Bundeszentralamt
für Steuern

Kommunikationshandbuch ELMA-Standard 2.0

Standardisierte Datenübermittlung an das BZSt über die Massendatenschnittstelle ELMA
(verfahrensübergreifende technische Beschreibung)

Dokumenten-Version: 2.6
Stand: 27.01.2025

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

0. Informationen zum vorliegenden Dokument

Dokumententitel	Kommunikationshandbuch ELMA-Standard Standardisierte Datenübermittlung an das BZSt über die Massendatenschnittstelle ELMA (verfahrensübergreifende technische Beschreibung)
Verantwortlicher Autor	Bundeszentralamt für Steuern
Erstellt am	01.07.2020
Zuletzt geändert am	27.01.2025

0.1. Änderungshistorie

Dokument Version	**Datum**	**Änderung**
1.0	01.07.2020	Initiale Erstellung
1.1	18.08.2020	Kapitel 3.2: Aufnahme Hinweis zur Freischaltung nach Zertifikatsverlängerung Kapitel 3.3: Aufnahme Hinweis zum Public Key nach Generierung eines ELMA5-Zertifikats Kapitel 5.4: Ergänzung von Beschreibungen zur Konvertierung Kapitel 6: Redaktionelle Anpassungen und klarstellende Ergänzungen zur Übertragung von Dateien, insbesondere neue Beschreibung „Aufbau der Verbindung“ Kapitel 7: Redaktionelle Anpassungen

Dokument Version	Datum	Änderung
2.0	20.10.2021	Kapitel 0.2: Ergänzung weiterer Fachverfahren Kapitel 0.3.1: Hinweis auf Fremdanbieter aufgenommen Kapitel 6.1: Konkretisierungen zum XML-Upload Kapitel 7: Neues Kapitel 7.1 zum ELMA-Standard eingefügt Kapitel 7.2: Anpassung „Verarbeitungslauf“ in Tabelle 1 Kapitel 7.3: Information zur Namespace-Reihenfolge aufgenommen Kapitel 8.1.1: Verweis auf ELMA-Standard bzgl. ELMA Protokoll aufgenommen Kapitel 8.1.2: Fehlertext 8013 in Tabelle 5 angepasst Kapitel 9: Neues Kapitel „Referenzdokumente“ eingefügt und XSD zum ELMA-Standard abgelegt
2.1	30.11.2022	Allgemein: Aktualisierung auf ELMA-Standard 2.0
2.2	13.07.2023	Kapitel 0.2: Anpassung der Datenarten bei KOWA Kapitel 4.1: Anpassung Bezeichnung ‚Prüfumgebung‘ Kapitel 5: Anpassungen beim BOP-ELMA-Upload Kapitel 6.1.2: Anpassung Bezeichnung ‚Prüfumgebung‘ Kapitel 6.2.5: Anpassung Bezeichnung ‚Prüfumgebung‘, Anpassung Ausführungen zu Namenskonvention für die Datendatei Kapitel 8.2: Anpassung Bezeichnung ‚Prüfumgebung‘ Kapitel 9.2.1: Anpassung Bezeichnung ‚Prüfumgebung‘ Kapitel 9.3: Anpassung Bezeichnung ‚Prüfumgebung‘, Anpassung der Liste für Status Kapitel 9.4: Spezifizierung Timestamp Kapitel 10.1.1: Anpassung Bezeichnung ‚Prüfumgebung‘ Kapitel 10.2: Spezifizierung Timestamp und Erweiterung um optionalen Dateinamensbestandteil
2.3	29.08.2023	Kapitel 0.2: Anpassung Umstellungszeitpunkt bei den Fachverfahren KISTA, KOWA und FSAK Kapitel 9.4: Korrektur des Beispiels für eine Feedbackdatei

Dokument Version	Datum	Änderung
2.4	15.12.2023	Kapitel 9.4: Anpassung Erläuterung Element <Zeitstempel> und Beispiel Kapitel 10.2: Anpassung Erläuterung Element <Zeitstempel> und Beispiel Neues Kapitel 11.2: Beispiel für Namenskonventionen im Download-Verzeichnis‘ eingefügt

Dokument Version	Datum	Änderung
2.5	19.06.2024	Kapitel 0.2: Ergänzung weiterer Fachverfahren Neues Kapitel 0.4: Änderung des Schlüsselformats Kapitel 1.1.2: Ergänzung sicherheitsrelevanten Hinweises Kapitel 1.4: Änderungen Authentifizierung an der Übertragungskomponente Kapitel 2.2: Änderungen zur Authentifikation am ELMA-Server Neues Kapitel 2.3: Schlüssellebensdauer Kapitel 2.6: Anpassung zu ECDSA-Signatur Kapitel 3.1: Aktualisierung bei Registrierung im BOP Neues Kapitel 3.2: Erzeugung des Schlüsselpaars Kapitel 3.2: Änderung am Freischaltungsantrag BOP Entfernt Kapitel 3.3: Zertifikat im PEM-Format Kapitel 4.2: Korrektur Beispiel Kapitel 6.2.7: Erstellung einer Signaturdatei mit ECDSA Neues Kapitel 6.2.7.1: neue Anwendungsbeschreibung LINUX Neues Kapitel 6.2.7.2: neue Anwendungsbeschreibung MAC OS Neues Kapitel 6.2.7.3: neue Anwendungsbeschreibung Windows Kapitel 8.2: Aufbau der Verbindung mit dem neuen Schlüsselpaar Kapitel 8.3.1: Ergänzung Hinweis Signaturdatei zur Datenübermittlung Entfernt Kapitel 8.3.1.1: alter Anwendungsbeschreibung Linux Entfernt Kapitel 8.3.1.2: alter Anwendungsbeschreibung MAC OS Entfernt Kapitel 8.3.1.3: alter Anwendungsbeschreibung Windows Kapitel 8.6: Ergänzung Hinweis Signaturdatei zur Datenübermittlung Kapitel 8.7: Aktualisierung der Beispiele Entfernt Kapitel 8.8.1: PEM-Datei in das PPK-Format konvertieren Kapitel 8.8.2: Aktualisierung Ablaufbeschreibung Datenübertragung mit dem Programm WinSCP Kapitel 9.1: Ergänzung Feedbackdateien zur Eingangsprüfung Kapitel 9.2.3: Aktualisierung und Korrektur Beispiel Kapitel 9.3: Aktualisierung der Status und Fehlermeldungen Kapitel 10.2: Korrektur Namenskonvention Kapitel 11.2: Korrektur Namenskonvention

Dokument Version	Datum	Änderung
2.6	27.01.2025	Kapitel 0.2: Änderung der Datenart MiKaDiv Kapitel 0.4.: Festlegung des Enddatums der Umstellung Ende 2025 Kapitel 2.2: Korrektur der Anmeldedaten Neues Kapitel 3.2.1: PEM-Datei in das PPK-Format konvertieren Kapitel 8.2: Aktualisierung der Abbildungen Kapitel 8.8.1: Aktualisierung der Abbildungen

0.2. Teilnehmende Fachverfahren

Fachverfahren		Datenart	Gültig ab
ELStAM	Elektronische Lohnsteuerabzugsmerkmale	ELStAMKVPVDatenuebermittlung ELStAMKVPVRueckmeldung	01.04.2023
FSAK	Freistellungsaufträgekontrollverfahren (Meldewesen)	FSAK FSAKRM	01.04.2024
FSAK	Freistellungsaufträgekontrollverfahren (Auskunftswesen)	FSAKAuskunft FSAKAuskunftRM	01.04.2024
IBAN	IBAN-Meldung	IBANMeldung IBANMeldungRM	01.12.2023
KISTA	Kirchensteuerabzug auf abgeltend besteuerte Kapitalerträge	KISTA KISTARM	01.04.2024
KISTA	Kirchensteueradresslisten	KI KIRM	01.04.2025
KOWA	Kontenwahrheit	KOWAVM KOWAVMRM	01.04.2024
MiKaDiv	Mitteilungsverfahren Kapitalertragsteuer auf Dividenden aus Aktien und Hinterlegungsscheine	MiKaDiv MiKaDivRM	

Fachverfahren		Datenart	Gültig ab
MiKaDiv	Aktionärsregister	MiKaDivAktionaersregister MiKaDivAktionaersregisterRM	
OSS	One-Stop-Shop	OSSEUAufzeichnungen OSSEUAufzeichnungenRM OSSNonEUAufzeichnungen OSSNonEUAufzeichnungenRM IOSSAufzeichnungen IOSSAufzeichnungenRM	-
PUEG	PUEG – Datenabruf Elterneigenschaft und Anzahl Kinder (DaBPV)"	PuegRequest PuegResponse	01.11.2024
VATRefund-Inland	Umsatzsteuervergütung inländischer Unternehmer im Ausland	UStVEU UStVEURM	01.08.2022
VATRefund-Drittstaaten	Umsatzsteuervergütung ausländischer Unternehmer (Drittstaaten) im Inland	VVAEB VVAEBRM	01.08.2022

Tabelle 1: teilnehmende Fachverfahren

0.3. Aufbau und Zweck des Dokuments

Im vorliegenden Dokument wird das Verfahren zur Datenübermittlung von Massendaten über die Massendatenschnittstelle ELMA an das BZSt erläutert. Es enthält einen standardisierten verfahrensunabhängigen Teil I, in dem die grundlegenden technischen Voraussetzungen u.a. die Registrierung, Freischaltung, sowie die notwendigen Softwareinstallationen, beschrieben werden. In Teil II dieses Dokumentes wird die eigentliche Datenübertragung erläutert.
Die Informationen im Teil II beziehen sich auf die Fachverfahren *(vgl. Abschnitt 0.2)*, welche den in diesem Dokument beschriebenen Standardvorgaben für die ELMA-Übertragung unterliegen. Verfahrensspezifische Besonderheiten wurden in den entsprechenden Kapiteln kenntlich gemacht.

Zurzeit wird die elektronische Massendatenschnittstelle grundlegend überarbeitet. Die teilnehmende Fachverfahren werden sukzessive auf den neuen ELMA-Standard umgestellt, der Umstellungstermin ist der Spalte „Gültig ab“ in Abschnitt 0.2 Teilnehmende Verfahren zu entnehmen. Bitte verwenden Sie ab diesem Termin nur noch dieses Handbuch, vorherige Versionen verlieren ihre Gültigkeit.

Das ELMA Kommunikationsverfahren wurde für die Übertragung von Massendaten entwickelt. Die Zielgruppe sind Großkunden, wie z. B. Rechenzentren der Kreditwirtschaft. Es werden u. a. Kenntnisse in der Datenverarbeitung und Netzwerktechnik vorausgesetzt.
Die Massendatenschnittstelle ELMA stellt u.a. folgende Funktionen zur Verfügung:

- Massendatenübertragung via SFTP
- Verschlüsselte Datenübertragung mit Public-Key-Authentifizierung
- Verwendung offener Standards (alle Komponenten als OpenSource verfügbar).

Darüber hinaus besteht die Möglichkeit Massendaten, die dem ELMA XML-Schema entsprechen, über eine Schnittstelle im BZStOnline-Portal (Upload-Funktion) zu versenden.

Die nicht abschließende Aufzählung von Hard- und Software-Ausstattungen, Hinweise auf Seiten von Fremdanbietern und sonstige Tools liegen nicht in der Hoheit des BZSt und dienen lediglich beispielhaft der Bedienung der Massendatenschnittstelle.

0.4. Änderung des Schlüsselformats

Aufgrund der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) in der technischen Richtlinie TR-02102-4 müssen die bisher für die Massendatenschnittstelle verwendeten RSA-Schlüssel ersetzt werden.

Zum 23. Juli 2024 wird die Massendatenschnittstelle deshalb auf die Verwendung von ECDSA-Schlüsseln umgestellt. Anders als bisher werden diese Schlüssel nicht mehr dem

BOP-Zertifikat entnommen, sondern müssen vom Benutzer eigenständig generiert und mit dem ELMA-Server (über das BOP) ausgetauscht werden.

Gleichzeitig mit der Umstellung des Schlüsselformats ändert sich die Benutzerkennung zur Nutzung der ELMA-Schnittstelle von der BZSt-Nummer zur Benutzerkonto-ID. Zukünftig hat damit jedes Benutzerkonto eigene Verzeichnisse für den Up- und Download von Dateien.

Die Verwendung der bisherigen RSA-Schlüssel gemäß dem Kommunikationshandbuch in Version 2.4 bleibt für Nutzer, die am 23. Juli 2024 eine gültige ELMA-Freischaltung besitzen, für einen Übergangzeitraum bis voraussichtlich zum 31.12.2025 mit der bisherigen Verzeichnisstruktur möglich.

Teil I
Allgemeine Informationen

Die nachfolgenden Abschnitte des Teils I - Allgemeine Informationen - gelten für alle an ELMA angebundenen Fachverfahren und bieten einen Überblick über die technischen Voraussetzungen zur Nutzung der Massendatenschnittstelle ELMA (ELMA-SST).

1. Technische Voraussetzungen zur Nutzung der ELMA-SST

1.1. Systemvoraussetzungen

1.1.1. Für den Hardware-Einsatz

Die Systemvoraussetzungen für die Nutzung der Massendatenschnittstelle ELMA sind vom verwendeten Betriebssystem und dem zu übertragenden Datenvolumen abhängig. Die Mindestanforderungen für die jeweilige Hardware sind an den Vorgaben des jeweiligen Betriebssystems auszurichten.
Die Programme für die Datenübertragung sind durchgängig mit den normalen Betriebssystem-Ressourcen lauffähig.
Die freien Festplattenkapazitäten sind entsprechend den zu übertragenden Datenvolumen zu dimensionieren. Das System muss über die Möglichkeit eines Internetzugangs verfügen.

1.1.2. Für den Software-Einsatz

Für die Linux Betriebssystem-Derivate Suse, RedHat, Fedora, Debian werden in der Regel die OpenSSH-Module standardmäßig bei der Grundinstallation mit installiert. Die Nutzung der SSH-Programme sftp und von openssl ist somit sofort nach der Grundkonfiguration möglich. Das gleiche gilt auch für die UNIX-Derivate HP-UX, AIX, macOS und viele andere.
Für die Microsoft-Windows-Betriebssysteme sind kostenfreie Programme aus dem OpenSource-Umfeld nutzbar, die durch den Benutzer installiert werden müssen. Hier sind beispielsweise die Programme PuTTYgen, PSFTP, WinSCP, FileZilla und OpenSSL zu nennen.

In den Programmen PuTTY vor Version 0.81, WinSCP vor Version 6.3.3 und FileZilla vor Version 3.67.0 existiert eine Sicherheitslücke, die zur Kompromittierung Ihrer privaten Schlüssel führen kann. Achten Sie zu Ihrer eigenen Sicherheit bitte darauf, die genannten Programme nur in aktuellen Versionen einzusetzen.

1.2. Internetanbindung und Bandbreite

Für die Kommunikation mit dem ELMA-Server wird keine dezidierte Internetverbindung benötigt. In Abhängigkeit von dem zu übertragenden Datenvolumen ist eine entsprechende Bandbreite für den Internetzugang zu wählen.
Für die Datenübertragung ist senderseitig die Verwendung einer Datenkompression möglich. Der Kompressionslevel ist auf die Leistungsfähigkeit der Hardware abzustimmen.

1.3. Firewall Konfiguration

Bei der Verwendung einer Firewall ist beim Sender die Freischaltung der IP-Adresse des ELMA-Servers für Port 22 zu konfigurieren.

1.4. Identifizierung, Verbindung

Die Übertragungskomponente authentifiziert sich beim Zielsystem mittels PublicPrivate Key Verfahren (OpenSSH-Modul) und stellt so die Verbindung her.
Der Austausch der Public Keys erfolgt nach Überprüfung der Identität des Teilnehmers zwischen diesem Sender und dem ELMA-Server.
Die Verbindung besteht nur während der Datenübertragung und wird danach abgebaut.

1.5. Verfügbarkeit

Die ELMA-Kommunikationskomponente ist redundant ausgelegt. Eine Hochverfügbarkeit wird jedoch nicht garantiert. Durch planmäßige Wartungsarbeiten oder Betriebsstörungen kann es zu temporären Einschränkungen bei der Erreichbarkeit kommen.
Bei einem Verbindungsabbruch/Unterbrechung einer Datenübertragung erfolgt kein automatischer Wiederanlauf. Die Daten sind in diesem Fall erneut zu übertragen.

2. Technische Beschreibung der Kommunikation

2.1. Grundlagen

Die Massendatenschnittstelle ELMA kann benutzerorientiert konfiguriert werden.
Als Secure Shell (SSH) werden Protokolle und eine Sammlung von Anwendungen bezeichnet, durch deren Einsatz man eine verschlüsselte Verbindung zu einem entfernten Rechner herstellen kann. Die Protokollversion SSH-2 ermöglicht die Datenübertragung per SFTP.

Die Massendatenschnittstelle ELMA verwendet Public-Key-Authentifizierung und das SSH-2-Protokoll. Für die Übertragung ist nur SFTP zugelassen.

2.2. Authentifikation am ELMA-Server

Der Benutzername für die Anmeldung am ELMA-Server entspricht der Benutzerkonto-ID.
Für die Anmeldung am ELMA-Server wird eine Public-Key-Authentifikation verwendet.
Bei der Public-Key-Authentifizierung erzeugt der Benutzer ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel.
Der private Schlüssel wird ausschließlich auf dem Rechner des Benutzers gespeichert und sollte geheim gehalten werden. Der öffentliche Schlüssel wird mit dem Zielsystem ausgetauscht.
Bei der Authentifikation werden die Authentifikationsdaten mit dem privaten Schlüssel des Benutzers digital unterschrieben. Das Zielsystem verifiziert mittels öffentlichen Schlüssels die digitale Unterschrift und stellt so die Echtheit der Daten und die Identität des Benutzers fest. Um ein unberechtigtes Wiedereinspielen des Authentifikationstokens zu verhindern, wird eine Kombination aus Zeitstempel und Zufallszahl angewendet.
Das Schlüsselpaar muss vom Benutzer erzeugt werden. Der öffentliche Schlüssel wird im Rahmen der ELMA-Freischaltung mit dem ELMA-Server ausgetauscht.

