



Kommunikationshandbuch

Teil 3a - CRS:

Datenübermittlung an das BZSt über die
ELMA-Massendatenschnittstelle

Version:1.6

Stand:17.06.2019



**Bundeszentralamt
für Steuern**

Kommunikations- handbuch

Teil 3a

CRS: Datenübermittlung

an das BZSt über die

ELMA-

Massendatenschnittstelle

(verfahrenübergreifende

Informationen)

Inhaltsverzeichnis

0	INFORMATIONEN ZUM VORLIEGENDEN DOKUMENT	6
0.1	AUFBAU UND ZWECK DES DOKUMENTS	6
0.2	ÄNDERUNGSHISTORIE	6
0.3	ZWECK DES DOKUMENTS	8
0.4	ZIELGRUPPE UND VORAUSSETZUNGEN	8
0.5	DIE GRUNDFUNKTIONEN DER ELMA-MASSENDATENSCHNITTSTELLE IM ÜBERBLICK	9
1	TECHNISCHE VORAUSSETZUNGEN FÜR DIE NUTZUNG DER ELMA- MASSENDATENSCHNITTSTELLE	10
1.1	SYSTEMVORAUSSETZUNGEN FÜR DEN HARDWARE-EINSATZ	10
1.2	SYSTEMVORAUSSETZUNGEN FÜR DEN SOFTWARE-EINSATZ	10
1.3	INTERNETANBINDUNG UND BANDBREITE	10
1.4	FIREWALL KONFIGURATION	10
1.5	IDENTIFIZIERUNG, VERBINDUNG	11
1.6	VERFÜGBARKEIT UND FAILOVER	11
1.7	VERFAHRENAUFNAHME	11
2	TECHNISCHE BESCHREIBUNG DER KOMMUNIKATION	11
2.1	GRUNDLAGEN	11
2.2	X.509 AUTHENTIFIKATION	12
2.3	USERNAME UND PASSWORT AUTHENTIFIKATION	12
3	REGISTRIERUNG UND FREISCHALTUNG	12
3.1	REGISTRIERUNG AM BZSTONLINE-PORTAL	13
3.2	FREISCHALTUNG ZUR TEILNAHME AM ELMA-VERFAHREN	13
3.3	ZERTIFIKAT DOWNLOAD IM PEM-FORMAT	15
4	VERBINDUNGSPRÜFUNG ZUM ELMA-SERVER	16
4.1	FREISCHALTUNG FÜR SSH2 ÜBER PORT 22	16
4.2	IP-ADRESSE DES ELMA SERVERS ERMITTELN	17
4.3	DNS (DOMAIN NAME SYSTEM) NAMENAUFLÖSUNG STEHT NICHT ZUR VERFÜGUNG	17
4.3.1	<i>Ergänzung der hosts Tabelle unter Windows</i>	<i>18</i>
4.3.2	<i>Ergänzung der hosts Tabelle unter MAC OS</i>	<i>19</i>
4.3.3	<i>Ergänzung der hosts Tabelle unter Linux</i>	<i>20</i>
4.4	VERWENDUNG EINES PROXIES FÜR DEN INTERNETZUGANG	20
4.5	KEINE PORT 22 FREISCHALTUNG FÜR SSH-2 MÖGLICH	21

5	EINRICHTUNG DER ÜBERTRAGUNGSKOMPONENTE.....	21
5.1	OPENSSL INSTALLATION.....	21
5.1.1	<i>openssl Installation unter Linux.....</i>	21
5.1.2	<i>openssl Installation unter Mac OS</i>	22
5.1.3	<i>openssl Installation unter Windows.....</i>	22
5.2	OPENSSH INSTALLATION.....	23
5.2.1	<i>OpenSSH Installation unter Linux.....</i>	23
5.2.2	<i>OpenSSH Installation unter Mac OS</i>	23
5.2.3	<i>OpenSSH Installation unter Windows</i>	23
5.2.4	<i>Einrichtung der Übertragungsumgebung für Linux Systeme.....</i>	24
5.3	PEM-DATEI IN DAS PPK-FORMAT KONVERTIEREN	24
6	KONVENTIONEN FÜR DATEINAMEN.....	28
6.1	NAMENSKONVENTIONEN FÜR DIE DATENDATEI	28
6.2	NAMENSKONVENTION FÜR DIE SIGNATURDATEI	30
6.3	NAMENSKONVENTION FÜR DIE RÜCKMELDEDATEI.....	30
7	BEREITSTELLUNG DER ZU ÜBERTRAGENDEN DATEIEN	30
7.1	PRÜFUNG DER XML-DATENDATEI	31
7.1.1	<i>UTF-8 Kodierung</i>	31
7.1.2	<i>XSD-Schema Validierung.....</i>	31
7.1.3	<i>Unzulässige Zeichen und Beschränkungen</i>	31
7.1.4	<i>Dateigrößenbeschränkung</i>	32
7.1.5	<i>Aufbau ELMAKOM-Header</i>	32
7.2	SIGNATURDATEI ERSTELLEN.....	36
7.2.1	<i>Signaturdatei unter Linux erstellen</i>	36
7.2.2	<i>Signaturdatei unter Windows erstellen</i>	37
8	ÜBERTRAGUNG DATEN- UND SIGNATUR-DATEI AN DIE ELMA- MASSENDATENSCHNITTSTELLE.....	38
8.1	AUFBAU DER VERBINDUNG.....	38
8.2	ABLAUF DER DATENÜBERTRAGUNG	38
8.3	DATEIRECHTE SETZEN	39
8.4	UMBENENNUNG DER DATEIEN	39
8.5	ABHOLUNG RÜCKMELDEDATEI.....	39
9	ELMA EINGANGSPRÜFUNGEN	39
9.1	ALLGEMEINE FORMALE VORPRÜFUNG.....	40
9.2	ERWEITERTE VORPRÜFUNG FÜR XML-DATENLIEFERUNGEN.....	40


