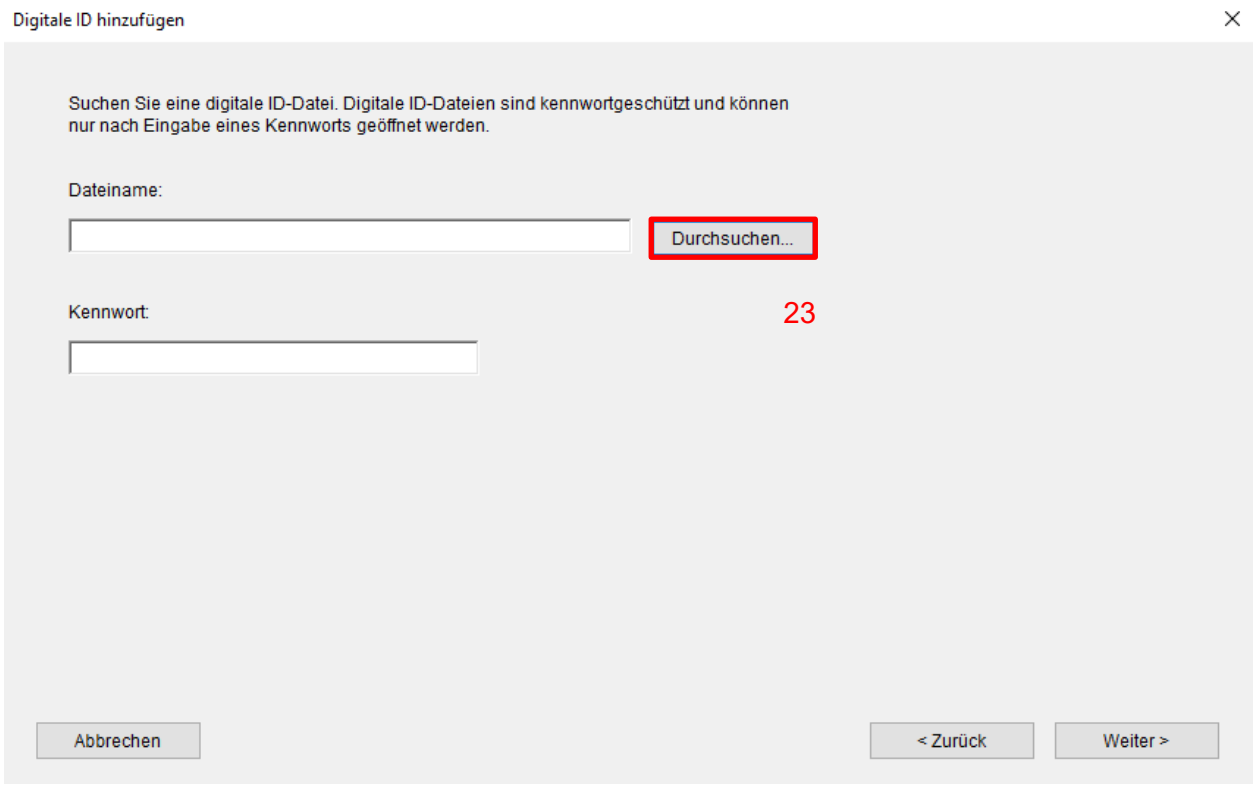
Wählen Sie nun “Digitale IDs” und “ID hinzufügen”.

Now select "Digital IDs" and "Add ID".

Wählen Sie nun Ihre Zertifikatsdatei.

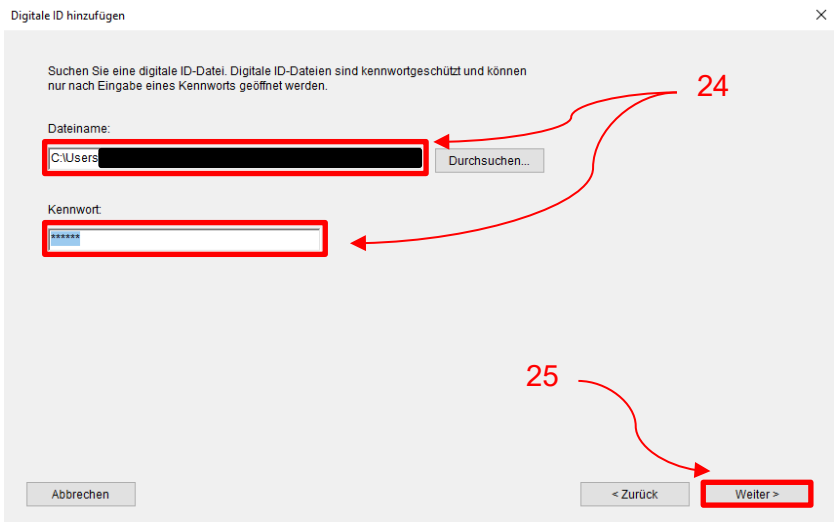
Now select your certificate file.