2.3. Schlüssellebensdauer

Das für die Authentifikation am ELMA-Server verwendete Schlüsselpaar ist regelmäßig zu wechseln. Die Gültigkeit der auf dem ELMA-Server hinterlegten Schlüssel ist deshalb auf drei Jahre begrenzt. Nach Ablauf dieser drei Jahre muss ein neuer öffentlicher Schlüssel per ELMA-Freischaltungsantrag hinterlegt werden. Über den notwendigen Schlüsseltausch werden Sie per Nachricht in Ihr BOP-Postfach informiert. Ein vorzeitiger Schlüsseltausch ist jederzeit möglich.

2.4. Username und Passwort Authentifikation

Die Authentifikation über Username und Passwort ist an der Massendatenschnittstelle ELMA nicht möglich.

2.5. Verschlüsselung

Die Verbindung zum Server ist symmetrisch verschlüsselt. Dazu wird im Rahmen des Verbindungsaufbaus ein Schlüssel zwischen SFTP-Client und ELMA-Server ausgetauscht.
Der verwendete Verschlüsselungsalgorithmus wird während des Schlüsselaustauschs automatisiert zwischen Client und Server ausgehandelt.
Der Schlüssel wird in regelmäßigen Abständen (abhängig von der Dauer der Verbindung und der übertragenen Datenmenge) erneuert.

2.6. Digitale Signatur

Zu jeder Datei, die über die ELMA-Schnittstelle übertragen werden soll, muss eine korrespondierende Signaturdatei übermittelt werden. Die digitale Signatur wird durch den

Benutzer mit seinem privaten Schlüssel erstellt. Sie beweist die Urheberschaft des Benutzers und stellt die Integrität der XML-Datei sicher.

Für ELMA werden ECDSA-Signaturen im DER-Format genutzt. Die Hashfunktion ist abhängig von der elliptischen Kurve des Schlüssels SHA-256, SHA-384 oder SHA-512.

3. Registrierung und Freischaltung

Über die Massendatenschnittstelle ELMA können Daten zwischen beliebigen Endstellen und dem ITZBund als Dienstleister für das BZSt übertragen werden. Voraussetzung hierfür ist eine erfolgreiche Registrierung beim Fachverfahren im BZStOnline-Portal sowie die Freischaltung für das ELMA-Verfahren über das Antragsformular „Freischaltung zur Teilnahme am ELMA5-Verfahren“.

3.1. Registrierung am BZStOnline-Portal (BOP)

Zur Teilnahme am ELMA-Verfahren benötigen Sie neben der Anmeldung beim jeweiligen Fachverfahren im BZSt ein Benutzerkonto im BZStOnline-Portal (BOP)[1]. Sofern Sie dieses noch nicht haben, führen Sie hierzu eine Registrierung im BOP durch.
Erläuterungen zum Registrierungsablauf finden Sie auf den Hilfsseiten des BOP oder in diesem Kommunikationshandbuch. Aus technischen Gründen ist es wichtig, dass Sie im Rahmen der Registrierung bei den Login-Optionen den Login mit einer Zertifikatsdatei auswählen.
Bitte beachten Sie zudem, dass mit einem EOP-Benutzerkonto die Versendung von Daten über ELMA nicht möglich ist. In diesem Fall ist die Beantragung einer neuen BZSt-Nummer (beginnt in der Regel mit BZ oder BX) bei dem betreffenden Fachverfahren sowie die Durchführung einer ELMA-Freischaltung notwendig.
Durch die Registrierung im BOP erhalten Sie ein Benutzerkonto, das über seine Benutzerkonto-ID identifiziert werden kann. Die Benutzerkonto-ID ergänzt um das Präfix „elster-“ ist gleichzeitig die Senderkennung und ermöglicht den Zugang zum ELMA-Kommunikationsserver.

3.2. Erzeugung des Schlüsselpaars

Wenn Sie die Massendatenschnittstelle über SFTP nutzen möchten, benötigen Sie ein Schlüsselpaar, dessen Public Key Sie anschließend mit dem ELMA-Server austauschen müssen. Möchten Sie die Massendatenschnittstelle nur über die im BOP angebotenen Dienste (https://www.elster.de/bportal/formulare-leistungen/versandmassendaten) nutzen, ist die Erzeugung eines Schlüsselpaars nicht notwendig.

[1] www.elster.de/bportal

Das Schlüsselpaar muss dem Typ ECDSA entsprechen. Als elliptische Kurve darf NIST P-256, NIST P-384 oder NIST P-521 gewählt werden.

Mittels OpenSSL kann ein (verschlüsseltes) ECDSA-Schlüsselpaar mit der elliptischen Kurve NIST P-521 im PKCS#8-Format mit folgendem Befehl erzeugt werden:

```
openssl genpkey -aes-256-cbc -pass stdin -algorithm EC -out <
Dateiname > -pkeyopt ec_paramgen_curve:P-521 -pkeyopt
ec_param_enc:named_curve
```

Nach Absenden des Befehls müssen Sie ohne Eingabehinweis ein Passwort vergeben und die Eingabe nochmals mit Enter bestätigen. Der private Key wird mittels OpenSSL im PEM-Format abgespeichert und muss bei der Verwendung der Programme WinSCP oder FileZilla (oder anderen auf PuTTY basierende Programme) zur weiteren Verwendung in das PPK-Format umgewandelt werden, siehe Abschnitt 3.2.1.

Nach der Erzeugung des Private Keys können Sie den Public Key zur Übermittlung an den ELMA-Server mit dem folgenden OpenSSL-Befehl im X.509-SubjectPublicKeyInfo-Format erstellen:

```
openssl pkey -in <Pfad zum Private Key> -out <Dateiname des
Public Keys> -pubout
```

Darüber hinaus kann das Schlüsselpaar auch mit dem PuTTY Key Generator (PuTTYgen) erzeugt werden. Dabei ist in den Parametern als „Type of key to generate“ „ECDSA“ und als „Curve to use for generating this key“ „nistp256“, „nistp384“ oder „nistp521“ zu wählen.
Der Public Key kann im PuTTY Key Generator (in dem in RFC 5656, Abschnitt 3.1 beschriebenen Format) aus dem Feld „Key“ kopiert werden.
Der private Key kann im PuTTY-eigenen PPK-Format über den Button „Save private Key“ gespeichert werden. Eine Umwandlung des Formats ist nicht mehr notwendig.

Für die Signaturerstellung mit OpenSSL müssen Sie den mit dem PuTTY Key Generator erstellten Private Key noch konvertieren. Klicken Sie dazu in der Menüleiste de PuTTY Key Generators auf „Conversions“ und anschließend auf „Export OpenSSH key“ und speichern Sie den Private Key am von Ihnen gewünschten Speicherort ab.

3.2.1. PEM-Datei in das PPK-Format konvertieren

Sofern Sie für die Datenübertragung (vornehmlich unter Windows) die Programme WinSCP oder FileZilla (oder andere auf PuTTY basierende Programme) verwenden möchten, müssen Sie vorab die PEM-Datei in das PPK-Format konvertieren. In anderen Fällen, z.B. bei der

Verwendung von OpenSSH, kann die PEM-Datei direkt verwendet werden. Sollten Sie bereits einen Schlüssel im PPK-Format besitzen, entfallen die folgenden Schritte.

Die Konvertierung wird bei den aktuellen Versionen von FileZilla (ab 3.46.3 x) und WinSCP (ab 5.15 x) durch die Software, wie folgt dargestellt, selbst durchgeführt.

WinSCP

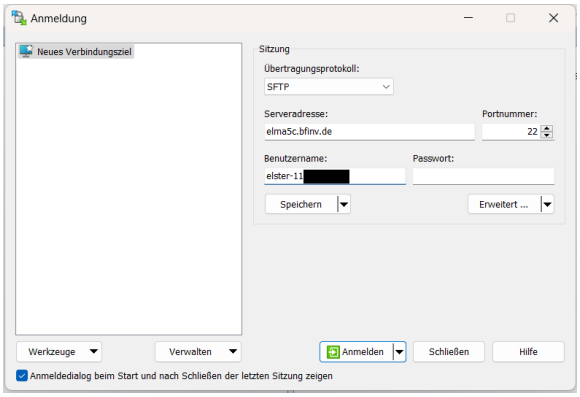

Abbildung 1: Anmeldemaske in WinSCP

Unter “Erweitert…“ > “Erweitert“ > “SSH“ > “Authentifizierung“ können Sie unter dem Menüpunkt “Authentifizierungsparameter“ Ihr ELMA5-Zertifikat hinterlegen.

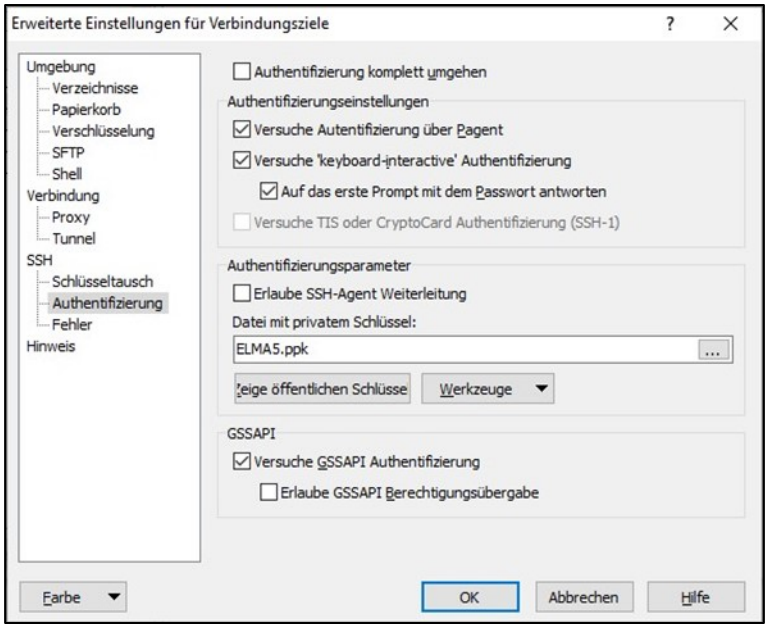

Abbildung 2: Einstellungsmaske im WinSCP

Abbildung 3: Bestätigungsfenster für die Konvertierung des Zertifikats

FileZilla

Unter “Bearbeiten“ > “Einstellungen…“ können Sie unter dem Menüpunkt “Verbindung“ > “SFTP“ Ihr ELMA5-Zertifikat hinterlegen.

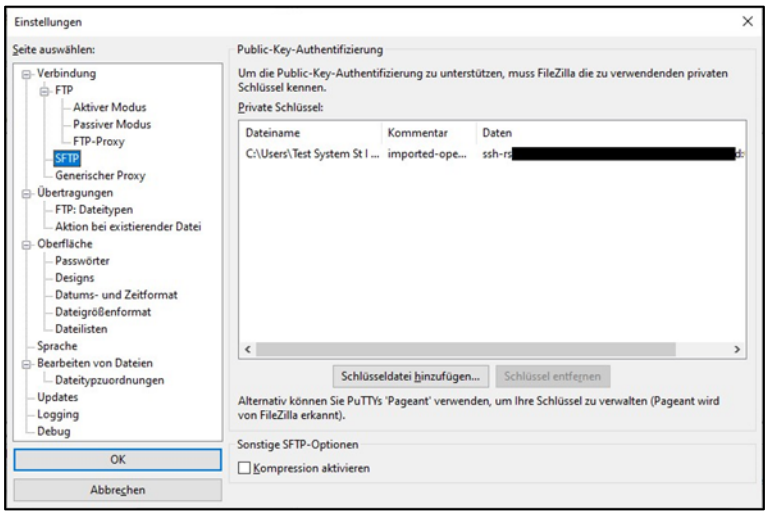

Abbildung 4: Abbildung 20: Einstellungsmaske im FileZilla

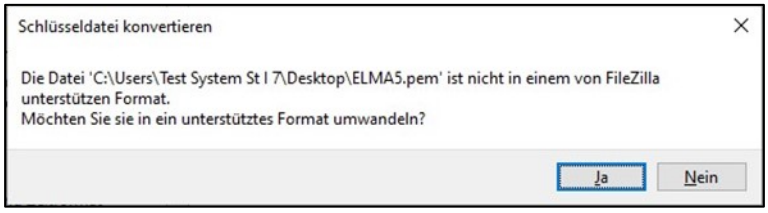

Abbildung 5: Bestätigungsfenster für die Konvertierung des Zertifikats

Die Konvertierung ist bei älteren Versionen von FileZilla (vor 3.46.3 x) und WinSCP (vor 5.15 x) wie folgt durchzuführen:

Öffnen Sie das Key-Generator-Programm `PuTTYgen.exe`:

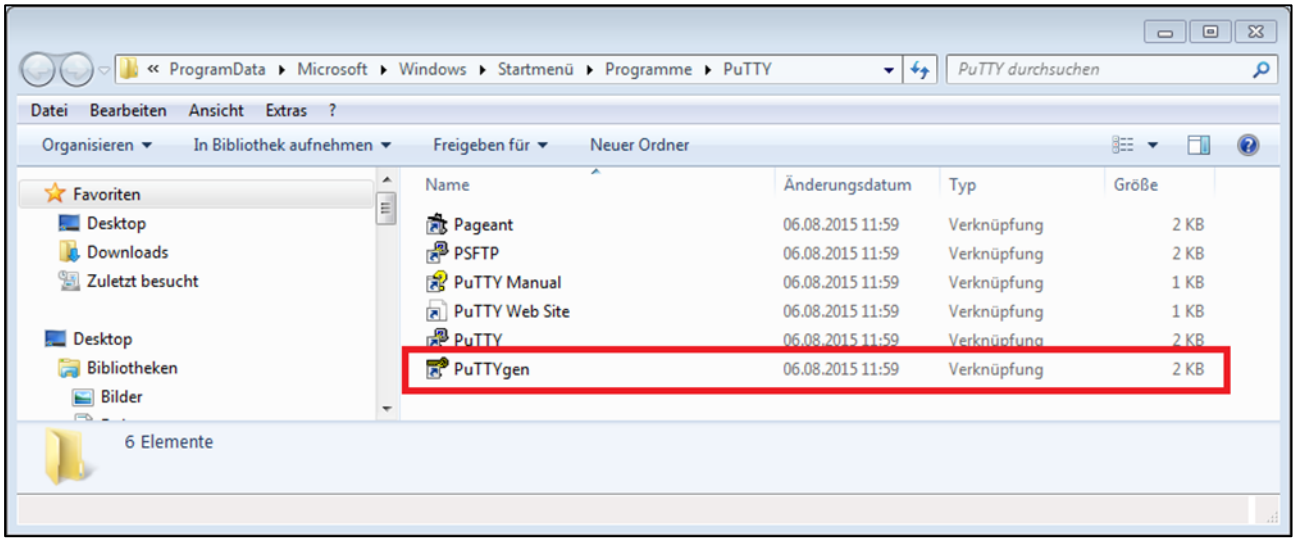

Abbildung 6: PuTTY Programmgruppe

Der PuTTY-Key-Generator startet.

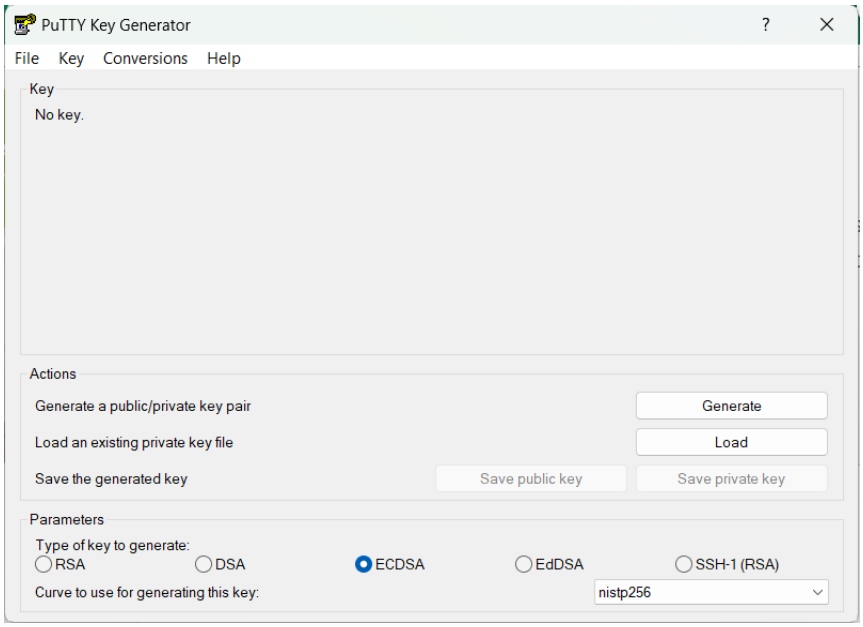

Abbildung 7: Key Generator Startseite

Klicken Sie auf „Load“ und wählen Sie die gewünschte PEM-Datei aus.