9.2.1	Liste der möglichen ELMA Fehlercodes und deren Bedeutung	40
9.2.2	Prüfung auf Schemakonformität	43
9.2.3	Prüfung des XML-Rahmens	44
9.2.4	Prüfung der Berechtigung.....	44
9.3	ELMA PRÜFUNGEN ERFOLGREICH ABSOLVIERT	45
9.4	ABFOLGE DER ELMA DATEIPRÜFUNG	45
10	ABGRENZUNG ZUM XML-UPLOAD ÜBER BOP	48
11	INFORMATION DER VERFAHRENSTEILNEHMER.....	49
11.1	BEEINTRÄCHTIGUNG VON SICHERHEITSRELEVANTEN KOMPONENTEN.....	49
12	ABKÜRZUNGSVERZEICHNIS	50
13	GLOSSAR.....	50
14	REFERENZDOKUMENTE / VERWEISE.....	50
15	ANHÄNGE	50

Abbildungsverzeichnis

Abbildung 1: Versand von Massendaten (ELMA5)	14
Abbildung 2: Antrag auf Freischaltung zur Teilnahme am ELMA5-Verfahren des BZSt.....	14
Abbildung 3: ELMA5-Zertifikat für die Erstellung der Signaturdatei generieren.....	15
Abbildung 4: Lokalisation der "hosts" Datei im Explorer.....	18
Abbildung 5: Datei mit Editor öffnen	18
Abbildung 6: Ergänzung der <code>hosts</code> Datei um <code>mach5</code> Servereintrag.....	19
Abbildung 7: Dateityp bei Speicherung setzen	19
Abbildung 8: PuTTY Programmgruppe.....	25
Abbildung 9: Key Generator Startseite	25
Abbildung 10: Auswahl der PEM-Datei.....	26
Abbildung 11: Eingabe der Passphrase zur Nutzungsfreischaltung.....	26
Abbildung 12: PuTTYgen Notice	27
Abbildung 13: Anzeige der Schlüsselinformationen	27
Abbildung 14: Beispiel mit ELMACS als Root-Element für das CRS-Fachverfahren.....	33
Abbildung 15: Aufbau des ELMAHeader	34

Tabellenverzeichnis

Tabelle 1: Aufbau Dateinamen bei Lieferung.....	30
Tabelle 2: Übersicht unzulässiger Zeichen	32
Tabelle 3: Inhalt ELANKOMHeader	36
Tabelle 4: Liste der möglichen ELMA Fehlercodes.....	43
Tabelle 5: Abfolge der ELMA Prüfungen und deren Fehlercodes	47
Tabelle 6: Weitere ELMA Fehlergründe.....	48

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

0 Informationen zum vorliegenden Dokument

Verfahrensbezeichnung	CRS						
Dokumententitel	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle (verfahrenübergreifende Informationen)						
Verantwortlicher Autor	Bundeszentralamt für Steuern (BZSt) – CRS-Bereich						
Erstellt am	20.06.2016						
Zuletzt geändert am	17.06.2019						
Bearbeitungszustand	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30px;"></td> <td>In Bearbeitung / Entwurf</td> </tr> <tr> <td></td> <td>Vorgelegt</td> </tr> <tr> <td style="text-align: center;">X</td> <td>Fertiggestellt</td> </tr> </table>		In Bearbeitung / Entwurf		Vorgelegt	X	Fertiggestellt
	In Bearbeitung / Entwurf						
	Vorgelegt						
X	Fertiggestellt						

0.1 Aufbau und Zweck des Dokuments


In diesem Dokument (KHB-Teil 3a) werden für die Nutzer der Massendatenschnittstelle die Einrichtung der Sendekomponente, die Zusammenstellung der Daten für den Transport und die eigentliche Übertragung beschrieben.

Im verfahrensspezifischen KHB Teile 3b werden Abweichungen und Ergänzungen beschrieben.

