Schleswig-Holstein
Staatskanzlei

Handreichung zum Registrierungsprozess von ELSTER-Organisationszertifikaten im Rahmen von Mein Unternehmenskonto

- Modell: „zentrale Stelle“

Version 1.2

Inhalt

1 Haftungsausschluss und Hinweis zu externen Links 3
2 Mein Unternehmenskonto – Ein kurzer Überblick 4
3 Beschaffung und Verwaltung von ELSTER-Organisationszertifikaten 5
3.1 Feststellung oder Beschaffung einer Steuernummer 5
3.2 Feststellung einer vorhandenen Steuernummer 5
3.3 Beschaffung einer neuen Steuernummer 5
4 Aufbau einer zentralen Stelle für Organisationszertifikate 8
4.1 Zuständigkeit und Verankerung in der Organisation 8
4.2 Einrichten des Zertifikatsmanagements in KeePass 2 9
4.3 Erstmalige Beschaffung eines Organisationszertifikats 13
4.4 Erstmalige Einrichtung der Berechtigungssteuerung 14
5 Verwaltung von Organisationszertifikaten für Mitarbeitende 16
5.1 Grundlagen der Zertifikatsbeschaffung 16
5.2 Neuanlage von Organisationszertifikaten für Mitarbeitende 18
5.2.1 Beschaffung der Zertifikatsdatei bei ELSTER 19
5.2.2 Dokumentation in KeePass 2 21
5.2.3 Bereitstellen des Organisationszertifikats an die Mitarbeitenden 24
5.2.4 Anmelden und Konfiguration in der Berechtigungssteuerung 24
5.3 Änderung von Organisationszertifikaten 25
5.4 Sperrung von Organisationszertifikaten 26
5.5 Löschung von Organisationszertifikaten 28
5.6 Erteilen von Berechtigungen für digitale Verwaltungsleistungen 29
5.6.1 Pauschale Berechtigungen für die Organisation festlegen 29
5.6.2 Berechtigungsgruppen in der Berechtigungssteuerung anlegen 30
5.6.3 Individuelle Berechtigungen für Mitarbeitende 30
5.6.4 Berechtigungsanfragen durch Mitarbeitende 31
6 Weiterführende Informationen 31

1 Haftungsausschluss und Hinweis zu externen Links

Dieses Dokument wurde basierend auf den Inhalten der folgenden Webseiten und Quellen erstellt:

- Beschluss 2020/01 - Einheitliches Unternehmenskonto auf Basis von ELSTER | IT- Planungsrat
- https://mein-unternehmenskonto.de/mup/infoseite/nutzen_und_vorteile_mup
- https://info.mein-unternehmenskonto.de
- https://www.elster.de/eportal/helpGlobal?themaGlobal=wo_ist_meine_steuernummer

Folgende Informationen wurden sorgfältig zusammengetragen und für die Nutzenden aufbereitet. Dennoch wird keine Gewähr für die Richtigkeit, Vollständigkeit oder Aktualität der Inhalte übernommen.

Bitte beachten Sie, dass dieses Dokument den Stand vom 23.09.2025 widerspiegelt und nach diesem Datum nicht mehr aktualisiert wird. Es können sich Änderungen der beschriebenen Prozesse, Inhalte oder Informationen auf den verlinkten Webseiten ergeben, für die keine Verantwortung übernommen wird. Für die neuesten und genauesten Informationen konsultieren Sie bitte direkt die Originalquellen.

2 Mein Unternehmenskonto – Ein kurzer Überblick

Das bundesweit einheitliche Unternehmenskonto (Mein Unternehmenskonto) bietet die Möglichkeit, digitale Verwaltungsleistungen verschiedenster Behörden über einen deutschlandweit einheitlichen Zugang zu nutzen. Es stellt das bundesweit einheitliche Nutzerkonto für Unternehmen dar und ist darauf ausgelegt, dass es für alle Bereiche im Umfeld der öffentlichen Verwaltung genutzt werden kann. Mein Unternehmenskonto ist ein zentraler Authentifizierungs- und Identifizierungsdienst und bietet u.a. auch Postfächer für die Kommunikation mit verschiedensten Behörden.

Es handelt sich bei Mein Unternehmenskonto um ein Kooperationsprojekt von Bayern und Bremen, Auftraggeber ist der IT-Planungsrat. Am Projekt beteiligte Stellen sind das Finanzministerium Bremen mit der Verantwortung für die Entwicklung des OZG+-Postfachs durch Governikus und die Entwicklung der Berechtigungssteuerung durch Dataport, das Bayrische Staatsministerium für Steuern, verantwortlich für Branding, Informationsseite und Logo und das Bayrische Landesamt für Steuern mit der Verantwortung für Elster, Identitäten und Postfach 2.0.

Gesetzesgrundlage & Anbindungsverpflichtung

(2) Das Bundesministerium des Innern und für Heimat wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates zu bestimmen, **welche staatlichen Stellen ein einheitliches Organisationskonto im Portalverbund bereitstellen**.

(3) Für öffentliche Stellen, die Verwaltungsleistungen im Portalverbund anbieten, ist die **Verwendung des Organisationskontos verpflichtend**.

§ 3 Abs. 2 – 3 OZG

Diese Dokumentation beschreibt den Registrierungsprozess zur Erstellung von ELSTER Organisationszertifikaten im Rahmen von „Mein Unternehmenskonto“.

3 Beschaffung und Verwaltung von ELSTER-Organisationszertifikaten

Die Bereitstellung und Nutzung von Organisationszertifikaten für die Landes- und Kommunalbehörden sowie Landes- und Kommunalbetriebe erfolgt in drei wesentlichen Schritten. Zunächst muss als Voraussetzung eine Steuernummer vorliegen, welche u. U. zunächst beschafft werden muss. Im nächsten Schritt muss eine zentrale Stelle innerhalb der Landes- bzw. Kommunalbehörden oder Landes- bzw. Kommunalbetriebe benannt bzw. aufgebaut werden, welche die Zertifikate für die jeweilige Organisation administriert (Zertifikatsverwaltung). Die zentrale Stelle beschafft die Organisationszertifikate und stellt diese an entsprechende Mitarbeiterinnen und Mitarbeiter zur Nutzung bereit. Auch verwaltet die zentrale Stelle bei Bedarf die Berechtigungen für den Zugang zu Verwaltungsleistungen, kann Zertifikate sperren und löschen sowie Berechtigungen entziehen.

1. Feststellung oder Beschaffung einer Steuernummer
2. Aufbau einer zentralen Stelle für die Organisationszertifikate
3. Verwaltung von Organisationszertifikaten für Mitarbeitende

3.1 Feststellung oder Beschaffung einer Steuernummer

Um Organisationszertifikate für die Verwendung von „Mein Unternehmenskonto“ (MUK) beschaffen zu können, ist das Vorhandensein einer deutschen Steuernummer unabhängig auf welcher Grundlage (z. B. Lohnsteuer, Umsatzsteuer, Grundsteuer) Voraussetzung. Jede Landes- oder Kommunalbehörde sowie jeder Landes- oder Kommunalbetrieb muss über eine eigene Steuernummer verfügen.

3.2 Feststellung einer vorhandenen Steuernummer

Verfügt die Landes- oder Kommunalbehörde bzw. Landes- oder Kommunalbetrieb bereits über eine eigene Steuernummer, so wird grundsätzlich empfohlen, diese Steuernummer auch für MUK zu verwenden, um eine redundante Pflege von Stammdaten zu vermeiden.

3.3 Beschaffung einer neuen Steuernummer

Für den Fall, dass keine geeignete Steuernummer vorliegt, kann beim Finanzamt Neubrandenburg ein Ordnungskriterium für ElsterOnline beantragt werden. Das Finanzamt Neubrandenburg ist bundesweit die einzige Stelle für die Neuanlage solcher Ordnungskriterien. Hierbei handelt es sich um Steuernummern, welche nur eingeschränkt verwendbar sind. In diesem Kontext ist diese Steuernummer für MUK nutzbar; eine Steuererklärung kann mit dieser Steuernummer nicht eingereicht werden.

Das Antragsdokument ist hier downloadbar und in der folgenden Abbildung beispielhaft ausgefüllt.

ELSTER

Finanzamt Neubrandenburg – RAB
Registrierung in Sonderfällen

Finanzamt Neubrandenburg – RAB
Postfach 11 01 40
17041 Neubrandenburg
Germany

Bitte ergänzen Sie die fehlenden Angaben und senden Sie das ausgefüllte Formular unterschrieben an das Finanzamt Neubrandenburg – RAB zurück.

Weitere Informationen finden Sie im Bereich Hilfe von Mein ELSTER (www.elster.de) unter Häufige Fragen zu Mein ELSTER - FAQ („Registrierung in Sonderfällen").

Antrag auf Erteilung eines Ordnungskriteriums (Steuernummer) zum Zwecke der Registrierung bei Mein ELSTER

Hiermit beantrage ich die Vergabe eines Ordnungskriteriums (Steuernummer) zur Registrierung im Onlineportal Mein ELSTER.

Firma bzw. Name, unter der die Person / Gesellschaft / Gemeinschaft / Behörde auftritt:
Musterbehörde SH
Anschrift der Person / Gesellschaft / Gemeinschaft / Behörde:
Musterstraße 123 12345 Musterstadt
Staat:
Deutschland

Telefon:		
Vorwahl international:	**Vorwahl national:**	**Rufnummer:**
+49	0431	1234569
E-Mail:		
muk@musterbehoerde-sh.de		

Grund der Beantragung eines Ordnungskriteriums (falls nicht ausreichen auf gesondertem Blatt):
Es wird eine Steuernummer zur Anmeldung der Behörde beim einheitlichen Organisationskonto (Mein Unternehmenskonto) benötigt.

Mit der Unterschrift wird bestätigt, dass für den Antragsteller/die Antragstellerin, für den/die dieser Antrag gestellt wird, kein anderes gültiges Ordnungskriterium (inländische Steuernummer) vorhanden ist.

Musterstadt, 01.08.2025

Ort, Datum

Unterschrift(en) vertretungsberechtigte(r) Geschäftsführer(in) oder Gesellschafter(in) / Beteiligte(r) / Bevollmächtigte(r)

Finanzamt Neubrandenburg – RAB
Neustrelitzer Str. 120
17033 Neubrandenburg (Germany)

E-Mail: rab@finanzamt-neubrandenburg.de

Telefon: +49 385 588 47000
Telefax: +49 385 588 47100
Webseite: www.finanzamt-neubrandenburg.de

Es wird empfohlen, bei der Angabe der E-Mail-Adresse ein Funktionspostfach zu hinterlegen, welche für MUK-Angelegenheiten verwendet werden kann.

Soweit dem Antrag stattgegeben wurde, wird seitens des Finanzamtes Neubrandenburg eine zehnstellige Steuernummer auf postalischem Wege versendet. Diese Steuernummer wird im weiteren Verlauf benötigt.

Sollte eine Änderung der Steuernummer erforderlich sein oder sich der Name der Landes- oder Kommunalbehörde bzw. des Landes- oder Kommunalbetriebes ändern, so kann dies nicht im Rahmen der Verwaltung der Organisationszertifikate über ELSTER erfolgen, sondern muss über das Finanzamt Neubrandenburg geklärt werden.

Hinweis: eine „echte“ Steuernummer ist mit der kommenden Wirtschafts-Identifikationsnummer kompatibel, das Ordnungskriterium wird dies nicht sein. Die Steuernummern (Ordnungskriterium), die das FA Neubrandenburg herausgibt, werden bei ELSTER in einem „besonderen“ Datentopf verwaltet, da sie nicht über die GINSTEER Infrastruktur der Länder zu ELSTER kommen.

Bei nachgeordneten Behörden kann bei getrennter MUK-Verwaltung das Ordnungskriterium als ausreichend betrachtet werden.