Digitale ID hinzufügen
Füge eine digitale ID zum Unterschreiben und Verschlüsseln von Dokumenten hinzu bzw. erstelle eine digitale ID. Das zur digitalen ID gehörende Zertifikat wird an andere Personen gesendet, damit diese deine Unterschrift überprüfen können. Wähle aus, womit du eine digitale ID erstellen oder hinzufügen möchtest:
Meine bestehende digitale ID von:
einer Datei
einer digitalen Roaming-ID, auf die über einen Server Zugriff besteht
einem Gerät, das an diesen Computer angeschlossen ist
Neue digitale ID, die ich jetzt erstellen möchte
22
Abbrechen
< Zurück
Weiter >



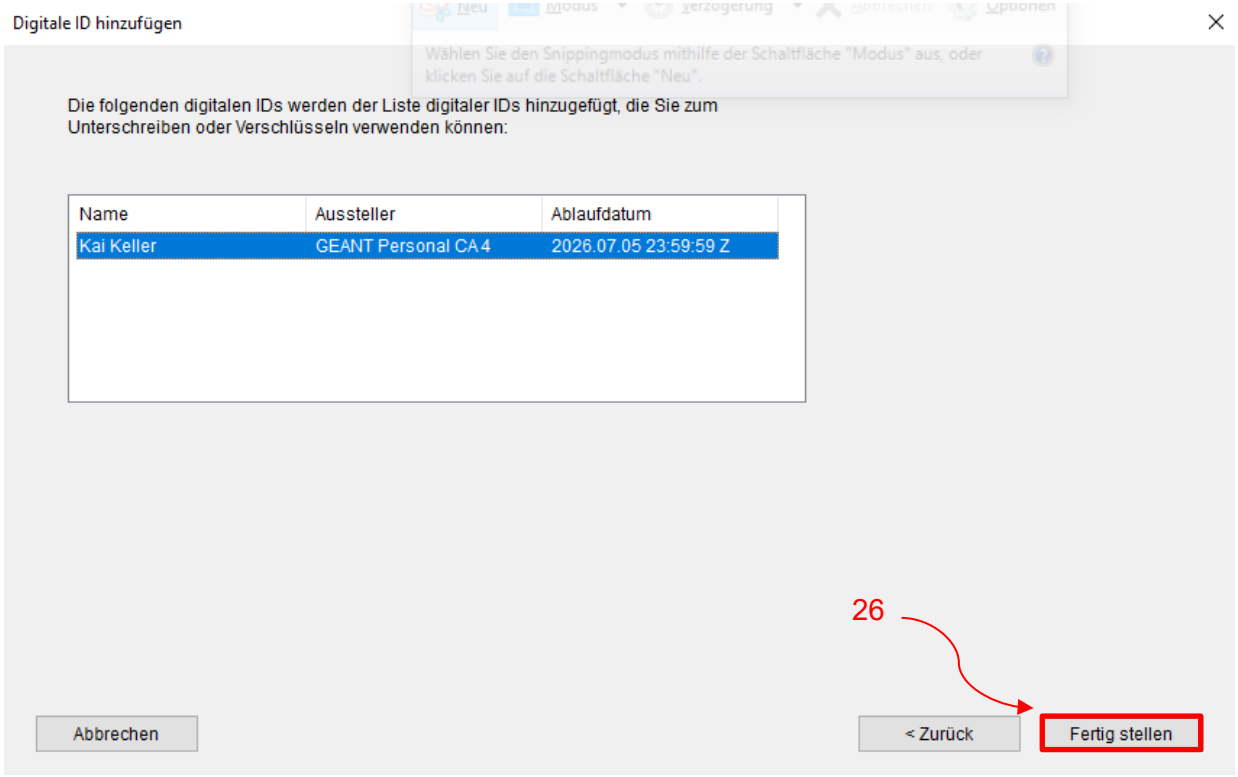
Geben Sie nun den Speicherplatz an, in dem sich Ihre Zertifikatsdatei befindet. Anschließend geben Sie noch das Passwort ein, mit dem Sie die Zertifikatsdatei beim Erstellen gesichert haben und klicken auf “Weiter”.

Now enter the location where your certificate file is located. Then enter the password that you used to secure the certificate file when you created it and click "Next".



