



Bundeszentralamt  
für Steuern

# Kommunikationshandbuch ELMA-Standard 1.0

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

Dokumenten-Version: 2.1  
Stand: 24.07.2024





## Inhaltsverzeichnis

<b>Inhaltsverzeichnis</b> .....	<b>2</b>
<b>Abbildungsverzeichnis</b> .....	<b>4</b>
<b>Tabellenverzeichnis</b> .....	<b>4</b>
<b>0. Informationen zum vorliegenden Dokument</b> .....	<b>6</b>
0.1. Änderungshistorie.....	6
0.2. Teilnehmende Fachverfahren .....	9
0.3. Aufbau und Zweck des Dokuments.....	10
0.3.1. Zielgruppe und Voraussetzungen.....	10
0.4. Änderung des Schlüsselformats .....	10
<b>Teil I Allgemeine Informationen</b> .....	<b>12</b>
<b>1. Technische Voraussetzungen zur Nutzung der ELMA-SST</b> .....	<b>12</b>
1.1. Systemvoraussetzungen .....	12
1.1.1. Für den Hardware-Einsatz .....	12
1.1.2. Für den Software-Einsatz.....	12
1.2. Internetanbindung und Bandbreite .....	13
1.3. Firewall Konfiguration .....	13
1.4. Identifizierung, Verbindung.....	13
1.5. Verfügbarkeit .....	13
<b>2. Technische Beschreibung der Kommunikation</b> .....	<b>13</b>
2.1. Grundlagen.....	13
2.2. X.509 Authentifikation .....	14
2.3. Schlüssellebensdauer.....	14
2.4. Username und Passwort Authentifikation .....	14
<b>3. Registrierung und Freischaltung</b> .....	<b>14</b>
3.1. Registrierung am BZStOnline-Portal (BOP).....	14
3.2. Erzeugung des Schlüsselpaars .....	15
3.3. Freischaltung zur Teilnahme am ELMA-Verfahren .....	16
<b>4. Verbindungsprüfung zum ELMA-Server</b> .....	<b>18</b>
4.1. Freischaltung für SSH2 über Port 22 .....	18
4.2. IP-Adresse des ELMA-Servers ermitteln.....	19
4.3. DNS-Namenauflösung steht nicht zur Verfügung.....	19
4.3.1. Ergänzung der hosts-Tabelle unter Windows.....	20



4.3.2.	Ergänzung der hosts Tabelle unter MAC OS.....	22
4.3.3.	Ergänzung der hosts-Tabelle unter Linux.....	22
4.4.	Verwendung eines Proxys für den Internetzugang .....	23
4.5.	Übertragung ohne Port 22-Freischaltung.....	23
<b>5.</b>	<b>Einrichtung der Übertragungskomponente.....</b>	<b>23</b>
5.1.	OpenSSL-Installation.....	23
5.1.1.	OpenSSL-Installation unter Linux.....	24
5.1.2.	OpenSSL-Installation unter Mac OS .....	24
5.1.3.	OpenSSL-Installation unter Windows.....	24
5.2.	OpenSSH-Installation .....	25
5.2.1.	OpenSSH-Installation unter Linux.....	25
5.2.2.	OpenSSH Installation unter Mac OS .....	25
5.2.3.	OpenSSH-Installation unter Windows .....	25
5.3.	Einrichtung der Übertragungsumgebung für Linux Systeme .....	25
<b>6.</b>	<b>Übertragung der Daten- und Signatur-Datei .....</b>	<b>26</b>
6.1.	Abgrenzung zum XML-Upload über BOP .....	26
6.2.	Aufbau der Verbindung.....	27
6.3.	Ablauf der Datenübertragung.....	29
6.3.1.	Signaturdatei.....	29
6.3.1.1.	Namenskonvention für die Signaturdatei .....	30
6.3.1.2.	Erstellung Signaturdatei.....	30
6.3.1.2.1.	Linux.....	30
6.3.1.2.2.	MAC OS .....	30
6.3.1.2.3.	Windows.....	31
6.4.	Upload .....	32
6.5.	Dateirechte setzen.....	32
6.6.	Umbenennung der Dateien.....	32
<b>Teil II</b>	<b>Weitergehende Informationen für Verfahren mit ELMA-Standard.....</b>	<b>33</b>
<b>7.</b>	<b>Anforderungen an die zu übertragende Datendatei .....</b>	<b>33</b>
7.1.	ELMA- Standard .....	33
7.2.	Aufbau der Datendatei (Wurzelement und ELMA-Header).....	34
7.3.	XSD-Schema Validierung .....	37
7.4.	UTF-8 Kodierung .....	38
7.5.	Unzulässige Zeichen und Beschränkungen.....	38



7.6.	Dateigrößenbeschränkung .....	38
7.7.	Namenskonvention für die Datendatei.....	38
<b>8.</b>	<b>Prüfungen und Rückmeldungen zu den übertragenen Dateien .....</b>	<b>41</b>
8.1.	ELMA Eingangsprüfungen .....	41
8.1.1.	ELMAPROTOKOLL - XSD .....	41
8.1.2.	Rückmeldungen von ELMA (StatusIDs) .....	45
8.1.3.	Abfolge der ELMA Dateiprüfung .....	47
8.1.4.	Rückmeldung zum Ergebnis der ELMA-Prüfung.....	50
8.2.	Prüfungen im Fachverfahren .....	51
8.3.	Abholung Rückmeldedatei(en) .....	51
8.3.1.	Namenskonvention für die Rückmeldedatei.....	52
<b>9.</b>	<b>Referenzdokumente .....</b>	<b>52</b>
<b>10.</b>	<b>Abkürzungsverzeichnis/Glossar.....</b>	<b>53</b>

## Abbildungsverzeichnis

Abbildung 1: BOP > Formulare & Leistungen > Versand von Massendaten (ELMA5).....	16
Abbildung 2: Lokalisierung der "hosts" Datei im Explorer .....	20
Abbildung 3: Datei mit Editor öffnen.....	20
Abbildung 4: Ergänzung der hosts-Datei um elma5p Servereintrag .....	21
Abbildung 5: Dateityp bei Speicherung setzen .....	21
Abbildung 6: Anmeldemaske in WinSCP .....	28
Abbildung 7: Fenster zur Passwortabfrage des ELMA5-Zertifikats .....	28
Abbildung 8: Anmeldemaske in FileZilla.....	28
Abbildung 9: Fenster zur Passwortabfrage des ELMA5-Zertifikats .....	29
Abbildung 10: Aufruf des Terminals über die Spotlight-Suche unter macOS .....	31
Abbildung 11: Beispiel mit ELMADC als Root-Element für das Fachverfahren DAC6.....	34
Abbildung 12: Aufbau ELMA-Datei mit Detailsicht auf den standardisierten ELMA-Header.....	35
Abbildung 13: Aufbau des standardisierten ELMAProtokolls am Beispiel DAC6.....	42

## Tabellenverzeichnis

Tabelle 1: Befüllung des ELMAHeaders .....	37
Tabelle 2: Aufbau Dateinamen bei Lieferung .....	40
Tabelle 3: Befüllung des standardisierten ELMAProtokolls.....	44
Tabelle 4: ELMA StatusID 8000 (fehlerfreie Verarbeitung in ELMA) .....	45
Tabelle 5: Liste der möglichen ELMA StatusIDs (Fehlercodes) .....	47
Tabelle 6: Abfolge der ELMA Prüfungen und deren Fehlercodes .....	50
Tabelle 7: Weitere ELMA Fehlergründe .....	50



Tabelle 8: Referenzdokumente .....	52
Tabelle 9: Abkürzungsverzeichnis/Glossar .....	55



## 0. Informationen zum vorliegenden Dokument

Dokumententitel	Kommunikationshandbuch ELMA-Standard Standardisierte Datenübermittlung an das BZSt über die Massendatenschnittstelle ELMA (verfahrenübergreifende technische Beschreibung)
Verantwortlicher Autor	Bundeszentralamt für Steuern
Erstellt am	01.07.2020
Zuletzt geändert am	24.07.2024

### 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	<p>Kapitel 0.2: Ergänzung weiterer Fachverfahren</p> <p>Kapitel 0.3.1: Hinweis auf Fremdanbieter aufgenommen</p> <p>Kapitel 6.1: Konkretisierungen zum XML-Upload</p> <p>Kapitel 7: Neues Kapitel 7.1 zum ELMA-Standard eingefügt</p> <p>Kapitel 7.2: Anpassung „Verarbeitungslauf“ in Tabelle 1</p> <p>Kapitel 7.3: Information zur Namespace-Reihenfolge aufgenommen</p> <p>Kapitel 8.1.1: Verweis auf ELMA-Standard bezgl. ELMAProtokoll aufgenommen</p> <p>Kapitel 8.1.2: Fehlertext 8013 in Tabelle 5 angepasst</p> <p>Kapitel 9: Neues Kapitel „Referenzdokumente“ eingefügt und XSD zum ELMA-Standard abgelegt</p>



