



**Zertifikate
Adobe
Acrobat DC**

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

**Certificates
Adobe
Acrobat DC**

15.08.2024

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

Inhalt

Signieren (Unterschreiben, Zertifizieren und Verschlüsseln) von PDF-Dateien in Adobe Acrobat / Sign (Sign, Certify and Encrypt) PDF files in Adobe Acrobat	1
Allgemeines, Beschreibung und Voraussetzungen / General, description and requirements	1
Einstellungen konfigurieren / Configure settings	1
Einrichtung der digitalen Signatur (Unterschrift) / Digital signature setup (signature)	6
Zeitstempeldienst einrichten / Set up timestamp service	10

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.

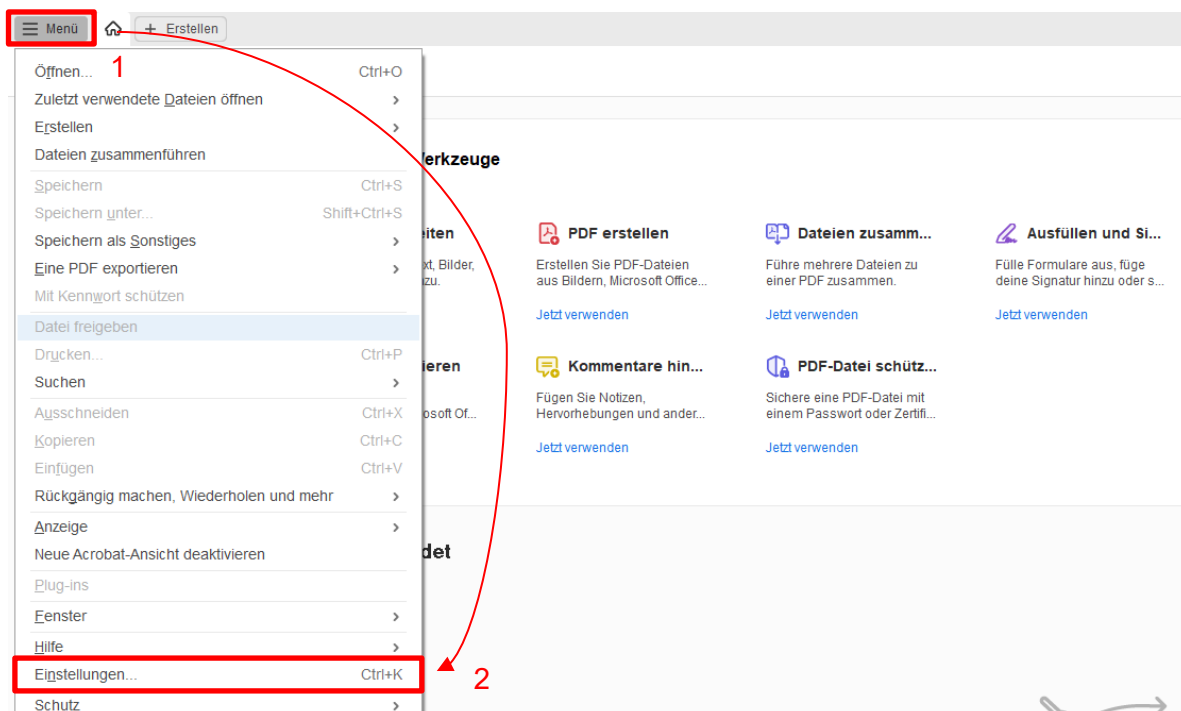
Alle folgenden Schritte müssen sowohl vom Ersteller der Signatur, als auch vom Empfänger der PDF-Datei durchgeführt werden. Ansonsten wird ein Fehler beim Empfänger ausgegeben!

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.