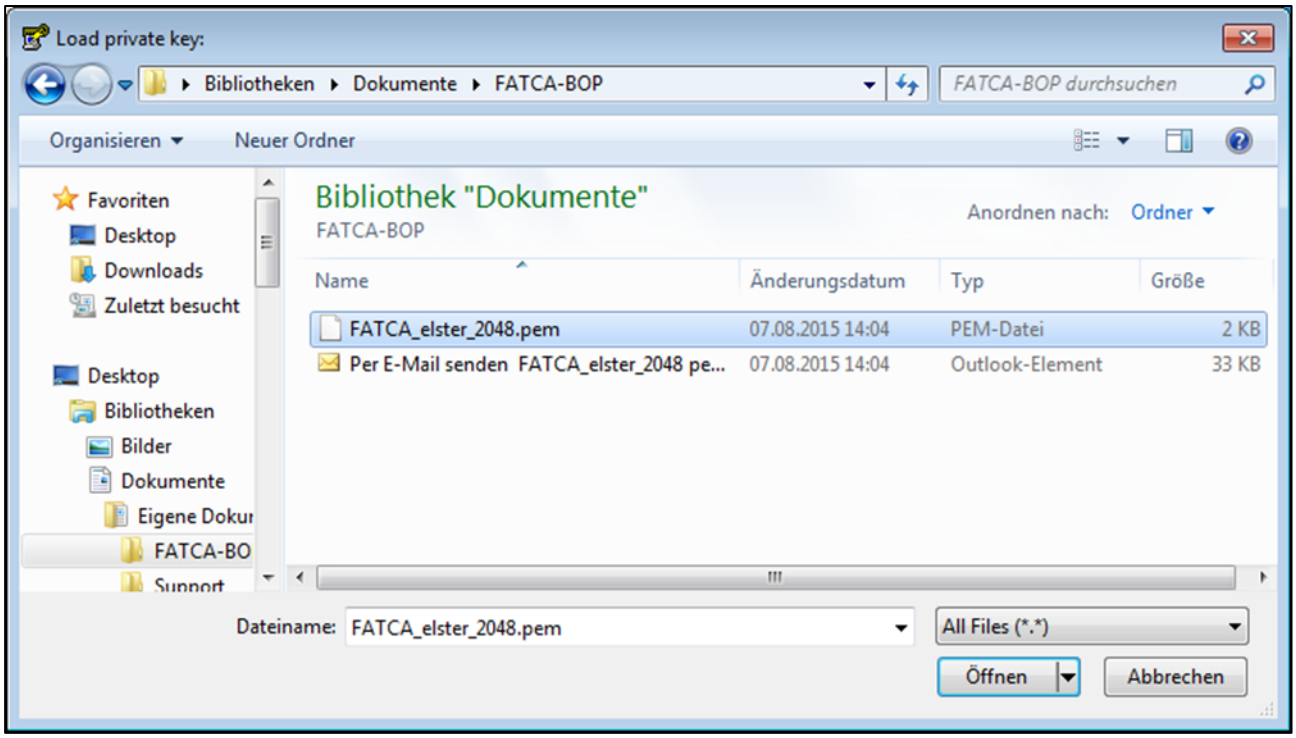

Abbildung 8: Auswahl der PEM-Datei

Die Nutzung der PEM-Datei wird durch die Eingabe der Passphrase (Passwort) freigeschaltet, die Sie beim Download der Zertifikatsdatei festgelegt haben. Es entspricht dem Passwort Ihres Benutzerkontos.

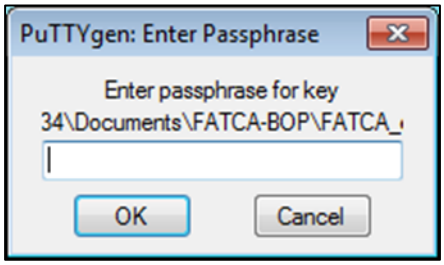

Abbildung 9: Eingabe der Passphrase zur Nutzungsfreischaltung

Wurde die korrekte Passphrase eingegeben, so erhalten Sie die folgende Meldung:

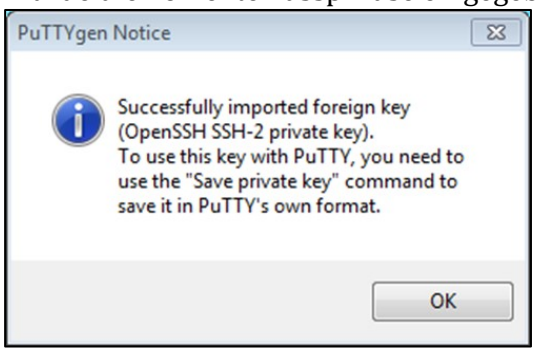

Abbildung 10: PuTTYgen Notice

Damit ist der private Schlüssel importiert und kann jetzt in dem PuTTY-eigenen PPK-Format gespeichert werden.

Speichern Sie den transformierten privaten Schlüssel mit „Save private key“ z.B. unter dem Dateinamen elster.ppk (Namensbeispiel, entscheidend ist die Endung ppk) im Dateisystem ab.

Für die Datenübermittlung bei Fachverfahren, die bisher nicht dem ELMA-Standard 2.0 unterliegen, sind die jeweils fachspezifischen Dokumentationen zu beachten.

3.3. Freischaltung zur Teilnahme am ELMA-Verfahren

Der Besitz des BOP-Benutzerkontos berechtigt noch nicht automatisch zur Teilnahme am ELMA-Verfahren. Hierzu ist eine explizite Freischaltung erforderlich. Das BOP bietet Ihnen die Möglichkeit, diese Freischaltung online durchzuführen.
Sie finden das Formular „Freischaltung zur Teilnahme am ELMA5-Verfahren“ im privaten Bereich des BOP über „Formulare & Leistungen“ -> „Versand von Massendaten (ELMA5)“.

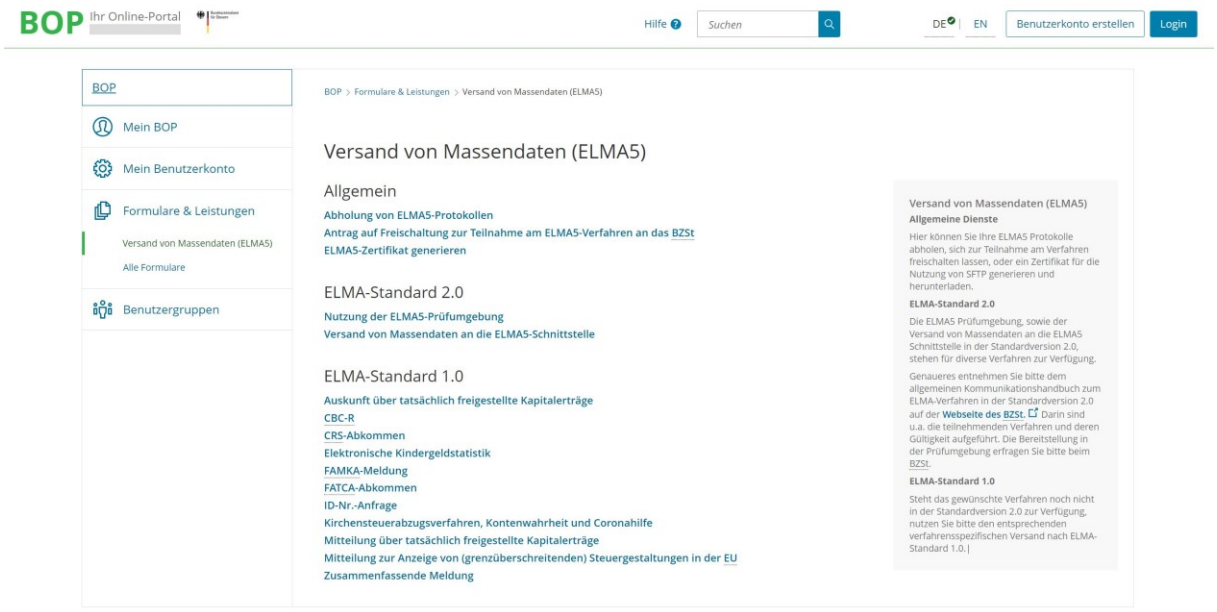

Abbildung 11: BOP > Formulare & Leistungen > Versand von Massendaten (ELMA5)

Die Bearbeitung des Antrags kann einige Zeit in Anspruch nehmen. Vom BZSt erhalten Sie die Bewertung Ihres Antrages als Nachricht in Ihr BOP-Postfach. Bei einer positiven Rückmeldung wird Ihnen die Senderkennung (entspricht der Benutzerkonto-ID) zur Nutzung der ELMA-Komponente bestätigt.

4. Verbindungsprüfung zum ELMA-Server

4.1. Freischaltung für SSH2 über Port 22

Für den direkten Upload per SFTP oder WinSCP.exe ist eine Portfreischaltung für Ihre Netzkomponenten / Router notwendig. Im Home-Office Bereich ist diese Freischaltung meistens im Router voreingestellt. In industriell gesicherten Netzen muss dieser Port aber oft explizit freigeschaltet werden.

Die folgenden Voraussetzungen müssen in Ihrem Netz für den Upload-Rechner erfüllt sein:

- Der **TCP-Port 22** muss für die IP-Adresse des ELMA-Servers freigeschaltet sein.
- Der Domain Name Service (DNS) zur Beantwortung von Anfragen zur Namenauflösung muss aktiviert sein.
- Für die Einlieferung von Produktionsdaten (Produktivumgebung) wird **elma5p.bfinv.de** verwendet.
- Für die Einlieferung von Testdaten (Prüfumgebung) wird **elma5c.bfinv.de** verwendet.

Die Freischaltung von Port 22 kann wie folgt überprüft werden:

Abhängig vom verwendeten Betriebssystem ist das Programm *terminal* unter Linux und MAC OS oder cmd unter Windows zu starten.
Führen Sie auf der Kommandozeile folgende Eingabe aus und schließen diese mit RETURN ab:

telnet elma5p.bfinv.de 22

Antwort im Gutfall:

Trying 80.245.147.91...

Connected to elma5p.bfinv.de.

Escape character is '^]'.

SSH-2.0-OpenSSH_5.5p1[2]

[2]Die OpenSSH Version kann ggf. abweichend sein.

In diesem Fall ist der Port 22 freigeschaltet und kann für einen Verbindungsaufbau genutzt werden. Die nachfolgenden Tests können damit entfallen.

Sollte der Hinweis erscheinen „telnet ist entweder falsch geschrieben oder konnte nicht gefunden werden“, ist in der Windows-Systemsteuerung unter „Windows-Features aktivieren oder deaktivieren“ der „Telnet-Client“ zu aktivieren.

Bei einem gesperrten Port werden die Zeilen Connected und SSH-2.0... nicht angezeigt werden. Die Freischaltung von Port 22 ist in diesem Fall abhängig von Ihrer Systemkonfiguration durchzuführen.

4.2. IP-Adresse des ELMA-Servers ermitteln

Die IP-Adresse des ELMA-Servers wird in der Regel nicht geändert, sie kann aber ohne Angabe von Gründen geändert werden, falls dies technisch notwendig ist.
Unter Windows, Linux und Mac OS können Sie mit dem nslookup-Befehl die IP-Adresse des ELMA-Servers über DNS ermitteln.
Abhängig vom verwendeten Betriebssystem ist das Programm terminal unter Linux und MAC OS oder cmd unter Windows zu starten.
Führen Sie auf der Kommandozeile folgende Eingabe aus und schließen diese mit RETURN ab:

```
nslookup elma5p.bfinv.de
```

Antwort im Gutfall:
Server: ….
Address: ….

Non-authoritative answer:
elma5p.bfinv.de canonical name = lxelma5p.bfinv.de
Name: lxelma5p.bfinv.de
Address: 80.245.147.91

4.3. DNS-Namenauflösung steht nicht zur Verfügung

Kann die IP-Adresse nicht über den DNS-Namen ermittelt werden, schlägt der Verbindungsaufbau fehl. In diesen Fällen kann man durch einen statischen lokalen Eintrag in der hosts-Tabelle des Rechners die IP-Adresse nutzen. Für das Editieren der hosts Datei sind Admin-Rechte notwendig.

4.3.1. Ergänzung der hosts-Tabelle unter Windows

Starten Sie den Windows-Explorer und bewegen Sie sich im Dateipfad zur der in der Kopfzeile angegebenen Position（C[3]:\Windows\System32\drivers\etc).

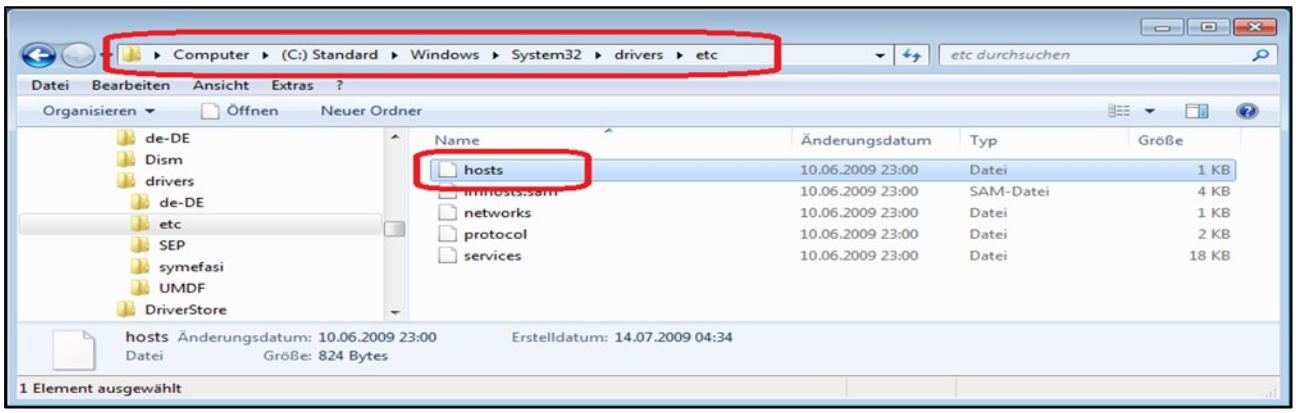

Abbildung 12: Lokalisiation der "hosts" Datei im Explorer

Öffnen Sie in der rechten Auswahlliste die hosts-Datei durch Doppelklick mit dem Editor Programm.

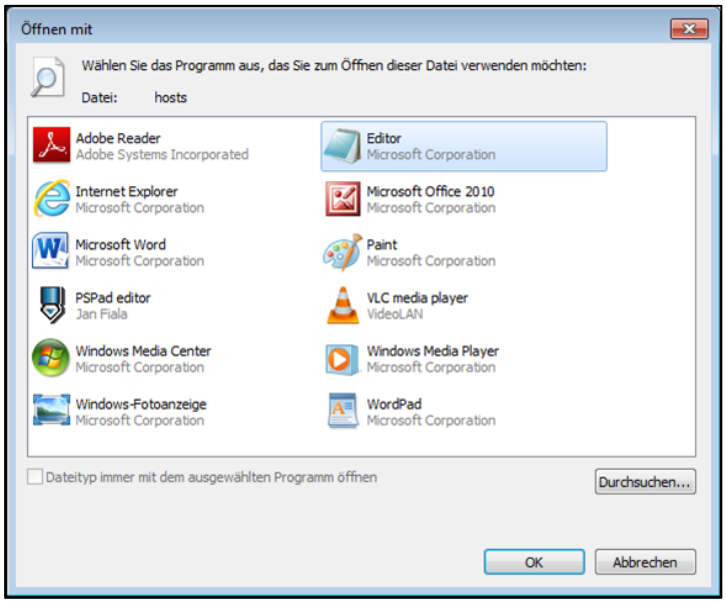

Abbildung 13: Datei mit Editor öffnen

[3] Bei einer auf einem anderen Laufwerk liegenden Systempartition verwenden Sie bitte den entsprechenden Laufwerksbuchstaben.

Erweitern Sie die Liste am Ende um den gewünschten Eintrag für den Server. Die aktuelle IP-Adresse ist vorab wie in *Abschnitt 4.2* beschrieben zu ermitteln.

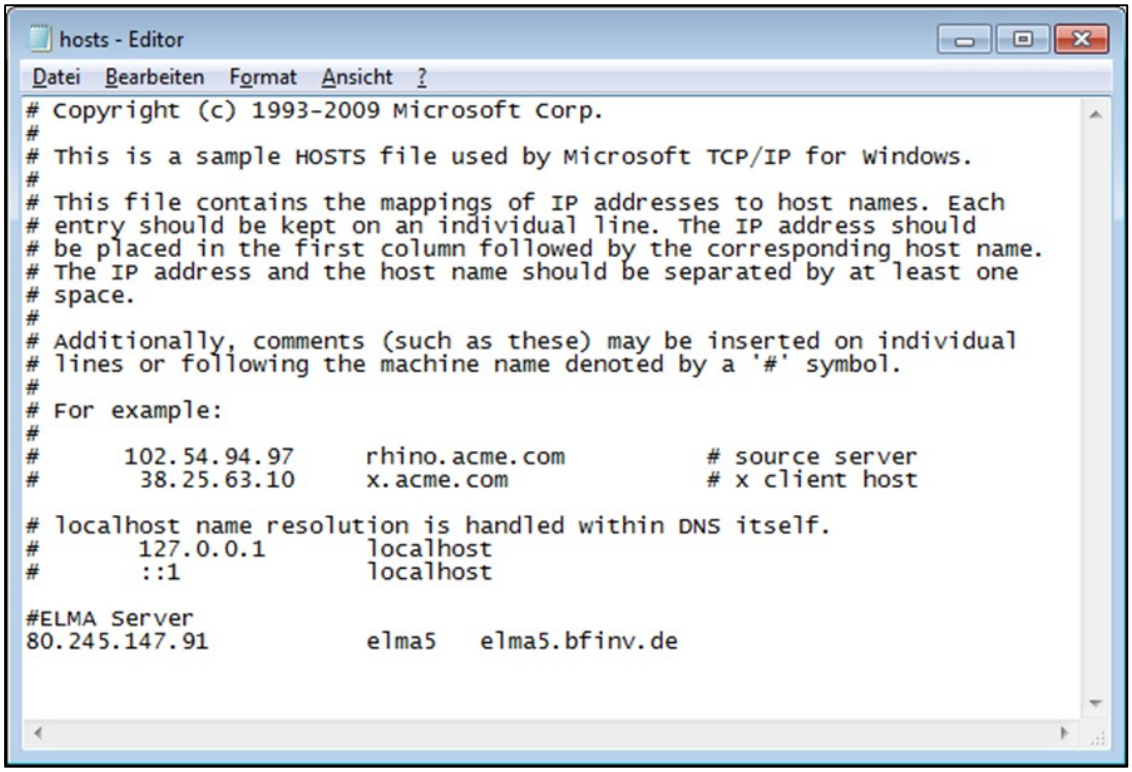

Abbildung 14: Ergänzung der hosts-Datei um elma5p Servereintrag

Danach speichern Sie die Datei unter demselben Namen wieder ab. Setzen Sie den Dateityp ggf. auf *.* um.