0.2 Änderungshistorie

Version	XML- Schema- Version	Datum	Änderung
1.0	1.00	20.06.2016	Initiale Erstellung
1.1	1.00	19.12.2016	7.1.2: Tagesdatum des voraussichtlichen Datei-Uploads 7.1.5: Erstellungsdatum und UUID Bereinigung von Tippfehlern
1.2	1.00	29.05.2017	9.2: Ergänzung der neuen ELMA Fehlercodes 9.4: Abfolge der ELMA Prüfungen Redaktionelle Änderungen
1.3	1.00	08.08.2017	Anpassung an die BZStOnline-Portal Layout-Umstellung

1.4	1.00	28.02.2018	5.1.2, 5.1.3 und 5.2.3: Aktualisierung der Programmversionen. 8.5: Bereitstellungszeit für nicht gelöschte Rückmeldedateien im „download“-Verzeichnis von 100 auf 20 Tage reduziert. 9.2.1: „FehlerID Code 8000“ Text ergänzt.
1.5	1.00	14.01.2019	3: Kapitel „3.1. BZStOnline-Portal Login“ entfernt. Weitere Kapiteln: Anpassung der Screenshots 7.2: Änderung der Signaturerstellung Neues Kapitel hinzugefügt: „10. Abgrenzung zum XML-Upload über BOP“ Redundante Kapiteln entfernt: „10.2. Beeinträchtigungen durch Wartungsarbeiten und Betriebsstörungen“ und „11 „Fehlermeldungen“ Redaktionelle Anpassungen
1.6	1.00	17.06.2019	Anpassung der Links an den neuen Internetauftritt.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

0.3 Zweck des Dokuments

In diesem Dokument werden die technischen Grundlagen für die Verwendung der ELMA Massendatenschnittstelle und die Übertragung der Daten an das BZSt beschrieben. Dieses Dokument ist verfahrensübergreifend für den ELMA Transportweg verwendbar. Verfahrensspezifische Abweichungen sind in den entsprechenden Kapiteln kenntlich gemacht.

0.4 Zielgruppe und Voraussetzungen


Im April 2006 stellte das BZSt erstmals ein Verfahren zur elektronischen Übertragung von Massendaten unter dem Namen MACH5 vor. Mit diesem Verfahren wurde Großkunden die Möglichkeit zur Ablösung von Bandverfahren durch ein schnelles und kostengünstiges elektronisches Übertragungsverfahren ermöglicht. Durch eine kontinuierliche Weiterentwicklung wurde seit dem ersten Quartal 2007 auch die Authentifizierung mit ELSTER-Zertifikaten unterstützt. Diese Neuerung wurde zum Anlass genommen, den Namen des Verfahrens in ELMA5 zu ändern. Ab 2013 wurde der Name in ELMA geändert. Damit gingen weitere Anpassungen und Standardisierungen einher.

Im vorliegenden Dokument wird das Verfahren zur Datenübermittlung von Massendaten über die ELMA-Schnittstelle an das BZSt dargestellt. Es enthält als standardisierten verfahrensunabhängigen Teil die Registrierung, die Freischaltung, die Softwareinstallation und die eigentliche Datenübertragung.

Das ELMA Kommunikationsverfahren wurde für die Übertragung von Massendaten entwickelt. Die Zielgruppe sind Großkunden, wie zum Beispiel Rechenzentren der Kreditwirtschaft, Softwarehäuser mit einer integrierten Übertragungskomponente und ambitionierte Datenlieferanten.

Für die Nutzung der ELMA-Massendatenschnittstelle ist eine Registrierung im BZStOnline-Portal notwendig. Die Registrierung und Authentifizierung entspricht den aktuellen steuerlichen Vorschriften (siehe KHB – Teil 1 Registrierung am BZStOnline-Portal (BOP)).

Für die Datenübertragung auf Senderseite sind frei erhältliche Open Source Produkte für alle gängigen Betriebssystem Plattformen verfügbar. Von verschiedenen Lieferanten für Bankensoftware sind kommerzielle Produkte mit Anbindung an deren Produktivsystem nutzbar. Ein flexibler Einsatz in unterschiedlichen Umgebungen ist somit gewährleistet. Im Standardfall kann eine Verbindung zur ELMA-Massendatenschnittstelle von einem Windows PC oder einer UNIX/Linux Maschine in wenigen Minuten hergestellt werden.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

Lediglich für die Integration in den Rechenzentrums-Betrieb werden besondere Kenntnisse im Bereich der Implementierung, Automatisierung und für die Firewall Konfiguration vorausgesetzt.

0.5 Die Grundfunktionen der ELMA-Massendatenschnittstelle im Überblick

Die ELMA-Massendatenschnittstelle stellt u.a. folgende Funktionen zur Verfügung:

- Nutzung des Internets als Übertragungsmedium zwischen den sendenden Endstellen und den ITZBUND Server Systemen
- Auslegung für Massendatenübertragung via SFTP
- SSH Verschlüsselung mit zertifikatsbasierter Authentifizierung (RSA 2048 Bits / Protokoll Version 2 / Passphrase / 3DES für Entschlüsselung des privaten Schlüssels)
- Datensignatur
- Datenkompression (optional)
- Verwendung offener Standards (alle Komponenten als OpenSource verfügbar)
- Einfache Integration und Überwachung in Management-Systemen

1 Technische Voraussetzungen für die Nutzung der ELMA-Massendatenschnittstelle

1.1 Systemvoraussetzungen für den Hardware-Einsatz

Die Systemvoraussetzungen für die Nutzung der ELMA-Massendatenschnittstelle 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 getesteten 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.

