

ElsterAuthenticator Benutzerhandbuch

Version 57.0.0

17.08.2023

Inhalt

1. Einleitung	3
2. Quickstart	3
2.1. Unterstützte Plattformen	3
2.2. Installation	4
2.2.1. Windows/macOS	4
2.2.1.1. Graphische Installation	4
2.2.1.2. Silent Installation	10
2.2.2. Linux Ubuntu 22.04 (64 Bit)	11
2.3. Deinstallation	12
2.3.1. Graphische Deinstallation	12
2.3.2. Silent Deinstallation	12
2.4. Konfiguration	13
2.4.1. Nutzung eines Sicherheitssticks	15
2.4.2. Nutzung einer Signaturkarte	17
2.4.3. Nutzung eines Proxys für den Internet-Zugriff	18
2.4.4. Erweitert	20
2.4.5. Logging	21
2.4.6. Diagnose-Informationen erstellen	22
2.5. Passwort ändern	23
2.5.1. Sicherheitsstick	23
2.5.1.1. Passwort ändern	23
2.5.1.2. Stick entsperren mittels PUK	23
2.5.2. Signaturkarten	24
3. Funktionsweise	24
3.1. Beispiel: Login bei Mein ELSTER	25
3.1.1. Login unter Windows Server	26
3.1.2. Kontoaktivierung unter Windows Server	26
3.2. Zertifikatswechsel	27
3.3. Wechsel der Signaturkarte	27

3.4. Wechsel von Signaturkarte zu Sicherheitsstick	29
3.5. Wechsel des Sicherheitssticks	31
3.6. Herunterladen von Dateien.	33

1. Einleitung

Die Nutzung von Mein ELSTER zusammen mit Sicherheitssticks oder Signaturkarten ist nur zusammen mit dem ElsterAuthenticator möglich, da verschiedene Browser die Verwendung von Java-Applets nicht mehr unterstützen werden oder die Applet-Technologie bereits entfernt haben (beispielsweise Google Chrome).

Zur Nutzung von Sicherheitssticks oder Signaturkarten (hier übergreifend als „Token“ bezeichnet) muss ein Benutzer folgende Schritte durchführen:

- ElsterAuthenticator von Mein ELSTER downloaden und installieren
- ElsterAuthenticator vor der Nutzung mit Mein ELSTER starten
- das zu verwendende Token über die ElsterAuthenticator-Oberfläche konfigurieren
- eine Registrierung / einen Login durchführen

Mein ELSTER bietet hier stets eine Schaltfläche „Weiter mit ElsterAuthenticator“ an. Wenn Sie auf diese Schaltfläche klicken, erscheint das ElsterAuthenticator-Fenster im Vordergrund und fordert von Ihnen eine Aktion an (wie zum Beispiel die Eingabe des Passworts Ihres Tokens), um den Login durchzuführen / eine Datenübermittlung zu authentisieren / Postfachnachrichten zu entschlüsseln etc.

Aus Gründen der Übersichtlichkeit werden alle Erklärungen und Beispiele anhand von Mein ELSTER beschrieben. Diese gelten ebenso für Mein BOP.

Im ElsterAuthenticator wird keine Unterscheidung zwischen einer PIN für Signaturkarten und einem Passwort für Sicherheitssticks gemacht. Die Begriffe werden synonym verwendet.

2. Quickstart

2.1. Unterstützte Plattformen

Der ElsterAuthenticator unterstützt folgende Plattformen:

- Windows 10 (32/64 Bit)
- Windows 11 (64 Bit)
- Windows Server 2019 / 2022
- macOS 11.06 / 12 / 13
- Linux Ubuntu 22.04 (64 Bit)

Die Installation, Konfiguration und Benutzung des ElsterAuthenticators ist auf allen Plattformen weitestgehend gleich.

2.2. Installation

2.2.1. Windows/macOS

2.2.1.1. Graphische Installation

Die Installation des ElsterAuthenticators starten Sie unter Windows und macOS per Doppelklick auf das Installationsprogramm, das Sie von Mein ELSTER auf Ihren Rechner geladen haben.

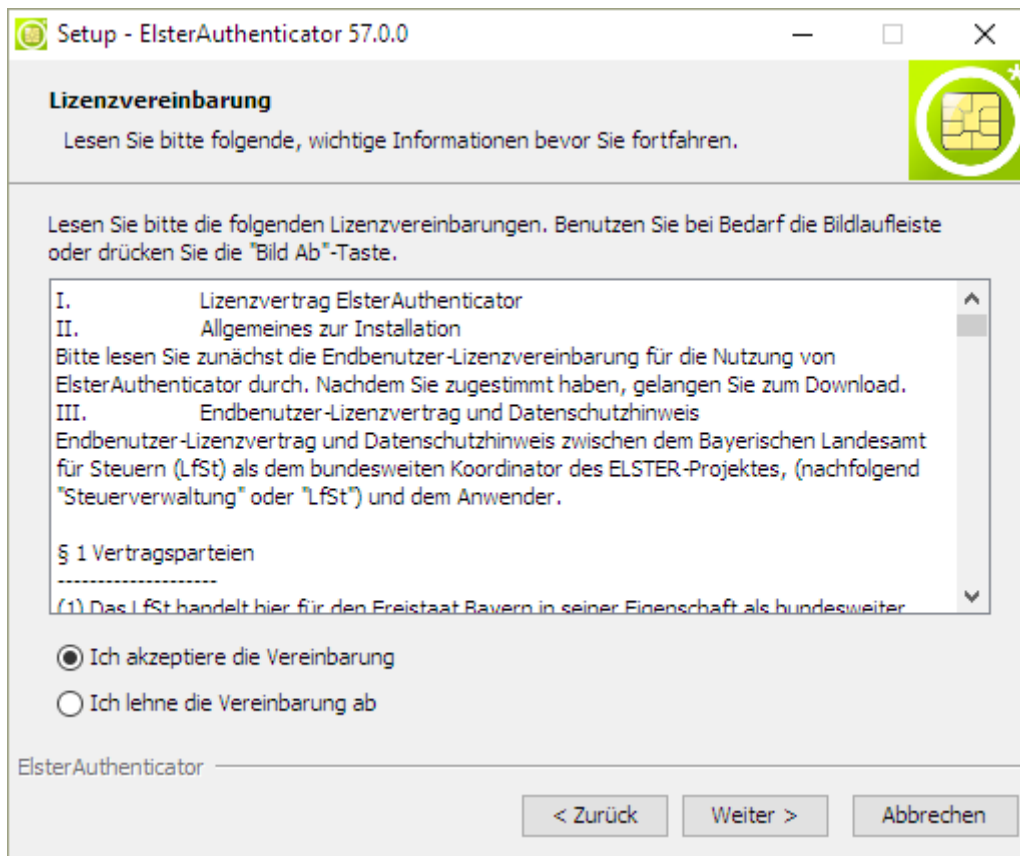
Nach Start des Programms prüft das Installationsprogramm, ob Sie bereits eine Installation des ElsterAuthenticators haben und schlägt Ihnen dann gegebenenfalls vor, diese zu aktualisieren. In diesem Fall belassen Sie die Einstellung auf „Ja, aktualisiere ...“.





Durch Betätigen der Schaltfläche „Weiter >“ wird die Installation fortgesetzt.

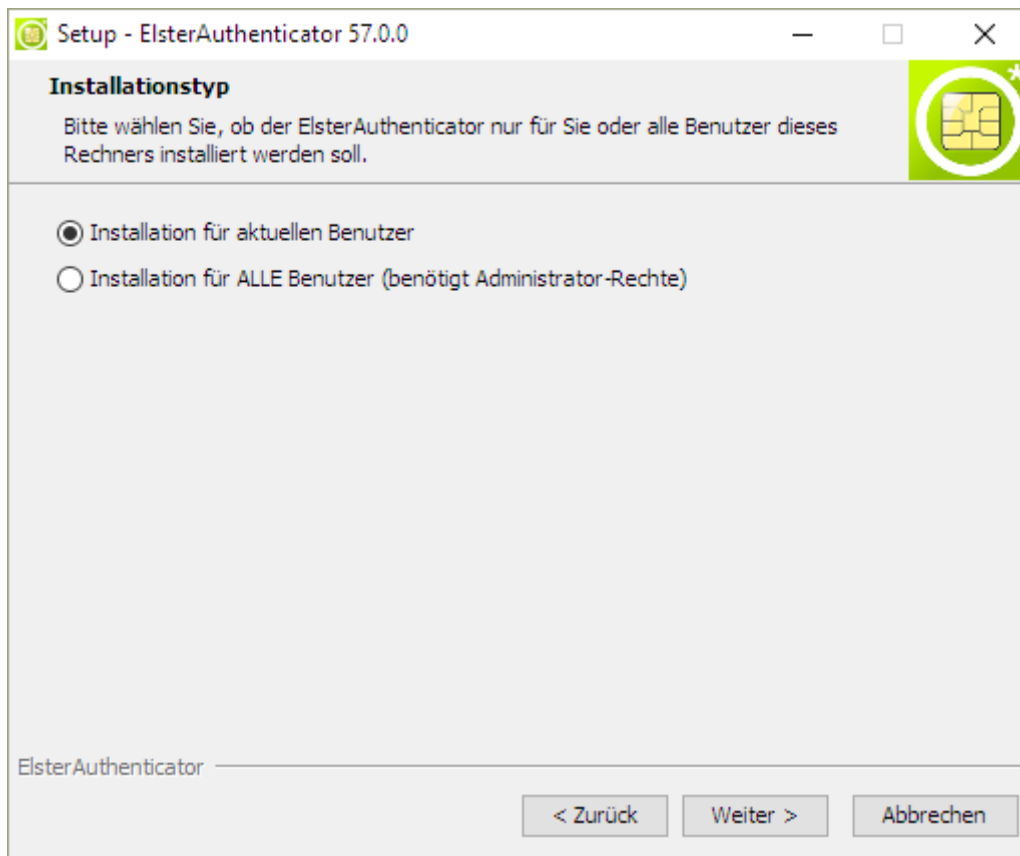
Die Lizenzvereinbarung, die Ihre Rechte zur Verwendung des ElsterAuthenticators regelt, wird angezeigt.



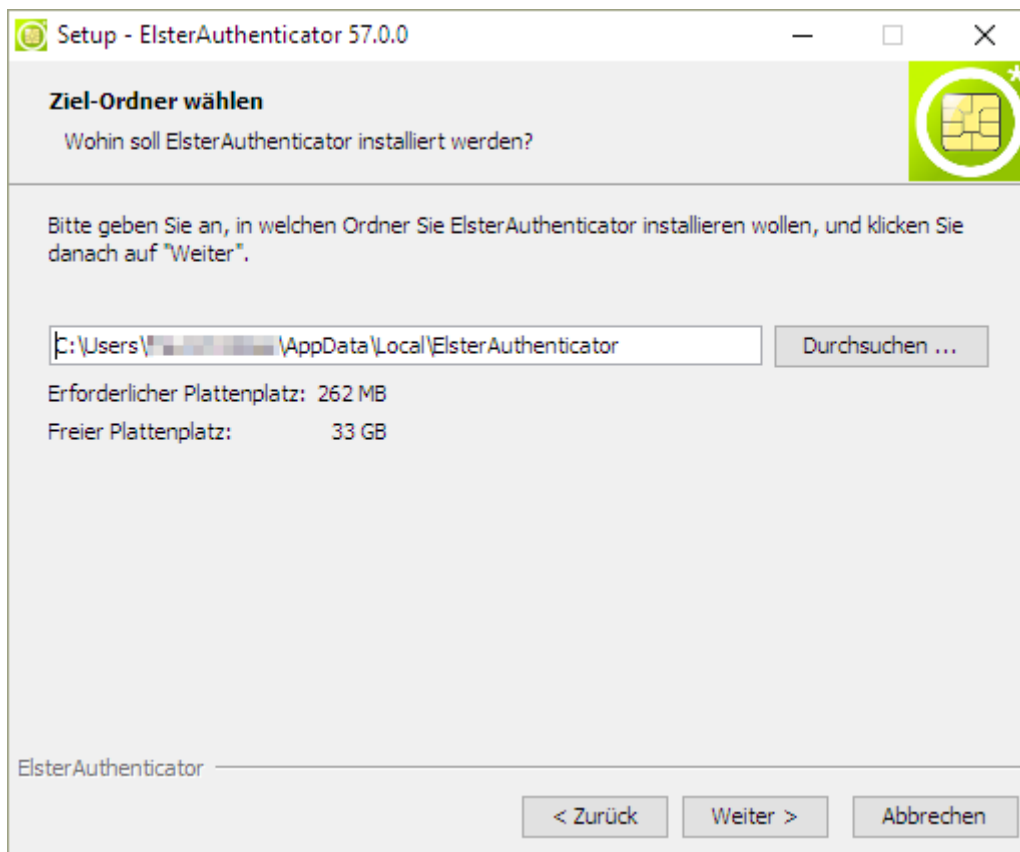
Lesen Sie die Lizenzvereinbarung, wählen Sie „Ich akzeptiere die Vereinbarung“ und klicken Sie dann auf „Weiter >“.