4 Aufbau einer zentralen Stelle für Organisationszertifikate

4.1 Zuständigkeit und Verankerung in der Organisation

Für die interne Zertifikatsverwaltung und dessen Dokumentation muss innerhalb der Landes- bzw. Kommunalbehörde oder des Landes- bzw. Kommunalbetriebes eine **zentrale Stelle** geschaffen werden. Die konkrete, organisatorische Verortung dieser zentralen Stelle obliegt der jeweiligen Behörde bzw. des jeweiligen Betriebes. Jedoch wird empfohlen, die zentrale Stelle organisatorisch im Bereich zentraler Dienste entweder im Bereich der IT oder des Haushaltswesens zu verankern. Es ist zu beachten, dass diese zentrale Stelle die Rolle des Administrators übernimmt und die Verantwortung dafür trägt, wer in der jeweiligen Landes- bzw. Kommunalbehörde oder in dem jeweiligen Landes- bzw. Kommunalbetrieb Zugang zu den Organisationszertifikaten erhält und durch diese bei organisationsbezogenen, digitalen Verwaltungsleistungen im Namen der Behörde bzw. des Betriebes handeln darf.

Die wesentlichen Aufgaben der zentralen Stelle sind:

- Anlegen, Ändern, Sperren und Löschen von Nutzerkonten,
- Zuweisen, Ändern und Entziehen von Berechtigungen zu einzelnen Nutzerkonten,
- Dokumentation von Nutzerkonten und Berechtigungen.

Es wird empfohlen, bei der Benennung der Stelle eine Vertreterrolle einzurichten und für die Kommunikation o. g. Funktionspostfach zu verwenden.

Es muss sichergestellt werden, dass nur die zentrale Stelle die Briefe, die im Rahmen der Registrierung von Organisationszertifikaten eingehen, erhält. Diese sind für den Registrierungsprozess für jedes Organisationszertifikat unbedingt erforderlich. Das genaue Vorgehen wird in Kapitel 5 erläutert. Hierdurch wird verhindert, dass Mitarbeiterinnen oder Mitarbeiter bei Kenntnis der Steuernummer selbstständig Organisationszertifikate ohne Zustimmung der zentralen Stelle beschaffen.

Die zentrale Stelle muss jederzeit Zugriff auf alle Organisationszertifikate sowie die verknüpften Postfächer haben. Daher sollten die Zertifikatsdatei, Informationen zum jeweiligen Nutzer und dem Zugang als Back-Up gesichert werden. Hierzu gehören folgende Informationen:

a) Name der Mitarbeiterin / des Mitarbeiters,

b) Benutzername,

c) Passwort,

d) Kopie der ELSTER-Zertifikatsdatei,

e) Benutzerkonto-ID (eine jedem Benutzerkonto zugewiesene Ziffer),

f) hinterlegte E-Mail-Adresse (eine E-Mail-Adresse kann für die Beantragung mehrerer Organisationszertifikate verwendet werden),

g) Sicherheitsabfrage mit Antwort (einheitlich für alle Zertifikate),

h) Zertifikatsgültigkeit.

4.2 Einrichten des Zertifikatsmanagements in KeePass 2

Es wird vorgeschlagen, das Zertifikatsmanagement mittels der Software KeePass 2 umzusetzen, da hiermit die Sicherheit der Zertifikatsverwaltung gewährleistet werden kann.

Andere zugriffsbeschränkte Möglichkeiten der Zertifikatsverwaltung sind nicht Teil dieser Handreichung, könnten aber analog zum hier vorgestellten Vorgehen aufgesetzt werden.

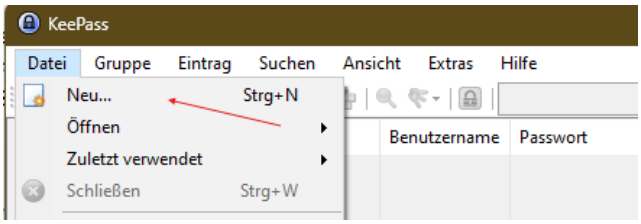
Für die allgemeine Nutzung von KeePass 2 wird hier eine Anleitung bereitgestellt. Im Folgenden wird die Einrichtung von KeePass 2 für die gemeinsame Nutzung durch mehrere Personen innerhalb einer zentralen Stelle für die Zertifikatsverwaltung beschrieben.

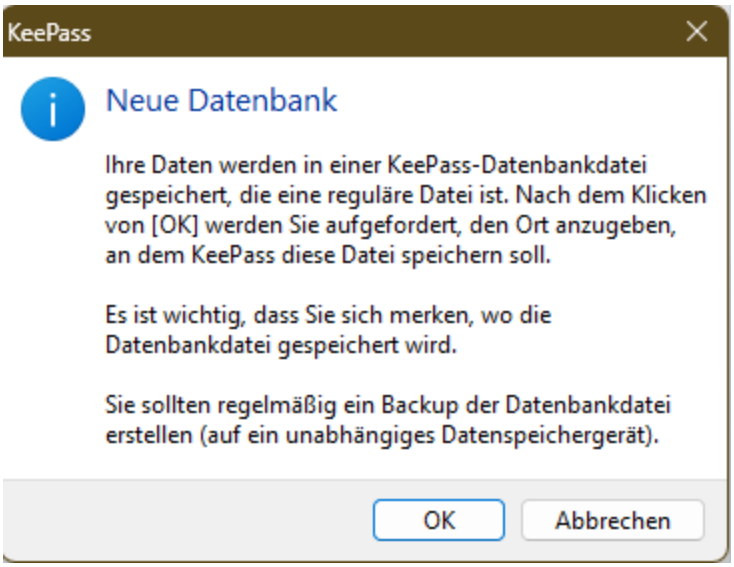
Dies weicht von der Nutzung von KeePass 2 für eigene Passwörter ab!

Als **technische Sicherheitsmaßnahme** wird die Einrichtung einer **Zwei-Faktor-Authentifizierung** (einfacher per Datenstick oder aufwendiger per Google-Authenticator o.ä.) empfohlen. **Das Einrichten einer 2-FA ist nicht Teil dieser Handreichung.**

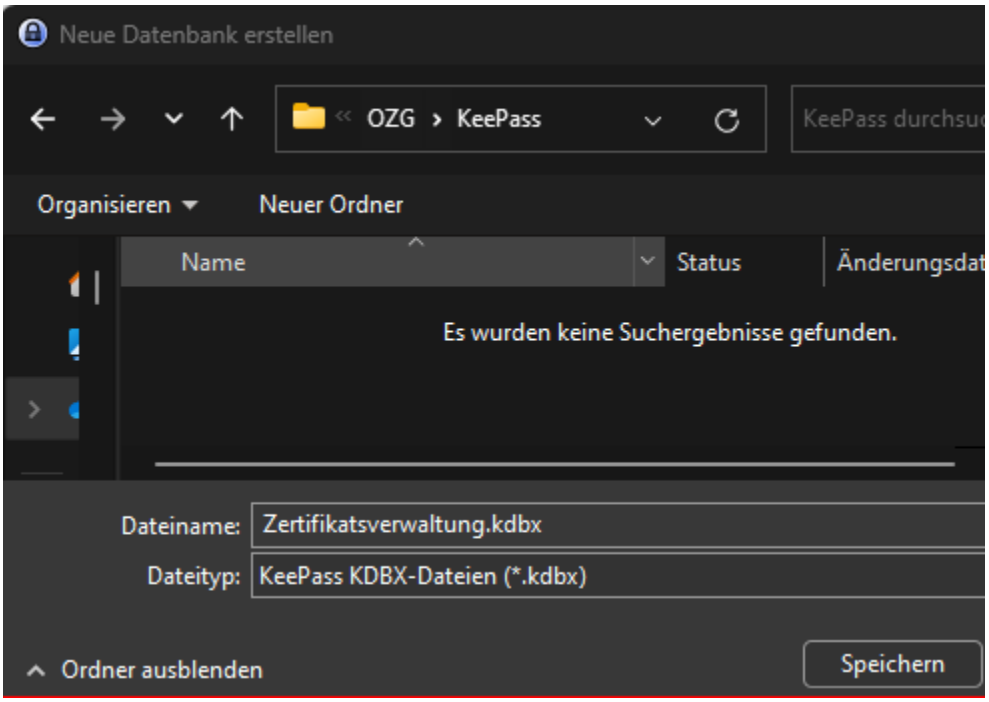
Nach dem erstmaligen Start von KeePass 2 erhalten Sie die Aufforderung zum Anlegen einer neuen Datenbank. Eine neue Datenbank kann auch mit «Datei»-«Neu…» angelegt werden.

Nach dem Start von KeePass 2 muss zunächst eine neue Datenbank angelegt werden.



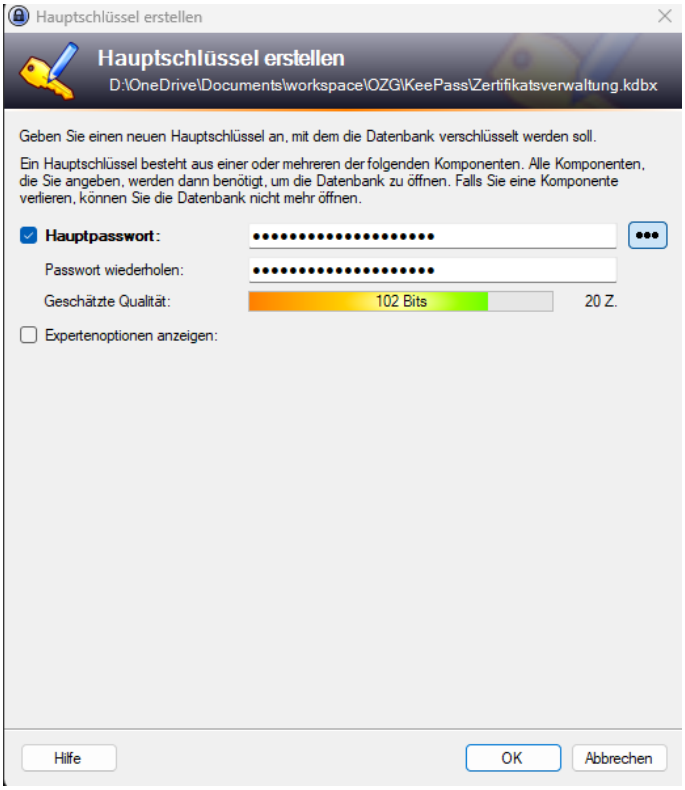


Mit «OK» wird die Neuanlage einer Datenbank bestätigt.

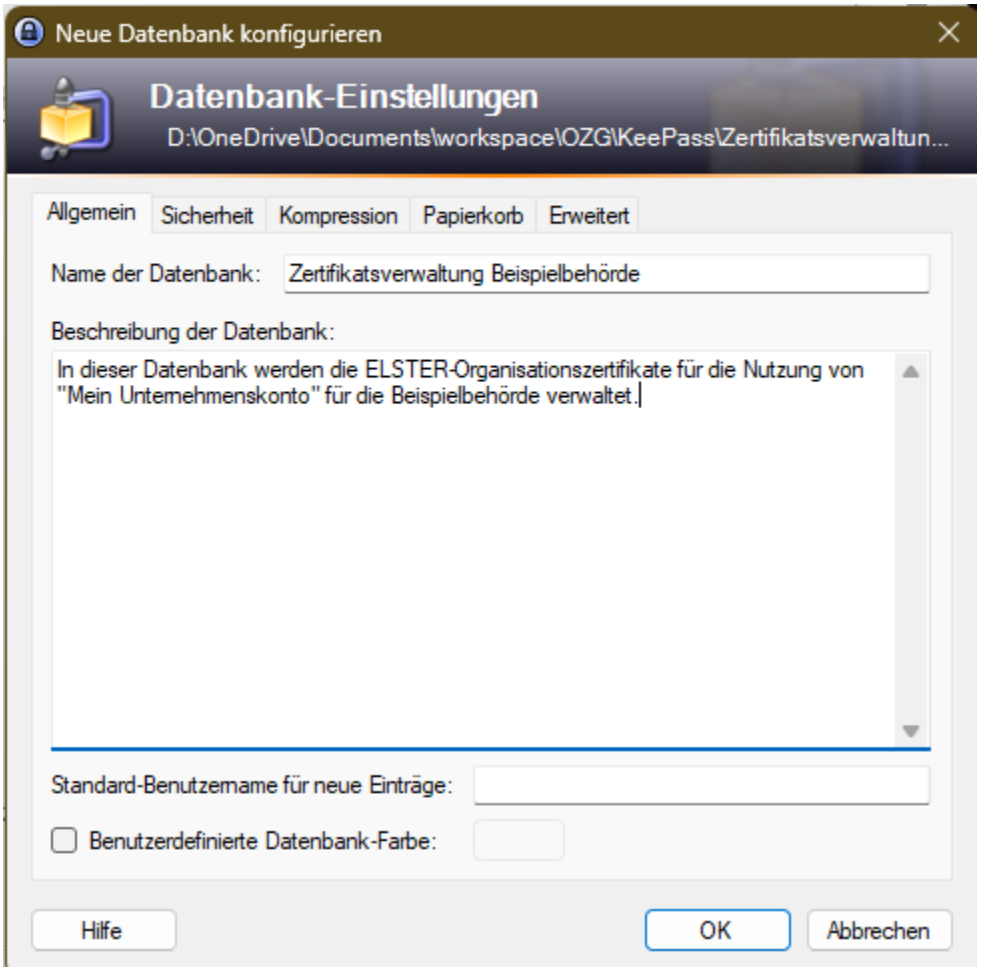


Es wird empfohlen, einen treffenden Dateinamen zu wählen. Wichtig ist die Speicherung an einem sicheren Ort, auf welchen nur ein zugangsbeschränkter Personenkreis Zugang hat.