Dokument Version	Datum	Änderung
2.1	24.07.2024	<p>Neues Kapitel 0.4: Änderung des Schlüsselformats</p> <p>Kapitel 1.1.2: Ergänzung sicherheitsrelevanten Hinweises</p> <p>Kapitel 1.4: Änderungen Authentifizierung an der Übertragungskomponente</p> <p>Kapitel 2.2: Änderungen zur Authentifikation am ELMA-Server</p> <p>Neues Kapitel 2.3: Schlüssellebensdauer</p> <p>Kapitel 3.1: Aktualisierung bei Registrierung im BOP</p> <p>Neues Kapitel 3.2: Erzeugung des Schlüsselpaars</p> <p>Kapitel 3.3: Änderung am Freischaltungsantrag BOP</p> <p>Entfernt Kapitel 3.4: Zertifikat im PEM-Format</p> <p>Kapitel 4.2: Korrektur Beispiel</p> <p>Entfernt: Kapitel 5.4: PEM-Datei in das PPK-Format konvertieren</p> <p>Kapitel 6.2: Aktualisierung Hinweise</p> <p>Kapitel 6.3.1: Erstellung einer Signaturdatei mit ECDSA</p> <p>Kapitel 6.3.1.1: Anpassung der Namenskonvention</p> <p>Kapitel 6.3.1.2: Ergänzung Hinweis zur Erstellung Signaturdatei</p> <p>Kapitel 6.3.1.2.1: Anpassung Anwendungsbeschreibung LINUX</p> <p>Kapitel 6.3.1.2.2: Anpassung Anwendungsbeschreibung MAC OS</p> <p>Kapitel 6.3.1.2.3: Anpassung Anwendungsbeschreibung Windows</p> <p>Kapitel 6.6: Ergänzung Hinweis zur Datenübermittlung</p> <p>Kapitel 8.1.1: Anpassung der StatusIDs</p> <p>Kapitel 8.1.2: Anpassung der StatusIDs</p> <p>Kapitel 8.1.3: Anpassung der StatusIDs</p>





## 0.2. Teilnehmende Fachverfahren

Fachverfahren		Verfahrens- kürzel	Datenart	Gültig ab
<b>CbCR</b>	Country-by-Country Reporting	CC	ELMA_CC	15.01.2021
<b>CRS</b>	Common Reporting Standard	CS	ELMA_CRS	01.02.2021
<b>DAC6</b>	Austausch von Steuergestaltungen	DC	ELMA_DC	01.07.2020
<b>eKIST</b>	Elektronische Kindergeldstatistik	EK	ELMA_EK	01.12.2020
<b>FAMKA</b>	IdNr- Kontrollverfahren Kindergeld	KF	ELMA_KF	01.12.2020
<b>FATCA</b>	Foreign Account Tax Compliance Act	FC	ELMA_FC	2022
<b>FSAK</b>	Freistellungsaufträgekontrollverfahren (Meldewesen)	FS	ELMA_FS	01.12.2020
<b>FSAK</b>	Freistellungsaufträgekontrollverfahren (Auskunftswesen)	FA	ELMA_FA	01.04.2021
<b>IDServ</b>	IdNr- Anfrage für Familienkassen	ID	ELMA_ID	01.12.2020
<b>KISTA</b>	Kirchensteuerabzug auf abgeltend besteuerte Kapitalerträge	KM	ELMA_KM	01.12.2020



### **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.

#### **0.3.1. Zielgruppe und Voraussetzungen**

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
- SSH Verschlüsselung mit zertifikatsbasierter Authentifizierung
- Verwendung offener Standards (alle Komponenten als OpenSource verfügbar).

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,



**Kommunikationshandbuch ELMA-Standard**  
Standardisierte Datenübermittlung an das BZSt über die  
Massendatenschnittstelle ELMA

für einen Übergangszeitraum bis voraussichtlich Mitte bzw. Ende 2025 mit der bisherigen Verzeichnisstruktur möglich.



# Teil I

## Allgemeine Informationen

Die nachfolgenden Abschnitte des Teils I - Allgemeine Informationen - gelten für alle an ELMA angebotenen 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 OpenSSH ist somit sofort nach der Grundkonfiguration möglich. Das gleiche gilt auch für die UNIX-Derivate HP-UX, AIX, OS X und viele andere.

Für die Microsoft-Windows-Betriebssysteme sind kostenfreie Programme aus dem OpenSource-Umfeld nutzbar. Hier sind die Programme PuTTYgen, PSFTP, WinSCP und OpenSSH 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 dedizierte 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 Public Private 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. X.509 Authentifikation**

Die X.509 Authentifikation basiert auf der Public-Key-Kryptographie. Es existiert dabei für jeden Benutzer ein kryptographisches Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel.

Die X.509 Datei enthält das Zertifikat, den Signaturalgorithmus und die Zertifikat-Signatur. Die Datei ist durch eine Passphrase vor missbräuchlicher Verwendung geschützt.

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.

# **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.

## **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 im BZStOnline-Portal (BOP)<sup>1</sup>. Sofern Sie dieses

---

<sup>1</sup> [www.elster.de/bportal](http://www.elster.de/bportal)



noch nicht haben, führen Sie hierzu eine Registrierung im BOP durch. Erläuterungen zum Registrierungsablauf finden Sie auf den Hilfsseiten des BOP oder in den Kommunikationshandbüchern der einzelnen Fachverfahren. 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.

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 Eingabebehinweis ein Passwort vergeben und die Eingabe nochmals mit Enter bestätigen.

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.

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

### 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 BZStOnline-Portal bietet Ihnen die Möglichkeit, diese Freischaltung online durchzuführen.

Sie finden das Formular „Antrag auf Freischaltung zur Teilnahme am ELMA-Verfahren an das BZSt“, im privaten Bereich des BZStOnline-Portals über „Formulare & Leistungen“ -> „Versand von Massendaten (ELMA5)“.

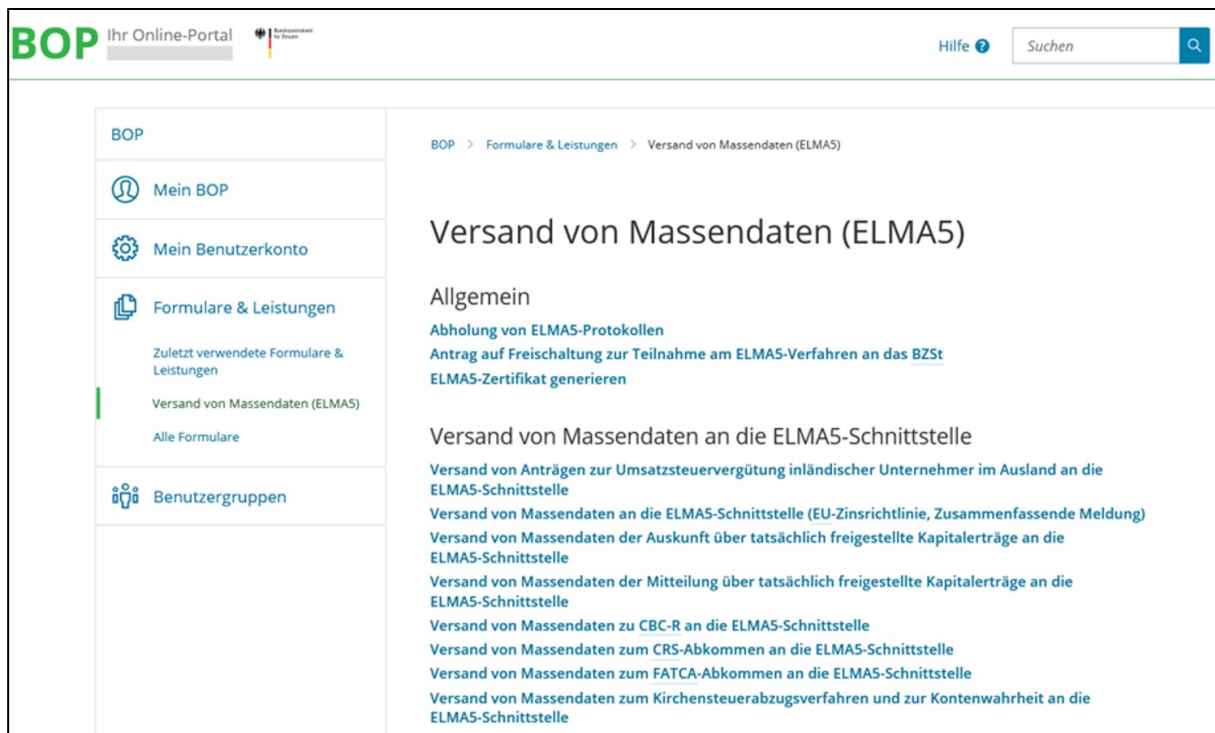


Abbildung 1: BOP > Formulare & Leistungen > Versand von Massendaten (ELMA5)

Nach Absenden des Formulars werden Ihre Eingaben auf Korrektheit geprüft. Sollten Ihre Angaben nicht plausibel sein, so erhalten Sie einen entsprechenden Hinweis und werden zur Korrektur Ihrer Eingabe aufgefordert.

Die Bearbeitung des Antrags kann einige Zeit in Anspruch nehmen. Vom BZSt erhalten Sie





**Kommunikationshandbuch ELMA-Standard**  
Standardisierte Datenübermittlung an das BZSt über die  
Massendatenschnittstelle ELMA

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 **Port 22** muss für den Verbindungsaufbau über SSH2 **freigeschaltet** sein.
- Der Domain Name Service (DNS) zur Beantwortung von Anfragen zur Namensauflösung muss **aktiviert** sein.
- Für die Einlieferung von Produktionsdaten wird **elma5.bfinv.de** verwendet.
- Für die Einlieferung von Testdaten 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 elma5.bfinv.de 22
```

Antwort im Gutfall:

```
Trying 80.245.147.91...
```

```
Connected to elma5p.bfinv.de.
```

```
Escape character is '^]'.  
^C
```

```
SSH-2.0-OpenSSH_5.5p12
```

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

---

<sup>2</sup>Die OpenSSH Version kann ggf. abweichend sein.



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 kann vom ITZBund ohne Angabe von Gründen geändert werden.

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<sup>3</sup>: \Windows\System32\drivers\etc).

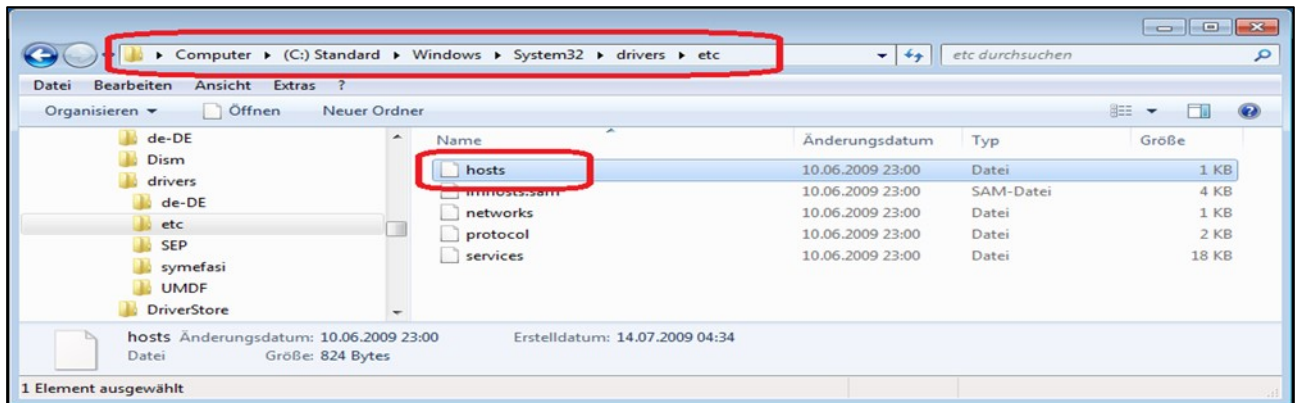


Abbildung 2: Lokalisation der "hosts" Datei im Explorer

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

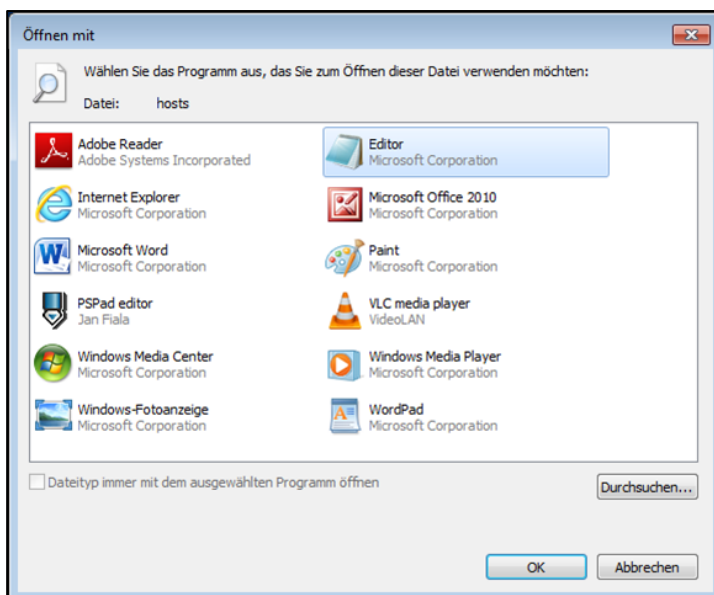


Abbildung 3: Datei mit Editor öffnen

<sup>3</sup> 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.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
#
#ELMA Server
80.245.147.91           elma5   elma5.bfinv.de
```

Abbildung 4: Ergänzung der hosts-Datei um elma5p Servereintrag

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

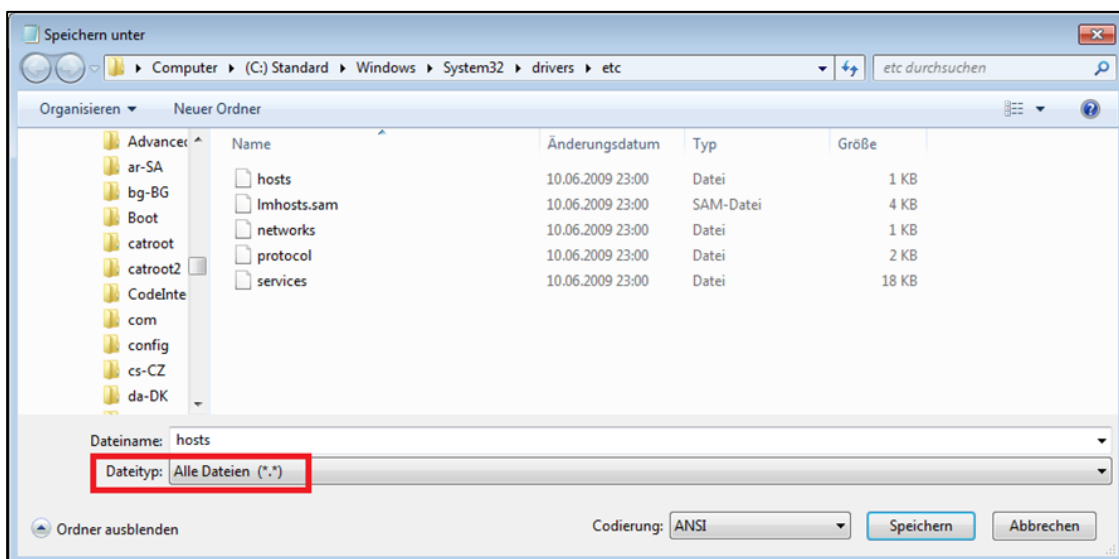


Abbildung 5: Dateityp bei Speicherung setzen



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
```

```
80.245.147.91  elma5p          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
```

```
80.245.147.91  elma5p          elma5p.bfinv.de
```



Speichern Sie die `hosts`-Datei durch Eingabe von `Control+O` gefolgt von `RETURN` und beenden den `nano`Editor 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. 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 das OpenSSL-Framework und eine vom verwendeten Betriebssystem abhängige Übertragungssoftware (`SFTP` / `WinSCP` / `FileZilla`) benötigt.

#### **5.1. 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.



### 5.1.1. OpenSSL-Installation unter Linux

Öffnen Sie per Tastenkombination **Alt + F2**<sup>4</sup> 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-1.1.1d5.tar.gz
```

```
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.

### 5.1.2. OpenSSL-Installation unter Mac OS

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

### 5.1.3. 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.

---

<sup>4</sup> Abhängig von der verwendeten Linux / Unix Installation kann die Tastenkombination abweichen.

<sup>5</sup> Die Version kann ggf. abweichen. Verwenden Sie immer die aktuell verfügbare Version.





## 5.2. OpenSSH-Installation

### 5.2.1. OpenSSH-Installation unter Linux

In vielen Linux-Distributionen ist die OpenSSH-Komponente Bestandteil der Grundinstallation.

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<sup>6</sup> installiert werden.

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

### 5.2.2. OpenSSH Installation unter Mac OS

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

### 5.2.3. 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<sup>7</sup> und führen die Installation aus.

## 5.3. Einrichtung der Übertragungsumgebung für Linux Systeme

Für die SFTP-Datenübertragung ist kein dezidiertes Account auf dem Linux-System notwendig. Es empfiehlt sich aber, für die Datenübertragung einen entsprechenden User Space für die zu übertragenden Daten einzurichten<sup>8</sup>. Geben Sie hierfür das folgende Kommando ein:

```
adduser <Userkennung>
```

---

<sup>6</sup> Hier als Beispiel für ein Debian System.

<sup>7</sup> Verwenden Sie als Download immer die aktuelle Version.

<sup>8</sup> Für die Ausführung dieses Kommandos sind Rootrechte notwendig.



Melden Sie sich unter der neu erzeugten Userkennung an und kopieren Sie die Datei `elster.pem` (Beispieldateiname) in das Verzeichnis `~/.ssh/elster.pem`. Ändern Sie die Dateirechte für `elster.pem`.

```
chmod 600 ~/.ssh/elster.pem
```

Eine Änderung der initialen Passphrase ist für den konvertierten Key möglich.