1.2 Systemvoraussetzungen für den Software-Einsatz

Für die Linux Betriebssystem Derivate (Suse, 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.

Für die Microsoft Windows Betriebssysteme sind kostenfreie Programme aus dem OpenSource Umfeld nutzbar. Hier sind die Programme `puttygen`, `psftp`, `winscp` und `openssl` zu nennen.

1.3 Internetanbindung und Bandbreite

Für die Kommunikation mit dem ELMA Server wird keine dedizierte Internetverbindung benötigt. In Abhängigkeit von den 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.

1.4 Firewall Konfiguration

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

1.5 Identifizierung, Verbindung

Die Übertragungskomponente authentifiziert sich beim Zielsystem mittels RSA Public Private Key Verfahren (OpenSSH Modul) und stellt so die Verbindung her.

Der Austausch der RSA 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.

Die RSA Zertifikate unterliegen den Richtlinien eines strukturierten Rechenzentrum Betriebes.

1.6 Verfügbarkeit und Failover

Der ELMA-Kommunikationskomponente ist redundant ausgelegt. Eine Hochverfügbarkeit wird jedoch nicht garantiert. Durch planmäßige Wartungsarbeiten¹ oder Betriebsstörungen kann es zu temporären Einschränkungen² bei der Erreichbarkeit kommen.

Eine abgebrochene Verbindung / Datenübertragung wird nicht transparent durch das redundante System übernommen. Die Daten sind in diesem Fall erneut zu übertragen.

1.7 Verfahrensaufnahme

Das ELMA-Verfahren steht seit 2007 als Übertragungsweg für die Einlieferung von Massendaten zur Verfügung. Die teilnehmenden Fachverfahren veröffentlichen die für ihren Bereich verwendeten Datenformate und Verfahrensbesonderheiten in gesonderten Dokumenten auf der BZSt-Internetseite.

2 Technische Beschreibung der Kommunikation

2.1 Grundlagen

Für die automatisierte Rechnerkopplung von Großkundensystemen, die Integration in eigene selbst erstellte Programme und für ambitionierte Lieferanten besteht die Möglichkeit die ELMA Massendatenschnittstelle für die Datenübertragung zu verwenden. Diese 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 Protokoll Version SSH-2 ermöglicht die Datenübertragung per SFTP.

¹ Planmäßige Wartungsarbeiten werden bekannt gegeben.

² Eine Ausfallzeit von max. 3 Stunden wird als verfahrenskritisch betrachtet.

Die Internet Assigned Numbers Authority³ (IANA) hat dem Protokoll den TCP-Port 22 zugeordnet.

OpenSSH⁴ wird vom OpenBSD Projekt gepflegt und weiterentwickelt. Die Protokolldefinition erfolgt in den Internet-Drafts der IETF Working Group Secure Shell (secsh)⁵.

Die ELMA-Massendatenschnittstelle verwendet Public Key Authentifizierung und das SSH-2 Protokoll.

Für die Übertragung ist nur `sftp` (Secure File Transfer Protokol) 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.

2.3 Username und Passwort Authentifikation

Die Anmeldung mit Username und Passwort ist an der ELMA-Massendatenschnittstelle nicht möglich.

3 Registrierung und Freischaltung

Über die ELMA-Massendatenschnittstelle können Daten zwischen beliebigen Endstellen und dem ITZBund als Dienstleister für das BZSt übertragen werden. Vor der Datenübertragung sind die nachfolgenden Schritte zu prüfen ggf. zu durchlaufen.

³ <http://www.iana.org>

⁴ <http://www.openssh.org>

⁵ <https://datatracker.ietf.org/doc/search/?name=ssh&sort=&rfcs=on&activedrafts=on>

3.1 Registrierung am BZStOnline-Portal

Zur Teilnahme am ELMA-Verfahren benötigen Sie ein BOP-Zertifikat. Sofern Sie dieses noch nicht haben, führen Sie hierzu eine Registrierung am BZStOnline-Portal durch. Aus technischen Gründen ist es erforderlich, dass Sie bei der Art des Logins ELSTERBasis als Zertifikatstyp auswählen. Als Ergebnis der Registrierung erhalten Sie eine BZSt-Nummer, die die Grundlage für die weiteren Aktivitäten ist. Die Beschreibung des Registrierungsablaufes ist nicht Bestandteil dieser Dokumentation. Ausführliche Informationen finden Sie im Kommunikationshandbuch – Teil 1 (Portalregistrierung).

Tipp: Richten Sie sich vor der Registrierung am BZStOnline-Portal in Ihrem Unternehmen ein Gruppenpostfach ein. Somit können Sie selbst den Teilnehmerkreis definieren und mehreren Mitarbeitern den benötigten Informationszugriff (zum Beispiel: IhreGruppe@IhreDomaene.de) einräumen. Eine Änderung des Teilnehmerkreises ist dann ohne Interaktion mit dem BZSt möglich.