Im nächsten Schritt wird der Hauptschlüssel definiert, welcher aus mindestens 16 Zeichen bestehen sollte.



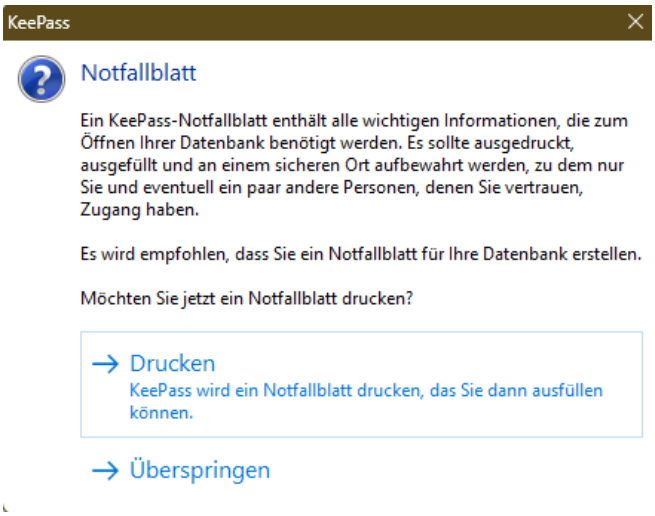
DIESER HAUPTSCHLÜSSEL MUSS SICHER DOKUMENTIERT WERDEN, DA NUR DURCH DIESEN HAUPTSCHLÜSSEL DER ZUGANG ZUR DATENBANKDATEI SICHERGESTELLT WIRD. ES GIBT KEINE MÖGLICHKEIT, DIESEN HAUPTSCHLÜSSEL AUßERHALB DER DATENBANK ZURÜCKZUSETZEN.



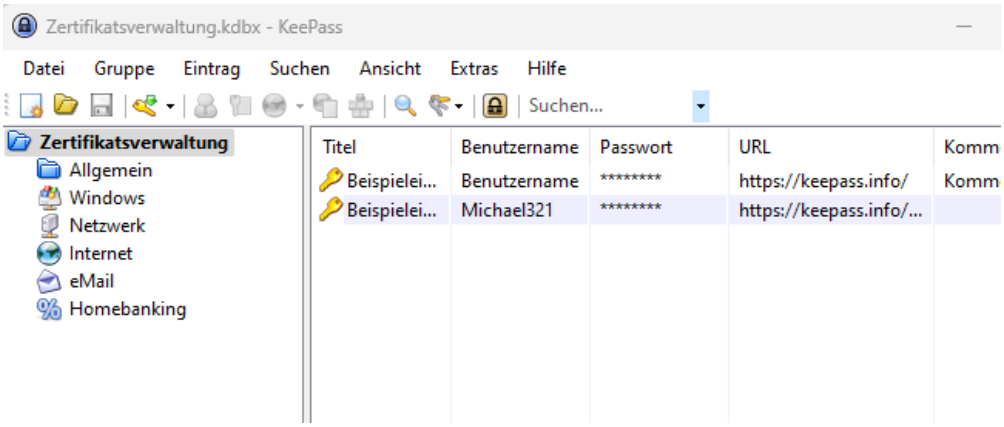
In der Registerkarte Allgemein sollte der Name der Datenbank sowie eine kurze Beschreibung festgelegt werden. Die Einstellungen in den anderen Registerkarten können unverändert übernommen werden.

Im folgenden Schritt kann ein Notfallblatt generiert werden.

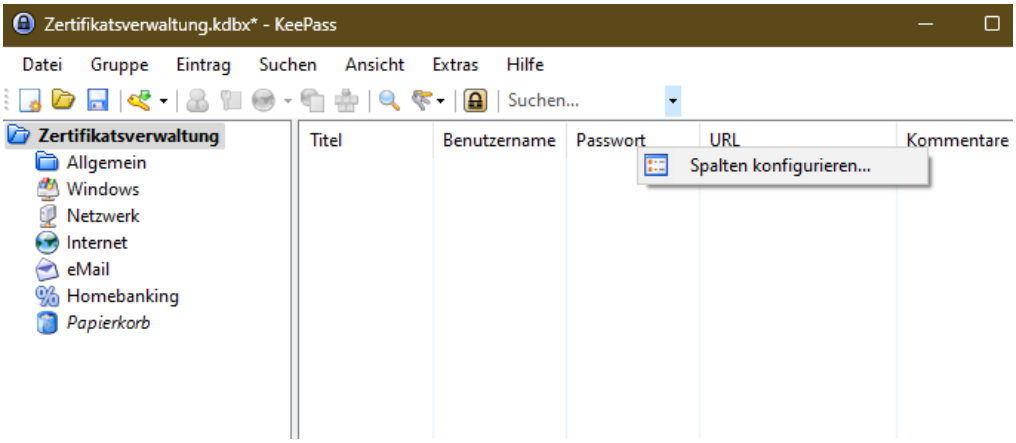
ACHTUNG! DER HAUPTSCHLÜSSEL WIRD NICHT AUTOMATISCH IN DAS DOKUMENT ÜBERNOMMEN UND MUSS HÄNDISCH NACHGETRAGEN WERDEN.



Im nächsten Schritt gelangt man zur Hauptansicht. Ggf. werden bereits Beispieleinträge angezeigt, welche gelöscht werden können.

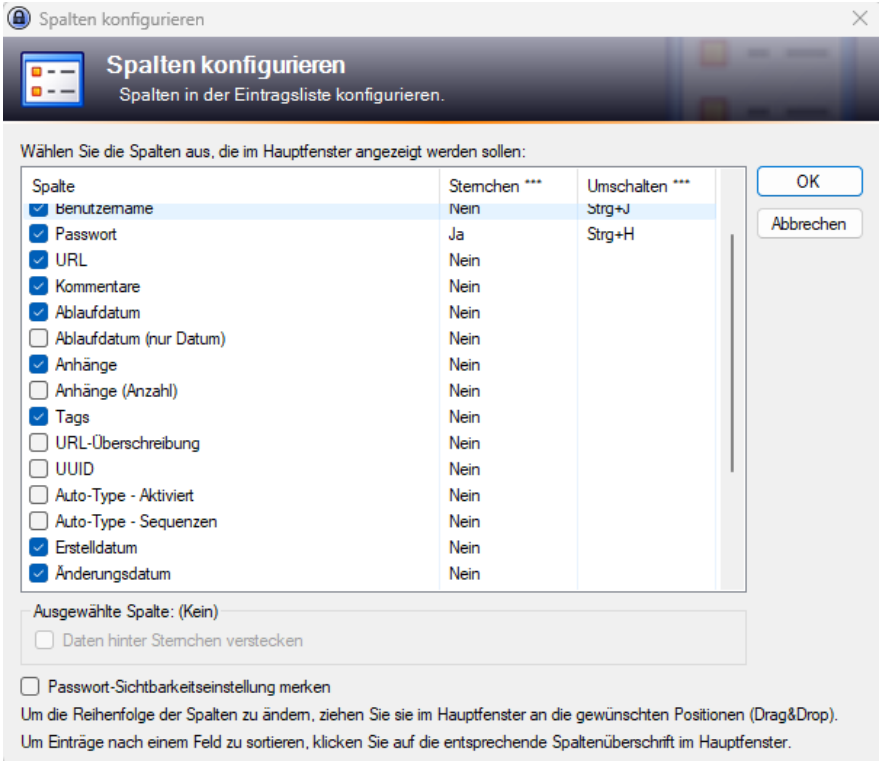


Mittels eines Rechtsklicks auf die Spaltenüberschriften können die Spalten konfiguriert sowie weitere Spalten hinzugefügt werden, welche für die Zertifikatsverwaltung hilfreich sein werden.



Folgende Spalten sollten aktiviert werden:

- Titel,
- Benutzername,
- Passwort,
- URL,
- Kommentare,
- Ablaufdatum,
- Anhänge,
- Tags,
- Erstelldatum,
- Änderungsdatum



Mit Abschluss dieser Spaltenkonfiguration ist die Zertifikatsverwaltung in KeePass 2 eingerichtet und kann zur Verwaltung der Organisationszertifikate genutzt werden.

4.3 Erstmalige Beschaffung eines Organisationszertifikats

Die zentrale Stelle muss sich als erste Stelle ein Organisationszertifikat beschaffen, um ihrer künftigen, administrativen Rolle gerecht werden zu können.

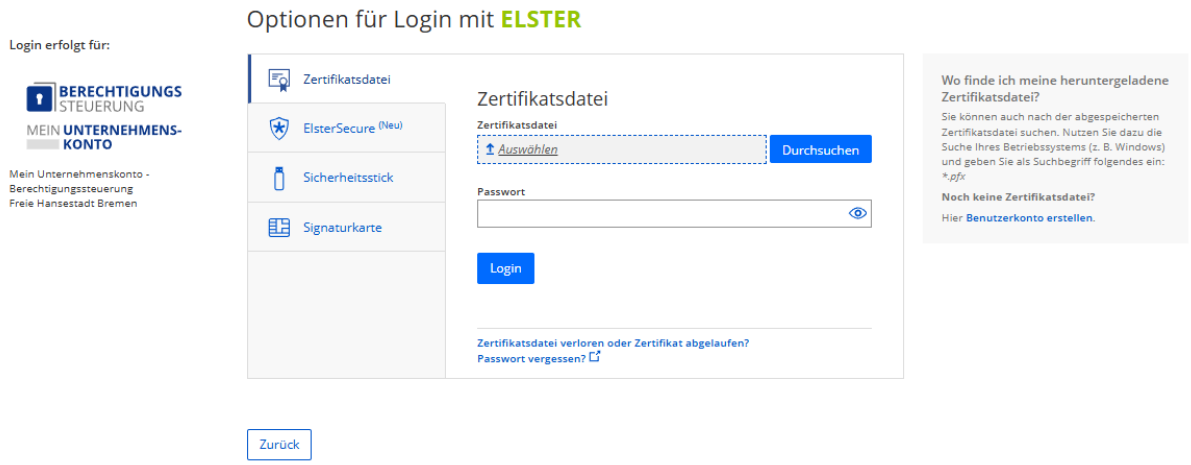
Der Prozess der Beschaffung folgt dem Prozess, welcher in Kapitel 5.2.1 beschrieben ist. Zusätzlich ist jedoch die Berechtigungssteuerung einzurichten, welche im nachfolgenden Kapitel beschrieben ist.

Führen Sie zunächst die Schritte des im Kapitel 5.2.1 beschriebenen Prozesses durch und fahren anschließend mit dem nachfolgenden Kapitel 4.4 fort.

4.4 Erstmalige Einrichtung der Berechtigungssteuerung

Bei „Mein Unternehmenskonto“ gibt es die Möglichkeit, Rollen und Rechtestrukturen der Unternehmens- bzw. Behördenmitarbeitenden sowie Berechtigungen mittels der Berechtigungssteuerung für einzelne Onlinedienste einzustellen und zu steuern.