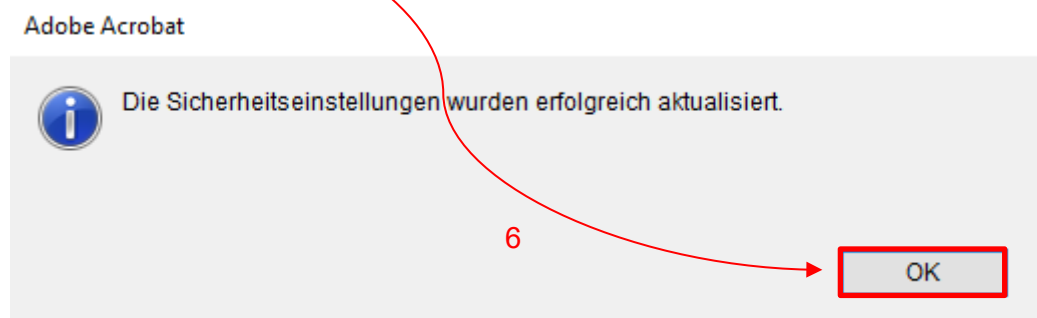
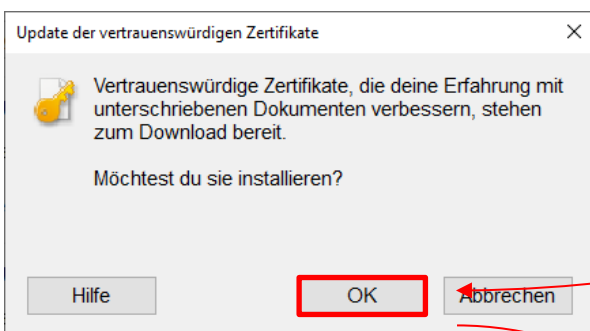
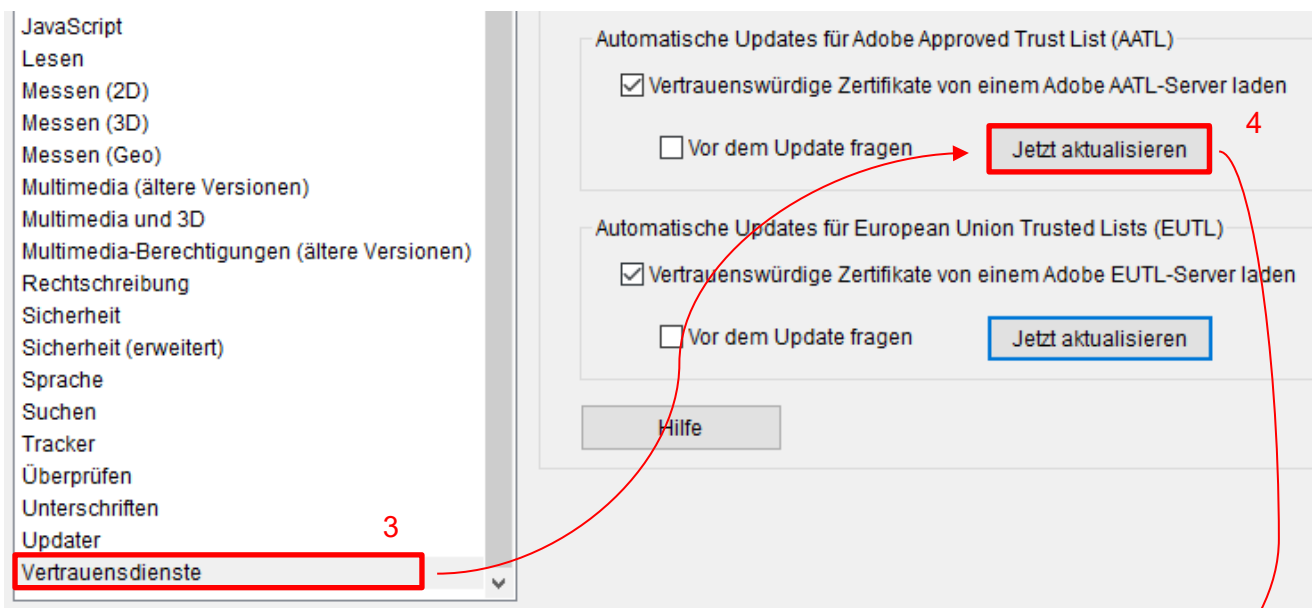
Start Adobe Acrobat. In the upper left corner, open the menu (burger icon) and select Settings.



Kommunikations-, Informations- und Medienzentrum (KIM)

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".



