MEIN UNTERNEHMENS-KONTO

NEZO Integrationsleitfaden

Stand 11/2024 – Version 2.82

Herausgegeben von

Bayerisches Staatsministerium für Digitales
Bayerisches Landesamt für Steuern
ELSTER

Hinweis zur geschlechterneutralen Sprache

Zur besseren Lesbarkeit wird in diesem Dokument das generische Maskulinum verwendet. Es wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter, sofern nicht explizit ein bestimmtes Geschlecht gemeint ist.

Inhaltsverzeichnis

1. Einleitung

Dieser Leitfaden richtet sich an Architekten, Entwickler sowie Vorhabensverantwortliche, die die NEZO-Schnittstelle von **Mein Unternehmenskonto** anbinden wollen, um die Authentifizierung und die Identitätsdaten in ihre Webanwendung zu integrieren. In den nachfolgenden Kapiteln soll insbesondere auf die über die Schnittstelle gelieferten Daten und die konkrete SAML-Schnittstelle für NEZO eingegangen werden.

Wenn Sie auf technische, organisatorische oder andere Herausforderungen bezüglich Ihrer Anbindung oder des Self Service Portals (SSP) stoßen, die der Leitfaden nicht beantworten kann, nutzen Sie bitte die Funktion **"Supportanfrage"** im SSP.

Beachten Sie bei der Anbindung der NEZO-Schnittstelle bitte folgendes: Wir möchten möglichst bundesweit eine Einheitlichkeit im „Branding“ des Unternehmenskontos gewährleisten. Wir bitten Sie daher, entsprechende Login-Buttons ausschließlich mit **„Login mit Mein UK“ oder „Login mit Mein Unternehmenskonto"** zu versehen.

Die Integration kann im Ergebnis wie folgt aussehen:

Dabei können Sie für das Anlegen eines Benutzerkontos unmittelbar auf folgenden Link verweisen: www.mein-unternehmenskonto.de/registrierung

Hilfreich kann für die Nutzer auch ein entsprechender Infotext zum Unternehmenskonto sein:

„Der Login erfolgt über **Mein Unternehmenskonto**. **Mein Unternehmenskonto** ist das bundesweit einheitliche Nutzerkonto für Unternehmen/Organisationen und darauf ausgelegt,

dass es für alle Bereiche im Umfeld der öffentlichen Verwaltung genutzt werden kann. Für den Login benötigen Sie ein ELSTER-Organisationszertifikat, das hier beantragt werden kann. Bitte beachten Sie, dass die Zusendung des Aktivierungsbriefes einige Zeit (durchschnittlich 2 – 5 Tage) in Anspruch nimmt. Sollten Sie noch kein ELSTER-Organisationszertifikat haben, sollte dies zeitnah beantragt werden.

Voraussetzung dabei ist immer das Vorhandensein einer deutschen Steuernummer (StNr) unabhängig davon, auf welcher Grundlage (z.B. Lohnsteuer, Umsatzsteuer, Grundsteuer) diese beruht. Die StNr ist das Merkmal, auf dem das ELSTER-Organisationszertifikat basiert.

In Abgrenzung zu den ELSTER-Organisationszertifikaten gibt es auch persönliche ELSTER-Zertifikate, denen die Steueridentifikationsnummer (IdNr) zugrunde liegt. Diese sind vor allem für Bürger relevant, können aber im Ausnahmefall auch in diesem Portal für einen Antrag genutzt werden. Dies gilt ausschließlich für solche Organisationen, Selbständige oder Einzelunternehmer, die kein ELSTER-Organisationszertifikat besitzen und auch keines beantragen können (z.B. weil keine betriebliche StNr vorhanden ist)."

Weitere Informationen finden Sie auch unter *Einbindung von* **Mein Unternehmenskonto** *in die eigene Benutzeroberfläche.*

2. Vorgehen bei der Integration Schritt-für-Schritt

Die nachfolgende Reihenfolge von Schritten zur Einbindung der NEZO-Schnittstelle stellt einen roten Faden dar, mit dem Sie sicher zum Ziel gelangen. Auch wenn der Vorschlag einen sequenziellen Verlauf beschreibt, so lassen sich die einzelnen Themen auch in anderer Reihenfolge bzw. parallel durchlaufen.Sie stellen somit eine Empfehlung dar, die sich ausschließlich auf die Unternehmenskonto-relevanten Aspekte Ihrer Integration beziehen.

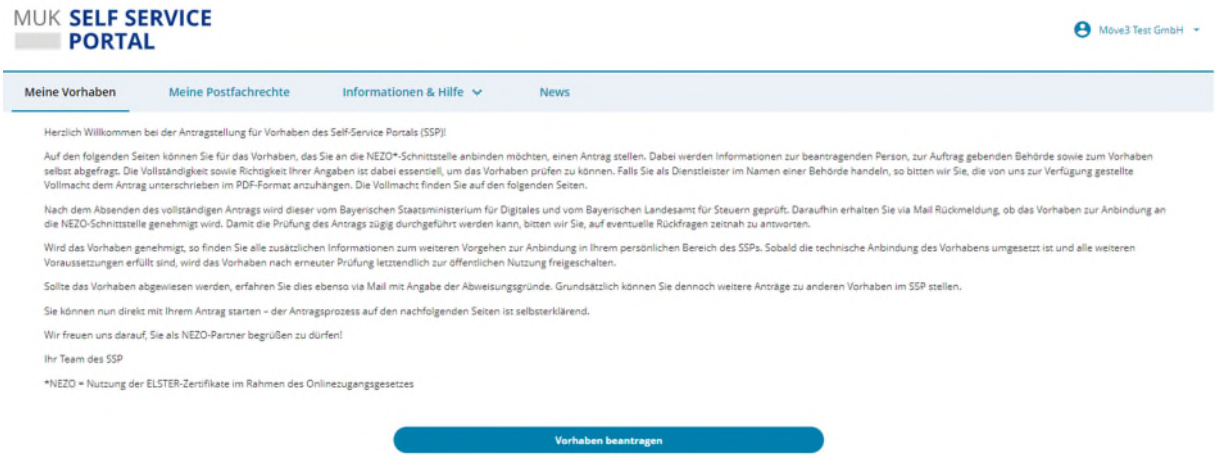
2.1. Schritt 1: Voraussetzungen für die Integration

Zur Unterstützung Ihrer Integration steht Ihnen das SSP des Unternehmenskontos zur Verfügung. Dort können Sie sich mit Ihrem ELSTER-Organisationszertifikat anmelden und im Rahmen des Onboardings strukturiert Ihre Vorhaben beschreiben. Später können Sie selbstständig Ihre Service Provider anlegen und verwalten. Gestellte Anfragen Ihrerseits werden medienbruchfrei von uns über unser Ticketsystem bearbeitet. Zudem stehen Ihnen im SSP alle relevanten Informationen zur Verfügung.

Das SSP ist unter folgender URL erreichbar: https://service.mein-unternehmenskonto.de

2.2. Schritt 2: Onboarding im SSP / Vorhaben beantragen

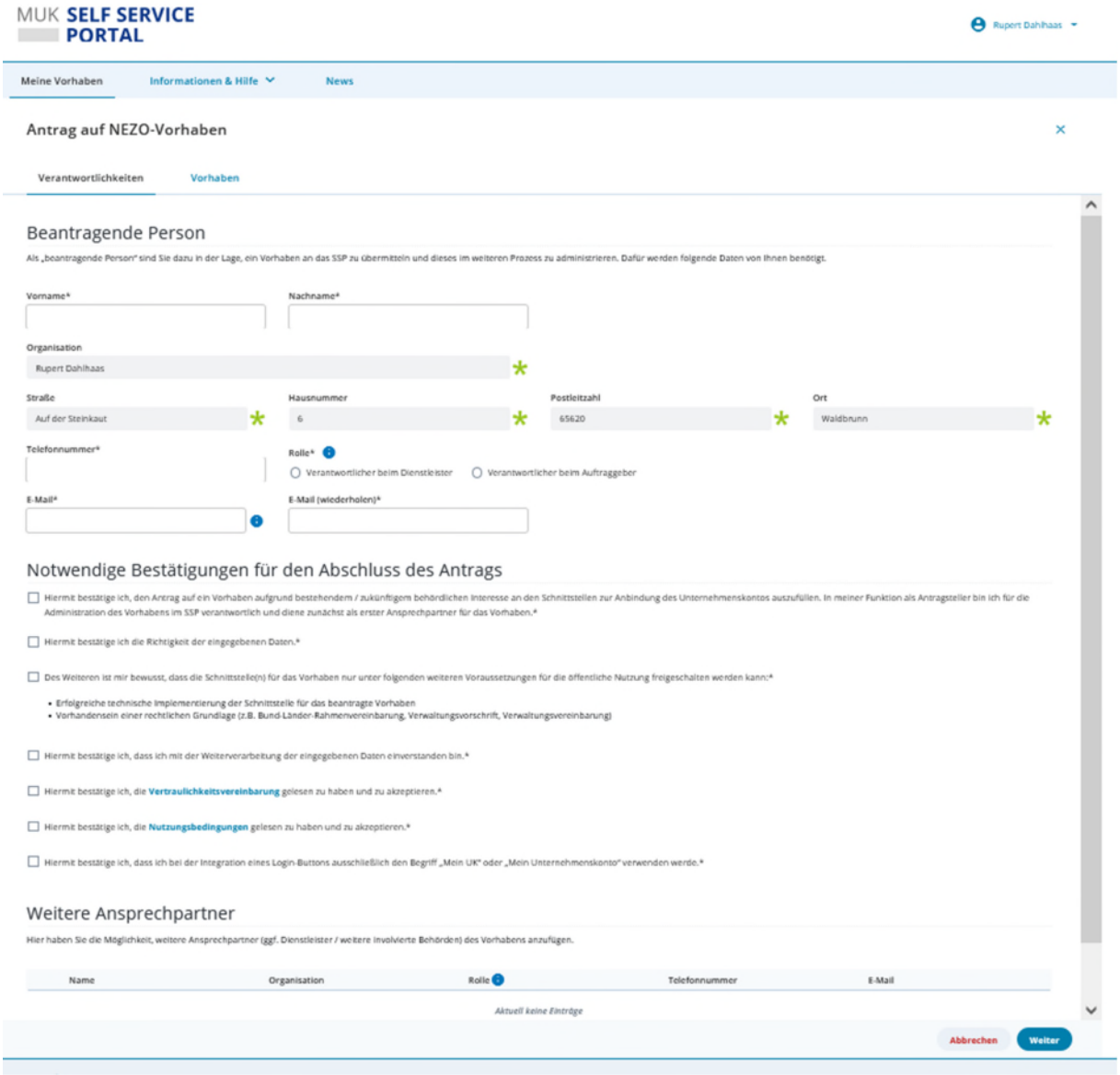
Sofern Sie sich erstmalig im SSP anmelden, können Sie umgehend damit starten, Ihr Vorhaben zu beschreiben und zu beantragen. Klicken Sie hierfür auf "Vorhaben beantragen". Sollten Sie bereits Anträge gestellt haben, können Sie diese in der Ansicht "Meine Vorhaben" finden.



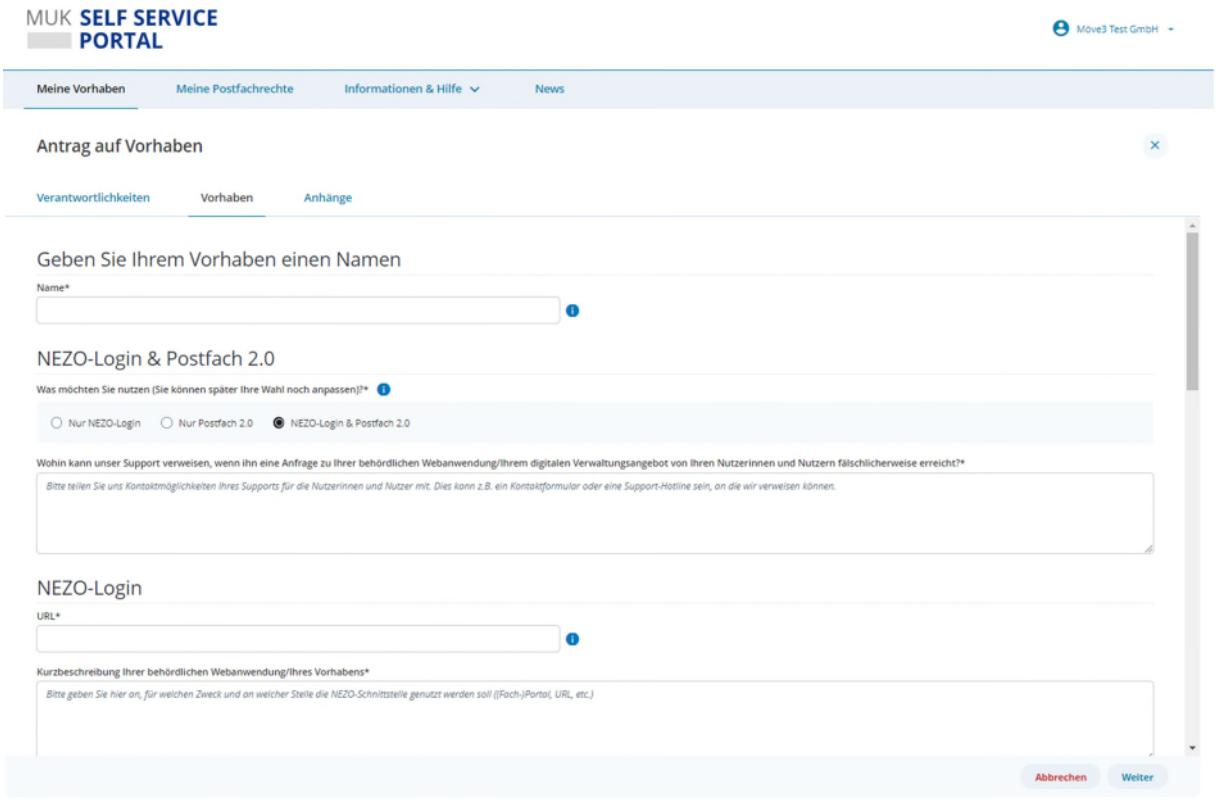
Das Formular besteht aus zwei Seiten. Pflichtangaben sind mit * gekennzeichnet. Wichtig sind auf der ersten Seite die Erfassung der für das Unternehmenskonto wichtigen Ansprechpartner Ihrerseits mit den zugehörigen Kontaktdaten.

Wenn Sie ein beauftragter Dienstleister sind, laden Sie bitte den unterschriebenen Nachweis über den Auftrag Ihres Auftraggebers hoch.

⚠ Bitte halten Sie die Liste der Ansprechpartner auch nach einer erfolgreichen NEZO-Integration für die gesamte Laufzeit Ihres Vorhabens stets aktuell. Für Ankündigungen von Neuigkeiten, Änderungen, möglichen Ausfallzeiten und anderen relevanten Mitteilungen ist es unerlässlich, aktuelle Kontaktdaten zu haben.



Die zweite Seite fragt Sie nach allgemeinen Informationen, die u.a. dazu dienen sollen, die Last- und Performanceanforderungen an **Mein Unternehmenskonto** abschätzen zu können. Bitte geben Sie dazu auch an, wenn Sie für Ihr Vorhaben während des Jahres Spitzenzeiten erwarten.



Durch Klicken auf die Schaltfläche "Abschicken" schicken Sie Ihren Antrag ab. Die zeitnahe Genehmigung erfolgt durch Mitarbeiter des Projektes **Mein Unternehmenskonto**. Sie werden per E-Mail über Genehmigung/Ablehnung/Rückfragen informiert.

2.3. Schritt 3: Auswahl des für Sie relevanten Datenkranzes und der weiteren Konfiguration

Spätestens nach Genehmigung Ihres Antrages für ein neues Vorhaben, sollten Sie die Vorbereitungen für die technische Integration treffen. Bei der nachfolgenden Einrichtung Ihres "Service Providers" müssen einige Einstellungen im SSP vorgenommen werden, die entsprechende Konsequenzen mit sich bringen. In den nachfolgenden Abschnitten sind die entsprechenden Möglichkeiten beschrieben.

2.3.1. Auswahl des Datenkranzes

ELSTER kann individuell pro angeschlossenem Service Provider unterschiedliche SAML-Assertion-Attribute zurückgeben. Die Attribute werden dabei zu sogenannten "Datenkränzen" zusammengefasst.

Eine Auflistung der aktuell vorhandenen Datenkränze findet sich in Kapitel Datenkränze.

2.3.2. Auswahl der für Sie relevanten "Zertifikatstypen" (Zum Login zugelassene(s) Ordnungsmerkmal(e))

Über **Mein Unternehmenskonto** stehen Ihnen zwei unterschiedliche Zertifikatstypen zur Verfügung, die die NEZO-Schnittstellen nutzen können. Dies sind

- Persönliche Zertifikate, die mit der persönlichen steuerlichen IdNr registriert wurden. Dies betrifft Privatpersonen, die aber u.U. auch unternehmerisch tätig sind (z.B. Betreiber einer Solaranlage) bzw. ein Unternehmen gründen wollen. Es kann nur ein Zertifikat pro IdNr registriert werden.
- Organisations-/Unternehmenszertifikate, die mit der StNr der jeweiligen Organisation registriert wurden. Dies betrifft Einzelunternehmer, juristische Personen (Unternehmen, Behörden, etc.), die über eine deutsche StNr verfügen, weil sie in Deutschland steuerpflichtig sind. Es kann mehrere 1.000 Zertifikate pro StNr geben.

Je nach dem auf Ihrer Seite angebotenen Fachverfahren können Sie auf Seiten des ELSTER Identity Providers (ELSTER-IdP) die für Sie relevanten Typen konfigurieren. Um alle relevanten Fälle abzudecken, wird empfohlen, beide Zertifikatstypen zuzulassen. Sind ausschließlich IdNr-Zertifikate für Sie relevant, so kann der ELSTER-IdP die anderen Zertifikatstypen "herausfiltern" und abweisen.

2.3.3. Benötigen Sie Testzertifikate für produktive Smoke-Tests?

Unter Umständen haben Sie Bedarf an "Smoke-Tests" Ihres Echtsystems gegen das ELSTER Echtsystem. Hierfür können sogenannte "Testzertifikate" genutzt werden. Die Nutzung der Testzertifikate muss explizit für Ihr Vorhaben im ELSTER-IdP konfiguriert werden UND zudem auch in Ihrer Software verankert werden. Es muss auf Seiten Ihrer Software sichergestellt werden, dass Testdaten und Echtdaten nicht vermischt werden können.

Testzertifikate werden mit einem zusätzlichen Parameter in der SAML-Antwort des ELSTER-IdP gekennzeichnet.

⚠ Produktiv können nur Zertifikate für Smoke-Tests angeboten werden. Für ausführliche Integrationstests Ihrer Anwendung steht Ihnen unsere E4K-Testumgebung zur Verfügung.

2.3.4. Speichern Sie ELSTER-Identitätsdaten?

Sofern Sie die von ELSTER erhaltenen Identitätsdaten in Ihrem System speichern, können wir Sie darüber informieren, sobald der Anwender bei ELSTER

a.) sein Konto komplett löscht oder

b.) der Verwendung seines Zertifikates außerhalb von ELSTER ("andere eGovernmentdienste") widerspricht.