Hat sich die zentrale Stelle erstmalig das Organisationszertifikat beschafft, so muss sich diese erstmalig in der Berechtigungssteuerung auf der Website der Berechtigungssteuerung registrieren, um dort die Rolle des Administrators einzunehmen und damit Rechte und Rollen für die Mitarbeiterinnen und Mitarbeiter der Landes- bzw. Kommunalbehörde oder Landes des Landes- bzw. Kommunalbetriebes verwalten zu können.



Die Anmeldung an der Berechtigungssteuerung erfolgt mit dem aus Kapitel 5.2.1 beschafften Organisationszertifikat und dem dazugehörigen Passwort.

Die Datenweitergabe ist zu bestätigen. Dieser Dialog muss grundsätzlich bei jeder Anmeldung mit MUK bei allen angeschlossenen Portalen bestätigt werden.

Sie befinden sich nun auf der zentralen Oberfläche der Berechtigungssteuerung, welche Ihnen zunächst im linken Menü «*Mein Bereich*» und «*Onlinedienste verwalten*». Klicken Sie nun unter «*MEIN BEREICH*» auf «*Mein Benutzerkonto*».

Im Menü «*Konto-Details*» unter «*Funktion*» ist gegenwärtig dem Organisationszertifikat keine Funktion zugewiesen. Klicken Sie auf «*Administration werden*».

Im Folgedialog tragen Sie Vorname, Nachname sowie die persönliche E-Mail-Adresse ein und klicken anschließend auf «*Jetzt Administrator*in werden*».

Nun wird eine E-Mail mit einem Aktivierungslink zur Bestätigung versendet.

ACHTUNG: DIE LEITUNG DER ORGANISATION WIRD HIERVON POSTALISCH IN KENNTNIS GESETZT UND KANN DIE ADMINISTRATIONSRECHTE FÜR DIE BERECHTIGUNGSSTEUERUNG MITTELS EINEM ÜBERSANDTEN WIDERRUFSCODE ENTZIEHEN.

Für den Fall, dass ein Mitarbeitender sich für die Organisation in der Berechtigungssteuerung angemeldet hat und sich selbst unberechtigterweise Admin-Rechte verliehen hat, bevor die zentrale sich erstmalig angemeldet hat, können im Menü «*Einstellungen (Zahnrad-Symbol)*» unter dem Menüpunkt «*Widerruf von Admin-Rechten anfordern*» alle mit der Organisation verbundenen Admin-Rechte zurückgesetzt werden. Hierzu ist o. g. Widerrufscode im zweiten Menüpunkt «*Widerrufscode eingeben und Admin-Rechte entziehen*» einzugeben. Damit können alle Admin-Rechte einer Organisation zurückgesetzt und neu vergeben werden.

Nun ist die Berechtigungssteuerung um den Bereich *Adminfunktionen* erweitert. Sofern es für die Behörde relevant ist, den Zugang für Mitarbeitende zu einzelnen Verwaltungsleistungen zu reglementieren, können pauschal Kontoberechtigungen eingeschaltet werden. Anderenfalls kann jeder Zertifikatsinhaber unbeschränkt MUK-fähige Verwaltungsleistungen im Namen der Landes- bzw. Kommunalbehörde oder des Landes- bzw. Kommunalbetriebes in Anspruch nehmen. Es wird daher empfohlen, die Kontoberechtigung zu aktivieren. Näheres zur Verwaltung der Berechtigungen werden in Kapitel 5.6 erläutert. Hierfür ist oben auf «*Kontoberechtigung*» (grüner Pfeil) zu klicken und im Menü «*Kontoberechtigungen einschalten*» den Dialogen zu folgen, bis die Kontoberechtigung eingeschaltet ist, was an der Blaufärbung des Icons erkennbar wird.

Damit ist die initiale Einrichtung der Berechtigungssteuerung abgeschlossen. Die notwendigen Schritte zur Nutzung im Rahmen des Zertifikatsmanagements werden in Kapitel 4 erläutert. Weiterführende Informationen zur Nutzung der Berechtigungssteuerung werden in Kapitel 5 bereitgestellt.

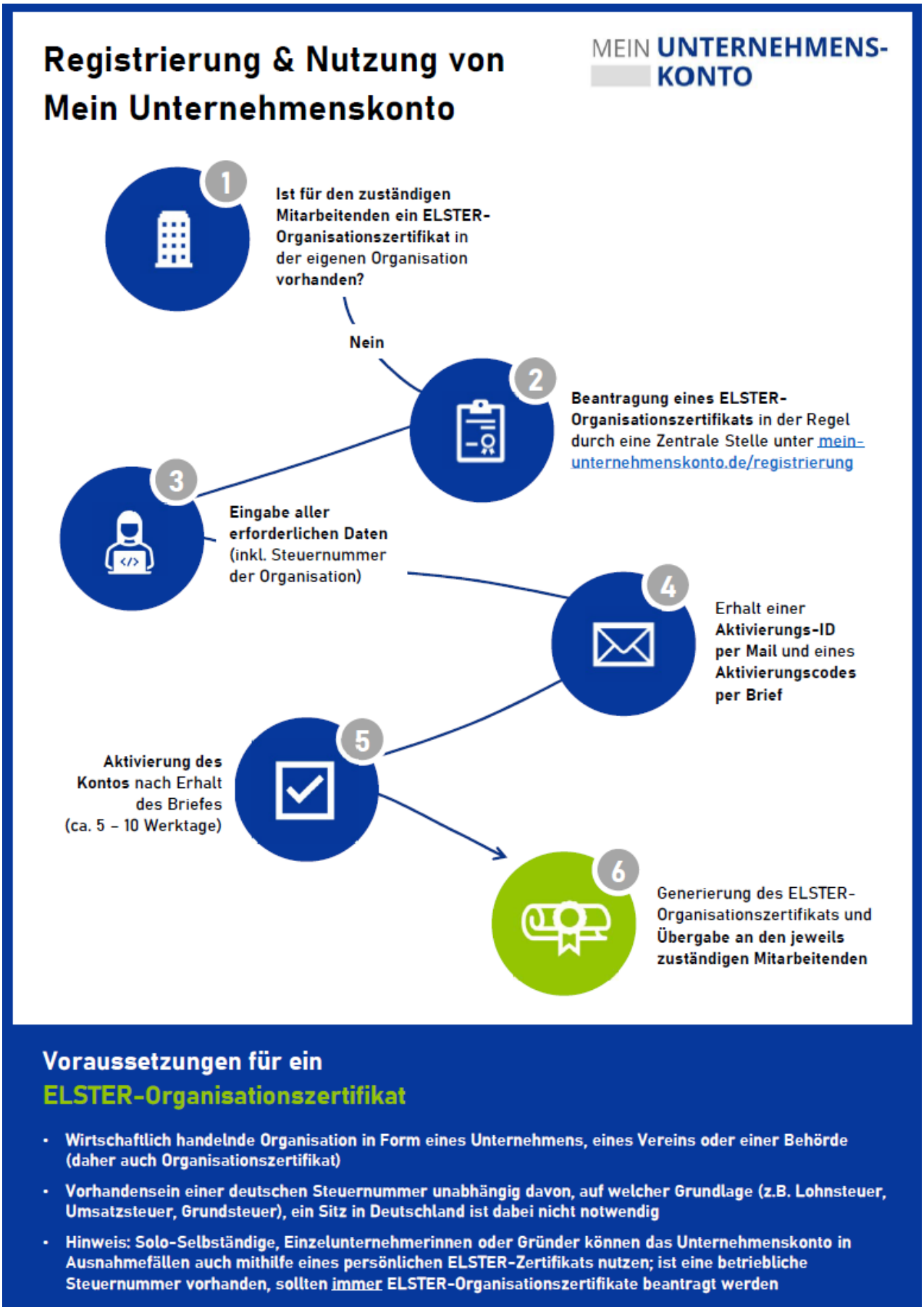
5 Verwaltung von Organisationszertifikaten für Mitarbeitende

5.1 Grundlagen der Zertifikatsbeschaffung

Mitarbeitende, die für Ihre Arbeit Organisationszertifikate benötigen, können sich nun an die zentrale Stelle für die Beschaffung wenden. Dabei sollen für das Land und die Kommunen Organisationszertifikate für jeden Mitarbeitenden einzeln beschafft werden, da einige Online-Dienste eine personengebundene Authentifizierung erfordern und hierdurch Nachvollziehbarkeit im Verwaltungshandeln sichergestellt ist.

Jedem Zertifikat ist ein Postfach zugeordnet, mit dem eine Kommunikation zwischen dienst-anbietender und dienstnutzender Stelle mit Rückkanal möglich ist.

Es können pro Organisation unter einer Steuernummer gegenwärtig maximal 5.000 Organisationszertifikate beschafft werden.


Registrierung & Nutzung von Mein Unternehmenskonto
MEIN UNTERNEHMENS-KONTO
1
Ist für den zuständigen Mitarbeitenden ein ELSTER-Organisationszertifikat in der eigenen Organisation vorhanden?
Nein
2
Beantragung eines ELSTER-Organisationszertifikats in der Regel durch eine Zentrale Stelle unter mein-unternehmenskonto.de/registrierung
3
Eingabe aller erforderlichen Daten (inkl. Steuernummer der Organisation)
4
Erhalt einer Aktivierungs-ID per Mail und eines Aktivierungscodes per Brief
5
Aktivierung des Kontos nach Erhalt des Briefes (ca. 5 – 10 Werktage)
6
Generierung des ELSTER-Organisationszertifikats und Übergabe an den jeweils zuständigen Mitarbeitenden
Voraussetzungen für ein ELSTER-Organisationszertifikat
• Wirtschaftlich handelnde Organisation in Form eines Unternehmens, eines Vereins oder einer Behörde (daher auch Organisationszertifikat)
• Vorhandensein einer deutschen Steuernummer unabhängig davon, auf welcher Grundlage (z.B. Lohnsteuer, Umsatzsteuer, Grundsteuer), ein Sitz in Deutschland ist dabei nicht notwendig
• Hinweis: Solo-Selbständige, Einzelunternehmerinnen oder Gründer können das Unternehmenskonto in Ausnahmefällen auch mithilfe eines persönlichen ELSTER-Zertifikats nutzen; ist eine betriebliche Steuernummer vorhanden, sollten immer ELSTER-Organisationszertifikate beantragt werden

Es wird darauf hingewiesen, dass durch die Herausgabe des Organisationszertifikates an die Mitarbeitenden der Organisation diese im Namen der Landes- bzw. Kommunalbehörde oder des Landes- bzw. Kommunalbetriebes digitale Verwaltungsangebote nutzen können. Hierzu muss bei den betroffenen Personen ausreichend Bewusstsein geschaffen werden.

Es wird empfohlen, den Guidelines für die Nutzung der Organisationszertifikate aus dem Leitfaden zur Verwendung & Verwaltung von ELSTER-Organisationszertifikaten im Rahmen von Mein Unternehmenskonto zu folgen:

Kommunikation der Reichweite der Berechtigung:

Erhalten Mitarbeitende ein Organisationszertifikat, berechtigt sie dies im Außenverhältnis zur Beantragung von Verwaltungsleistungen. Die Landes- bzw. Kommunalbehörde oder der Landes- bzw. Kommunalbetrieb sollte daher klar definieren, welche digitalen Verwaltungsangebote die Mitarbeitenden mit dem Organisationszertifikat in Anspruch nehmen sollen bzw. dürfen.

Weitergabe der Zugangsberechtigung an Dritte:

Die konkludente Innenvollmacht, die in der Übergabe eines Organisationszertifikats an die jeweiligen Mitarbeitenden zu sehen ist, gilt grundsätzlich nur gegenüber der ausgewählten Person – dies sollte explizit kommuniziert werden. Sollte eine Weitergabe des Organisationszertifikats und der Zugangsdaten notwendig sein, sollte dies ausschließlich nach Rücksprache mit der zentralen Stelle erfolgen.