Nun können Sie auswählen, ob die Installation für den aktuellen Benutzer (hierzu sind keine Administrator-Rechte erforderlich) oder für alle Benutzer des Betriebssystems (hierzu sind Administrator-Rechte erforderlich) erfolgen soll.

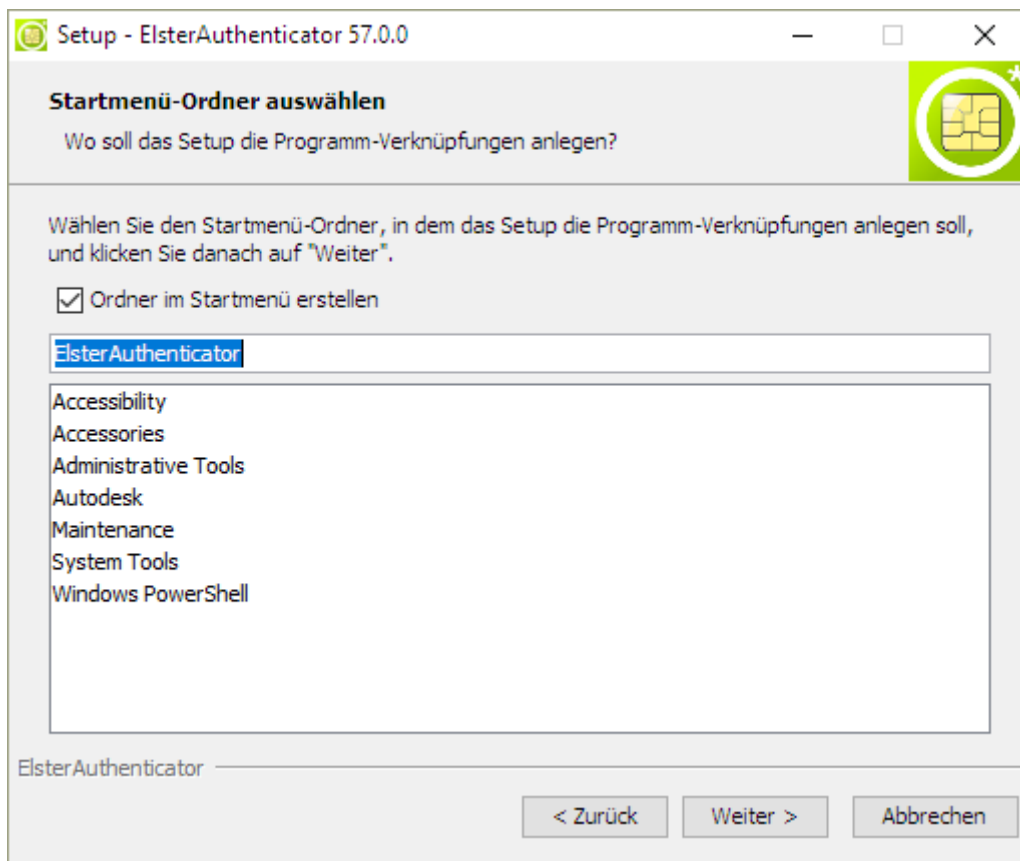
HINWEIS Falls der ElsterAuthenticator bereits auf dem System installiert ist, steht diese Wahlmöglichkeit gegebenenfalls nicht zur Verfügung. Um erneut zwischen den beiden Varianten wählen zu können, muss der bestehende ElsterAuthenticator deinstalliert werden. Es wird nicht empfohlen, die Anwendung mehrfach auf einem System zu installieren (hierzu zählt auch die Installation als Benutzer mit und ohne Administrator-Rechte), da dies zu unerwünschten Effekten und technischen Problemen führen kann.



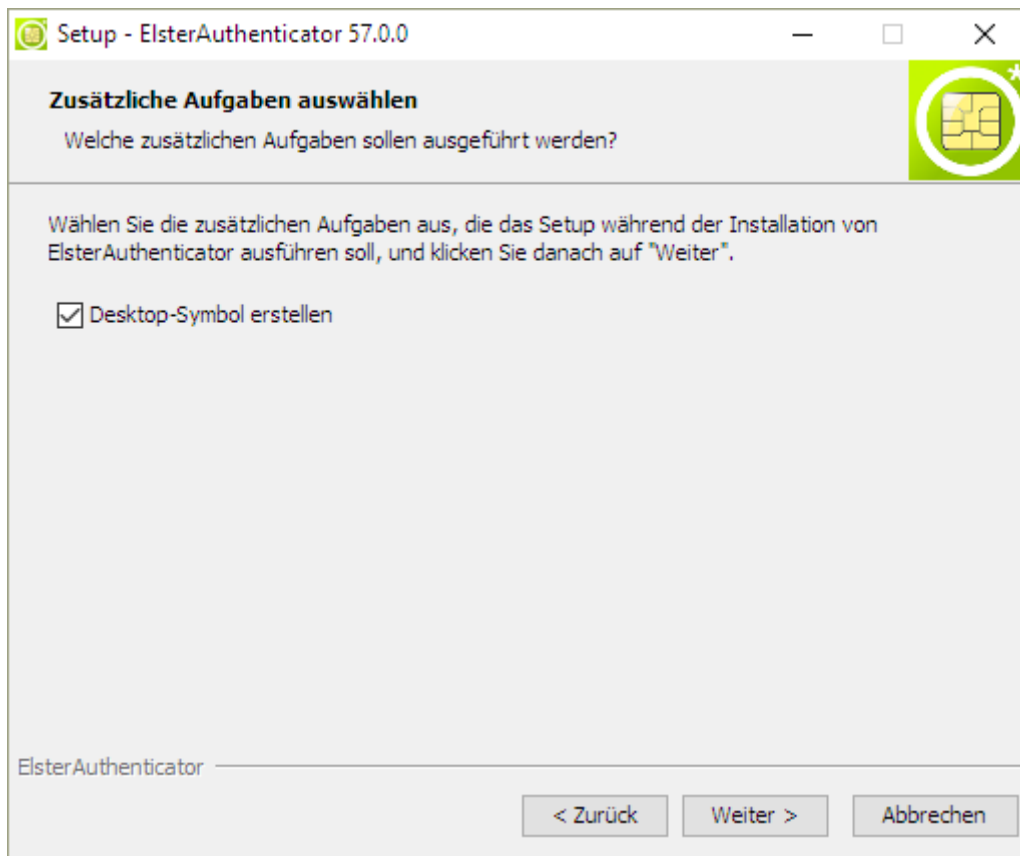
Nach Auswahl der Installationsart können Sie einen Ziel-Ordner, abweichend vom Standardverzeichnis, angeben.



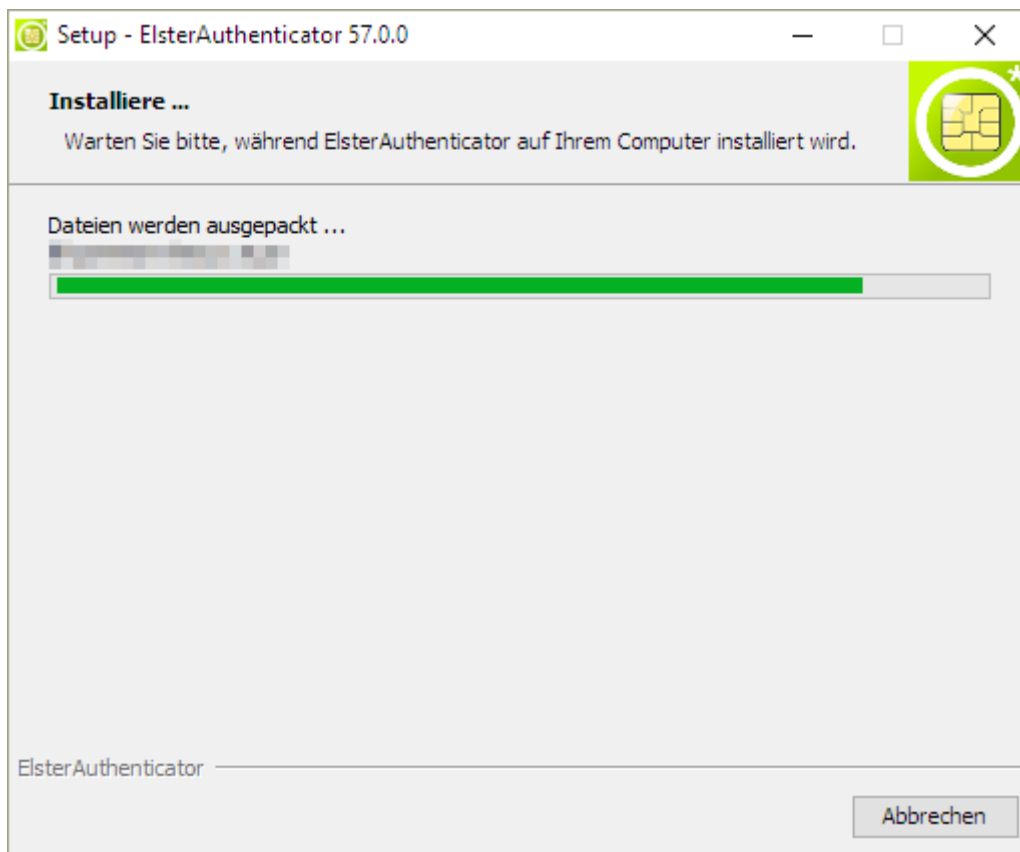
Bitte beachten Sie, dass Sie über Schreibrechte im Installationsverzeichnis verfügen müssen.



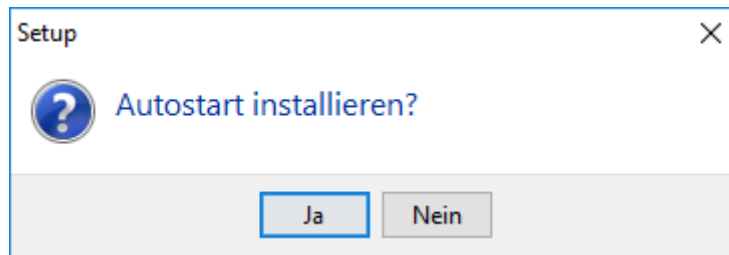
Anschließend können Sie, bei Bedarf, den Start-Menü Eintrag umbenennen.



Nach der Auswahl, ob ein Desktop-Symbol angelegt werden soll, klicken Sie auf „Weiter >“. Die Installation wird anschließend durch das Installationsprogramm ausgeführt.



Abschließend werden Sie gefragt, ob der ElsterAuthenticator automatisch beim Systemstart ausgeführt werden soll.



Nach erfolgreicher Installation können Sie das Setup durch Klicken auf „Fertigstellen“ beenden.