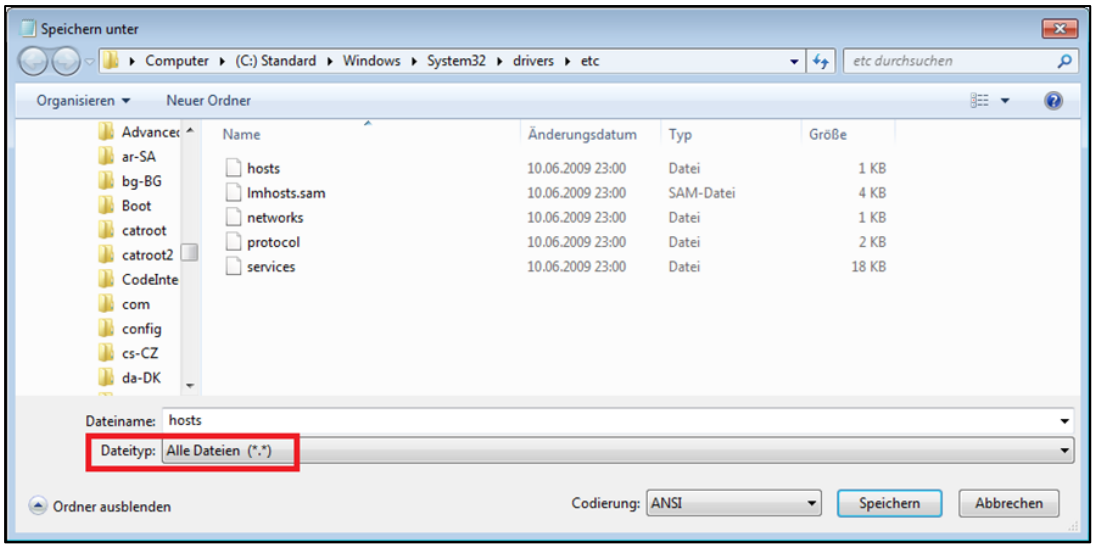

Abbildung 15: Dateityp bei Speicherung setzen

Abschließend beenden Sie alle Browser-Instanzen.

4.3.2. Ergänzung der hosts Tabelle unter MAC OS

Für die Durchführung der folgenden Befehle wird ein Admin-Zugang (das Admin-Kennwort) benötigt.
Starten Sie das Terminal-Programm.
Führen Sie auf der Kommandozeile den folgenden Befehl aus:

```
sudo nano /private/etc/hosts
```

Fügen Sie nach der Eingabe des Admin-Kennwortes die folgenden Zeilen am Ende der Datei ein:

ELMA Server

80.245.147.91elma5p elma5p.bfinv.de

Speichern Sie die hosts-Datei durch Eingabe von Control+O gefolgt von RETURN und beenden Sie den nano-Editor durch Eingabe von Control+X.

Führen Sie abschließend einen DNS-Flush mit dem folgenden Kommando aus:

```
dscacheutil –flushcache; sudo killall –HUP mDNSResponder
```

4.3.3. Ergänzung der hosts-Tabelle unter Linux

Für die Durchführung der folgenden Befehle wird das Admin-Kennwort benötigt.
Starten Sie das Terminal-Programm.
Führen Sie auf der Kommandozeile den folgenden Befehl aus:

```
sudo nano /etc/hosts
```

Fügen Sie nach der Eingabe des Admin-Kennwortes die folgenden Zeilen am Ende der Datei ein:

ELMA Server

80.245.147.91elma5p elma5p.bfinv.de

Speichern Sie die hosts-Datei durch Eingabe von Control+O gefolgt von RETURN und beenden den nanoEditor durch Eingabe von Control+X.
Führen Sie abschließend einen Neustart von networking mit dem folgenden Kommando aus:

```
sudo /etc/init.d/networking restart
```

4.4. Verwendung eines Proxys für den Internetzugang

Die Proxy-Konfiguration kann an dieser Stelle nur generell behandelt werden. Die Vielzahl der verschiedenen Produkte macht eine detaillierte Betrachtung schwierig. Generell unterscheidet man zwischen Elite Proxy (L1 Proxy), Anonyme Proxy (L2 Proxy) und Transparente Proxy (L3 Proxy).
Im Falle einer notwendigen Proxy-Freischaltung wird die Verbindung vom Client zum Proxy durch einen Eintrag in der hosts-Tabelle realisiert, *vgl. Abschnitt 4.3.1*. Anstatt der IP-Adresse des ELMA-Servers ist die IP-Adresse des Proxys einzutragen.
Im Proxy ist danach die tatsächliche IP-Adresse des ELMA Servers zu hinterlegen. Bei einem SSH-2 Verbindungsaufbau über Port 22 wird über den Eintrag in der lokalen hosts-Tabelle der Weg zum Proxy gefunden. Dieser verwendet dann die Adresse des ELMA-Servers und leitet die Anfrage an den Server im Internet weiter.

4.5. Übertragung ohne Port 22-Freischaltung

Sollte eine Portfreischaltung nicht möglich sein, so kann die Datenübertragung nur über einen speziell für diese Eintragung eingerichteten PC mit Netzanbindung erfolgen.

5. Nutzung von ELMA über BOP

Es besteht die Möglichkeit, die XML-Datendatei über einen Upload-Client in BOP an das BZSt zu übertragen. Dies gilt sowohl für die Dateneinlieferung in die Produktiv- (elma5p) als auch in die Prüfumgebung (elma5c).

Sie erreichen den Upload-Client wie folgt:

Produktivumgebung:

"Formulare & Leistungen“-> “Versand von Massendaten (ELMA5)“ -> “ELMA Standard 2.0“ -> “Versand von Massendaten an die ELMA5-Schnittstelle“

Prüfumgebung:

"Formulare & Leistungen“ -> “Versand von Massendaten (ELMA5)“ -> “ELMA Standard 2.0“ -> “Nutzung der ELMA5-Prüfumgebung“

Bitte beachten Sie, dass für den Upload von XML-Dateien ebenfalls eine Freischaltung für die ELMA-Schnittstelle sowie die Einbindung des Zertifikats im Browser erforderlich ist. Eine Anleitung für die Einbindung des Zertifikats in den Browser ist auf den Hilfeseiten von BOP zu finden.

Der Aufbau der XML-Datendatei folgt denselben Regeln wie bei der Übertragung an die ELMA-Schnittstelle. Daher sind bzgl. der Übertragung der XML-Datei insbesondere das Kapitel 6.1 (Aufbau des ELMA XML Schema) zu beachten.

Die Rückmeldungen zu einer über BOP übertragenen Datei sind nicht im BOP-Postfach abrufbar, sondern müssen direkt vom ELMA-Server abgeholt werden.

Um diese Rückmeldungen ohne direkte SFTP-Verbindung abzuholen, besteht aus BOP heraus die Möglichkeit, den Inhalt des Download-Verzeichnisses abzurufen. Der Weg dorthin führt über folgende Navigation:

Formulare & Leistungen -> Versand von Massendaten (ELMA5) -> Allgemein -> Abholung von ELMA5-Protokollen

Bei der Abholung der Protokolle ist nun eine Auswahl zwischen Produktiv- und Prüfumgebung vorgeschaltet. Die Inhalte der Rückmeldungen und die diesbezüglichen Prüfungen sind identisch mit einer per SFTP über das ELMA-Upload-Verzeichnis übertragenen Datei (siehe dazu Kapitel 9).

Teil II Datenübertragung

Die nachfolgenden Kapitel beschreiben die weitere Vorgehensweise bei der Datenübertragung für Verfahren, die dem ELMA-Standard unterliegen (siehe Kapitel 0.2) Für die Datenübermittlung bei Fachverfahren, die bisher nicht dem ELMA-Standard 2.0 unterliegen, sind die jeweils fachspezifischen Dokumentationen zu beachten.

6. Anforderung an die zu übertragenden Dateien

6.1. Aufbau des ELMA XML-Schemas

Das folgende Kapitel beinhaltet eine kurze Beschreibung des Aufbaus des ELMA XML-Schemas. Für genauere Informationen zum Aufbau, insbesondere zu Feldtypen und -längen, ist die entsprechende XSD zu Rate zu ziehen.

6.1.1. Aufbau des Wurzelelements ELMA

Es wurde eine verfahrensübergreifende standardisierte Schema Definition für die Nutzung der ELMA-Schnittstelle geschaffen, in die die jeweiligen Fachverfahrensdaten in dem Element ELMA einzubetten sind.

Der ELMA-Standard 2.0 wird im Folgenden exemplarisch am Verfahren UStVEU dargestellt und gilt analog für alle teilnehmenden Verfahren unter *Abschnitt 0.2*.

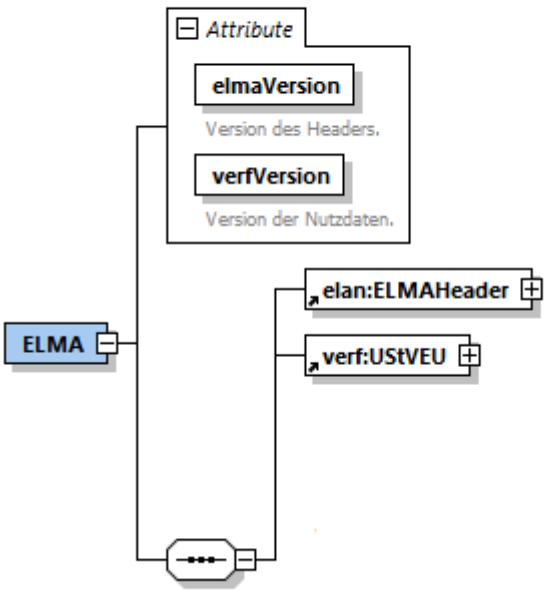

Abbildung 16: Aufbau des ELMA XML-Schemas

Das Wurzelelement ELMA wird wie ein „Umschlag“ um die eigentlichen Dateninhalte herumgelegt.

Unterhalb des Wurzelelements folgen der ELMAHeader und die verfahrensspezifischen Nutzdaten (hier UStVEU).

Nachfolgende Tabelle beschreibt die Attribute des Wurzelelements ELMA.

Attribut	Inhalt / Erläuterung	Bemerkungen
elmaVersion	Version des ELMA-Headers	fester Wert: 2
verfVersion	Version der zu Nutzdaten	siehe Schnittstellenbeschreibung des Fachverfahrens

Tabelle 2: Aufbau des Wurzelelements ELMA

6.1.2. Aufbau des Elements ELMAHeader

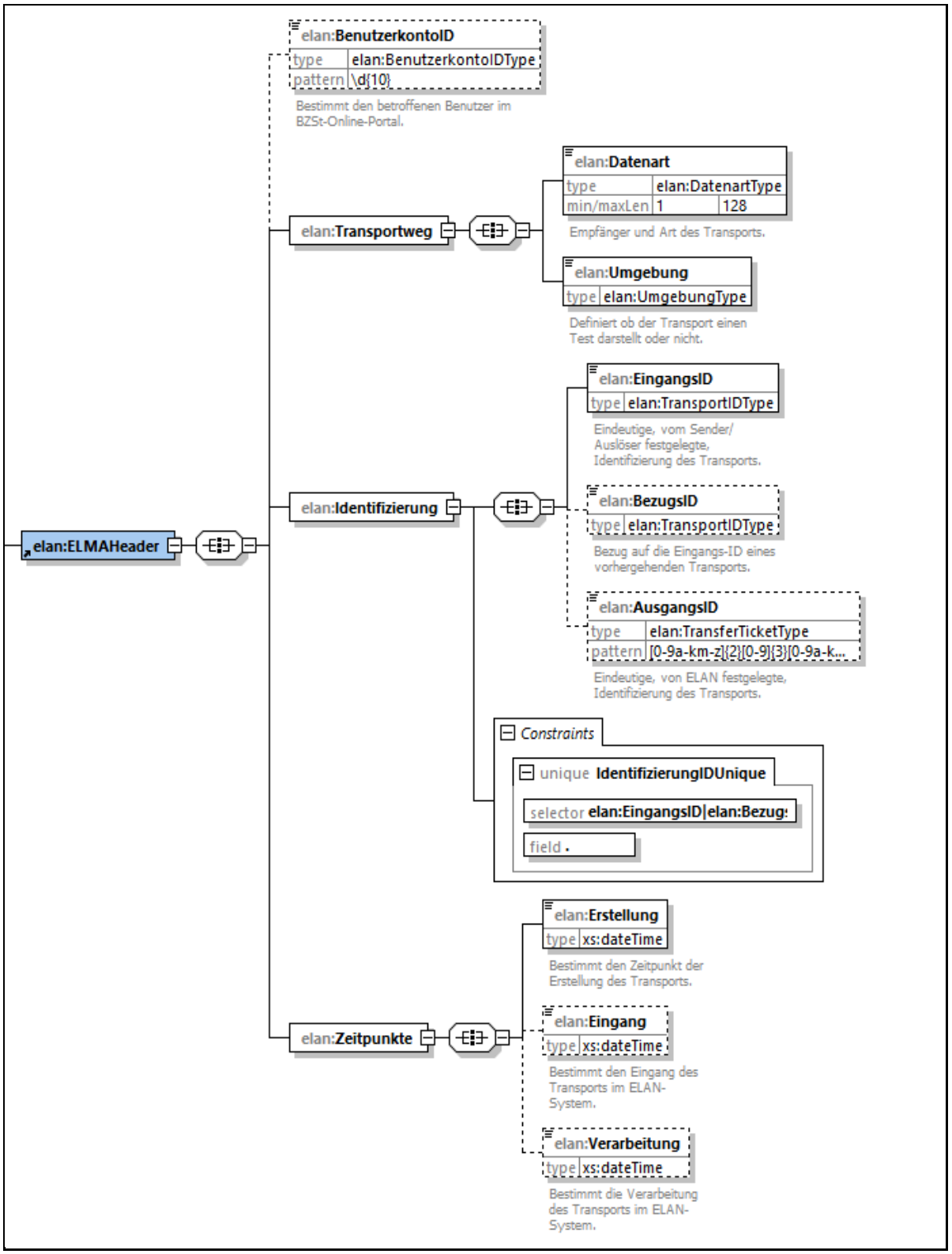

Abbildung 17: Aufbau des Elements ELMAHeader

Nachfolgende Tabelle beschreibt die Befüllung des ELMA-Headers:

Element		Inhalt / Erläuterung	Bemerkungen
BenutzerkontoID		Kennung des Benutzerkontos in Mein BOP	Die Angabe ist verpflichtend.
Transportweg	Datenart	Die Datenart bestimmt den Inhalt der Nutzdaten und das verarbeitende Fachverfahren.	siehe Tabelle 1: Teilnehmende Fachverfahren
Transportweg	Umgebung	Unterscheidung zwischen Produktiv- und Prüfumgebung	für elma5p „PRODUKTION“, für elma5c „TEST“
Identifizierung	EingangsID	Die EingangsID wird vom Absender gesetzt und dient diesem als Identifizierung des Transports.	Format: UUID
Identifizierung	BezugsID	Die Bezugs-ID wird vom Absender gesetzt und entspricht der Eingangs-ID des Transports auf den sich bezogen werden möchte.	
Identifizierung	AusgangsID	Eindeutige Identifizierung des Transports	Wird durch ELMA gesetzt. Format: 32-stellig alphanumerisch
Zeitpunkte	Erstellung	Zeitpunkt der Erstellung der XML-Datei	
Zeitpunkte	Eingang	Zeitpunkt des Eingangs auf dem ELMA-Server.	Wird durch ELMA gesetzt.
Zeitpunkte	Verarbeitung	Zeitpunkt der Verarbeitung durch die ELMA-Schnittstelle.	Wird durch ELMA gesetzt.

Tabelle 3: Inhalte des ELMAHeaders

6.1.3. Aufbau der verfahrensspezifischen Nutzdaten

Der Aufbau des Nutzdatenschemas ist der Schnittstellenbeschreibung des jeweiligen Fachverfahrens und den durch das Fachverfahren bereitgestellten XML-Schemata zu entnehmen.

