

Elektronischer Befähigungsausweis für Sicherungspersonale (EIBa)

Anleitung für die Registrierung und Anmeldung mit einem Sicherheitsschlüssel

Inhaltsverzeichnis

<u>1 Was ist FIDO2?</u>	<u>3</u>
1.1 Inhalt dieser Anleitung	3
1.2 Sicherheit	3
<u>2 Registrierung</u>	<u>5</u>
2.1 Voraussetzungen	5
2.2 Registrierungsmail	5
2.3 Klick auf den Link	5
2.4 Möglicher Fehlerfall: Registrierungslink abgelaufen	6
2.5 Registrierungsmaske	6
2.6 Bestätigung der Registrierung	7
2.7 Bestätigung der Datenübertragung	7
2.8 Möglicher Fehlerfall: Windows Hello eingerichtet	7
2.9 (Optional): Einstecken des Sicherheitsschlüssels	9
2.10 Einrichtung der PIN	9
2.11 Möglicher Fehlerfall: PIN abgelehnt	10
2.12 (Optional) Sicherheitsschlüssel antippen	11
2.13 Erfolgreiche Registrierung	11
<u>3 Anmeldung</u>	<u>12</u>
3.1 Voraussetzungen	12
3.2 Aufrufen der EIBa WebApp	12
3.3 (Optional) Wahl der Anmeldeart	12
3.4 Eingabe der E-Mail Adresse	13
3.5 Möglicher Fehlerfall: E-Mail-Adresse falsch	13
3.6 Möglicher Fehlerfall: Windows Hello PIN eingerichtet	14
3.7 Möglicher Fehlerfall: Sicherheitsschlüssel nicht verbunden	15
3.8 PIN-Eingabe	15
3.9 (Optional) Sicherheitsschlüssel antippen	16
3.10 Möglicher Fehlerfall: Falscher Sicherheitsschlüssel	16
3.11 Anmeldung erfolgreich	17

1 Was ist FIDO2?

In EIBa werden sensible personenbezogene Daten verarbeitet. Es ist wichtig, diese Daten vor unbefugten Zugriffen zu schützen. Dazu ist es nicht ausreichend Ihr Benutzerkonto nur mit einem Passwort zu versehen, welches früher oder später erraten werden kann.

Im Bereich der Computersicherheit hat sich durchgesetzt, dass Sie, um sich anzumelden, nicht nur ein Geheimnis wissen müssen (das ist Ihr Passwort), sondern auch im Besitz eines einmaligen Gegenstandes sein müssen, welcher bei Verlust gesperrt werden kann.

Bisher wurde in EIBa dazu ein Verfahren eingesetzt, bei dem Sie in regelmäßigen Abständen oder bei Anmeldung an einem neuen Computer durch die Eingabe eines sechsstelligen Codes beweisen mussten, dass Sie im Besitz Ihres Mobiltelefons sind. Zur Erhöhung des Komforts, insbesondere bei der Registrierung, wird in EIBa dieses Verfahren nun durch den Industriestandard FIDO2 ersetzt.

In diesem Rahmen bietet EIBa mehrere Möglichkeiten zur Anmeldung:

1. Sie beweisen, dass Sie von einem bestimmten Computer aus arbeiten (das ist der Gegenstand). Sie beweisen außerdem, dass Sie einen speziellen Speicher auf diesem Computer mit einer PIN, einem Fingerabdruck o.Ä. entsperren können (das ist das Geheimnis).
Dies hat den Nachteil, dass eine Anmeldung in EIBa von einem anderen Computer aus für Sie nicht mehr möglich ist. Die Einrichtung von mehreren Computern für Ihre Anmeldung wird von EIBa nicht unterstützt.
Dieses Verfahren wird unter Windows 10 mit der Funktion „Windows Hello“ durchgeführt. Diese Funktion muss normalerweise durch Sie oder Ihren Administrator auf Ihrem Computer aktiviert werden.
Die Einrichtung von Windows Hello ist **nicht** Gegenstand dieser Anleitung.
2. Sie beweisen, dass Sie im Besitz eines speziellen Gerätes, dem „Sicherheitsschlüssel“ sind, der vorher mit Ihrem Benutzerkonto registriert wurde und der mit dem Computer verbunden ist. Sie beweisen außerdem, dass Sie die PIN kennen, mit der dieser Sicherheitsschlüssel entsperrt werden kann.
Dadurch, dass der Sicherheitsschlüssel nicht dauerhaft mit dem Computer verbunden werden muss, können Sie ihn an verschiedenen Computern verwenden.
Dies ist das von uns empfohlene Verfahren.
Diese Anleitung beschreibt die Registrierung eines solchen Sicherheitsschlüssels am Beispiel eines YubiKey Security Key NFC oder eines YubiKey 5 NFC FIPS.

1.1 Inhalt dieser Anleitung

Diese Anleitung beschreibt die Einrichtung eines Sicherheitsschlüssels für die Anmeldung in EIBa und den Anmeldeprozess.

1.2 Sicherheit

Um die Sicherheit der Anmeldung zu gewährleisten ist es wichtig, dass Sie folgende Punkte beachten:

- Der verwendete Sicherheitsschlüssel ist personengebunden. Es ist nicht zulässig, dass mehrere Personen denselben Sicherheitsschlüssel verwenden, da ansonsten mehrere Personen die PIN des Sicherheitsschlüssels kennen müssten.
- Nutzen Sie keine leicht zu erratene PIN für Ihren Sicherheitsschlüssel, wie z.B. „123“ oder Ihr Geburtsdatum. Die PIN muss bei Verlust des Sicherheitsschlüssels so schwer

zu erraten sein, dass Sie den Verlust schneller bemerken als der Finder Zeit braucht, um die PIN zu raten, damit der Sicherheitsschlüssel rechtzeitig in EIBa gesperrt werden kann.

Anders als z.B. Ihre Bankkarte erlauben Sicherheitsschlüssel wie der YubiKey auch **PINs, die nicht nur aus Zahlen, sondern auch aus Klein- und Großbuchstaben sowie Sonderzeichen bestehen**. Die PIN kann auch länger als vier Zeichen sein. Nutzen Sie diese Möglichkeiten. Halten Sie die Mindestanforderungen Ihres Unternehmens für Passwörter auch bei der Vergabe der PIN ein.

- Merken Sie sich die PIN Ihres Sicherheitsschlüssels und notieren Sie diese nicht. Notieren Sie insbesondere die PIN **nicht** auf Ihrem Sicherheitsschlüssel oder auf einem Zettel, den Sie zusammen mit dem Sicherheitsschlüssel oder an Ihrem Arbeitsplatz aufbewahren.
- Wenden Sie sich bei Verlust Ihres Sicherheitsschlüssels umgehend an die fachliche Betriebsführung, damit er gesperrt und später ein neuer Sicherheitsschlüssel eingerichtet werden kann. Selbst wenn Sie noch keinen Ersatz haben, ist es trotzdem wichtig, den verlorenen Sicherheitsschlüssel umgehend in EIBa zu sperren.