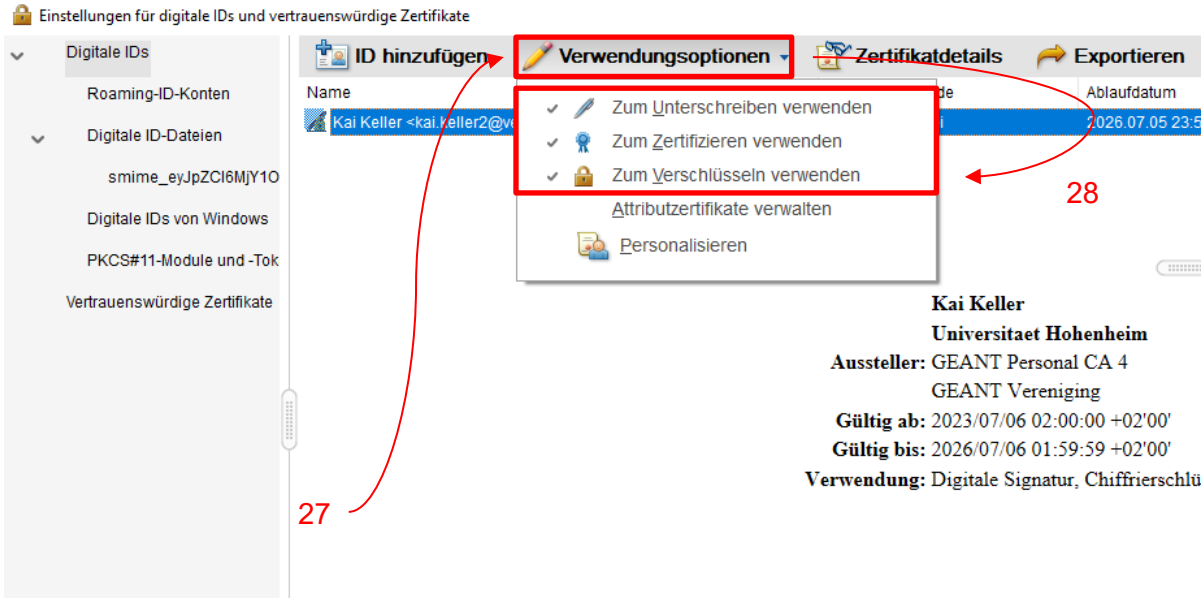
Nun wird Ihnen die Digitale ID angezeigt. Bestätigen Sie mit “Fertig stellen”.

Now the Digital ID is displayed. Confirm with "Finish".



Bei Erfolg wird Ihnen nun nochmals die ID angezeigt. Unter “Verwendungsoptionen” aktivieren Sie bitte noch “Zum Unterschreiben verwenden”, “Zum Zertifizieren verwenden” und “Zum Verschlüsseln verwenden”.

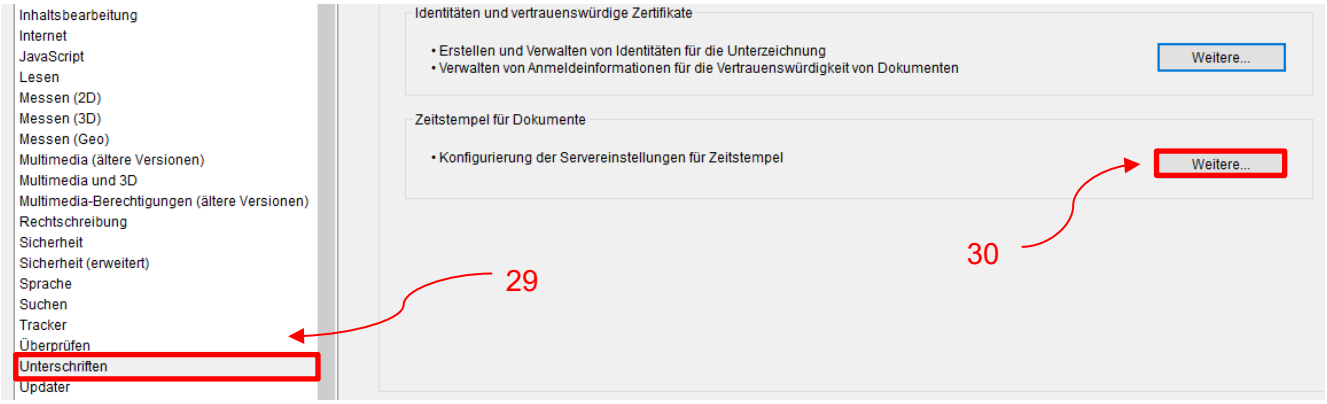
If successful, the ID will now be displayed again. Under "Usage options" please activate "Use for signing", "Use for certifying" and "Use for encrypting".



