

NEZO Integrationsleitfaden

Stand 05/2026 – Version 365

Herausgegeben von



Bayerisches Staatsministerium
für Digitales



Bayerisches
Landesamt
für Steuern



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	6
2	Vorgehen bei der Integration Schritt-für-Schritt.....	8
2.1	Schritt 1: Voraussetzungen für die Integration.....	8
2.2	Schritt 2: Onboarding im Self Service Portal / Vorhaben beantragen	8
2.3	Schritt 3: Auswahl des für Sie relevanten Rechtsrahmens und der weiteren Konfiguration.....	10
2.3.1	Auswahl des Rechtsrahmens.....	11
2.3.2	Auswahl der für Sie relevanten "Zertifikatstypen" (Zum Login zugelassene(s) Ordnungsmerkmal(e))	11
2.3.3	Benötigen Sie Testzertifikate für produktive Smoke-Tests?.....	11
2.3.4	Speichern Sie ELSTER-Identitätsdaten?.....	12
2.3.5	Möchten Sie am Single-Sign-On Verbund teilnehmen?.....	12
2.4	Schritt 4: Konfiguration Ihres Service Providers	12
2.5	Schritt 5: Kontinuierliche Administration Ihres Vorhabens im Self Service Portal...	19
3	Konfiguration von benötigten Attributen.....	20
3.1	Voraussetzung: Rechtsrahmen	20
3.2	Verfügbarkeit von Attributen.....	21
4	Übersicht und Erklärung möglicher Attribute.....	22
4.1	Allgemeine Attribute zu allen Konten.....	22
4.2	Attribute zu Konten mit Steuernummer	26
4.3	Attribute zu Konten mit Identifikationsnummer	33
4.4	Funktionale Attribute: Bausteinpseudonyme	36
5	Einbindung von Mein Unternehmenskonto in die eigene Benutzeroberfläche.....	37
5.1	Einheitliches Wording.....	37
5.2	Registrierungsprozess	37
6	Schnittstelle Service Provider-ELSTER	39
6.1	Bindung der Identität an den Sitzungskontext	39
6.2	Allgemeine Festlegungen für die SAML-Kommunikation.....	40
6.3	SAML-Nachrichten zwischen Service Provider und ELSTER.....	40

6.3.1	Kryptographische Schlüssel für die SAML-Kommunikation, Schlüsselmanagement	42
6.3.2	Zeitsynchronisation der Server (Service Provider und ELSTER)	44
6.3.3	NEZO-XML-Schema zur Verwendung in SAML-Nachrichten	44
6.3.4	SAML-AuthnRequest	47
6.3.5	SAML-Response	50
6.3.6	ManageNameIDRequest	56
6.3.7	ManageNameIDResponse	59
6.3.8	LogoutRequest	60
6.3.9	LogoutResponse	62
6.3.10	Bausteinpseudonyme	64
6.3.11	RechtsformText und TaetigkeitText	66
6.4	SingleLogout	66
6.4.1	Funktionsweise	67
7	Zertifikate	69
7.1	Testzertifikate und Keystore mit OpenSSL selber erzeugen	69
7.2	Wechsel Ihrer Zertifikate	70
7.2.1	Wechsel Ihres Signaturzertifikates	70
7.2.2	Wechsel Ihres Verschlüsselungszertifikates	70
8	Troubleshooting	72
8.1	Ich kann meinen Antrag für einen Service Provider nicht absenden	72
8.2	Ich kann den Antrag für einen Service Provider zwar absenden, bekomme dann aber eine Fehlermeldung	72
8.3	Ich habe einen genehmigten Service Provider, mir wird bei der Weiterleitung meines SAML-Requests bei ELSTER aber ein Fehler angezeigt.	73
8.4	Ich konnte mich bei ELSTER zwar anmelden, bekomme aber unmittelbar danach eine Fehlermeldung	73
8.5	Ich konnte mich bei ELSTER anmelden und die Datenweitergabe bestätigen, kann die SAML-Response aber nicht parsen	73
8.6	Ich konnte die SAML-Response zwar parsen, finde aber die NameID mit der AccountPseudonymID nicht	74

8.7	Ich möchte meinen ManageNameID-Service testen	74
9	Begriffsbestimmungen (Ergänzungen)	74
10	Anhang	75
10.1	Wichtige Links zu ELSTER und Unternehmenskonto.....	75
10.2	Liste der unterstützten Rechtsformen.....	77
10.3	Liste der unterstützten Tätigkeiten	80
10.4	SAML-Metadaten des ELSTER-IdP in der E4K-Integrationsumgebung (Sandbox) 80	
10.5	SAML-Metadaten des ELSTER-IdP in der Produktionsumgebung	80
10.6	IP-Ranges für ausgehende Requests von ELSTER	80

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: Unsere Vorstellung ist, möglichst bundesweit eine Einheitlichkeit im „Branding“ des Unternehmenskontos zu 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:



Abbildung 1 Integration mit Mein Unternehmenskonto

Dabei kann für das Anlegen eines Benutzerkontos unmittelbar auf folgenden Link verwiesen werden: 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 bei der Registrierung die IdNr zugrunde liegt. Diese sind vor allem für Bürger relevant, können aber im Ausnahmefall auch in diesem Portal/Antrag genutzt werden. Dies gilt ausschließlich für solche Organisationen, Selbständige oder Einzelunternehmerinnen, 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 (ausgestellt für Ihre Behörde oder Ihr Unternehmen) anmelden und im Rahmen des Onboardings strukturiert Ihre Vorhaben beschreiben. Später können Sie Ihre Service Provider selbst 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 Self Service Portal / 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.

The screenshot shows the 'MUK SELF SERVICE PORTAL' interface. At the top left, there is a logo and the text 'MUK SELF SERVICE PORTAL'. On the right, there is a user profile icon and the text 'Move3 Test GmbH'. Below the header, there is a navigation bar with four items: 'Meine Vorhaben', 'Meine Postfachrechte', 'Informationen & Hilfe', and 'News'. The main content area contains several paragraphs of text providing instructions on how to apply for a project. At the bottom of the page, there is a prominent blue button labeled 'Vorhaben beantragen'.

Herzlich Willkommen bei der Antragstellung für Vorhaben des Self-Service Portals (SSP)!

Auf den folgenden Seiten können Sie für das Vorhaben, das Sie an die NEZO*-Schnittstelle anbinden möchten, einen Antrag stellen. Dabei werden Informationen zur beantragenden Person, zur Auftrag gebenden Behörde sowie zum Vorhaben selbst abgefragt. Die Vollständigkeit sowie Richtigkeit Ihrer Angaben ist dabei essentiell, um das Vorhaben prüfen zu können. Falls Sie als Dienstleister im Namen einer Behörde handeln, so bitten wir Sie, die von uns zur Verfügung gestellte Vollmacht dem Antrag unterschrieben im PDF-Format anzuhängen. Die Vollmacht finden Sie auf den folgenden Seiten.

Nach dem Absenden des vollständigen Antrags wird dieser vom Bayerischen Staatsministerium für Digitales und vom Bayerischen Landesamt für Steuern geprüft. Daraufhin erhalten Sie via Mail Rückmeldung, ob das Vorhaben zur Anbindung an die NEZO-Schnittstelle genehmigt wird. Damit die Prüfung des Antrags zügig durchgeführt werden kann, bitten wir Sie, auf eventuelle Rückfragen zeitnah zu antworten.