2 Registrierung

2.1 Voraussetzungen

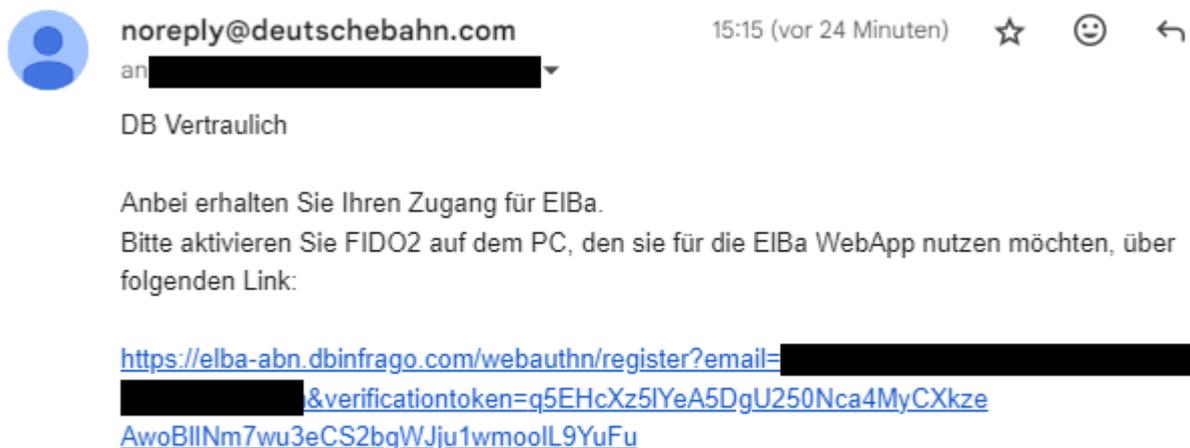
Diese Anleitung geht davon aus, dass auf Ihrem Computer Windows 10 mit den neuesten Sicherheits- und Funktionsupdates installiert ist (Stand 04.04.2024). Diese Anleitung nutzt Chrome als Browser. Auf dem Computer muss Zugang zu dem E-Mail-Konto bestehen, mit dem Sie in EIBa registriert sind. Bitte halten Sie Ihren Sicherheitsschlüssel bereit, für einige Schritte im Registrierungsprozess steht nur eine begrenzte Zeit zur Verfügung.

Wenn auf Ihrem Computer die Funktion „Windows Hello“ aktiviert ist, kann der Prozess in einigen Fällen abweichen. Diese Anleitung weist auf einige mögliche Abweichungen an den entsprechenden Stellen hin. Bitte wenden Sie sich gegebenenfalls an den Administrator in Ihrem Unternehmen, wenn Sie andere Dialoge bei der Registrierung sehen und nicht fortfahren können.

2.2 Registrierungsmail

Sie erhalten von EIBa eine E-Mail wie folgt. Bitte beachten Sie dabei:

1. Der Link in der E-Mail kann benutzt werden, um genau einen Computer oder einen Sicherheitsschlüssel bei EIBa zu registrieren. Nach *erfolgreicher* Registrierung wird der Link abgeschaltet. Solange die Registrierung nicht erfolgreich war, können Sie den Registrierungsprozess durch erneutes Klicken des Links aber neu starten.
2. Der Link in der E-Mail ist nur begrenzte Zeit gültig

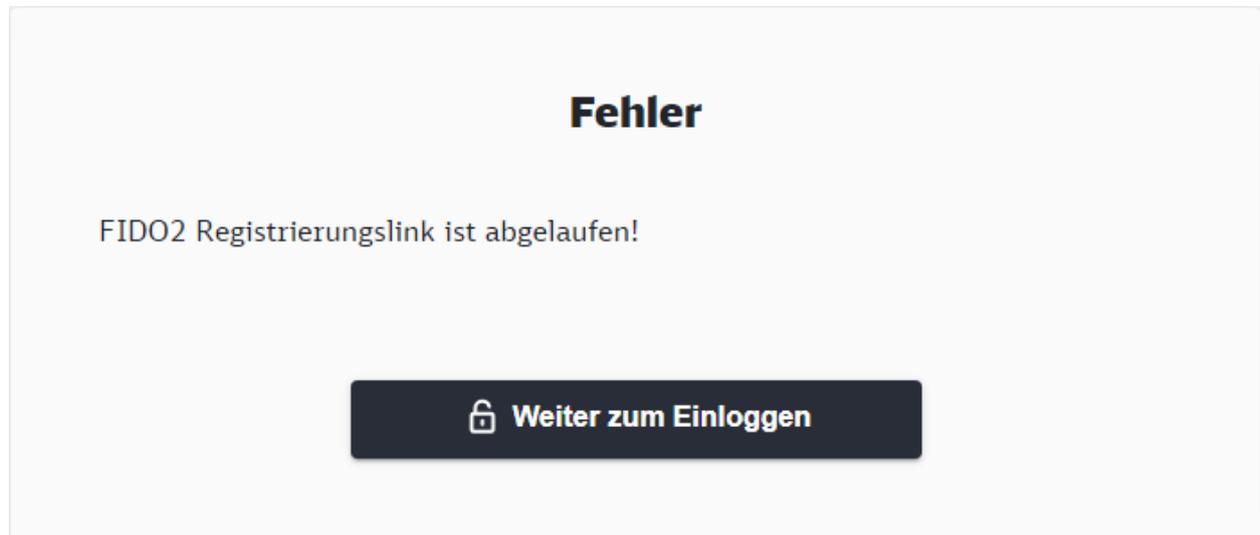


2.3 Klick auf den Link

Um den Registrierungsprozess zu starten, klicken Sie auf den Registrierungslink in der E-Mail. Es öffnet sich die EIBa WebApp.