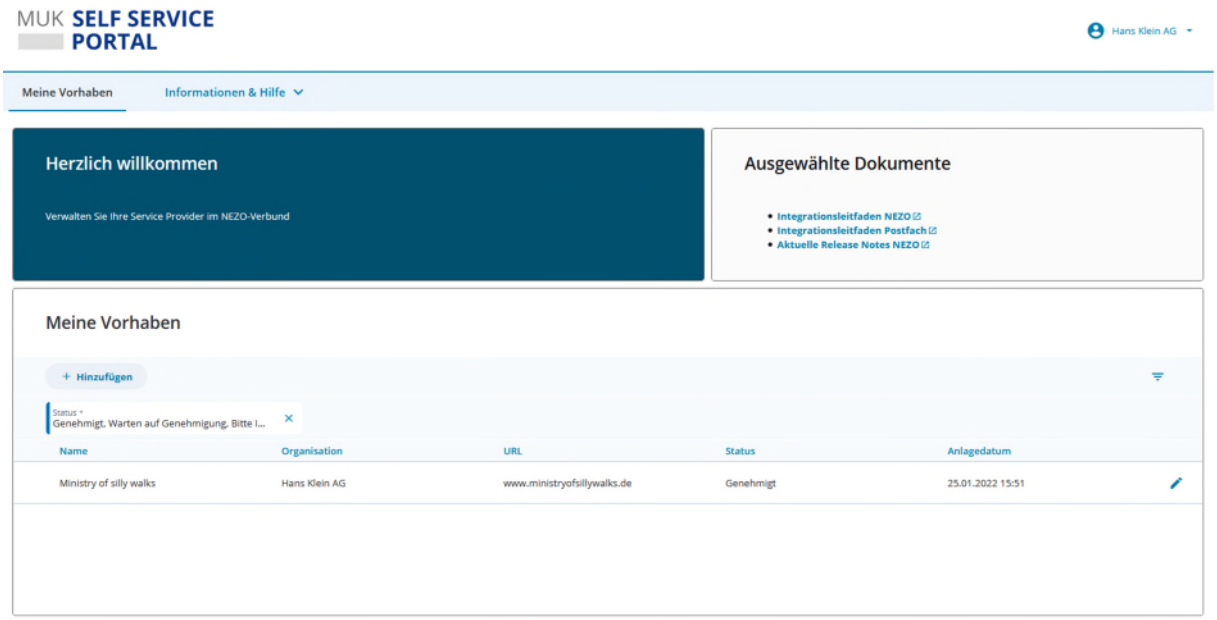
In diesen Fällen schickt der ELSTER-IdP einen ManageNameID-Request an Ihren Service Provider. Es ist also möglich, einen entsprechenden ManageNameID-Serviceendpunkt anzubieten und deren URL bei der Anlage Ihres Service Providers im SSP zu hinterlegen.

2.3.5.Möchten Sie am Single-Sign-On Verbund teilnehmen?

Einige der an das Unternehmenskonto angebundenen Dienste nutzen die vorhandene Single-Sign-On Funktionalität. Um an diesem Verbund teilzunehmen, ist es unbedingt erforderlich auf Seiten Ihrer Anwendung eine Logout-Möglichkeit zu implementieren, die den `SingleLogoutService` des ELSTER-IdP anspricht. Die entsprechende Logout URL kann im Schritt 4 bei der Konfiguration des Service Providers angegeben werden. Weitere Informationen zum Single-Sign-On sind im Kapitel Begriffsbestimmung zu finden.

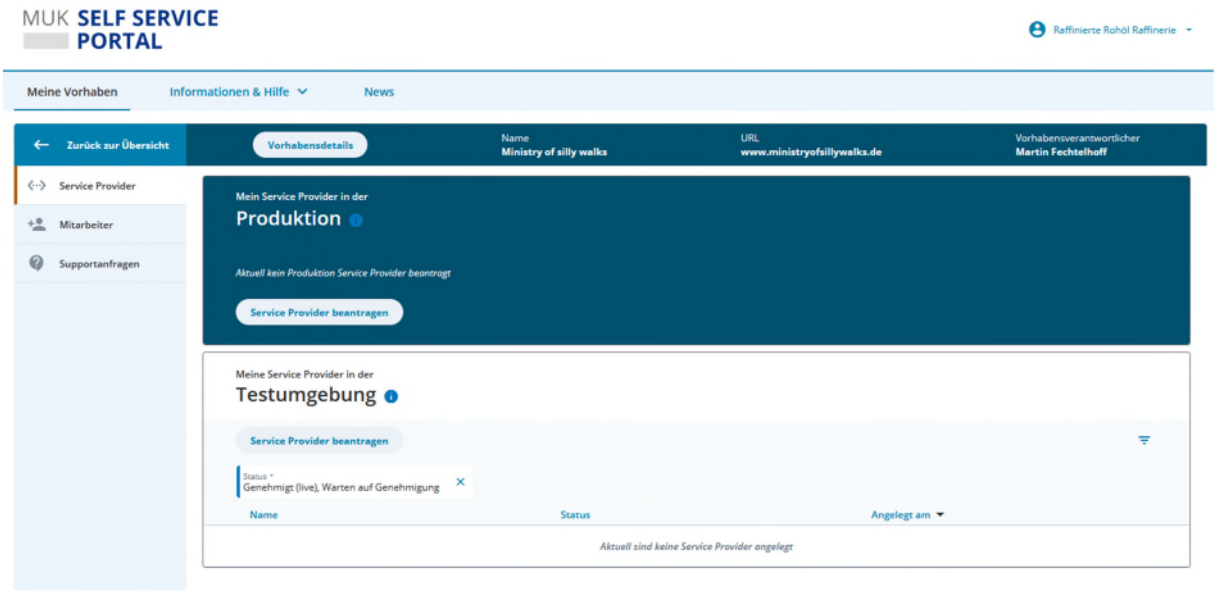
2.4. Schritt 4: Konfiguration Ihres Service Providers

Vor der Konfiguration eines Service Providers melden Sie sich am SSP an und wählen aus der Liste Ihrer Vorhaben das aus, für das Sie einen Service Provider anlegen wollen.



In dem ausgewählten Vorhaben können Sie nun die Konfiguration Ihrer Service Provider (SAML-Endpunkte) vornehmen. Zu Integrationszwecken können Sie diverse Konfigurationen in der Testumgebung anlegen und genau einen Service Provider für das Produktivsystem. Legen Sie erst dann einen Service Provider in Produktion an, wenn Ihre Integration erfolgreich abgeschlossen ist.

Bitte beachten Sie auch, dass Ihre Anlage eines neuen Service Providers nicht sofort wirksam ist. Ihr Antrag wird zuerst überprüft und dann bei Genehmigung wirksam. Dies gilt sowohl für die Service Provider in der Testumgebung als auch in Produktion.



Füllen Sie für Ihren Service Provider das entsprechende Formular aus:

- **Bezeichnung des Service Providers**: Eine durch Sie frei wählbare Bezeichnung zu Ihrer Unterscheidung mehrerer Konfigurationen
- **Entity-ID (SP-ID)**: Muss eine systemweit eindeutige URL sein, mehrere Konfigurationen mit gleicher Entity-ID sind nicht möglich.

  ⚠ Es gibt eine Fehlermeldung, wenn Sie für Ihr Vorhaben eine Entity-ID verwenden, die bereits in einem anderen Vorhaben verwendet wird.

  ⚠ Achten Sie darauf, dass Ihre späteren SAML-Requests die Entity-ID als Issuer enthalten.
- **Datenkranztyp**: Siehe Kapitel "Schritt 3: Auswahl des für Sie relevanten Datenkranzes und der weiteren Konfiguration"
- **Zum Login zugelassene(s) Ordnungsmerkmal(e)**: Siehe Kapitel "Schritt 3: Auswahl des für Sie relevanten Datenkranzes und der weiteren Konfiguration"
- **Zugelassene Zertifikate**: Hinweis: Diese Konfiguration ist nur bei "Service Provider Konfigurationen für die Produktion" verfügbar. Für den produktiven Betrieb sind nur sogenannte Echtzertifikate zugelassen.
  - Echtzertifikate: Diese Auswahl stellt sicher, dass eine Authentisierung nur mit echten Zertifikaten von ELSTER erfolgen darf und somit nur echte

Identitätsdaten übergeben werden. In den meisten Fällen ist daher die Auswahl "Echtzertifikate" ausreichend.

  - Testzertifikate: kommen lediglich zum Einsatz, wenn Sie in Ihrer produktiven Anwendung Smoketests durchführen müssen. Sie können im SSP per Supportanfrage ein Testzertifikat für Ihren Service Provider beantragen.
  - Echt- und Testzertifikate: Bei dieser Auswahl ist eine Authentisierung mit Echt- und Testzertifikaten möglich.
  - Siehe Kapitel "Schritt 3: Auswahl des für Sie relevanten Datenkranzes und der weiteren Konfiguration"

- **Name des Portals:** Bitte geben Sie hier den offiziellen Namen Ihres Portals/Ihrer Anwendung an. Dieser wird beispielsweise verwendet, um Nutzern unter www.mein-unternehmenskonto.de anzuzeigen, in welchen Portalen sie sich zuletzt eingeloggt haben.
- **URL der Startseite Ihres Portals:** Bitte geben Sie hier die offizielle URL der Startseite Ihres Portals/Ihrer Anwendung ein. Diese wird beispielsweise verwendet, um den Nutzer nach dem Registrierungsprozess zurück zu Ihrem Portal zu leiten.
- **Portalbeschreibung bzw. angezeigte Beschreibung**: Dieser Text wird unterhalb Ihres Logos auf der NEZO Login Seite angezeigt, z.B. Name des Dienstes, der verantwortlichen Behörde inkl. Adresse. Ziel dabei ist es, dass die Anwender genau erkennen können, an wen ihre Daten übermittelt werden. Wir empfehlen folgende Aufteilung: - Zeile 1: Name der Anwendung / des Portals - Zeile 2: Verantwortliche Behörde - Zeile 3: Adresse der verantwortlichen Behörde.
- **Portal-Logo**: Ist eine Verwaltungsleistung an die NEZO-Schnittstelle angebunden, so werden Anwender bei Benutzung der ELSTER-Login-GUI auf die entsprechende Webseite weitergeleitet. Um dem Nutzer den Kontext seiner Anfrage zu vermitteln, zeigt ELSTER Ihr Portal-Logo und Anzeigetext zu der/dem aufrufenden Verwaltungsleistung/Serviceportal an. Es sind nur SVG-, PNG- oder JPG-Dateiformate erlaubt und das Logo darf eine Größe von 100 kB und 272 px x 272 px nicht überschreiten.

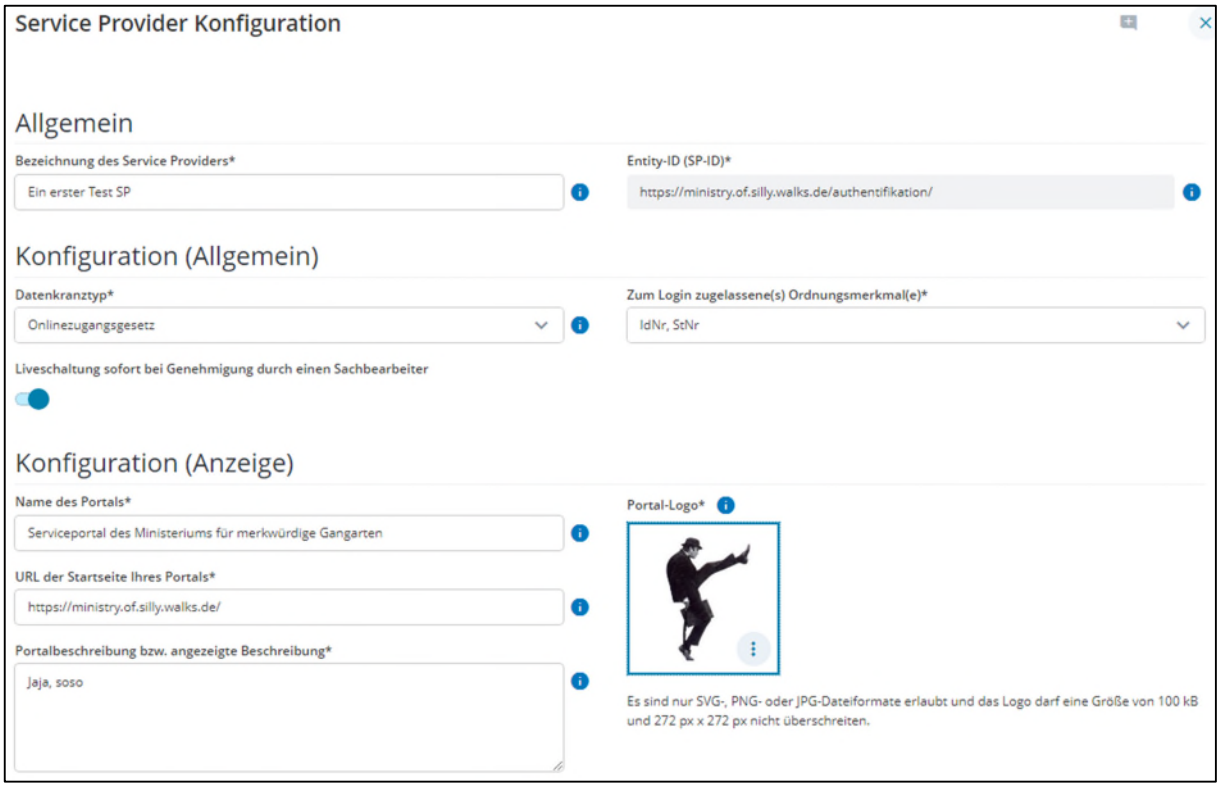


Abbildung 1 Service Provider Konfiguration

Danach ergänzen Sie bitte:

Signaturzertifikat 1: Zertifikat, mit dem ELSTER die Signatur Ihrer SAML-Requests prüfen soll. Das Zertifikat muss gültig sein, die Schlüssellänge muss mindestens 4096 Bit betragen.

⚠ Hier gibt es diverse Fehlermöglichkeiten:

- Das Eingabeformat muss Base64 sein. Oftmals sind Zertifikate jedoch blockweise formatiert und enthalten CR/LF. CR/LF müssen vorher entfernt werden. Ansonsten wird das Abschicken des Antragen nicht möglich sein.
- Das für Zertifikate beliebte PEM-Format ist zwar Base64 codiert, enthält jedoch das zusätzlich Base64 codierte Zertifikat. B64-Decodieren Sie die PEM-Datei, schneiden Sie den B64-Teil zwischen "---Begin Certificate---" und "---End Certificate---" heraus und entfernen aus diesem Teil CR/LF. Tipp: Testen Sie, ob sich der nun ausgeschnittenen Teil parsen lässt. (z.B. Mit https://gchq.github.io/CyberChef/#recipe=Parse_X.509_certificate('Base64')
- Bitte achten Sie auch darauf, dass der in Ihrem System hinterlegte PrivateKey und das im SSP hinterlegte Zertifikat zusammenpassen. Insbesondere auf

Entwicklungsumgebungen kommt es häufig dazu, dass auf der Entwicklungsumgebung andere Schlüssel verwendet werden, als im Zertifikat im SSP hinterlegt.

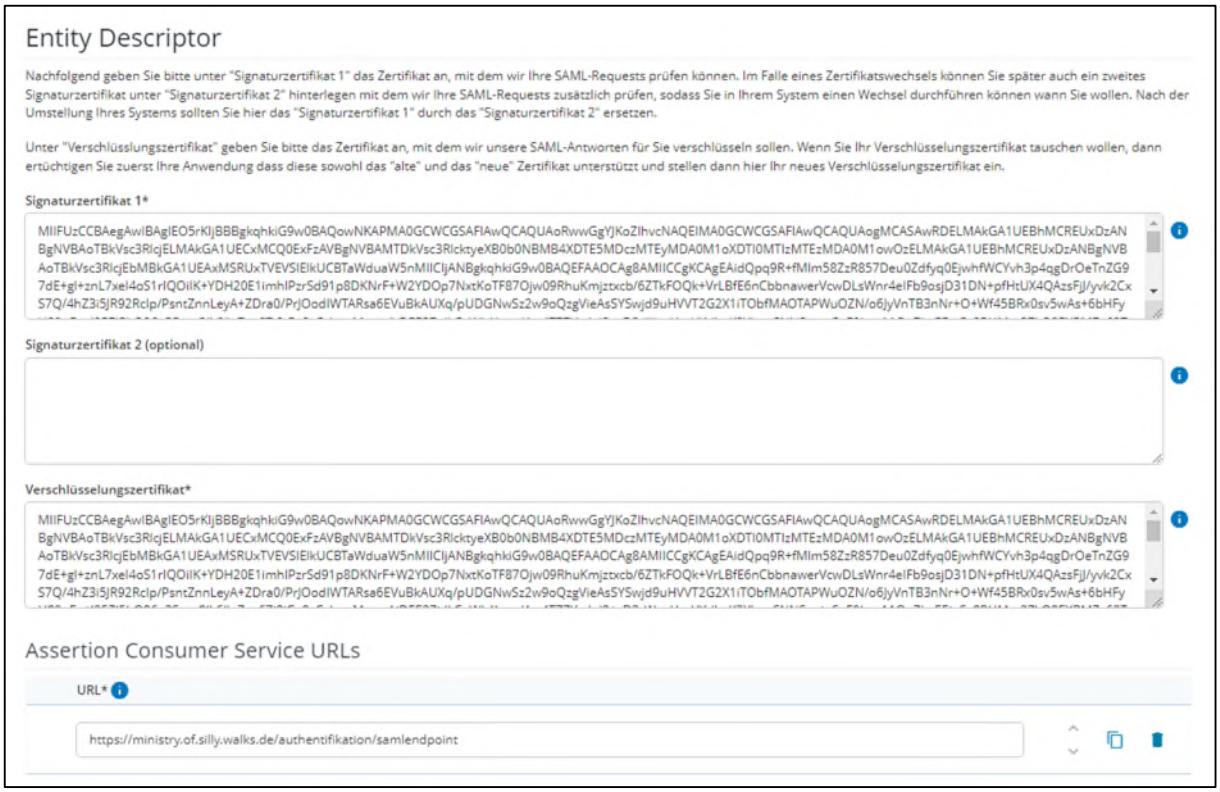
- Wenn der im Zertifikat enthaltene Schlüssel kürzer als 4096 Bit ist kommt es NACH dem Absenden Ihres Antrages zu einem Fehler. Prüfen Sie VOR Antragsstellung die Schlüssellänge. Dafür können Sie einen im Internet verfügbaren Parser für X.509 Zertifikate verwenden.

- **Signaturzertifikat 2 (optional):** Sie können ein zweites Signaturzertifikat zusätzlich angeben. Dies ist für einen reibungslosen Zertifikatswechsel wichtig.
- **Verschlüsselungszertifikat**: Zertifikat mit dem ELSTER die SAML-Antworten an Ihren SP verschlüsseln soll. Das Zertifikat muss gültig sein, die Schlüssellänge muss mindestens 4096 Bit betragen.

  ⚠ Es gibt hier die selben Fehlermöglichkeiten wie beim Signaturzertifikat.
- **Assertion Consumer Service URLs:** Eine oder mehrere URLs, an die eine SAML-Response von ELSTER gesendet werden kann. Muss als URL mit "https://" und ohne Parameter dargestellt werden.

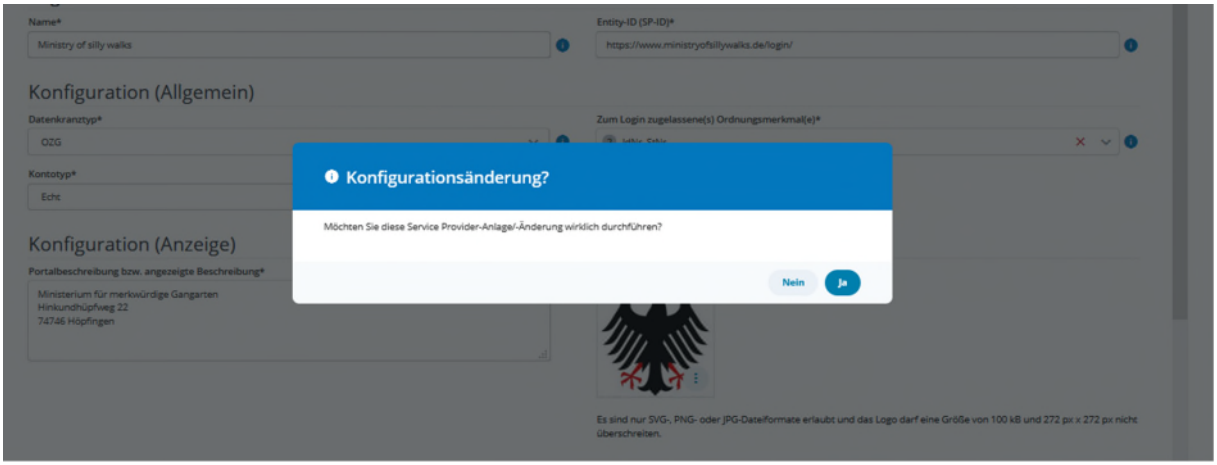
  ⚠ Die Anzahl der möglichen Assertion Consumer Service URLs ist auf 10 begrenzt.