Wird das Vorhaben genehmigt, so finden Sie alle zusätzlichen Informationen zum weiteren Vorgehen zur Anbindung in Ihrem persönlichen Bereich des SSPs. Sobald die technische Anbindung des Vorhabens umgesetzt ist und alle weiteren Voraussetzungen erfüllt sind, wird das Vorhaben nach erneuter Prüfung letztendlich zur öffentlichen Nutzung freigeschaltet.

Sollte das Vorhaben abgewiesen werden, erfahren Sie dies ebenso via Mail mit Angabe der Abweisungsgründe. Grundsätzlich können Sie dennoch weitere Anträge zu anderen Vorhaben im SSP stellen.

Sie können nun direkt mit Ihrem Antrag starten - der Antragsprozess auf den nachfolgenden Seiten ist selbsterklärend.

Wir freuen uns darauf, Sie als NEZO-Partner begrüßen zu dürfen!

Ihr Team des SSP

*NEZO = Nutzung der ELSTER-Zertifikate im Rahmen des Onlinezugangsgesetzes

Vorhaben beantragen

Abbildung 2 Anmeldemaske im SSP

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

MUK SELF SERVICE PORTAL Rupert Dahhaas

Meine Vorhaben | Informationen & Hilfe | News

Antrag auf NEZO-Vorhaben

Verantwortlichkeiten | **Vorhaben**

Beantragende Person

Als „beantragende Person“ sind Sie dazu in der Lage, ein Vorhaben an das SSP zu übermitteln und dieses im weiteren Prozess zu administrieren. Dafür werden folgende Daten von Ihnen benötigt.

Vorname* Nachname*

Organisation *

Straße * Hausnummer * Postleitzahl * Ort *

Telefonnummer* Rolle* Verantwortlicher beim Dienstleister Verantwortlicher beim Auftraggeber

E-Mail* E-Mail (wiederholen)*

Notwendige Bestätigungen für den Abschluss des Antrags

Hiermit bestätige ich, den Antrag auf o in Vorhaben aufgrund bestehendem / zukünftigem behördlichen Interesse an den Schnittstellen zur Anbindung des Unternehmenskontos auszufüllen. In meiner Funktion als Antragsteller bin ich für die Administration des Vorhabens im SSP verantwortlich und diene zunächst als erster Ansprechpartner für das Vorhaben.*

Hiermit bestätige ich die Richtigkeit der eingegebenen Daten.*

Des Weiteren ist mir bewusst, dass die Schnittstelle(n) für das Vorhaben nur unter folgenden weiteren Voraussetzungen für die öffentliche Nutzung freigeschaltet werden kann:*

- Erfolgreiche technische Implementierung der Schnittstelle für das beantragte Vorhaben
- Verhandeln einer rechtlichen Grundlage (z.B. Bund-Länder-Rahmenvereinbarung, Verwaltungsvorschrift, Verwaltungsvereinbarung)

Hiermit bestätige ich, dass ich mit der Weiterverarbeitung der eingegebenen Daten einverstanden bin.*

Hiermit bestätige ich, die **Vertraulichkeitsvereinbarung** gelesen zu haben und zu akzeptieren.*

Hiermit bestätige ich, die **Nutzungsbedingungen** gelesen zu haben und zu akzeptieren.*

Hiermit bestätige ich, dass ich bei der Integration eines Login-Buttons ausschließlich den Begriff „Mein UK“ oder „Mein Unternehmenskonto“ verwenden werde.*

Weitere Ansprechpartner

Hier haben Sie die Möglichkeit, weitere Ansprechpartner (ggf. Dienstleister / weitere involvierte Behörden) des Vorhabens anzufügen.

Name	Organisation	Rolle	Telefonnummer	E-Mail
Aktuell keine Einträge				

Abbrechen Weiter

Abbildung 3 Antrag auf NEZO-Vorhaben: Angaben zur beantragenden Person

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

Abbildung 4 Antrag auf Vorhaben, Reiter Vorhaben

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

2.3 Schritt 3: Auswahl des für Sie relevanten Rechtsrahmens 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 Rechtsrahmens

ELSTER kann individuell pro angeschlossenem Service Provider unterschiedliche SAML-Assertion-Attribute zurückgeben. Die Attribute werden dabei über den gewählten Rechtsrahmen verfügbar (was dürfen wir Ihnen übermitteln) und durch Sie selbst in der Attributkonfiguration ausgewählt. Bedenken Sie dabei das Gebot der Datensparsamkeit in der DSGVO.

Eine Auflistung der aktuell verfügbaren Attribute findet sich im Kapitel "Konfiguration von benötigten Attributen".

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

- Organisations-/Unternehmenszertifikate, die mit der StNr der jeweiligen Organisation registriert wurden. Dies sind Einzelunternehmer, juristische Personen (Unternehmen, Behörden, etc.), die über eine deutsche StNr verfügen, weil sie in Deutschland steuerpflichtig sind. Es können bis zu 17.000 Konten pro Steuernummer registriert werden.
- Persönliche Zertifikate, die mit der persönlichen steuerlichen Identifikationsnummer (IdNr) registriert wurden. Dies sind 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.

Je nach auf Ihrer Seite angebotenen Fachverfahren können Sie auf Seiten des ELSTER Identity Providers (ELSTER-IdP) die für Sie relevanten Typen konfigurieren. Sind ausschließlich StNr-Zertifikate für Sie relevant, so kann der ELSTER-IdP die anderen Zertifikatstypen "herausfiltern" und abweisen. Privatpersonen sollten laut OZG grundsätzlich über die BundID abgedeckt werden.

2.3.3 Benötigen Sie Testzertifikate für produktive Smoke-Tests?

Unter Umständen haben Sie Bedarf an "Smoke-Tests" Ihres Echtsystems gegen das ELSTER Echtssystem. 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 Echtdateien 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 eGovernment-dienste") 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 angebotenen 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 SingleLogout-Service 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.

Meine Vorhaben
Informationen & Hilfe

Herzlich willkommen

Verwalten Sie Ihre Service Provider im NEZO-Verbund

Ausgewählte Dokumente

- [Integrationsleitfaden NEZO](#)
- [Integrationsleitfaden Postfach](#)
- [Aktuelle Release Notes NEZO](#)

Meine Vorhaben

[+ Hinzufügen](#)

Status · Genehmigt, Warten auf Genehmigung, Bitte ...

Name	Organisation	URL	Status	Anlagdatum
Ministry of silly walks	Hans Klein AG	www.ministryofsillywalks.de	Genehmigt	25.01.2022 15:51

Abbildung 5 Übersicht Meine Vorhaben

In dem ausgewählten Vorhaben können Sie nun die Konfiguration Ihrer Service Provider (SAML-Endpunkte) vornehmen. Zu Integrationszwecken können Sie beliebig viele Konfigurationen in der E4K-Testumgebung anlegen. Für das Produktivsystem sollten Sie nur einen Service Provider verwenden. Um ggf. Systemumzüge o.Ä. zu verwalten, erlaubt das System bis zu zwei produktive Service Provider. 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. Die Genehmigung eines produktiven Service Providers erfolgt erst, wenn in unseren Logs ein erfolgreicher Test in der E4K-Testumgebung sichtbar ist.