Mitwirkung bei Ausscheiden aus der Landes- bzw. Kommunalbehörde oder dem Landes- bzw. Kommunalbetrieb:

Wenn Mitarbeitende der Landes- bzw. Kommunalbehörde oder den Landes- bzw. Kommunalbetrieb verlassen, sollte sichergestellt werden, dass die Mitarbeitenden die eigene Kopie des Organisationszertifikats löschen und eine Kopie bei einer zentralen Stelle vorhanden ist. Außerdem sollte über die zentrale Stelle ein Passwortwechsel für das Zertifikat durchgeführt werden. Damit werden alle alten, bisher existierenden Kopien des Zertifikats ungültig und können nicht mehr verwendet werden.

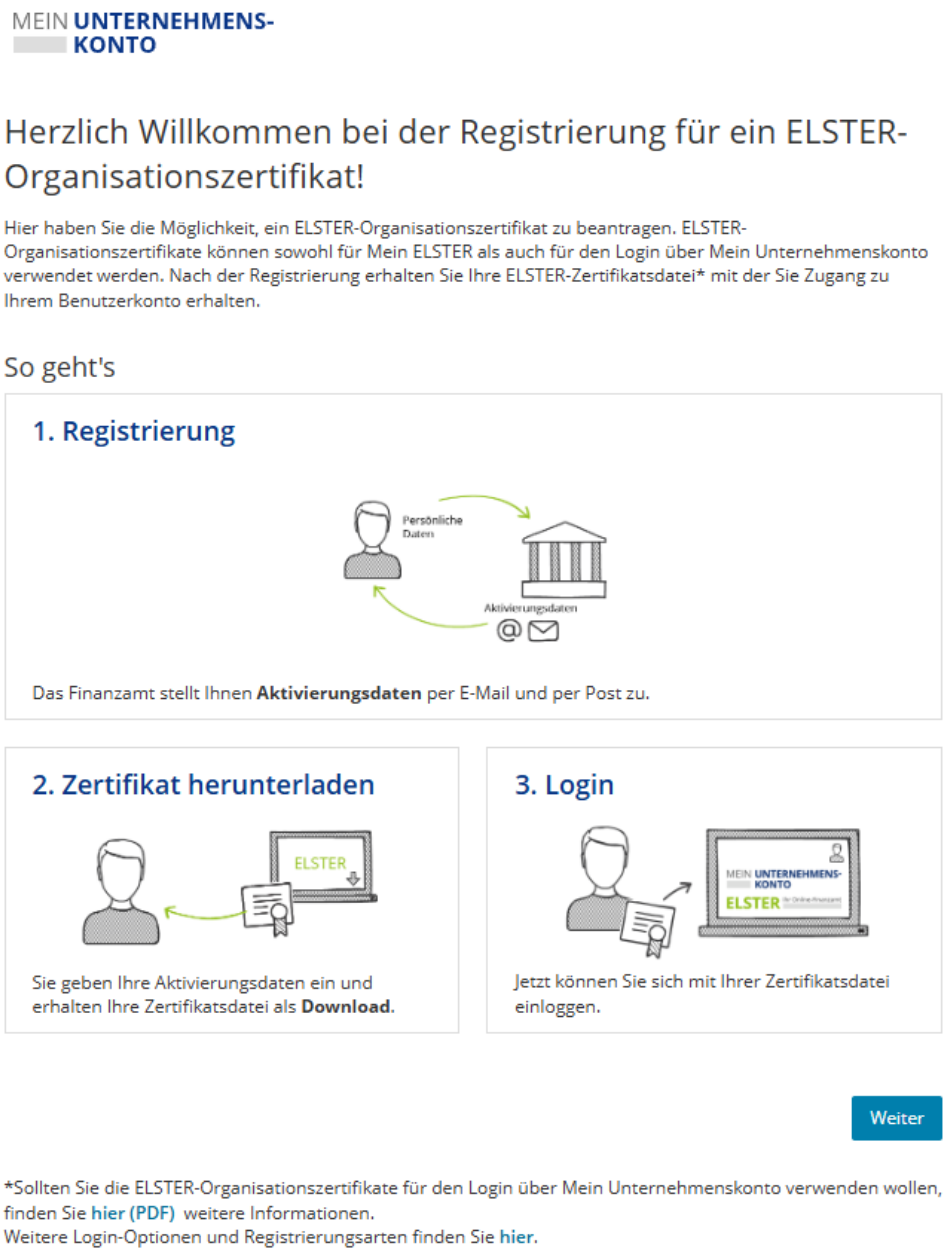
Die folgenden Schritte bauen auf den genannten Guidelines auf.

5.2 Neuanlage von Organisationszertifikaten für Mitarbeitende

Der Beschaffungsprozess sollte für den betroffenen Mitarbeitenden vollständig durch die zentrale Stelle durchgeführt werden und **nicht** durch den betroffenen Mitarbeitenden selbst. Dies ist notwendig, um eine saubere Administration zu gewährleisten. Anderenfalls besteht die Gefahr, dass die zentrale Stelle keinen Zugriff mehr auf Organisationszertifikate hat und für die folgenden Prozesse stets die betroffenen Mitarbeiter einbezogen werden müssen.

5.2.1 Beschaffung der Zertifikatsdatei bei ELSTER

Ein neues Organisationszertifikat wird bei ELSTER unter https://www.elster.de/eportal/unternehmerorientiert/registrierungsprozess mit Eingabe aller erforderlichen Daten angelegt. Nach Aufruf des Links erscheint folgender Dialog.



Nach der Bestätigung mit «*Weiter*»“, müssen im Folgenden die Stammdaten für das Zertifikat eingetragen werden.

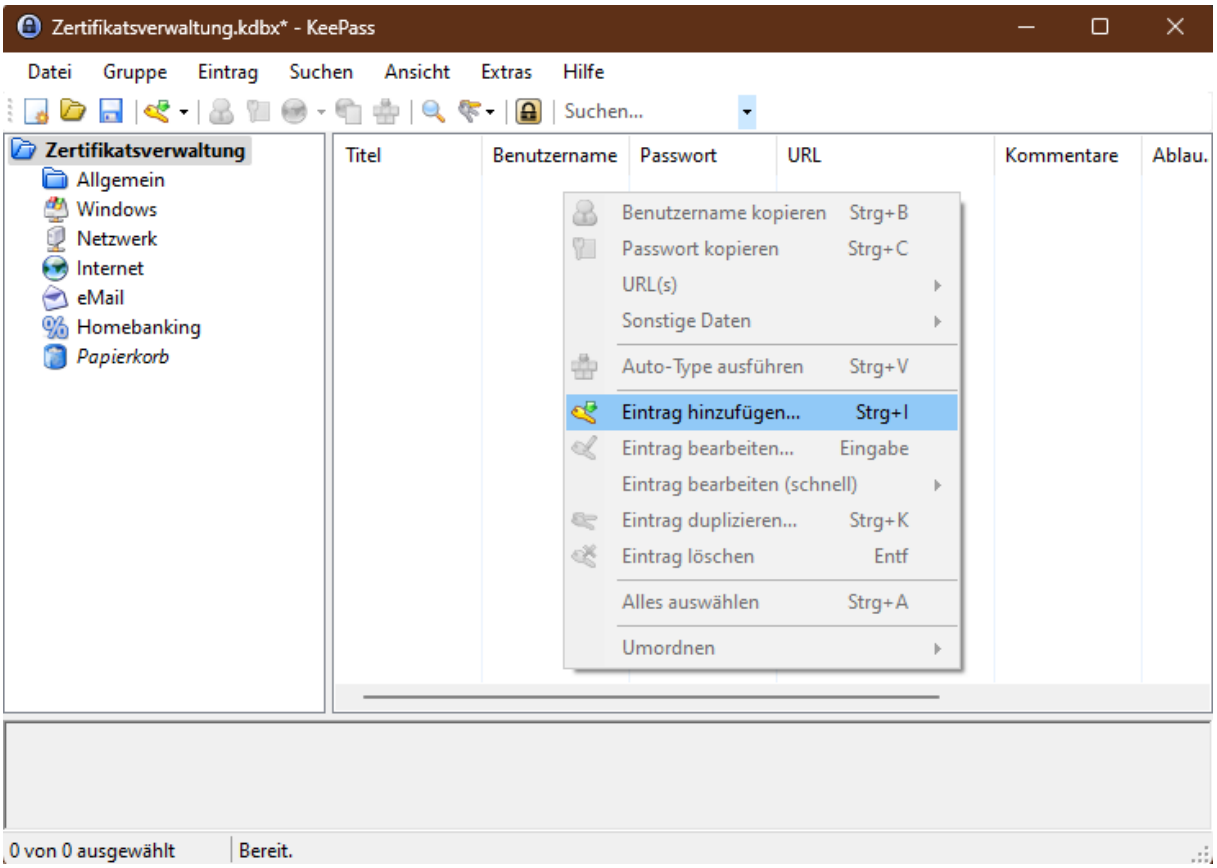
- Der Name der Organisation darf maximal 30 Zeichen lang sein. Die Bezeichnung darf vom Organisationsnamen gemäß Finanzamt abweichen. Sofern ein Ordnungskriterium (Steuernummer) des Finanzamtes Neubrandenburg verwendet wird, ist unter Steuernummer der Organisation das Land «*Mecklenburg-Vorpommern*» auszuwählen.
- Im Abschnitt «*Ansprechpartner*» sind die Angaben zum Mitarbeitenden mit Ausnahme seiner E-Mail-Adresse zu tätigen. Unter E-Mail-Adresse ist die Funktionspostfachadresse der zentralen Stelle einzutragen. Nach der Finalisierung des Zertifizierungsprozesses wird diese E-Mail-Adresse auf die E-Mail-Adresse des Mitarbeiters geändert.
- Die Angabe des Benutzernamens ist auf acht Zeichen beschränkt. Die zentrale Stelle sollte hier eine eigene Nomenklatur festlegen. Es ist auf Groß- und Kleinschreibung zu achten. Die Sicherheitsabfrage sollte einheitlich gestaltet und sicher verwahrt werden. Diese ist für die Löschung von Zertifikaten notwendig.
- Abschließend ist die Kenntnisnahme zum Hinweis für den Aktivierungsprozess zu bestätigen und auf «*Prüfen* >» zu klicken.
- Der Prozess wird mit der bestätigenden Eingabe des Captchas fortgesetzt. Geben Sie die angezeigten Buchstaben bzw. Ziffern ein und klicken auf «*Weiter* >».
- Abschließend werden die Daten nochmals zusammengefasst. Mit «*Absenden* >» wird die Richtigkeit der Daten bestätigt.
- Es wird eine E-Mail versendet, mit der der Registrierungsprozess bestätigt wird. Der Registrierungslink hat eine Gültigkeit von sieben Tagen. Nach dieser Zeit verfällt die Registrierung und die Beschaffung des Organisationszertifikates muss erneut erfolgen.
- Nach der Bestätigung der E-Mail-Adresse wird eine weitere E-Mail versandt, welche eine 18-stellige **Aktivierungs-ID** enthält.
- Innerhalb weniger Tage erhält die Landes- bzw. Kommunalbehörde oder der Landes- bzw. Kommunalbetrieb einen Brief mit einem 12-stelligen **Aktivierungscode**, mit welchem die Registrierung abgeschlossen wird.
- Es ist sicherzustellen, dass ausschließlich die zentrale Stelle diese Briefe erhält.
- Nach Erhalt des Briefes sind die Aktivierungsdaten einzugeben, indem dem Link aus der Aktivierungsmail gefolgt wird. Es öffnet sich eine Seite, in welcher die Aktivierungs-ID der E-Mail sowie der Aktivierungscode aus dem Brief eingegeben werden muss.
- Im Anschluss ist ein Passwort zu definieren. Das Passwort sollte entsprechend der geltenden Passwortrichtline zusammengesetzt sein und mindestens acht Zeichen lang sein.
- Nach dem Erstellen der Zertifikatsdatei muss diese heruntergeladen und lokal auf dem Computer gespeichert werden.
- Zum erstmaligen Login ist «*Mein Unternehmenskonto*» auszuwählen und man wird auf die Login-Seite geleitet.
- Zum Login klicken Sie auf «*Durchsuchen*» wählen die soeben erstellte Zertifikatsdatei aus und tragen unter «*Passwort*» das gesetzte Passwort ein.
- Im Folgenden müssen verschiedene Datenschutzhinweise und Haftungsausschlüsse für das Postfach bestätigt werden.
- Danach gelangt man auf eine zentrale Übersichtsseite der Benutzerverwaltung. Für einige Menüpunkte kann man zu ELSTER weitergeleitet werden (grüne Nutzeroberfläche).
- Damit ist die Beschaffung des Organisationszertifikates abgeschlossen. Anschließend kann man sich mittels der Zertifikatsdatei bei angeschlossenen Behördenportalen zur Nutzung von MUK anmelden.