2.2.1.2. Silent Installation

Alternativ zur graphischen Installation kann der ElsterAuthenticator auch über einen Aufruf in der Kommandozeile ohne weitere Benutzerinteraktion installiert werden.

Beispielaufruf:

- `ElsterAuthenticator_57_0_0.exe -q -dir "C:\ElsterAuthenticator"`

Folgende Parameter werden unterstützt:

-dir <Installationsverzeichnis>

Bitte beachten Sie, dass zwischen dem Parameter -dir und der eigentlichen Pfadangabe des Installationsverzeichnisses zwingend ein Leerzeichen erforderlich ist!

-Vautostart\$Boolean (true/false)

Autostart Eintrag erstellen

-VcreateDesktopLinkAction\$Boolean

Ein Desktop-Icon anlegen

-Vsys.programGroupName

Der Programmgruppenname

-Vsys.programGroupDisabled\$Boolean (true/false)

Keine Programmgruppe anlegen

-Vsys.programGroupAllUsers\$Boolean (true/false)

Installation für alle Benutzer (Administrator-Rechte notwendig)

2.2.2. Linux Ubuntu 22.04 (64 Bit)

Bitte beachten Sie, dass folgende Pakete installiert sein müssen:

- pcsd

Sie können mittels folgender Kommandos in einer Linux Shell die Pakete installieren:

- `sudo apt-get install pcsd`

Bevor das Skript in der Linux-Shell ausgeführt werden kann, muss es durch folgenden Befehl modifiziert werden:

- `chmod +x ElsterAuthenticator_unix_57_0_0.sh`

Anschließend kann die Installation wie folgt gestartet werden:

- `./ElsterAuthenticator_unix_57_0_0.sh`

HINWEIS Mit Ubuntu 18.04 hat sich der Library-Pfad des pcsd geändert. Während die `libpcsc-lite.so.1` in Ubuntu 17.10 unter `/lib/x86_64-linux-gnu/` installiert

wurde, erfolgt die Installation unter Ubuntu 18.04 nun unter `/usr/lib/x86_64-linux-gnu/`

Bitte stellen Sie sicher, dass der ElsterAuthenticator die `libpcsclite.so.1` unter `/lib/x86_64-linux-gnu/` findet. Hierzu reicht es aus, nach der Installation des `pcscd`, folgendes Kommando auszuführen und mit dem Admin Passwort zu bestätigen.

Ubuntu 64 Bit Systeme:

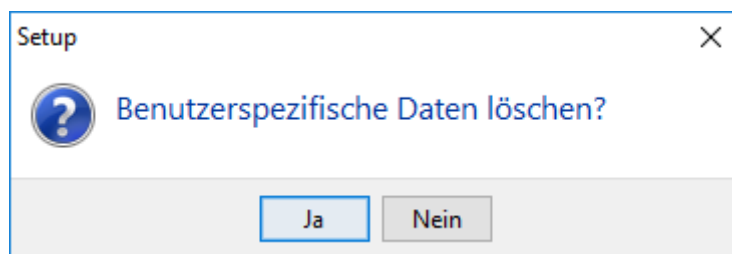
- `cd /lib/x86_64-linux-gnu/ ; sudo ln -s /usr/lib/x86_64-linux-gnu/libpcsclite.so.1`

2.3. Deinstallation

2.3.1. Graphische Deinstallation

Der ElsterAuthenticator kann über die graphische Deinstallations-Routine und über die Kommandozeile deinstalliert werden.

Die Deinstallation kann auf Wunsch auch das Anwenderverzeichnis mit Ihrem gesamten Inhalt löschen.



Starten Sie die Deinstallation auf macOS und Linux Betriebssystemen, indem Sie im Installationsverzeichnis `uninstall` aufrufen und der graphischen Deinstallation folgen.

macOS: `./uninstall` Ubuntu: `./uninstall`

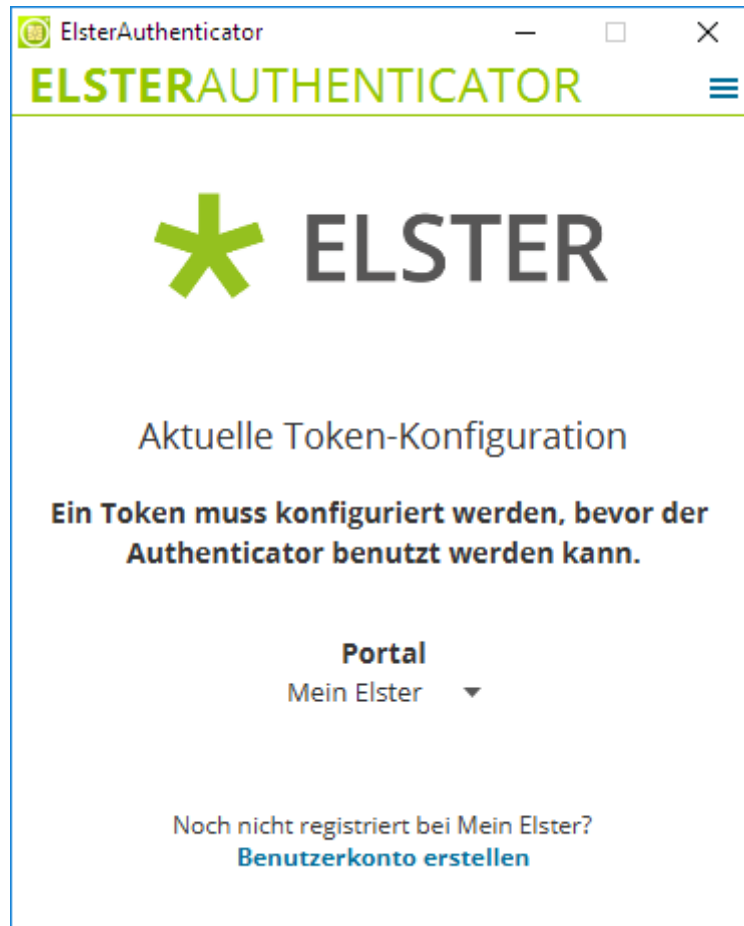
2.3.2. Silent Deinstallation

Beispielaufruf:

- `uninstall.exe -q -Vuserfilesdelete$Boolean=true`

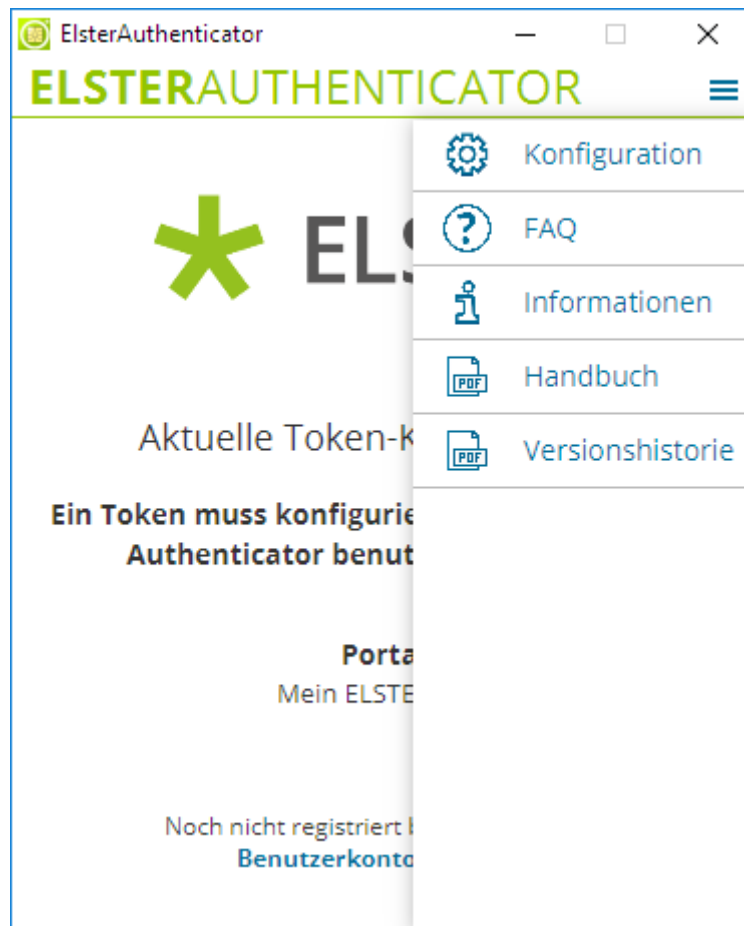
2.4. Konfiguration

Der ElsterAuthenticator kann mit dem Sicherheitsstick oder mit einer Signaturkarte ausgewählter Anbieter verwendet werden.

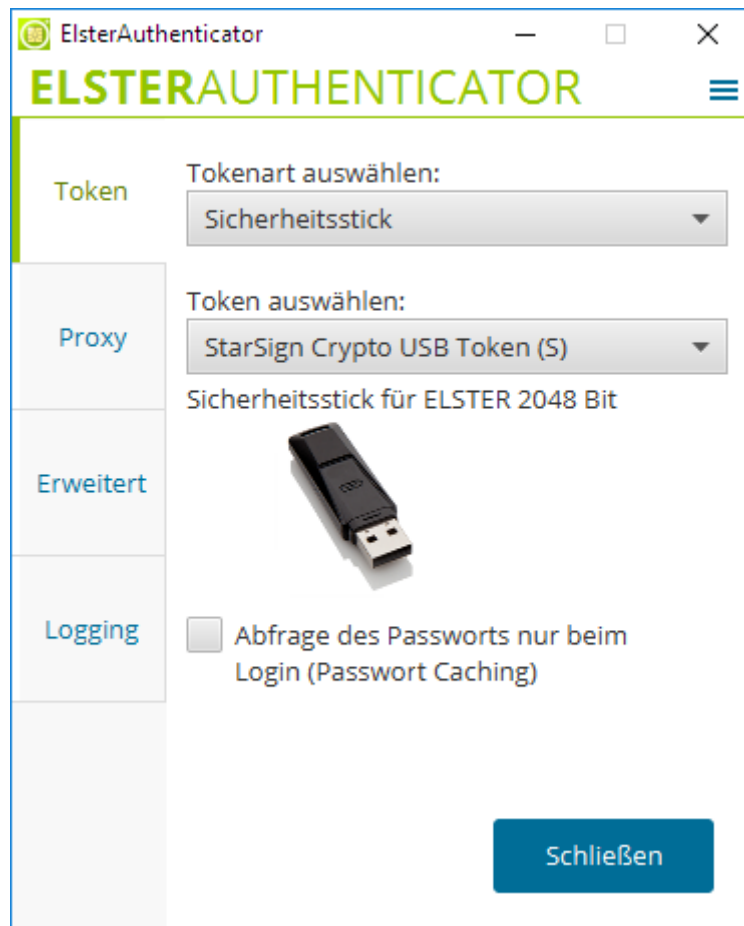


Nach erstmaligem Start des ElsterAuthenticators erscheint ein Fenster mit dem Hinweis, dass Sie den ElsterAuthenticator zunächst konfigurieren müssen.

Nach Klick auf den Menü-Button oben rechts erscheint ein Auswahlménü mit „Konfiguration“, „FAQ“, „Informationen“, „Handbuch“ und „Versionshistorie“. Abhängig vom eingestellten Token wird hier ein weiterer Menüpunkt „Passwort ändern“ angezeigt. Im Menüpunkt „Konfiguration“ kann der Token ausgewählt werden.



Nun erscheinen im Fenster vier seitliche Reiter mit den Bezeichnungen „Token“, „Proxy“, „Erweitert“ und „Logging“. Ein Klick auf jeden dieser Reiter öffnet rechts davon einen dazugehörigen Eingabedialog. Alle Änderungen werden unmittelbar übernommen.