  ⚠ Achten Sie darauf, dass Ihre SAML-Requests eine der ACS-URLs enthält, die Sie hier hinterlegt haben. Andernfalls werden die SAML-Requests mit einem Fehler abgelehnt.
- **Manage Name ID URLs:** Eine oder mehrere URLs, an die ELSTER einen ManageNameID-Request schicken soll. Muss als URI mit "https://" und ohne Parameter dargestellt werden. Wenn hier eine URL angegeben wird, werden Sie über die Löschung bzw. Deaktivierung der ELSTER-Konten Ihrer Benutzer informiert. Wichtig: ManageNameID-Requests werden per SOAP (Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP") an die URL(s) geschickt. Siehe auch Kapitel "Schritt 3: Auswahl des für Sie relevanten Datenkranzes und der weiteren Konfiguration".
- **Single Logout Service URL:** URL, an die ELSTER die SAML-LogoutResponse schickt. Die Angabe dieser URL ist Voraussetzung und gleichzeitig die Beantragung für die Teilnahme am Single-Sign-On Verbund.



Zum Absenden Ihres Antrages drücken Sie bitte die Schaltfläche "Speichern" und bestätigen Sie die Konfigurationsänderung.

Hinweis: Alle Angaben können später noch geändert werden, resultieren jedoch in einem neuen Antrag.



Sobald Ihr Antrag genehmigt wurde, ist Ihre jeweilige Konfiguration aktiv.

2.5. Schritt 5: Kontinuierliche Administration Ihres Vorhabens im SSP

Bitte kümmern Sie sich auch nach dem Produktivgang der NEZO-Schnittstelle um die kontinuierliche Pflege Ihrer Vorhaben im SSP. Nur wenn Sie regelmäßig die Liste der Ansprechpartner aktuell halten, können wir Sie bezüglich geplanter und durchgeführter Änderungen auf unserer Seite informieren.

⚠️ Bitte behalten Sie die Gültigkeit Ihrer Zertifikate im Auge und kümmern Sie sich rechtzeitig um deren Austausch.

3. Einbindung von Mein Unternehmenskonto in die eigene Benutzeroberfläche

3.1. Einheitliches Wording

Bitte beachten Sie folgendes: Uns ist sehr daran gelegen, ein einheitliches Wording in den Webanwendungen der Integrationspartner zu schaffen. Wenn Sie einen Login-Button in Ihre Lösung integrieren, würden wir Sie bitten, einen der folgenden Texte zu verwenden:

- Login mit **Mein UK**
- Login mit **Mein Unternehmenskonto**

Sofern Sie das **Mein Unternehmenskonto**-Logo in seiner aktuellen Fassung einbauen möchten, finden Sie dies im Dokumentenbereich des SSPs.

Wenn sie einen Logout-Button in Ihre Lösung integrieren wollen, bitten wir Sie, einen der folgenden Texte zu verwenden:

Im Fall eines PartialLogouts/SingleLogouts:

- Logout aus dieser Session

Im Fall eines Globalen Logouts:

- Logout aus allen Sessions

3.2. Registrierungsprozess

Sofern der Nutzer noch kein ELSTER-Organisationszertifikat für sich oder seine Organisation beantragt hat, kann dies über **Mein Unternehmenskonto**, die zentrale Administrationsoberfläche für das Unternehmenskonto erfolgen. Der Nutzer gelangt über einen entsprechenden Button in den Registrierungsprozess zur Beantragung eines ELSTER-Zertifikats.

Damit dieser Prozess auch von einem Verwaltungsportal angestoßen werden kann, möchten wir Sie als Integrationspartner gerne auf die Möglichkeit aufmerksam machen, einen entsprechenden "*Hier* **Mein Unternehmenskonto** *beantragen*"- oder "*Hier* ***Mein UK*** *beantragen*"-Button zu hinterlegen und via Link https://www.elster.de/eportal/unternehmerorientiert/registrierungsprozess?entity-id=*Ihre_Entity-Id* zum Registrierungsprozess zu leiten. Der Parameter *entity-id* wird verwendet, um den Nutzer nach dem Registrierungsprozess zurück zu Ihrem Portal zu leiten. *Ihre_Entity-Id* entspricht dem Wert, den Sie in das Feld *Entity-ID (SP-ID)* im *SSP* (unter Service Provider Konfiguration) eingetragen haben. Bitte tragen Sie auch *Name des Portals* und *URL der Startseite des Portals* in die Service Provider Konfiguration ein, damit die Nutzer-Rückführung erfolgen kann.

4. Aufbau der Datenkränze

Je nachdem, ob ELSTER Informationen zu einem persönlichen Zertifikat (IdNr) oder einem Organisationszertifikat (StNr) an den Service Provider weitergibt, unterscheiden sich die übergebenen Daten. Die Datenkranzfelder werden vom ELSTER-IdP innerhalb der SAML-Assertion zurück geliefert. Ein besonderes Element in der SAML-Assertion ist die NameID, die die pseudonymisierte Benutzerkonto-ID enthält. Sie ist eindeutig pro Benutzer und Service Provider. Es handelt sich hier um ein Pflichtelement, das unabhängig vom verwendeten Datenkranztyp vom ELSTER-IdP zurückgeliefert wird. Die NameIDs des ELSTER-IdP sind stets 43 Zeichen lang und werden im Format "ek-<40 Hexadezimalzeichen>" angegeben, "ek" steht hierbei für ELSTER-Konto, bspw. `ek-3bd72e6f67f0ff13e355b5eab2dab0ec3fdffb99`. Die NameID wird als EncryptedID in der SAML-Assertion übertragen. Alle weiteren Datenkranzfelder werden in der SAML-Assertion als Assertion-Attribute übermittelt. Im Folgenden werden zuerst die geteilten (allgemeinen) Datenkranzfelder gelistet, dann in separaten Tabellen die IdNr-spezifischen und die StNr-spezifischen.

4.1. Handelnde Person

Es ist von nun an möglich, den OZG-Datenkranz um die sog. "Handelnde Person" zu erweitern. Relevant wird dieser Erweiterung vor allem für solche Verwaltungsleistungen, die bei der Identifizierung und Authentifizierung neben Informationen zur antragstellenden Organisation zwingend auch verifizierte Daten über die hinter dem Benutzerkonto stehende natürliche Person benötigen. Dieser Anforderung wird dadurch Rechnung getragen, dass ein ELSTER-Organisationszertifikat über eine einmalige Verknüpfung mit einem persönlichen ELSTER-Zertifikat mit Name, Vorname und Geburtsdatum der handelnden Person angereichert werden kann. Falls Sie derartige Verwaltungsleistungen in Ihrem Portfolio haben, bitten wir Sie, den Datenkranz OZG - Version1+hP auszuwählen. Weitere fachliche Informationen finden Sie in den Release Notes vom Release 55 (im Downloadbereich des SSP).

4.2. Datenkränze

Die nachfolgend aufgeführten Datenkränze können Sie für Ihre Service Provider über das SSP auswählen:

Bezeichnung im SSP	Kurzbezeichnung für Zuordnung der nachfolgenden Attributs-Tabellen	Beschreibung
AO - Version1 (Nur mit Vorabgenehmigung durch ELSTER)	AOv1	Service Provider, die ausschließlich Leistungen im Rechtsrahmen der Abgabenordnung (AO) anbieten und damit Teil der Finanzverwaltung sind, können auch weitere Daten (steuerliche IdNr, StNr, UmsatzsteuerID) übermittelt bekommen, die den Rahmen des OZG überschreiten. Bei der Verwendung persönlicher Zertifikate werden im Gegensatz zum OZG-Datenkranz jedoch Geburtsort, -name und -land nicht übertragen.
AO - Version1 zzgl. IBAN (Nur mit Vorabgenehmigung durch ELSTER)	AOv1+IBAN	wie AOv1 zuzüglich aller dem Steuerkontoinhaber zugehörigen Bankverbindungen
AO - Version2 (Nur mit Vorabgenehmigung durch ELSTER)	AOv2	wie AOv1 mit getrennten Attributen an Stelle des Firmennamens bei NatPers mit StNr
OZG - Version1	OZGv1	Service Provider, die Leistungen im Rechtsrahmen des Online Zugangsgesetzes (OZG) anbieten, können den "OZG-Datenkranz" übermittelt bekommen. Hierbei gilt es zu beachten, dass ELSTER für Organisationen nicht in der Lage ist, ALLE im OZG erlaubten Daten (z.B. Namen der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter) zu liefern, da diese in der Finanzverwaltung nicht erfasst werden.
OZG - Version1 zzgl. handelnder Person	OZGv1+hP	wie OZGv1, für Organisationszertifikate zuzüglich der optionalen Attribute zur

Bezeichnung im SSP	Kurzbezeichnung für Zuordnung der nachfolgenden Attributs-Tabellen	Beschreibung
		natürlichen Person, die hinter dem jeweiligen Organisationszertifikat steht.
MIN (keine Identitätsattribute, nur Identifier)	min	Der minimal-Datenkranz (min) ist für Service Provider gedacht, die keine Organisations- und Personenattribute wie Namen, Adresse etc. übermittelt bekommen. Es werden ausschließlich IDs übermittelt, die dazu dienen, Organisationen und Personen auseinanderzuhalten. Eine von ELSTER zurückgesandte SAML-Response hat also die Aussagekraft "Der Benutzer ist bei ELSTER bekannt und wurde erfolgreich authentifiziert". Eine Identifizierung kann im Missbrauchsfall anhand der IDs bei ELSTER vorgenommen werden. Neben der pseudonymisierten Benutzerkonto-ID in der NameID ist ein weiteres wichtiges Attribut zur Identifizierung die DatenuebermittlerPseudonymID, ein eindeutiger Identifier für eine Organisation mit Organisationszertifikat.
ELSTER - Intern Version1 (Nur mit Vorab Genehmigung durch ELSTER)	-	nur für ELSTER/Unternehmenskonto-interne Verwendung.
ELSTER - Intern Version2 (Nur mit Vorab Genehmigung durch ELSTER)	-	nur für ELSTER/Unternehmenskonto-interne Verwendung.

Alle in den nachfolgenden Tabellen mit AO* oder OZG* markierten Attribute, werden bei allen AO/OZG Datenkränzen mitgeliefert.

4.3. Wichtige Hinweise und Spaltenerläuterungen:

- ⚠ **WICHTIG**: Alle Integrationspartner **MÜSSEN** darauf achten, Ihre Implementierung abwärtskompatibel zu gestalten. D.h. es kann vorkommen, dass ohne Ankündigung zusätzliche Attribute in die Datenkränze aufgenommen werden. Alle Integrationspartner sollen von daher Ihre Schnittstellen so gestalten, dass weitere Attribute in den SAML-Responses die Funktionsfähigkeit der angebundenen Dienste nicht gefährden. Somit sollen Stichtagsumstellungen vermieden werden. ⚠

- "na" - bedeutet nicht anwendbar und bezieht sich auf Datenelemente, die im Kontext des jeweiligen Service Providers keine Rolle spielen.
- Pflichtfelder (Spalte *Optional*: Nein): Sollte ELSTER keine Daten zu einem Pflichtfeld ermitteln können, so wird ELSTER den jeweiligen Datenkranz nicht weitergeben, das heißt der SAML-Login wird nicht erfolgreich abgeschlossen. ELSTER zeigt dem Benutzer jeweils einen Hinweis an, an wen er sich wenden kann, um Daten zu korrigieren/nachzutragen.
- Optionale Felder (Spalte *Optional*: Ja): Bei solchen Feldern ist es legitim, wenn keine Daten zum Benutzer vorliegen. In diesem Fall fehlt das jeweilige SAML-Attribut komplett.
- Informative Felder (*Anzeige am IdP*: Ja, *Weitergabe an SP*: Nein): Es kann Daten geben, die dem Benutzer ausschließlich angezeigt werden, aber nicht weitergegeben werden dürfen. Hierzu zählen z.B. die IdNr und die aktuelle StNr, die reine bereichsspezifische Kennziffern sind. Im Bereich der Finanzverwaltung (AO-Datenkranz) dürfen diese weitergegeben werden, im Rahmen des OZG aber explizit nicht. Sie sollen dem Benutzer aber angezeigt werden, um den Kontext der jeweiligen Daten anzuzeigen.
- Technische Felder (*Anzeige am IdP*: Nein, *Weitergabe an SP*: Ja): Nicht optionale Felder (Pflichtfelder), die nicht am ELSTER-IdP angezeigt werden sollen, sind technische Felder, die immer gesetzt sind, z.B. die DatenuebermittlerPseudonymId bei Organisations(StNr)zertifikaten
- Bei Organisationszertifikaten (StNr) gilt folgende Unterscheidung beim PersTyp: natürlichen Personen (NATPERS) ist eine Tätigkeit, nicht-natürlichen (NNATPERS) ist eine Rechtsform zugeordnet (Firmen, Vereine, etc.).

- Alle Anwender einer Organisation bekommen dieselbe DatenuebermittlerPseudonymId. Diese ID wird pseudonymisiert an den Service Provider übergeben (für Organisations(StNr)zertifikate).
- Sofern nicht explizit vom Service Provider erwünscht, sind nur Logins mit echten ELSTER-Konten möglich. Testkonten können nur nach Anforderung in der initialen Anbindung verwendet werden. Siehe dazu 5) Erste Schritte zur Anbindung der NEZO-Schnittstelle.
- Die SAML-NameID (pseudonymisierte Benutzerkonto-ID) fungiert auch als "PostfachHandle" beim Postfach 2.0

4.4. Allgemeine Datenkranzfelder

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
DatenkranzTyp	`ekona:DatenkranzTyp Type`	Nein	Nein	Ja	4	min, AO*, OZG*	StNr (bei einem Organisationszertifikat) oder IdNr (bei einem persönlichen Zertifikat)
Adresse	Das Attribut Adresse ist ein komplexer Datentyp und enthält die nachfolgenden Unterelemente						
Adresse.Typ	`xs:string`	Nein	Nein	Ja	7	AO*, OZG*	INLAND oder AUSLAND
Adresse.Strasse	`xs:string`	~~Nein~~ **Ja (ab 24.07.2024)**	Ja	Ja	72/120	AO*, OZG*	INLAND/AUSLAND **NEU ab Release 60 (24.07.2024)**: Straße optional
Adresse.Hausnummer	`xs:string`	~~Nein~~ **Ja (ab 27.03.2024)**	Ja	Ja	25	AO*, OZG*	Werte 0-9999, mit Zusatz: String, konkateniert "(Hausnr)(einzel-Leerzeichen)(Zusatz)" **NEU ab Release 59 (27.03.2024)**: Hausnummer optional

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
Adresse.PLZ	xs:string	Nein (bei INLAND) Ja (bei AUSLAND)	Ja	Ja	12	AO*, OZG*	Inland: 5-stellig, sonst String der Länge 1-12
Adresse.Ort	xs:string	Nein	Ja	Ja	72	AO*, OZG*	
Adresse.Ortsteil	xs:string	Ja	Ja	Ja	50	AO*, OZG*	
Adresse.Adressergaenzung	xs:string	Ja	Ja	Ja	46	AO*, OZG*	Nicht gesetzt bei Auskunftssperre,
Adresse.Land	xs:string	Nein	Ja	Ja	2	AO*, OZG*	ALPHA-2 Länderkürzel nach ISO 3166-1. DE bei Inlandsadressen. Nicht gesetzt bei Auskunftssperre

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
ElsterVertrauensniveau Identifizierung	`ekona:VertrauensniveauType`	Nein	Nein	Ja	12	AO*, OZG*	"SUBSTANZIELL" für alle, die per Brief oder persönlich Identifiziert wurden. "HOCH" für die mit nPA
ElsterVertrauensniveau Authentifizierung	`ekona:VertrauensniveauType`	Nein	Nein	Ja	12	AO*, OZG*	"SUBSTANZIELL" für alle NEZO Token (Zertifikatsdatei/Sicherheitsstick/Signaturkarten)
IstTestkonto	`xs:boolean`	Nein	Nein	Ja	5	min, AO*, OZG*	Gibt an, ob der Login mit einem ELSTER-Testkonto erfolgte oder nicht. true = Wenn ein ELSTER-Testkonto genutzt wurde false = Wenn ein ELSTER-Echtkonto genutzt wurde **Hinweis**: Sofern nicht explizit vom Service Provider erwünscht, sind nur Logins mit echten ELSTER-Konten möglich. Anzeigemerker für Testzugriff. Liefert neuen Fehlertext "OPERATION_MIT_ECHTZERTIFIKAT_NIC

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
							HT_MOEGLICH: Die Verarbeitung ist für Echt-Zertifikate nicht erlaubt." wenn mit einem Testkonto auf Echtkonten zugegriffen werden sollte.
Bausteinpseudonyme	Für die im Rahmen des Unternehmenskontos beauftragten zusätzlichen Bausteine "OZG-Plus Postfach" und das "Autorisierungsmodul" ist es erforderlich, bei deren Aufruf (Details finden sich in den Handbüchern der jeweiligen Module) entsprechende "Bausteinpseudonyme" mitzugeben. Das Attribut Bausteinpseudonyme ist ein komplexer Datentyp (ekona:BausteinpseudonymeJwtType) und enthält eine Liste von "Pseudonyme"-Unterelementen. Pro im ELSTER-IdP registrierten Baustein ist ein "Pseudonyme"-Element im SAML-Attribut enthalten. Anfänglich werden zwei Bausteine im ELSTER-IdP registriert, künftig aber ggf. noch weitere, wodurch die Datenmenge dieses SAML-Attributs auch erhöht wird.						
Pseudonyme[i].@empfaenger (Attribut)	`xs:anyURI`	Ja	Nein	Ja	1024	OZG*	Der Baustein (als Entity-ID angegeben), für den jeweiligen Pseudonyme angegeben werden.
Pseudonyme[i] (Elementwert)	`xs:string`	Ja	Nein	Ja	keine Begrenz	OZG*	Die Pseudonyme des Nutzers (NameID, bei StNr-Datenkranz auch

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
					ung, siehe Bemerkung		DatenuebermittlerPseudonymId), wie sie beim jeweiligen Baustein bekannte sind (siehe Attribut empfaenger). Die Pseudonyme werden in einem JSON-Web-Token in signierter und verschlüsselter Form dargestellt. Weitere Details finden Sie im weiteren Verlauf dieses Dokumentes im Abschnitt "Bausteinpseudonyme". Die Länge des JSON-Web-Tokens ist prinzipiell nicht beschränkt, bei den aktuelle Signatur- und Verschlüsselungsalgorithmen liegt die Größe eines solchen JWT aktuell bei ca. 1200 Zeichen.
E-Mail-Adresse	`xs:string`	Nein	Ja	Ja	256	OZG*, AOv2	**NEU ab Release 59 (27.03.2024)** Die E-Mail Adresse, die von der Registrierung an im ELSTER-Benutzerkonto hinterlegt wurde. ⚠ Achtung: Die E-Mail-Adresse ist bei ELSTER nicht eindeutig nur einem Account

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
							zugeordnet! Verschiedene Accounts können dieselbe E-Mail Adresse hinterlegt haben.

Hinweis zu den Bausteinpseudonymen: Ausnahmen (Opt-Out) müssen vorab per Supportanfrage im SSP beantragt werden.

4.5. Datenkranz mit persönlichen Zertifikat (IdNr)

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
Anschrift	`ekona:AdresseType`	Nein	Nein	Ja (Nur bei IdNr-Zertifikat)	21	AO*, OZG*	Alle Adressinformationen werden bei persönlichen-Zertifikaten mit IdNr in einem eigenen Datentyp zurückgegeben
IdNr	`xs:string`	Nein	Ja	Ja (nur bei AO)	11	AO*	Steuer IdNr vom BZSt
Name	`xs:string`	Nein	Ja	Ja	72	AO*, OZG*	Der Nachname des Benutzers. *Hinweis:* In sehr seltenen Fällen werden Namensinformationen von den Meldebehörden nur im Vornamen-

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
							Element, manchmal jedoch nur im Nachnamen übermittelt
Vorname	xs:string	Ja	Ja	Ja	72	AO*, AOv2(Optional) OZG*	Hinweis: Es gibt Konstellationen, bei denen kein Vorname vorhanden ist. Dies kann z.B. bei Personen mit südostasiatischem kulturellen Hintergrund der Fall sein.
Geburtsdatum	xs:string	Nein	Ja	Ja	10	AO*, OZG*	Achtung: Gemäß (PassVwV Skt. 4.1.5.3) sind bei teilbekannten Geburtsdaten (Tag unbekannt, oder Tag und Monat unbekannt), die unbekannten Teile mit "XX" zu kennzeichnen.
Geburtsname	xs:string	Ja	Ja	Ja	72	OZG*	
Geburtsort	xs:string	Ja	Ja	Ja	72	OZG*	
Geburtsland	xs:string	Ja	Ja	Ja	2	OZG*	ALPHA-2 Länderkürzel nach ISO 3166-1. siehe Hinweis zu historischen Staaten.