```
ssh-keygen -p -f ~/.ssh/elster.pem
```

## 6. Übertragung der Daten- und Signatur-Datei

### 6.1. Abgrenzung zum XML-Upload über BOP

In einzelnen Verfahren ist es möglich, die XML-Datendatei über einen Upload-Client im BOP an das BZSt zu übertragen. Den XML-Upload finden Sie im BOP unter "BOP" --> "Formulare & Leistungen" --> "Versand von Massendaten (ELMA5)". Nach Auswahl des betreffenden Fachverfahrens führt Sie das BOP durch den Upload.

Bitte beachten Sie, dass für den Upload von XML-Datendateien ebenfalls eine Freischaltung für die Massendatenschnittstelle ELMA sowie die Einbindung des BOP-Zertifikats (.pfx Login-Zertifikatsdatei) im Browser erforderlich ist. Hierzu finden Sie auf der Internetseite des BZSt Video-Tutorials, die u.a. die Einbindung des BOP-Zertifikats in den Browser zeigen.

Der Aufbau der XML-Datendatei folgt denselben Regeln wie bei der Übertragung an die Massendatenschnittstelle ELMA. Außerdem sind die Vorgaben für die Namenskonvention zu beachten. Daher sind bezüglich der Übertragung der XML-Datendatei insbesondere die *Abschnitte 3, 4.1, Fehler! Verweisquelle konnte nicht gefunden werden.* und ggfs. verfahrensspezifische Besonderheiten für den XML-Upload zu beachten.

Bitte beachten Sie jedoch, dass der Upload-Client direkt an die Produktivsysteme der Verfahren angeschlossen ist. Eine Nutzung des XML-Uploads für Testzwecke ist somit nicht zulässig!

Die Rückmeldungen zu einer über das BOP übertragenen Datei sind nicht im BOP-Postfach abrufbar. Da der XML-Upload wie eine Übertragung über ELMA behandelt wird, sind die Rückmeldungen nur im zugehörigen Download-Verzeichnis, nicht aber im BOP-Postfach, wo die Datei hochgeladen wurde, abrufbar.

Um diese Rückmeldungen ohne direkte SFTP-Verbindung abzuholen, besteht aus dem BOP heraus die Möglichkeit, den Inhalt des Download-Verzeichnisses abzurufen. Der Weg dorthin führt über folgende Navigation im BOP: "BOP" --> "Formulare & Leistungen" --> "Versand von Massendaten (ELMA5)" --> "Allgemein" --> "Abholung von ELMA5-Protokollen"



Die Inhalte der Rückmeldungen und die diesbezüglichen Prüfungen sind identisch mit einer per SFTP über das Upload-Verzeichnis übertragenen Datei, vgl. *Abschnitt 8*.

## **6.2. Aufbau der Verbindung**

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

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

### Lieferung in das Produktivsystem

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 das Testsystem

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

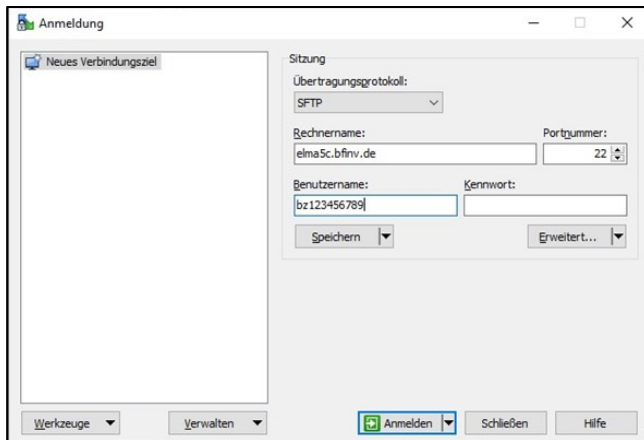


Abbildung 6: Anmeldemaske in WinSCP

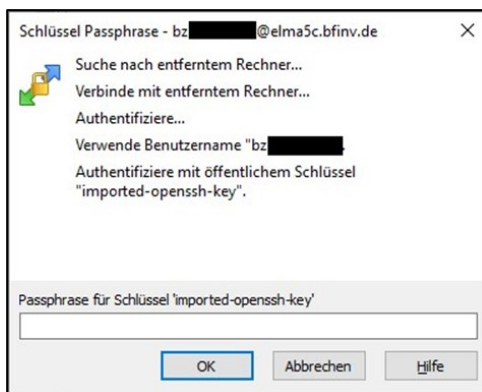


Abbildung 7: Fenster zur Passwortabfrage des ELMA5-Zertifikats

## FileZilla

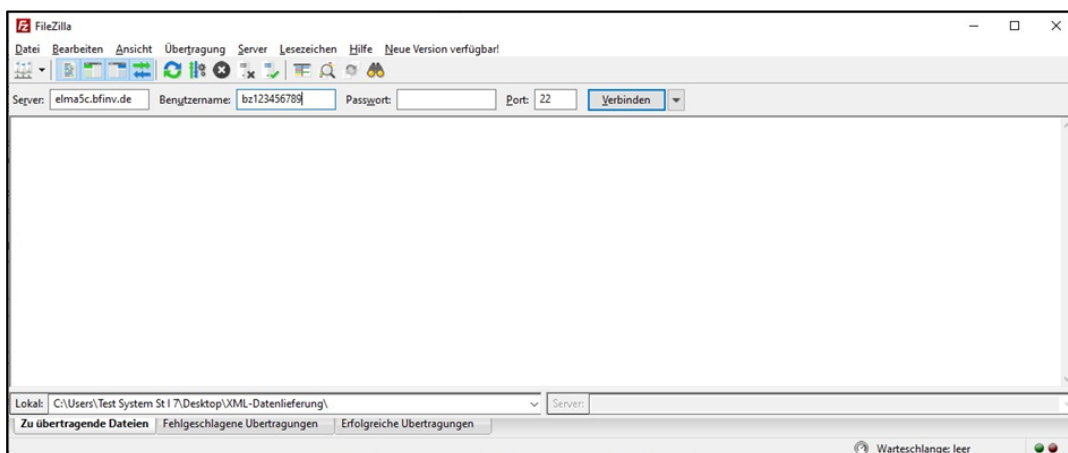


Abbildung 8: Anmeldemaske in FileZilla

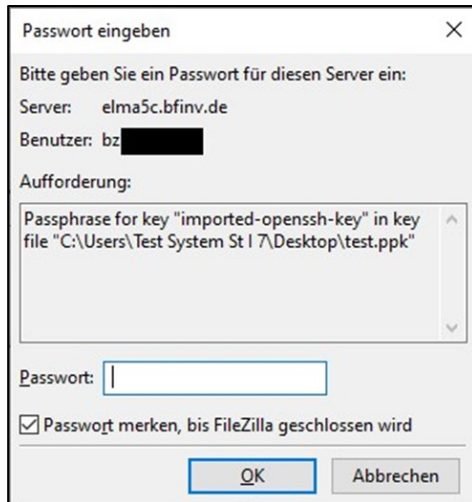


Abbildung 9: Fenster zur Passwortabfrage des ELMA5-Zertifikats

### 6.3. 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 und wird im Teil II dieses Handbuches näher beschrieben, vgl. *Abschnitt 7.2 ff.*

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.

#### 6.3.1. Signaturdatei

Zu jeder Datendatei muss eine korrespondierende Signaturdatei erstellt und übermittelt werden.

Die Passphrase wird bei jeder Signaturerstellung verwendet und sollte daher sicher verwahrt 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



### **6.3.1.1. Namenskonvention für die Signaturdatei**

Zu jeder Datendatei gehört eine korrespondierende Signaturdatei. Der Name der Signaturdatei besteht aus dem Namen der Datendatei (*vgl. Abschnitt 7.7*), erweitert um den Suffix `.sig`.

### **6.3.1.2. Erstellung Signaturdatei**

Die Passphrase wird bei jeder Signaturerstellung verwendet und sollte daher sicher verwahrt werden.

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.

#### **6.3.1.2.1. Linux**

Auf Linux-Systemen kann für die Erstellung der Signaturdatei das OpenSSL Command-Line-Tool verwendet werden.

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.

#### **6.3.1.2.2. MAC OS**

Auf macOS-Systemen kann für die Erstellung der Signaturdatei das OpenSSL Command-Line-Tool verwendet werden.



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.

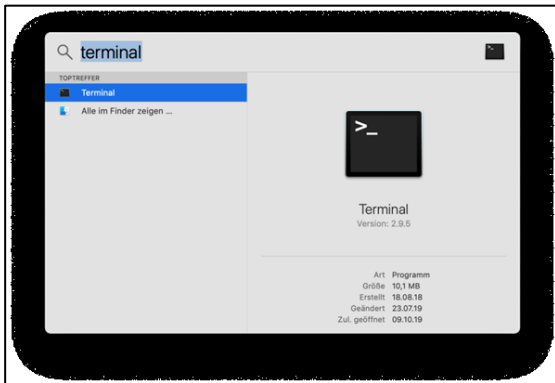


Abbildung 10: Aufruf des Terminals über die Spotlight-Suche unter macOS

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.

### 6.3.1.2.3. 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> ^9  
-inkey <Pfad zum Private Key> -rawin -digest <Hashfunktion> ^  
-out <Dateiname der Signaturdatei>
```

Nach Eingabe der Passphrase wird die Signaturdatei erstellt.

---

<sup>9</sup> Das Zeichen „^“ stellt die Fortsetzung der Eingabe in einer neuen Zeile dar. Wird die Eingabe nicht in einer neuen Zeile fortgesetzt, kann dies entfallen.



## 6.4. Upload

Es sind die Namenskonventionen zur Datendatei (vgl. Abschnitt 7.7) und zur Signaturdatei (vgl. Abschnitt 6.3.1.1) zu beachten.

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

Datendatei: m5\_<pb>\_<BZStNr>\_<AccountID>\_<DateiId>.xml.tmp

Signaturdatei: m5\_<pb>\_<BZStNr>\_<AccountID>\_<DateiId>.xml.sig.tmp

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.

## 6.5. 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.

## 6.6. 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.

**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.**





## Teil II

# Weitergehende Informationen für Verfahren mit ELMA-Standard

Die nachfolgenden Abschnitte enthalten die notwendigen Informationen für Verfahren, die dem ELMA-Standard unterliegen, *vgl. Abschnitt 0.2*. Für die Datenübermittlung bei Fachverfahren, die bisher nicht dem ELMA-Standard unterliegen, sind die jeweils fachspezifischen Dokumentationen zu beachten.

## 7. Anforderungen an die zu übertragende Datendatei

Jeder DateiUpload auf den ELMA-Server besteht immer aus 2 Dateien (Datendatei und Signaturdatei, *vgl. Abschnitt 6.3*). Die Datendatei enthält neben einem standardisierten ELMA-Header (ELMA-Standard), der nachfolgend beschrieben wird, immer auch den durch das Fachverfahren spezifizierten Meldungsdatensatz (dieser ist nicht Bestandteil dieser Dokumentation, hierzu wird auf das jeweilige Fachverfahren verwiesen.)

### 7.1. ELMA- Standard

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

Der ELMA-Standard wird im Folgenden exemplarisch am Verfahren DAC6 (Verfahrenskürzel DC) dargestellt und gilt analog für alle teilnehmenden Verfahren unter *Abschnitt 0.2*.

Die Schema-Definition zum ELMA- Standard kann im *Abschnitt 9* abgerufen werden.