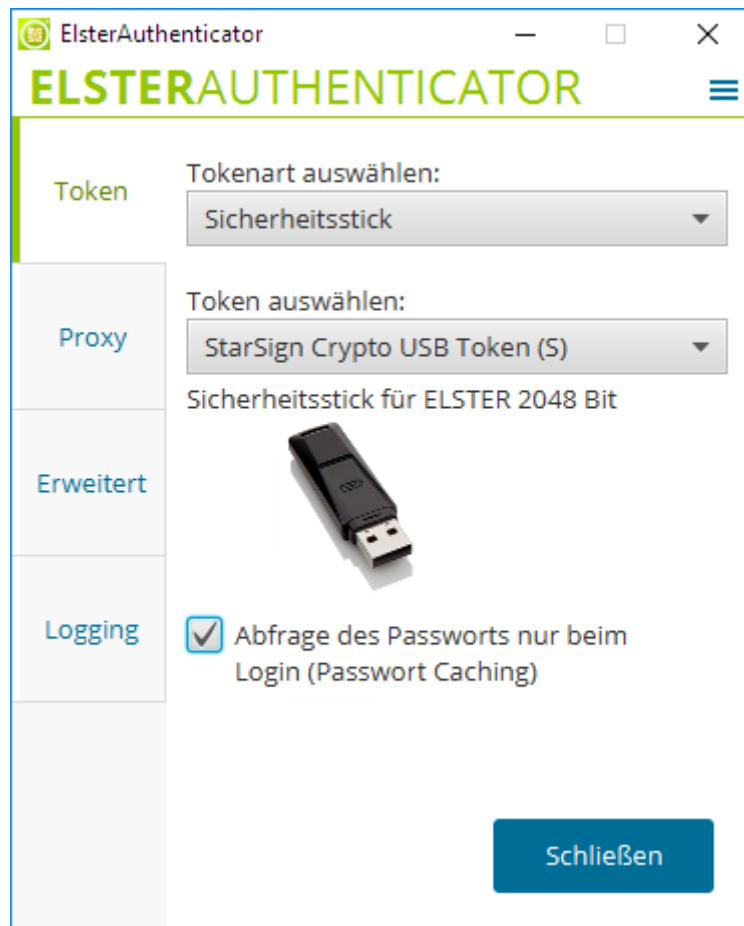


Im Reiter Token kann der gewünschte Token eingerichtet werden. Die Tokenart (Sicherheitsstick, Signaturkarte) und der Token müssen, abhängig davon welcher Token zum Einsatz kommt, angepasst werden.

Zur erleichterten Bedienung kann bei einem Sicherheitsstick die Option Passwort Caching aktiviert werden. Ist das Passwort Caching aktiviert, so wird das Passwort bei der nächsten Aktion automatisch eingetragen. Das Passwort wird nach einer halben Stunde Inaktivität, beim Ändern des Passworts oder Beenden der Anwendung verworfen, und muss anschließend erneut eingegeben werden. Der Timeout für das Passwort Caching wird bei jeder Aktion zurückgesetzt. Die Verwaltung des Passworts für Signaturkarten erfolgt über die entsprechende Middleware.

2.4.1. Nutzung eines Sicherheitssticks

Nach Auswahl der Tokenart „Sicherheitsstick“ und dem Ihnen vorliegenden Modell kann die Konfiguration über die Schaltfläche „Schließen“ beendet werden.



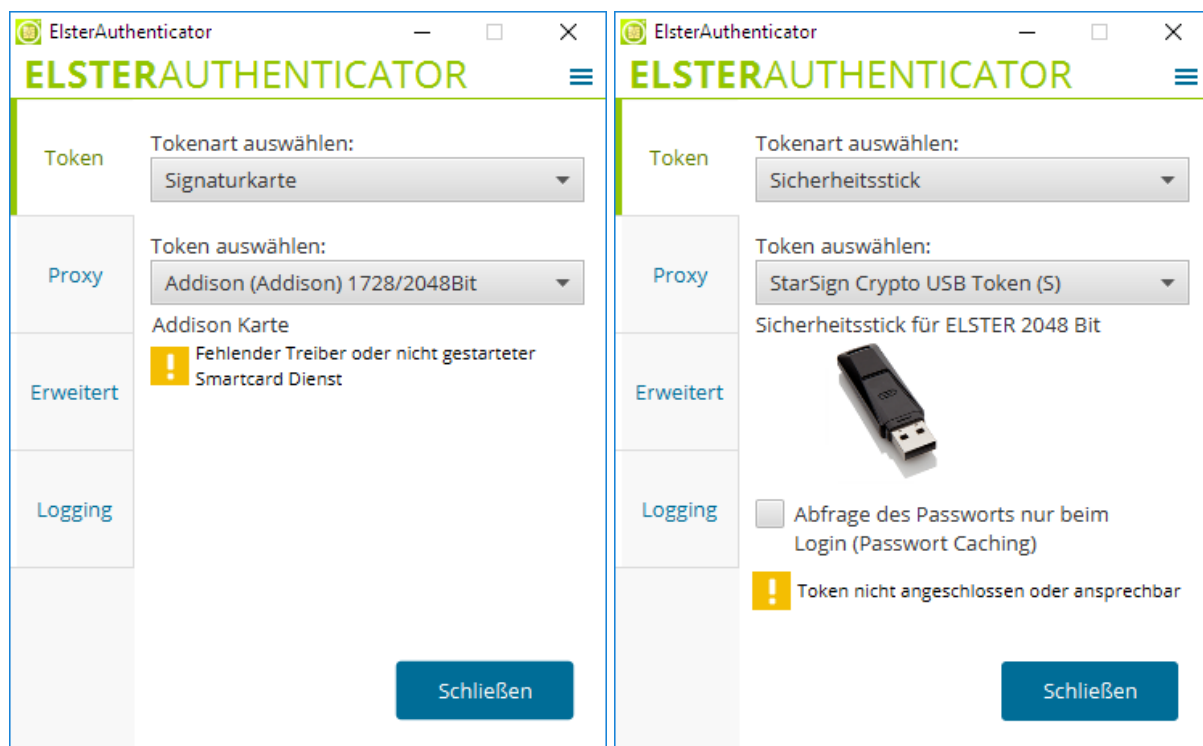
HINWEIS Der Sicherheitsstick steht in zwei Varianten zur Verfügung:

1. „StarSign Crypto USB Token“ mit Unterstützung von Windows 10/11 in 32 Bit/64 Bit und macOS 10.10
2. „StarSign Crypto USB Token S“ mit Unterstützung von Windows 10/11 in 32 Bit/64 Bit, Windows Server 2019/2022, macOS 11.06/12 und Linux Ubuntu 22.04

Diese beiden Varianten werden im ElsterAuthenticator und in diesem Benutzerhandbuch zusammenfassend als „StarSign Crypto USB Token (S)“ bezeichnet.

Treiber und weitere Informationen zu den Sicherheitssticks finden Sie unter: www.sicherheitsstick.de

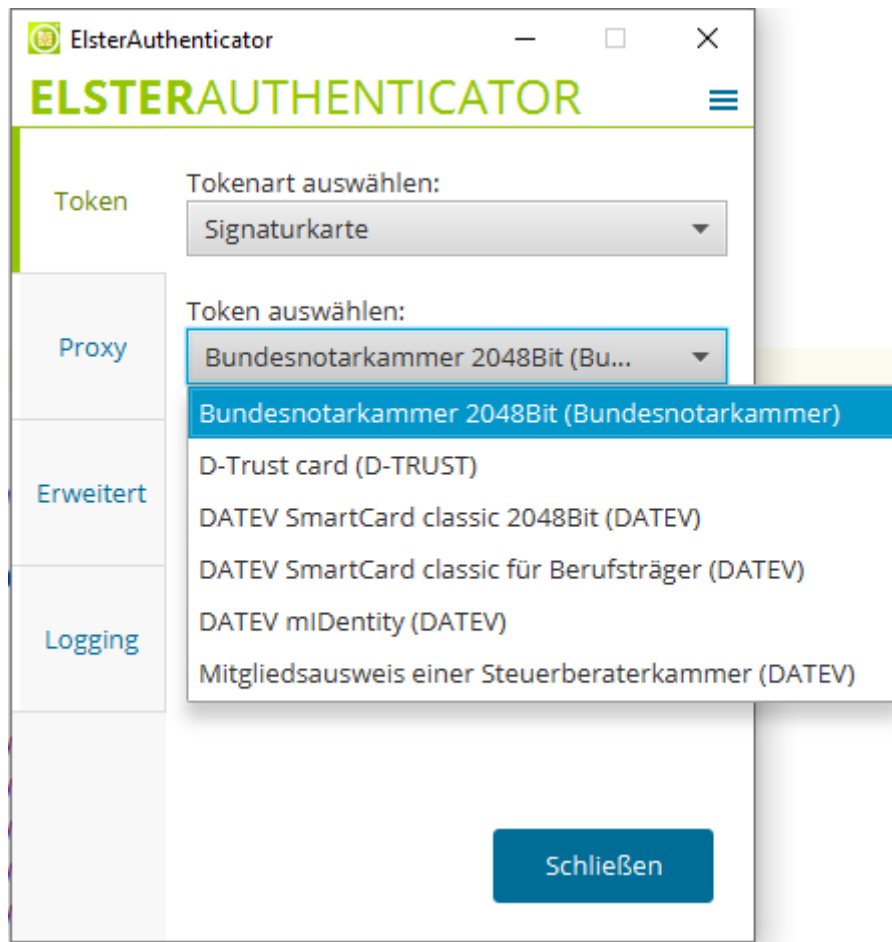
Bei der Auswahl eines Tokens wird unmittelbar überprüft, ob der Treiber installiert und der Token angeschlossen ist.



HINWEIS Bitte beachten Sie, dass unter allen Windows Betriebssystemen der Smartcard-Dienst gestartet sein muss.

2.4.2. Nutzung einer Signaturkarte

Sind Sie Nutzer einer der von ELSTER unterstützten Signaturkarten externer Kartenherausgeber, dann wählen Sie „Signaturkarte“ aus. Im darunterliegenden Eingabefeld „Token auswählen“ können Sie nun Ihren Kartentyp auswählen.



Mit Betätigung der Schaltfläche „Schließen“ wird die Konfiguration abgeschlossen.

HINWEIS Es darf jeweils nur ein Token am System angeschlossen sein.

2.4.3. Nutzung eines Proxys für den Internet-Zugriff

Wenn Sie auf das Internet über einen Proxy zugreifen, dann müssen Sie auch beim ElsterAuthenticator den Proxy-Zugang konfigurieren. Diese Konfiguration stellen Sie über den Reiter „Proxy“ ein.

Hier haben Sie die Konfigurationsmöglichkeit zwischen „Kein Proxy“, „System-Proxy verwenden“ und „Manuelle Proxy-Konfiguration“.