The screenshot shows the 'Service Provider' configuration page in the MUK Self Service Portal. The page is divided into two main sections: 'Produktion' and 'Testumgebung'. The 'Produktion' section has a 'Service Provider beantragen' button and a message 'Aktuell kein Produktion Service Provider beantragt'. The 'Testumgebung' section has a 'Service Provider beantragen' button and a table with columns for 'Name', 'Status', and 'Angelegt am'. The table is currently empty, with a message 'Aktuell sind keine Service Provider angelegt' below it. The status 'Genehmigt (live), Warten auf Genehmigung' is shown in a dropdown menu. The page header includes 'Meine Vorhaben', 'Informationen & Hilfe', and 'News'. The top navigation bar shows 'Zurück zur Übersicht', 'Vorhabensdetails', 'Name: Ministry of silly walks', 'URL: www.ministryofsillywalks.de', and 'Vorhabensverantwortlicher: Martin Fechtelhoff'.

Abbildung 6 Service Provider

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.
- **Rechtsrahmen:** Legen Sie fest, ob Sie im Rahmen des Onlinezugangsgesetzes (OZG) oder im Rahmen der Abgabenordnung (AO) handeln.
- **Zum Login zugelassene(s) Ordnungsmerkmal(e):** Wählen Sie, ob Sie nur Konten von Organisationen (StNr) oder auch Konten von natürlichen Personen zulassen möchten (IdNr).
- **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 Rechtsrahmens 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.

Service Provider Konfiguration in der E4K-Testumgebung



Allgemein

Bezeichnung des Service Providers* <input type="text" value="Demo Service Provider"/>	Entity-ID (SP-ID)* <input type="text" value="demo.serviceprovider.com"/>
--	---


Konfiguration (Allgemein)

Rechtsrahmen* <input type="text" value="Onlinezugangsgesetz"/>	Zum Login zugelassene(s) Ordnungsmerkmal(e)* <input type="text" value="IdNr, StNr"/>
---	---

Liveschaltung sofort bei Genehmigung durch einen Sachbearbeiter*



Konfiguration (Anzeige)

Name des Portals* <input type="text" value="Testportal"/>	Portal-Logo* 
URL der Startseite Ihres Portals* <input type="text" value="https://mein-unternehmenskonto.de"/>	<small>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.</small>
Portalbeschreibung bzw. angezeigte Beschreibung* <input type="text" value="Test Service Provider"/>	

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 Antrags 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\('Base64'\)](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 URL:** Eine URL, 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 geschickt. Siehe auch Kapitel "Schritt 3: Auswahl des für Sie relevanten Rechtsrahmens 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.

Entity Descriptor

Nachfolgend geben Sie bitte unter "Signaturzertifikat 1" das Zertifikat an, mit dem wir Ihre SAML-Requests prüfen können. Im Falle eines Zertifikatswechsels können Sie später auch ein zweites Signaturzertifikat unter "Signaturzertifikat 2" hinterlegen mit dem wir Ihre SAML-Requests zusätzlich prüfen, sodass Sie in Ihrem System einen Wechsel durchführen können wenn Sie wollen. Nach der Umstellung Ihres Systems sollten Sie hier das "Signaturzertifikat 1" durch das "Signaturzertifikat 2" ersetzen.

Unter "Verschlüsselungszertifikat" geben Sie bitte das Zertifikat an, mit dem wir unsere SAML-Antworten für Sie verschlüsseln sollen. Wenn Sie Ihr Verschlüsselungszertifikat tauschen wollen, dann ertüchtigen Sie zuerst Ihre Anwendung dass diese sowohl das "alte" und das "neue" Zertifikat unterstützt und stellen dann hier Ihr neues Verschlüsselungszertifikat ein.

Signaturzertifikat 1*

```
MIIFUzCCBAegAwIBAgIEO5rKjBBBgkqhkiG9w0BAQowNKPMA0GCWCSAFIAwQCAQUAoRwwGgYJKoZIhvcNAQEI...
BgnVBAoTBKvSc3RicjELMAkGA1UECXMCMQ0eXZAVBgNVBAMTDkVsc3Ric3RiYXN0B0NBMB4XDTE5MDczMTEyMDA0M1oXDTE0MTIzMTIzMDA0M1owOzELMAkGA1UEBHMCREUxDzANBgNVB...
```

Signaturzertifikat 2 (optional)

Verschlüsselungszertifikat*

```
MIIFUzCCBAegAwIBAgIEO5rKjBBBgkqhkiG9w0BAQowNKPMA0GCWCSAFIAwQCAQUAoRwwGgYJKoZIhvcNAQEI...
BgnVBAoTBKvSc3RicjELMAkGA1UECXMCMQ0eXZAVBgNVBAMTDkVsc3Ric3RiYXN0B0NBMB4XDTE5MDczMTEyMDA0M1oXDTE0MTIzMTIzMDA0M1owOzELMAkGA1UEBHMCREUxDzANBgNVB...
```

Assertion Consumer Service URLs

URL* 📘

Abbildung 7 Entity Descriptor

Manage Name ID URL

URL 📘

Single Sign on and Single Logout

Für die Teilnahme am Single Sign on Verbund (SSO) sind URLs und deren technische Implementierung notwendig. Da die Protokolle HTTP-POST und SOAP zum Einsatz kommen, können Sie wahlweise eine oder zwei URLs angeben. **Lassen Sie die Felder leer, wenn Sie den Single Sign On Service nicht oder erst später umsetzen.** Das Ausfüllen der Single Logout Service URL aktiviert die Teilnahme am SSO-Verbund.

Single Logout Service URL 📘

Session Termination URL 📘

Abschließend wählen Sie noch die Attribute, die Sie für Ihren Online Dienst benötigen. Bedenken Sie dabei die gesetzlichen Anforderungen zur Datensparsamkeit. Details dazu finden Sie im Kapitel "Konfiguration von benötigten Attributen".

Attribute

Zwingend benötigt	Wenn vorhanden	Nutzer entscheidet	Nicht benötigt
2	0	0	23

Attribute bearbeiten

Abbrechen Speichern

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.