2.4 Möglicher Fehlerfall: Registrierungslink abgelaufen

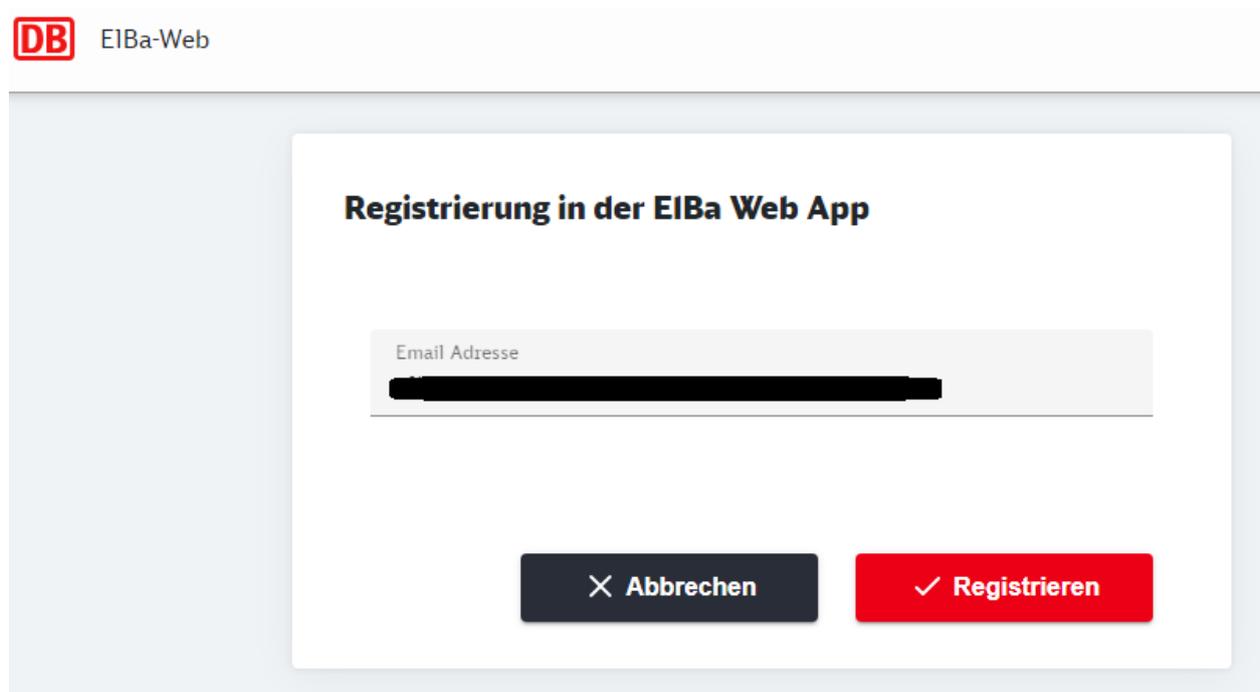
Wenn Sie die folgende Fehlermeldung sehen, dann wurde der Registrierungslink entweder bereits erfolgreich verwendet oder er ist abgelaufen. In diesem Fall melden Sie sich bitte bei der fachlichen Betriebsführung.



2.5 Registrierungsmaske

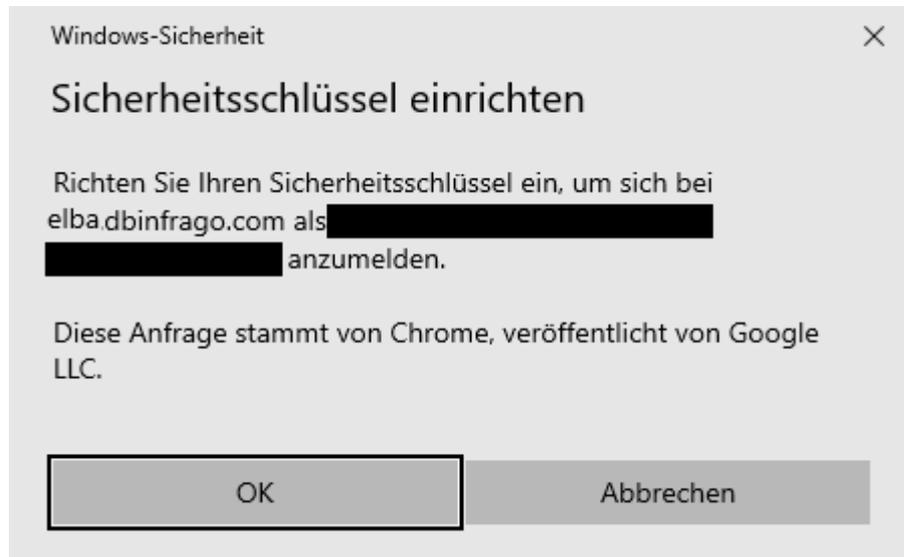
Wenn der Registrierungslink gültig ist, dann sehen Sie die folgende Eingabemaske. Ihre E-Mail-Adresse wird vorausgefüllt. **Ändern Sie die E-Mail-Adresse nicht**, da der Registrierungslink nur für diese Adresse gültig ist.

Klicken Sie in der Registrierungsmaske auf den Knopf „Registrieren“.



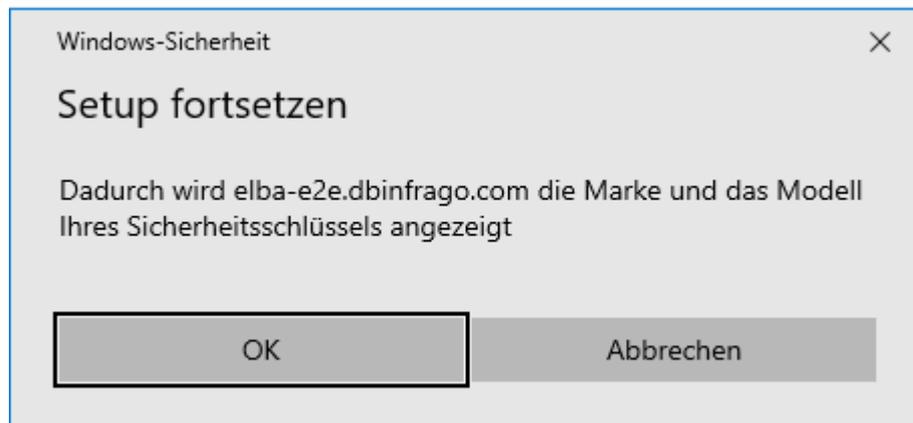
2.6 Bestätigung der Registrierung

Es öffnet sich außerhalb von Chrome das folgende Fenster. Stellen Sie sicher, dass Sie sich bei *elba.dbinfrago.com* anmelden und dass Ihre E-Mail-Adresse korrekt ist. Klicken Sie dann auf „OK“.