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
AkademischerGrad	xs:string	Ja	Ja	Ja	30	AO*, OZG*	**Für AO* NEU ab Release 59 (27.03.2024)**
Namenszusatz	xs:string	Ja	Ja	Ja	60	AO*, OZG*	**NEU ab Release 59 (27.03.2024)**
Namensvorsatz	xs:string	Ja	Ja	Ja	25	AO*, OZG*	**NEU ab Release 59 (27.03.2024)**

4.5.1. Hinweis zu historischen Staaten im Attribut Geburtsland

Es ist bei einer möglichen Rückumwandlung des 2-stelligen ISO 3166 Ländercodes in einen Ländernamen zu berücksichtigen, dass die 2 stelligen Länderkürzel nach ISO 3166 doppelte Eintragungen für verschiedene ehemalige Staatenaufweisen können.

Beispiel: Die Länder "Serbien und Montenegro" und die "Tschechoslowakei" besitzen beide das Kürzel CS. Es ist dabei jedoch zu berücksichtigen, dass die Länderkürzel bzw. die Staaten mit einem Gültigkeitsdatum versehen sind. Die "Tschechoslowakei" ist mit der "Existenz bis" 31.12.1992 eingetragen und "Serbien und Motenegro" vom 5.2.2003 bis zum 2.6.2006. Eine Ermittlung des Staatsnamens ist bei uneindeutigen Länderkürzeln von daher immer unter Auswertung des Geburtsdatums vorzunehmen.

Die entsprechenden Mapping-Tabellen und die Erläuterung der Systematik ist auf der WebSeite des statistischen Bundesamtes unter dem Begriff "Staats- und Gebietssystematik" zu finden. Eine EXCEL-Datei findet sich (Stand 21.09.2023) unter:

https://www.destatis.de/DE/Methoden/Klassifikationen/Staat-Gebietsystematik/Staatsangehoerigkeitsgebietsschluessel_xls.xlsx?__blob=publicationFile

4.6. Datenkranz mit Organisationszertifikat (StNr)

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
PersTyp	`ekona:PersTypType`	Nein	Nein	Ja (Nur bei Organisationszertifikat)	8	min, AO*, OZG*	Gibt an, ob es sich bei der Identität um eine natürliche "NatPers" oder nicht-natürliche (juristische) Person "NNatPers" handelt. *Bemerkung:* Bei DatenkranzTyp = "IdNr" wird PersTyp NIE zurückgeliefert.
Unternehmensanschrift	`ekona:AdresseType`	Nein	Nein	Ja (Nur bei Organisationszertifikat)	21	AO*, OZG*	Alle Adressinformationen werden bei Organisationszertifikaten mit StNr in einem eigenen Datentyp zurückgegeben
StNr	`xs:string`	Nein	Ja	Ja (nur bei AO)	13	AO*	StNr der Organisation im Bundeseinheitlichen StNr-Format

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
Firmenname	`xs:string`	Nein	Ja	Ja	120	AOv1*, OZG*	Der Name der Organisation. Bei NNatpers ist in der Regel immer ein Firmenname vorhanden. Dieser wird beim Finanzamt (Steuerkonto) geführt. Bei NatPers kann dies auch der konkatenierte Vor- und Nachname des Steuerkontoinhabers sein, wenn kein Betriebsname hinterlegt ist. Beispiele: Betriebsname: "Pferdesport Inh. M.Mustermann" Betriebsname: "Pferdesport" Konkatenierter Vor-/Nachname: "Martin Mustermann"

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
Betriebsname	xs:string	Ja	Ja	Ja	120	AOv2	Für PersTyp NATPERS: Name des Betriebes, sofern im Steuerkonto hinterlegt
Vorname	xs:string	Ja	Ja	Ja	72	AOv2	Für PersTyp NATPERS: Vorname des Betriebsinhabers
Name	xs:string	Nein	Ja	Ja	72	AOv2	Für PersTyp NATPERS: Nachname des Betriebsinhabers
HandelndePerson	Das Attribut HandelndePerson ist ein komplexer Datentyp und enthält die nachfolgenden Unterelemente						
Vorname	xs:string	Ja	Ja	Ja	72	OZGv1+hP, AOv2	Vorname der Person, die das Organisationzertifikat "bedient". Sofern dies durch den Anwender durch zusätzliche Identifizierung mit IdNr-Zertifikat selbst vorgenommen wurde
Nachname	xs:string	Nein	Ja	Ja	72	OZGv1+hP, AOv2	Name der Person, die das Organisationzertifikat "bedient". Sofern dies durch den Anwender

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
							durch zusätzliche Identifizierung mit IdNr-Zertifikat selbst vorgenommen wurde
Geburtsdatum	xs:string	Nein	Ja	Ja	10	OZGv1+hP	Geburtsdatum der Person, die das Organisationzertifikat "bedient". Sofern dies durch den Anwender durch zusätzliche Identifizierung mit IdNr-Zertifikat selbst vorgenommen wurde
AkademischerGrad	xs:string	Ja	Ja	Ja	30	OZGv1+hP	**NEU ab Release 59 (27.03.2024)**
Namenszusatz	xs:string	Ja	Ja	Ja	60	OZGv1+hP	**NEU ab Release 59 (27.03.2024)**
Namensvorsatz	xs:string	Ja	Ja	Ja	25	OZGv1+hP	**NEU ab Release 59 (27.03.2024)**
RechtsformText	xs:string	Nein (bei NNatPers)	Ja	Ja	s. Anhang	AO*, OZG*	Für PersTyp NNATPERS (Werteliste siehe Anhang)

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
Rechtsform	xs:string	Nein (bei NNatPers)	Nein	Ja	3	AO*, OZG*	Für PersTyp NNATPERS (Werteliste siehe Anhang)
TaetigkeitText	xs:string	Nein (bei NatPers)	Ja	Ja	s. Anhang	AO*, OZG*	Für PersTyp NATPERS (Werteliste siehe Anhang)
Taetigkeit	xs:string	Nein (bei NatPers)	Nein	Ja	3	AO*, OZG*	Für PersTyp NATPERS (Werteliste siehe Anhang)
Registernummer	xs:string	Ja	Ja	Ja	11	AO*, OZG*	Kann Daten enthalten, die folgendem regulären Ausdruck entsprechen: "[\d A-Z]{1,11}"
Registerart	xs:string	Ja	Ja	Ja	4	AO*, OZG*	Es können folgende Registerarten zurückgegeben werden: HRA, HRB, VR, GR, PR ab DUEbEL 24.1.1: GnR|GesR
Registergericht	xs:string	Ja	Ja	Ja	128	AO*, OZG*	

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
betriebsGruendungsDatum	xs:string	Ja	Ja	Ja	10	AO*	Das Datum, an dem die steuerliche Tätigkeit des Betriebs begonnen wurde. Entspricht NICHT dem Gründungsdatum lt. Handelsregister
betriebsEndeDatum	xs:string	Ja	Ja	Ja	10	AO*	Datum der Beendigung des Betriebs aus steuerfachlicher Sicht. Nur vorhanden, wenn dieses Datum zeitlich nach dem Gründungsdatum liegt.
UStId	xs:string	Ja	Ja	Ja	15	AO*	Umsatzsteuer IdNr
DatenuebermittlerPseudonymId	xs:string	Nein	Nein	Ja	43	min, AO*, OZG*	für den jeweiligen Service Provider pseudonymisierte ID der Organisation, welcher das ELSTER-Konto angehört. Der Präfix "du-" steht für Datenübermittler.

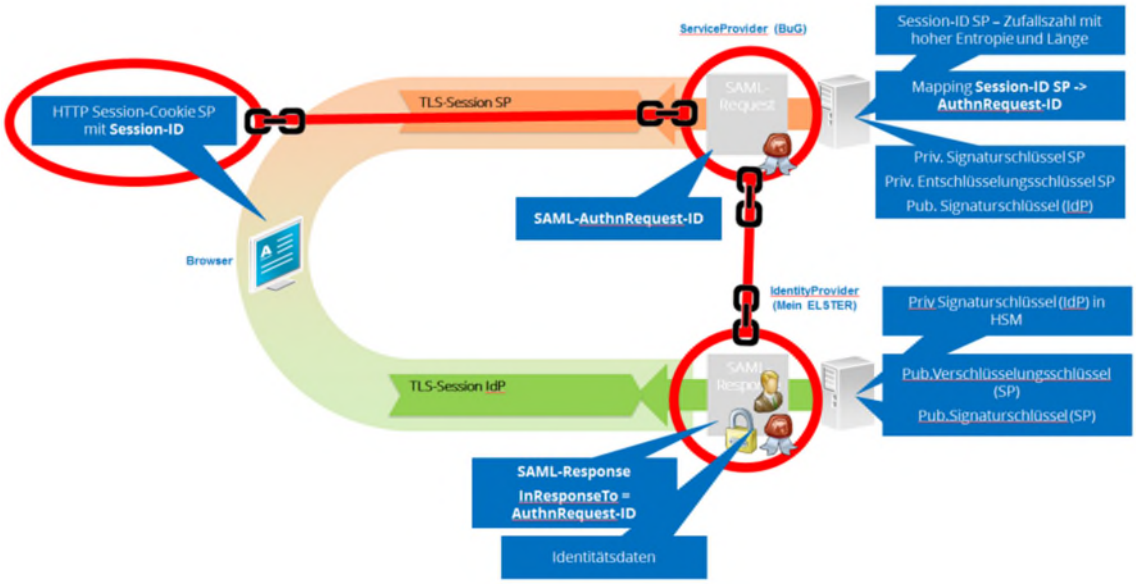
Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
							⚠Hinweis: Es kann mehrere 1000 Accounts/Zertifikate mit unterschiedlichen pseudonymisierte Benutzerkonto-IDs pro Organisation (repräsentiert durch eine DatenuebermittlerPseudonymID) geben.
Bankkonten	Das Attribut Bankkonten ist ein komplexer Datentyp und kann die folgenden Elemente enthalten						
Bankkonto	Das Attribut Bankkonto ist ein komplexer Datentyp und kann die folgenden Elemente enthalten						
IBAN	`xs:string`	Ja	Ja	Ja	34	AOv1+IBAN	International Bank Account Number
BIC	`xs:string`	Ja	Ja	Ja	11	AOv1+IBAN	Business Identifier Code oder auch Bank Identifier Code
Kontoinhaber	`xs:string`	Ja	Ja	Ja	295	AOv1+IBAN	Name des Bankkontoinhabers. Es werden ausschließlich Kontoinformationen zurückgeliefert, bei denen der

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Datenkranz	Bemerkung
							Steuerkontoinhaber (oder bei NatPers sein Ehegatte) Kontoinhaber sind.

5. Schnittstelle Service Provider-ELSTER

5.1. Bindung der Identität an den Sitzungskontext

Die TR-3107-1 des BSI fordert, dass die übertragene Identität an den Sitzungskontext gebunden werden muss. Dies bedeutet unter anderem, dass die Identität eines Anwenders eindeutig einer bestimmten Session und nicht lediglich einem bestimmten Kommunikationsendpunkt zugeordnet werden muss und auch nur dort gültig sein darf. Für Vertrauensniveaus substantiell / hoch muss diese Bindung über geeignete technische / kryptographische Mechanismen erfolgen.
Die folgende Grafik zeigt, wie diese Bindung erreicht wird.



Der Client des Anwenders und die dort vorhandene Session mit dem Service Provider wird repräsentiert durch eine Session-ID, die clientseitig in einem Session-Cookie sicher abgelegt ist. Auf Seiten des Service Providers wird bei Erzeugung des SAML-AuthnRequest die SessionID auf eine AuthnRequest-ID gemappt. Die AuthnRequest-ID ist im, durch den Service Provider signierten, SAML-Request enthalten und damit integritätsgeschützt. Der Request wird an den IdentityProvider weitergeleitet und dort wird die ID integritätsgeschützt in die SAML-Response übernommen (Attribut InResponseTo). Zurück am Service Provider kann dieser anhand Session-ID / AuthnRequest-ID im InResponseTo-Attribut ausschließen, dass die SAML-Response entwendet wurde. Ein Angreifer müsste also in der Lage sein, sowohl die SAML-Response zu stehlen und gleichzeitig auch die Sitzung des Benutzers zu übernehmen, um sich als dieser auszuweisen.
Die bei "Mein ELSTER" nachgewiesene Identität des Anwenders wird in die SAML-Response

eingefügt, integritätsgeschützt und verschlüsselt an den Service Provider zurückgegeben. Die Bindung der Identität an die Benutzersession (Session-ID) des Anwenders ist damit durchgehend kryptografisch abgesichert.

5.2. Allgemeine Festlegungen für die SAML-Kommunikation

Die nachfolgenden Festlegungen sind für den gesamten Kontext dieses Dokumentes gültig:

- Der Begriff SAML bezieht sich immer auf SAML 2.0.
- Alle SAML-Request und –Response-Objekte werden als XML-Dokumente per HTTPS-POST-Requests bzw. in der HTTPS-Response zurück geliefert.
- Die Trust-Stellung zwischen dem Service Provider (SP) und "Mein ELSTER" (IdP) erfolgt durch gegenseitiges Hinterlegen der öffentlichen Schlüssel / Zertifikate des jeweils anderen Kommunikationspartners.
- Es werden ausschließlich TLS Cipher Suites verwendet, die den technischen Richtlinien des BSI entsprechen.
- Es werden ausschließlich kryptographische Verfahren verwendet, die den technischen Richtlinien des BSI entsprechen.
- Die notwendigen kryptographischen Schlüssel werden nach Stand der Technik erzeugt und gespeichert.
- Die grundlegende Sicherheit der Browser-Session wird mit den entsprechenden Mechanismen gewährleistet. Dies sind u.A.:
    - Es wird davon ausgegangen, dass "M 4.394 Session-Management bei Webanwendungen und Web-Services" umgesetzt wird.
    - Es wird davon ausgegangen, dass "M 4.401 Schutz vertraulicher Daten bei Webanwendungen" umgesetzt wird.

Hinweis: Es sind soweit wie möglich alle Festlegungen in Ihrer eigenen Software umzusetzen. Organisatorische Lösungen sollten Sie im Rahmen Ihres eigenen ISM festschreiben.

5.3. SAML-Nachrichten zwischen Service Provider und ELSTER

Die folgenden Abschnitte beschreiben die SAML-Nachrichten, die zwischen Service Provider und dem ELSTER-IdP ausgetauscht werden sollen. Da im SAML-Standard diverse Begriffe definiert werden, soll hier kurz erläutert werden, wie diese Begriffe im NEZO-Kontext zuzuordnen sind.

- *Service Provider (SP) / Relying Party*: In den folgenden Beispielen wird hierzu ein fiktiver Service Provider mit Entity ID "https://demoserviceprovider.de" verwendet.

Dieser fiktive Service Provider bietet seine verschiedenen Dienste unterhalb https://demoserviceprovider.de/nezo/ an (z.B. AssertionConsumerService und weitere).

- *Identity Provider / (IdP) / Asserting Party*: Dies ist der ELSTER Identity Providers (ELSTER-IdP). In den folgenden Beispielen wird hierzu die URL https://www.elster.de (und Unterseiten) verwendet. https://www.elster.de ist auch die Entity-ID des ELSTER-IdP in Produktion. Bitte beachten Sie, dass die E4K-Integrationsumgebung (Sandbox) eine abweichende Entity-ID und auch abweichende Serviceendpunkte verwendet.
- *Subject*: Der Benutzer, der den Service Provider nutzen möchte und sich dazu bei ELSTER authentisiert.
- *Requester*: Der Provider der einen SAML-Request ausgelöst hat (SP oder ELSTER-IdP).
- *Responder*: Der Provider, der auf einen SAML-Request mit einer Response antwortet (SP oder ELSTER-IdP).

Die in den folgenden Abschnitten erwähnten SAML-Nachrichten werden an bestimmte Endpunkte versendet. Es gibt folgende Endpunkte:

Service Provider	Link	Bezeichnung
Service Provider (SP)	https://demoserviceprovider.de/nezo/acs	SST zum Erhalt einer SAML-Response mit SAML-Assertion (AssertionConsumerService)
Service Provider (SP)	https://demoserviceprovider.de/nezo/mni	SST zum Erhalt eines SAML-ManageNameIDRequest
Service Provider (SP)	https://demoserviceprovider.de/nezo/slo	SST zum Erhalt einer SAML-LogoutResponse
ELSTER (IdP)	https://www.elster.de/ekona/sso	SST zum Erhalt eines SAML-AuthnRequest
ELSTER (IdP)	https://www.elster.de/ekona/slo	SST zum Erhalt eines SAML-LogoutRequests

5.3.1. Terminologie der SAML-Datenstruktur-Tabellen

Einige der folgenden Tabellen definieren die Elemente und Attribute der SAML-XML-Nachrichten. Die Hierarchie der XML-Elemente wird über Nummerierungen gekennzeichnet. So stellt z.B. in Tabelle *AuthnRequest-Datenstruktur für NEZO* der <AuthnRequest> in der ersten Zeile einer Tabelle das Root-Element des Dokumentes dar. 2.) <NameIDPolicy> stellt das zweite Unterelement des Root-Elements <AuthnRequest> dar. 2.a) Format ist eines der Attribute des <NameIDPolicy>-Elements. Attribute sind an den fehlenden spitzen Klammern "<>" zu erkennen und werden alphabetisch nummeriert.

5.3.2. Kryptographische Schlüssel für die SAML-Kommunikation, Schlüsselmanagement

Für den sicheren Austausch der SAML-Nachrichten werden diese vom Initiator signiert und und in manchen Fällen partiell verschlüsselt (Bsp. `<EncryptedAssertion>`). Es wird folgendes Schlüsselmaterial verwendet:

- ELSTER-IdP
    - Signieren: IdP-SAML-Sign-Key RSA-4096 mit Algorithmus RSA-PSS
    - Entschlüsseln: IdP-SAML-Enc-Key RSA-4096 mit Algorithmus RSA-OAEP (mit SHA-256 als Digest und als Hash-Funktion für MGF1)
- Service Provider
    - Signieren: Service-Provider-SAML-Sign-Key RSA-4096 mit Algorithmus RSA-PSS
    - Entschlüsseln: Service-Provider-SAML-Enc-Key RSA-4096 mit Algorithmus RSA-OAEP

Es werden Zertifikate genutzt, um die öffentlichen Schlüssel bei der jeweiligen Gegenseite abzulegen. Diese sollten eine Gültigkeitsdauer von 5 Jahren besitzen. Die Schlüssel werden bei den jeweiligen SAML-Nachrichten folgendermaßen genutzt:

Request-Name	**Absender**	**Empfänger**	**beteiligter Signaturschlüssel**	**beteiligter Verschlüsselungsschlüssel**
AuthnRequest	Service Provider	ELSTER-IdP	ServiceProvider-SAML-Sign-Key	-
Response	ELSTER-IdP	Service Provider	IdP-SAML-Sign-Key	ServiceProvider-SAML-Enc-Key

Request-Name	Absender	Empfänger	beteiligter Signaturschlüssel	beteiligter Verschlüsselungsschlüssel
ManageNameIDRequest	ELSTER-IdP	Service Provider	IdP-SAML-Sign-Key	ServiceProvider-SAML-Enc-Key
ManageNameIDResponse	Service Provider	ELSTER-IdP	ServiceProvider-SAML-Sign-Key	-
LogoutRequest	Service Provider	ELSTER-IdP	ServiceProvider-SAML-Sign-Key	-
LogoutResponse	ELSTER-IdP	Service Provider	IdP-SAML-Sign-Key	-

Alle an NEZO beteiligten Parteien müssen in der Lage sein, mehrere Schlüssel der/den jeweiligen Gegenstelle zu verwalten, damit ein Schlüsselaustausch möglich ist ohne die dazu erforderliche betriebliche Tätigkeit ggf. sogar mit einer Downtime synchronisieren zu müssen. Ein Austausch des Signaturschlüssels bedeutet, dass der Schlüssel / das Zertifikat im Voraus erzeugt wird, der Gegenstelle zur Verfügung gestellt wird, um diesen bereits in die Anwendung zu importieren. Erst dann wird der Schlüsselaustausch durchgeführt, so dass die SAML-Nachrichten mit dem neuen Schlüssel signiert werden.
Beim Austausch des Verschlüsselungsschlüssels muss die entschlüsselnde Anwendung den Schlüssel importieren, bevor die Gegenstelle mit diesem Schlüssel verschlüsselt.