Die bei der Registrierung im BZStOnline-Portal vergebene BZSt-Nummer ist gleichzeitig die Senderkennung und der Zugang zum ELMA-Kommunikationsserver. Sie kann für alle freigeschalteten Verfahren verwendet werden.

3.2 Freischaltung zur Teilnahme am ELMA-Verfahren

Für die folgenden Schritte wird eine vorab durchgeführte erfolgreiche Registrierung vorausgesetzt.

Der Besitz des BOP-Zertifikates berechtigt noch nicht zur Teilnahme am ELMA-Verfahren. Hierzu ist eine explizite verfahrensbezogene Freischaltung erforderlich. Das BZStOnline-Portal bietet Ihnen die Möglichkeit, diese Freischaltung online durchzuführen.

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



Abbildung 1: Versand von Massendaten (ELMA5)

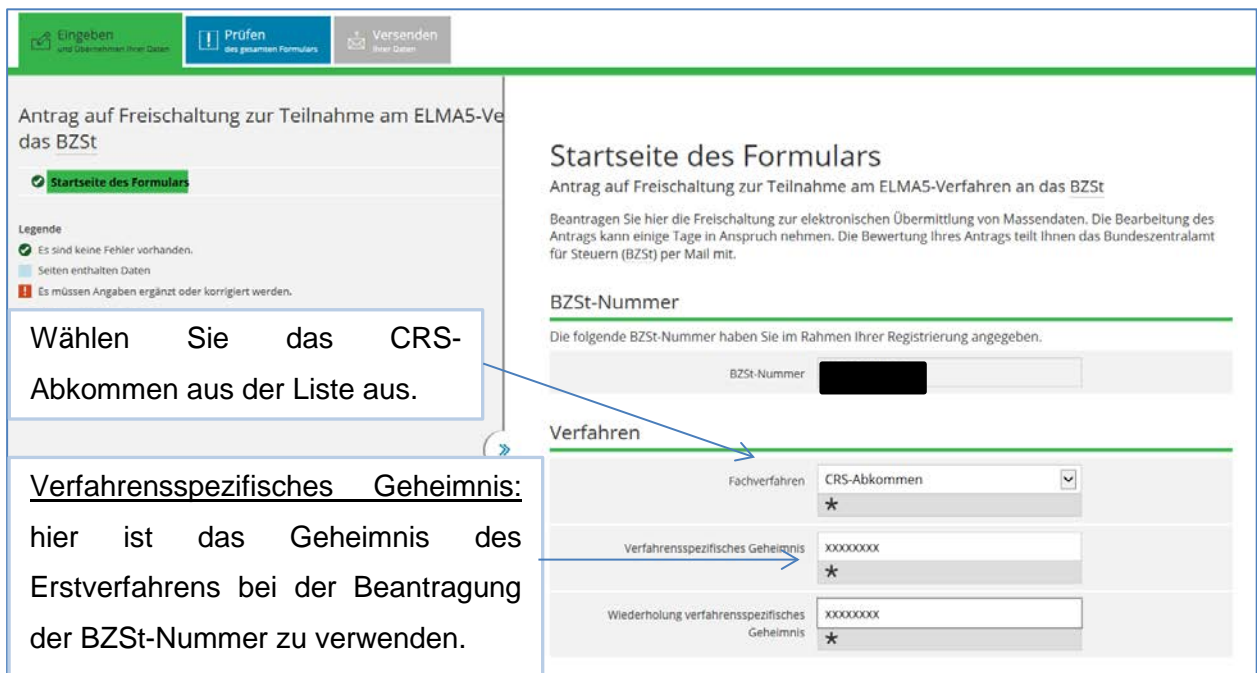



Abbildung 2: Antrag auf Freischaltung zur Teilnahme am ELMA5-Verfahren des BZSt

Im Schritt „Prüfen des gesamten Formulars“ werden Ihre Eingaben auf Plausibilität geprüft. Sollten Ihre Angaben nicht plausibel sein, so erhalten Sie einen entsprechenden Hinweis und werden zur Korrektur Ihrer Eingabe aufgefordert.

Erst wenn Ihre Daten vollständig und geprüft sind, gelangen Sie auf die nachfolgende Formularseite „Versenden Ihrer Daten“, auf der Ihnen die eingegebenen Daten noch einmal

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

angezeigt werden. Überprüfen Sie Ihre Eingaben. Wenn die Daten korrekt sind, drücken Sie auf „Absenden“. Ihre Daten werden authentifiziert und zur weiteren Bearbeitung an das BZSt übermittelt.

Die Bearbeitung des Antrags kann einige Zeit in Anspruch nehmen. Vom BZSt erhalten Sie per E-Mail die Bewertung Ihres Antrages und bei einer positiven Rückmeldung die Senderkennung zur Nutzung der ELMA-Komponente mitgeteilt.

Die Beantragung der Freischaltung zur Teilnahme am ELMA-Massendatenverfahren muss für jedes der unterstützten Verfahren separat erfolgen und setzt voraus, dass Sie über ein verfahrensspezifisches Geheimnis aus dem Erstverfahren verfügen.