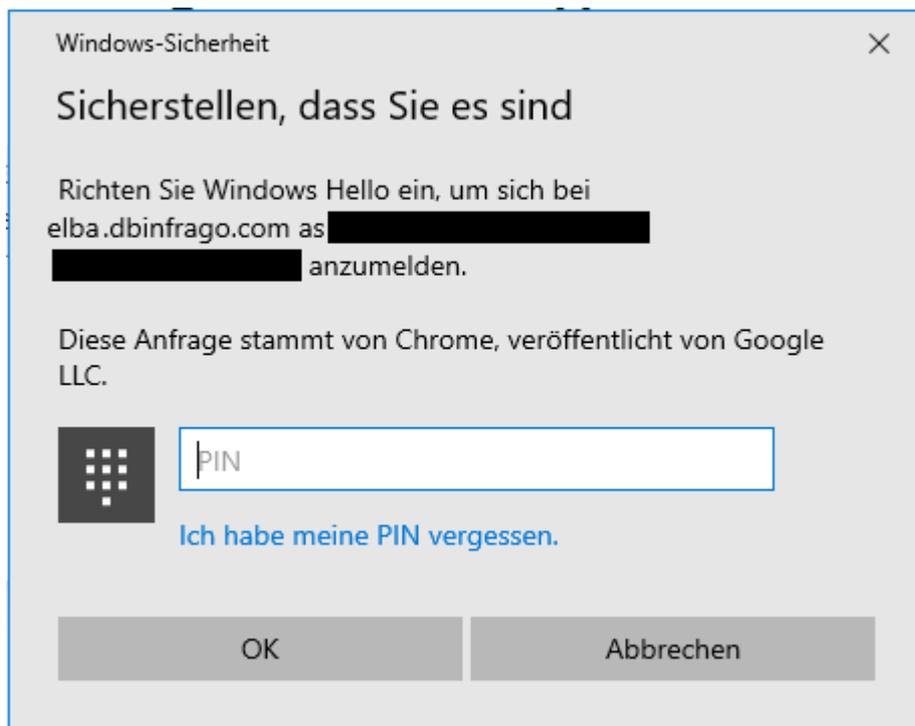
2.7 Bestätigung der Datenübertragung

Es öffnet sich folgendes Fenster. Fahren Sie mit einem Klick auf „OK“ fort.



2.8 Möglicher Fehlerfall: Windows Hello eingerichtet

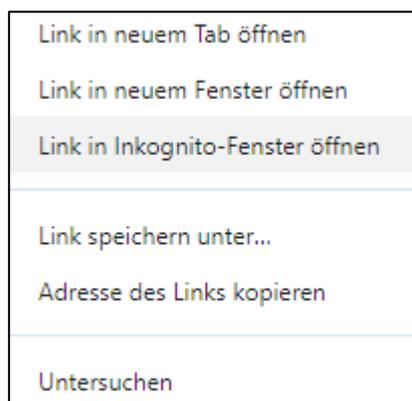
Wenn sich statt des obigen Fensters das folgende Fenster öffnet, dann ist auf Ihrem Computer Windows Hello mit PIN eingerichtet.



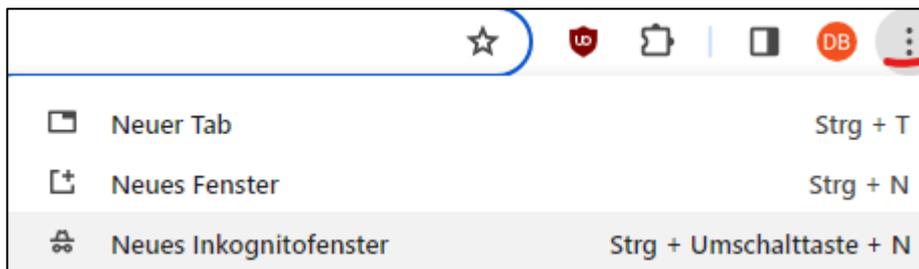
In diesem Fall klicken Sie auf „Abbrechen“. In den meisten Fällen sollte sich dann einer der Dialoge „Bestätigung der Datenübertragung“, „Einstecken des Sicherheitsschlüssels“ oder „Einrichtung der PIN“ öffnen und Sie können an der entsprechenden Stelle dieser Anleitung fortfahren.

Wenn das nicht der Fall ist, dann beenden Sie den Registrierungsprozess, indem Sie in allen weiteren Fenstern auf „Abbrechen“ klicken.

Wenn Sie die Registrierungsmail im Browser geöffnet haben, dann rufen Sie erneut die Registrierungsmail auf, starten Sie aber dieses Mal den Registrierungsprozess nicht durch einen Klick auf den Link, sondern durch einen Rechtsklick auf den Link und wählen Sie die Option „Link in Inkognito-Fenster öffnen“. Führen Sie dann den Registrierungsprozess durch.



Wenn Sie die Registrierungsmail nicht im Browser sondern in einem externen E-Mail-Programm geöffnet haben, dann kopieren Sie die Adresse des Registrierungslinks durch einen Rechtsklick auf den Link und einen Klick auf „Adresse des Links kopieren“. Öffnen Sie dann ein neues Inkognito-Fenster, indem Sie im Browser auf die drei Punkte oben rechts klicken und die Option „Neues Inkognitofenster“ wählen.

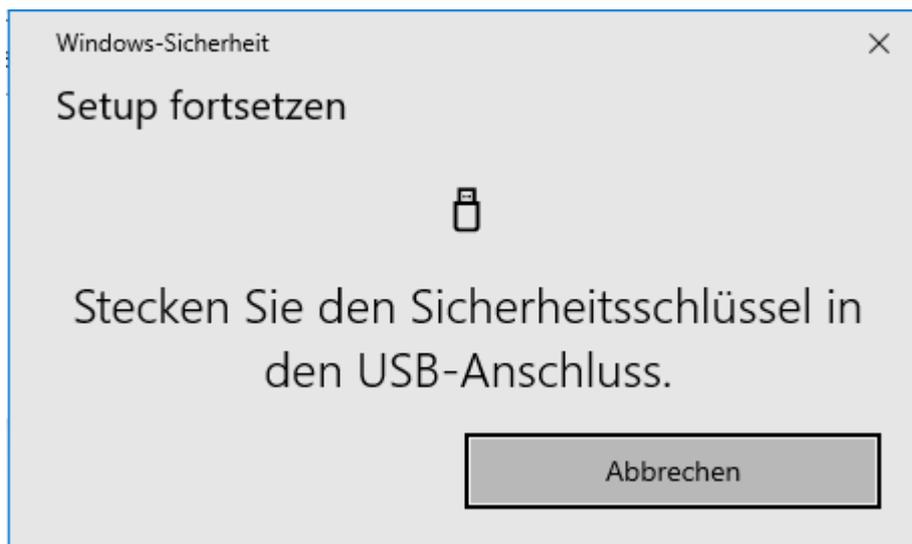


Fügen Sie dann den kopierten Registrierungslink in die Adresszeile des neuen Fensters ein und besuchen Sie die Adresse. Dann können Sie den Registrierungsprozess durchführen.