5.2.2 Dokumentation in KeePass 2

Nach der erfolgreichen Anmeldung mit dem Organisationszertifikat bei ELSTER müssen nun die 10-stellige Benutzerkonto-ID sowie die Gültigkeit des Zertifikats in die Zertifikatsverwaltung von KeePass 2 übertragen werden.

Diese Daten finden sich je nach Browsereinstellung entweder unten oder rechts auf der Übersichtsseite. Mittels der «*Benutzerkonto-ID*» lässt sich ein Konto auch bei einem Wechsel der Zertifikatsdatei und im Falle von Nichtangabe einer Person eindeutig zuordnen. Die «*Gültigkeit des Zertifikats*» gibt an, wie lange die Zertifikatsdatei genutzt werden kann, ehe diese wiederbeschafft werden muss.

In KeePass 2 kann mit all diesen vorliegenden Informationen ein neuer Eintrag für die Zertifikatsdatei angelegt werden. Mittels Rechtsklick auf die Listenfläche wählen Sie über das Kontextmenü «*Eintrag hinzufügen…*».



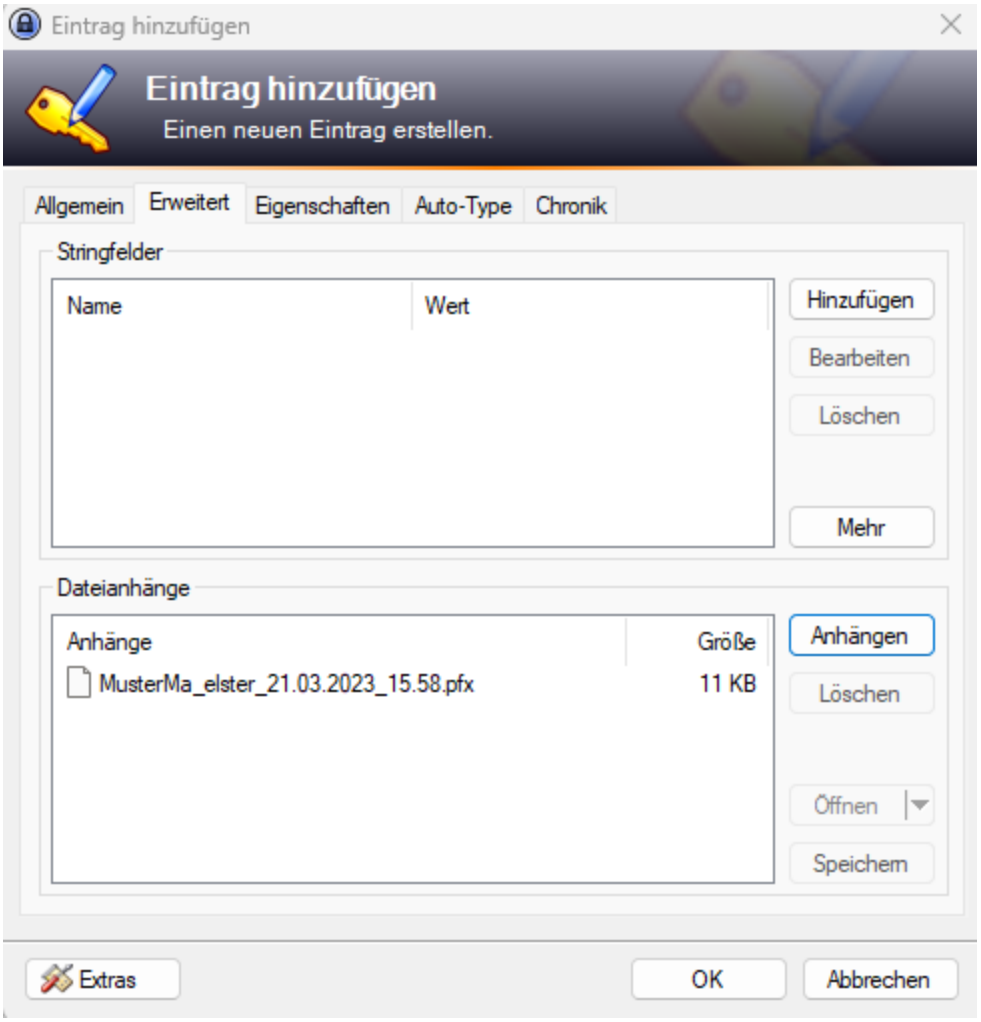
Es öffnet sich ein neues Dialogfeld mit mehreren Reitern zur Eintragsbearbeitung.

Unter «*Titel*» wird die 10-stellige Benutzerkonto-ID und unter «*Benutzername*» den vergebenen Namen aus der Registrierung ein. Das zu hinterlegende «*Passwort*» ist das Passwort der Zertifikatsdatei. Bei «*URL*» wird die aktuelle mit dem Zertifikat verbundene E-Mail-Adresse eingetragen.

Sofern im nächsten Schritt das Zertifikat dem betroffenen Mitarbeiter zur Verfügung gestellt werden soll, kann hier die dienstliche E-Mail-Adresse des Mitarbeiters hinterlegt werden.

Unter «*Kommentare*» können verschiedene Informationen zum betroffenen Zertifikat angegeben werden. Unter «*Gültig bis*» ist die Checkbox zu aktivieren und die Gültigkeit des Zertifikats einzutragen. KeePass 2 zeigt dann automatisch an, wenn das Zertifikat abgelaufen ist.

Auf der Registerkarte «*Erweitert*» kann unter «*Dateianhänge*» die Zertifikatsdatei angehängt werden.



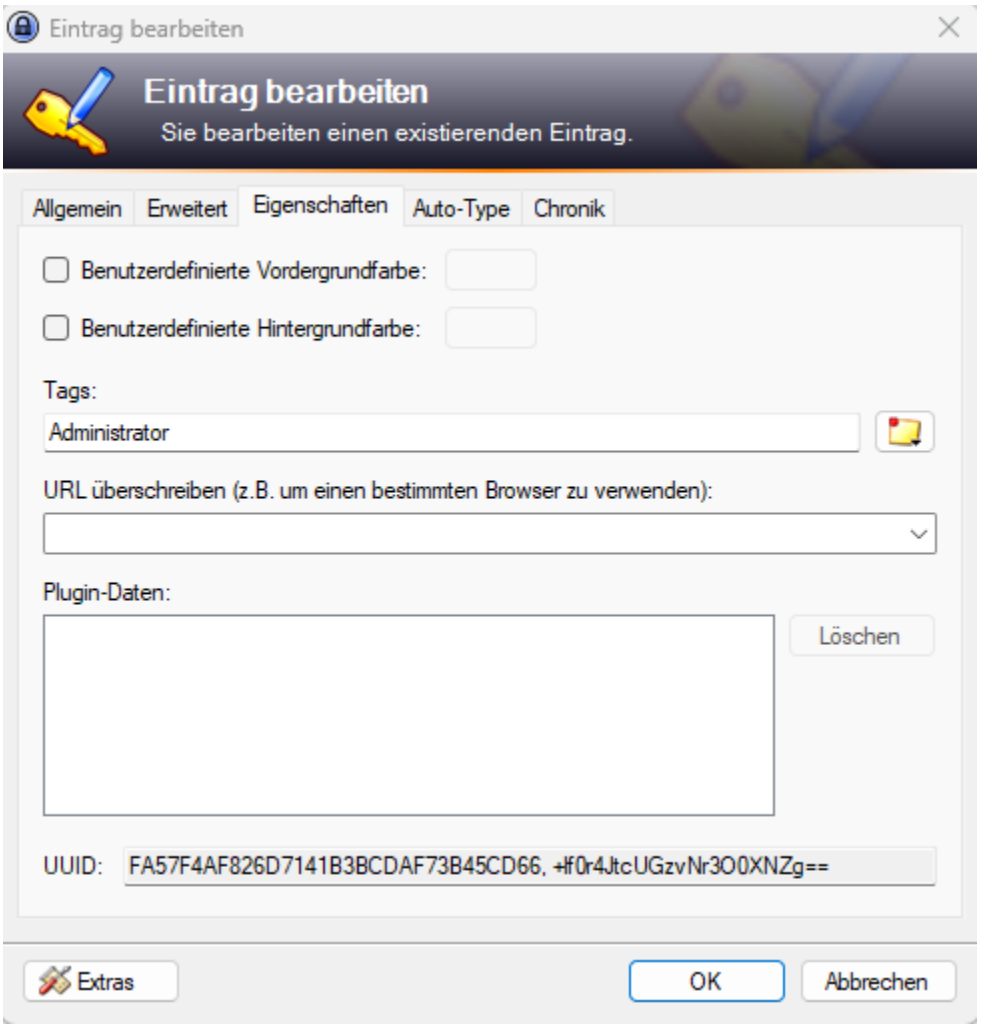
Auf der Registerkarte «*Eigenschaften*» ist unter «*Tags*» die Rolle einzutragen.

Es werden drei Rollengruppen empfohlen:

ADMINISTRATOR: Personen, die innerhalb der Organisation die Rolle der zentralen Stelle einnehmen und Organisationszertifikate verwalten (Adressaten dieses Leitfadens),

SACHBEARBEITER: Personen, die innerhalb der Organisation Anbieter von Verwaltungsleistungen sind (Service Owner) und durch die Berechtigungssteuerung Zugriff auf ihre Onlinedienste verwalten können,

KEINE FUNKTION: Personen, die MUK lediglich entsprechend ihrer Berechtigung für Verwaltungsleistungen nutzen. Hier besteht kein Handlungsbedarf zu den nächsten Schritten, da im Grundsatz zu einem Nutzer keine Funktion zugewiesen ist.



5.2.3 Bereitstellen des Organisationszertifikats an die Mitarbeitenden

Bevor das Organisationszertifikat an die Mitarbeitenden bereitgestellt wird, ist ihre / seine dienstliche E-Mail-Adresse im Zertifikat zu hinterlegen, so dass entsprechende Benachrichtigungen zur Nutzung des MUK bei ihm eingehen.

Hierzu meldet man sich mit dem betroffenen Zertifikat in der Benutzerverwaltung bei ELSTER an und klickt links auf «*Mein Benutzerkonto*», anschließend im sich öffnenden Menü auf «*E-Mail-Einstellungen*».

Im Folgedialog kann nun die E-Mail-Adresse angepasst werden und das dort hinterlegte Postfach der zentralen Stelle durch das persönliche, dienstliche E-Mail-Postfach des Mitarbeiters getauscht werden. Ggf. wird man aufgefordert, vorab fehlende Daten zu ergänzen. Dort sollen nur Pflichtfeldangaben ergänzt werden und keine Steuernummer ergänzt werden. Im Verlauf werden jeweils E-Mails sowohl an die alte als auch an die neue E-Mail-Adresse versendet. Der betroffene Mitarbeiter muss die Änderung bestätigen.