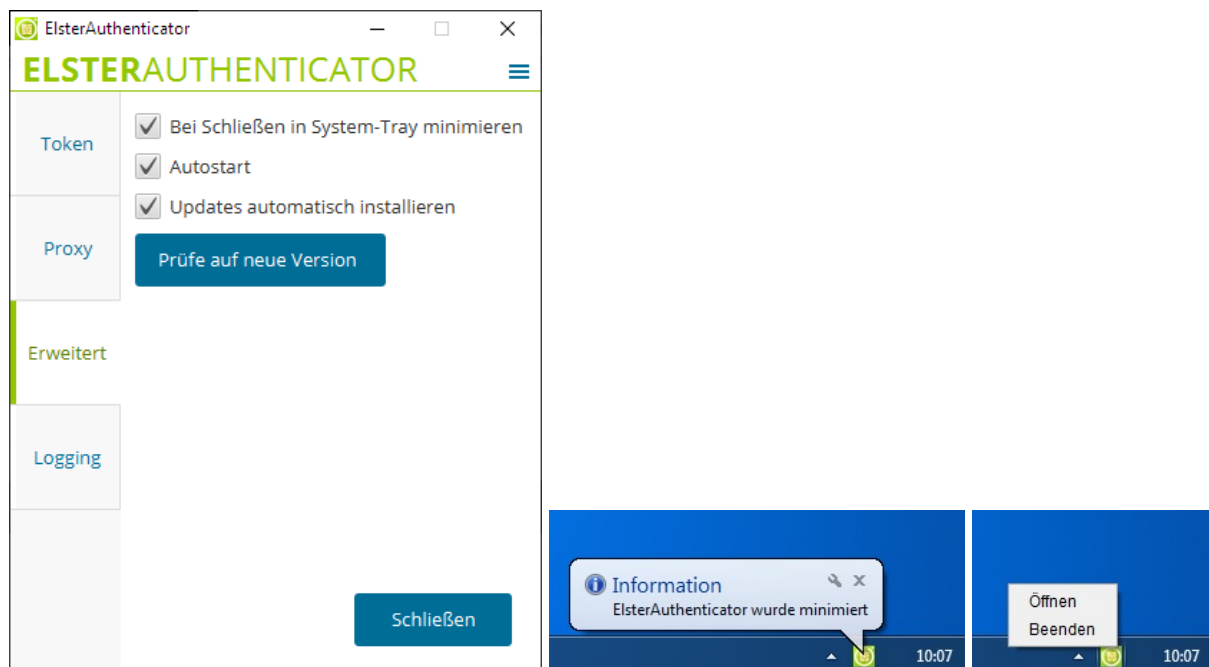
- Bei der Auswahl von „System-Proxy verwenden“ wird der im Betriebssystem konfigurierte Proxy verwendet. Sollte hier kein Proxy konfiguriert sein oder der Zugriff über diesen Proxy fehlschlagen, wird intern auf „Kein Proxy“ umgeschaltet. Für die Konfiguration eines System-Proxys konsultieren Sie bitte die Betriebssystem-Dokumentation.
- Bei der „Manuellen Proxy-Konfiguration“ tragen Sie die vollständige Proxy-URL ein, gegebenenfalls mit Portnummer, wenn der Proxy-Port ein anderer Port als 80 ist. Eine vollständige Proxy-URL hat die Struktur [http://\(sub-\)domain:portnummer](http://(sub-)domain:portnummer).
- Sollte der Proxy-Server eine http Authentisierung erfordern, dann muss zusätzlich der Benutzername und das Passwort eingegeben werden.

- HINWEIS**
1. Bitte beachten Sie, abhängig von dem von Ihnen eingesetzten Browser, dass „localhost“ bzw. die IP-Adresse „127.0.0.1“ in die Liste der nicht über den Proxy zu routenden Adressen aufgenommen werden muss.
 2. Bei Windows-Betriebssystemen kann – je nach Konfiguration – in der Systemsteuerung bei der „Automatischen Proxyeinrichtung“ die Verwendung der Option „Einstellungen automatisch erkennen“ einen manuell konfigurierten Proxy übersteuern, so dass der

ElsterAuthenticator trotz eingestellter Option „System-Proxy verwenden“ keine Verbindung zum Portal „Mein ELSTER“ aufbauen kann. Für die Konfiguration wenden Sie sich bitte an Ihre System-Administration.

2.4.4. Erweitert

Ist die Option „Bei Schließen in System-Tray minimieren“ aktiviert, minimiert sich der ElsterAuthenticator beim Klick auf den Schließen-Button in den System-Tray. Mit einem Doppelklick auf das ElsterAuthenticator Logo im System-Tray öffnet sich der ElsterAuthenticator erneut. Ein Klick mit der rechten Maustaste auf das ElsterAuthenticator Logo bietet Ihnen die Möglichkeiten, die Anwendung zu beenden oder zu öffnen. Solange die oben genannte Option aktiviert ist, lässt sich der ElsterAuthenticator nur über das System-Tray beenden.



Mit Aktivierung der Autostart-Option bei der Installation wird der ElsterAuthenticator nach dem Systemstart automatisch gestartet. Auf Windows-Systemen kann die Autostart-Option in den Einstellungen im Registerreiter „Erweitert“ nachträglich angepasst werden.

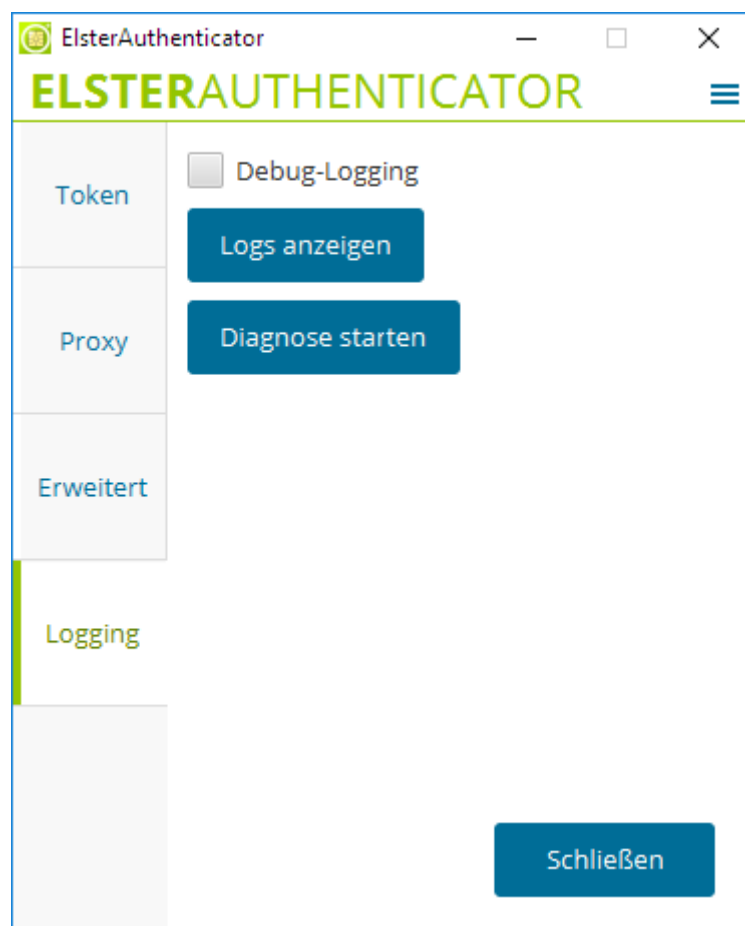
- HINWEIS**
1. Wurde die Autostart-Option systemweit durch den Administrator aktiviert, wird dieser Aktivierungsstatus als in der Bearbeitung gesperrtes, angehaktes Auswahlfeld angezeigt.
 2. Unter Linux- und macOS-Systemen ist die nachträgliche Bearbeitung der Autostart-Option nicht möglich. Der nebenstehende Text lautet dann „Autostart (ggf. extern)“, das Auswahlfeld ist in der Bearbeitung gesperrt und ein „-“ Symbol wird anstelle des Häkchens angezeigt.

Beim Aktivieren der Option „Updates automatisch installieren“ wird in regelmäßigen Abständen nach einer neuen ElsterAuthenticator-Version gesucht. Diese wird im Erfolgsfall automatisch heruntergeladen und nach der Einwilligung installiert. Die Prüfung auf eine neue Version kann auch über den „Prüfe auf neue Version“ Button manuell gestartet werden. In diesem Fall werden der Download und die Installation nur ausgeführt, wenn gleichzeitig die Option zum automatischen Updaten („Updates automatisch installieren“) aktiviert ist.

HINWEIS Auf dem Betriebssystem „Windows Server“ steht eine automatische Update-Funktion nicht zur Verfügung.

2.4.5. Logging

Der letzte Reiter „Logging“ muss nur aufgerufen werden, wenn Sie nach Problemen bei der Verwendung von Mein ELSTER mit dem ElsterAuthenticator den ELSTER-Support in Anspruch nehmen und der Support-Mitarbeiter Sie dazu auffordert.



Hier kann die Protokollierung des ElsterAuthenticators aktiviert und angezeigt werden, die dem ELSTER-Support bei der Fehlersuche hilft. Der ElsterAuthenticator protokolliert den Programmablauf und eventuell auftretende Fehler im Anwenderverzeichnis des jeweiligen Benutzers in der Datei `elster-authenticator.log`. Nicht protokolliert werden benutzerspezifische Passwörter,

Schlüssel und Zertifikate. Das Anwenderverzeichnis ist benutzerspezifisch und befindet sich im Home Verzeichnis des Anwenders.

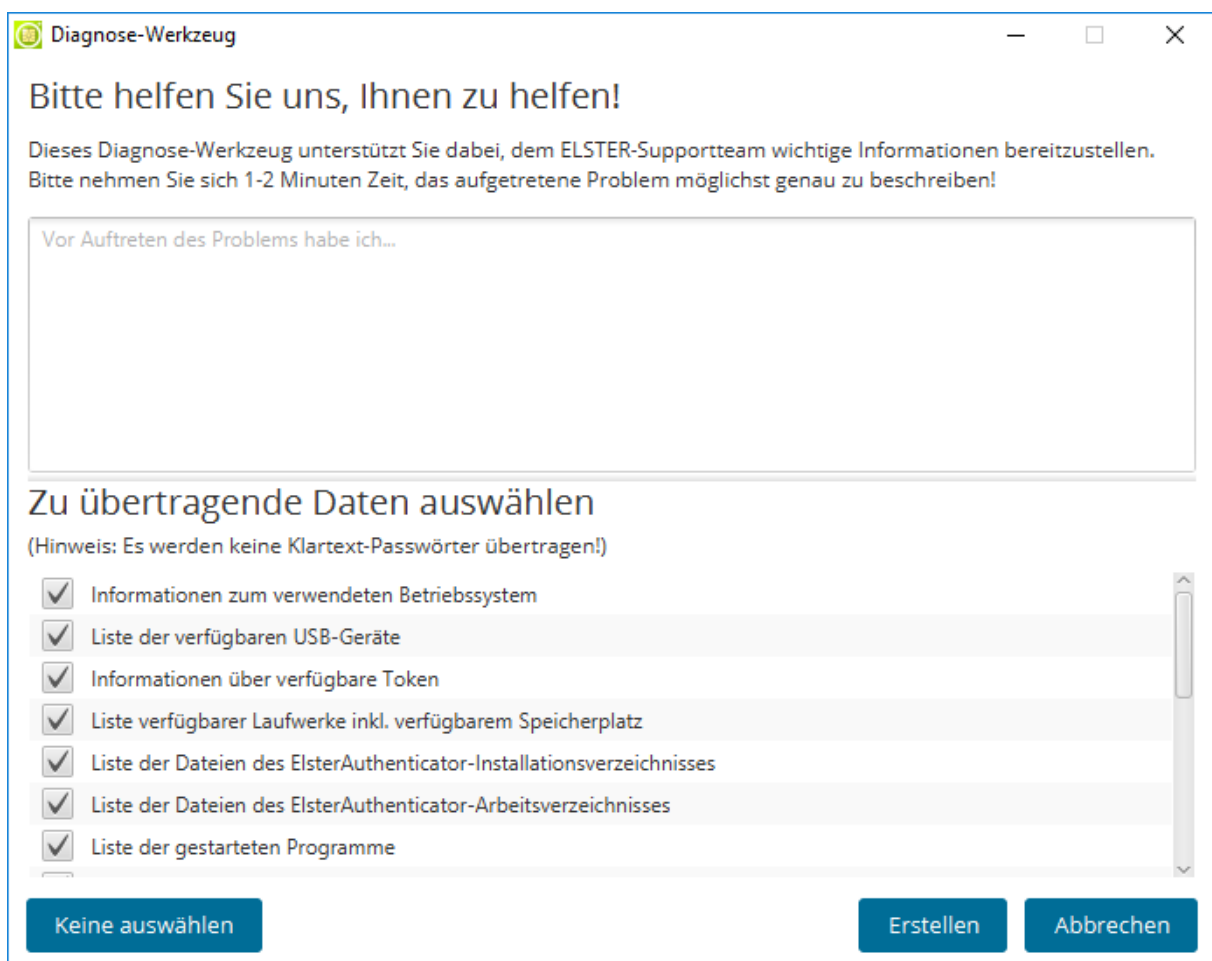
Die Log-Datei ist üblicherweise unter folgendem Pfad zu finden:

- Windows: C:\Benutzer\<Benutzerkonto>\.elster-authenticator\
- macOS: ~/ .elster-authenticator
- Ubuntu: ~/ .elster-authenticator

HINWEIS Bitte beachten Sie, dass nach dem Aktivieren des „Debug-Logging“ der Vorgang wiederholt werden muss, da ansonsten die notwendigen Debug-Aufzeichnungen noch nicht protokolliert worden sind.