Aus einem Inkognito-Fenster besteht in den meisten Fällen kein Zugriff auf Windows Hello, so dass automatisch versucht wird, Ihren Sicherheitsschlüssel zu registrieren. Sollte die Registrierung auch so nicht möglich sein, dann wenden Sie sich bitte an Ihren Administrator.

2.9 (Optional): Einstecken des Sicherheitsschlüssels

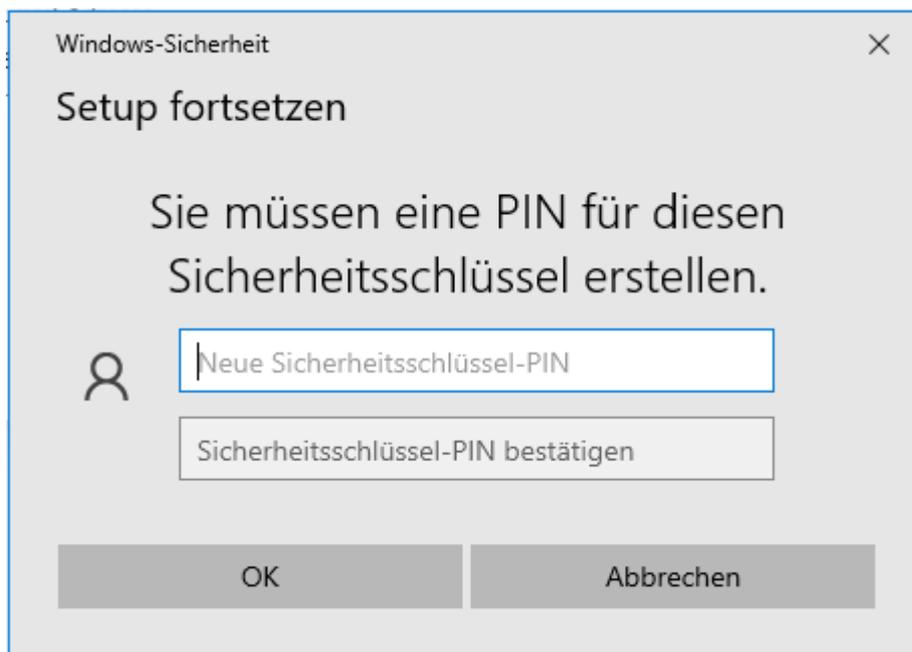
Wenn der Sicherheitsschlüssel noch nicht in einem USB-Anschluss Ihres Computers angebracht ist, dann wird der folgende Dialog angezeigt. Bitte stecken Sie den Sicherheitsschlüssel ein. Der Dialog verschwindet mit dem Einstecken automatisch.



2.10 Einrichtung der PIN

Im folgenden Dialog werden Sie dazu aufgefordert, die PIN Ihres Sicherheitsschlüssels zu vergeben. Bitte beachten Sie, dass (je nach verwendetem Sicherheitsschlüssel) **nicht nur Zahlen, sondern auch Buchstaben und Sonderzeichen** erlaubt sind. Nutzen Sie diese Möglichkeit, um die PIN sicherer zu machen. Beachten Sie ggf. auch die Vorgaben Ihres Unternehmens zur Passwortsicherheit. Merken Sie sich die PIN oder speichern Sie die PIN in einem Passwortmanager, auf den nur Sie Zugriff haben. Notieren Sie die PIN nicht. Notieren Sie auf keinen Fall die PIN auf dem Sicherheitsschlüssel oder auf einem Zettel, den Sie zusammen mit dem Sicherheitsschlüssel aufbewahren.

Die PIN muss zweimal übereinstimmend eingegeben werden. Bestätigen Sie danach mit einem Klick auf „OK“.



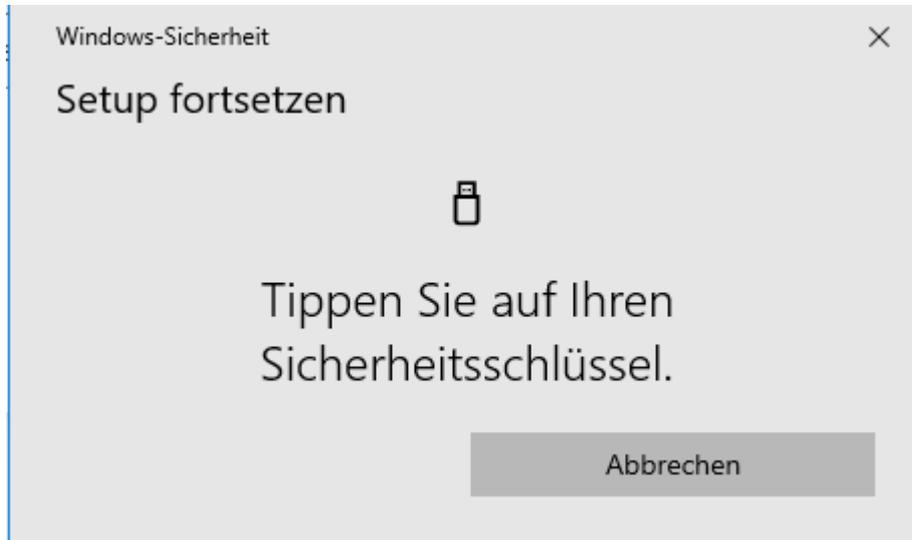
2.11 Möglicher Fehlerfall: PIN abgelehnt

Je nach verwendetem Sicherheitsschlüssel kann es sein, dass der Sicherheitsschlüssel Mindestanforderungen an die PIN stellt. Dies ist z.B. beim FIPS-Modell des YubiKey 5 der Fall. Wenn Ihre PIN den Sicherheitsansprüchen Ihres Sicherheitsschlüssels nicht entspricht, dann sehen Sie den folgenden Fehler. Starten Sie in diesem Fall den Registrierungsprozess erneut und wählen Sie eine komplexere PIN (mit Buchstaben, Zahlen und Sonderzeichen) und/oder eine längere PIN.