## 7.2. Aufbau der Datendatei (Wurzelement und ELMA-Header)

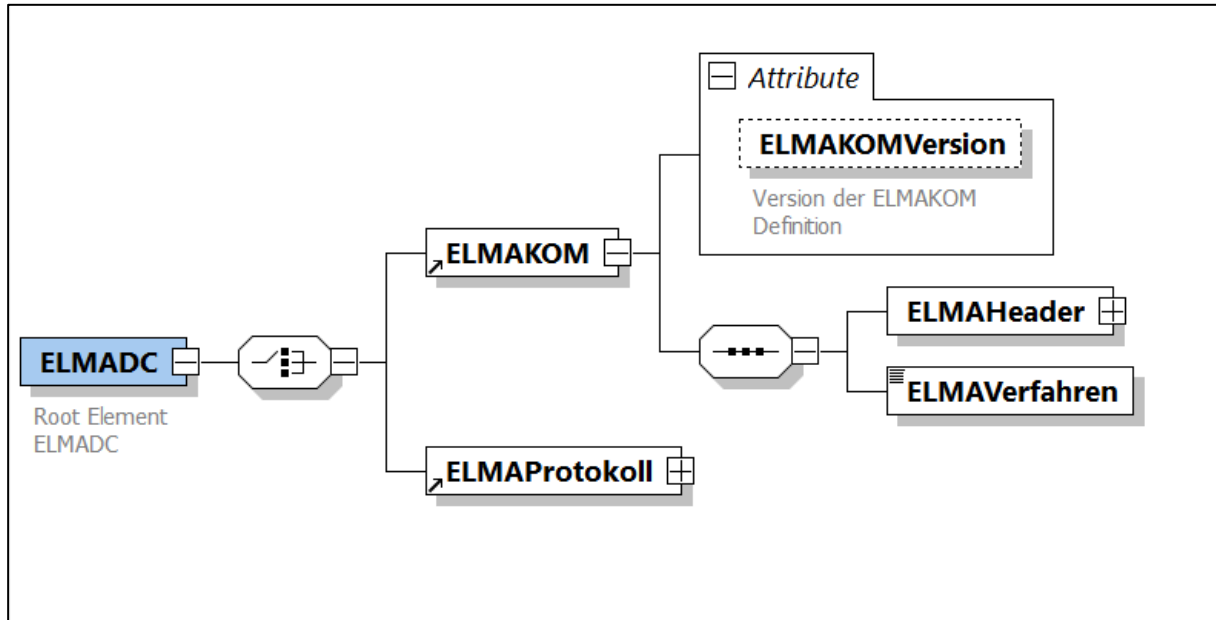


Abbildung 11: Beispiel mit ELMADC als Root-Element für das Fachverfahren DAC6

Die Metadaten des ELMA-Verfahrens werden wie ein „Umschlag“ um die eigentlichen Dateninhalte herumgelegt. Der Aufbau der XML-Struktur beginnt jeweils mit einem Root-Element für das jeweilige Fachverfahren. Dieses Element ist der Wurzelknoten für die gesamte zu übertragene Datei und stellt den Einstieg in den Baum dar. Der Name des Root-Elements besteht aus der festen Bezeichnung „ELMA“ und der zweistelligen Produktbezeichnung des jeweiligen Fachverfahrens (z.B. ELMADC für DAC6, ELMACC für CbCR).

Im Falle einer Datenlieferung folgt der ELMAKOM-Abschnitt. Dieser beinhaltet die Teile ELMAHeader und ELMAVerfahren. ELMAHeader und ELMAVerfahren sind Bestandteil einer jeden ELMA-Lieferung. Der ELMAHeader, der nunmehr standardisiert wurde, enthält alle Informationen des Senders für die Fachverfahrens- und Sender-Zuordnung.

Unter ELMAVerfahren ist das fachverfahrensspezifische XML einzubetten.

Die verfahrensspezifischen Beschreibungen zum ELMAVerfahren sind nicht Bestandteil dieser Dokumentation. Hier wird auf das jeweilige Fachverfahren verwiesen.

Für die Rückgabe der Statusinformationen (Verarbeitungsergebnisse) zur eingereichten Datei folgt dem Root-Element der ELMAProtokoll-Abschnitt, vgl. Abschnitt 8.





Nachfolgende Tabelle beschreibt die Befüllung des ELMAHeaders.

Feldname	Anzahl Zeichen	Typ	Kardinalität	Inhalt/ Erläuterung	Bemerkungen
DatenArt	10		1		<i>Vgl. Spalte „Datenart“ in Abschnitt 0.2.</i>
AuthSteuernummer	11	an	1	Die verwendete BZSt-Nummer des Anwenders	11-stelliges Textfeld, das nur aus zwei Großbuchstaben sowie 9 Ziffern (0-9) bestehen darf. Dabei handelt es sich um die BZSt-Nummer mit welcher die BOP-Registrierung des Benutzerkontos vorgenommen wurde. Sie wird im privaten Bereich des BOP-Benutzerkontos unter „Mein BOP“ bei den "Informationen zur Registrierung" angezeigt.
AccountID	10	an	1	Die verwendete AccountID des Anwenders	10-stelliges Textfeld, das nur Ziffern (0-9) beinhalten darf. Die AccountID wird im privaten Bereich des BOP-Benutzerkontos unter „Mein BOP“ als „Benutzerkonto-ID“ innerhalb der Übersicht "Benutzerkontoinformationen" angezeigt.
ErstellungsDatum	19	an	1	Tagesdatum des Uploads der Dateien	Dieses Feld ist mit dem Erstellungsdatum zu füllen. Das Feld wird aktiv durch den Nutzer befüllt. Form: Jahr-Monat-TagTStunde:Minute: Sekunde Beispiel: 2014-12-31T13:20:00
KundeneigeneID	255	an	0.1		Dieses Feld kann mit internen Referenzinformationen des Nutzers befüllt werden.



Feldname	Anzahl Zeichen	Typ	Kardinalität	Inhalt/ Erläuterung	Bemerkungen
UUID	Unbegrenzt	an	0..1	Kennzeichnung der Datenlieferung	Hexadezimal notierte Zahl UUID Beispiel: 550e8400-e29b-11d4-a716-446655440000
Verarbeitungslauf	ENUM		1	PRODUKTIONS-LAUF <b>oder</b> TESTLAUF	Unterscheidung des Dateneingangs zwischen Test- und Produktivdatenübermittlung. Es ist auf eine korrekte Verwendung zu achten. Auf der Produktionsumgebung werden Dateien mit „TESTLAUF“ abgewiesen. Auf der Testumgebung werden Dateien mit „PRODUKTIONS-LAUF“ abgewiesen.

Tabelle 1: Befüllung des ELMAHeaders

### 7.3. XSD-Schema Validierung

Die XML-Datendatei sollte vor der Versendung gegen die aktuellen (verfahrensspezifischen) XSD Schemata (ausgehend vom verfahrensspezifischen Root-Element des standardisierten ELMAHeaders bis hin zu dem verfahrensspezifischen ELMAVerfahren-Element) validiert werden, soweit die gesamten diesbezüglichen XSDs (zusammengefasst) vom jeweiligen Fachverfahren zur Verfügung gestellt werden.

Dabei sind folgende Punkte zu beachten:

- Die „Namespace“-Einsetzungen müssen korrekt sein.
  - Die Reihenfolgen der „Namespace“ im XML - Schema ist variabel und nicht festgelegt und können sich jederzeit ändern. An der Schemakonformität ändert sich dadurch nichts.
- Für jeden Namespace-Prefix muss das `xmlns:prefix` Attribut einmalig vorhanden sein.
- Das `xsi:schemaLocation` Attribut muss einmalig vorhanden sein.



## 7.4. UTF-8 Kodierung

Für die Erstellung der XML-Datei ist die UTF-8 Kodierung ohne BOM<sup>10</sup> zu verwenden. Abweichende Kodierungen werden nicht unterstützt und führen zu einer ganzheitlichen Abweisung.

Es wird empfohlen, nur die üblicherweise in Namens- und Adresdaten enthaltenen Zeichen der UTF-8 Kodierung zu nutzen<sup>11</sup>. Nur so ist 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<sup>12</sup> herangezogen werden. Informationen zur UTF-8 Zeichencodierung und Validierung finden Sie unter der URL:

<https://www.w3.org/International/questions/qa-validator-charset-check.de>.

Öffnen Sie die Datei in einem Hex-Editor und entfernen Sie ggf. am Anfang der Datei die Bytesequenz EF BB BF. Die Verwendung von Byte Order Mark wird nicht unterstützt.

## 7.5. 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.

## 7.6. Dateigrößenbeschränkung

Die zu übermittelnde Datendatei sollte kleiner als 100 Megabyte sein. Eine Überschreitung dieser Maximalgröße kann zu einer Dateiabweisung führen. Davon abweichende Regelungen sind fachverfahrensspezifisch hinterlegt.

## 7.7. Namenskonvention für die Datendatei

Der Dateiname besteht aus folgenden Teilen:

```
m5_<pb>_<BZSt-Nr>_<AccountID>_<DateiId>.xml
```

Die Elemente <BZSt-Nr> und <AccountID> des Dateinamens müssen mit dem Inhalt der Felder im „ELMAHeader“ der Datei übereinstimmen, *vgl. Tabelle 1*.

Der Teil des Dateinamens, der durch das Fachverfahren und den Lieferanten der Datei vorgegeben ist, besteht nur aus **kleinen Buchstaben** [a-z] und **Ziffern** [0-9]. Im speziellen

---

<sup>10</sup> Als Byte Order Mark wird das Unicode Zeichen U+FEFF verwendet.

<sup>11</sup> Je nach dem gewählten Fachverfahren können die erlaubten Zeichen eingeschränkt sein.

<sup>12</sup> [https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/13\\_Sitzung/Unicode.html](https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/13_Sitzung/Unicode.html)



Teil des Dateinamens (DateiId) dürfen ebenso nur **kleine Buchstaben** [a-z] verwendet werden. Die Verwendung von davon abweichenden Zeichen (A, B, ö,ä,ß usw.) führt zu einer Abweisung der Datenlieferung. Die einzelnen Bestandteile des Dateinamens werden mit einem Unterstrich „\_“ getrennt. Zwischen dem Dateinamen und dem Suffix wird ein Punkt „.“ als Trennzeichen verwendet. Der Dateiname der Datendatei endet mit dem Suffix xml. Dateinamen müssen im System eindeutig sein.

Ein bereits für die Übertragung verwendeter Dateiname darf nicht erneut genutzt werden. Dies gilt auch im Fehlerfall bei einer formalen Abweisung durch die ELMA-Prüfung und ebenso für eingelieferte Testdaten. Ein im Testsystem verwendeter Dateiname darf auch in Produktion nicht erneut verwendet werden.