5.3.3.XML-Beispiele für Signatur und Verschlüsselung mit RSA-OAEP / RSA-PSS

```
<saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="_1d3391e951e4fd4c1159f62caa25ee28"
Type="http://www.w3.org/2001/04/xmlenc#Element">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes128-
gcm"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <xenc:EncryptedKey Id="_f0512fe8f2b7056a13cf11bd972f8234">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#rsa-
oaep">
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <xenc11:MGF xmlns:xenc11="http://www.w3.org/2009/xmlenc11#"
Algorithm="http://www.w3.org/2009/xmlenc11#mgf1sha256"/>
        </xenc:EncryptionMethod>
        <xenc:CipherData>
          <xenc:CipherValue>T5Yl9OOGyUJXh36q4mTz9+q9C9mQ/noLZzvBCCz........kED/u
Zwq1gQ4=</xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedKey>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>s/ajt7nUWo/V9pl6xa3........RJD+U5/7qYCyhSy+s=</xenc:Ciph
erValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</saml2:EncryptedAssertion>
```

Codeblock 1 Beispiel <EncryptedAssertion> mit RSA-OAEP Verschlüsselung

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https:// demoserviceprovider.de/acs"
                ID="_36a3671945fc31d105d3d58ce18d7764c9418efd"
InResponseTo="_44e290994b4cb1e96f0b7157b868260e"
                IssueInstant="2018-07-10T06:15:56.425Z" Version="2.0">
    <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://www.elster.de</saml2
:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2007/05/xmldsig-
more#sha256-rsa-MGF1"/>
            <ds:Reference URI="#_36a3671945fc31d105d3d58ce18d7764c9418efd">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>V3d+fWJyD9NdP7o16GkzHSbrl0sGVPYWygovKpwSAiM=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>

<ds:SignatureValue>C4IdSURPe0sqXbgU/ttvCPXvNW3D04MrUhsgylPaHg=</ds:SignatureValu
e>
        <ds:KeyInfo>
            <ds:X509Data>

<ds:X509Certificate>MIIEtTCCAp2gAwIBAgIGDQE.......O5xrKhDCSXRdM+6Uavvvmha/fsRlPb
Z2gsSw</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
```

Codeblock 2 Beispiel <Response> mit RSA-PSS Signatur

5.3.4. Zeitsynchronisation der Server (Service Provider und ELSTER)

Die Systemuhren des Service Providers und des Identity-Providers müssen mit einem Time-Server synchronisiert werden, um eine zeitliche Validierung der SAML-Nachrichten realisieren können (SAMLSecure, Skt. 6.4.1 Stolen Assertion).

5.3.5. NEZO-XML-Schema zur Verwendung in SAML-Nachrichten

Folgendes XML-Schema definiert erweiterte Datentypen, die in NEZO-SAML-Nachrichten eingesetzt werden, insbesondere im `AttributeStatement` der SAML-Assertion. Der Namespace des Schemas lautet **"http://www.elster.de/schema/ekona/saml/extensions".**

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ekona="http://www.elster.de/schema/ekona/saml/extensions"
targetNamespace="http://www.elster.de/schema/ekona/saml/extensions"
elementFormDefault="qualified" attributeFormDefault="unqualified" version="1">
    <xs:simpleType name="LaendercodeType">
        <xs:annotation>
            <xs:documentation xml:lang="DE">ISO 3166-1 alpha-2 Ländercode, wie
z.B. DE, FR, AT</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:pattern value="[A-Z]{2}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="VertrauensniveauType">
        <xs:annotation>
            <xs:documentation>Vertrauensniveaus, wie in BSI TR-03107-1 bzw. BSI
TR-03147 vorgegeben.</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:enumeration value="normal"/>
            <xs:enumeration value="substanziell"/>
            <xs:enumeration value="hoch"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="DatenkranzTypType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="StNr"/>
            <xs:enumeration value="IdNr"/>
            <xs:enumeration value="BZStNr"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="PersTypType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="NatPers"/>
            <xs:enumeration value="NNatPers"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="AdresstypType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Inland"/>
            <xs:enumeration value="Ausland"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="DatenquelleType">
```

```
        <xs:restriction base="xs:string">
            <xs:enumeration value="Meldebehoerde"/>
            <xs:enumeration value="Finanzamt"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="AdresseType">
        <xs:sequence>
            <xs:element name="Typ" type="ekona:AdresstypType"/>
            <xs:element name="Strasse" type="xs:string" minOccurs="0"/>
            <xs:element name="Hausnummer" type="xs:string" minOccurs="0"/>
            <xs:element name="PLZ" type="xs:string"/>
            <xs:element name="Ort" type="xs:string"/>
            <xs:element name="Ortsteil" type="xs:string" minOccurs="0"/>
            <xs:element name="Adressergaenzung" type="xs:string" minOccurs="0"/>
            <xs:element name="Land" type="ekona:LaendercodeType"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="Adresse" type="ekona:AdresseType"/>
    <xs:complexType name="BankkontenType">
        <xs:sequence>
            <xs:element name="Bankkonto" type="ekona:BankkontoType"
minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="BankkontoType">
        <xs:sequence>
            <xs:element name="IBAN" type="xs:string"/>
            <xs:element name="BIC" type="xs:string" minOccurs="0"/>
            <xs:element name="Kontoinhaber" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="HandelndePerson">
        <xs:sequence>
            <xs:element name="Vorname" type="xs:string" minOccurs="0"/>
            <xs:element name="Nachname" type="xs:string"/>
            <xs:element name="Namensvorsatz" type="xs:string" minOccurs="0"/>
            <xs:element name="Namenszusatz" type="xs:string" minOccurs="0"/>
            <xs:element name="AkademischerGrad" type="xs:string" minOccurs="0"/>
            <xs:element name="Geburtsdatum" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="BausteinpseudonymeType">
        <xs:sequence>
            <xs:element name="Pseudonyme" type="ekona:BausteinpseudonymeJwtType"
minOccurs="0" maxOccurs="unbounded"/>
```

```
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="BausteinpseudonymeJwtType">
        <xs:simpleContent>
            <xs:extension base="xs:string">
                <xs:attribute name="empfaenger" use="required"
type="xs:anyURI"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
</xs:schema>
```

Codeblock 3 Beispiel XML-Schema

5.3.6.SAML-AuthnRequest

Der Service Provider muss einen AuthnRequest gemäß folgender Tabelle erzeugen, um eine ELSTER-Authentifizierung zu initiieren:

<AuthnRequest>	Bezeichnung
a) Version	Legt die SAML-Version fest. Muss den Wert "2.0" enthalten.
b) ID	Zufällig gewählte ID, s. (SAMLCore, Z. 1467 + Skt. 1.3.4)
c) IssueInstant	Erstellungszeitpunkt des SAML-AuthnRequest (aktuelle Systemzeit synchronisiert mit Time Server)
d) Destination	"https://www.elster.de/ekona/sso", die URL für den Empfang des SAML-AuthnRequest
e) ProtocolBinding	Legt das Protocol Binding für die <Response> fest. Zu verwendender Wert: "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" für POST Binding. Andere Bindings werden bei ELSTER nicht unterstützt, insb. Redirect Binding, s. auch (SAMLProf, Z. 424).
f) ForceAuthn	Muss Wert "true" haben, wenn SingleSign-On nicht erwünscht ist, muss Wert "false" haben, wenn SingleSign-On erwünscht ist. Erzwingt damit stets eine neue Authentisierung bei ELSTER, s. (SAMLCore, Z. 2042)

g) AssertionConsumerServiceURL	"https://demoserviceprovider.de/nezo/acs", die URL für den Empfang von SAML-Assertions
1) <Issuer>	"https://demoserviceprovider.de" entity-ID des Service Providers
1.a) Format	Kann weggelassen werden, oder es muss "urn:oasis:names:tc:SAML:2.0:nameid-format:entity" verwendet werden (SAMLProfiles, Z. 515).
2.) <NameIDPolicy>	Optional. Wenn nicht gesetzt, verwendet der ELSTER-IdP implizit das NameID-Format "persistent". Wenn gesetzt, dann müssen die Werte aber gemäß 2.a) und 2.b) gesetzt, da der ELSTER-IdP derzeit *ausschließlich* das das Format "persistent" unterstützt.
2.a) AllowCreate	"true", so dass ELSTER für den Benutzer einen neuen Pseudonym-Identifier festlegt, s. (SAMLCore, Z. 2143) (SAMLProfiles, Z. 521)
2.b) Format	"urn:oasis:names:tc:SAML:2.0:nameid-format:persistent", hiermit legt ELSTER eine Service-Provider-spezifisches Pseudonym für den Benutzer fest. Siehe (SAMLCore, Skt. 8.3.7), (SAMLTechOverview Skt. 5.4.3)

5.3.6.1. Beispiel-AuthnRequest-XML

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"

AssertionConsumerServiceURL="https://demoserviceprovider.de/nezo/acs"
                    Destination="https://www.elster.de/ekona/sso"
                    ForceAuthn="true"
                    ID="_3d203a2485e531505e83ec19e0cb6cc1232ad9d4"
                    IssueInstant="2023-02-17T10:35:29.418Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST"
                    Version="2.0">
    <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:de:elster:esig:demo-
service-provider:nezo</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2007/05/xmldsig-
more#sha256-rsa-MGF1"/>
            <ds:Reference URI="#_0f6ab1c2041160ce0ebe313d5315d58c6098ef55">
                <ds:Transforms>
                    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>KQNjNjDAEW+c/Ra8va2CPJlbbvZDaDDgK8YGmH1VSkM=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>t9zTBexpag......</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>

<ds:X509Certificate>MIIFPDCCAyQCCQCN9m5747lR1TANBgkq........</ds:X509Certificate
>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <saml2p:NameIDPolicy AllowCreate="true"/>
</saml2p:AuthnRequest>
```

Codeblock 4 Beispiel- AuthnRequest (unverschlüsselt, mit abgekürzten Signaturinhalten)

5.3.6.2. Prüfung des SAML-AuthnRequest durch den ELSTER-IdP

Wenn ELSTER den AuthnRequest über den Endpoint https://www.elster.de/ekona/sso (SAML-Endpunkt des ELSTER-Produktivsystems) im Rahmen des Authentifizierungsprozesses erhält, so prüft der ELSTER-IdP folgende Eigenschaften:

- Der AuthnRequest muss erfolgreich geparst werden können und schema-valide sein
- Der SAML-AuthnRequest muss signiert sein, nur folgende Signatur-Algorithmen werden bei ELSTER unterstützt: `sha256-rsa-MGF1`
- Der Service Provider (identifiziert durch den `<Issuer>`) muss bei ELSTER bekannt sein und unterstützt werden
- Die vom Service Provider vorgegebene `<AssertionConsumerServiceURL>` muss mit der im ELSTER-IdP hinterlegten URL des Service Providers übereinstimmen (SAMLProfiles, Z. 533).
- Das `<Issuer>` -Format-Attribut muss fehlen oder den Wert "`urn:oasis:names:tc:SAML:2.0:nameid-format:entity`" enthalten (SAMLProfiles, Z. 515).
- Das in der Signatur verwendete Zertifikat muss mit einem der im ELSTER-IdP zum Service Provider hinterlegten Signatur-Zertifikate übereinstimmen, die Signatur muss erfolgreich geprüft werden.
- Die `<NameIDPolicy>`-Vorgaben aus Tabelle "AuthnRequest-Datenstruktur für NEZO" müssen erfüllt, s. auch (SAMLProfiles, Z. 521)
- `ProtocolBinding` muss den Wert `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST` enthalten.

Ist eine dieser Eigenschaften nicht erfüllt, dann zeigt ELSTER dem Nutzer einen Fehler an ohne eine Umleitung zum Service Provider durchzuführen. *Anmerkung*: Eine Umleitung zurück zum Service Provider ist nicht möglich, da die Zielseite nicht aus dem AuthnRequest ermittelt werden kann bzw. die AssertionConsumerURL (die Ziel-URL der SAML-Response) nicht von ELSTER-IdP unterstützt wird.
Sind die bisherigen Prüfungen erfolgreich, so wird der erfolgreich authentifizierte AuthnRequest weiter geprüft.
Wenn der AuthnRequest eine von "2.0" abweichende Version enthält, dann erzeugt ELSTER eine SAML-Response mit Fehler TopLevelCode VersionMismatch + 2ndLevelCode RequestVersionTooHigh (wenn Version > 2.0) / RequestVersionTooLow (wenn Version < 2.0)
.

Wenn eine der folgenden Bedingungen nicht erfüllt ist, dann erzeugt ELSTER eine SAML-Response mit Fehler TopLevelCode Requester + 2ndLevelCode AuthnFailed:

- Der Erstellungszeitpunkt des AuthnRequest (IssueInstant) darf nicht vor mehr als 5 Minuten liegen
- Falls vom Service Provider ein RelayState übermittelt wurde, dann darf dieser nicht länger als 80 Bytes sein (SAMLProfiles, Skt. 3.4.3 RelayState)

5.3.7.SAML-Response

Nach erfolgreicher Authentifizierung, vorliegender Freischaltung des ELSTER-Benutzerkontos für außersteuerliche Zwecke und Bestätigung der Datenweitergabe an Service Provider muss der ELSTER-IdP eine SAML-Response gemäß folgender Tabelle erzeugen:

XML-Element / -Attribut	Beschreibung
<Response>	
a) Version	Legt die SAML-Version fest. Muss den Wert "2.0" enthalten.
b) ID	Zufällig gewählte ID, s. (SAMLCore, Z. 1539 + Skt. 1.3.4)
c) InResponseTo	Referenz zum AuthnRequest, muss mit der ID des AuthnRequest übereinstimmen
d) IssueInstant	Erstellungszeitpunkt der SAML-Response
e) Destination	"https://demoserviceprovider.de/nezo/acs", die URL für den Empfang des SAML-AuthnRequest. Entspricht der AssertionConsumerServiceURL des AuthnRequest
1) <Issuer>	"https://www.elster.de"
1.a) Format	Kann weggelassen werden, oder es muss "urn:oasis:names:tc:SAML:2.0:nameid-format:entity" verwendet werden (SAMLProfiles, Z. 541).
2.) <Status>	Status der Verarbeitung des dazugehörigen Request (AuthnRequest)
2.1) <StatusCode>	TopLevelCode (SAMLCore, Z. 1634)
2.1.a) Value	Statuscode-Wert
2.1.1) <StatusCode>	Optionaler 2nLevelCode (SAMLCore, Z. 1646)

XML-Element / -Attribut	Beschreibung
2.1.1a) Value	Statuscode-Wert
3.) <EncryptedAssertion> (<Assertion>)	<EncryptedAssertion> ist die mit dem Service-Provider-Public-Key verschlüsselte <Assertion>. Die im folgenden beschriebenen Unterelemente beziehen sich auf die entschlüsselte <Assertion>
3.1.a) Version	Identisch zur SAML-Version. Muss den Wert "2.0" enthalten.
3.1.b) ID	Zufällig gewählte ID, s. (SAMLCore, Z. 1539 + Skt. 1.3.4)
3.1.c) IssueInstant	Erstellungszeitpunkt der SAML-Assertion (aktuelle Systemzeit synchronisiert mit Time Server)
3.1.1) <Issuer>	identisch zu 1)
3.1.2) <Subject>	Enthält Informationen über den authentifizierten Benutzer
3.1.2.1) <NameID>	Der Name der Identität. Da Format "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" verwendet wird, werden hier "Pseudonym Identifiers" vergeben (SAMLTechOverview, Skt. 5.4.3). Der in diesem Element enthaltene Wert ist bei NEZO ein 40-Zeichen-Hexwert mit Präfix "ek-" (steht für ELSTER-Konto, Bsp: ek-92429d82a41e930486c6de5ebda9602d55c39986), der das ELSTER-Konto im Kontext des Service Providers eindeutig identifiziert. Die NameID enhält die für jeden ELSTER-Benutzer eindeutige, pseudonymisierte Benutzerkonto-ID, die gleichzeitig als Postfachhandle für das Postfach2.0 fungiert.
3.1.2.1.a) Format	identisch zu <AuthnRequest> 2.b)
3.1.2.2) <SubjectConfirmation>	
3.1.2.2.a) Method	Hat den Wert "urn:oasis:names:tc:SAML:2.0:cm:bearer", s. (SAMLProfiles, Skt. 3.3), (SAMLProfiles, Z. 549)
3.1.2.2.1) <SubjectConfirmationData>	

XML-Element / -Attribut	Beschreibung
3.1.2.2.1.a) InResponseTo	Referenz zum AuthnRequest, muss mit der ID des AuthnRequest übereinstimmen - wie c)
3.1.2.2.1.b) NotOnOrAfter	Zeitpunkt, bis zu dem diese SAML- Response beim Ziel e) (Destination) eingereicht. ELSTER setzt für diesen Wert den aktuellen Systemzeitpunkt + 5 Minuten (SAMLProfiles, Z. 556). Der Zeitpunkt sollte nicht das Zeitfenster aus <Conditions> überschreiten (SAMLCore, Z. 756).
3.1.2.2.1.c) Recipient	muss identisch zu <AuthnRequest> g) sein (AssertionConsumerServiceURL)
3.1.3) <Conditions>	Schränkt die Gültigkeit dieser Assertion ein
3.1.3.a) NotOnOrAfter	Zeitpunkt, bis zu dem diese Assertion gültig ist. Wird identisch zu 3.1.2.2.1.b) gewählt.
3.1.3.1) <AudienceRestriction>	Gibt an, für welchen Empfängerkreis die Assertion gilt.
3.1.3.1.1) <Audience>	Muss identisch zum Service Provider-Identifier in <AuthnRequest> 1) (<Issuer>) sein (SAMLProfiles Z. 566).
3.1.4) <AuthnStatement>	Enthält Informationen über die Art und Weise, mit der der Identity-Provider den Benutzer authentifiziert hat.
3.1.4.a) AuhtnInstant	Authentifizierungszeitpunkt
3.1.4.b) SessionIndex	Ein Session-Index, der für das SingleLogout-Profil verwendet wird
3.1.4.2 <AuthnContext>	Kontext der erfolgten Authentifizierung
3.1.4.2.1 <AuthnContextClassRef>	Die ELSTER-Authentisierung erfolgt derzeit stets zertifikatsbasiert, daher enthält dieses Element stets den Wert "urn:oasis:names:tc:SAML:2.0:ac:classes:X509" (SAMLAuthnCxt Skt. 3.4.11)
3.1.5) <AttributeStatement>	Enthält eine Liste von <Attribute>-Elementen, die Informationen über das "Subject", also den sich authentisierenden Benutzer liefert.

XML-Element / -Attribut	Beschreibung
3.1.5.1) <Attribute> (0..*)	Die Liste von Attributen. Abhängig vom Ordnungsmerkmal des Benutzers (IdNr, StNr) werden unterschiedliche Attribute der natürlichen Person bzw. des Unternehmens zurückgeliefert. Die zurückgeliefern Attribute sind in den drei Tabellen des Unterabschnitts "Aufbau des Datenkranzes..." zu sehen

5.3.7.1. NEZO-Attribute eines SAML-Response-AttributeStatement

Ein Attribut wird stets durch dessen *Name* (im folgenden Beispiel: "Ordnungsmerkmal") festgelegt. Dessen Value hat einen XML-Datentyp (hier ein simpler Datentyp "xs:string"). Das <AttributeValue> enthält dann schließlich den Wert des Attributs (hier: IdNr).