Kommunikations-, Informations- und Medienzentrum (KIM)

The image shows a sequence of three screenshots from Adobe Acrobat:

- Top Screenshot:** The 'Vertrauensdienste' (Trust Services) settings panel. Under 'Automatische Updates für Adobe Approved Trust List (AATL)', the checkbox 'Vertrauenswürdige Zertifikate von einem Adobe AATL-Server laden' is checked. The 'Jetzt aktualisieren' button is highlighted with a red box and labeled '7'.
- Middle Screenshot:** A dialog box titled 'Update der vertrauenswürdigen Zertifikate'. It contains the text: 'Vertrauenswürdige Zertifikate, die deine Erfahrung mit unterschriebenen Dokumenten verbessern, stehen zum Download bereit. Möchtest du sie installieren?'. The 'OK' button is highlighted with a red box and labeled '8'.
- Bottom Screenshot:** An 'Adobe Acrobat' notification message: 'Die Sicherheitseinstellungen wurden erfolgreich aktualisiert.' The 'OK' button is highlighted with a red box and labeled '9'.

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

Kommunikations-, Informations- und Medienzentrum (KIM)

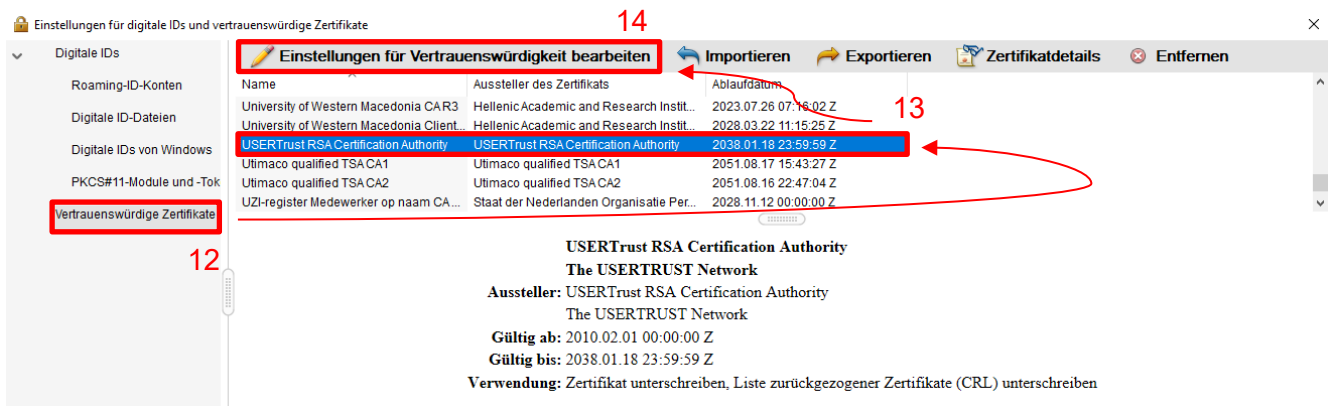
now opens under "Trusted Certificates" and scroll down to the entry mentioned above. Now click on "Edit trust settings" and select the "Policy restrictions" tab. Delete all existing policy restrictions from the "Certificate policies" field and confirm with "OK".



10

11

This screenshot shows the Windows Settings application. On the left sidebar, the 'Unterschriften' (Signatures) option is highlighted with a red box and labeled '10'. The main window displays the 'Identitäten und vertrauenswürdige Zertifikate' (Identities and trusted certificates) section. A red arrow points from the 'Unterschriften' option to the 'Weiter...' button in the 'Identitäten und vertrauenswürdige Zertifikate' section, which is labeled '11'.



12

13

14

This screenshot shows the 'Einstellungen für digitale IDs und vertrauenswürdige Zertifikate' (Settings for digital IDs and trusted certificates) window. The 'Vertrauenswürdige Zertifikate' (Trusted certificates) option is highlighted in the left sidebar and labeled '12'. The main window shows a table of trusted certificates. The 'Einstellungen für Vertrauenswürdigkeit bearbeiten' (Edit trust settings) button is highlighted with a red box and labeled '14'. A red arrow points from this button to the 'Ablaufdatum' (Expiration date) column of the table, which is labeled '13'. The table contains the following data:

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

Below the table, the details for the selected 'USERTrust RSA Certification Authority' certificate are displayed:

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

Kommunikations-, Informations- und Medienzentrum (KIM)

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** 15

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: 16

Beschreibung: Sectigo Certified Document Services

Richtlinieneinschränkungen auf alle Zertifikate der Kette anwenden
 Richtlinieneinschränkungen nur auf das Signaturzertifikat anwenden

Zertifikatdetails...