Während der Eingangsprüfung wird über die Eingangsdatei ein Hash gebildet, welcher zusammen mit dem Dateinamen persistiert wird. Damit kann eine irrtümliche Doppellieferung von bereits verarbeiteten Lieferungen ausgeschlossen werden. Nach einer Abweisung ist daher immer ein neuer Dateiname zu bilden und in der Datei mindestens ein Zeichen zu ändern. So erkennt die ELMA-Prüfung, dass es sich bei der Datenlieferung nicht um eine versehentliche Doppellieferung handelt.

Beispiel für eine FATCA Datendatei:

m5\_fc\_bz123456789\_1234567890\_sparkohl0001.xml

Feldname	Anzahl Zeichen	Inhalt / Erläuterung	Bemerkungen
m5	2	ELMA-Dateikennung	Konstant für alle Verfahren
_	1	Unterstrich	konstant
<pb>	2	Produktbezeichnung 2-stellig, alphanumerisch, Verfahrenskürzel wird vom Fachverfahren vorgegeben	<i>Vgl. Spalte „Verfahrenskürzel“ in Abschnitt 0.2.</i>
_	1	Unterstrich	konstant
<BZSt-Nr>	11	Alphanumerische BZSt- Nummer des Senders. Diese wurde während der Registrierung im BZStOnline-Portal vergeben.	11-stelliges Textfeld, dass nur aus zwei Kleinbuchstaben sowie 9 Ziffern (0-9) bestehen darf. Dabei handelt es sich um die BZSt- Nummer mit welcher die BOP- Registrierung des Benutzerkontos vorgenommen wurde. Sie wird im privaten Bereich des BOP- Benutzerkontos unter „Mein



Feldname	Anzahl Zeichen	Inhalt / Erläuterung	Bemerkungen
			BOP“ bei den "Informationen zur Registrierung" angezeigt. Beispiel: bz123456789 Wichtig: Kleinschreibung(bz/bx) beachten!
_	1	Unterstrich	konstant
<AccountID>	10	AccountID des verwendeten Zertifikats	10-stelliges Textfeld, das nur Ziffern (0-9) beinhalten darf. Die AccountID wird im privaten Bereich des BOP-Benutzerkontos unter „Mein BOP“ als „Benutzerkonto-ID“ innerhalb der Übersicht "Benutzerkontoinformationen" angezeigt.10-stelliges Textfeld.
_	1	Unterstrich	konstant
<Dateiid>	1-12	Von der versendenden Stelle zu vergebender, interner Kurzname für die Datendatei. Dieser Bezeichner dient nur der internen Zuordnung des Versenders.	1 bis max. 12 Zeichen. Darf nur Zeichen aus [a-z, 0-9] enthalten. Es sind keine Großbuchstaben, Sonderzeichen, Leerzeichen oder Unterstriche ( ) erlaubt.
.	1	Punkt Trennung Präfix.Suffix	konstant
xml	3	Suffix	konstant

Tabelle 2: Aufbau Dateinamen bei Lieferung





## **8. Prüfungen und Rückmeldungen zu den übertragenen Dateien**

### **8.1. ELMA Eingangsprüfungen**

Nach der Einlieferung einer Datei in das Upload-Verzeichnis der Massendatenschnittstelle ELMA werden formale Prüfungen vorgenommen. Es wird eine Antwortdatei (in XML) über das standardisierte Element `ELMAProtokoll` mit einer StatusID erzeugt und anschließend im Download-Verzeichnis bereitgestellt. Zusätzlich wird ein E-Mail an den Lieferanten der Datei erzeugt, falls dies technisch möglich ist, d.h. falls der Lieferant mithilfe von BZSt-Nummer und AccountID ermittelt werden kann.

#### **8.1.1. ELMAPROTOKOLL - XSD**

Die Rückmeldung als `ELMAProtokoll` wurde ebenso standardisiert und ergibt sich aus der Schema-Definition zum ELMA- Standard, welche im *Abschnitt 9* abgerufen werden kann.

Hierbei ist zu beachten, dass die darin enthaltenen Fehlercodes 8014-8020 sowie alle 9000er-Codes derzeit noch keine Relevanz haben. Diese StatusIDs sind eingefügt worden, um ggf. auf ergänzende Prüfungen und Abbrüche ohne erneute XSD-Änderung reagieren zu können.

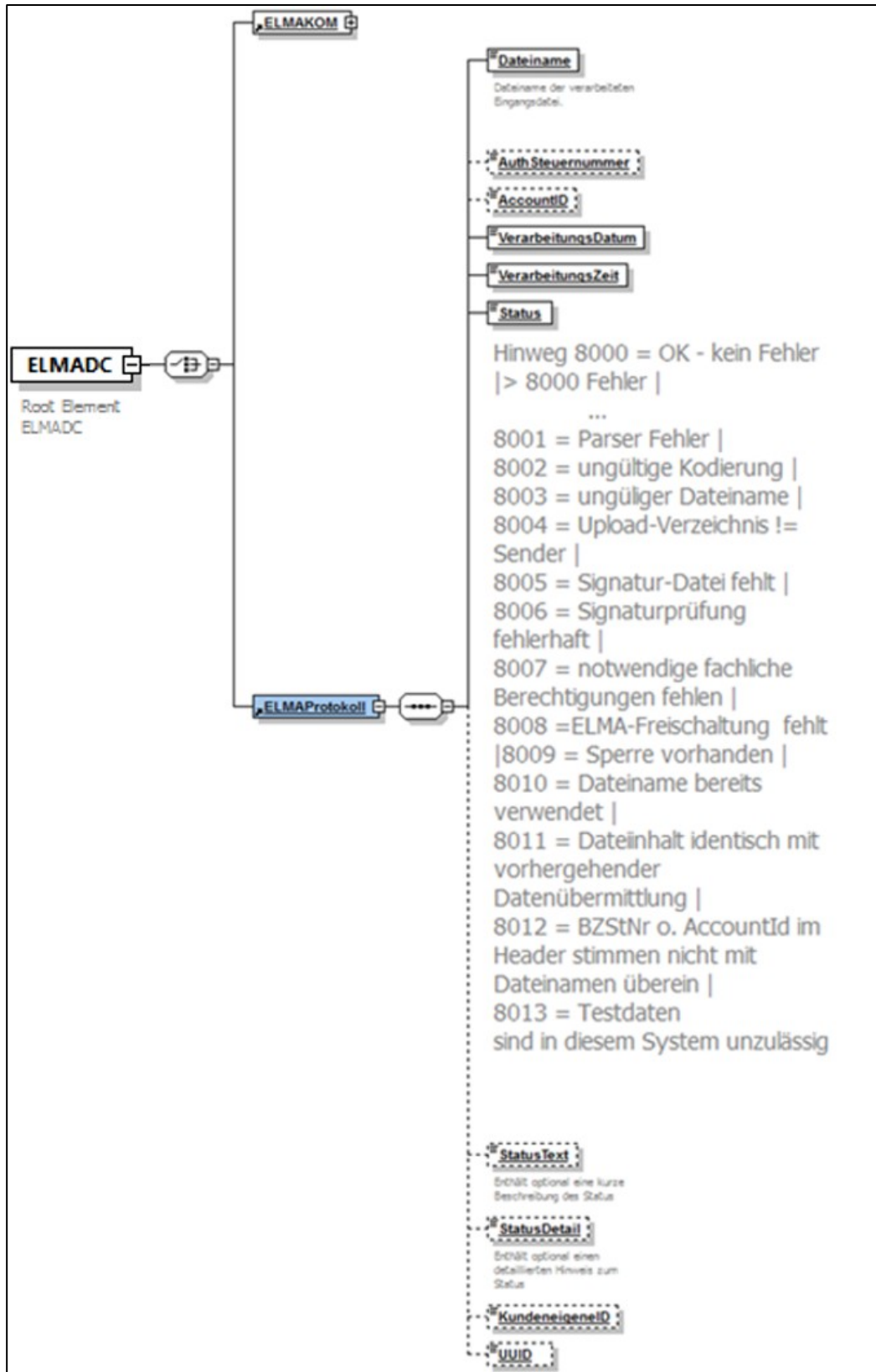


Abbildung 13: Aufbau des standardisierten ELMAProtokolls am Beispiel DAC6



Nachfolgende Tabelle beschreibt die Befüllung des ELMAProtokolls:

<b>Feldname</b>	<b>Kardi- nalität</b>	<b>Inhalt / Erläuterung</b>	<b>Bemerkungen</b>
Dateiname	1	Dateiname der verarbeiteten Eingangsdatei	Enthält den Dateinamen auf den sich das ELMA-Protokoll bezieht.
AuthSteuernummer	0..1	BZSt-Nummer	Enthält die BZSt-Nr. des ELAN-Nutzers aus dem ELMA-Header der Anfrage, falls technisch möglich.
AccountID	0..1	Benutzerkonto im BZStOnline-Portal	Enthält die AccountID des Portalkontoinhabers, der die Anfrage übermittelt hat.
VerarbeitungsDatum	1	Datum zu dem die Anfrage von ELAN verarbeitet wurde	Bezieht sich auf das Verarbeitungsdatum der Anfrage, auf die dieses Protokoll reagiert.
VerarbeitungsZeit	1	Dauer der Verarbeitung durch ELAN	Bezieht sich auf die Verarbeitungszeit der Anfrage, auf die dieses Protokoll reagiert.
KundeneigeneID	0..1	Entspricht der Zuordnung der gesendeten Datei zu kundeneigenem Informationssystem.	Kundeneigene ID aus der Anfrage, entnommen aus dem ELMA-Header.
UUID	0..1	Eine UUID besteht aus einer 16-Byte-Zahl, die hexadezimal notiert und in fünf Gruppen unterteilt wird.	Bezieht sich auf die UUID der Anfrage aus dem ELMA- Header, damit eine eindeutige Zuordnung zu der Anfrage ermöglicht wird.
Status	1	Hinweg 8000 = OK - kein Fehler   > 8000 Fehler   8001 = Parser Fehler 8002 = ungültige Kodierung	