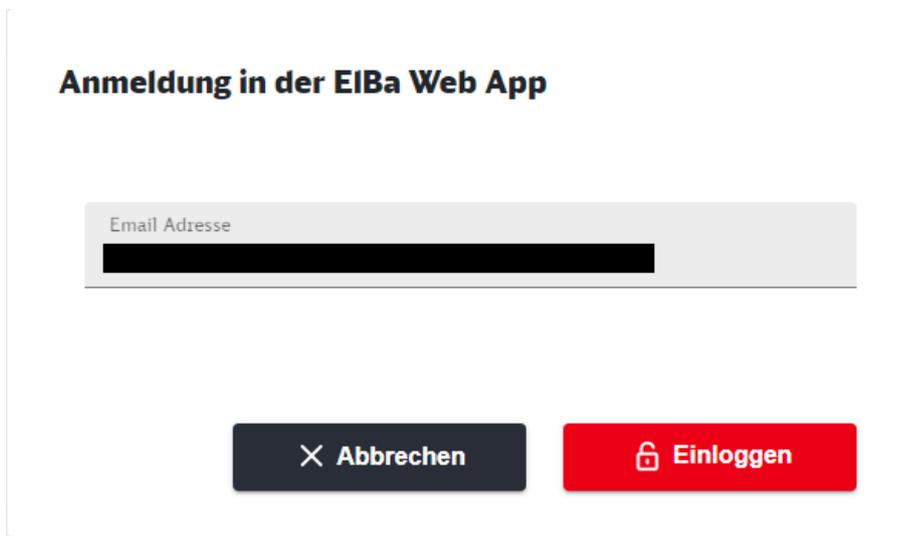
2.12 (Optional) Sicherheitsschlüssel antippen

Je nach verwendetem Sicherheitsschlüssel kann es nötig sein, den Sicherheitsschlüssel freizuschalten. Wenn Sie den folgenden Dialog sehen, dann drücken Sie (im Falle eines YubiKey) auf den mittig befindlichen runden, goldenen Kontakt um fortzufahren.



2.13 Erfolgreiche Registrierung

Ihr Sicherheitsschlüssel wird nun in EIBa mit Ihrem Benutzerkonto verbunden. Wenn dies erfolgreich war, wechselt die EIBa WebApp zur Anmeldemaske und Ihre E-Mail wird vorausgefüllt:



Wenn Sie stattdessen eine Fehlermeldung in der Registrierungsfläche sehen, dann wenden Sie sich bitte an die fachliche Betriebsführung.

3 Anmeldung

3.1 Voraussetzungen

Diese Anleitung geht davon aus, dass auf Ihrem Computer Windows 10 mit den neuesten Sicherheits- und Funktionsupdates installiert ist (Stand 04.04.2024). Bitte halten Sie Ihren Sicherheitsschlüssel bereit.

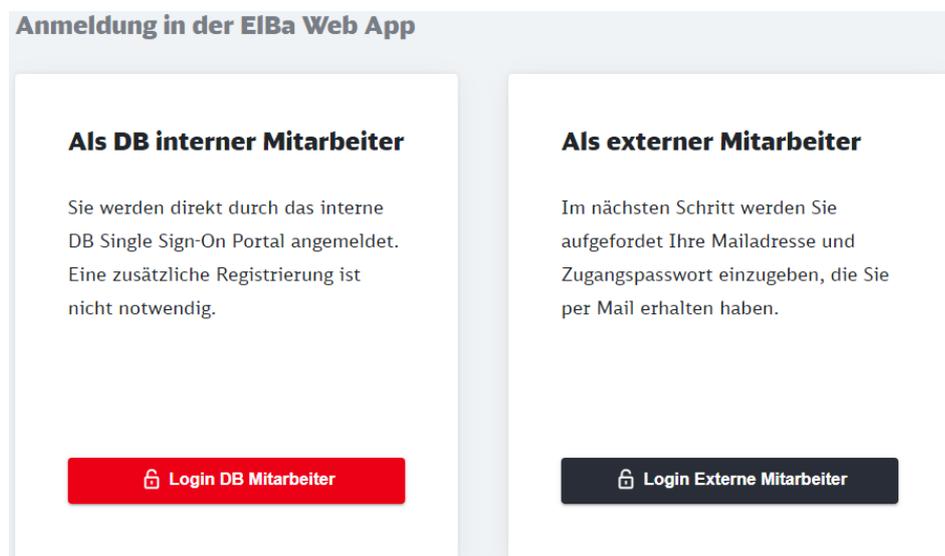
Wenn auf Ihrem Computer die Funktion „Windows Hello“ aktiviert ist, kann der Prozess in einigen Fällen abweichen. Diese Anleitung weist auf einige mögliche Abweichungen an den entsprechenden Stellen hin. Bitte wenden Sie sich gegebenenfalls an den Administrator in Ihrem Unternehmen, wenn Sie andere Dialoge bei der Registrierung sehen und nicht fortfahren können.

3.2 Aufrufen der EIBa WebApp

Öffnen Sie Ihren Browser und navigieren Sie zu <https://elba.dbinfrago.com>.

3.3 (Optional) Wahl der Anmeldeart

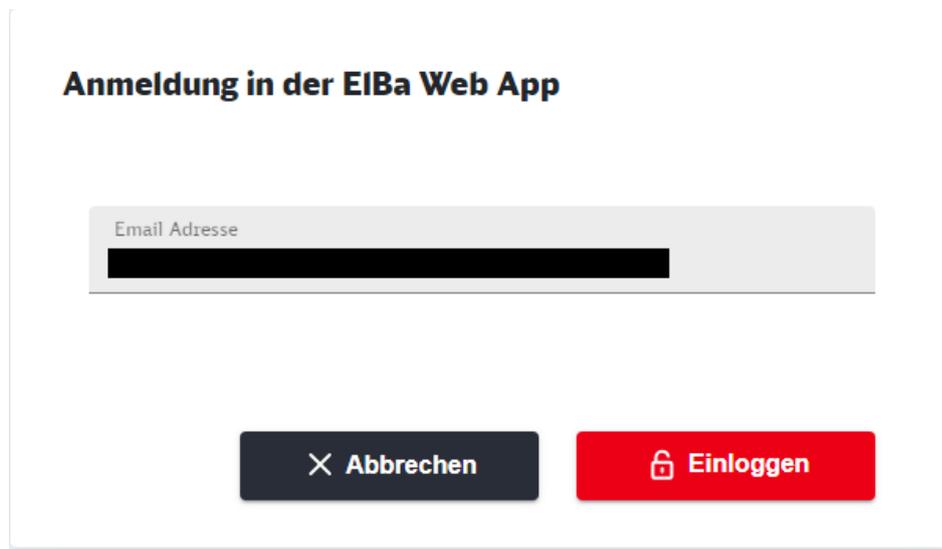
Wenn Sie EIBa auf diesem Computer das erste Mal aufrufen oder einen Inkognito-Fenster verwenden, dann werden Sie dazu aufgefordert, die Anmeldeart auszuwählen. Klicken Sie auf „Login Externe Mitarbeiter“.