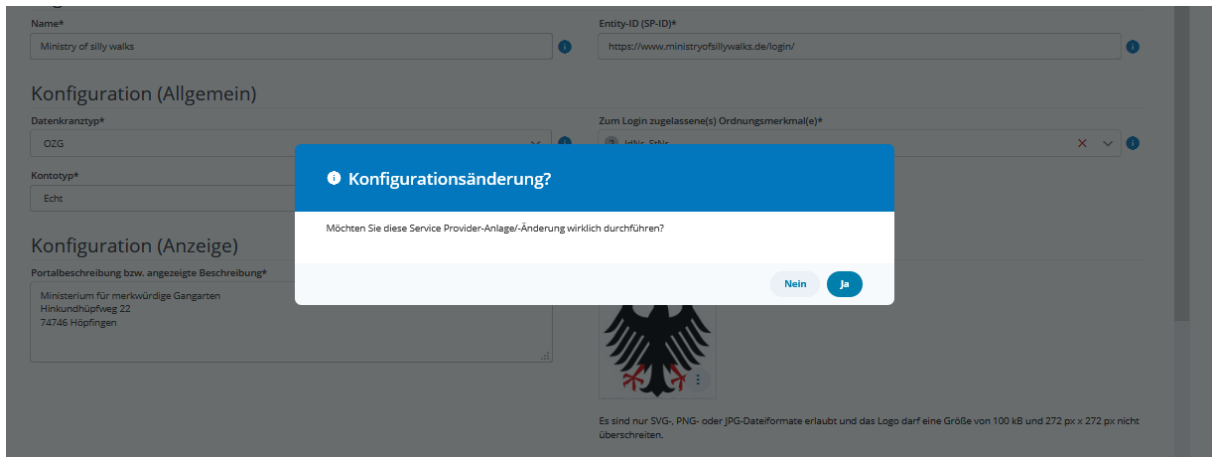


Abbildung 8 Konfigurationsänderung

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

2.5 Schritt 5: Kontinuierliche Administration Ihres Vorhabens im Self Service Portal

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 Konfiguration von benötigten Attributen

Im Self Service Portal legen Sie pro Service Provider fest, welche Attribute Ihnen in der SAML-Response übermittelt werden sollen. Sie sind dafür verantwortlich, die Konfiguration so Datensparsam wie möglich zu gestalten.

Sie haben dabei grundsätzlich folgende Möglichkeiten

Datenerfordernis	Bedeutung	Hinweise
Zwingend benötigt	Das betroffene Attribut wird von Ihrem SP immer benötigt. Ist es nicht in den ELSTER-Stammdaten vorhanden, wird der Login durch den Identity-Provider (also uns) mit einer Fehlermeldung abgelehnt.	Achtung: Ist ein Attribut mit der Verfügbarkeit "Basis" gekennzeichnet, ist es in unseren Daten immer vorhanden. Bei Attributen der Verfügbarkeit "Zusatz" kann es sein, dass diese in den Stammdaten nicht immer vorhanden sind. Überlegen Sie daher gut, ob Sie für solche Attribute "Zwingend benötigt" wirklich erzwingen wollen.
Wenn vorhanden	Das betroffene Attribut wird immer mitgeschickt, wenn es in den Stammdaten vorhanden ist.	Wir empfehlen die Auswahl "Wenn vorhanden", wenn Sie "Zusatz"-Attribute benötigen.
Benutzer entscheidet	Dem Nutzer wird auf der Datenweitergabeseite während des Login-Prozesses die Möglichkeit gegeben, ein Attribut abzuwählen.	Dies ist als datensparsame Komfort-Option für die Anwender vorgesehen. Achten Sie darauf, dass ein Nutzer solche Attribute bei Ihnen ggf. auch selbst erfassen könnte, falls Sie diese benötigen. Beispiel: E-Mail Adresse.
Nicht benötigt	Das Attribut wird nicht übermittelt und auch nicht auf der Datenweitergabeseite angezeigt.	

3.1 Voraussetzung: Rechtsrahmen

Rechtsrahmen	Erläuterung
OZG (Onlinezugangsgesetz)	In der Regel erfolgt die Anbindung an Mein Unternehmenskonto unter den Voraussetzungen des OZG. Anbindungspartnern steht ein bestimmtes Set an Attributen zur Verfügung.
AO (Abgabenordnung)	Einzelne Integrationen sind Sonderfälle und können weitere Attribute nach den Regelungen der Abgabenordnung erhalten. Dies muss entsprechend vorab abgestimmt und genehmigt werden.

3.2 Verfügbarkeit von Attributen

Die Spalte "Verfügbarkeit" gibt an, ob ein Attribut in den Stammdaten immer enthalten ist, oder ob es sich um ein optionales Attribut handelt. Basis = Attribut ist immer verfügbar; Zusatz: Attribut ist nicht immer verfügbar.

Tipp: Wird ein Attribut mit Verfügbarkeit "Zusatz" auf Datenerfordernis "Zwingend benötigt" gesetzt, scheitert der Login, wenn das Attribut im Datensatz des Nutzers nicht vorhanden ist. Wir empfehlen daher, überwiegend mit "Wenn vorhanden" zu arbeiten.

4 Übersicht und Erklärung möglicher Attribute

Die Verwendung einzelner Attribute ergibt sich auch aus dem Rechtrahmen Ihrer Anwendung. **In der Regel ist dies das OZG. Folglich stehen Ihnen alle Attribute mit "Ja" in der Spalte OZG grundsätzlich zur Verfügung.**

4.1 Allgemeine Attribute zu allen Konten

Die folgenden Attribute sind zu allen Konten vorhanden, werden ggf. nur durch den Rechtsrahmen eingeschränkt. Attribute, die nicht im SSP konfigurierbar sind, sind immer in der SAML-Response enthalten.

MEIN UNTERNEHMENS- KONTO

Name	SAML value	Datentyp	Zeichenlänge	Verfügbarkeit	Rechtsrahmen			Zugelassene Ordnungsmerkmale			In SSP konfigurierbar	Bemerkung
					AO	OZG	Intern	STNR	IDNR	BZSTNR		
NameID	Nameld	saml:Nameld-Type	43	Basis	Ja	Ja	Ja	Ja	Ja	Ja	Nein	<p>Anhand der Nameld erkennen Sie ein einzelnes ELSTER-Konto wieder. Es handelt sich um eine pseudonymisierte Benutzerkonto-ID. Die NameID ist eindeutig pro Benutzer und Service Provider.</p> <p>Format "ek-<40 Hexadezimalzeichen>", "ek" steht hierbei für ELSTER-Konto, bspw. ek-3bd72e6f67f0ff13e355b5eab2dab0ec3fdffb99.</p> <p>Die NameID wird als EncryptedID in der SAML-Assertion übertragen.</p>
Vertrauensniveau der Authentifizierung	ElsterVertrauensniveau Identifizierung	ekona:VertrauensniveauType	12	Basis	Ja	Ja	Ja	Ja	Ja	Ja	Ja	"SUBSTANZIELL" für alle, die per Brief oder persönlich identifiziert wurden. "HOCH" für die mit nPA
Vertrauensniveau der Authentifizierung	ElsterVertrauensniveau Authentifizierung	ekona:VertrauensniveauType	12	Basis	Ja	Ja	Ja	Ja	Ja	Ja	Ja	"SUBSTANZIELL" für alle NEZO Token (Zertifikatsdatei/Sicherheitsstick/Signaturkarten)

MEIN UNTERNEHMENS- KONTO

Identifizierung												
E-Mail-Adresse	EMailAdresse	xs:string	256	Basis	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Die E-Mail Adresse, die von der Registrierung an im ELSTER-Benutzerkonto hinterlegt wurde. (Warnung) Achtung: Die E-Mail-Adresse ist bei ELSTER nicht eindeutig nur einem Account zugeordnet! Verschiedene Accounts können dieselbe E-Mail Adresse hinterlegt haben.
Testkonto	IstTestkonto	xs:boolean	5	Zusatz	Ja	Ja	Ja	Ja	Ja	Ja	Nein	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_NICHT_MOEGLICH: Die Verarbeitung ist für Echt-Zertifikate nicht erlaubt." wenn mit einem Testkonto auf Echtkonten zugegriffen werden sollte.