```
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ...>
   ....
 <saml2:Attribute Name="Ordnungsmerkmal">
    <saml2:AttributeValue xsi:type="xs:string">IdNr</saml2:AttributeValue>
  </saml2:Attribute>
  ....
</saml2p:Response>
```

Codeblock 5 Beispiel- NEZO-Attribute eines SAML-Response-AttributeStatement

Häufig wird der simple Datentyp "string" aus dem xs-Namespace "http://www.w3.org/2001/XMLSchema" verwendet. In manchen Fällen werden jedoch ELSTER-/NEZO-spezifische Datentypen verwendet. Hierzu wird das in vorigen Abschnitten erwähnte EKONA-SAML-XML-Schema mit der Namespacedefinition xmlns:ekona="http://www.elster.de/schema/ekona/saml/extensions" verwendet. Alle Attribute werden in NEZO mit ihrem Vertrauensniveau markiert. Dies wird im Attribut ElsterVertrauensniveauIdentifizierung abgebildet.

5.3.7.2. Beispiel-SAML-Response

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                 xmlns:xs="http://www.w3.org/2001/XMLSchema"
                 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                 xmlns:ekona="http://www.elster.de/schema/ekona/saml/extensions"
                 Version="2.0"
                 ID="_8fbb95c8037fa13ced0b2ae2943a38f5"
                 InResponseTo="_44e290994b4cb1e96f0b7157b868260e"
                 Destination="https://demoserviceprovider.de/nezo/acs"
                 IssueInstant="2018-09-26T14:54:32.050Z">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <!-- Signaturinhalte siehe Codeblock "<Response> mit RSA-PSS Signatur" -
->
    </ds:Signature>
    <saml2:Issuer>https://www.elster.de</saml2:Issuer>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </saml2p:Status>
    <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                     Version="2.0"
                     ID="_637f10a0ad5fb9a1e902c4af34349d6b"
                     IssueInstant="2018-09-26T14:54:32.043Z">
        <saml2:Issuer>https://www.elster.de</saml2:Issuer>
        <saml2:Subject>
            <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">ek-92429d82a41e930486c6de5ebda9602d55c39986
            </saml2:NameID>
            <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml2:SubjectConfirmationData
InResponseTo="_44e290994b4cb1e96f0b7157b868260e"
                                               NotOnOrAfter="2018-09-
26T14:55:32.045Z"

Recipient="https://demoserviceprovider.de/nezo/acs"/>
            </saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions NotOnOrAfter="2018-09-26T14:55:32.043Z">
            <saml2:AudienceRestriction>
                <saml2:Audience>https://demoserviceprovider.de</saml2:Audience>
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement AuthnInstant="2018-09-26T14:54:32.043Z">
            <saml2:AuthnContext>
```

```
<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</saml2:AuthnContextClassRef>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <saml2:Attribute Name="DatenuebermittlerPseudonymId">
                <saml2:AttributeValue xsi:type="xs:string">du-986b2b54ab89cf4ed674ad8c3126b966b54d4872</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="ElsterVertrauensniveauIdentifizierung">
                <saml2:AttributeValue xsi:type="ekona:VertrauensniveauType">substanziell</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="ElsterVertrauensniveauAuthentifizierung">
                <saml2:AttributeValue xsi:type="ekona:VertrauensniveauType">substanziell</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="IstTestkonto">
                <saml2:AttributeValue xsi:type="xs:boolean">true</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="PersTyp">
                <saml2:AttributeValue xsi:type="ekona:PersTypType">NNatPers</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="Name">
                <saml2:AttributeValue xsi:type="xs:string">Musterfirma GmbH</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="Unternehmensanschrift">
                <saml2:AttributeValue xsi:type="ekona:AdresseType">
                    <ekona:Typ>Inland</ekona:Typ>
                    <ekona:Strasse>Musterstraße</ekona:Strasse>
                    <ekona:Hausnummer>1</ekona:Hausnummer>
                    <ekona:PLZ>11011</ekona:PLZ>
                    <ekona:Ort>Berlin</ekona:Ort>
                    <ekona:Land>DE</ekona:Land>
                </saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="Rechtsform">
                <saml2:AttributeValue xsi:type="xs:string">140</saml2:AttributeValue>
            </saml2:Attribute>
```

```
            <saml2:Attribute Name="Registernummer">
                <saml2:AttributeValue
xsi:type="xs:string">1234</saml2:AttributeValue>
            </saml2:Attribute>
            <saml2:Attribute Name="Registerart">
                <saml2:AttributeValue
xsi:type="xs:string">HRA</saml2:AttributeValue>
            </saml2:Attribute>
            <!-- ... usw. -->
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

Codeblock 6 Beispiel SAML-Response von ELSTER (unverschlüsselt, ohne Signaturinhalte)

5.3.7.3. Prüfung der SAML-Response durch Service Provider

Wenn der Service Provider die Response nach erfolgreicher Authentifizierung und Datenfreigabe bei ELSTER erhält, so **muss** diese unmittelbar überprüft werden. Wenn die Response nicht erfolgreich geparst werden kann (da z.B. nicht schema-valide) , dann zeigt der Service Provider dem Benutzer einen Fehler an. Darüber hinaus werden weitere Eigenschaften der SAML-Response sichergestellt, tritt hier ein Fehler auf so zeigt der Service Provider dem Benutzer einen Fehler an:

- Die SAML-Response **muss** signiert sein.
- Das in der Signatur verwendete Zertifikat **muss** mit dem offiziellen ELSTER-IdP-Zertifikat übereinstimmen, die Signatur muss erfolgreich geprüft werden.
- Der TopLevelStatusCode **muss** den Wert "urn:oasis:names:tc:SAML:2.0:status:Success" haben.
- Eine Assertion mit einem <AuthnStatement> und <SubjectConfirmation> mit Method-Attribut "urn:oasis:names:tc:SAML:2.0:cm:bearer" **muss** vorhanden sein (SAMLProfiles Z. 549)
- Der <Issuer> der <Response> **muss** den Wert "https://www.elster.de" enthalten (SAMLProfiles Z. 541), ebenso der <Issuer> der <Assertion>
- <SubjectConfirmationData>-Prüfungen:
    - Das Recipient-Attribut in <SubjectConfirmationData> **muss** mit der Assertion-Consumer-Service-URL des Service Providers ("https://demoserviceprovider.de/nezo/acs") übereinstimmen (SAMLProfiles Z.576). Ebenso **muss** diese URL mit dem Destination-Attribut der <Response> übereinstimmen (SAMLCore Z.1557).

- Das NotOnOrAfter-Attribut in <SubjectConfirmationData> **darf nicht abgelaufen sein** (SAMLProfiles Z.578)
- Das InResponseTo-Attribut in<SubjectConfirmationData> **muss** mit der AuthnRequest-ID übereinstimmen, die der Service Provider in der Session vorgemerkt hat. (SAMLProfiles Z.580)
  - *Bemerkung*: Dies setzt voraus, dass der Service Provider bei der Erstellung des AuthnRequest die ID in der Session hinterlegt, damit die später erhaltene SAML-Response gegen diese ID geprüft werden kann. Durch das Abspeichern der AuthnRequest-ID in den Session-Daten wird insbesondere sichergestellt, dass ein Angreifer mit gestohlener SAML-Response nicht in der Lage ist diese am Service Provider zu nutzen, da der Angreifer die SAML-Response in einer anderen Session übermittelt (vorausgesetzt er hat nicht auch die Session gestohlen).
  - *Bemerkung 2*: Dieses Verhalten stellt sicher, dass die Identitätsdaten gemäß (TR-03107-1, Skt. 5.2.3) an den Sitzungskontext gebunden werden, s. auch Bindung der Identität an den Sitzungskontext.
- Die Response **muss** in der bei der Erstellung des AuthnRequest verwendeten Session übermittelt werden.

- <Conditions>-Prüfungen:
  - Das NotOnOrAfter-Attribut in <Conditions> **darf nicht abgelaufen sein** (SAMLProfiles Z.568)
  - Die Assertion mit Bearer-Subject muss eine <AudienceRestriction> enthalten, und die darin enthaltene <Audience> **muss** der ID des Service Provider entsprechen ("https://demoserviceprovider.de")
- <AuthnStatement>-Prüfungen:
  - keine, diese Sektion hat im NEZO-Kontext eher informativen Charakter.

5.3.8. ManageNameIDRequest

Möchte ein Benutzer die Freischaltung des ELSTER-Benutzerkontos für außersteuerliche Zwecke wieder zurückziehen oder löscht er sein ELSTER-Benutzerkonto, so kann der ELSTER-IdP den Service Provider über diesen Widerruf informieren, damit der Service Provider die Verknüpfung zu ELSTER aufhebt.
Bei erneuter Freischaltung eines ELSTER-Benutzerkontos für außersteuerliche Zwecke vergibt der ELSTER-IdP weiterhin die alte pseudonymisierte NameID an die Service Provider, mit denen der Benutzer in der Vergangenheit Kontakt hatte.

Sofern ein Service Provider kein eigenes Konto führt bzw. die ELSTER-Identitätsdaten nicht dauerhaft persistiert, muss ELSTER diesen auch nicht über den Widerruf informieren. Bitte geben Sie in diesem Fall auch keinen ManageNameIDServer bei der Service Provider Konfiguration im SSP an, siehe auch Punkt "Persistieren Sie ELSTER-Identitätsdaten?".

⚠ **Hinweis #1**: Wenn Sie auf Seite Ihres Service Providers ein eigenes Benutzerkonto führen, das nur abhängig von der ELSTER-Authentifizierung ist, dann können Sie einen ManageNameIDService betreiben. ELSTER informiert Ihren Service Provider per ManageNameIDRequest, wenn Sie das Konto auf Ihrer Seite entsprechend löschen/deaktivieren können. Dies gilt auch für den Fall, wenn Sie z.B. abhängig von der gewählten ELSTER Authentifizierung Formulardaten anlegen und so persistieren, dass ein ELSTER Benutzer nach erneutem Login diese Daten erneut abrufen kann.

⚠ **Hinweis #2:** Im Falle des ManageNameIDRequest ist es der ELSTER-IdP, der die Verbindung zum Service Provider aufbaut. Aus diesem Grund werden ManageNameIDRequest per SOAP (`Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"`) vom ELSTER-IdP an den Service Provider geschickt.

Im Abschnitt "Troubleshooting" gibt es eine Anleitung zum Testen des MangeNameId-Services.

XML-Element / -Attribut	Beschreibung
<ManageNameIDRequest>	
a) Version	Legt die SAML-Version fest. Muss den Wert "2.0" enthalten.
b) ID	Zufällig gewählte ID, s. (SAMLCore, Z. 1467 + Skt. 1.3.4)
c) IssueInstant	Erstellungszeitpunkt des SAML-Request
d) Destination	"https://demoserviceprovider.de/nezo/mni", die URL für den Empfang des SAML-Request
1) <Issuer>	"https://www.elster.de"
2) <EncryptedID> / <NameID>	Lediglich die ID der Identität ist im ManageNameIDRequest verschlüsselt. Nach Entschlüsselung liegen die Informationen über die Identität im <NameID>-Element.

XML-Element / -Attribut	Beschreibung
2.a) Format	identisch zu <AuthnRequest> 2.b): "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
2.b) NameQualifier	Die Entity-ID des Identity-Providers, der die NameID erzeugt hat (s. SAMLCore Z. 2493).
2.c) SPNameQualifier	Die Entity-ID des Service Providers, in dessen Kontext die NameID gültig ist (s. SAMLCore Z. 2493).
3) <Terminate>	Information, dass das Konto gelöscht/deaktiviert werden kann. (Hinweis: Das Element hat einen leeren Inhalt.)

5.3.8.1. Beispiel-ManageNameIDRequest-XML

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:ManageNameIDRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                            Version="2.0"
                            ID="_e8b0dd41938018a871a13dd92bed4614"
                            IssueInstant="2018-05-26T14:54:31.812Z"

Destination="https://demoserviceprovider.de/nezo/mni">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <!-- Signaturinhalte -->
    </ds:Signature>
    <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://www.elster.de</saml2
:Issuer>
    <saml2:NameID NameQualifier="https://www.elster.de"
                  SPNameQualifier="https://demoserviceprovider.de"
                  Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">ek-92429d82a41e930486c6de5ebda9602d55c39986</saml2:NameID>
    <saml2p:Terminate/>
</saml2p:ManageNameIDRequest>
```

Codeblock 7 Beispiel- ManageNameIDRequest (unverschlüsselt, ohne Signaturinhalte, fehlende Namespace-Präfix zwecks Übersichtlichkeit)

5.3.8.2. Prüfung des SAML-ManageNameIDRequest durch Service Provider

Wenn der Service Provider den ManageNameIDRequest über den Endpoint https://demoserviceprovider.de/nezo/mni erhält, so muss der ManageNameIDRequest unmittelbar überprüft werden. Der Service Provider prüft dann zunächst folgende Eigenschaften:

- Der ManageNameIDRequest muss erfolgreich geparst werden können und schema-valide sein
- Der SAML-ManageNameIDRequest muss signiert sein, nur folgende Signatur-Algorithmen werden bei ELSTER unterstützt: sha256-rsa-MGF1
- Das <Issuer>-Format-Attribut muss fehlen oder den Wert "urn:oasis:names:tc:SAML:2.0:nameid-format:entity" enthalten.
- Das in der Signatur verwendete Zertifikat muss mit einem der im Service Provider hinterlegten Zertifikate des IdP übereinstimmen, die Signatur muss erfolgreich geprüft werden.

Ist eine dieser Eigenschaften nicht erfüllt, dann antwortet der Service Provider mit HTTP-Fehler 400 (Bad Request).
Sind die bisherigen Prüfungen erfolgreich, so wird der erfolgreich authentifizierte ManageNameIDRequest weiter geprüft.
Wenn der ManageNameIDRequest eine von "2.0" abweichende Version enthält, dann erzeugt der Service Provider eine ManageNameIDResponse mit Fehler TopLevelCode VersionMismatch + 2ndLevelCode RequestVersionTooHigh (wenn Version > 2.0) / RequestVersionTooLow (wenn Version < 2.0) .
Wenn eine der folgenden Bedingungen nicht erfüllt sind, dann erzeugt der Service Provider eine ManageNameIDResponse mit Fehler TopLevelCode Requester + 2ndLevelCode RequestDenied:

- Die Destination muss mit einer vom Service Provider unterstützten URL für Verarbeitung von SAML-ManageNameIDRequests übereinstimmen.
- Der Erstellungszeitpunkt des ManageNameIDRequest (IssueInstant) darf nicht vor mehr als 5 Minuten liegen.
- Das SPNameQualifier-Attribut muss mit der Entity-ID des Service Providers (https://demoserviceprovider.de) übereinstimmen.

5.3.9.ManageNameIDResponse

Der ManageNameIDResponse wird vom Service Provider als Antwort auf den ManageNameIDRequest per SOAP (SOAP Envelope) an den ELSTER-IdP gesendet.

XML-Element / -Attribut	Beschreibung
<ManageNameIDRequest>	
a) Version	Legt die SAML-Version fest. Muss den Wert "2.0" enthalten.

XML-Element / -Attribut	Beschreibung
b) ID	Zufällig gewählte ID, s. (SAMLCore, Z. 1467 + Skt. 1.3.4)
c) IssueInstant	Erstellungszeitpunkt des SAML-AuthnRequest
d) InResponseTo	Referenz zum ManageNameIDRequest, muss mit der ID des ManageNameIDRequest übereinstimmen
1) <Issuer>	"https://demoserviceprovider.de"
2.) <Status>	Status der Verarbeitung des dazugehörigen ManageNameIDRequest
2.1) <StatusCode>	TopLevelCode (SAMLCore, Z. 1634)
2.1.a) Value	Statuscode-Wert
2.1.1) <StatusCode>	Optionaler 2nLevelCode (SAMLCore, Z. 1646)
2.1.1a) Value	Statuscode-Wert

5.3.9.1. Beispiel-ManageNameIDResponse-XML

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:ManageNameIDResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                             xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                             Version="2.0"
                             ID="_92429d82a41e930486c6de5ebda9602d"
                             IssueInstant="2018-05-26T14:54:31.812Z"
                             InResponseTo="_e8b0dd41938018a871a13dd92bed4614">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <!-- Signaturinhalte -->
    </ds:Signature>
    <saml2:Issuer>https://demoserviceprovider.de</saml2:Issuer>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </saml2p:Status>
</saml2p:ManageNameIDResponse>
```

Codeblock 8 Beispiel- ManageNameIDResponse (unverschlüsselt, ohne Signaturinhalte)

5.3.9.2. Prüfung der ManageNameIDResponse durch ELSTER

Wenn der ELSTER-IdP die Response erhält, so wird dieser unmittelbar überprüft.

- Die ManageNameIDResponse muss erfolgreich geparst werden können und schema-valide sein.

- Die ManageNameIDResponse muss signiert sein, nur folgende Signatur-Algorithmen werden bei ELSTER unterstützt: sha256-rsa-MGF1.
- Das <Issuer>-Format-Attribut muss fehlen oder den Wert "urn:oasis:names:tc:SAML:2.0:nameid-format:entity" enthalten (SAMLProfiles, Z. 515).
- Das in der Signatur verwendete Zertifikate muss mit einem der im ELSTER-IdP zum Service Provider hinterlegten Zertifikaten übereinstimmen, die Signatur muss erfolgreich geprüft werden.
- Der TopLevelStatusCode muss den Wert "urn:oasis:names:tc:SAML:2.0:status:Success" haben.

5.3.10. LogoutRequest

LogoutRequests treten in zwei Versenderichtungen auf: Als Aufforderung zum Nutzerlogout durch den ServiceProvider an den IdP, und als Session-Termination-Aufforderung vom IdP einen SSO-Session-Teilnehmer (ServiceProvider). Achtung: zweiteres nur bei entsprechender Konfiguration im Rahmen des globalen Logouts.

XML-Element / -Attribut	**Beschreibung (SP an IdP)**	**Beschreibung (IdP an SP) "Session-Termination-Request"**
<LogoutRequest>		
a) Version	Legt die SAML-Version fest. Muss den Wert "2.0" enthalten.	Legt die SAML-Version fest. Muss den Wert "2.0" enthalten.
b) ID	Zufällig gewählte ID, s. (SAMLCore, Z. 1467 + Skt. 1.3.4)	Zufällig gewählte ID, s. (SAMLCore, Z. 1467 + Skt. 1.3.4)
c) IssueInstant	Erstellungszeitpunkt des SAML-Request	Erstellungszeitpunkt des SAML-Request
1) <Issuer>	"https://demoserviceprovider.de"	"https://www.elster.de"
<NameID>	Die pseudonymisierte Benutzerkonto-ID der Identität für die die Session beendet werden soll. Bei Bedarf verschlüsselt (in dem Fall wird Element <EncryptedID> übermittelt.	

XML-Element / -Attribut	Beschreibung (SP an IdP)	Beschreibung (IdP an SP) "Session-Termination-Request"
3) <SessionIndex>	Optionales Element. Liste an Identifiern der Sessions, die ausgeloggt werden sollen. Der ELSTER-IdP liefert dem Service Provider in der SAML-Response einen Session-Index. Wird kein SessionIndex angegeben, wird nach der NameId aufgelöst und der Nutzer aus allen SSO-Sessions ausgeloggt.	

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                      Destination="https://www.elster.de/ekona/slo"
                      ID="_323ea88978196bc77475a0c402360987f33667a9"
                      IssueInstant="2021-09-24T15:51:19.124Z"
                      Version="2.0">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                  Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://demoserviceprovider.de</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <!-- Signaturinhalte -->
    </ds:Signature>
    <saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                  Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">ek-8d4150a0a57601d3bd122eab25ec425953276afa</saml2:NameID>

<saml2p:SessionIndex>_ee3f59ff079f8f11058f669df76f37b062603beb</saml2p:SessionIn
dex>
</saml2p:LogoutRequest>
```

Codeblock 9 Beispiel- LogoutRequest SP an IDP (unverschlüsselt, ohne Signaturinhalte)

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                      Destination="https://demoserviceprovider.de/slo"
                      ID="_323ea88978196bc77475a0c402360987f33667a9"
                      IssueInstant="2021-09-24T15:51:19.124Z"
                      Version="2.0">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                  Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://www.elster.de</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <!-- Signaturinhalte -->
    </ds:Signature>
    <saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                  Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">ek-8d4150a0a57601d3bd122eab25ec425953276afa</saml2:NameID>