Zeitstempeldienst einrichten / Set up timestamp service

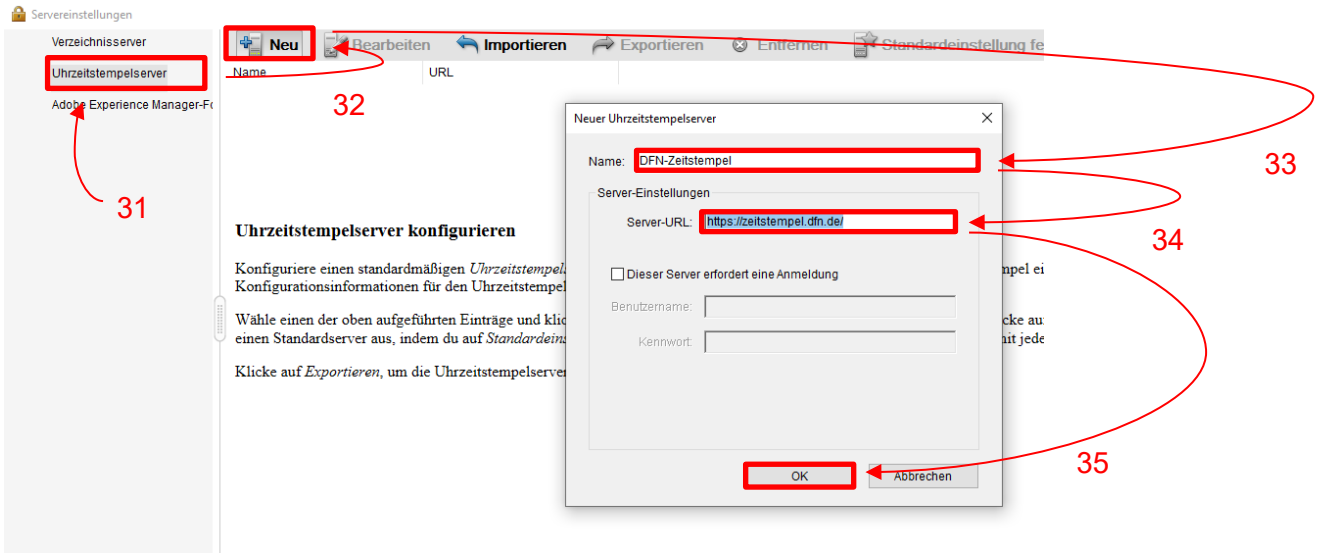
Zusätzlich kann ein zertifizierter Zeitstempel zur Unterschrift hinzugefügt warden. Wechseln Sie hierzu wieder in die “Einstellungen” und wählen Sie die Kategorie “Unterschriften”. Recht unter “Zeitstempel für Dokumente” wählen Sie “Weitere…”.

In addition, a certified time stamp can be added to the signature. To do this, switch back to the "Settings" and select the "Signatures" category. Right under "Timestamps for documents" select "More...".



Wählen Sie nun “Uhrzeitstempelserver” und legen über “Neu” einen neuen Uhrzeitstempelserver an. Verwenden Sie folgende Konfiguration:
Name: DFN-Zeitstempel
Server-URL: https://zeitstempel.dfn.de/

Now select "Time stamp server" and create a new time stamp server via "New".
Use the following configuration:
Name: DFN timestamp
Server URL: https://zeitstempel.dfn.de/


Servereinstellungen
Verzeichnisserver
Uhrzeitstempelserver
Adobe Experience Manager-Fe
Neu
Bearbeiten
Importieren
Exportieren
Entfernen
Standardeinstellung fe
Name
URL
31
32
33
34
35
Uhrzeitstempelserver konfigurieren
Konfiguriere einen standardmäßigen Uhrzeitstempel
Konfigurationsinformationen für den Uhrzeitstempel
Wähle einen der oben aufgeführten Einträge und klic
einen Standardserver aus, indem du auf Standardeins
Klicke auf Exportieren, um die Uhrzeitstempelserver
Neuer Uhrzeitstempelserver
Name: DFN-Zeitstempel
Server-Einstellungen
Server-URL: https://zeitstempel.dfn.de/
Dieser Server erfordert eine Anmeldung
Benutzername:
Kennwort:
OK
Abbrechen

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
KIM IT-Service-Desk
Biogebäude 1, Garbenstraße 30, 1. Basement
email us at
kim-it@uni-hohenheim.de