3.3 Zertifikat Download im PEM-Format

Mit der BZStOnline-Portal Registrierung haben Sie eine Zertifikatsdatei im PFX-Format erhalten. Dieses Zertifikat ist für die ELMA-Massendatenübertragung mit einer eigenen `sftp` Verbindung in diesem Format nicht nutzbar. Für den `sftp` Verbindungsaufbau zum ELMA-Server und für die Signaturerstellung wird das Zertifikat im PEM-Format benötigt. Es handelt sich dabei um dieselbe Schlüsselinformation. Sie wird lediglich in einem anderen Format für die Verwendung im BZStOnline-Portal zum Download zur Verfügung gestellt.

Auf Linux Maschinen wird das PEM-Format für die `sftp` Datenübertragung verwendet. Auf Windows Systemen ist das PEM-Format vor der Verwendung mit dem `puttygen.exe` Programm in das PPK- Dateiformat zu konvertieren.

Das benötigte PEM-Zertifikat kann im BZStOnline-Portal unter „Formulare & Leistungen“ -> „Versand von Massendaten (ELMA5)“ / “ELMA5-Zertifikat generieren“ generiert werden.

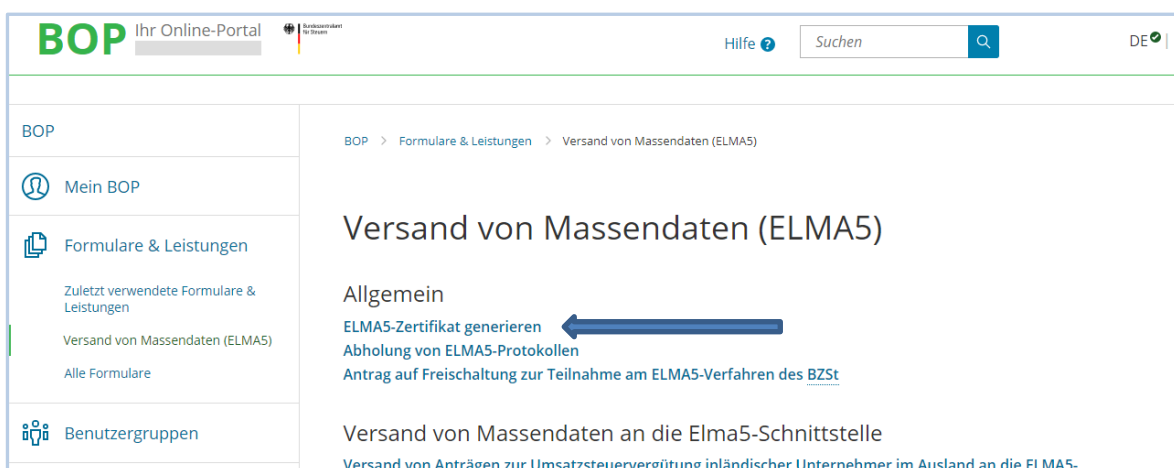



Abbildung 3: ELMA5-Zertifikat für die Erstellung der Signaturdatei generieren

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

Nach erfolgreichem Download verfügen Sie neben der .pfx-Datei über eine weitere Datei mit der .pem-Endung, die Ihnen die Authentifizierung bei der Übermittlung Ihrer Massendaten ermöglicht.

4 Verbindungsprüfung zum ELMA-Server

4.1 Freischaltung für SSH2 über Port 22

Sowohl für den Datenupload über das BZStOnline-Portal, als auch 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 professionell gesicherten großen Netzen muss diese Richtlinie 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 `elma5p.bfinv.de` (IP-Adresse 80.245.147.91⁶) 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 lxmach5x.bfinv.de.
```

```
Escape character is '^]'
```

```
SSH-2.0-OpenSSH_5.5p17
```

⁶ Die IP-Adresse kann ohne vorherige Ankündigung wechseln. Verwenden Sie daher den DNS Service für die Ermittlung der IP-Adresse.

⁷ 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.

Bei einem gesperrten Port würden die Zeilen `Connected` und `SSH-2.0...` nicht angezeigt werden.

Die Port 22 Freischaltung 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 mittels 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 elma5.bfinv.de
```

Antwort im Gutfall:

```
Server:      ....  
Adress:     ....
```

Non-authoritative answer:

```
elma5.bfinv.de  canonical name = lxelma5p.bfinv.de  
Name:          lxelma5p.bfinv.de  
Address:       80.245.147.91
```

4.3 DNS (Domain Name System) Namensauflösung steht nicht zur Verfügung

Der BOP-Upload-Client stellt die Verbindung zum ELMA-Server unter Verwendung des DNS Namen her. 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^8 : \Windows\System32\drivers\etc).