MEIN UNTERNEHMENS- KONTO

AccountID	AccountID	xs:string		Basis	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Die AccountID wird nur in Sonderfällen nach vorheriger Abstimmung genehmigt. Zur Identifizierung eines Kontos nutzen Sie bitte die standardmäßig übermittelte NameID
-----------	-----------	-----------	--	-------	----	------	----	----	----	----	----	--

4.2 Attribute zu Konten mit Steuernummer

Name	SAML value	Datentyp	Zeichenlänge	Verfügbarkeit	Rechtsrahmen			Zugelassene Ordnungsmerkmale			Konfigurierbar	Bemerkung
					AO	OZG	Intern	STNR	IDNR	BZSTNR		
PersonaTyp	PersTyp	ekona:PersTypType	8	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Gibt an, ob die wirtschaftliche Tätigkeit der Organisation einer natürlichen "NatPers" oder einer nicht-natürlichen (juristische) Person "NNatPers" zugeordnet ist.
Datenübermittler-ID	DatenuebermittlerPseudonymId	xs:string	43	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Jede Organisation (Firma, Behörde, ...) erhält eine eindeutige ID, an der Sie Konten dieser Organisation erkennen können. Der Präfix "du-" steht für Datenübermittler. (Warnung)Hinweis: Es kann mehrere 1000 Accounts/Zertifikate mit unterschiedlichen pseudonymisierte Benutzerkonto-IDs pro Organisation (repräsentiert durch eine DatenuebermittlerPseudonymID) geben.
Firmenname (V1)	Firmenname	xs:string	120	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Bei FirmennameV1 wird der Name immer als Firmenname angezeigt und weitergegeben. Verwendet wird entweder der hinterlegte Firmenname (bei nicht natürlichen Personen) bzw. (bei

MEIN UNTERNEHMENS- KONTO

												natürlichen Personen) der Betriebsname (falls vorhanden) oder der Vor- und Nachname (bei nicht natürlichen Personen ohne Betriebsname).
Firmenname, Betriebsname mit Inhaber (V2)				Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Bei FirmennameV2 wird der Name entweder als Firmenname oder als Betriebsname sowie Vor- und Nachname angezeigt und weitergegeben. Der Firmenname V2 besteht aus folgenden Attributen mit den angegebenen Verfügbarkeiten und Einschränkungen: - Firmenname (Basis) nur bei nicht natürlichen Personen - Betriebsname (Zusatz) nur bei natürlichen Personen - Vorname (Zusatz) nur bei natürlichen Personen - Nachname (Basis) nur bei natürlichen Personen
	Firmenname	xs:string	120	Basis (NNat-Pers)	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
	Betriebsname	xs:string	120	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
	Vorname	xs:string	72	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
	Name	xs:string	72	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Betriebsgründungsdatum	betriebsGründungsDatum	xs:string	10	Zusatz	Ja	Nein	Ja	Nein	Nein	Nein	Ja	Das Datum, an dem die steuerliche Tätigkeit des Betriebs begonnen wurde.

MEIN UNTERNEHMENS- KONTO

												Entspricht NICHT dem Gründungsdatum lt. Handelsregister
Betriebs- endedatum	betriebsEnde- Datum	xs:string	10	Zusatz	Ja	Nein	Ja	Nein	Nein	Nein	Ja	Datum der Beendigung des Betriebs aus steuerfachlicher Sicht. Nur vorhanden, wenn dieses Datum zeitlich nach dem Gründungsdatum liegt.
Regis- tereintrag				Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
	Registernum- mer	xs:string	11	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Kann Daten enthalten, die folgendem regulären Ausdruck entsprechen: "[\d A-Z]{1,11}"
	Registerart	xs:string	4	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Es können folgende Registerarten zurückgegeben werden: HRA, HRB, VR, GR, PR, GnR, GesR
	Registerge- richt	xs:string	128	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Tätigkeit				Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
	Taetigkeit	xs:string	s. An- hang	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
	TaetigkeitText	xs:string	3	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Rechtsform					Ja	Ja	Ja	Ja	Nein	Nein	Ja	
	Rechtsform	xs:string	3	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Für PersTyp NNATPERS (Werteliste siehe Anhang)
	Rechtsform- text	xs:string	s. An- hang	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Für PersTyp NNATPERS (Werteliste siehe Anhang)

MEIN UNTERNEHMENS- KONTO

Umsatzsteuer-ID	UStId	xs:string	15	Zusatz	Ja	Nein	Ja	Ja	Nein	Nein	Ja	
Steuernummer	StNr	xs:string	13	Basis	Ja	Nein	Ja	Ja	Nein	Nein	Ja	StNr der Organisation im Bundeseinheitlichen StNr-Format
Adresse	Unternehmensanschrift	ekona:AdresseType			Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Typ	Adresse.Typ	xs:string	8	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	INLAND, AUSLAND oder POSTFACH
Straße	Adresse.Straße	xs:string	120	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Hausnummer	Adresse.Hausnummer	xs:string	25	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Postfach	Adresse.Postfach	xs:string	16	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Nur bei Adresstyp Postfach
PLZ	Adresse.PLZ	xs:string	12	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Ort	Adresse.Ort	xs:string	72	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Ortsteil	Adresse.Ortsteil	xs:string	50	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Adressergänzung	Adresse.Adressergänzung	xs:string	46	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Land	Adresse.Land	ekona:LaendercodeType	2	Basis	Ja	Ja	Ja	Ja	Nein	Nein	Ja	

MEIN UNTERNEHMENS- KONTO

Handelnde Person		Handelnde-Person		Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Komplexer Datentyp HandelndePerson
Vorname der handelnden Person	Vorname	xs:string	72	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Vorname der Person, die das Organisationzertifikat "bedient". Sofern dies durch den Anwender durch zusätzliche Identifizierung mit IdNr-Zertifikat selbst vorgenommen wurde
Nachname der handelnden Person	Nachname	xs:string	72	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Nachname der verknüpften handelnden Person
Namensvorsatz der handelnden Person	Namensvorsatz	xs:string	25	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Geburtsdatum der verknüpften handelnden Person
Namenszusatz der handelnden Person	Namenszusatz	xs:string	60	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Geburtsdatum der handelnden Person	Geburstdatum	xs:string	10	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	
Akademi-scher Grad der handelnden Person	Akade-mischerGrad	xs:string	30	Zusatz	Ja	Ja	Ja	Ja	Nein	Nein	Ja	