<saml2p:SessionIndex>_ee3f59ff079f8f11058f669df76f37b062603beb</saml2p:SessionIn
dex>
</saml2p:LogoutRequest>
```

Codeblock 10 Beispiel- LogoutRequest IDP an SP (unverschlüsselt, ohne Signaturinhalte)

5.3.11. LogoutResponse

LogoutResponses treten in zwei Versenderichtungen auf: Als Quittierung des Nutzerlogouts nach Anfrage des ServiceProvider an den IdP, und als Session-Termination-Request vom ServiceProvider an den IdP. Die Richtung ServiceProvider→IdP muss für die Teilnahme am SingleSignO verpflichtend implementiert und konfiguriert sein. Der Session-Termination-Prozess muss nur konfiguriert und implementiert sein, wenn eine Teilnahme am Globalen Logout gewünscht ist. Dies ist derzeit optional und bedarf aktuell einer Freigabe nach Abstimmung.

5.3.11.1. Prüfung des LogoutRequests durch ELSTER

Wenn der ELSTER-IdP den LogoutRequest erhält, so wird dieser unmittelbar überprüft.

- Der LogoutRequest muss erfolgreich geparst werden können und schema-valide sein.
- Der LogoutRequest muss signiert sein, nur folgende Signatur-Algorithmen werden bei ELSTER unterstützt: sha256-rsa-MGF1.
- Das in der Signatur verwendete Zertifikate muss mit einem der im ELSTER-IdP zum Service Provider hinterlegten Zertifikaten übereinstimmen, die Signatur muss erfolgreich geprüft werden.

5.3.11.2. LogoutResponse

XML-Element / -Attribut	Beschreibung (IdP zu SP)	Beschreibung (SP zu IdP) "Session-Termination-Response"
<LogoutResponse>		
a) Version	Legt die SAML-Version fest. Muss den Wert "2.0" enthalten.	Legt die SAML-Version fest. Muss den Wert "2.0" enthalten.
b) ID	Zufällig gewählte ID, s. (SAMLCore, Z. 1467 + Skt. 1.3.4)	Zufällig gewählte ID, s. (SAMLCore, Z. 1467 + Skt. 1.3.4)
c) IssueInstant	Erstellungszeitpunkt des SAML-Request	Erstellungszeitpunkt des SAML-Request
d) Destination	"https://demoserviceprovider.de/nezo/slo", die URL für den Empfang des SAML-Request	https://www.elster.de
e) InResponseTo	Referenz zum LogoutRequest, muss mit der ID des LogoutRequest übereinstimmen	Referenz zum LogoutRequest, muss mit der ID des LogoutRequest übereinstimmen
1) <Issuer>	https://www.elster.de	https://www.demoserviceprovider.de
2) <Status>	SAML-konforme Erfolgsmeldung **SUCCESS = "urn:oasis:names:tc:SAML:2.0:status:Success"** wird ausgegeben, wenn eine Globale Logout-Benachrichtigung an alle SSO-Session-Teilnehmer versandt werden konnte. **SamlStatusCode - Hinweis** Wenn der SP, der den Logout initiiert, selbst kein passendes SOAP-Binding hinterlegt hat, oder nicht alle SSO-session-Teilnehmenden SP technisch	SAML-konforme Erfolgsmeldung: **SUCCESS = "urn:oasis:names:tc:SAML:2.0:status:Success"**

XML-Element / -Attribut	Beschreibung (IdP zu SP)	Beschreibung (SP zu IdP) "Session-Termination-Response"
	erreichbar sind, geben wir statt Statuscode **SUCCESS = "urn:oasis:names:tc:SAML:2.0:status:Success"** einen Statuscode mit Statusmessage **PARTIAL_LOGOUT = "urn:oasis:names:tc:SAML:2.0:status:PartialLogout" message = "Logout konnte für den initiierenden ServiceProvider nicht vollzogen werden." minorCode = "0"** zurück. Der PartialLogout ist für den Fall, dass kein Globaler Logout gewünscht ist und konfiguriert wurde, als Erfolg zu verstehen.	

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                       Destination="https://demoserviceprovider/slo"
                       ID="_00d5c6dc21ba15f1a2872b5548fc51c67c67443a"
                       IssueInstant="2021-09-24T15:51:19.124Z"
                       Version="2.0"
                       InResponseTo="_323ea88978196bc77475a0c402360987f33667a9">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                  Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://www.elster.de</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <!-- Signaturinhalte -->
    </ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </saml2p:Status>
</saml2p:LogoutResponse>
```

Codeblock 11 Beispiel- LogoutResponse IDP an SP (unverschlüsselt, ohne Signaturinhalte)

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutResponse xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                       Destination="https://www.elster.de/ekona/slo"
                       ID="_00d5c6dc21ba15f1a2872b5548fc51c67c67443a"
                       IssueInstant="2021-09-24T15:51:19.124Z"
                       Version="2.0"
                       InResponseTo="_323ea88978196bc77475a0c402360987f33667a9">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                  Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://demoserviceprovider</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <!-- Signaturinhalte -->
    </ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </saml2p:Status>
</saml2p:LogoutResponse>
```

Codeblock 12 Beispiel- LogoutResponse SP an IDP (unverschlüsselt, ohne Signaturinhalte)

5.3.11.3. Prüfung der LogoutResponse durch den Service Provider

Wenn der Service Provider die LogoutResponse über den Endpoint https://demoserviceprovider.de/nezo/slo erhält, so muss die LogoutResponse unmittelbar überprüft werden.
Der Service Provider prüft dann zunächst folgende Eigenschaften:

- Die LogoutResponse muss erfolgreich geparst werden können und schema-valide sein
- Die SAML-LogoutResponse ist signiert, nur folgende Signatur-Algorithmen werden bei ELSTER unterstützt: sha256-rsa-MGF1
- Das in der Signatur verwendete Zertifikat muss mit einem der im Service Provider hinterlegten Zertifikate des ELSTER-IdP übereinstimmen, die Signatur muss erfolgreich geprüft werden.

Ist eine dieser Eigenschaften nicht erfüllt, dann antwortet der Service Provider mit HTTP-Fehler 400 (Bad Request).

5.3.12. Bausteinpseudonyme

In einigen Konstellationen kann es erforderlich sein, dass einige angebundene Module in der Lage sein müssen, die pseudonymisierten IDs der Anwender und Unternehmen "aufzulösen". Hierfür ist es erforderlich, dass diese Bausteine eindeutige, von den jeweiligen Service-Providern unabhängige, IDs (Account-ID, Datenübermittler-ID) erhalten. Die eindeutigen IDs sollen für diese Module in der SAML-Assertion verschlüsselt an die Service-Provider

übertragen werden. Möchte ein Service-Provider nun eine Anfrage an eines der weiteren Module stellen, so schickt der Service-Provider die verschlüsselten IDs an das Modul, welches die IDs entschlüsselt und in seinem Datenbestand zuordnen kann.

5.3.12.1. Übermittlung der verschlüsselten Pseudonyme in der SAML-Assertion

Die verschlüsselten Pseudonyme werden während eines NEZO-Logins durch einen Nutzer vom ELSTER-IdP über den Browser des Nutzers zum Service-Provider und von dort direkt an den jeweiligen Baustein übermittelt, da diese wie die Datenkranz-Attribute in der SAML-Assertion enthalten sind. Die Pseudonyme sind im neuen SAML-Attribut "Bausteinpseudonyme" in verschlüsselter Form enthalten. Dieses Attribut enthält eine Liste von JSON Web Tokens- ein Listenelement für jeden Baustein, mit dem der Service-Provider interagiert. Das JSON Web Token ist vom ELSTER-IdP signiert und für den jeweiligen Baustein verschlüsselt.

Der Inhalt dieses neuen SAML-Attributs wird exemplarisch an folgendem Beispiel erläutert, darauf folgt die XML-Schemadefinition des hierzu verwendeten komplexen XML-Datentyps "BausteinpseudonymeType".

⚠ **Hinweis**: Die Bausteinpseudonyme sind als optionales Attribut anzusehen. Sie werden (derzeit) immer an alle Service-Provider ausgeliefert, die den OZG-Datenkranz verwenden, unabhängig davon ob diese mit dem Autorisierungsmodul / OZG-Plus-Postfach arbeiten werden oder nicht. Das Attribut ist dennoch optional, weil es nur dann übermittelt wird, wenn im ELSTER-IdP (also auf unserer Seite) Bausteine konfiguriert und aktiv sind. Diese sind derzeit aktiv, könnten aber auch inaktiv sein. Der Inhalt und Aufbau des JSON Web Tokens ist lediglich für die Implementierung von Bausteinen relevant und wird hier nicht weiter erläutert. Die jeweiligen Bausteine werden erst dann im ELSTER-IdP konfiguriert und in den SAML-Assertions mitgeschickt, wenn die jeweiligen Module im Produktivbetrieb verfügbar sind.

Anmerkung: Die im nachfolgenden Beispiel enthaltenen base64-kodierten Daten bilden kein valides JWT, ein valides JWT würde ca. 1200 Zeichen umfassen.

SAML-Beispiel mit Attribut "Bausteinpseudonyme"

```
<saml2:AttributeStatement xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:ekona="http://www.elster.de/schema/ekona/saml/extensions">
  <!-- weitere Attribute -->
  <saml2:Attribute Name="Bausteinpseudonyme">
    <saml2:AttributeValue xsi:type="ekona:BausteinpseudonymeType">
      <ekona:Pseudonyme empfaenger="urn:governikus:ozg-plus-
postfach">TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQ=.Y29uc2V0ZXR1ciBzYWRpcHNjaW5nIG
```

```
VsaXRy.c2VkIGRpYW0gbm9udW15IGVpcm1vZCB0ZW1wb3I=</ekona:Pseudonyme>
      <ekona:Pseudonyme empfaenger="urn:dataport:aut-
modul">c2VkIGRpYW0gdm9sdXB0dWE=.aW52aWR1bnQgdXQgbGFib3JlIGV0IGRvbG9yZSBtYWduY
SBhbGlxdXlhbSBlcmF0.QXQgdmVybyBlb3MgZXQgYWNjdXNhbSBldCBqdXN0byBkdW8gZG9sb3Jlc
yBldCBlYSByZWJ1bQ==</ekona:Pseudonyme>
    </saml2:AttributeValue>
    <!-- weitere Attribute -->
</saml2:AttributeStatement>
```

Das XML-Schema für die Bausteinpseudonyme ist Bestandteil des NEZO-XML-Schemas (Namespace "http://www.elster.de/schema/ekona/saml/extensions") und im Abschnitt "NEZO-XML-Schema zur Verwendung in SAML-Nachrichten" dokumentiert.

5.3.13. RechtsformText und TaetigkeitText

Rechtsform und Tätigkeit werden ausgehend von ihrer Schlüsselzahl zu Text konvertiert (s. Anhang). Das Textfeld ist bei bestimmten Datenkranztypen ein Pflichtfeld der SAML-Assertion. Wenn die zugrundeliegende Kennzahl nicht konvertiert werden kann, wird das Feld nicht befüllt und es wird ein Fehler ausgegeben. Anbei ein Assertion-Attribut-Beispiel für die Rechtsform (StNr-Datenkranz einer NNatPers):

```
<!-- bereits existierendes Datenkranzelement -->
<saml2:Attribute Name="Rechtsform">
    <saml2:AttributeValue xsi:type="xs:string">230</saml2:AttributeValue>
</saml2:Attribute>
<!-- neues Datenkranzelement -->
<saml2:Attribute Name="RechtsformText">
    <saml2:AttributeValue xsi:type="xs:string">Ges. mit beschr. Haftung und
Co.KG</saml2:AttributeValue>
</saml2:Attribute>
```

Anbei ein Assertion-Attribut-Beispiel für die Tätigkeit (StNr-Datenkranz einer NatPers):

```
<!-- bereits existierendes Datenkranzelement -->
<saml2:Attribute Name="Taetigkeit">
    <saml2:AttributeValue xsi:type="xs:string">140</saml2:AttributeValue>
</saml2:Attribute>
<!-- neues Datenkranzelement -->
<saml2:Attribute Name="TaetigkeitText">
    <saml2:AttributeValue xsi:type="xs:string">Angehörige der freien
Berufe</saml2:AttributeValue>
</saml2:Attribute>
```

5.4. SingleLogout

ELSTER als IdentityProvider bietet für Teilnehmer am Single Sign-On die Möglichkeit, die Authentifizierung beim eigenen ServiceProvider für alle SingleSign-On-Teilnehmer zu widerrufen. Damit kann die für einen ServiceProvider erstellte und für alle anderen ServiceProvider im Verbund verwendbare Authentifizierungssession beendet werden, ein weiterer Login bei einem ServiceProvider muss erneut vollständig durchgeführt werden. Dies wird im Folgenden als SingleLogout bezeichnet.

Das Verfahren ermöglicht es, im Logoutfall alle teilnehmenden ServiceProvider über den Logout zu informieren, sodass sie ihre Sessions terminieren. Dies führt für den Nutzer zu erhöhter Sicherheit, da eine offene Session bei zwei ServiceProvidern durch einen Logout beidseitig beendet wird. Dies verhindert, dass der Nutzer einseitig einen Logout durchführt und die andere Seite weiter eine offene Session aufrechterhält, in der Nutzerdaten angezeigt oder verändert werden können, obwohl der Nutzer annimmt, er wäre ausgeloggt. Dieses Verfahren zur Session Termination bei allen Partnern wird als Globaler Logout bezeichnet.

Um die Logout-Funktionalität verwenden können, muss der ServiceProvider zwei URLs pflegen, die SingleLogout Service URL und die Session Termination URL. Diese unterscheiden sich im wesentlichen im Binding und in ihrer Funktion: An Single Logout Service URL wird die Antwort gesendet, wenn Ihr Service Provider den Logout initiiert. An die Session Termination URL wird ein Request gesendet, wenn ein anderer Service Provider einen Logout initiiert hat, der dann über ELSTER an Ihren Service Provider weitergereicht wird. Daher wird die Single Logout Service URL mit HTTP-Post-Binding und die Session Termination URL mit SOAP-Binding verwendet.

Hinweis: Haben Sie vor Oktober 2024 bereits das Single Logout Verfahren eingesetzt und nur die Single Logout Service URL gepflegt, erhalten Sie die Antwort "Partial Logout" (s. LogoutRequest (dort linke Seite der Tabelle)). Bitte ergänzen Sie das Handling der Session Termination URL und informieren Sie uns per Mail an projektbuero.nezo@elster.de unter Angabe der verwendeten Entity-ID.

5.4.1. Funktionsweise

Mit der SingleLogout-Funktionalität kann der ServiceProvider dem IdP einen LogoutRequest (dort linke Seite der Tabelle) für einen Nutzer oder eine Nutzersession senden. Dieser LogoutRequest muss den dort genannten Anforderungen genügen und an den Logout-Endpunkt (i.A. https://elster.de/slo) des IdP adressiert sein. Daraufhin entwertet der IdP alle Zugangstoken für die Nutzersession - auch vor derem zeitlichen Ablauftermin. Dadurch muss sich der Nutzer im Single-Sign-On-Verbund neu authentifizieren. Dies erlaubt dem Nutzer/ServiceProvider Kontrolle über seine Authentifizierung. Der IdP antwortet dem ServiceProvider mit einer LogoutResponse (linke Seite der Tabelle) an dessen SingleLogout-Endpunkt mit Binding HTTP-Post und informiert über den Erfolg der Funktion.

Die zusätzliche Konfiguration eines SingleLogout-Endpunkts mit Binding SOAP (im Feld "Session Termination URL"), d.h. es müssen zwei SingleLogout-Endpunkte konfiguriert sein (1x HTTP-Post, 1x SOAP als Binding), erlaubt die Information darüber, dass sich der Nutzer bei einem anderen Service Provider aus dem SSO-Verbund ausgeloggt hat. Die URL des Endpunkts kann identisch sein, wenn die eingehenden Nachrichten getrennt nach Art und Binding unterschiedlich abgehandelt werden. Wenn der IdP von einer Drittpartei (üblicherweise: anderer ServiceProvider im SSO-Verbund) einen SingleLogoutRequest erhält, verschickt er an ServiceProvider, die am Globalen Logout teilnehmen, einen Logoutrequest (dort rechte Seite der Tabelle). Dies bedeutet für den ServiceProvider, dass der Nutzer eine Beendigung seiner SingleSign-On-Session im Verbund zu beenden wünscht, und eine Terminierung der laufenden Session notwendig ist. Der ServiceProvider beendet die Session des Nutzers. Damit sind a) alle Zugangstoken des Nutzers entwertet (dies passiert im SingleLogout) und b) alle Sessions des Nutzers bei allen ServiceProvidern des Verbunds terminiert. Dies bietet dem Nutzer die Sicherheit, dass z.B. ein offener Browsertab, in dem der Nutzer noch in einer Session eingeloggt ist, automatisch mit beendet wird. Der ServiceProvider quittiert den LogoutRequest und die Behandlung mit einer LogoutResponse (rechte Seite der Tabelle) an den SingleLogout-Endpunkt des IdP (binding darf hier nicht geprüft werden).

6. Zertifikate

Die für die SAML-Kommunikation erforderlichen Zertifikate müssen seitens des Unternehmenskontos keine großen Anforderungen erfüllen:

- Es muss sich um X.509 Zertifikate handeln
- Die Zertifikate müssen einen 4096Bit-Schlüssel enthalten

Es gibt seitens Unternehmenskonto keine Anforderungen an die Signatur der Zertifikate oder sonstiger Inhalte. Bitte machen Sie sich innerhalb Ihres Vorhabens Gedanken zum Schlüsselmanagement bzw. wenden Sie sich dafür an die zuständigen Stellen wie z.B. das Sicherheitsmanagement.

6.1. Testzertifikate und Keystore mit OpenSSL selber erzeugen

Sofern Sie sich nicht innerhalb Ihrer Organisation Zertifikate zur Nutzung an der E4K-Testumgebung des Unternehmenskontos erhalten können ist nachfolgend kurz beschrieben, wie Sie sich Zertifikate und Schlüssel selber erzeugen können. Mittels OpenSSL können Sie sich Zertifikate zur Nutzung an der E4K-Testumgebung des Unternehmenskontos sowie die dazugehörigen privaten Schlüssel zur Verwendung in Ihrer Software selber erzeugen.

Die nachfolgenden Befehle wurden auf der Kommandozeile mittels OpenSSL 3.0.9 auf Windows 10 ausgeführt.