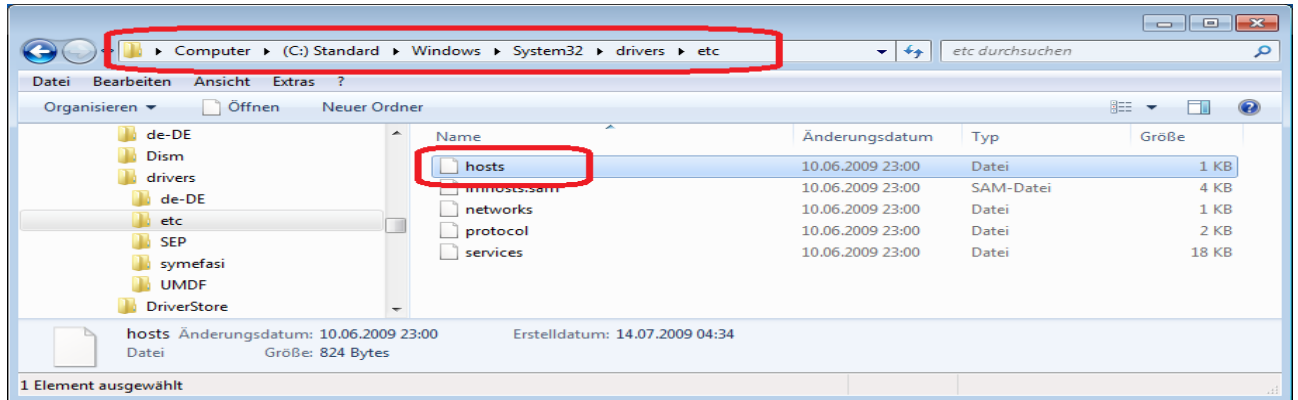


Abbildung 4: Lokalisierung der "hosts" Datei im Explorer

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

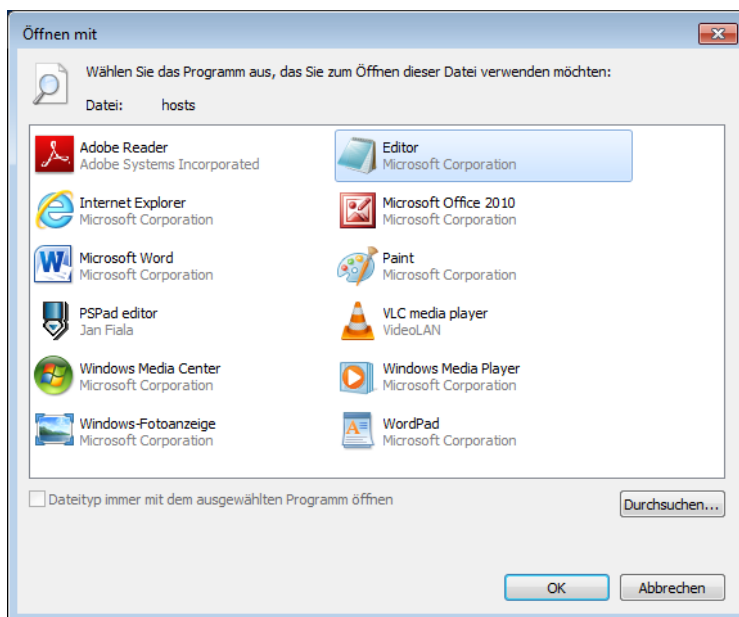


Abbildung 5: Datei mit Editor öffnen

Erweitern Sie die Liste am Ende um den gewünschten Eintrag für den Server (roter Rahmen in Abbildung 6: Ergänzung der `hosts` Datei um `mach5` Servereintrag). Die aktuelle IP-Adresse ist vorab wie unter 4.2 beschrieben zu ermitteln.

⁸ Bei einer auf einem anderen Laufwerk liegenden Systempartition verwenden Sie bitte den entsprechenden Laufwerksbuchstaben.