Hilfe **OK** 17 Abbrechen

Deaktivieren Sie nun noch die Updates für die AATL.

Now deactivate the updates for the AATL.

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
Vertrauensdienste 18

Automatische Updates für Adobe Approved Trust List (AATL) 19

Vertrauenswürdige Zertifikate von einem Adobe AATL-Server laden

Vor dem Update fragen

Automatische Updates für European Union Trusted Lists (EUTL)

Vertrauenswürdige Zertifikate von einem Adobe EUTL-Server laden

Vor dem Update fragen

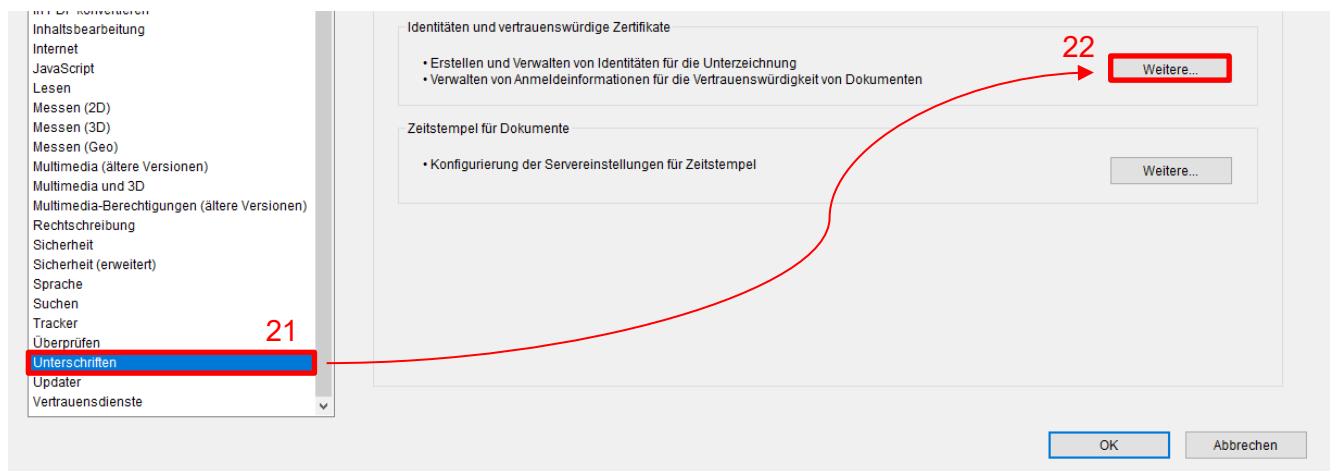
Hilfe

OK 20

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

Abbrechen

< Zurück

Weiter >

25

Digitale ID hinzufügen

×

Suchen Sie eine digitale ID-Datei. Digitale ID-Dateien sind kennwortgeschützt und können nur nach Eingabe eines Kennworts geöffnet werden.

Dateiname:

Durchsuchen...

Kennwort:

26

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".

Digitale ID hinzufügen

×

Suchen Sie eine digitale ID-Datei. Digitale ID-Dateien sind kennwortgeschützt und können nur nach Eingabe eines Kennworts geöffnet werden.

Dateiname:

Durchsuchen...

Kennwort:

27

28

Abbrechen

< Zurück

Weiter >

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

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

Kommunikations-, Informations- und Medienzentrum (KIM)

Digitale ID hinzufügen

Die folgenden digitalen IDs werden der Liste digitaler IDs hinzugefügt, die Sie zum Unterschreiben oder Verschlüsseln verwenden können:

Name	Aussteller	Ablaufdatum
Kai Keller	GEANT Personal CA 4	2026.07.05 23:59:59 Z

Abbrechen < Zurück Fertig stellen

29 (red arrow pointing to 'Fertig stellen')

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".