2.4.6. Diagnose-Informationen erstellen

In manchen Fällen kann es notwendig sein, für eine detaillierte Fehleranalyse, eine vollständige Diagnose des Anwender-Systems zu erstellen und einzusenden. Das Diagnose-Werkzeug können Sie in der ElsterAuthenticator-Konfiguration im Reiter „Logging“ oder über das Startmenü starten.



Diagnose-Werkzeug

Bitte helfen Sie uns, Ihnen zu helfen!

Dieses Diagnose-Werkzeug unterstützt Sie dabei, dem ELSTER-Supportteam wichtige Informationen bereitzustellen. Bitte nehmen Sie sich 1-2 Minuten Zeit, das aufgetretene Problem möglichst genau zu beschreiben!

Vor Auftreten des Problems habe ich...

Zu übertragende Daten auswählen

(Hinweis: Es werden keine Klartext-Passwörter übertragen!)

- ☒ Informationen zum verwendeten Betriebssystem
- ☒ Liste der verfügbaren USB-Geräte
- ☒ Informationen über verfügbare Token
- ☒ Liste verfügbarer Laufwerke inkl. verfügbarem Speicherplatz
- ☒ Liste der Dateien des ElsterAuthenticator-Installationsverzeichnisses
- ☒ Liste der Dateien des ElsterAuthenticator-Arbeitsverzeichnisses
- ☒ Liste der gestarteteten Programme

Keine auswählen Erstellen Abbrechen

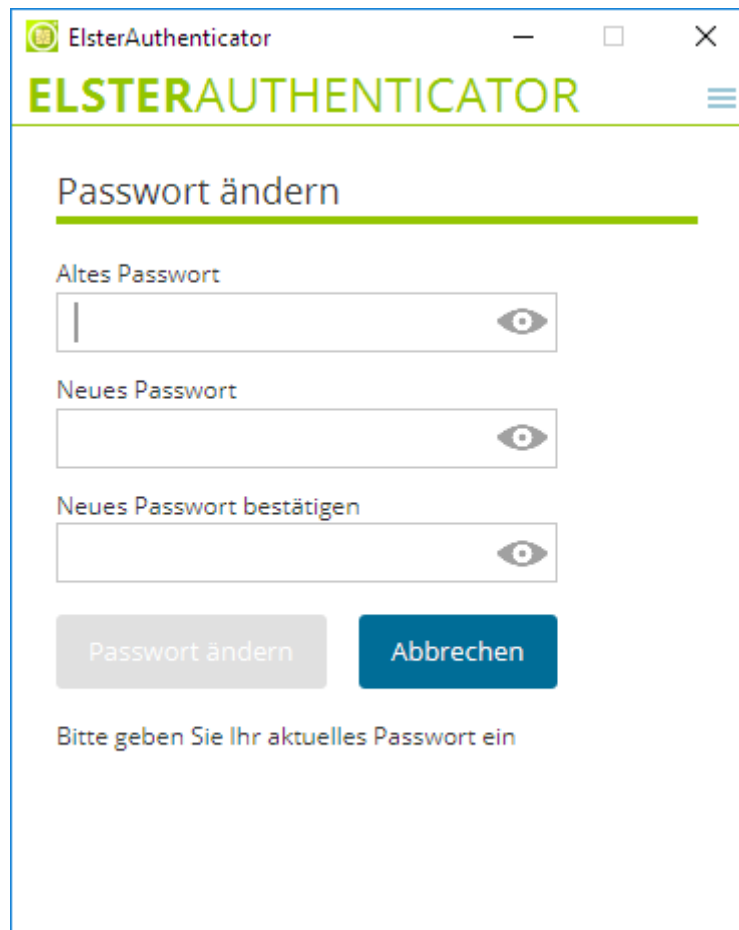
Erstellen Sie die Diagnose-Informationen, indem Sie nach Bedarf eine Fehlerbeschreibung eingeben

und mit „Erstellen“ bestätigen. Sie können einzelne Punkte aus der Protokollierung ausschließen. Beachten Sie aber, dass das Fehlen von Daten zu erneuten Nachfragen führen kann.

2.5. Passwort ändern

2.5.1. Sicherheitsstick

2.5.1.1. Passwort ändern



The screenshot shows a window titled 'ElsterAuthenticator' with a green header bar containing the text 'ELSTERAUTHENTICATOR' and a menu icon. Below the header, the title 'Passwort ändern' is displayed. The form contains three input fields: 'Altes Passwort' (Old Password), 'Neues Passwort' (New Password), and 'Neues Passwort bestätigen' (Confirm New Password). Each field has a corresponding eye icon for toggling visibility. At the bottom, there are two buttons: 'Passwort ändern' (Change Password) and 'Abbrechen' (Cancel). A message at the bottom reads 'Bitte geben Sie Ihr aktuelles Passwort ein' (Please enter your current password).

Der Menüpunkt „Passwort ändern“ wird nur angezeigt, wenn ein ELSTER Sicherheitsstick konfiguriert ist. Über diesen Menüpunkt können Sie das Passwort des Sicherheitssticks gemäß den Passwortvorgaben jederzeit ändern. Das Ändern des Passworts erfolgt unmittelbar nach dem Klick auf „Passwort ändern“ ohne weitere Sicherheitsabfragen.

2.5.1.2. Stick entsperren mittels PUK

Beim Einsatz des StarSign Crypto USB Token (S) kann ein vergessenes Passwort mittels PUK zurückgesetzt werden. Die PUK wird während des Registrierprozesses in Schritt 2 generiert.

The screenshot shows a window titled "ElsterAuthenticator" with standard Windows window controls (minimize, maximize, close). The main title bar is green with the text "ELSTERAUTHENTICATOR" in white. Below the title bar, the text "Passwort ändern / Stick entsperren mit PUK-Eingabe" is displayed. There are three input fields, each with a toggle icon (an eye) to its right: "PUK", "Neues Passwort", and "Neues Passwort bestätigen". At the bottom, there are two buttons: "Passwort ändern" (disabled, grey) and "Abbrechen" (active, blue).

2.5.2. Signaturkarten

Eine Passwort-Änderung bei Signaturkarten erfolgt mittels Ihrer Middleware, die zum korrekten Funktionieren installiert sein muss.

Zum Zurücksetzen des Passworts einer Signaturkarte konsultieren Sie bitte den jeweiligen Signaturkarten-Anbieter.

3. Funktionsweise


Der ElsterAuthenticator ist die Schnittstelle zwischen Ihrem Sicherheitsstick bzw. Ihrer Signaturkarte und Mein ELSTER. Wenn Sie Mein ELSTER mit Ihrem Sicherheitsstick oder Ihrer Signaturkarte verwenden, muss der ElsterAuthenticator auf Ihrem System gestartet sein.

Der ElsterAuthenticator wird während einer Sitzung mit Mein ELSTER unter anderem verwendet für:

- die Registrierung Ihres Sicherheitssticks bzw. Ihrer Signaturkarte bei Mein ELSTER als Anmeldetoken oder
- die Anmeldung („Login“) bei Mein ELSTER mit Ihrem bereits registrierten Sicherheitsstick oder Ihrer registrierten Signaturkarte

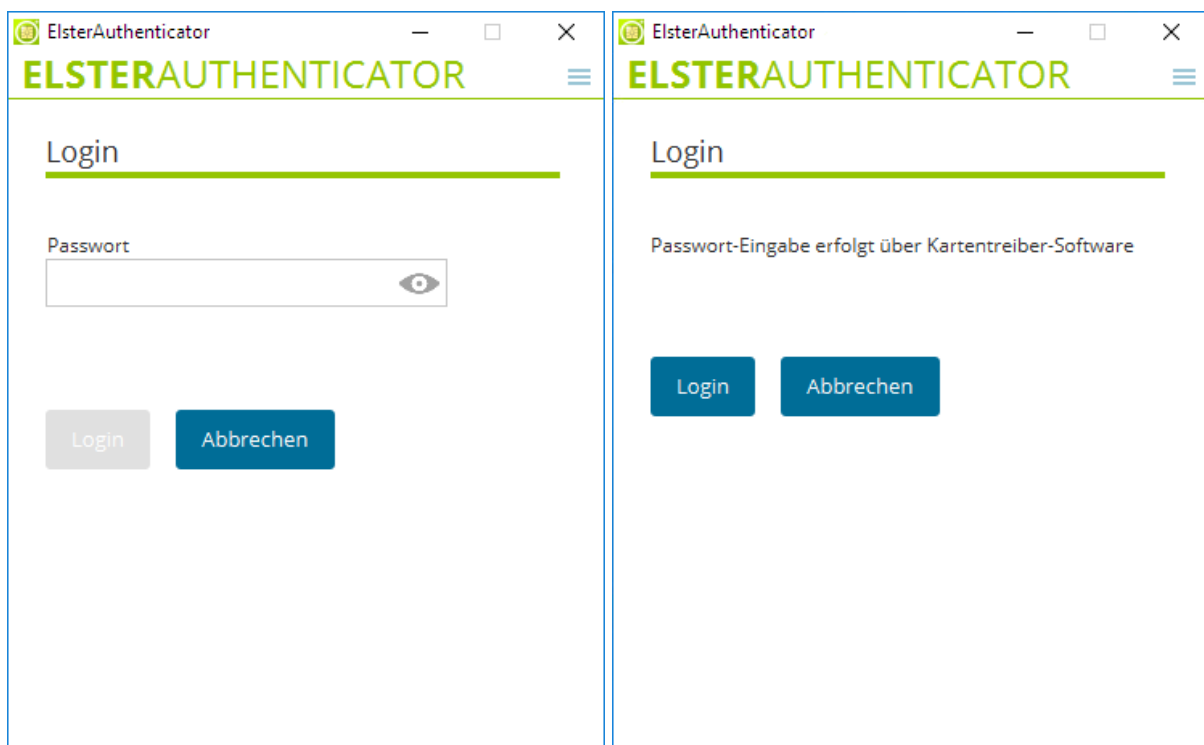
- die authentifizierte Datenübermittlung (Versenden eines Formulars)
- das Speichern von entschlüsselten Postfachnachrichten

Bei derartigen Funktionen wird Ihnen Mein ELSTER eine Schaltfläche „Weiter mit ElsterAuthenticator“ anbieten:

Weiter mit ElsterAuthenticator 

Bei Klick auf diese Schaltfläche wechselt der ElsterAuthenticator in den Vordergrund und Sie werden gebeten, die nötigen Informationen für die Durchführung der jeweiligen Aktion einzugeben, üblicherweise das Passwort für die Nutzung des privaten Schlüssels auf Ihrem Sicherheitsstick / Ihrer Signaturkarte.