MEIN UNTERNEHMENS- KONTO

Funktionspostfächer		ekona:FunktionspostfächerType		Zusatz	Nein	Ja	Ja	Ja	Nein	Nein	Ja	Funktionspostfächer im Rahmen des OZG-PLUS-Postfachs (Baustein 5). Hinweis: Dieses Element ist nur in der SAML-Response enthalten, wenn der Service Provider, bei dem ein NEZO-Login durchgeführt wird, das OZG-PLUS-Postfach-Feature im SP-Antrag im SSP aktiviert hat, und die Organisation, dessen Konto für den NEZO-Login verwendet wird, Funktionspostfächer besitzt.
	Funktionspostfach	ekona:FunktionspostfachType		Zusatz	Nein	Ja	Ja	Ja	Nein	Nein	Ja	
	Anzeigename	ekona:AnzeigeNameType	50	Zusatz	Nein	Ja	Ja	Ja	Nein	Nein	Ja	
	ID	ekona:UUID-Type	36	Zusatz	Nein	Ja	Ja	Ja	Nein	Nein	Ja	
Bankverbindungen	Bankkonten			Zusatz	Ja	Nein	Ja	Ja	Nein	Nein	Ja	Das Attribut Bankkonten ist ein komplexer Datentyp und kann die folgenden Elemente enthalten
	Bankkonto			Zusatz	Ja	Nein	Ja	Ja	Nein	Nein	Ja	Das Attribut Bankkonto ist ein komplexer Datentyp und kann die folgenden Elemente enthalten
	IBAN	xs:string	22	Basis	Ja	Nein	Ja	Ja	Nein	Nein	Ja	
	BIC	xs:string	11	Zusatz	Ja	Nein	Ja	Ja	Nein	Nein	Ja	

MEIN UNTERNEHMENS- KONTO

	Kontoinhaber	xs:string	145	Basis	Ja	Nein	Ja	Ja	Nein	Nein	Ja	Name des Bankkontoinhabers. Es werden ausschließlich Kontoinformationen zurückgeliefert, bei denen der Steuerkontoinhaber (oder bei NatPers sein Ehegatte) Kontoinhaber sind.
--	--------------	-----------	-----	-------	----	-------------	----	----	------	------	----	---

4.3 Attribute zu Konten mit Identifikationsnummer

Name	SAML value	Datentyp	Zeichenlänge	Verfügbarkeit	Rechtsrahmen			Zugelassene Ordnungsmerkmale			Bemerkung	
					AO	OZG	Intern	STNR	IDNR	BZSTNR		Konfigurierbar
Steuerliche Identifikationsnummer	IdNr	xs:string	11		Ja	Nein	Ja	Nein	Ja	Nein	Ja	Steuerliche Identifikationsnummer
Akademischer Grad	AkademischerGrad	xs:string	30		Ja	Ja	Ja	Nein	Ja	Nein	Ja	
Vorname	Vorname	xs:string	72		Ja	Ja	Ja	Nein	Ja	Nein	Ja	Hinweis: Es gibt Konstellationen, bei denen kein Vorname vorhanden ist. Dies kann z.B. bei Personen mit südostasiatischem kulturellen Hintergrund der Fall sein.
Nachname	Name	xs:string	72		Ja	Ja	Ja	Nein	Ja	Nein	Ja	Der Nachname des Benutzers. Hinweis: In sehr seltenen Fällen werden Namensinformationen von den Meldebehörden nur im Vornamen-Element, manchmal jedoch nur im Nachnamen übermittelt
Namensvorsatz	Namensvorsatz	xs:string	25		Ja	Ja	Ja	Nein	Ja	Nein	Ja	
Namenszusatz	Namenszusatz	xs:string	60		Ja	Ja	Ja	Nein	Ja	Nein	Ja	

MEIN UNTERNEHMENS- KONTO

Geburtsdatum	Geburtsdatum	xs:string	10		Ja	Ja	Ja	Nein	Ja	Nein	Ja	Achtung: Gemäß (PassVwV Skt. 4.1.5.3) sind bei teilbekannten Geburtsdaten (Tag unbekannt, oder Tag und Monat unbekannt), die unbekannt Teile mit "XX" zu kennzeichnen.
Geburtsort	Geburtsort	xs:string	72		Ja	Ja	Ja	Nein	Ja	Nein	Ja	
Geburtsland	Geburtsland	xs:string	2		Ja	Ja	Ja	Nein	Ja	Nein	Ja	ALPHA-2 Länderkürzel nach ISO 3166-1. siehe Hinweis zu historischen Staaten.
Geburtsname	Geburtsname	xs:string	72		Ja	Ja	Ja	Nein	Ja	Nein	Ja	Achtung: Bis voraussichtlich November 2026 kann es vorkommen, dass der Geburtsname auch dann nicht übermittelt wird, wenn die Person eigentlich einen Geburtsnamen besitzt. Es sollte folglich kein Abgleich auf das Vorhandensein des Geburtsnamens erfolgen.
Anschrift	Anschrift	ekona:AdresseType			Ja	Ja	Ja	Nein	Ja	Nein	Ja	Alle Adressinformationen werden bei persönlichen-Zertifikaten mit IdNr in einem eigenen Datentyp zurückgegeben
Typ	Adresse.Type	xs:string	8	Basis	Ja	Ja	Ja	Nein	Ja	Nein	Ja	INLAND oder AUSLAND
Straße	Adresse.Straße	xs:string	120	Zusatz	Ja	Ja	Ja	Nein	Ja	Nein	Ja	
Hausnummer	Adresse.Hausnummer	xs:string	25	Zusatz	Ja	Ja	Ja	Nein	Ja	Nein	Ja	

MEIN UNTERNEHMENS- KONTO

Postfach	Adresse.Postfach	xs:string	16	Basis	Ja	Ja	Ja	Nein	Ja	Nein	Ja	In der Regel enthalten die Daten zu Konten mit Identifikationsnummer keine Postfachadressen, da die Meldeadresse kein Postfach sein kann.
PLZ	Adresse.PLZ	xs:string	12	Basis	Ja	Ja	Ja	Nein	Ja	Nein	Ja	
Ort	Adresse.Ort	xs:string	72	Basis	Ja	Ja	Ja	Nein	Ja	Nein	Ja	
Ortsteil	Adresse.Ortsteil	xs:string	50	Zusatz	Ja	Ja	Ja	Nein	Ja	Nein	Ja	
Adressergänzung	Adresse.Adressergänzung	xs:string	46	Zusatz	Ja	Ja	Ja	Nein	Ja	Nein	Ja	
Land	Adresse.Land	ekona:Laender-codeType	2	Basis	Ja	Ja	Ja	Nein	Ja	Nein	Ja	

4.4 Funktionale Attribute: Bausteinpseudonyme

Attributname	Datentyp	Optional	Anzeige	Weitergabe	Länge [Zeichen]	Rechtsahmen	Bemerkung
Bausteinpseudonyme	<p>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.</p> <p>Das Attribut Bausteinpseudonyme ist ein komplexer Datentyp (ekona:BausteinpseudonymeJwtType) und enthält eine Liste von "Pseudonyme"-Unterelementen.</p> <p>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.</p>						
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 Begrenzung, siehe Bemerkung	OZG	<p>Die Pseudonyme des Nutzers (NameID, bei StNr-Datenkranz auch DatenebermittlerPseudonymId), wie sie beim jeweiligen Baustein bekannte sind (siehe Attribut empfaenger).</p> <p>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".</p> <p>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.</p>

5 Einbindung von Mein Unternehmenskonto in die eigene Benutzeroberfläche

5.1 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 von SSP.

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

- Logout aus dieser Session

5.2 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, würden 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.

6 Schnittstelle Service Provider-ELSTER

6.1 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.