6.1.4. Beispiel

```
<n1:ELMA xmlns:n1="http://www.itzbund.de/elan"
xmlns:elan="http://www.itzbund.de/elan/elemente" elmaVersion="2" verfVersion="1.0.0">
    <elan:ELMAHeader>
        <elan:BenutzerkontoID>6098575621</elan:BenutzerkontoID>
        <elan:Transportweg>
            <elan:Datenart>TestDatenart</elan:Datenart>
            <elan:Umgebung>PRODUKTION</elan:Umgebung>
        </elan:Transportweg>
        <elan:Identifizierung>
            <elan:EingangsID>fe8test2-18d6-45c8-bbf9-32e991test63</elan:EingangsID>
        </elan:Identifizierung>
        <elan:Zeitpunkte>
            <elan:Erstellung>2020-11-28T09:27:47Z</elan:Erstellung>
        </elan:Zeitpunkte>
    </elan:ELMAHeader>
      <verf:Test xmlns:verf="http://www.itzbund.de/elan/test/01">
          <verf:ElementA>Ein einfaches Beispiel für Nutzdaten!</verf:ElementA>
    </verf:Test>
</n1:ELMA>
```

6.2. Weitere Anforderungen

6.2.1. XSD-Schema Validierung

Die XML-Datendatei sollte vor der Versendung gegen die aktuellen XML-Schemata validiert werden, soweit die gesamten diesbezüglichen XSDs vom jeweiligen Fachverfahren zur Verfügung gestellt werden.

6.2.2. UTF-8 Kodierung

Für die Erstellung der XML-Datei ist die UTF-8 Kodierung zu verwenden. Abweichende Kodierungen werden nicht unterstützt und können zu einer Abweisung führen. Es wird empfohlen, nur die üblicherweise in Namens- und Adressdaten enthaltenen Zeichen der UTF-8 Kodierung zu nutzen[4]. Nur so sind eine unverfälschte Speicherung und Verarbeitung der Daten gewährleistet. Als Orientierungshilfe kann der von der Koordinierungsstelle für IT-Standards (KoSIT) des IT-Planungsrats im Bundesministerium des Innern definierte Satz der lateinischen Zeichen[5] herangezogen werden.

[4] Je nach dem gewählten Fachverfahren können die erlaubten Zeichen eingeschränkt sein.
[5] https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/13_Sitzung/Unicode.html

6.2.3. Unzulässige Zeichen und Beschränkungen

ELMA nimmt Daten gemäß UTF-8 grundsätzlich ohne Einschränkung an. In den einzelnen Fachverfahren können jedoch unzulässige Zeichen und weitere Restriktionen festgelegt sein, die zu einer Abweisung führen können.

6.2.4. Dateigrößenbeschränkung

Die zu übermittelnde Datendatei sollte kleiner als 200 Megabyte sein. Eine Überschreitung dieser Maximalgröße führt zu einer Abweisung.

6.2.5. Namenskonvention für die Datendatei

Der Name der XML-Datei muss dem Muster <Datenart>.<BenutzerkontoID>.<DateiID>.xml entsprechen. Die Datenart des Fachverfahrens kann Abschnitt 0.2 (Teilnehmende Fachverfahren) entnommen werden. Die DateiID ist frei wählbar, sie muss zwischen vier und 36 Zeichen enthalten. Zulässige Zeichen in der DateiID sind große und kleine Buchstaben [A-z, a-z], Ziffern [0-9] sowie – und _. Zwischen dem Dateinamen und dem Suffix wird ein Punkt „.“ als Trennzeichen verwendet. Der Dateiname der Datendatei endet mit dem Suffix xml. Abweichende Dateinamen werden nicht abgewiesen, sondern nicht in die Verarbeitung genommen. Die Lieferungen bleiben folglich im Upload-Verzeichnis liegen.

Je Umgebung (Produktiv- bzw. Prüfumgebung) darf ein bereits für die Übertragung verwendeter Dateiname nicht erneut genutzt werden.
Die entsprechende Eingangsprüfung (Kapitel 9.3 Prüfung k) verhindert die Wiederverwendung von Dateinamen – auch im Fehlerfall bei einer formalen Abweisung durch die ELMA-Prüfung.

Es wird daher empfohlen, für die DateiID den Wert des Header-Elements EingangsID zu verwenden, da die EingangsID je Übermittlung immer eindeutig sein soll.

Beispiele für eine UStVEU-Datendatei:

```
UStVEU.1234567890.Spar-Kohl_0001.xml
UStVEU.1234567890.c4755118-e6c9-4be9-b462-3fc9bbef5e52.xml
UStVEU.1234567890.halloNutzer.xml
```

Feldname	Anzahl Zeichen	Inhalt / Erläuterung	Bemerkungen
<Datenart>		Die Datenart für die Information des Fachverfahrens.	*Vgl. Spalte „Datenart“ in Abschnitt 0.2.*
.	1	Punkt	konstant

Feldname	Anzahl Zeichen	Inhalt / Erläuterung	Bemerkungen
<BenutzerkontoID>	10	BenutzerkontoID des verwendeten Zertifikats	10-stelliges Textfeld, dass nur Ziffern (0-9) beinhalten darf. Die BenutzerkontoID wird im privaten Bereich des BOP-Benutzerkontos unter „Mein BOP“ als „Benutzerkonto-ID“ innerhalb der Übersicht "Benutzerkontoinformationen" angezeigt.
.	1	Punkt	konstant
<DateiId>	4-36	Von der versendenden Stelle zu vergebender, interner Kurzname für die Datendatei. Dieser Bezeichner dient nur der internen Zuordnung des Versenders.	4 bis max. 36 Zeichen. Zulässige Zeichen: große und kleine Buchstaben [A-z, a-z], Ziffern [0-9] sowie – und _ Hinweis: Es wird empfohlen, den Wert des Header-Elements EingangsID zu verwenden.
.	1	Punkt Trennung Präfix.Suffix	konstant
xml	3	Suffix	konstant

Tabelle 4: Aufbau Dateinamen bei Lieferung

6.2.6. Namenskonvention für die Signaturdatei

Zu jeder Datendatei gehört eine korrespondierende Signaturdatei. Der Name der Signaturdatei besteht aus dem Namen der Datendatei erweitert um das Suffix .sig.

6.2.7. Erstellung Signaturdatei

Für die Erstellung der Signaturdatei kann beispielsweise das OpenSSL Command Line Tool verwendet werden.

Für ELMA müssen die Signaturen mit ECDSA im DER-Format erzeugt werden. Die zu verwendende Hashfunktion ist abhängig von der für den Private Key gewählten Kurve.

- für die Kurve NIST P-256 ist die Hashfunktion SHA-256 (im OpenSSL-Befehl sha256) zu wählen

- für die Kurve NIST P-384 ist die Hashfunktion SHA-384 (im OpenSSL-Befehl sha384) zu wählen
- für die Kurve NIST P-521 ist die Hashfunktion SHA-512 (im OpenSSL-Befehl sha512) zu wählen

6.2.7.1. Linux

Öffnen Sie per Tastenkombination "Alt" + "F2" den Anwendungsstarter und geben Sie den Begriff "Terminal" ein. Führen Sie das Programm mit RETURN aus.

Wechseln Sie in das Verzeichnis der Datendatei und führen Sie im Terminal-Fenster die folgende Kommandozeile aus.

```
openssl pkeyutl -sign -in <Pfad zur XML-Datei> \
-inkey <Pfad zum Private Key> -rawin -digest <Hashfunktion> \
-out <Dateiname der Signaturdatei>
```

Nach Eingabe der Passphrase wird die Signaturdatei erstellt.

6.2.7.2. MAC OS

Öffnen Sie per Tastenkombination "command" (cmd-Taste) + "Space" (Leertaste) die "Spotlight-Suche" und geben Sie den Begriff "`Terminal`" ein. Führen Sie das Programm mit RETURN (Eingabetaste) aus.

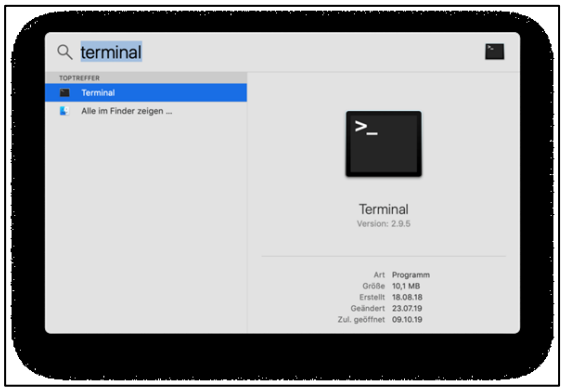

Abbildung 18: Aufruf des Terminals über die Spotlight-Suche unter macOS

Wechseln Sie in das Verzeichnis ("cd" + Pfad zum Verzeichnis) der Datendatei und führen Sie im Terminal-Fenster die folgende Kommandozeile aus.

```
openssl pkeyutl -sign -in <Pfad zur XML-Datei>
-inkey <Pfad zum Private Key> -rawin -digest <Hashfunktion>
-out <Dateiname der Signaturdatei>
```

Nach Eingabe der Passphrase wird die Signaturdatei erstellt.

6.2.7.3. Windows

Öffnen Sie das Kommandozeilen-Fenster (Eingabe von `cmd.exe` in Start->Programme/Dateien durchsuchen `cmd.exe`).

Wechseln Sie in das Verzeichnis, in dem die Datendatei abgelegt ist. Führen Sie im Kommandozeilen-Fenster die folgende Kommandozeile aus. Ersetzen Sie [Pfadangabe] durch das Installationsverzeichnis der `openssl.exe` Datei.

```
<Pfadangabe>\openssl.exe pkeyutl -sign -in <Pfad zur XML-Datei> ^[6]
-inkey <Pfad zum Private Key> -rawin -digest <Hashfunktion> ^
-out <Dateiname der Signaturdatei>
```

Nach Eingabe der Passphrase wird die Signaturdatei erstellt.

7. Einrichtung der Übertragungskomponente

Mit Hilfe des ELMA-Zertifikates und geeigneter openSource-Software kann die Authentisierung und die Datenübertragung an der ELMA-Komponente durchgeführt werden.
Auf dem sendenden Rechner wird Software für die Signaturerstellung (z.B. OpenSSL) und eine vom verwendeten Betriebssystem abhängige Übertragungssoftware (SFTP / WinSCP / FileZilla) benötigt.

7.1. OpenSSL-Installation

Bei einem neu aufzusetzenden Übertragungsdienst wird die OpenSSL-Komponente zwingend für die Signaturerstellung benötigt. Laden Sie bitte immer die aktuellste Version herunter. Für die Installation sind erweiterte Rechte notwendig.

7.1.1. OpenSSL-Installation unter Linux

Öffnen Sie per Tastenkombination `Alt + F2`[7] den Anwendungsstarter und geben Sie den Begriff terminal ein. Starten Sie das Programm mit RETURN.

Führen Sie Im Terminal-Fenster die folgenden Kommandozeilen aus:

```
wget http://www.openssl.org/source/openssl-1.1.1d[8].tar.gz
```

[6] Das Zeichen „^“ stellt die Fortsetzung der Eingabe in einer neuen Zeile dar. Wird die Eingabe nicht in einer neuen Zeile fortgesetzt, kann dies entfallen.
[7] Abhängig von der verwendeten Linux / Unix Installation kann die Tastenkombination abweichen.
[8] Die Version kann ggf. abweichen. Verwenden Sie immer die aktuell verfügbare Version.

```
tar -xvzf openssl-1.1.1d.tar.gz
cd openssl-1.1.1d
./config --prefix=/usr/
make
sudo make install
```

Überprüfen Sie Ihre OpenSSL- Version durch Eingabe von openssl Version auf der Kommandozeilenebene.

7.1.2. OpenSSL-Installation unter Mac OS

Ab MacOS Mojave (10.14.x) ist OpenSSL (LibreSSL) bereits im System integriert. Eine separate Installation ist nicht notwendig.

7.1.3. OpenSSL-Installation unter Windows

Vorkompilierte Win32 / 64 Bibliotheken finden Sie unter folgender Adresse:

https://slproweb.com/products/Win32OpenSSL.html

Der Download der aktuellsten Version erfolgt als ZIP-Archiv. Dieses ist auf dem lokalen Windows-Rechner zu entpacken. Die Installation entspricht der unter Windows üblichen Prozedur.

7.2. OpenSSH-Installation

7.2.1. OpenSSH-Installation unter Linux

In vielen Linux-Distributionen 8z.B. für die Linux-Betriebssystem-Derivate Suse, RedHat, Fedora, Debian) werden in der Regel die OpenSSH-Module sowie OpenSSL standartmäßig bei der Grundeinstellung mit installiert.
Öffnen Sie per Tastenkombination „Alt + F2“ den Anwendungsstarter und geben den Begriff terminal ein. Starten Sie das Programm mit RETURN.
Führen Sie im Terminal-Fenster die folgende Kommandozeile aus:

```
ssh -V
```

Bei einer installierten Komponente wird die SSH Versionsnummer angezeigt.

Andernfalls kann OpenSSH über die folgenden Kommandozeile[9] installiert werden.

```
sudo apt-get install openssh-server
```

7.2.2. OpenSSH Installation unter Mac OS

Die OpenSSH Komponente ist integraler Bestandteil des OS X Betriebssystems. Eine Installation ist daher nicht notwendig.

7.2.3. OpenSSH-Installation unter Windows

Laden Sie sich von der „Putty Download Page“
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
die aktuellste Version der Datei `putty` herunter[10] und führen die Installation aus.

8. Übertragung der Daten- und Signatur-Datei

8.1. Verzeichnisstruktur

Dem Benutzer werden auf dem ELMA-Server die beiden Verzeichnisse „upload“ und „download“ zur Verfügung gestellt. In das upload-Verzeichnis sind die Anfragen des Benutzers im XML-Format einzustellen. Über das download-Verzeichnis erhält der Benutzer Informationen der ELMA-Schnittstelle und der Fachverfahren.

Sämtliche Dateien werden direkt in den Verzeichnissen upload und download abgelegt. Das Erstellen von Unterordnern ist nicht zulässig.

8.2. Aufbau der Verbindung

Die Einlieferung einer ELMA-Datei erfolgt über eine Rechner-zu-Rechner-Kopplung per SFTP.

Bevor Sie eine Verbindung zum Server aufbauen können, müssen Sie sicherstellen, sofern Sie für die Datenübertragung (vornehmlich unter Windows) die Programme WinSCP oder FileZilla verwenden, dass eine Signaturdatei im ECDSA-Format vorliegt, *vgl. Abschnitt 3.2.*

Für den anschließenden Aufbau der Verbindung zum Server sind folgende Anmeldedaten zu verwenden:

[9] Hier als Beispiel für ein Debian System.
[10] Verwenden Sie als Download immer die aktuelle Version.

Lieferung in die Produktivumgebung

DNS-Name: elma5p.bfinv.de
Username: Ihre Benutzerkonto-ID ergänzt um das Präfix „elster“(Beispiel: elster-1003427800)
Passwort: es ist hier kein Passwort einzugeben*
Port: 22

Lieferung in die Prüfumgebung

DNS-Name: elma5c.bfinv.de
Username: Ihre Benutzerkonto-ID ergänzt um das Präfix „elster“ (Beispiel: elster-1003427800)
Passwort: es ist hier kein Passwort einzugeben*
Port: 22

* Die Abfrage des Passwortes erfolgt während der Anmeldung. Das Passwort haben Sie im Rahmen der Erzeugung des Schlüsselpaars vergeben.

Es ist zu beachten, dass zur Konfiguration der Serververbindung nur diese DNS-Namen zu verwenden sind und nicht die resultierenden IP-Adressen.

Nachfolgende Abbildungen zeigen die Passwortabfrage im Rahmen der Anmeldung per WinSCP und FileZilla.