```
openssl genrsa -out c:\temp\nezo-saml\devnezo.encr.saml-key.pem 4096
```

```
openssl req -x509 -out c:\temp\nezo-saml\devnezo.encr.saml-cert.pem -days 3650 -
key c:\temp\nezo-saml\devnezo.encr.saml-key.pem
-subj "/C=DE/O=apgemini und pegasystems/CN=devnezo.encr.saml" -sigopt
rsa_padding_mode:pss -sigopt rsa_mgf1_md:sha256 -sha256
```

```
openssl pkcs12 -out c:\temp\nezo-saml\devnezo.encr.saml.p12 -inkey c:\temp\nezo-
saml\devnezo.encr.saml-key.pem
-in c:\temp\nezo-saml\devnezo.encr.saml-cert.pem -export -name devnezo.encr.saml
```

Die 3 Kommandozeilen-Befehle erzeugen die folgenden Artefakte:

1. ein Keystore mit dem Namen "devnezo.encr.saml.p12",
2. einen privaten Schlüssel zur Signaturerzeugung "devnezo.encr.saml-key.pem" sowie
3. das dazu passende Zertifikat "devnezo.encr.saml-cert.pem"

Hinweis: Das Zertifikat kann so noch nicht im SSP verwendet werden. Die PEM-spezifische Anfangs- und Endzeile sowie CR+LF müssen entfernt werden.

⚠ Die oben beschriebenen Befehle sind als Beispiele gedacht. Anfragen dazu werden nicht beantwortet. Die Artefakte sind nicht als Empfehlung zu verstehen.

6.2. Wechsel Ihrer Zertifikate

Für ein reibungsloses Funktionieren Ihrer SAML-Anbindung ist es erforderlich, dass Sie gültige Zertifikate für Signatur und Verschlüsselung im SSP zu Ihren Service Providern hinterlegt haben. Die Verwaltung der Gültigkeit Ihrer Zertifikate obliegt Ihnen. Behalten Sie diese von daher immer im Blick und sorgen Sie rechtzeitig für den Austausch Ihrer Zertifikate, da Ihre SAML-Requests nach Ablauf der Zertifikate ansonsten zurückgewiesen werden.

6.2.1. Wechsel Ihres Signaturzertifikates

Ist ein Austausch fällig, empfehlen wir Ihnen die nachfolgende Vorgehensweise zum Zertifikatsaustausch OHNE dass dafür eine Downtime, eine Stichtagsumstellung oder eine Mithilfe seitens Unternehmenskonto vonnöten ist.

1. Hinterlegen Sie im SSP zu den betroffenen Service Providern das neue Signaturzertifikat, so dass sowohl altes-, als auch neues Signaturzertifikat hinterlegt sind. Warten Sie auf die Genehmigung der Konfigurationsänderung. Nach Genehmigung ist das Unternehmenskonto in der Lage SAML-Requests zu verarbeiten, die mit altem-, oder neuem Zertifikat signiert wurden.
2. Stellen Sie Ihre Anwendung so um, dass diese mit dem neuen Zertifikat signiert.
3. Räumen Sie ggf. danach auf indem Sie im SSP das alte Zertifikat entfernen.

6.2.2.Wechsel Ihres Verschlüsselungszertifikates

Ist ein Austausch fällig, empfehlen wir Ihnen die nachfolgende Vorgehensweise zum Zertifikatsaustausch OHNE dass dafür eine Downtime, eine Stichtagsumstellung oder eine Mithilfe seitens Unternehmenskonto vonnöten ist.

1. Stellen Sie Ihre Anwendung so um, dass diese in der Lage ist SAML-Responses zu verarbeiten, die entweder mit Ihrem alten- oder neuen Verschlüsselungszertifikat verschlüsselt wurden.
2. Hinterlegen Sie im SSP zu den betroffenen Service Providern das neue Verschlüsselungszertifikat und warten Sie auf die Genehmigung der Konfigurationsänderung. Nach Genehmigung verschlüsselt das Unternehmenskonto alle SAML-Responses mit Ihrem neuen Zertifikat.
3. Räumen Sie ggf. danach auf indem Sie in Ihrer Anwendung das alte Zertifikat entfernen.

7. Troubleshooting

Im nachfolgenden sind häufige Probleme mit Ihren möglichen Ursachen aufgeführt. Sollten Sie ähnliche Probleme haben, bitten wir Sie, zunächst die einzelnen Problempunkte zu überprüfen, bevor Sie eine Supportanfrage stellen. So können wir Ihnen schneller und gezielter weiterhelfen.

7.1. Ich kann meinen Antrag für einen Service Provider nicht absenden

Dies liegt häufig daran, dass Pflichtfelder nicht gefüllt sind, oder die in den Tooltips beschriebenen Vorgaben nicht erfüllt wurden.

- Generell: Bitte Prüfen Sie, welche Pflichtfelder das Formular bemängelt und füllen Sie diese aus
- Signatur-/Entschlüsselungszertifikat: Bitte Prüfen Sie, ob das von Ihnen eingefügte Zertifikat CR/LF enthält. Wenn ja, dann entfernen Sie diese nicht sichtbaren Zeichen
- Logo: Bitte beachten Sie die Vorgaben für Dateiformat, Dateigröße und Bildgröße

7.2. Ich kann den Antrag für einen Service Provider zwar absenden, bekomme dann aber eine Fehlermeldung

Fehler, welche NACH Beantragung zurückgemeldet werden liegen häufig an den Zertifikaten. Prüfen Sie die folgenden Dinge:

- Lässt sich das in das Eingabefeld eingefügte Zertifikat parsen? Nutzen Sie dafür einfach ein frei im Internet verfügbares Werkzeug, wie z.B. den Cyberchef (https://gchq.github.io/CyberChef/#recipe=Parse_X.509_certificate('Base64')) Kann dort das Zertifikat nicht erfolgreich geparst werden, dann wird dies auch bei Beantragung im SSP abgelehnt werden.
    - Eine häufige Ursache ist die Verwendung des PEM Formates, welches beim SSP nicht akzeptiert wird. Das PEM-Format ist selber Base64 codiert und enthält das Base64 codierte Zertifikat.
- Parsen Sie das Zertifikat und prüfen Sie die Schlüssellänge. Oft werden versehentlich Zertifikate mit 2048 Bit Schlüsseln bei uns eingereicht. Im SSP sind ausschließlich Zertifikate mit 4096 Bit-Schlüsseln erlaubt.
- Parsen Sie das Zertifikat und prüfen Sie die Gültigkeit Ihres Zertifikates. Abgelaufene Zertifikate werden im SSP nicht akzeptiert.

7.3. Ich habe einen genehmigten Service Provider, mir wird bei der Weiterleitung meines SAML-Requests bei ELSTER aber ein Fehler angezeigt.

Folgende Ursachen treten bei diesem Fehlerbild häufig auf:

- Die im SAML-Request als "Issuer" angegebene entity-Id entspricht nicht der Id, die im Service-Provider Antrag eingegeben wurde
- Sie kommunizieren mit dem falschen ELSTER-System. Die URL unserer Testumgebung lautet: https://e4k-portal.een.elster.de/ekona/sso Bitte laden Sie sich die ELSTER-Entity-Descriptoren im Downloadbereich des SSPs
- Die im SAML-Request angegeben AssertionConsumer-URL wurde nicht im Service-Provider Antrag eingegeben.
- Der zur Signatur des SAML-Request verwendete Private-Key passt nicht zu dem im Service-Provider Antrag eingegebenen Zertifikat
- Der zur Signatur des SAML-Requests verwendete Kryptoalgorithmus wird durch das Unternehmenskoto nicht unterstützt. Bitte stellen Sie sicher, dass der folgende Algorithmus verwendet wird: SignatureMethod Algorithm="http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1"

7.4. Ich konnte mich bei ELSTER zwar anmelden, bekomme aber unmittelbar danach eine Fehlermeldung

Mögliche Gründe sind häufig:

- Downtime einiger Komponenten in der ELSTER-Umgebung
- Verwendung von ELSTER-Zertifikatsdateien, die auf der Umgebung, die Sie nutzen unbekannt sind. Nehmen Sie für das Produktivsystem wirklich nur "Echte" Echtzertifikate. Nutzen Sie für die E4K-Testumgebung nur solche Zertifikate, die Sie per Support Ticket im SSP beantragt haben.

7.5. Ich konnte mich bei ELSTER anmelden und die Datenweitergabe bestätigen, kann die SAML-Response aber nicht parsen

Mögliche Gründe sind häufig:

- Der in Ihrer Umgebung hinterlegte Private Key für die Entschlüsselung passt nicht zu dem im Service-Provider Antrag eingegebenen Zertifikat
- Ihr System unterstützt nicht den für die Entschlüsselung benötigten Kryptoalgorithmus RSA-OAEP

7.6. Ich konnte die SAML-Response zwar parsen, finde aber die NameID mit der AccountPseudonymID nicht

- Die NameID ist (wie es der SAML-Standard durchaus erlaubt) doppelt verschlüsselt. Die NameID wird verschlüsselt als EncryptedID in die SAML-Assertion gepackt, welche

wiederum verschlüsselt wird. Wenn in Ihrem Ergebnis nach Entschlüsselung noch eine EncryptedID vorhanden ist, dann entschlüsseln Sie diese bitte.

7.7. Ich möchte meinen ManageNameID-Service testen

1. Tragen Sie im "SSP" eine "Manage Name ID URL" in Ihrer Service Provider Konfiguration ein.
2. Für eines der e4k-Testzertifikate legen Sie einen Account bei sich in Ihrem Service Provider an: Hierfür muss mit dem e4k-Testzertifikat ein NEZO-Login durchgeführt werden. Während des NEZO-Logins müssen eventuell die Datenschutz- und Freigabe-Einwilligungen bestätigt werden. Im Anschluss erhält Ihr Service Provider die Daten des, hinter dem Zertifikat stehenden, Elster-Kontos.
3. Melden Sie sich mit dem e4k-Testzertifikat bei "Mein ELSTER" in der E4K-Testumgebung an und widerrufen Sie die Freischaltung zur "Nutzung für andere eGovernment-Dienste" (ELSTER -> Mein Benutzerkonto -> Andere eGovernment-Dienste freischalten).
4. Anschließend erhalten Sie, unter der im SSP angegebenen "Manage Name ID URL", einen ManageNameIDRequest.

8. Begriffsbestimmungen (Ergänzungen)

ELSTER-Testkonten: Vereinzelte Benutzergruppen wie bspw. Softwarehersteller erhalten bei ELSTER die Möglichkeit, über einen getrennten Zugang zur ELSTER-Seite sogenannte Testkonten zu erstellen. Diese Konten verfügen über eingeschränkte Funktionalität, sodass bspw. ausgefüllte Formulare nicht an das Finanzamt zur fachlichen Bearbeitung geleitet werden, sondern frühzeitig ausgesteuert werden. Diese Konten können jedoch für Schnittstellentests eingesetzt werden. Testkonten können mit den echten Daten eines Bürgers bzw. eines Unternehmens registriert werden, die Zustellung des Aktivierungscodes erfolgt in diesem Fall umgehend per E-Mail (anstelle per Brief). Es besteht aber auch die Möglichkeit, Testkonten zu fiktiven Testdaten zu verwenden (die Registrierung erfolgt mit Test-IdNrn bzw. Test-StNrn). Bei der Nutzung von ELSTER-Testkonten über die NEZO-Schnittstelle besteht jedoch die Einschränkung, dass nur Testkonten mit fiktiven Testdaten verwendet können, um Datenschutzprobleme zu verhindern.

ELSTER-Echtkonten: Die Konten, die wie gewöhnlich über die offizielle ELSTER-Seite (https://www.elster.de) registriert werden. Zur Abgrenzung siehe auch Begriff "ELSTER-Testkonten". Wichtig: Auch auf einem Testsystem gibt es Konten, die das jeweilige System für "Echt" hält. In der Regel sind alle Testzertifikate, die zu Testzwecken herausgegeben "Echt"zertifikate. Es sind dort allerdings nur Testdaten hinterlegt.

Single Sign-On: NEZO bietet die Möglichkeit, eine bestehende ELSTER-IdP-Session des Nutzers für Logins bei Service Providern weiterzuverwenden und damit für den Nutzer den Login-Vorgang abzukürzen. Dies ist nur für einen begrenzten Zeitraum nach dem ersten Login möglich - die Sessiondauer bei Mein ELSTER beträgt derzeit 30 Minuten. Dabei ist zu beachten, dass bestehende Sessions weiterer Service Provider nicht sofort beendet werden, um dem Nutzer die verlustfreie Fertigstellung von Formularen etc. zu gewährleisten. Wenn ein Service Provider den Single Sign-On Mechanismus nutzen möchte, dann muss dieser auch das SingleLogout-Profil unterstützen. ELSTER kann unabhängig von der Angabe "ForceAuth=false" im AuthnRequest kontrollieren, ob der Nutzer ggf. doch einen frischen Login durchführen muss. Mit diesem Mechanismus erhalten sowohl der ServiceProvider, der die Session initial authentisieren lässt, Kontrolle über dessen Verwendung (Zustimmung in der Konfiguration ist notwendig für die SingleSign-On-Teilnahme), als auch der ServiceProvider, bei dem ein Nutzer sich mittels SSO versucht zu authentifizieren. Der im SSO-Verbund nachgelagerte ServiceProvider (!=Initiator der SSO-Session) übt dieses Kontrolle mittels des forceAuthn Attributs im Authnrequest oder der Konfiguration aus, dies erzwingt einen frischen Login).

9. Anhang

9.1. Wichtige Links zu ELSTER und Unternehmenskonto

Zur Administration der dem Unternehmenskonto zugrundeliegenden ELSTER-Accounts kann es notwendig sein sich sowohl in der E4K-Testumgebung, als auch in Produktion bei "Mein ELSTER" oder **Mein Unternehmenskonto** einzuloggen. Die Verlängerung von Zertifikatsdateien, Änderung von E-Mail-Adressen, verknüpfen von handelnden Personen u.v.m. können selber durchgeführt werden. Nachfolgend die Links:

- **Mein Unternehmenskonto** in der E4K-Testumgebung: https://e4k-muk.een.elster.de/public/#Startseite
- "Mein ELSTER" in der E4K-Testumgebung: https://e4k-portal.een.elster.de/eportal/start
- **Mein Unternehmenskonto** in der Produktivumgebung: https://mein-unternehmenskonto.de/public/
- "Mein ELSTER" in der Produktivumgebung: https://mein-unternehmenskonto.de/public/
- "SSP" in der Produktivumgebung: https://service.mein-unternehmenskonto.de/

- (TR-03107-1) „BSI TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government - Teil 1: Vertrauensniveaus und Mechanismen“. BSI, o. J. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=2.
- (SAMLCore): „Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0“. OASIS, 15. März 2005. https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.
- (SAMLTechOverview): „Security Assertion Markup Language (SAML) V2.0 Technical Overview“, o. J. https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf.
- (SAMLBindings): „Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0“. OASIS, o. J. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf.
- (SAMLProfiles): „Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0“. OASIS, o. J. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

- (SAMLSecure): „Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0“. OASIS, o. J. http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf.
- (SAMLAuthnCxt): „Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0“. OASIS, o. J. http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf.
- (PassVwV): „Passverwaltungsvorschrift - PassVwV“, 17. Dezember 2009. http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_17122009_IT464400311.htm.

9.2. Liste der unterstützten Rechtsformen

Ist eine juristische Person Inhaber des Steuerkontos, für das ELSTER-Zertifikate ausgestellt wurden, können die nachfolgenden Werte als Rechtsform zurückgegeben werden:

Rechtsform	RechtsformText
200	"atypische stille Gesellschaft"
210	"Offene Handelgesellschaft"
220	"Kommanditgesellschaft"
230	"Ges. mit beschr. Haftung & Co. KG"
240	"Ges. mit beschr. Haftung & Co.OHG"
250	"Aktiengesellschaft & Co. KG"
260	"Aktiengesellschaft & Co. OHG"
270	"Gesellschaft des bürgerlichen Rechts"
280	"Europäische wirtschaft. Interessenvereinigung (EWIV)"
290	"sonstige Personengesellschaft"
291	"Gemeinschaft (z.B. Erben-, Grundstücks-)"
292	"Partenreederei (§§489 ff HGB)"
293	"Partnerschaft (§1 PartGG)"
294	"Sozietät"
295	"Unterbeteiligung"

Rechtsform	RechtsformText
310	"Aktiengesellschaft"
320	"Kommanditgesellschaft auf Aktien"
330	"Kolonialgesellschaft"
340	"Bergrechtliche Gesellschaft"
350	"Gesellschaft mit beschränkter Haftung"
360	"Europäische Gesellschaft (SE)"
410	"Kreditgenossenschaft, Kredite ausschl.an Mitgl."
420	"Zentralkasse, Kredite ausschl.an Mitgl.,gen.Aufg."
430	"Landwirtschaftliche Nutzungs- und Verwertungsgenossenschaft"
440	"Realgemeinde"
490	"sonstige Genossenschaft i. S. des Genossenschaftsgesetzes"
510	"Versicherungsverein auf Gegenseitigkeit"
590	"sonstige juristische Person des privaten Rechts"
610	"nicht rechtsfähiger Verein, Anstalt, Stiftung und anderes Zweckvermögen"
621	"nichtrechtsfähiger Verein"
622	"rechtsfähiger sonstiger Verein"
623	"Wirtschaftlicher Verein"
624	"Sonstiges Zweckvermögen"
625	"Stiftung"
710	"Staatsbank"
720	"öffentliche oder unter Staatsaufsicht stehende Sparkasse"
730	"Sonstige Kreditanstalt des öffentlichen Rechts"
740	"öffentlich-rechtlicher Versorgungs-, Verkehrs- und Hafenbetrieb"
751	"wirtschaftlicher Geschäftsbetrieb"

Rechtsform	RechtsformText
752	"Zweckbetrieb"
790	"sonstiger Betrieb gewerblicher Art von juristischen Personen des öffentlichen Rechts"
810	"Gebietskörperschaft"
820	"öffentlich-rechtliche Religionsgesellschaft"
831	"berufsständige Körperschaft des öffentlichen Rechts"
832	"Innung"
833	"öffentlich-rechtliche Rundfunk- und Fernsehanstalt"
834	"sonstige juristische Person des öffentlichen Rechts"
835	"Sozialversicherungsträger"
836	"Stiftung des öffentlichen Rechts"
900	"sonstige ausländische Rechtsform"
910	"ausländische Rechtsform, die einer Kapitalgesellschaft entspricht"
920	"ausländische Rechtsform, die einer Personengesellschaft entspricht"
000	gelöscht
221	"Investmentkommanditgesellschaft"
370	"Unternehmergesellschaft (haftungsbeschränkt)"
380	"Investment-Aktiengesellschaft"
381	"Investment-Kommanditgesellschaft"
382	"Sondervermögen"
390	"sonstige Kapitalgesellschaft"
391	"Investmentaktiengesellschaft"
450	"Europäische Genossenschaft"
460	"eingetragene Genossenschaft"

Rechtsform	RechtsformText
511	"Pensionsfondsverein auf Gegenseitigkeit"
520	"eingetragener Verein (rechtsfähig)"
540	"rechtsfähige Stiftung des Privatrechts"
611	"Sondervermögen"
620	ab Sept/09 entfallen, da nicht benötigt
650	"nichtrechtsfähige Stiftung des Privatrechts"
811	"rechtsfähige Anstalt des öffentlichen Rechts"
837	"europäischer Verbund für territoriale Zusammenarbeit"
838	"nichtrechtsfähige Anstalt des öffentlichen Rechts"
840	"rechtsfähige Stiftung des öffentlichen Rechts"
850	"nichtrechtsfähige Stiftung des öffentlichen Rechts"
901	"ausländische Rf., die einem Zweckvermögen nach § 1 Abs. 1 Nr. 5 KStG entspricht"
930	"ausländische Rechtsform, die einer Genossenschaft entspricht"
940	"ausländische Rechtsform, die einer sonst. jur. Person des priv. Rechts entspricht"
950	"ausländische Rechtsform, die einer Pers.vereinigung oder Vermögensmasse i. S. des § 1 (1) Nr.5 KStG entspricht"
960	"ausländische Körperschaft des öffentlichen Rechts"
990	"sonstige nicht-nat. Rechtsform"

9.3. Liste der unterstützten Tätigkeiten

Ist eine natürliche Person Inhaber des Steuerkontos, für das ELSTER-Zertifikate ausgestellt wurden, können die nachfolgenden Werte an Stelle einer Rechtsform als Tätigkeit zurückgegeben werden:

Taetigkeit	TaetigkeitText
110	Hausgewerbetreibende und gleichgest. Personen

Taetigkeit	TaetigkeitText
120	Sonstige Einzelgewerbetreibende (außer Hausgewerbe und gleichgest.)
130	Land- und Forstwirte
140	Angehörige der freien Berufe
150	Sonstige selbständig tätige Personen
160	Personen mit Beteiligungen an gewerbl. Persges.
190	Sonstige natürliche Personen

9.4. SAML-Metadaten des ELSTER-IdP in der E4K-Integrationsumgebung (Sandbox)

Der Entity-Deskriptor des ELSTER-IdP wird als XML-Datei zum Download im SSP zur Verfügung gestellt: https://service.mein-unternehmensportal.de/api/downloads/entity_descriptoren_sp

9.5. SAML-Metadaten des ELSTER-IdP in der Produktionsumgebung

Der Entity-Deskriptor des ELSTER-IdP wird als XML-Datei zum Download im SSP zur Verfügung gestellt: https://service.mein-unternehmensportal.de/api/downloads/entity_descriptoren_sp

9.6. IP-Ranges für ausgehende Requests von ELSTER

Um auf Ihrer Seite ManageNameID-Requests von ELSTER empfangen zu können müssen auf Ihrer Seite u.U. Firewalls entsprechend konfiguriert werden.

Um die IP-Adressen für ausgehende Requests seitens ELSTER zu erfragen, loggen Sie sich bitte im SSP ein und stellen Sie eine Supportanfrage. Geben Sie bitte an, ob Sie die IP-Adresse für das Integrationssystem oder das Produktivsystem benötigen.