The screenshot shows a web interface titled "Anmeldung in der EIBa Web App". It features two main selection cards side-by-side. The left card is titled "Als DB interner Mitarbeiter" and contains the text: "Sie werden direkt durch das interne DB Single Sign-On Portal angemeldet. Eine zusätzliche Registrierung ist nicht notwendig." Below this text is a red button with a lock icon and the text "Login DB Mitarbeiter". The right card is titled "Als externer Mitarbeiter" and contains the text: "Im nächsten Schritt werden Sie aufgefordert Ihre Mailadresse und Zugangspasswort einzugeben, die Sie per Mail erhalten haben." Below this text is a dark grey button with a lock icon and the text "Login Externe Mitarbeiter".

3.4 Eingabe der E-Mail-Adresse

Die EIBa WebApp öffnet nun die Eingabemaske zur Anmeldung. Geben Sie in das Eingabefeld die E-Mail-Adresse ein, mit der Sie bei EIBa registriert sind und bestätigen Sie durch einen Klick auf „Einloggen“.

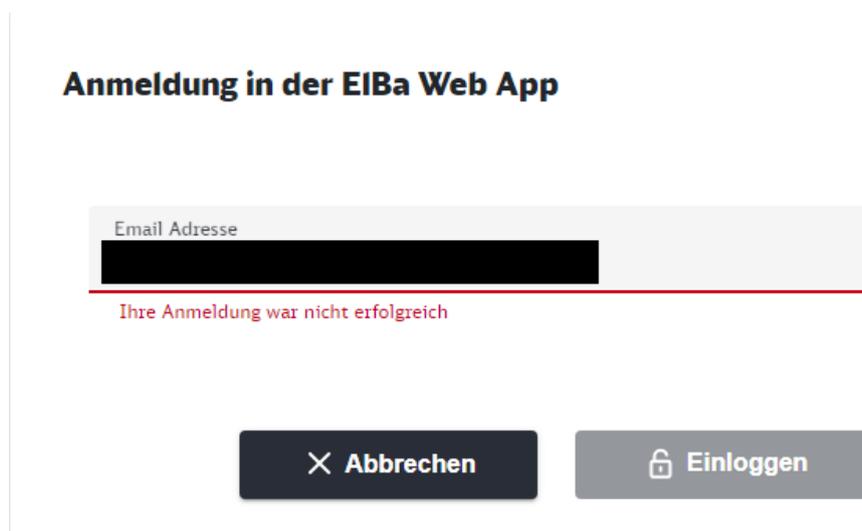


The screenshot shows a login form titled "Anmeldung in der EIBa Web App". It features a text input field labeled "Email Adresse" with a blacked-out email address. Below the input field are two buttons: a dark grey button with a white 'X' icon and the text "Abbrechen", and a red button with a white lock icon and the text "Einloggen".

3.5 Möglicher Fehlerfall: E-Mail-Adresse falsch

Wenn die eingegebene E-Mail-Adresse nicht in EIBa registriert ist, sehen Sie die folgende Fehlernachricht. Korrigieren Sie Ihre Eingabe und versuchen Sie erneut, sich anzumelden.

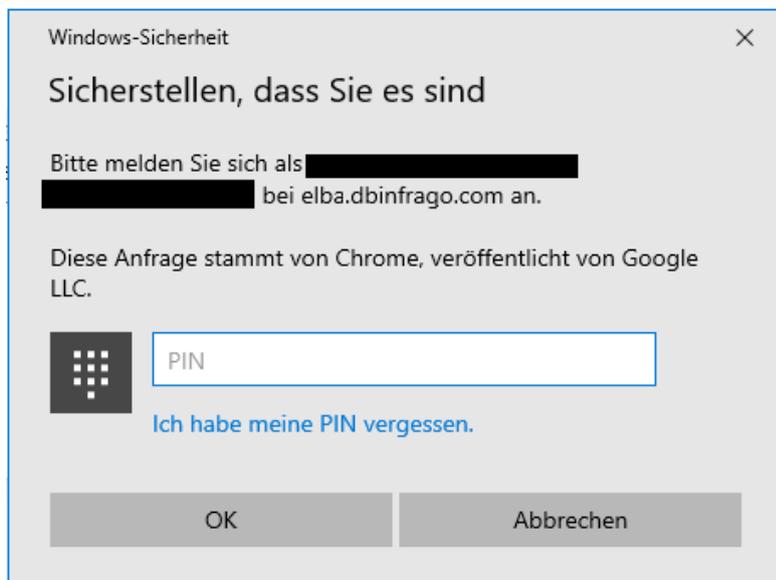
Sollte dieser Fehler trotz mehrfacher Prüfung der E-Mail-Adresse erscheinen, dann wenden Sie sich bitte an die fachliche Betriebsführung.



The screenshot shows the same login form as in 3.4, but with an error message. The "Email Adresse" input field is blacked out. Below the input field, a red horizontal line is followed by the text "Ihre Anmeldung war nicht erfolgreich" in red. The "Abbrechen" button remains dark grey, but the "Einloggen" button is now greyed out.

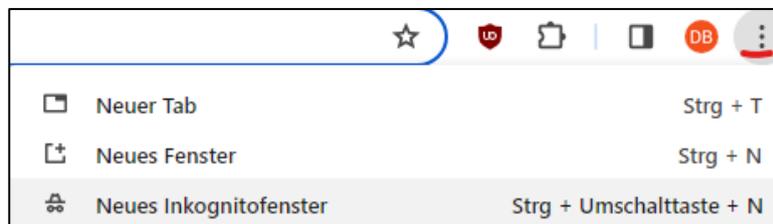
3.6 Möglicher Fehlerfall: Windows Hello PIN eingerichtet

Wenn der folgende Dialog angezeigt wird, dann versucht Ihr Computer, Sie über Windows Hello mit PIN statt über Ihren Sicherheitsschlüssel bei EIBa anzumelden.



In diesem Fall können Sie die Anmeldung über Ihren Sicherheitsschlüssel erzwingen, indem Sie die EIBa WebApp in einem Inkognito-Fenster benutzen.

Klicken Sie dazu im Browser auf die drei Punkte oben rechts und wählen Sie die Option „Neues Inkognito-Fenster“.

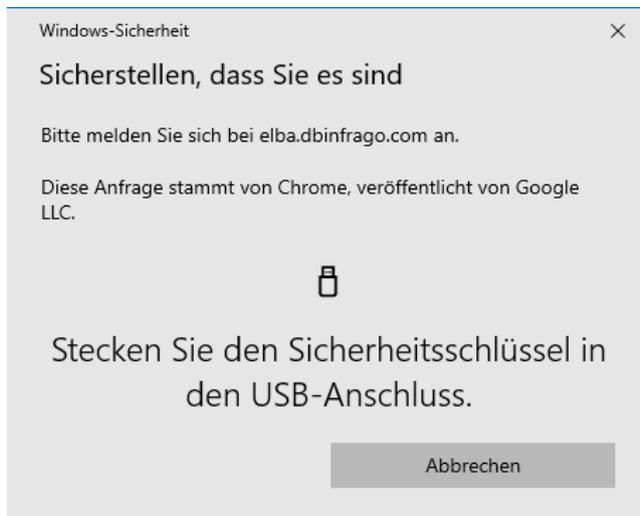


Rufen Sie in dem neuen Browser-Fenster <https://elba.dbinfrago.com> auf und versuchen Sie erneut, sich anzumelden.