WinSCP

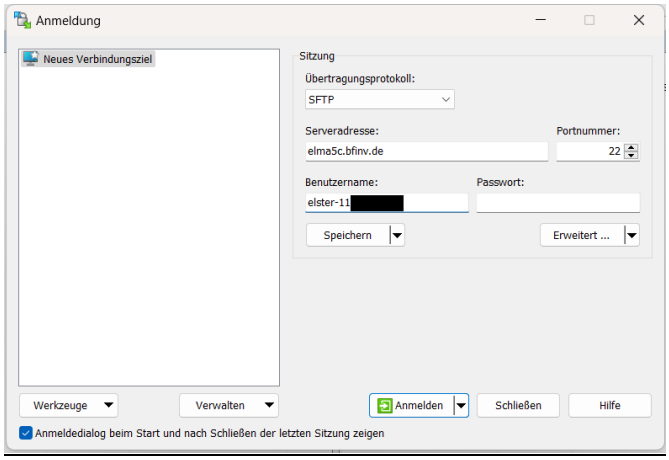

Abbildung 19: Anmeldemaske in WinSCP

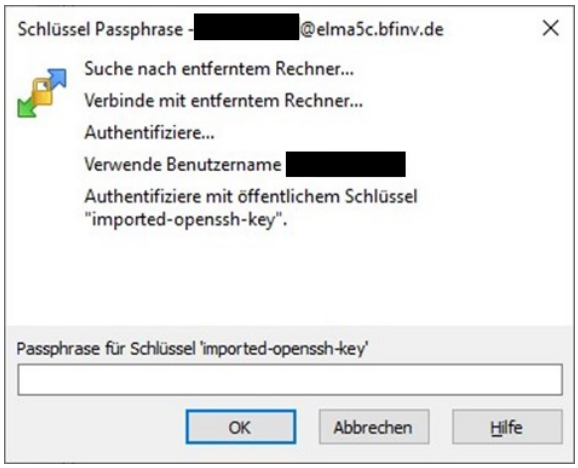

Abbildung 20: Fenster zur Passwortabfrage des ELMA5-Zertifikats

FileZilla

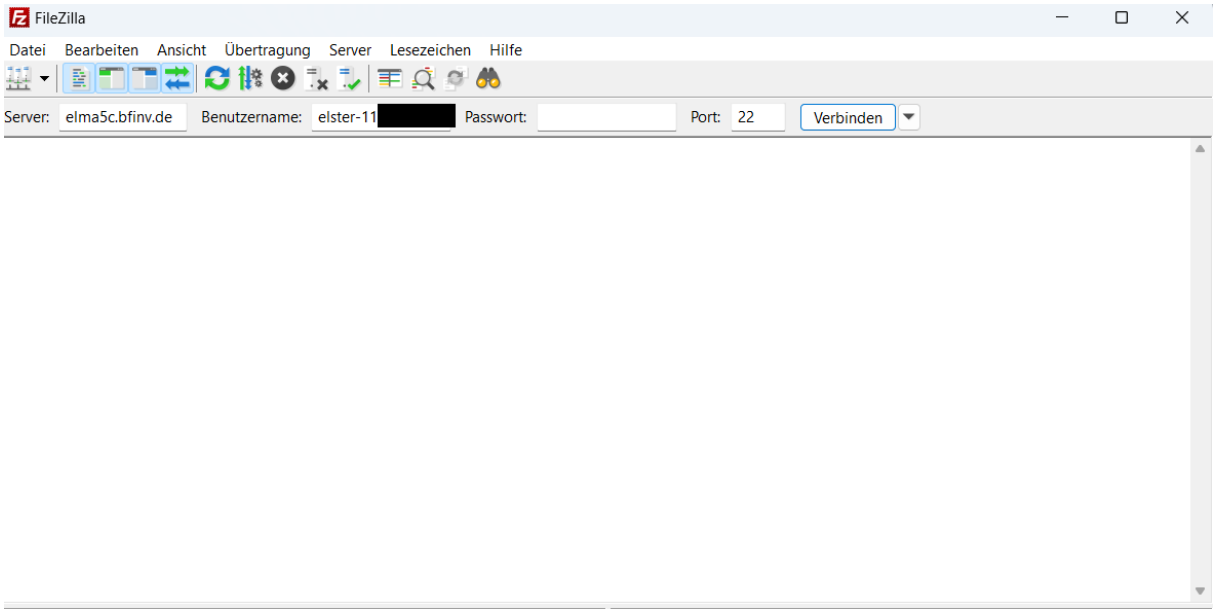

Abbildung 21: Anmeldemaske in FileZilla

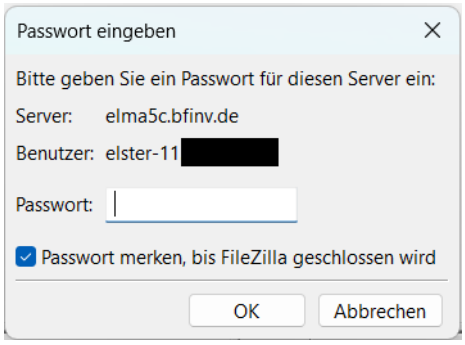

Abbildung 22: Fenster zur Passwortabfrage des ELMA5-Zertifikats

8.3. Ablauf der Datenübertragung

Jede Datenübertragung (Upload) auf den ELMA-Server besteht immer aus 2 Dateien (Datendatei und Signaturdatei). Die Datendatei enthält den durch das Fachverfahren spezifizierten Meldungsdatensatz. Dieser unterscheidet sich je Fachverfahren.
Über die zugehörige Signaturdatei werden die Authentizität des Senders und die Datenintegrität der Datendatei festgestellt.

Es ist immer eine Datendatei und die korrespondierende Signaturdatei in das Upload-Verzeichnis auf dem ELMA-Server einzustellen.

Unter dem ELMA-Standard 2.0 werden die Übermittlungen innerhalb von Sekunden aus den Upload-Verzeichnissen abgeholt (u.a. zur Erfassung des Eingangszeitpunktes).
Eine wiederholte Übermittlung, weil die erste Übertragung 'verschwunden' ist, führt zu Abweisungen aufgrund der Übermittlung einer Dublette (doppelte EingangsID, doppelter Dateiname).

8.3.1. Erstellung der Signaturdatei

Die Passphrase wird bei jeder Signaturerstellung verwendet und sollte daher sicher verwahrt werden. Die Erstellung der Signaturdatei ist in Kapitel 6.2.7 beschrieben.

Bitte beachten Sie, dass Ihre Datenübertragung nur dann durch den ELMA-Server angenommen wird, wenn sowohl die Datendatei als auch die Signaturdatei im Upload-Verzeichnis vorhanden sind. Fehlt die Signaturdatei, verbleibt die Datendatei ohne weiteren Hinweis im Upload-Verzeichnis. Sollten Sie zu einer Datenübermittlung innerhalb eines Tages kein Feedback der ELMA-Schnittstelle erhalten, prüfen Sie bitte Ihr Upload-Verzeichnis.

8.4. Upload

Beim Upload der Dateien mittels SFTP sind diese zunächst mit der Endung „.tmp“ zu übertragen.

Für den SFTP-Datentransport ist die Übertragungsart „**binär**“ zu wählen.

Unterbleibt dies, wird insbesondere bei einem File-Transfer von einem Windows-basiertem System die Signaturdatei nicht mehr zur Datendatei passen, weil im Rahmen des Transfers bspw. das Zeilenende CR/LF in das Unix-Format LF des Zielrechners gewandelt wird. Der Sender würde einen Hinweis auf einen Signaturfehler erhalten.

8.5. Dateirechte setzen

Nach dem Upload ist die Dateimaske für die Datendatei und die Signaturdatei zu setzen. Der Sender muss dabei sicherstellen, dass die UNIX-Datei-Rechte für eingelieferte Dateien auf „660“ (Eigentümer = R/W, Gruppe = R/W, Andere = <kein Zugriff>) stehen.

8.6. Umbenennung der Dateien

Erst nach erfolgreichem Transfer der Daten- und Signaturdatei (mit der Endung „.tmp“) sind diese auf die erforderliche Zielendung (.xml, .sig) umzubenennen. Dadurch wird vermieden, dass Verarbeitungsprogramme beim Datenempfänger bereits noch im Upload-Vorgang befindliche Dateien in den Zugriff nehmen. Dieses Vorgehen ist insofern wichtig, da sonst im Upload-Prozess befindliche XML abgeholt werden und diese in der weiteren Verarbeitung aufgrund des unvollständigen XML zu einem Schemafehler führen (es wird auf die Erläuterungen unter Kapitel 8.3 verwiesen).

Es ist stets zuerst die Signaturdatei und erst danach die korrespondierende Datendatei umzubenennen. Bitte beachten Sie außerdem, dass nur vollständige Lieferungen bestehend aus Datendatei und Signaturdatei aus Ihrem Upload-Verzeichnis abgeholt und verarbeitet werden.

8.7. Anmeldung am ELMA-Server unter Linux / macOS

Unter Linux / macOS kann zur Übertragung das Programm sftp benutzt werden, welches häufig bereits vorinstalliert ist. Die Optionen und Parameter zur Verwendung des Programms sind vielfältig. Eine ausführliche Beschreibung kann auf Linux Systemen mit dem Befehl man sftp angezeigt werden. Der gesamte Übertragungsvorgang kann in einer Batchdatei festgelegt und automatisiert ausgeführt werden.

Beispiel:

Kopieren Sie die Schlüsseldatei mit Ihrem privaten Schlüssel, den Sie zuvor erstellt haben (siehe Kapitel 3.2), in das Verzeichnis ~/.ssh

Ändern Sie die Dateirechte für die Datei wie folgt

chmod 600 ~/.ssh/elster.pem

(ersetzen Sie hierbei elster.pem durch den Dateinamen Ihrer Schlüsseldatei).

Eine (interaktive) Verbindung zum ELMA-Server kann dann für einen Nutzer mit der Benutzerkonto-ID 1003427800z.B. mit folgendem Befehl aufgebaut werden:

sftp elster-1003427800@elma5p.bfinv.de

Wenn Sie die Schlüsseldatei nicht im Verzeichnis abgelegt haben, müssen Sie den Pfad explizit angeben:

sftp -i elster.pem elster-1003427800@elma5p.bfinv.de

Die Batchdatei batchdatei.bat können Sie mit folgendem Befehl ausführen:

sftp –b batchdatei.bat -i elster.pem elster-1003427800@elma5p.bfinv.de

8.8. Datenübermittlung an den ELMA-Server unter Windows

Im Folgenden werden die wichtigsten Voraussetzungen, Konfigurationen und Kommandos zur Bedienung der PuTTY Suite dokumentiert. PuTTY ist eine Windowsportierung der OpenSSH-Programme. Weiterhin wird das Open Source Programm WinSCP vorgestellt, das es jedem Windowsnutzer ermöglicht, SFTP über eine komfortable graphische Oberfläche zu bedienen.

8.8.1. Datenübertragung mit dem Programm WinSCP

Mit dem Programm WinSCP kann der Datentransfer skriptgesteuert oder interaktiv durchgeführt werden. Der Datentransfers ist komfortabel per Drag and Drop über das Windows GUI möglich. Für die Darstellung kann zwischen Norton Commander und Windows Explorer gewählt werden.

Im Anmeldedialog von WinSCP müssen Sie Rechnername, Portnummer und Benutzername ausfüllen und die Schlüsseldatei im ppk-Format auswählen.

Der Rechnername lautet elma5p.bfinv.de bei Verbindung über das Internet bzw. 192.168.46.153 bei Nutzung des NdB-Verbindungsnetzes.

Ihr Benutzername entspricht Ihrer Benutzerkonto-ID ergänzt durch das Präfix „elster-“.

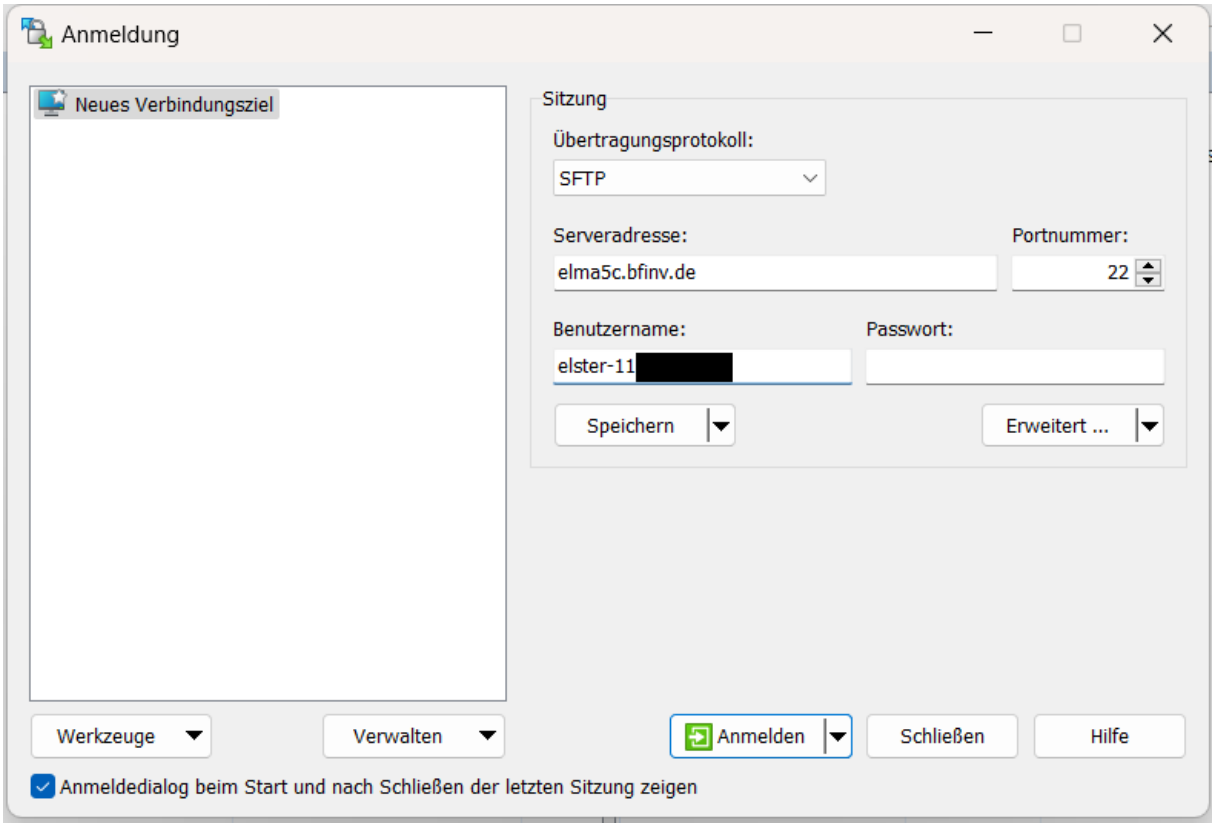

Abbildung 23: WinSCP - Anmeldung

Nach einem Klick auf „Anmelden“ sehen Sie das Authentifizierungsbanner, das Sie mit einem Klick auf „Fortsetzen“ bestätigen.

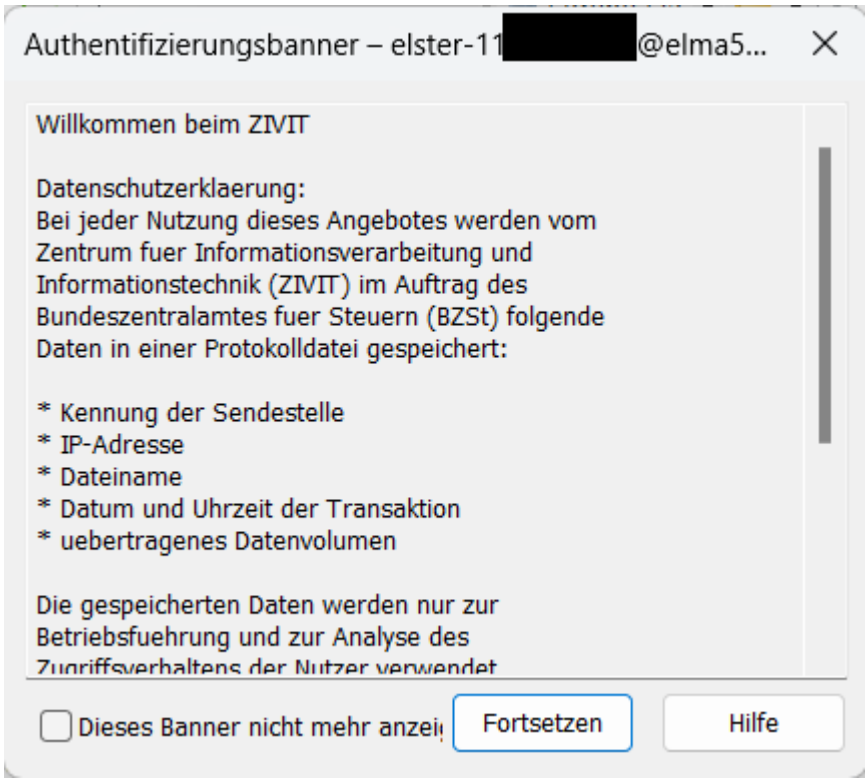

Abbildung 24: Authentifizierungsbanner

Anschließend werden Sie dazu aufgefordert Ihr Passwort einzugeben und sind dann mit dem ELMA-Server verbunden.