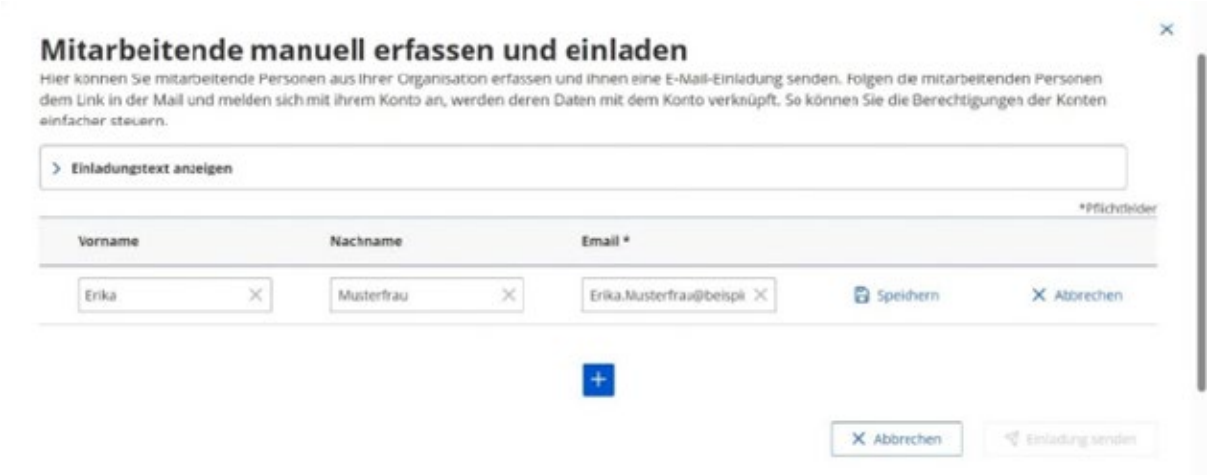
Stellen Sie diese Änderungsbestätigung durch jeweiligen Mitarbeiter organisatorisch sicher.

Damit ist die Zertifikatseinrichtung abgeschlossen und im nächsten Schritt kann das Zertifikat an den betroffenen Mitarbeitenden ausgehändigt werden. Für die Bereitstellung ist in jedem Fall erforderlich, dass die Zertifikatsdatei nicht gemeinsam mit dem zugehörigen Passwort übermittelt wird. Das Passwort soll in einer separaten vertraulichen E-Mail bereitgestellt werden.

5.2.4 Anmelden und Konfiguration in der Berechtigungssteuerung

Zunächst muss man sich mit dem Admin-Organisationszertifikat an der Berechtigungssteuerung anmelden.

In der Hauptansicht kann im Bereich der «*Admin-Funktionen*» der Menüpunkt «*Mitarbeitende verwalten und einladen*» gewählt werden. Hier können Mitarbeiter zur Berechtigungssteuerung hinzugefügt werden. Hierzu muss der Button «*Manuell hinzufügen*» gewählt werden.



Im folgenden Dialog ist der Vorname, Name und die dienstliche E-Mail-Adresse des Mitarbeitenden einzugeben und anschließend via «*Einladung senden*» dem Mitarbeitenden eine E-Mail zu senden. Der betroffene Mitarbeitende wird eine E-Mail erhalten, in der er aufgefordert wird, sich mit seinem Organisationszertifikat an der Benutzersteuerung anzumelden.

Nach erfolgreichem Abschluss der Anmeldung durch den Mitarbeitenden taucht dieser nunmehr in der Liste der bestätigten Mitarbeitenden auf.

Jetzt muss dem Mitarbeitenden in der Berechtigungssteuerung eine Rolle zugewiesen werden. Hinsichtlich der zu vergebenden Rollen wird auf die in Kapitel 5.2.2 beschriebenen Rollengruppen verwiesen.

Um die Zuweisung durchzuführen, wechselt man in der Hauptansicht zu den «*Konten meiner Organisation*».

Unter «*Konto-Details*» klickt man auf «*Bearbeiten*», um dem Mitarbeitenden eine Funktion (Rolle) zuzuweisen.

Hier kann dem Mitarbeitenden unter «*Funktion*» die entsprechende Rolle zugewiesen werden. Es ist hier möglich, mehrere Rollen zuzuweisen. Für die Rolle der zentralen Stelle wird der Haken bei «*Administrator*» gesetzt. Bei Bedarf kann dem Konto zusätzlich ein Alias sowie eine Alias-Beschreibung angefügt werden.

Mit Klick auf «*Speichern*» ist das Setzen der Berechtigung für die Person abgeschlossen.

5.3 Änderung von Organisationszertifikaten

Grundsätzlich können Änderungen in der Benutzerkontoverwaltung von ELSTER von den Mitarbeitenden selbstständig getätigt werden. Dies ist technisch nicht zu unterbinden, sollte jedoch organisatorisch untersagt werden, um die Einheitlichkeit der Einträge weiterhin zu gewährleisten und die selbstständige Übertragung von Zertifikaten zu vermeiden.

Folgende Änderungen können hier eigenverantwortlich ohne Unterstützung der zentralen Stelle vorgenommen werden:

- E-Mail-Adresse,
- Vor- und Zuname (nur intern),
- Neue Personen zu Zertifikat hinzufügen (nur intern),
- Organisationsname (nur intern),
- Organisationsadresse (nur intern)

Es ist den Mitarbeitenden mitzuteilen, dass keine Änderungen ohne Rücksprache mit der zentralen Stelle durchzuführen sind.

Nur mit Unterstützung der zentralen Stelle können folgende Änderungen durchgeführt werden:

- Name des Benutzerkontos,
- Passwort,
- Löschung des Zertifikats,
- Berechtigung des Organisationszertifikats in der Berechtigungssteuerung.

5.4 Sperrung von Organisationszertifikaten

Muss ein Organisationszertifikat wegen Missbrauch gesperrt werden, so erfolgt dies durch die Änderung des Passwortes in der Benutzerverwaltung von ELSTER. Sollte kein Zugriff auf das Zertifikat möglich, so ist eine Löschung (Kapitel 5.5) und Neuanlage (Kapitel 5.2) erforderlich.

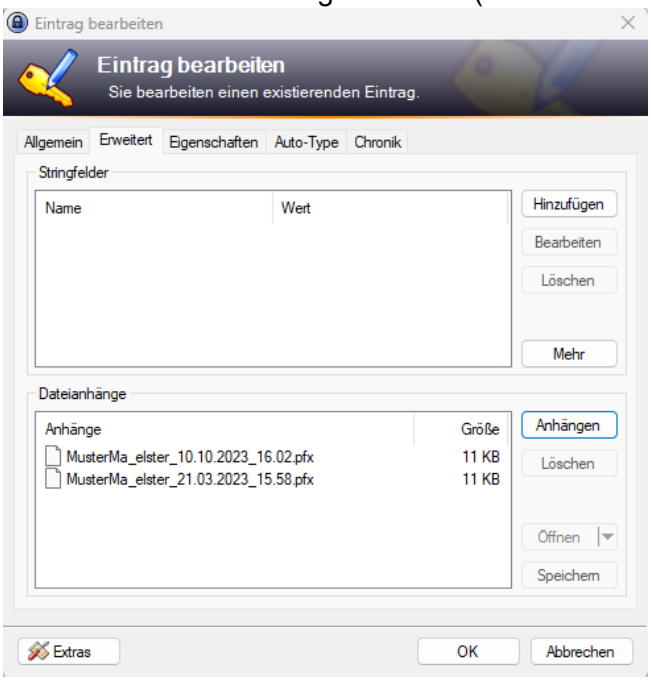
Zunächst muss man sich mit dem Zertifikat anmelden, welches gesperrt werden soll.

Zunächst sollte die E-Mail-Adresse auf die E-Mail-Adresse der zentralen Stelle zurückgesetzt werden, da dann alle Benachrichtigungen zum Zertifikat bei der zentralen Stelle eingehen. Mit Klick auf «*Übernehmen*» wird der Vorgang abgeschlossen. Anschließend wechselt man über den Menübereich «*Mein Benutzerkonto*» auf die «*Passwort-Einstellungen*».

Hier wird «*Passwort ändern*» ausgewählt.

Hier ist zunächst das aktuelle Passwort und danach ein neues Passwort einzutragen. Es wird empfohlen, den Namen der herunterzuladenden Zertifikatsdatei beizubehalten. Unter «*Passwort ändern und Zertifikatsdatei herunterladen*» wird der Vorgang abgeschlossen.

Die neue Zertifikatsdatei wird nun in der Zertifikatsverwaltung von KeePass 2 dem betroffenen Nutzer hinterlegt (Reiter «*Erweitert*», «*Dateianhänge*»).



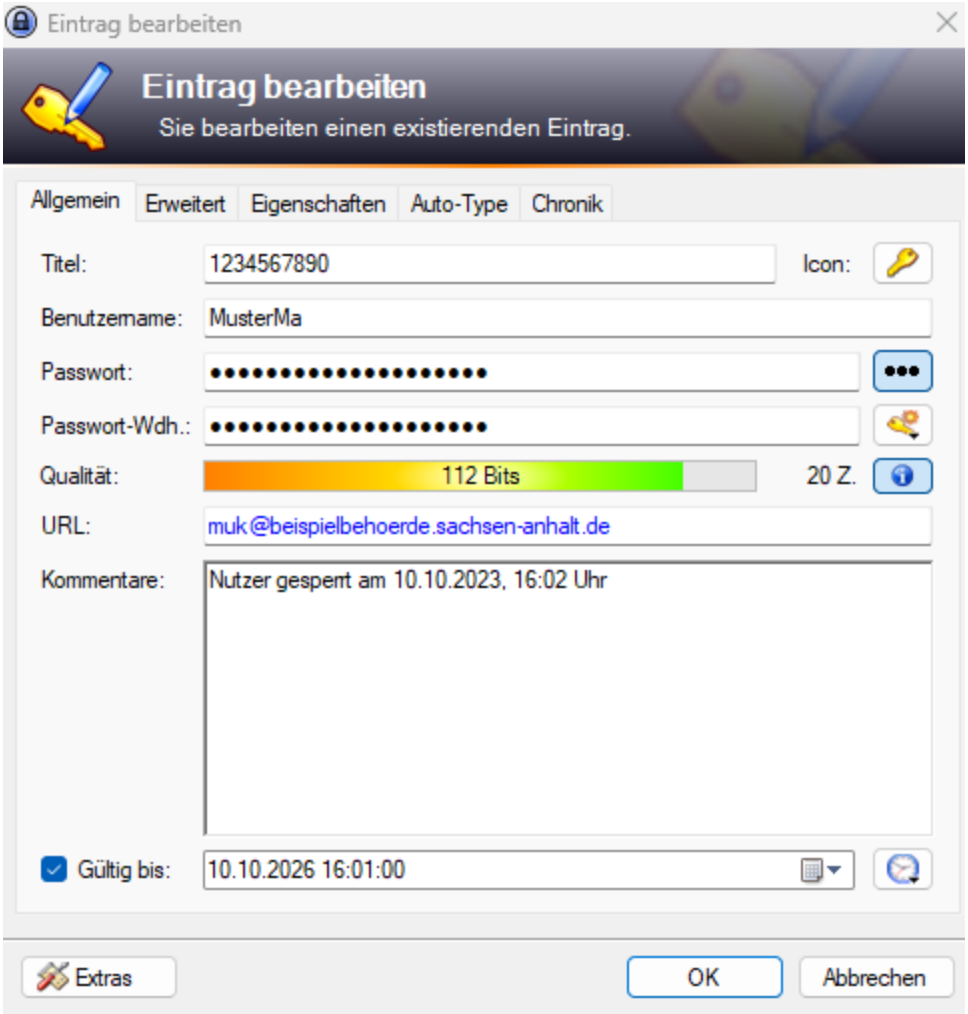
Die Datei mit dem neuesten Datum ist diejenige, die aktuell und gültig ist.

Im Reiter «*Allgemein*» sind folgende Änderungen vorzunehmen:

- Neues Passwort des Zertifikates,
- Neue E-Mail-Adresse,
- Neue Gültigkeit des Zertifikates,
- Kommentar zur Sperrung des Zertifikates.

Damit ist die Sperrung abgeschlossen und dokumentiert.

Sobald die Sperrung aufgehoben wird, ist die E-Mail-Adresse wieder zu ändern und dem Mitarbeiter die Zertifikatsdatei sowie das Passwort analog zum Zertifikatsbeschaffungsprozess auszuhändigen.



5.5 Löschung von Organisationszertifikaten

Scheidet ein Mitarbeitender aus der Organisation aus oder benötigt er aus einem anderen Grund kein Organisationszertifikat mehr, so muss dieses gelöscht werden. Die Löschung des Zertifikats wird durch die zentrale Stelle im Benutzer von ELSTER durchgeführt.