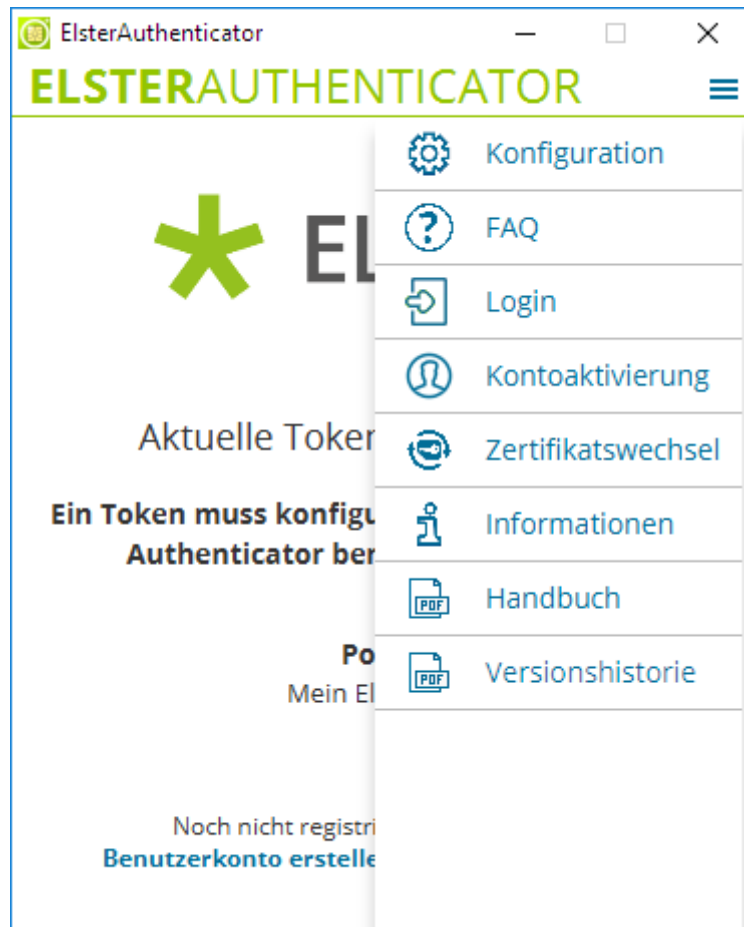
3.1. Beispiel: Login bei Mein ELSTER



Die Eingabe des Passworts erfolgt bei einigen Signaturkarten nicht über das Textfeld des ElsterAuthenticators, sondern über einen Passwort-Dialog der Treibersoftware bzw. über ein Tastenfeld des externen Kartenlesers. In diesem Fall ist kein Passwort-Eingabefeld im ElsterAuthenticator vorhanden und es ist der Hinweis „Passwort-Eingabe erfolgt über Kartentreiber-Software“ zu sehen.

3.1.1. Login unter Windows Server

Der Login auf dem Betriebssystem Windows Server muss zwingend vom ElsterAuthenticator aus erfolgen.



Mit einem Klick auf „Bei Mein ELSTER einloggen“ oder „Bei BZSt einloggen“ auf dem Startschirm oder dem Menüpunkt „Login“ im Konfigurationsmenü wird der System-Browser gestartet und auf die Login-Seite weitergeleitet.

HINWEIS Windows Server schränken den Betrieb eines Sicherheitstokens direkt am Windows Server ein. Der Betrieb eines Sicherheitstokens ist nur im Administrator Account möglich. Die Verwendung eines Sicherheitstokens in mehreren Benutzer-Accounts ist daher nicht möglich. Die übliche Benutzung sieht vor, den Sicherheitstoken am Client-Rechner zu betreiben und mit einer geeigneten Software (z. B. Microsoft-Remotedesktop) an den Remotecomputer durchzureichen.

3.1.2. Kontoaktivierung unter Windows Server

Die Kontoaktivierung auf dem Betriebssystem Windows Server muss über den ElsterAuthenticator mit dem Klick auf „Kontoaktivierung“ erfolgen.

3.2. Zertifikatswechsel

In diesem Abschnitt wird der Wechsel der Signaturkarte, der Wechsel von einer Signaturkarte zu einem Sicherheitsstick und der Wechsel von einem Sicherheitsstick auf einen anderen Sicherheitsstick beschrieben.

Hierfür müssen Sie sich in Mein ELSTER einloggen und im privaten Bereich einen „Zertifikatswechsel“ durchführen. Für den Wechsel erhalten Sie eine E-Mail mit der Aktivierungs-ID und eine Postfachnachricht in Mein ELSTER mit dem Aktivierungs-Code. Diese Nachricht müssen Sie mit Ihrer noch bestehenden Signaturkarte bzw. Ihrem noch bestehenden Sicherheitsstick speichern/sichern.

3.3. Wechsel der Signaturkarte

Der Zertifikatswechsel wird im Folgenden Schritt für Schritt erläutert. Bitte nehmen Sie sich die Zeit und lesen Sie die Anweisungen vor der Durchführung aufmerksam durch.

1. Loggen Sie sich mit der alten Signaturkarte und dem ElsterAuthenticator bei Mein ELSTER ein.
2. Wechseln Sie in Mein ELSTER zum Menüpunkt „Mein Benutzerkonto“.



Mein Benutzerkonto

3. Wählen Sie den Punkt „Zertifikatswechsel“.

Mein Benutzerkonto

Zertifikatswechsel >

Benutzerkonto aktivieren >

Login wieder ermöglichen >

Benutzerkonto löschen >

4. Wählen Sie nun den „Wechsel der Signaturkarte“ an.

Wechsel der Signaturkarte >

Ihrem Benutzerkonto bei Mein ELSTER wird eine andere Signaturkarte zugewiesen. Dies ist insbesondere dann sinnvoll, wenn der Gültigkeitszeitraum Ihrer Signaturkarte in Kürze abläuft.

5. Mit dem Bestätigen des Wechsels wird die Aktivierungs-ID an die bei der Registrierung angegebene E-Mail-Adresse versandt. Der Aktivierungs-Code wird in Ihrem Mein ELSTER Postfach („Mein Posteingang“) abgelegt.

Ich habe die Hinweise gelesen und möchte
fortfahren

6. Wechseln Sie nun in das Mein ELSTER Postfach und öffnen Sie die Nachricht mit dem Titel „Aktivierungscode für Zertifikatswechsel“.

☐  **Aktivierungscode für Zertifikatswechsel**

Sichern Sie das Dokument mit dem Aktivierungs-Code.

7. Loggen Sie sich aus Mein ELSTER aus.
8. Wechseln Sie in Ihr E-Mail Konto und öffnen Sie die E-Mail mit der Ihnen zugesandten Aktivierungs-ID. Bitte beachten Sie, dass der Versand der Aktivierungs-ID gegebenenfalls mehrere Minuten in Anspruch nehmen kann.
9. Beenden Sie den ElsterAuthenticator. Wenn Sie zu einem anderen Kartenanbieter gewechselt haben, deinstallieren Sie den Treiber für Ihre alte Signaturkarte und installieren Sie anschließend den Treiber für die neue Signaturkarte. Beachten Sie hierbei die Installationsanweisung des Herstellers.
10. Entnehmen Sie die alte Signaturkarte aus Ihrem Kartenleser und führen Sie die neue Signaturkarte in den Kartenleser ein.
11. Starten Sie den ElsterAuthenticator, wechseln Sie in die Konfiguration und stellen Sie die neue Signaturkarte ein. (siehe [Kapitel 2.4.2](#))
12. Öffnen Sie in Ihrem bevorzugten Browser die Seite <https://www.elster.de> und wechseln Sie im öffentlichen Bereich von „Mein Benutzerkonto“ zu „Zertifikatswechsel“. Anschließend klicken Sie auf den Punkt „Wechsel der Signaturkarte“ und wählen dort dann den Punkt „Registrierung der neuen Signaturkarte“ aus.

Registrierung der neuen Signaturkarte >

Sie haben die neuen Aktivierungsdaten erhalten. Nun können Sie Ihre neue Signaturkarte mit den Aktivierungsdaten bei ELSTER registrieren und Ihrem bisherigen Benutzerkonto zuweisen.

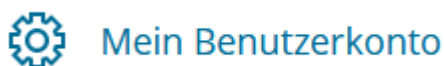
13. Mit dem Klick auf „Weiter mit ElsterAuthenticator“ der folgenden Seite wechselt der ElsterAuthenticator in den Vordergrund.

The screenshot shows a window titled "ElsterAuthenticator" with a green header bar containing the text "ELSTERAUTHENTICATOR". Below the header, the main title "Signaturkarte registrieren" is underlined. The form contains two input fields: "Aktivierungs-ID" and "Aktivierungs-Code". Below these fields, a note states "Passwort-Eingabe erfolgt über Kartentreiber-Software". At the bottom, there are two blue buttons: "Karte registrieren" and "Abbrechen".

14. Geben Sie nun die Aktivierungs-ID und den Aktivierungs-Code im ElsterAuthenticator ein und bestätigen Sie Ihre Angaben mit „Karte registrieren“. Das Passwort für die Signaturkarte muss am Kartenleser eingegeben werden. Nach dem erfolgreichen Signaturkarten-Wechsel werden Sie automatisch in Mein ELSTER eingeloggt.

3.4. Wechsel von Signaturkarte zu Sicherheitsstick

1. Loggen Sie sich mit der alten Signaturkarte und dem ElsterAuthenticator bei Mein ELSTER ein.
2. Wechseln Sie in Mein ELSTER zum Menüpunkt „Mein Benutzerkonto“.



3. Wählen Sie den Punkt „Zertifikatswechsel“.

Mein Benutzerkonto

Zertifikatswechsel >

Benutzerkonto aktivieren >

Login wieder ermöglichen >

Benutzerkonto löschen >

4. Wählen Sie nun den „Wechsel von Signaturkarte zu Sicherheitsstick“.

Wechsel von Signaturkarte zu Sicherheitsstick >

Ihr Benutzerkonto bei Mein ELSTER, das Sie bisher mit einer Signaturkarte genutzt haben, wird auf einen Sicherheitsstick umgestellt.

5. **Bitte beachten Sie, dass mit dem Zertifikatswechsel Änderungen der Berechtigungen Ihres Benutzerkontos verbunden sind.**

Bestätigen Sie bitte die Berechtigungs-Änderungen.

Ich habe die Hinweise gelesen und möchte
fortfahren

6. Wechseln Sie nun in das Mein ELSTER Postfach („Mein Posteingang“) und öffnen Sie die Nachricht mit dem Titel „Aktivierungscode für Zertifikatswechsel“.

☐  **Aktivierungscode für Zertifikatswechsel**

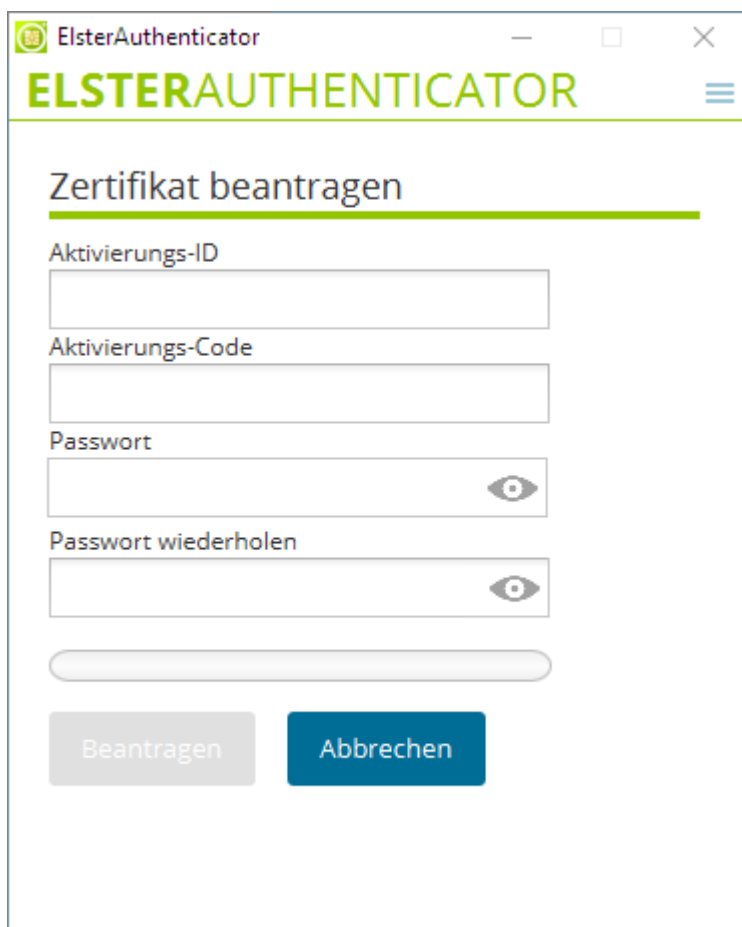
Sichern Sie das Dokument mit dem Aktivierungs-Code.