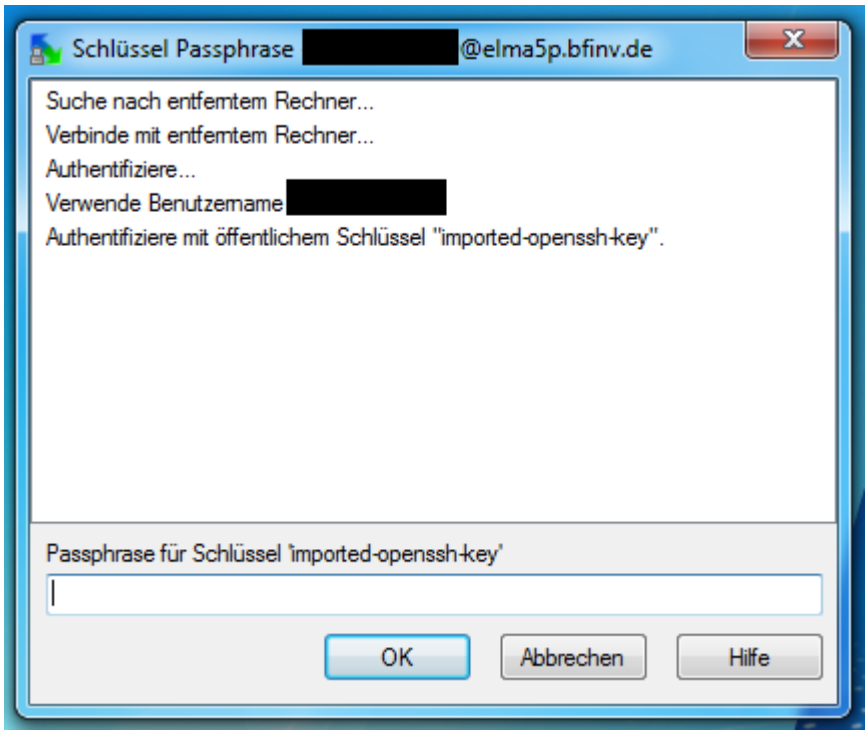

Abbildung 25: Passworteingabe

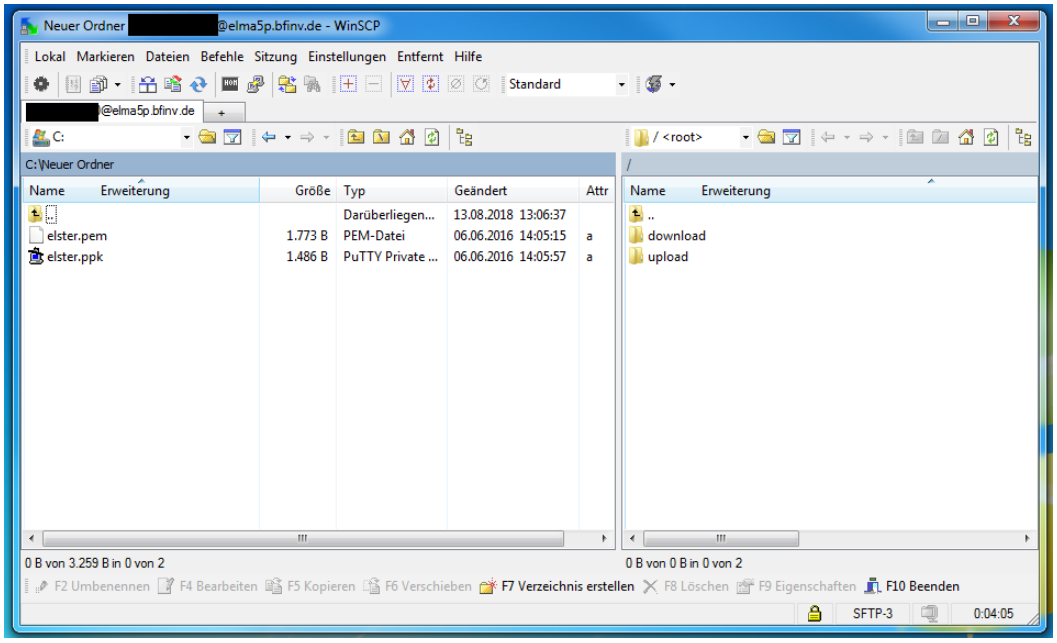

Abbildung 26: WinSCP - Ansicht Commander

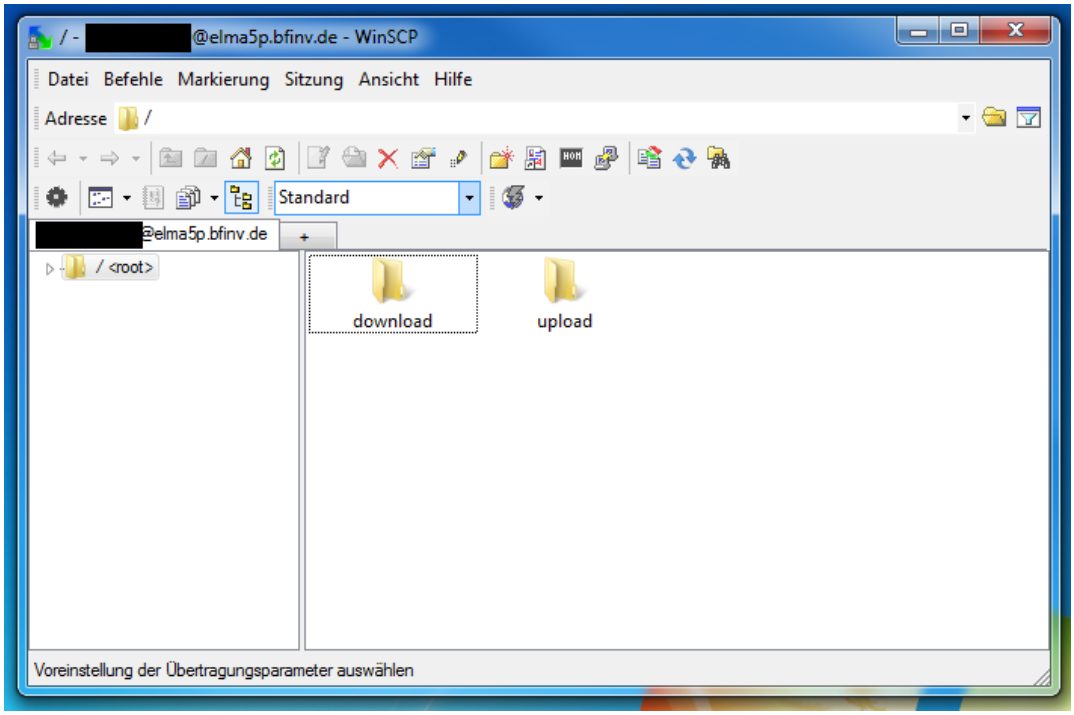

Abbildung 27: WinSCP - Ansicht Explorer

Um Dateien fehlerfrei zu übertragen, öffnen Sie bitte die Einstellungen und gehen Sie dort zum Punkt „Übertragung“. Klicken Sie anschließend auf „Bearbeiten…“

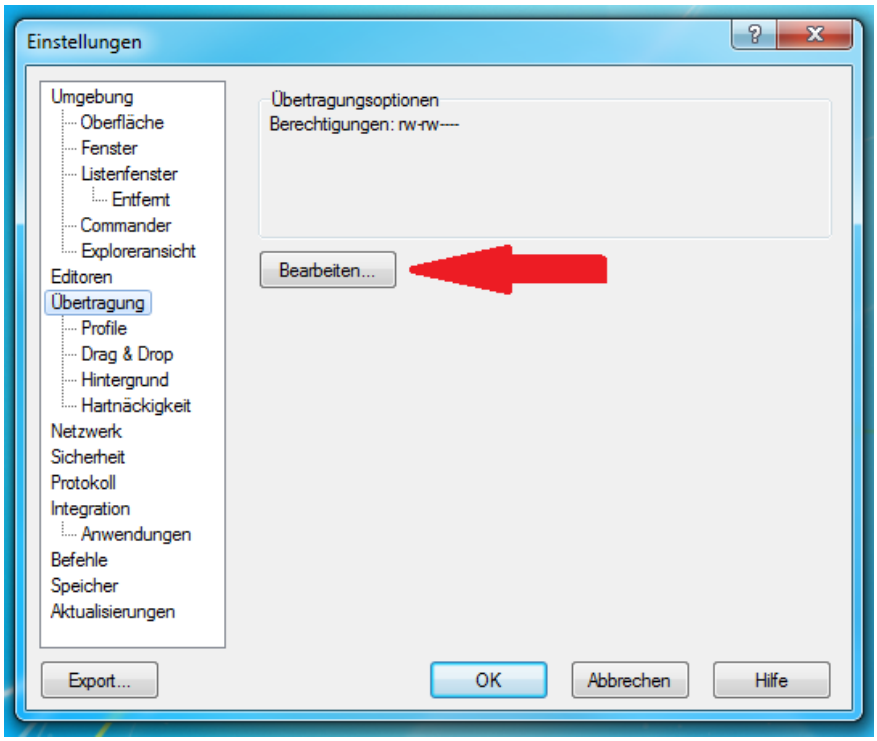

Abbildung 28: WinSCP - Einstellungen

Setzen Sie im anschließend erscheinenden Menü „Übertragungsoptionen“ den Übertragungsmodus auf „Binär (.zip, .doc, .exe, ...)“ und die Berechtigungen auf „rw-rw----“ (0660).

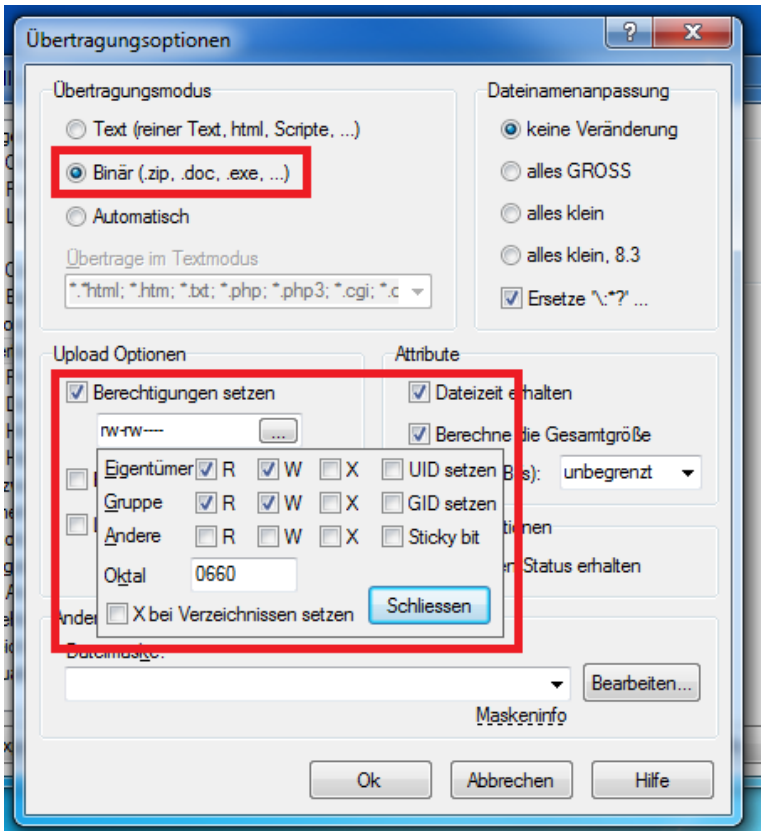

Abbildung 29: WinSCP - Übertragungsoptionen

9. Prüfungen und Rückmeldungen der ELMA-Schnittstelle

9.1. ELMA Eingangsprüfungen

Nach der Einlieferung einer Datei in das Upload-Verzeichnis der Massendatenschnittstelle ELMA werden formale Prüfungen vorgenommen. Es wird eine Feedbackdatei (in XML) erzeugt und anschließend im download-Verzeichnis bereitgestellt.

Rückmeldungen der ELMA-Schnittstelle erhalten Sie ausschließlich per Feedbackdatei. Es werden keine E-Mails mit dem Verarbeitungsstatus versendet.

9.2. Aufbau des Feedback-XML-Schemas

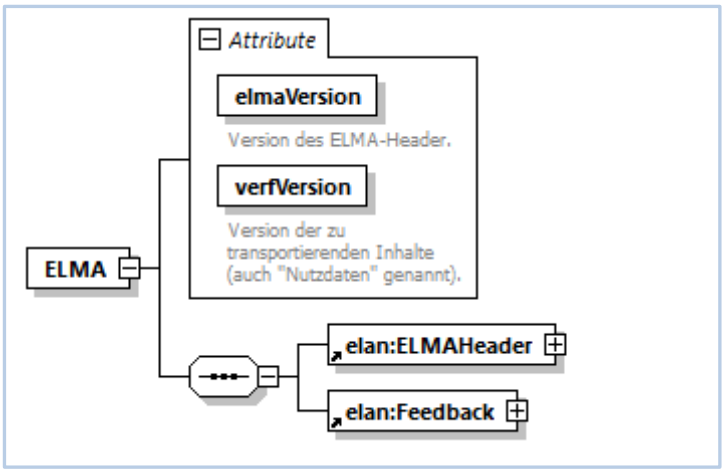

Abbildung 30: Aufbau des Feedback- XML-Schemas

Wie die Sendedatei besteht auch die Feedbackdatei aus dem Wurzelelement ELMA und dem ELMAHeader. Anstelle verfahrensspezifischer Nutzdaten enthält sie das Element Feedback.

9.2.1. Inhalte des Elements ELMAHeader

Ist der ELMA-Umschlag valide, wird das Element ELMAHeader in der Feedbackdatei wie folgt befüllt:

Element	Inhalt / Erläuterung	Bemerkungen
BenutzerkontoID	Kennung des Benutzerkontos in Mein BOP	Wird aus dem auslösenden Transport übernommen

Transportweg	Datenart	Die Datenart der Feedbackdatei	fest „Feedback“
Transportweg	Umgebung	Unterscheidung zwischen Produktiv- und Prüfumgebung	Wird aus dem auslösenden Transport übernommen
Identifizierung	EingangsID	EingangsID der Sendedatei	Wird aus dem auslösenden Transport übernommen
Identifizierung	BezugsID	BezugsID der Sendedatei	Wird aus dem auslösenden Transport übernommen
Identifizierung	AusgangsID	Eindeutige Identifizierung des Transports	Wird durch ELMA gesetzt
Zeitpunkte	Erstellung	Zeitpunkt der Erstellung der Sendedatei	Wird aus dem auslösenden Transport übernommen
Zeitpunkte	Eingang	Zeitpunkt des Eingangs der Sendedatei auf dem ELMA-Server	Wird durch ELMA gesetzt
Zeitpunkte	Verarbeitung	Zeitpunkt der Verarbeitung der Sendedatei durch die ELMA-Schnittstelle	Wird durch ELMA gesetzt

Tabelle 5: Inhalte des ELMAHeaders der Feedbackdatei bei Validität des ELMA-Headers

Ist der ELMA-Umschlag nicht valide oder werden in der Datei nicht UTF-8-konforme Zeichen verwendet, können keine Informationen aus dem auslösenden Transport übernommen werden. Aus diesem Grund werden in diesem Fehlerfall die Elemente im ELMAHeader wie folgt befüllt:

Element		Inhalt / Erläuterung	Bemerkungen
Transportweg	Datenart	Die Datenart der Feedbackdatei	fest „Feedback“
Transportweg	Umgebung	Unterscheidung zwischen Produktiv- und Prüfumgebung	Wird durch ELMA gesetzt
Identifizierung	EingangsID	EingangsID der Sendedatei	Wird durch ELMA gesetzt

		Entspricht der AusgangsID	
Identifizierung	AusgangsID	Eindeutige Identifizierung des Transports	Wird durch ELMA gesetzt
Zeitpunkte	Erstellung	Zeitpunkt der Erstellung der Sendedatei Entspricht der Verarbeitung	Wird durch ELMA gesetzt
Zeitpunkte	Verarbeitung	Zeitpunkt der Verarbeitung der Sendedatei durch die ELMA-Schnittstelle Verarbeitung = Erstellung	Wird durch ELMA gesetzt

Tabelle 6: Inhalte des ELMAHeaders der Feedbackdatei bei fehlender Validität des ELMA-Headers

9.2.2. Aufbau des Elements Feedback

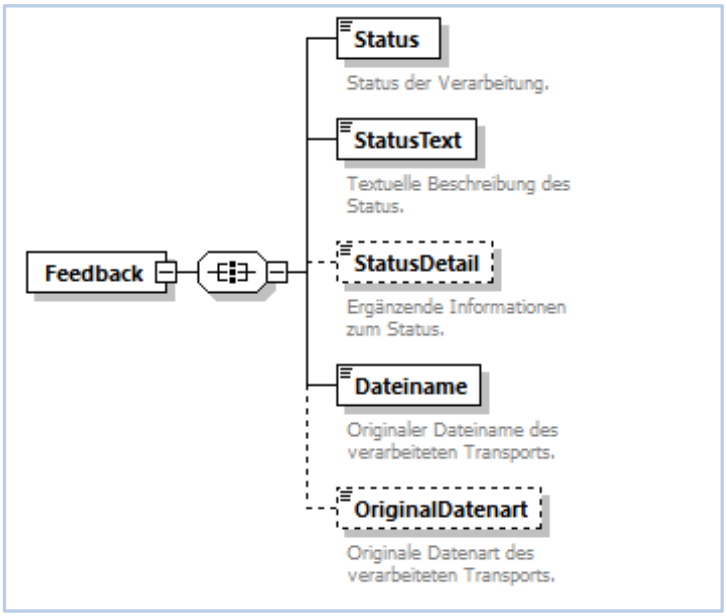

Abbildung 31: Aufbau des Elements Feedback

Nachfolgende Tabelle beschreibt die Befüllung des Elements Feedback:

Element	Inhalt / Erläuterung	Bemerkungen
Status	alphanumerische Zeichenfolge, die den Status des Transports beschreibt	siehe Tabelle 8: Übersicht möglicher Status
StatusText	kurze Beschreibung des Status	

StatusDetail	ergänzender Text mit einer detaillierteren Erklärung zum Status	
Dateiname	Dateiname der Sendedatei	
OriginalDatenart	Datenart der Sendedatei	Aus dem auslösenden Transport übernommen

Tabelle 7: Inhalte des Elements Feedback

9.2.3. Beispiel

Das im untenstehenden Beispiel genannte Namespacepräfix steht hier lediglich beispielhaft. Es kann sich in Ihren tatsächlichen Feedback-Dateien unterscheiden und kann sich auch ändern.