Zunächst sollte die E-Mail-Adresse auf die E-Mail-Adresse der zentralen Stelle zurückgesetzt werden, da dann alle Benachrichtigungen zum Zertifikat bei der zentralen Stelle eingehen. Navigieren Sie in das Menü «*Mein Benutzerkonto*» und wählen «*E-Mail-Einstellungen*» und danach «*E-Mail-Adresse ändern*». Ändern Sie die E-Mail-Adresse auf die Funktionspostfach-Adresse der zentralen Stelle.

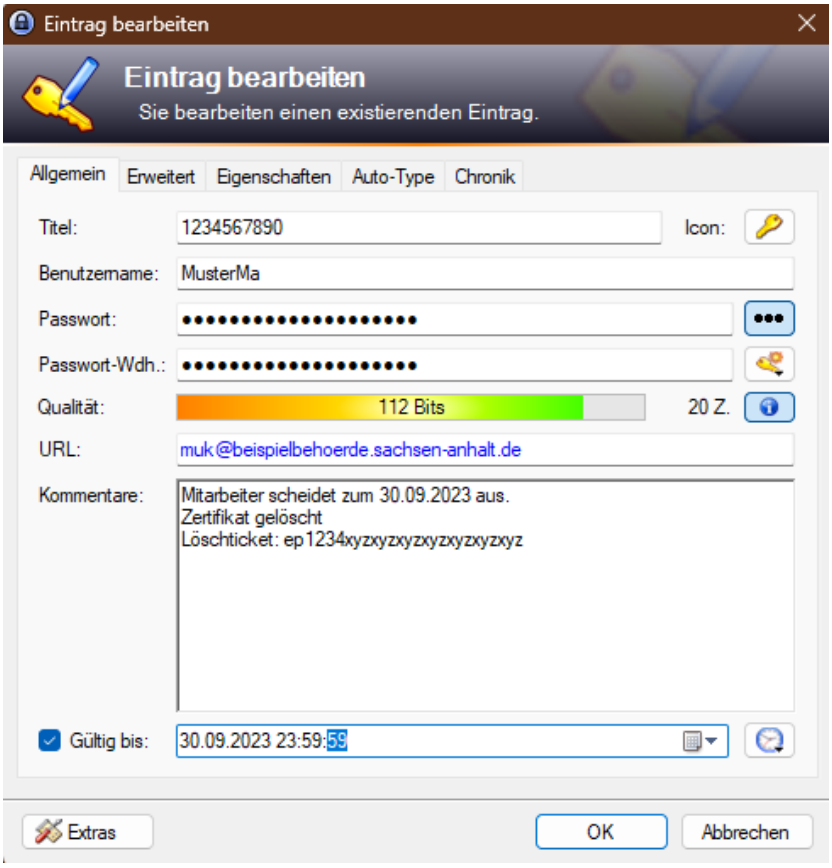
Mit Klick auf «*Übernehmen >*» wird der Vorgang abgeschlossen.

Kehren Sie zum Hauptmenü zurück und wählen dort «Benutzerkonto löschen»“ aus.

Hier ist die nur der zentralen Stelle bekannte Sicherheitsabfrage mit zugehöriger Antwort einzugeben. Für eine ordnungsgemäße Löschung wird unter Begründung «*Konto wird nicht mehr benötigt*» ausgewählt und anschließend auf «*Weiter >*» geklickt.

Es erscheint ein Hinweis, welcher die Konsequenzen der Löschung aufzeigt. Mit «*Ja, Benutzerkonto löschen*» wird der Löschvorgang initiiert.

Die Kontolöschung seitens ELSTER ist nun abgeschlossen. Es wird empfohlen, die Ticketnummer zu kopieren und in der Zertifikatsverwaltung von KeePass 2 zu hinterlegen. Zudem erhält die zentrale Stelle eine Bestätigungs-Mail.



In der Zertifikatsverwaltung von KeePass 2 ist die Löschung zu vermerken. Unter «*Kommentare*» ist der Grund für die Löschung sowie die Ticketnummer einzutragen. Unter «*Gültig bis*» ist der Zeitpunkt der Löschung anzugeben.

Der gelöschte Nutzende wird in der Zertifikatsverwaltung von KeePass 2 durchgestrichen, da das Gültigkeitsdatum in der Vergangenheit liegt. Der Eintrag zu diesem Mitarbeitenden darf nicht gelöscht werden, da sonst eine dokumentierte Historie zu diesem Zertifikat nicht dokumentiert werden kann.

Das Löschen des Zertifikats ist damit abgeschlossen und dokumentiert.

5.6 Erteilen von Berechtigungen für digitale Verwaltungsleistungen

Für Ihre Mitarbeitenden, die MUK nutzen, kann mithilfe der Berechtigungssteuerung der Zugriff auf zugangsbeschränkte Online-Dienste gesteuert werden. Voraussetzung ist die Aktivierung der Konto-Berechtigung aus Kapitel 4.4, sodass nicht pauschal alle Leistungen für alle Zertifikatsinhaber verfügbar sind.

Vertiefende Einzelheiten zur Verwendung der Berechtigungssteuerung finden sich im Quick-Start-Guide der Berechtigungssteuerung für nutzende Organisationen. Im Folgenden wird an dieser Stelle auf die pauschale Berechtigungssetzung für Ihre Behörde oder Landesbetrieb, dem Anlegen von Berechtigungsgruppen sowie die individuelle Berechtigung je Mitarbeitenden eingegangen. Da die Berechtigungssetzung für Online-Dienste nicht Aufgabe der zentralen Stelle ist, wird dies im Weiteren nicht vertieft.

Alle in den folgenden beschriebenen Schritten erfordern eine Anmeldung als Administrator in der Berechtigungssteuerung.

5.6.1 Pauschale Berechtigungen für die Organisation festlegen

Mit der pauschalen Berechtigung kann für alle Mitglieder einer Organisation festgelegt werden, zu welchen an der Berechtigungssteuerung angeschlossenen Online-Diensten grundsätzlich der Zugriff gewährt wird. Hierbei ist zu beachten, dass die jeweilige Verwaltungsleistung an der Berechtigungssteuerung angeschlossen sein muss. Andernfalls kann diese nicht durch die Berechtigungssteuerung reglementiert werden.

In der Hauptansicht der Berechtigungssteuerung klickt man hierzu auf «*Berechtigungen meiner Organisation*».

Im Folgedialog im Reiter «*Explizite Berechtigungen*» werden nun die zugangsbeschränkten Online-Dienste angezeigt, auf welche die Organisation grundsätzlich Zugriff hat. Im Reiter «*Beantragte Berechtigungsverfahren*» können ein Überblick zu laufenden Berechtigungsbeantragungen bieten. Mit Klick auf «*+ Berechtigung hinzufügen*» können hier weitere Online-Dienste hinzufügt werden.

Durch einen Klick auf «*+ Berechtigung hinzufügen*» kann nun der Onlinedienst ausgewählt werden, welcher für die Organisation hinzugefügt werden soll.

Nachdem der Onlinedienst angefügt wurde bzw. die erforderliche Zustimmung zur Nutzung erteilt wurde, sind diese Onlinedienste für die pauschale Berechtigung für alle Mitarbeiter der Organisation angefügt.

5.6.2 Berechtigungsgruppen in der Berechtigungssteuerung anlegen

Durch Anlage von Berechtigungsgruppen kann der Zugriff weiter differenziert werden, sodass beispielsweise einer Abteilung innerhalb einer Organisation dediziert Zugriff auf einen an die Berechtigungssteuerung angeschlossenen Onlinedienst gewährt werden kann.

Im ersten Schritt müssen die Berechtigungsgruppen in der Berechtigungssteuerung angelegt werden, welche mit den jeweiligen Rechten ausgestattet werden können.

Hierzu muss in der Hauptansicht der Berechtigungsteuerung auf «*Berechtigungsgruppen*» geklickt werden.

Die Übersichtsseite zu den Berechtigungsgruppen sollte zunächst leer sein. Mit Klick auf «+ *Gruppe anlegen*» kann eine neue Berechtigungsgruppe angelegt werden.

Im Folgemenü unter dem Reiter «Gruppen-Details» ist der Name der Gruppe festzulegen. Optional kann eine kurze Beschreibung hinzugefügt werden.

Im nächsten Reiter «*Berechtigungen*» können nun zur Berechtigungsgruppe der Zugang zu einem Onlinedienst hinzufügt werden. Hier ist auf «+ *Berechtigung hinzufügen*» zu klicken. Anschließend kann der Onlinedienst ausgewählt werden, zu welchem die Berechtigungsgruppe Zugang erhalten soll. Das Vorgehen ist hier analog zu Abschnitt 5.6.1.

Im letzten Reiter Mitglieder der Gruppe können nun die Mitglieder der Organisation durch Klick auf «+ *Mitglieder hinzufügen*» zu Ihrer Berechtigungsgruppe hinzugefügt werden, die den gleichen Zugang zu Onlinediensten erhalten sollen. Die Mitglieder müssen Inhaber eines ELSTER-Organisationszertifikats sein und wie in Abschnitt 5.2.4 beschrieben an der Berechtigungssteuerung bekannt sein. Es ist hierbei möglich, dass Mitglieder mehreren Berechtigungsgruppen zugeordnet werden können.

5.6.3 Individuelle Berechtigungen für Mitarbeitende

Es wird grundsätzlich die Anlage von Berechtigungsgruppen empfohlen. Falls das Erfordernis besteht, einzelnen Mitarbeitern individuelle Berechtigungen zu erteilen, ist dies möglich. In der Hauptansicht klickt man auf «*Konten meiner Organisation*».

In diesem Menü befinden sich alle Mitarbeitenden, die zur jeweiligen Organisation an die Berechtigungssteuerung angebunden sind. In der Tabelle unter Konto ist zur jeweiligen Person ein Link zu weiteren Einstellungen hinterlegt. Es ist der Link der betroffenen Person auszuwählen, welcher eine individuelle Berechtigung erteilt werden soll.

Man erreicht nun die Verwaltung der jeweiligen in der Berechtigungssteuerung. Es muss der Reiter «*Berechtigungen*» ausgewählt werden.

Hier werden die Onlinedienste angezeigt, zu welchen die Person bereits Zugang hat. Durch Klick auf «*+ Berechtigung hinzufügen*» kann die Person für weitere Onlinedienste berechtigt werden.

5.6.4 Berechtigungsanfragen durch Mitarbeitende

Wird einem Mitarbeitenden der Zugang zu einem an der Berechtigungssteuerung angeschlossenen Onlinedienst verweigert, liegt dies an fehlenden Berechtigungen entweder für die gesamte Organisation oder für den anfragenden Mitarbeitenden.

Dem betroffenen Mitarbeitenden wird der Dialog *„Fehlende Berechtigungen“* gezeigt. Fehlen der Organisation noch die Berechtigungen, werden diese vom Mitarbeitenden im Anfrageprozess direkt für die Organisation beantragt. Die zentrale Stelle wird zu diesem Prozess über eine Benachrichtigung auf dem Laufenden gehalten. Die Benachrichtigungen finden sich durch Klick auf «*Benachrichtigungen*» im Hauptmenü.

An dieser Stelle wird eine Übersicht über offene Berechtigungsanfragen sowohl seitens der Organisation gegenüber über als auch Anfragen Dritter zu eigenen Onlinediensten angezeigt. Beispielsweise hat die Organisation die Berechtigung erhalten, den angefragten Onlinedienst zu nutzen.

Es ist zu beachten, dass die beantragenden Mitarbeitenden explizit individuell auf den Dienst über eine Berechtigungsgruppe berechtigt werden müssen. Anderenfalls erhält der Mitarbeiter einen Hinweis, dass er sich an den Administrator wenden soll. In diesem Fall wird er sich direkt an die zentrale Stelle wenden, ohne eine integrierte Berechtigungsanfrage zu stellen.

Es muss der Kontakt zum Fachbereich sichergestellt werden, um Mitarbeiter auf Anfrage sachgerecht berechtigen zu können.

6 Weiterführende Informationen

Weiterführende Informationen finden sich unter:

Das Unternehmenskonto auf Basis von ELSTER - Unternehmenskonto (mein-unternehmens-konto.de)

Mein Unternehmenskonto - Wissensdatenbank (dataport.de)

Downloads - Unternehmenskonto (mein-unternehmenskonto.de)