7. Loggen Sie sich aus Mein ELSTER aus.
8. Wechseln Sie in Ihr E-Mail Konto und öffnen Sie die E-Mail mit der Ihnen zugesandten Aktivierungs-ID. Bitte beachten Sie, dass der Versand der Aktivierungs-ID gegebenenfalls mehrere Minuten in Anspruch nehmen kann.
9. Bitte Signaturkarte entfernen, Kartenleser vom Rechner trennen und gegebenenfalls Signaturkarten-Treiber deinstallieren.
10. Schließen Sie den Sicherheitsstick an Ihrem Rechner an. Bei der ersten Verwendung des Sicherheitssticks warten Sie bitte bis die Windows-Hardwareerkennung den Sicherheitsstick eingebunden hat. Dieser wird anschließend im Windows Gerätemanager angezeigt.
11. Installieren Sie gegebenenfalls den Treiber für den Sicherheitsstick. Wechseln Sie anschließend zum ElsterAuthenticator und rufen Sie die Konfiguration auf. Stellen Sie den Sicherheitsstick ein. (siehe [Kapitel 2.4.2](#)) Beachten Sie hierbei die Installationsanweisung des Herstellers.
12. Öffnen Sie in Ihrem bevorzugten Browser die Seite <https://www.elster.de> und wechseln Sie im öffentlichen Bereich von „Mein Benutzerkonto“ zu „Zertifikatswechsel“, „Wechsel von Signaturkarte zu Sicherheitsstick“. Dort wählen Sie den Punkt „Aktivierung und erstmaliges Login mit neuem Zertifikat“ aus.

Aktivierung und erstmaliges Login mit neuem Zertifikat >

Sie haben die neuen Aktivierungsdaten erhalten. In diesem Schritt können Sie nun Ihr neues Zertifikat erzeugen.

13. Mit dem Klick auf „Weiter mit ElsterAuthenticator“ der folgenden Seite wechselt der ElsterAuthenticator in den Vordergrund.

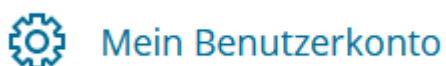


The screenshot shows a web browser window titled 'ElsterAuthenticator'. The main heading is 'ELSTERAUTHENTICATOR' in green. Below it, the section 'Zertifikat beantragen' is underlined in green. The form contains four input fields: 'Aktivierungs-ID', 'Aktivierungs-Code', 'Passwort' (with an eye icon for visibility), and 'Passwort wiederholen' (also with an eye icon). Below these fields is a horizontal progress bar. At the bottom, there are two buttons: 'Beantragen' (disabled, grey) and 'Abbrechen' (active, blue).

14. Geben Sie nun bitte die Aktivierungs-ID, den Aktivierungs-Code, das Passwort und die Passwort-Wiederholung im ElsterAuthenticator ein und bestätigen Sie Ihre Angaben mit „Beantragen“. Nach dem erfolgreichen Wechsel zum Sicherheitsstick werden Sie automatisch in Mein ELSTER eingeloggt.

3.5. Wechsel des Sicherheitssticks

1. Loggen Sie sich mit Ihrem alten Sicherheitstoken und dem ElsterAuthenticator bei Mein ELSTER ein.
2. Wechseln Sie in Mein ELSTER zum Menüpunkt „Mein Benutzerkonto“.



3. Wählen Sie den Punkt „Zertifikatswechsel“.

Mein Benutzerkonto

Zertifikatswechsel >

Benutzerkonto aktivieren >

Login wieder ermöglichen >

Benutzerkonto löschen >

4. Wählen Sie nun den „Wechsel des Sicherheitssticks“.

Wechsel des Sicherheitssticks >

Ihrem Benutzerkonto bei Mein ELSTER wird ein anderer Sicherheitsstick zugewiesen.

5. Bestätigen Sie den Wechsel.

Ich habe die Hinweise gelesen und möchte
fortfahren

6. Wechseln Sie nun in das Mein ELSTER Postfach („Mein Posteingang“) und öffnen Sie die Nachricht mit dem Titel „Aktivierungscode für Zertifikatswechsel“.

☐  **Aktivierungscode für Zertifikatswechsel**

Sichern Sie das Dokument mit dem Aktivierungs-Code.

7. Loggen Sie sich aus Mein ELSTER aus.
8. Wechseln Sie in Ihr E-Mail Konto und öffnen Sie die E-Mail mit der Ihnen zugesandten Aktivierungs-ID. Bitte beachten Sie, dass der Versand der Aktivierungs-ID gegebenenfalls mehrere Minuten in Anspruch nehmen kann.
9. Trennen Sie den alten Sicherheitsstick von Ihrem Rechner und deinstallieren Sie gegebenenfalls den Treiber für den alten Sicherheitsstick.
10. Stecken Sie den neuen Sicherheitsstick an einen freien USB-Steckplatz. Achten Sie darauf, dass kein USB-Hub zwischengeschaltet ist, sondern die Verbindung direkt erfolgt. Die Status-LED muss flackerfrei durchgehend leuchten.
11. Bei der ersten Verwendung des neuen Sicherheitssticks warten Sie bitte bis die Windows Hardwareerkennung den Sicherheitsstick eingebunden hat. Dieser wird anschließend im Windows Gerätemanager angezeigt.
12. Installieren Sie gegebenenfalls den Treiber für den neuen Sicherheitsstick.
13. Wechseln Sie anschließend zum ElsterAuthenticator und rufen Sie die Konfiguration auf. Stellen Sie den neuen Sicherheitsstick ein. (siehe [Kapitel 2.4.2](#)) Beachten Sie hierbei die

Installationsanweisung des Herstellers.

14. Öffnen Sie in Ihrem bevorzugten Browser die Seite <https://www.elster.de> und wechseln Sie im öffentlichen Bereich von „Mein Benutzerkonto“ zu „Zertifikatswechsel“, „Wechsel des Sicherheitssticks“. Dort wählen Sie den Punkt „Aktivierung und erstmaliges Login mit neuem Zertifikat“ aus.

Aktivierung und erstmaliges Login mit neuem Zertifikat >

Sie haben die neuen Aktivierungsdaten erhalten. In diesem Schritt können Sie nun Ihr neues Zertifikat erzeugen.

15. Mit dem Klick auf „Weiter mit ElsterAuthenticator“ der folgenden Seite wechselt der ElsterAuthenticator in den Vordergrund.

The screenshot shows a window titled 'ElsterAuthenticator' with a green header bar containing the text 'ELSTERAUTHENTICATOR'. Below the header, the main title 'Zertifikat beantragen' is displayed. The form contains four input fields: 'Aktivierungs-ID', 'Aktivierungs-Code', 'Passwort', and 'Passwort wiederholen'. The password fields have eye icons for toggling visibility. Below the input fields is a large, light blue button labeled 'Beantragen' and a smaller, dark blue button labeled 'Abbrechen'.

16. Geben Sie nun bitte die Aktivierungs-ID, den Aktivierungs-Code, das Passwort und die Passwort-Wiederholung im ElsterAuthenticator ein und bestätigen Sie Ihre Angaben mit „Beantragen“. Nach dem erfolgreichen Wechsel zum neuen Sicherheitsstick werden Sie automatisch in Mein ELSTER eingeloggt.

3.6. Herunterladen von Dateien

Das Herunterladen von Dateien ist eine der zentralen Funktionen des ElsterAuthenticators. Die Dateien können im .CSV-, .HTML-, .JPEG-, .PDF-, .PNG-, .TXT-, .XML- oder .ZIP-Format

vorliegen.

Das Herunterladen wird im ausgewählten Portal (z. B. Mein ELSTER) gestartet, woraufhin das Hauptfenster des ElsterAuthenticators im Vordergrund angezeigt wird und eine Liste der herunterzuladenen Dateien anzeigt.

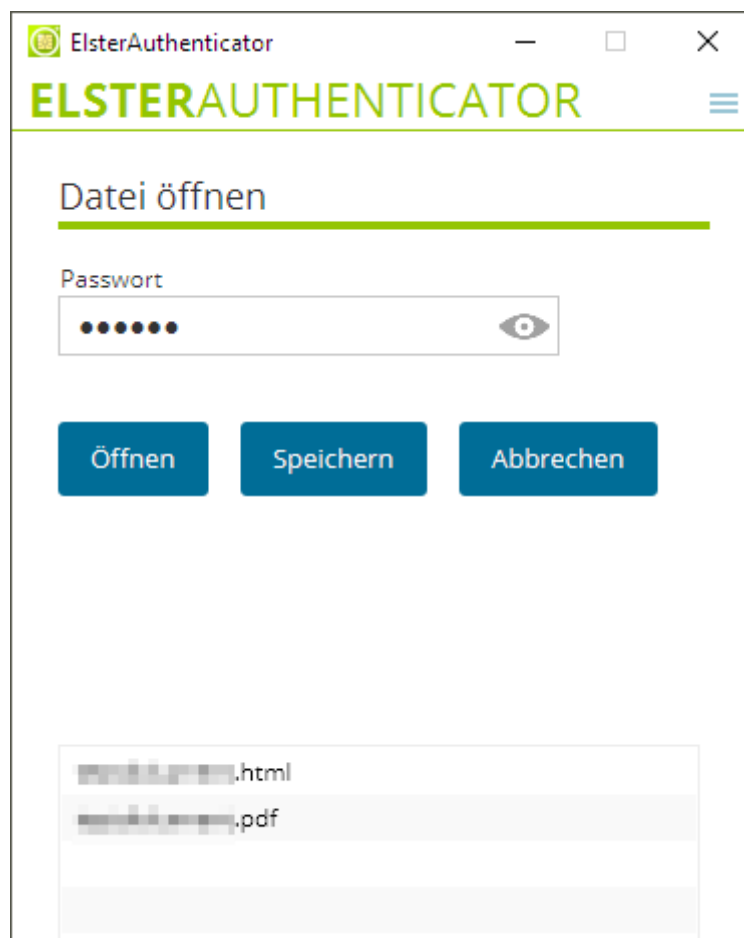
Je nachdem, ob in der Liste der durch das Portal bereitgestellten Dateien auch verschlüsselte Dateien enthalten sind, wird zusätzlich ein Passwort-Eingabefeld angezeigt.

HINWEIS Sofern das Passwort-Caching aktiv ist, wird das Passwort aus dem Login bereits vorbelegt und muss nicht neu eingegeben werden.

Nun kann über die Schaltflächen "Öffnen" bzw. "Speichern" ausgewählt werden, ob die Dateien

- zur lesenden Anzeige geöffnet
- auf dem Dateisystem gespeichert

werden sollen.



Sofern die Dateien verschlüsselt sind, werden diese durch den ElsterAuthenticator entschlüsselt und (entsprechend obiger Auswahl) entweder auf dem Dateisystem des Computers gespeichert oder

temporär vorgehalten und anschließend zur Ansicht geöffnet. Hierfür werden die auf dem Computer installierten und als Standard für den jeweiligen Dateitypen verknüpften Anwendungen (z. B. der Adobe Acrobat Reader für .PDF-Dateien) verwendet. In diesem Falle werden die temporär vorgehaltenen Dateien nach der Beendigung des ElsterAuthenticators sicher entfernt.

Wenn die Dateien gespeichert werden sollen, wird ein Dialog zur Verzeichnis-Auswahl angezeigt, der die Auswahl eines Zielverzeichnisses ermöglicht. In diesem Fall werden die gespeicherten Dateien nicht automatisch geöffnet.