Aus einem Inkognito-Fenster besteht in den meisten Fällen kein Zugriff auf Windows Hello, so dass automatisch versucht wird, Sie mit Ihrem Sicherheitsschlüssel anzumelden. Sollte die Anmeldung auch so nicht möglich sein, dann wenden Sie sich bitte an Ihren Administrator.

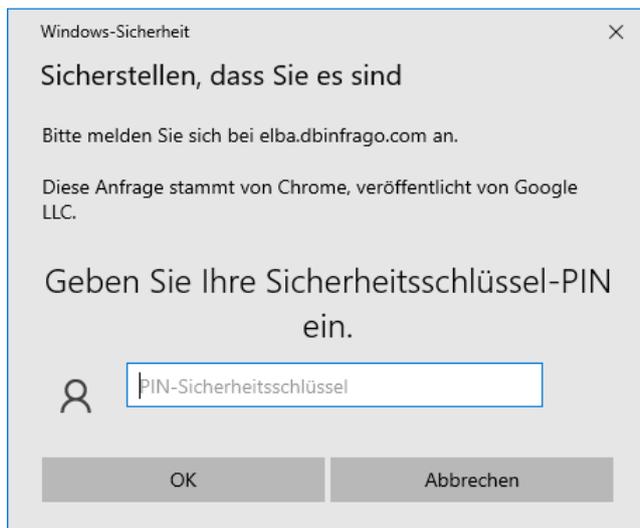
3.7 Möglicher Fehlerfall: Sicherheitsschlüssel nicht verbunden

Wenn der folgende Dialog angezeigt wird, dann ist Ihr Sicherheitsschlüssel nicht mit dem Computer verbunden oder konnte nicht erkannt werden. Verbinden Sie Ihren Sicherheitsschlüssel erneut mit dem Computer. Sobald der Sicherheitsschlüssel erkannt wird, schließt sich der Dialog.



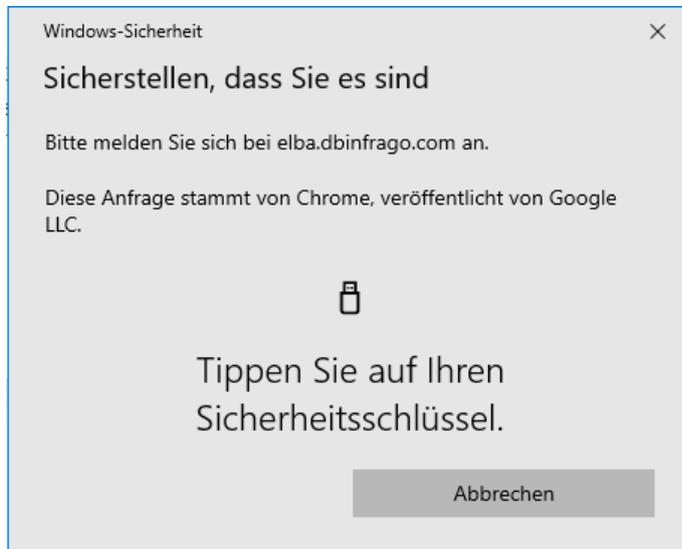
3.8 PIN-Eingabe

Wenn der folgende Dialog angezeigt wird, dann prüfen Sie anhand des Textes, dass Sie sich für elba.dbinfrago.com anmelden. Geben Sie dann die PIN Ihres Sicherheitsschlüssels an und bestätigen Sie mit einem Klick auf „OK“:



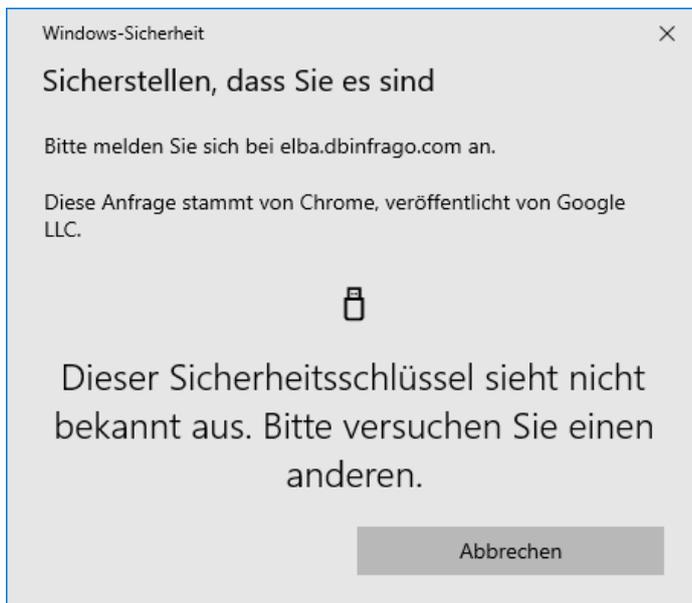
3.9 (Optional) Sicherheitsschlüssel antippen

Je nach verwendetem Sicherheitsschlüssel kann es nötig sein, den Sicherheitsschlüssel freizuschalten. Wenn Sie den folgenden Dialog sehen, dann drücken Sie (im Falle eines YubiKey) auf den mittig befindlichen runden, goldenen Kontakt um fortzufahren.



3.10 Möglicher Fehlerfall: Falscher Sicherheitsschlüssel

Wenn Sie den folgenden Dialog sehen, dann konnte der mit dem Computer verbundene Sicherheitsschlüssel nicht verwendet werden, um Sie in ElBa anzumelden. Stellen Sie sicher, dass Sie nur einen - und den richtigen - Sicherheitsschlüssel am Computer angeschlossen haben und versuchen Sie die Anmeldung erneut.



Auch wenn Sie nur einen Sicherheitsschlüssel besitzen und ihn auf Werkseinstellungen zurückgesetzt haben, kann dieser Dialog angezeigt werden. In diesem Fall muss der Sicherheitsschlüssel neu in ElBa registriert werden. Melden Sie sich bitte bei der fachlichen Betriebsführung, um eine neue Registrierungsmail zu erhalten.

3.11 Anmeldung erfolgreich

Nach dem Antippen des Sicherheitsschlüssels sollten Sie erfolgreich angemeldet werden. Ist dies nicht der Fall, dann melden Sie sich bitte bei der fachlichen Betriebsführung.