Feldname	Kardi- nalität	Inhalt / Erläuterung	Bemerkungen
		8003 = ungültiger Dateiname  8004 = Upload-Verzeichnis = Sender  8005 = Signatur-Datei fehlt  8006 = Signaturprüfung fehlerhaft  8007 = notwendige fachliche Berechtigungen fehlen  8009 = Sperre vorhanden  8010 = Dateiname bereits verwendet  8011 = Dateiinhalt identisch mit einer bereits gelieferten Datei  8012 = BZStNr o. AccountID im Header stimmen nicht mit Dateinamen überein  8013 = Testdaten sind in diesem System unzulässig	
StatusText	0..1	Enthält optional eine kurze Beschreibung des Status	
StatusDetail	0..1	Enthält optional einen detaillierten Hinweis zum Status	

Tabelle 3: Befüllung des standardisierten ELMAProtokolls



### 8.1.2. Rückmeldungen von ELMA (StatusIDs)

StatusID	Beschreibung	E-Mail Text (vgl. Abschnitt 8.1.4)
8000	OK - kein Fehler Datei wurde fehlerfrei verarbeitet und zur weiteren Bearbeitung an das Fachverfahren übergeben.	Wir haben Ihre im Betreff genannte Datei erhalten. Die formale Prüfung ergab keine Fehler. Die Datei wurde zur weiteren Verarbeitung an das Fachverfahren weitergeleitet.

Tabelle 4: ELMA StatusID 8000 (fehlerfreie Verarbeitung in ELMA)

StatusID	Beschreibung	Fehlerfall	E-Mail Text (vgl. Abschnitt 8.1.4)
8001	Parser Fehler	Nicht Schema-valide	Wir haben Ihre im Betreff genannte Datei erhalten. Der Inhalt Ihrer Datendatei konnte nicht gegen das aktuelle XSD-Schema validiert werden. Die Datei wurde abgewiesen.
8002	ungültige Kodierung	Keine UTF-8 Datei bzw. mit BOM	Wir haben Ihre im Betreff genannte Datei erhalten. Als Codepage wurde leider nicht UTF-8 gewählt. Die Datei wurde abgewiesen.
8003	ungültiger Dateiname	Dateiname nicht korrekt	Wir haben Ihre im Betreff genannte Datei erhalten. Der Dateiname entspricht leider nicht den Namenskonventionen. Die Datei wurde abgewiesen.
8004	Upload-Verzeichnis≠ Sender	Falsche BZSt Nummer verwendet	Wir haben Ihre im Betreff genannte Datei erhalten. Die BZSt-Nummer im Dateinamen entspricht leider nicht Ihrer Senderkennung. Die Datei wurde abgewiesen.
8004	Upload-Verzeichnis≠ Sender	Falsche AccountID verwendet	Wir haben Ihre im Betreff genannte Datei erhalten. Die Account-ID im Dateinamen entspricht leider keinem Ihrer Benutzerkonten unter Ihrer BZSt-Nummer. Die Datei wurde abgewiesen.



StatusID	Beschreibung	Fehlerfall	E-Mail Text (vgl. Abschnitt 8.1.4)
8005	Signatur-Datei fehlt	Signatur-Datei fehlt	Wir haben Ihre im Betreff genannte Datei erhalten. Leider fehlt die zugehörige Signaturdatei. Die Datei wurde abgewiesen.
8006	Signaturprüfung fehlerhaft	Signaturprüfung fehlgeschlagen	Wir haben Ihre im Betreff genannte Datei erhalten. Die Signaturprüfung ist leider fehlgeschlagen.
8007	notwendige fachliche Berechtigungen fehlen	Verfahrensverknüpfung nicht vorhanden	Wir haben Ihre im Betreff genannte Datei erhalten. Ihnen fehlt leider eine zum Übermitteln der Anfrage notwendige fachliche Zulassung. Zur Klärung wenden Sie sich bitte an den zuständigen Fachbereich im Bundeszentralamt für Steuern. Weitere Informationen zu den Fachbereichen finden Sie unter <a href="http://www.bzst.bund.de">www.bzst.bund.de</a> . Die Datei wurde abgewiesen.
8009	Sperre vorhanden	BZSt-Nummer gesperrt	Wir haben Ihre im Betreff genannte Datei erhalten. Ihre BZSt-Nummer bzw. Ihr Benutzerkonto ist leider für die Übermittlung von Anfragen gesperrt bzw. stillgelegt. Zur Klärung wenden Sie sich bitte an den zuständigen Fachbereich im Bundeszentralamt für Steuern. Weitere Informationen zu den Fachbereichen finden Sie unter <a href="http://www.bzst.bund.de">www.bzst.bund.de</a> . Die Datei wurde abgewiesen.
8009	Sperre vorhanden	Benutzerkonto gesperrt	Wir haben Ihre im Betreff genannte Datei erhalten. Ihre BZSt-Nummer bzw. Ihr Benutzerkonto ist leider für die Übermittlung von Anfragen gesperrt bzw. stillgelegt. Zur Klärung wenden Sie sich bitte an den zuständigen Fachbereich im Bundeszentralamt für Steuern. Weitere Informationen zu den



StatusID	Beschreibung	Fehlerfall	E-Mail Text (vgl. Abschnitt 8.1.4)
			Fachbereichen finden Sie unter <a href="http://www.bzst.bund.de">www.bzst.bund.de</a> . Die Datei wurde abgewiesen.
8010	Dateiname bereits verwendet	Dateiname bereits verwendet	Wir haben Ihre im Betreff genannte Datei erhalten. Der Dateiname wurde bereits verwendet. Doppelte Dateinamen sind nicht erlaubt. Die Datei wird nicht verarbeitet und abgewiesen.
8011	Dateiinhalte identisch mit vorhergehender Datenübermittlung	Dateiinhalte bereits übermittelt	Wir haben Ihre im Betreff genannte Datei erhalten. Der Inhalt der Datendatei wurde wahrscheinlich schon mal übertragen. Wir haben eine Übereinstimmung des Hashes festgestellt. Die Datei wird nicht verarbeitet und abgewiesen.
8012	BZStNr o. AccountID im Header stimmen nicht mit Dateinamen überein	Headerdaten=Dateiname	Wir haben Ihre im Betreff genannte Datei erhalten. Die BZSt Nummer und/oder die Account-ID sind im Dateinamen und im ELMA-Header der Datei unterschiedlich. Die Datei wird nicht verarbeitet und abgewiesen.
8013	Testdaten  Produktivdaten	„TESTLAUF“ in Produktionsumgebung verwendet  „PRODUKTIONS-LAUF“ in Testumgebung verwendet	Wir haben Ihre im Betreff genannte Lieferung erhalten. Der verwendete Verarbeitungslauf ist ungültig. Daher wurde die Lieferung abgewiesen.

Tabelle 5: Liste der möglichen ELMA StatusIDs (Fehlercodes)

### 8.1.3. Abfolge der ELMA Dateiprüfung

Die formalen Prüfungen an der Massendatenschnittstelle ELMA können zu einer Abweisung der Datendatei und der Signaturdatei führen. In diesem Fall werden die betroffenen Dateien im Upload-Verzeichnis gelöscht und eine Antwortdatei in das Download-Verzeichnis



eingestellt.

Der Dateiname der Antwort entspricht dem Namen der eingestellten Datendatei. Über die in der Antwortdatei enthaltene StatusID kann eine Analyse der Ursache im Abweisungsfall durchgeführt werden. Zusätzlich wird eine E-Mail an die in Ihrem Benutzerkonto (AccountID) im BZStOnline-Portal zur BZSt-Nummer hinterlegte E-Mail-Adresse versendet. Alle Prüfungen werden nacheinander durchgeführt. Schlägt eine Prüfung fehl, wird die Prüfung abgeschlossen und die Datei wird abgewiesen. Die ELMA-Prüfabfolge und die möglichen resultierenden Fehler sind in der folgenden Tabelle zusammen mit Lösungshinweisen beschrieben.

Nr.	Was wird geprüft?	Hinweise	StatusID
1	Ist die entsprechende Signaturdatei vorhanden?  Entspricht der Name der Signaturdatei dem Namen der Datendatei plus dem Dateianhang (Suffix) „.sig“?	Es müssen die Datendatei und die Signaturdatei mit gleichlautenden Dateinamen im Namenteil vor dem Suffix vorhanden sein.  Fehlerhafte Dateien bleiben ggfs. mehrere Tage im Upload-Verzeichnis liegen.	8005
2	Handelt es sich bei der XML-Datendatei um eine UTF-8-konforme Datei ohne Byte Order Mark (BOM)?	Informationen zur UTF-8 Zeichencodierung und Validierung finden Sie unter der URL: <a href="https://www.w3.org">https://www.w3.org</a> .  Öffnen Sie die Datei in einem Hex-Editor und entfernen Sie ggf. am Anfang der Datei die Byte Sequenz EF BB BF. Die Verwendung von Byte Order Mark wird nicht unterstützt.	8002
3	Kann die XML-Datendatei gegen das verfahrensspezifische Schema validiert werden?  Handelt es sich um eine Datendatei?		8001
4	Entspricht der Dateiname den Konventionen?	<i>Vgl. Abschnitt 7.7.</i>	8003
5	Entspricht die im Dateinamen verwendete BZSt-Nummer dem Namen des ELMA-Home Verzeichnisses?	Die im Dateinamen verwendete BZ-Nummer muss gleich dem Namen des ELMA Home-Verzeichnis sein.	8004