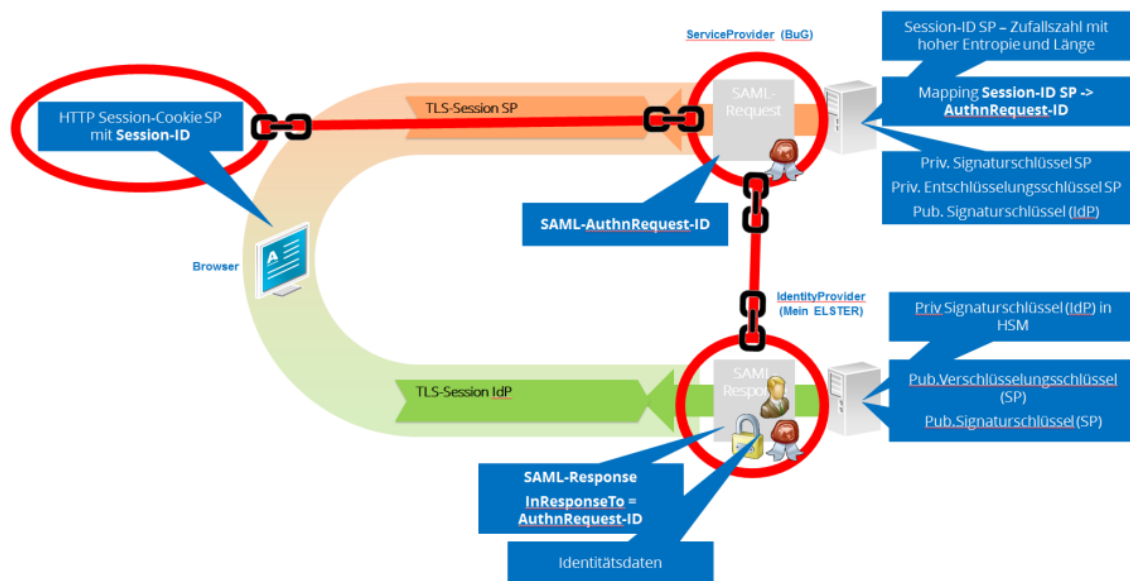


Abbildung 9 Bindung der Identität an den Sitzungskontext
 Der Client des Anwenders und die dort vorhandene Session mit dem Service Provider wird repräsentiert durch eine Session-ID, die clientseitig in einem Session-Cookie sicher abgelegt ist. Auf Seiten des Service Providers wird bei Erzeugung des SAML-AuthnRequest 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.

6.2 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.

6.3 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/e-kona/sso	SST zum Erhalt eines SAML-AuthnRequest
ELSTER (IdP)	https://www.elster.de/e-kona/slo	SST zum Erhalt eines SAML-LogoutRequests

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.

6.3.1 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
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.

6.3.1.1 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#" Algo-
          rithm="http://www.w3.org/2009/xmlenc11#mgf1sha256"/>
        </xenc:EncryptionMethod>
        <xenc:CipherData>
          <xenc:CipherValue>T5Yl900-
          GyUJXh36q4mTz9+q9C9mQ/noLZzvBCCz.....kED/uZwqlgQ4=</xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedKey>
    </ds:KeyInfo>
    <xenc:CipherData>
      <xenc:CipherVa-
      lue>s/ajt7nUWo/V9pl6xa3.....RJD+U5/7qYCyhSy+s=</xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</saml2:EncryptedAssertion>
```

```

        <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 Algo-
rithm="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 Algo-
rithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <ds:DigestValue>V3d+fWJyD9NdP7o16GkzHSbrl0sGVPYWygo-
vKpwSAiM=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>C4IdSURPe0sqXbgU/ttvCPXvNW3D04MrUhsGYlPaHg=</ds:Sig-
natureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>MIIEtTCCAp2gAwIBAgIGDQE.....05xrK-
hDCSXRdM+6UavvVmha/fsRlPbZ2gsSw</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>

```

```

    <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:element name="PersTyp" type="ekona:PersTypType" />

<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:element name="Datenquelle" type="ekona:DatenquelleType" />

<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:complexType name="FunktionspostfaecherType">
  <xs:sequence>
    <xs:element name="Funktionspostfach" type="ekona:FunktionspostfachType" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="FunktionspostfachType">
  <xs:simpleContent>
    <xs:extension base="xs:base64Binary">
      <xs:attribute name="ID" type="ekona:UUIDType" />
      <xs:attribute name="AnzeigeName" type="ekona:AnzeigeNameType" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="UUIDType">
  <xs:restriction base="xs:string">
    <xs:minLength value="36" />
  </xs:restriction>
</xs:simpleType>

```

```
        <xs:maxLength value="36" />
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="AnzeigeNameType">
    <xs:restriction base="xs:string">
        <xs:maxLength value="50" />
    </xs:restriction>
</xs:simpleType>

</xs:schema>
```

2.a) AllowCreate	"true", so dass ELSTER für den Benutzer einen neuen Pseudonym-Identifizier 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)

6.3.4.1 Beispiel-AuthnRequest-XML

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://demoserviceprovi-
  der.de/nez0/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:asser-
  tion">urn:de:elster:esig:demo-service-provider:nez0</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 Algo-
          rithm="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 Algo-
        rithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <ds:DigestValue>KQNjNjDAEW+c/Ra8va2CPJlb-
        bvZDaDDgK8YGmH1VskM=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>t9zTBexpag.....</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>MIIFPDCCAyQCCQCN9m57471R1TAN-
          Bgkq.....</ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </saml2:Signature>
    <saml2p:NameIDPolicy AllowCreate="true" />
  </saml2p:AuthnRequest>
```

- Der AuthnRequest muss erfolgreich geparkt 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 (SAML-Profiles, 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. Ist nach einem Zeitraum von ca. 30 Minuten keine Antwort auf den Request erfolgt, sollte der ServiceProvider davon ausgehen, dass der Request nicht erfolgreich

wr.
 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)

6.3.5 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)
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)

XML-Element / -Attribut	Beschreibung
3.1.1) <Issuer>	identisch zu 1)
3.1.2) <Subject>	Enthält Informationen über den authentifizierten Benutzer
3.1.2.1) <NameID>	<p>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).</p> <p>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.</p> <p>Die NameID enthält die für jeden ELSTER-Benutzer eindeutige, pseudonymisierte Benutzerkonto-ID, die gleichzeitig als Postfachhandle für das Postfach2.0 fungiert.</p>
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>	
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	<p>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).</p> <p>Der Zeitpunkt sollte nicht das Zeitfenster aus <Conditions> überschreiten (SAMLCore, Z. 756).</p>
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.