Einstellungen für digitale IDs und vertrauenswürdige Zertifikate

Digitale IDs

- Roaming-ID-Konten
- Digitale ID-Dateien
 - smime_eyJpZCI6MjY1O
- Digitale IDs von Windows
- PKCS#11-Module und -Tok
- Vertrauenswürdige Zertifikate

ID hinzufügen Verwendungsoptionen Zertifikatdetails Exportieren

Name	Aussteller	Ablaufdatum
Kai Keller <kai.keller2@w	GEANT Personal CA 4	2026.07.05 23:59:59 Z

30 (red arrow pointing to 'Verwendungsoptionen')

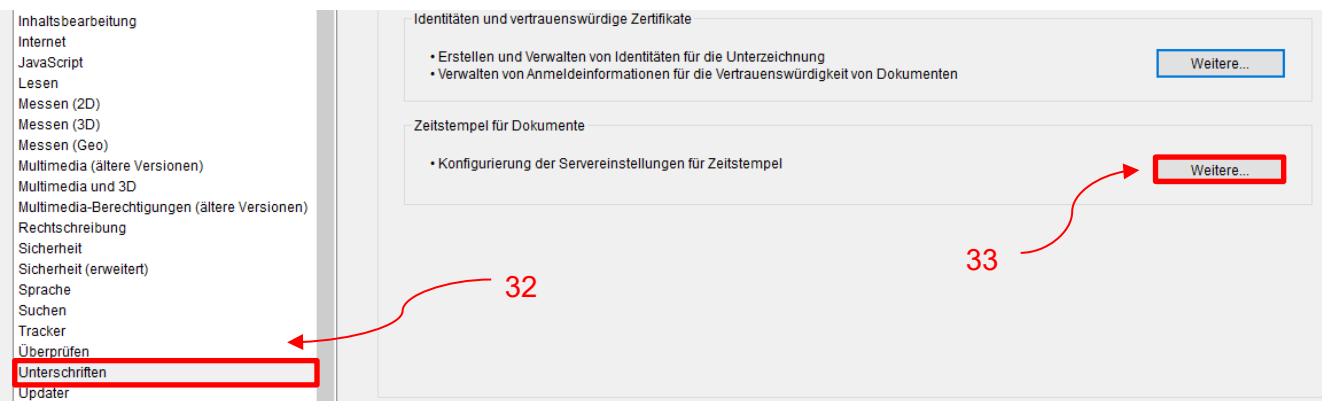
31 (red arrow pointing to 'Zum Verschlüsseln verwenden')

Kai Keller
Universitaet Hohenheim
Aussteller: GEANT Personal CA 4
GEANT Vereniging
Gültig ab: 2023/07/06 02:00:00 +02'00'
Gültig bis: 2026/07/06 01:59:59 +02'00'
Verwendung: Digitale Signatur, Chiffrierschlü

Zeitstempeldienst einrichten / Set up timestamp service

Zusätzlich kann ein zertifizierter Zeitstempel zur Unterschrift hinzugefügt werden. Wechseln Sie hierzu wieder in die "Einstellungen" und wählen Sie die Kategorie "Unterschriften". Rechts 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 "Uhrzeitstempelservers" und legen über "Neu" einen neuen Uhrzeitstempelservers an. Verwenden Sie folgende Konfiguration:

Name: DFN-Zeitstempel

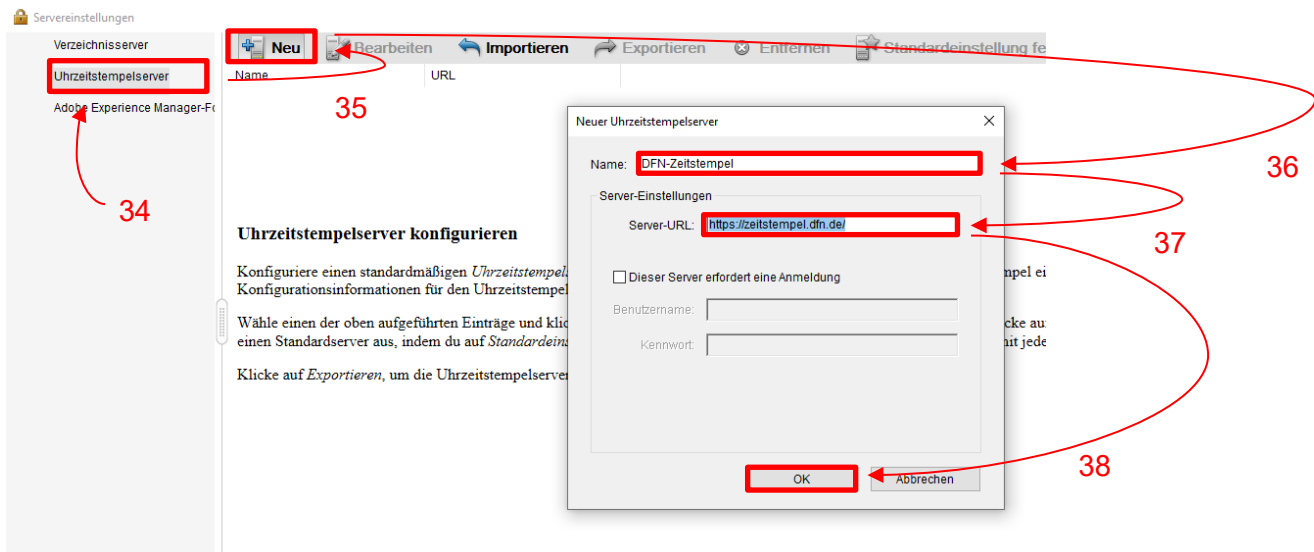
Server-URL: <https://zeitstempel.dfn.de/>

Now select "Time stamp server" and create a new time stamp server via "New".

Use the following configuration:

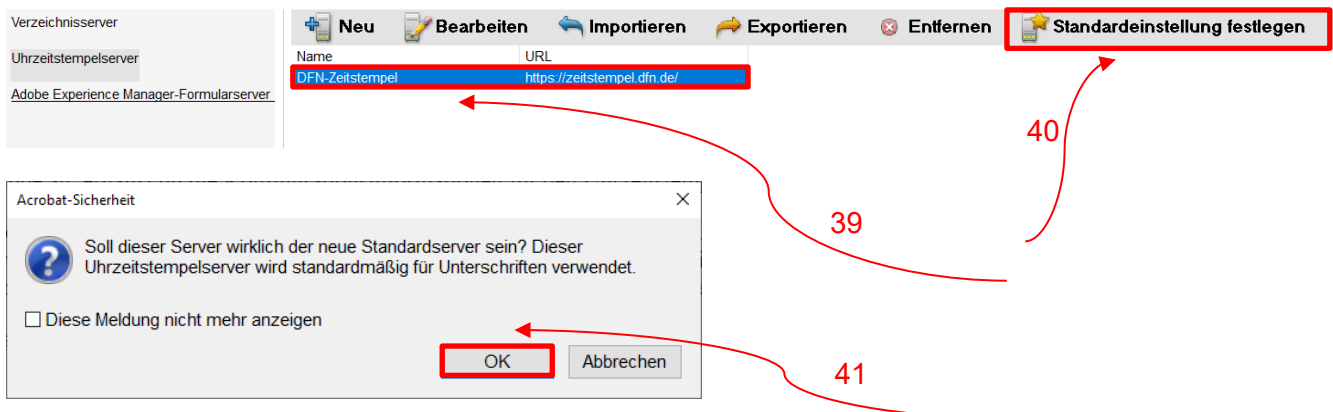
Name: DFN timestamp

Server URL: <https://zeitstempel.dfn.de/>



Nun muss dieser Zeitstempelserver noch als „Standard“ gesetzt werden. Markieren Sie hierzu den neu angelegten Uhrzeitstempelserver und wählen Sie „Standardeinstellungen festlegen“. Bestätigen Sie mit „OK“.

This time stamp server must now be set as the “Default”. To do this, select the newly created timestamp server and select “Set default settings”. Confirm with “OK”.



Probleme / Lösungen

Das Burgermenü wie oben beschrieben ist nicht sichtbar!?

Es gibt eine neue und alte Acrobat Ansicht. Die neue Ansicht beinhaltet das Burgermenü, die alte Ansicht nicht. Ändern können Sie dies über die Menüleiste „Anzeige“ → „Neue Acrobat-Ansicht aktivieren“.

There is a new and old Acrobat view. The new view contains the burger menu, the old view does not. You can change this via the menu bar “Display” → “Activate new Acrobat view”.



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