Ebenso ist die Präzision des Sekundenbruchteils in den Zeitstempeln nicht festgelegt.

```
<n1:ELMA xmlns:n1="http://www.itzbund.de/elan"
xmlns:elan="http://www.itzbund.de/elan/elemente" elmaVersion="2" verfVersion="1.0.0">
    <elan:ELMAHeader>
        <elan:BenutzerkontoID>6098575621</elan:BenutzerkontoID>
        <elan:Transportweg>
            <elan:Datenart>Feedback</elan:Datenart>
            <elan:Umgebung>PRODUKTION</elan:Umgebung>
        </elan:Transportweg>
        <elan:Identifizierung>
            <elan:EingangsID>fe8test2-18d6-45c8-bbf9-32e991test63</elan:EingangsID>
            <elan:AusgangsID>is3337oho8cfcm513k1tjpgd8v1f0xa2</elan:AusgangsID>
        </elan:Identifizierung>
        <elan:Zeitpunkte>
            <elan:Erstellung>2020-11-28T09:27:47Z</elan:Erstellung>
            <elan:Eingang>2020-11-28T09:39:27.863482919+01:00</elan:Eingang>
            <elan:Verarbeitung>2020-11-28T10:00:02.484126+01:00</elan:Verarbeitung>
        </elan:Zeitpunkte>
    </elan:ELMAHeader>
    <elan:Feedback>
        <elan:Status>ER0000</elan:Status>
        <elan:StatusText>Das enthaltene XML entspricht nicht dem erwarteten
Schema.</elan:StatusText>
        <elan:StatusDetail>cvc-complex-type.2.4.a: Ungültiger Inhalt beginnend mit Element
'verf:ElementZ' wurde gefunden. Eines der Attribute '{"http://www.itzbund.de/elan/test/01":ElementA,
"http://www.itzbund.de/elan/test/01":ElementB, "http://www.itzbund.de/elan/test/01":ElementC}'
wurde erwartet.</elan:StatusDetail>
        <elan:Dateiname>TestDatenart.fe8test2-18d6-45c8-bbf9-32e991test63.xml</elan:Dateiname>
        <elan:OriginalDatenart>TestDatenart</elan:OriginalDatenart>
    </elan:Feedback>
</n1:ELMA>
```

9.3. Prüfungen und Status

Die ELMA-Schnittstelle führt die folgenden Eingangsprüfungen durch:

a) Dateigröße: Prüft, dass die Dateigröße 200 MB nicht überschreitet.
b) Zeichensatz: Prüft, dass die Datei mit dem erwarteten Zeichensatz (UTF-8) kompatibel ist.
c) Schema-Validierung: Prüft, dass die Datei dem erwarteten Schema entspricht.
d) Eingangs-ID eindeutig: Prüft, dass die Eingangs-ID noch nicht verwendet wurde.
e) Bezugs-ID bekannt: Prüft, dass die Bezugs-ID (sofern angegeben) bekannt ist.
f) Umgebung erlaubt: Prüft, dass die angegebene Umgebung dem aktuellen System entspricht.
g) Benutzer ist gültig: Prüft, dass der Benutzer aktiv (nicht stillgelegt und nicht gesperrt) ist.
h) Verfahrensfreischaltung: Prüft, dass der angegebene Benutzer eine aktive Freischaltung zum Fachverfahren besitzt.
i) Signatur Valide: Prüft, dass die Signatur zu einem Transport verifiziert werden kann.
j) Dateiname eindeutig: Prüft, dass der Dateiname noch nicht verwendet wurde.

Nachfolgend eine Liste der möglichen Status, die über Feedbackdateien mitgeteilt werden kann:

Status	Beschreibung
OK0000	Die Datei hat die Eingangsprüfung erfolgreich absolviert und wurde weitergeleitet.
ER0000	Das enthaltene XML entspricht nicht dem erwarteten Schema.
ER0001	Die Datei verwendet einen unerwarteten Zeichensatz.
ER0002	Die Kombination von Datenart und Version ist unbekannt.
ER0003	Die Datei ist zu groß.
ER0004	Die Eingangs-ID wurde bereits verwendet.
ER0006	Die Bezugs-ID ist unbekannt.

ER0008	Die BZSt-Nummer ist für das Fachverfahren gesperrt.
ER0010	Das Benutzerkonto ist für das Fachverfahren gesperrt.
ER0014	Die BZSt-Nummer hat keine Zulassung zum Fachverfahren.
ER0016	Die Validierung der Datei mit der Signatur ist fehlgeschlagen.
ER0017	Die gesetzte Umgebung ist ungültig in diesem System.
ER0019	Die BZSt-Nummer ist stillgelegt.
ER0020	Das Benutzerkonto ist stillgelegt.
ER0024	Das Benutzerkonto ist unbekannt.
ER0026	Der Dateiname wurde bereits verwendet.

Tabelle 8: Übersicht möglicher Status

9.4. Namenskonvention für die Feedbackdatei

Die Namen der abgelegten Feedbacks entsprechen grundsätzlich dem vom Absender deklarierten Namen der Sendedatei. ELMA wird im Zuge der Verarbeitung einen Zeitstempel voranstellen um sicherzustellen, dass die Dateinamen in dem Verzeichnis eindeutig bleiben und somit nicht überschrieben werden.

Aufbau: <Zeitstempel>_<Sendedatei-Name>.xml

Der Aufbau des Elements <Sendedatei-Name> ergibt sich aus dem Kapitel 6.2.5 (Namenskonventionen für die Datendatei).

Element		Inhalt / Erläuterung	Bemerkungen
Zeitstempel	Timestamp	yyyy-mm-dd'T'HH-MM-SS.SSSXX	Das XX steht für die mitteleuropäische Zeitzonenangabe im Format +0100 bzw. +0200.

Beispiel für eine Feedbackdatei:

2023-05-26T10-10-17.838+0200_DATENART.1234567890.DateiIDAnfrage.xml

10. Informationen des Fachverfahrens

10.1. Aufbau des XML-Schemas

Der Aufbau der XML-Datei entspricht dem Aufbau der Sendedatei des ELMA-Nutzers. Die Information des Fachverfahrens ist Teil der verfahrensspezifischen Nutzdaten.

10.1.1. Inhalte des Elements ELMAHeader

Der ELMAHeader wird in einer Information des Fachverfahrens wie folgt befüllt.

Element		Inhalt / Erläuterung	Bemerkungen
BenutzerkontoID		Kennung des Benutzerkontos in Mein BOP (Empfänger der FV-Information)	Wird durch das Fachverfahren gesetzt.
Transportweg	Datenart	Die Datenart für die Information des Fachverfahrens	siehe Tabelle 1 0.2 teilnehmende Fachverfahren
Transportweg	Umgebung	Unterscheidung zwischen Produktiv- und Prüfumgebung	Wird durch ELMA gesetzt.
Identifizierung	EingangsID	Durch das Fachverfahren festgelegte Identifizierung des Transports der Information	Wird durch das Fachverfahren gesetzt Format: UUID
Identifizierung	BezugsID	EingangsID der Sendedatei, auf die sich die Information bezieht	Wird durch das Fachverfahren gesetzt Format: UUID

Identifizierung	AusgangsID	Eindeutige Identifizierung des Transports	Wird durch ELMA gesetzt Format: 32-stellig alphanumerisch
Zeitpunkte	Erstellung	Zeitpunkt der Erstellung der Information im Fachverfahren	Wird durch das Fachverfahren gesetzt
Zeitpunkte	Eingang	Zeitpunkt des Eingangs der Information auf dem ELMA-Server	Wird durch ELMA gesetzt
Zeitpunkte	Verarbeitung	Zeitpunkt der Verarbeitung der Information durch die ELMA-Schnittstelle	Wird durch ELMA gesetzt

Tabelle 9: Inhalte des ELMAHeaders der Rückmeldung des Fachverfahrens

10.1.2. Aufbau der Information des Fachverfahrens

Der Aufbau der Information des Fachverfahrens ist der Schnittstellenbeschreibung des jeweiligen Verfahrens und den durch das Fachverfahren bereitgestellten XML-Schemata zu entnehmen.

10.2. Namenskonvention für die Information des Fachverfahrens

Die Namen der Rückmeldungsdateien entsprechen grundsätzlich dem vom Fachverfahren deklarierten Namen. ELMA wird im Zuge der Verarbeitung einen Zeitstempel voranstellen um sicherzustellen, dass die Dateinamen in dem Verzeichnis eindeutig bleiben und somit nicht überschrieben werden.

Die DateiID entspricht dabei in der Regel **nicht** der DateiID der Sendedatei, auf die sich die Rückmeldung bezieht.

Der dritte Dateinamensbestandteil DateiID2 ist optional. Die Nutzung und der tatsächliche Inhalt obliegt den einzelnen Fachverfahren und ist den verfahrensspezifischen Kommunikationshandbüchern zu entnehmen.

Aufbau: <Zeitstempel>_<Datenart>.<DateiID><optional:.DateiID2>.xml

Element		Inhalt / Erläuterung	Bemerkungen
Zeitstempel	Timestamp	yyyy-mm-dd'T'HH-MM-SS.SSSXX	Das XX steht für die mitteleuropäische Zeitzonenangabe im Format +0100 bzw. +0200.

Beispiel für eine Information des Fachverfahrens:

2023-05-26T10-10-17.838+0200_DATENART.<DateiID><optional:.DateiID2>.xml

11. Zusätzliche Informationen

11.1. Beispiel der XML-Elemente zur „Identifizierung“

Dieses Beispiel zeigt den Ablauf der Identifikationsmerkmale für zwei Transporte (Transport von einem Benutzer, worauf das Fachverfahren anschließend reagiert). Zur visuellen Unterstützung sind die gleichen Inhalte mit der gleichen Farbe markiert.

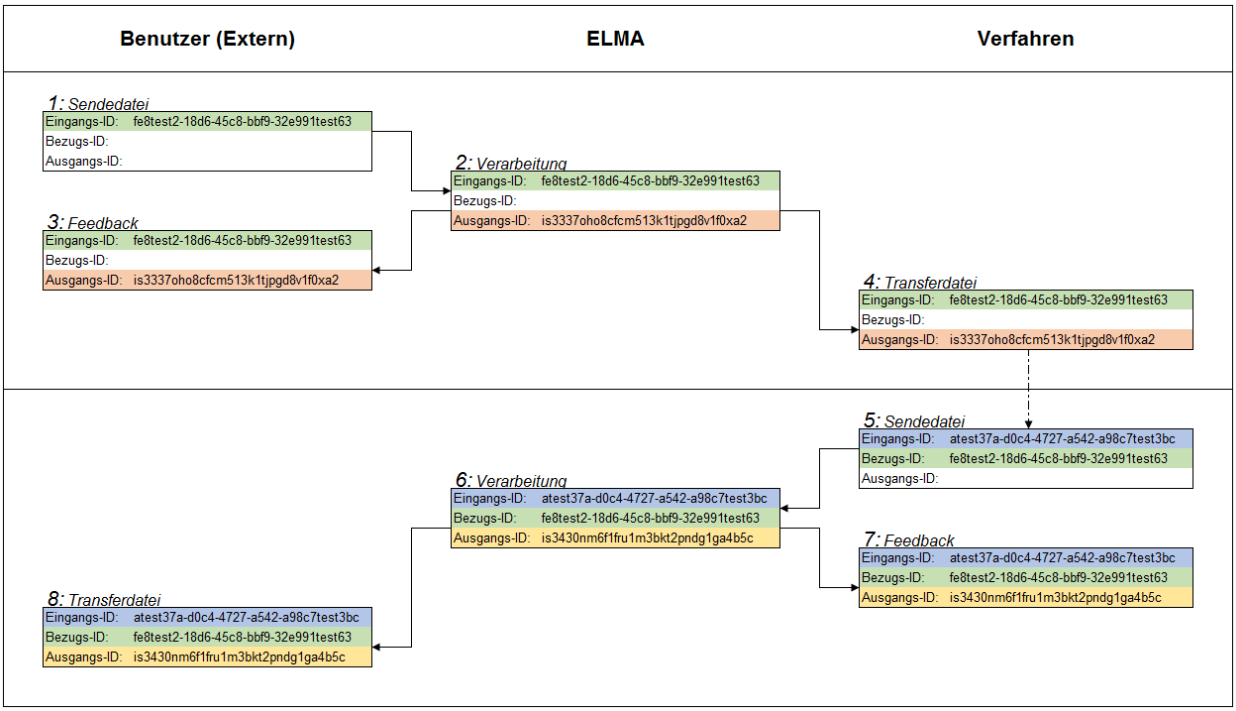

Abbildung 32: Beispielablauf der Identifikationsmerkmale

11.2. Beispiel für Namenskonventionen im Download-Verzeichnis

Dieses Beispiel zeigt die zu erwartenden Dateien im Download-Verzeichnis.

	Dateiname und Datenart Sendedatei		**Dateiname und Datenart Download-Verzeichnis**	
Anfrage ELMA-Kunde (vgl. Abschnitt 6)	Dateiname	BEISPIEL.1234567890.a-b-c-d.xml	Dateiname	2023-12-01T09-00-00.123+0100_BEISPIEL.1234567890.a-b-c-d.xml

	Datenart	BEISPIEL	Datenart	FEEDBACK
Information des Fachverfahrens (vgl. Abschnitt 10)	Dateiname	BEISPIELRM.e-f-g-h[.a-b-c-d].xml	Dateiname	2023-12-02T07-00-00.456+0100_BEISPIELRM.e-f-g-h[.a-b-c-d].xml
	Datenart	BEISPIELRM	Datenart	BEISPIELRM

Tabelle 10: Namenskonventionen im Download-Verzeichnis

12. Abkürzungsverzeichnis/Glossar

Begriff	Abkürzung	Begriffserklärung
Aktivierungs-Code		Persönlicher Code zur Aktivierung des jeweiligen Benutzerkontos im BZStOnline-Portal (BOP).
Aktivierungs-ID		Persönliche Kennung zur Aktivierung des jeweiligen Benutzerkontos im BOP.
Benutzerkonto		Benutzerkonto im BZStOnline-Portal (BOP)
Benutzerkontoinhaber		Vom ELAN-Nutzer angelegter Nutzer für BZStOnline-Portal (BOP)
Bundeszentralamt für Steuern	BZSt	Das Bundeszentralamt für Steuern ist eine zum 1. Januar 2006 gegründete Bundesoberbehörde in Deutschland, die direkt dem Bundesministerium der Finanzen unterstellt ist.
BZSt-Geheimnis		Das BZSt-Geheimnis ist ein eindeutig vergebener textueller Schlüssel, der nur dem ELAN-Nutzer oder dem Portalkontoinhaber bekannt ist. Dieses wird bei der erstmaligen Beantragung einer BZSt-Nummer vergeben und ist daher u.a. auch für Anträge bei Folgeverfahren aufzubewahren.
BZSt-Nummer		Die BZSt-Nummer ist eine eindeutig vergebene Nummer für den ELAN-Nutzer.
BZStOnline-Portal	BOP	Das BZStOnline-Portal bietet eine Reihe von Diensten, Formularen und zusätzlichen Funktionen, mit denen Privatpersonen, Unternehmen, Steuerberater Daten zu Steuerbelangen ans BZSt übermitteln können.
Byte Order Mark	BOM	Die Bytereihenfolge Markierung wird am Anfang einer XML-Datendatei durch das Unicode Zeichen U+FEFF (zero with no-break space) implementiert.
BOP-Zertifikat		Das BOP-Zertifikat ist eine während des Registrierungsvorganges im BOP erstellte Datei. Das Software-Zertifikat dient zur Identifizierung beim Login ins BZStOnline-Portal und ermöglicht den Zugriff auf das persönliche Benutzerkonto. Die Nutzung der Massendatenschnittstelle ELMA setzt ein BOP-Zertifikat der Registrierungsart ELSTERBasis voraus.

Begriff	Abkürzung	Begriffserklärung
Elektronische Antragstellung	ELAN	Die Elektronische Antragstellung (ELAN) bietet dem Antragsteller die Möglichkeit, über Online-Formulare oder durch die Massendatenübermittlung Daten an das BZSt zu übermitteln. Voraussetzung dafür ist der Besitz eines Elster- oder BOP-Zertifikates.
ELAN-Nutzer		BOP-Nutzer, der die Erstanmeldung am BOP mit der BZSt-Nummer und dem BZSt-Geheimnis ausgeführt hat.
Elektronische Massendatenschnittstelle ELMA	ELMA (-SST)	Verfahren zur elektronischen Übertragung von Massendaten über SFTP
ELMA-Server		Physikalischer SFTP-Verbindungspunkt für den Up- und Download.
ELSTER Online-Portal	EOP	ELSTER Online Portal
Extensible Markup Language	XML	XML ist eine Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten. Diese wird u.a. beim Austausch Massendaten über ELMA verwendet.
Informationstechnik-zentrum Bund	ITZBund	EDV-Dienstleister der Bundesfinanzverwaltung
Kommunikationshandbuch	KHB	Im Kommunikationshandbuch werden die technischen und fachlichen Modalitäten für den Datenaustausch festgelegt.
Massendaten-Lieferung		Vom Anwender unter Verwendung der Massendatenschnittstelle ELMA bereitgestellte Daten.
Passphrase		Passwort für das BOP-Zertifikat im Rahmen der ELMA-Datenübermittlung
Secure File Transfer Program	SFTP	Ist ein interaktives Programm, mit dem der Anwender vor dem eigentlichen Transfer Verzeichnisse und deren Inhalt auf dem Server einsehen und Kommandos auf dem Server ausführen kann.
Secure Shell	SSH	SSH ist sowohl ein Programm als auch ein Netzwerkprotokoll, mit dessen Hilfe man Daten gesichert über das Internet übertragen kann.

Begriff	Abkürzung	Begriffserklärung
Zeitstempel der Lieferdatei	Timestamp	Der Zeitstempel gibt das Datum und die Zeit der Erstellung einer Lieferung seitens des Senders an.
Unicode Transformation Format	UTF	UTF ist eine Methode, Unicode-Zeichen auf Folgen von Bytes abzubilden.
8-Bit Universal Character Set Transformation Format	UTF-8	Zu verwendende Kodierung für Unicode-Zeichen. Die entsprechenden Normendokumente werden von der IETF, dem Unicode Consortium und der ISO gegenwärtig identisch definiert: • RFC 3629 / STD 63 (2003) • The Unicode Standard, Version 4.0, §3.9–§3.10 (2003) • ISO/IEC 10646-1:2000 Annex D (2000)
Universally Unique Identifier	UUID	Ist ein für die Identifikation in der Softwareentwicklung verwendeter Standard für die Kennzeichnung von Informationen in verteilten Systemen.
XML-Schema-Definition	XSD	Die XML Schema Definition enthält Definitionen von Strukturen für XML-Dokumente.

Tabelle 11: Abkürzungsverzeichnis/Glossar

Impressum

Herausgeber:
Bundeszentralamt für Steuern
An der Küppe 1
53225 Bonn
Telefon: +49 228 406-0
Internet: www.bzst.de

Stand:
Version 2.6 27.01.2025

Bildnachweis:
Titelseite: Hardy Welsch (http://www.hardy-welsch.de)

Text:
BZSt