XML-Element / -Attribut	Beschreibung
3.1.3.1.1) <Audience>	Muss identisch zum Service Provider-Identifizier 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) AuthnInstant	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.
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 zurückgelieferten Attribute sind in den drei Tabellen des Unterabschnitts "Aufbau des Datenkranzes..." zu sehen

6.3.5.1 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>
```

in NEZO mit ihrem Vertrauensniveau markiert. Dies wird im Attribut ElsterVertrauensniveau-Identifizierung abgebildet.

6.3.5.2 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="_44e290994b4cble96f0b7157b868260e"
  Destination="https://demoserviceprovider.de/nez0/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:per-
sistent">ek-92429d82a41e930486c6de5ebda9602d55c39986
      </saml2:NameID>
      <saml2:SubjectConfirmation Method="urn:oasis:na-
mes:tc:SAML:2.0:cm:bearer">
        <saml2:SubjectConfirmationData InRespon-
seTo="_44e290994b4cble96f0b7157b868260e"
          NotOnOrAfter="2018-09-
26T14:55:32.045Z"
          Recipient="https://demoservice-
provider.de/nez0/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:clas-
ses:X509</saml2:AuthnContextClassRef>
      </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
      <saml2:Attribute Name="DatenebermittlerPseudonymId">
        <saml2:AttributeValue xsi:type="xs:string">du-
986b2b54ab89cf4ed674ad8c3126b966b54d4872</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute Name="ElsterVertrauensniveauIdentifizierung">
```

```

        <saml2:AttributeValue xsi:type="ekona:VertrauensniveauType">sub-
stanziell</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute Name="ElsterVertrauensniveauAuthentifizierung">
        <saml2:AttributeValue xsi:type="ekona:VertrauensniveauType">sub-
stanziell</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute Name="IstTestkonto">
        <saml2:AttributeValue xsi:type="xs:boolean">>true</saml2:Attribu-
teValue>
    </saml2:Attribute>
    <saml2:Attribute Name="PersTyp">
        <saml2:AttributeValue xsi:type="ekona:PersTypType">NNat-
Pers</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:Attribute-
Value>
    </saml2:Attribute>
    <saml2:Attribute Name="Registernummer">
        <saml2:AttributeValue xsi:type="xs:string">1234</saml2:Attribu-
teValue>
    </saml2:Attribute>
    <saml2:Attribute Name="Registerart">
        <saml2:AttributeValue xsi:type="xs:string">HRA</saml2:Attribute-
Value>
    </saml2:Attribute>
    <!-- ... usw. -->
</saml2:AttributeStatement>
</saml2:Assertion>
</saml2p:Response>

```

- 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/nez/acs>") übereinstimmen (SAMLProfiles Z.576). Ebenso **muss** diese URL mit dem Destination-Attribut der <Response> übereinstimmen (SAML-Core 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.

6.3.6 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 ManageNameID-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.
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.)

6.3.6.1 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://demoserviceprovi-
der.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:asser-
tion">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:persis-
tent">ek-92429d82a41e930486c6de5ebda9602d55c39986</saml2:NameID>
  <saml2p:Terminate/>
</saml2p:ManageNameIDRequest>
```

6.3.6.2 Prüfung des SAML-ManageNameIDRequest durch Service Provider

Wenn der Service Provider den ManageNameIDRequest über den Endpoint <https://demoserviceprovider.de/nezomni> erhält, so muss der ManageNameIDRequest unmittelbar überprüft werden.

Der Service Provider prüft dann zunächst folgende Eigenschaften:

- Der ManageNameIDRequest muss erfolgreich geparkt 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.

6.3.7 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.
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

6.3.7.1 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>
```

- Die ManageNameIDResponse muss erfolgreich geparkt 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.

6.3.8 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) <Session-Index>	<p>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.</p> <p>Wird kein SessionIndex angegeben, wird nach der Nameld aufgelöst und der Nutzer aus allen SSO-Sessions ausgeloggt.</p>	

```
<?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:SessionIndex>
</saml2p:LogoutRequest>
```

6.3.9 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.

6.3.9.1 Prüfung des LogoutRequests durch ELSTER

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

- Der LogoutRequest muss erfolgreich geparkt 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.

6.3.9.2 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/nez/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

XML-Element / - Attribut	Beschreibung (IdP zu SP)	Beschreibung (SP zu IdP) "Session-Termination- Response"
1) <Issuer>	https://www.elster.de	https://www.demoserviceprovider.de
2) <Status>	<p>SAML-konforme Erfolgsmeldung</p> <p>SUCCESS = "urn:oasis:names:tc:SAML:2.0:status:Success"</p> <p>wird ausgegeben, wenn eine Globale Logout-Benachrichtigung an alle SSO-Session-Teilnehmer versandt werden konnte.</p> <p>SamlStatusCode - Hinweis</p> <p>Wenn der SP, der den Logout initiiert, selbst kein passendes SOAP-Binding hinterlegt hat, oder nicht alle SSO-session-Teilnehmenden SP technisch erreichbar sind, geben wir statt Statuscode</p> <p>SUCCESS = "urn:oasis:names:tc:SAML:2.0:status:Success"</p> <p>einen Statuscode mit Statusmessage</p> <p>PARTIAL_LOGOUT = "urn:oasis:names:tc:SAML:2.0:status:PartialLogout" message = "Logout konnte für den initierenden ServiceProvider nicht vollzogen werden." minorCode = "0"</p> <p>zurück. Der PartialLogout ist für den Fall, dass kein Globaler Logout gewünscht ist und konfiguriert wurde, als Erfolg zu verstehen.</p>	<p>SAML-konforme Erfolgsmeldung:</p> <p>SUCCESS = "urn:oasis:names:tc:SAML:2.0:status:Success"</p>

```
<?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>
```

```
<?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>
```

6.3.10.1 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-Assertionen 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-post-fach">TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQ=.Y29uc2V0ZXR1ciBzYWRpchHNjaW5nIGVsaXRy.c2VkIGRpYW0gdm9udW15IGVpcm1vZCB0ZW1wb3I=

```

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.

6.3.11 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>
```

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.

6.4.1 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 deren 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-Endpoint des IdP (binding darf hier nicht geprüft werden).

7 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.

7.1 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
```

Hinweis: Das Zertifikat kann so noch nicht im SelfService-Portal 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.

7.2 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.

7.2.1 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.

7.2.2 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.

8 Troubleshooting

Im nachfolgenden sind häufige Probleme mit Ihren möglichen Ursachen aufgeführt. Sollten Sie ähnliche Probleme haben, dann gehen Sie bitte zuerst die einzelnen Problempunkte durch, bevor Sie eine Supportanfrage stellen.

8.1 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

8.2 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\('Base64'\)](https://gchq.github.io/CyberChef/#recipe=Parse_X.509_certificate('Base64'))) Kann dort das Zertifikat nicht erfolgreich geparkt 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.

8.3 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-Descriptor 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 Unternehmenskonto 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"

8.4 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.

8.5 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

8.6 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.

8.7 Ich möchte meinen ManageNameID-Service testen

1. Tragen Sie im "SelfService-Portal" 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.

9 Begriffsbestimmungen (Ergänzungen)

ELSTER-Testkonten: Vereinzelt 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 Aktivierungscode 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).

10 Anhang

10.1 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 EMail-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/>
- "SelfService-Portal" 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-inter-net.de/bsvwbund_17122009_IT464400311.htm.

10.2 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"
271	"Eingetragene 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"
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"

Rechtsform	RechtsformText
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"
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"

Rechtsform	RechtsformText
370	"Unternehmergesellschaft (haftungsbeschränkt)"
380	"Investment-Aktiengesellschaft"
381	"Investment-Kommanditgesellschaft"
382	"Sondervermögen"
390	"sonstige Kapitalgesellschaft"
391	"Investmentaktiengesellschaft"
450	"Europäische Genossenschaft"
460	"eingetragene Genossenschaft"
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"

10.3 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
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

10.4 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

10.5 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

10.6 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.