Nr.	Was wird geprüft?	Hinweise	StatusID
6	Sind die BZSt-Nr. und die AccountID im Dateinamen mit den Einträgen im ELMA-Header der Datendatei identisch?	Die im Dateinamen verwendete BZSt-Nr und die AccountID müssen mit den Angaben im ELMAHeader korrespondieren. In der Datendatei sind die beiden Buchstaben (BZ oder BX) als Großbuchstaben zu verwenden.	8012
7	Wurde die Signatur mit dem zugehörigen Zertifikat erstellt?  Wurde die Signaturdatei mit der korrekten Methode erstellt?	Für die Signaturerstellung ist SHA-256 in Verbindung mit dem korrekten Zertifikat zu verwenden.	8006
8	Wurde zu einem früheren Zeitpunkt bereits eine Datei gleichen Namens in die Produktions- oder Testumgebung gesendet?	Diese Prüfung erfolgt auch für bereits abgewiesene Dateien.	8010
9	Wurde zu einem früheren Zeitpunkt bereits eine Datei mit identischem Inhalt in die Produktions- oder Testumgebung eingestellt?	Über jede Datenlieferung wird ein Hashcode gebildet und gespeichert. Über den Hashcode soll die Doppellieferung von bereits verarbeiteten Lieferungen (diese könnten auch unter einem anderen Dateinamen eingeliefert worden sein) ausgeschlossen werden. Diese Prüfung erfolgt auch für bereits abgewiesene Dateien. Nach der Abweisung einer Lieferung ist daher sowohl der Dateiname als auch der Dateiinhalt (z.B. durch Einfügen eines Leerzeichens) zwingend zu verändern.	8011
10	Wurde in der Produktionsumgebung „TESTLAUF“ in dem Element „Verarbeitungslauf“ angegeben?		8013
11	Ist die BZSt-Nr. gesperrt oder stillgelegt?	Kontaktaufnahme mit dem Fachbereich im BZSt.	8009



Nr.	Was wird geprüft?	Hinweise	StatusID
12	Ist die AccountID gesperrt oder stillgelegt?	Kontaktaufnahme mit dem Fachbereich im BZSt.	8009
13	Ist die verwendete AccountID für die Dateiübertragung an das Fachverfahren zugelassen?	Eine Anmeldung im BZSt zur Nutzung der Massendatenschnittstelle ELMA hat beim jeweiligen Fachverfahren zu erfolgen.	8007
14	Ist für die verwendete AccountID eine gültige ELMA Freischaltung vorhanden?	Eine Beschreibung der ELMA Freischaltung finden Sie im <i>Abschnitt 3.3</i> .	8008
	Wurden alle ELMA-Vorprüfungen erfolgreich durchlaufen, wird die Datei zur fachlichen Prüfung an das Fachverfahren weitergeleitet.		8000

Tabelle 6: Abfolge der ELMA Prüfungen und deren Fehlercodes

Weitere Hinweise zu möglichen Fehlergründen:

Die Dateirechte wurden auf dem ELMA Server für die Dateien nicht- oder falsch gesetzt.	Nach dem Upload sind für die Daten- und Signaturdatei die Dateirechte (UNIX-Dateirechte) auf „0660“ (Eigentümer = R/W, Gruppe = R/W, Andere = <keine>). zu setzen.
Die Dateigröße darf die verfahrensspezifisch definierte maximal zulässige Größe nicht überschreiten.	Unnötige Leerzeichen entfernen und ggf. den Dateiinhalte in mehrere Einzeldateien aufteilen. Diese müssen jeweils das vollständige XML-Schema enthalten. Zu jeder Datei ist eine zugehörige Signaturdatei zu erstellen.

Tabelle 7: Weitere ELMA Fehlergründe

#### 8.1.4. Rückmeldung zum Ergebnis der ELMA-Prüfung

Nach Abschluss der ELMA-Prüfungen wird die Daten- sowie die Signaturdatei im Upload-Verzeichnis gelöscht und eine Antwortdatei ohne Signaturdatei im Download-Verzeichnis eingestellt.

Zusätzlich wird eine E-Mail an die zum Benutzerkonto (AccountID) der BZSt-Nummer gehörende E-Mail-Adresse versendet.

Für die E-Mail Betreffzeile wird folgender Eintrag verwendet:

ELMA5-Verarbeitungsstatus: <DATEINAME>



Somit können Sie Ihren Spamfilter entsprechend konfigurieren und die vom ELMA5-Server kommenden E-Mails in Ihr Postfach einstellen lassen.

Sofern die ELMA-Prüfungen alle erfolgreich absolviert wurden (Status 8000), wird die Datei an das jeweilige Fachverfahren weitergeleitet.

## **8.2. Prüfungen im Fachverfahren**

Nach erfolgreicher formaler ELMA-Prüfung wird die Datei ggfs. im jeweiligen Fachverfahren verfahrensspezifisch/inhaltlich geprüft. Hierzu wird auf das jeweilige Fachverfahren verwiesen.

Das Fachverfahren kann eine Rückmeldung z.B. über den Eingang der Datei und das Ergebnis der fachlichen Prüfung übermitteln. Diese werden ebenso im Download-Verzeichnis (Antwortdatei ohne Signaturdatei) auf dem ELMA-Server bereitgestellt. Zeitgleich wird eine E-Mail an den Benutzerkontoinhaber versendet.

## **8.3. Abholung Rückmeldedatei(en)**

Alle Antwortdateien stehen im Download-Verzeichnis auf dem ELMA-Server zur Abholung bereit. Zusätzlich wird eine E-Mail an die zum Benutzerkonto (AccountID) der BZSt-Nummer gehörende E-Mail-Adresse versendet.

Die Antwortdatei wird ebenso mit Hilfe des ELMA-Headers übertragen.

Hierbei ist jedoch zu beachten, dass sich die Datenart bei der Rückmeldung im Vergleich zu der an das BZSt übertragenden Datei ändert. Diese ist z.B. für DAC6: „ELMA\_DCRM“.

Die verfahrensspezifischen Schemabeschreibungen werden grds. vom jeweiligen Fachverfahren zur Verfügung gestellt.

Der Verbindungsaufbau und der Datentransfer erfolgt wie in *Abschnitt Fehler!* **Verweisquelle konnte nicht gefunden werden.** beschrieben. Es ändern sich lediglich die Übertragungsrichtung und das Verzeichnis.

Kopieren Sie die Dateien binär aus dem Download-Verzeichnis in ein Verzeichnis auf Ihrem lokalen Rechner. Erfolgreich transferierte Dateien sind nach dem Download auf dem ELMA Server zu löschen.



Nicht gelöschte Dateien werden 20 Tage nach der Bereitstellung<sup>13</sup> automatisiert gelöscht. Dies gilt unabhängig davon, ob die Datei zuvor bereits abgerufen wurde.

Eine erneute Bereitstellung der Datei ist nicht möglich. Das Anlegen von Unterverzeichnissen im Download-Verzeichnis ist grundsätzlich nicht zulässig. Das BZSt behält es sich vor, derartige Verzeichnisse und alle dort vorhandenen Daten ohne Vorankündigung zu löschen.

Hinweis:

Ein Abholen der Antwortdatei muss innerhalb von 20 Tagen erfolgen. Wird das Verarbeitungsprotokoll im Download-Verzeichnis abgerufen, steht es dort nicht mehr zur Verfügung. Wenn kein Verarbeitungsprotokoll vorgefunden werden kann, sollte dies zunächst hausintern geprüft werden, da das Download-Verzeichnis jedem zur BZSt-Nummer gehörenden Benutzerkontoinhaber zugänglich ist.

**8.3.1. Namenskonvention für die Rückmeldedatei**

Das Ergebnis der ELMA-Prüfung (vgl. Abschnitt 8.1.1) wird in einer Datei abgelegt, die denselben Dateinamen hat wie die eingeliferte Datei. Der Name aller weiteren Rückmeldedateien besteht aus dem Namen der Einlieferungsdatei, erweitert um einen Unterstrich und eine UUID. Für jede Rückmeldedatei wird eine eindeutige UUID vergeben. Verfahrensspezifische Ergänzungen vor der UUID sind möglich.

m5\_<pb>\_<BZSt-Nr>\_<AccountID>\_<DateiId>\_<uiuiuiui- uiui- uiui- uiui- uiuiuiuiuiui>.xml

Beispiel einer FATCA Rückmeldedatei:

m5\_fc\_bz123456789\_1234567890\_name0001\_da5b42ce-9d27-4255-920e-1a089ee0ec8.xml

## 9. Referenzdokumente


Nr.	Titel	Ablage
1	Schema-Definition zum ELMA- Standard	 ELMA Standard.zip

Tabelle 8: Referenzdokumente

<sup>13</sup> Ab dem Tag der E-Mailversendung.



## 10. 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	<a href="#">Das BZStOnline-Portal</a> 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



Begriff	Abkürzung	Begriffserklärung
		Nutzung der Massendatenschnittstelle ELMA setzt ein BOP-Zertifikat der Registrierungsart ELSTERBasis voraus.
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.
Informationstechnikzentrum 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



Begriff	Abkürzung	Begriffserklärung
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.
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 <a href="#">IETF</a> , dem <a href="#">Unicode Consortium</a> und der <a href="#">ISO</a> gegenwärtig identisch definiert: <ul style="list-style-type: none"><li>• <a href="#">RFC 3629</a> / STD 63 (2003)</li><li>• <a href="#">The Unicode Standard</a>, Version 4.0, §3.9–§3.10 (2003)</li><li>• ISO/IEC 10646-1:2000 Annex D (2000)</li></ul>
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 9: Abkürzungsverzeichnis/Glossar

## Impressum

**Herausgeber:**

Bundeszentralamt für Steuern

An der Kuppe 1

53225 Bonn

Telefon: +49 228 406-0

Internet: [www.bzst.bund.de](http://www.bzst.bund.de)

**Stand:**

Version 1.0, 01.07.2020

**Bildnachweis:**

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

**Text:**

BZSt