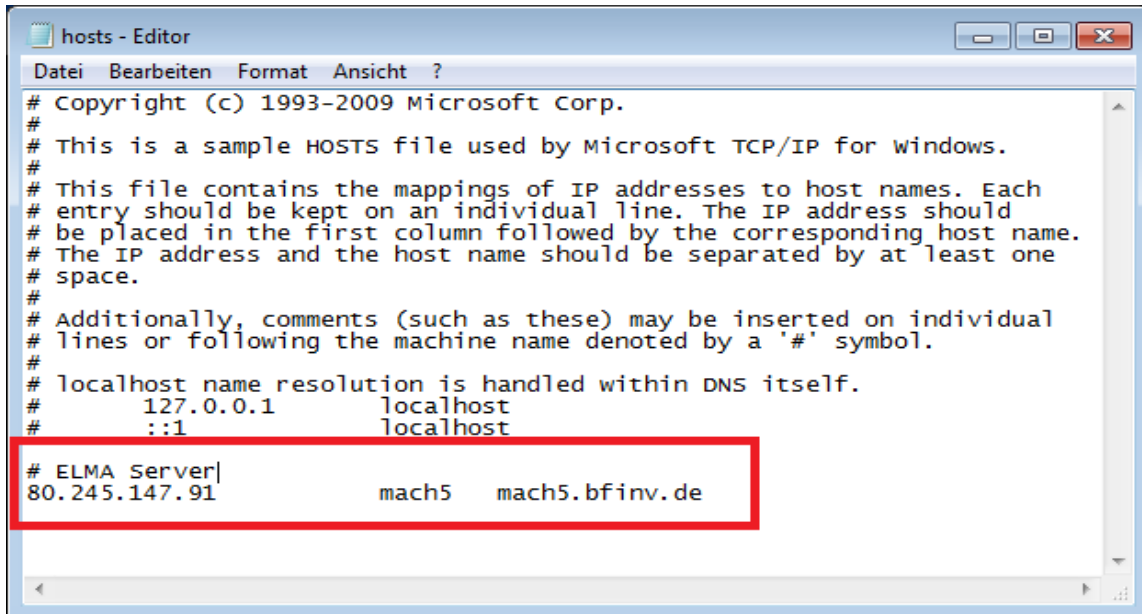


Abbildung 6: Ergänzung der hosts Datei um mach5 Servereintrag

Danach speichern Sie die Datei unter demselben Namen wieder ab. Setzen Sie den Dateityp ggf. auf *.* um (siehe Abbildung 7: Dateityp bei Speicherung setzen).

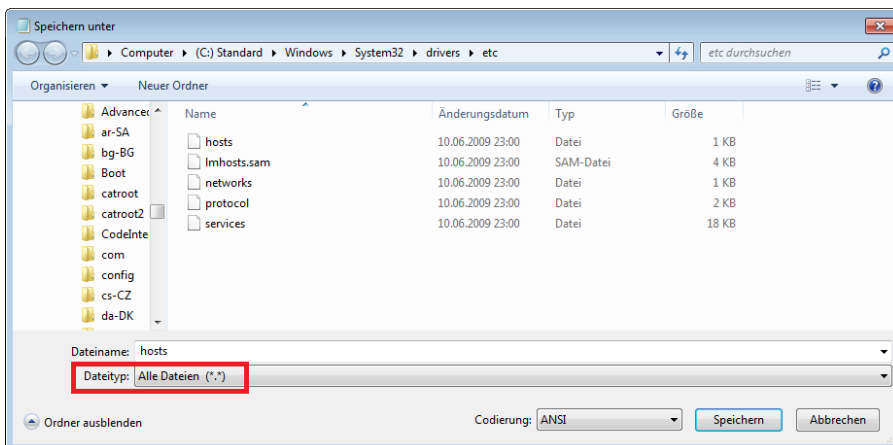


Abbildung 7: Dateityp bei Speicherung setzen

Abschließend beenden Sie alle Browser Instanzen. Geben Sie unter Start->Programme/Dateien durchsuchen das Kommando `ipconfig /flushdns` ein.

4.3.2 Ergänzung der hosts Tabelle unter MAC OS

Für die Durchführung der folgenden Einstellungen wird 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    mach5    mach5.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 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 Einstellungen 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    mach5    mach5.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 Proxies 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 (siehe Ergänzung der `hosts` Tabelle unter Windows). Anstatt der IP-Adresse des ELMA Servers ist die IP-Adresse des Proxies 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 Keine Port 22 Freischaltung für SSH-2 möglich

Sollte eine Portfreischaltung nicht möglich sein, so kann die Datenübertragung nur über einen dedizierten 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`⁹ den Anwendungsstarter und geben Sie den Begriff `terminal` ein. Starte Sie das Programm mit RETURN.

Führen Sie Im Terminal-Fenster die folgenden Kommandozeilen aus.

```
wget http://www.openssl.org/source/openssl-1.0.210n.tar.gz  
tar -xvzf openssl-1.0.2n.tar.gz
```

⁹ Abhängig von der verwendeten Linux / Unix Installation kann die Tastenkombination abweichen.

¹⁰ Die Version kann ggf. abweichen. Verwenden Sie immer die aktuell verfügbare stabile Version.

```
cd openssl-1.0.2d  
  
./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

Öffnen Sie per Tastenkombination `cmd + Leertaste` die Spotlight-Suche und geben den Begriff `Terminal` ein. Starten Sie das Programm durch Doppelklick auf die gewählte Komponente im Suchergebnis.

Führen Sie Im Terminal-Fenster die folgenden Kommandozeilen aus.


```
wget http://www.openssl.org/source/openssl-1.0.2n.tar.gz  
  
tar -xvzf openssl-1.0.2n.tar.gz  
  
cd openssl-1.0.2n  
  
./Configure darwin64-x86_64-cc --prefix=/usr  
  
make  
  
sudo make install
```

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

5.1.3 openSSL Installation unter Windows

Vorkompilierte Win32 / 64 Bibliotheken ohne externe Abhängigkeiten zu den Microsoft Visual Studio¹¹ Runtime-DLLs (Ausnahme System msvcrt.dll) finden Sie unter folgender Adresse:

¹¹ © 1987-2002 Microsoft Corporation. All rights reserved.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

<http://indy.fulgan.com/SSL/openssl-1.0.2n-i386-win32.zip>

http://indy.fulgan.com/SSL/openssl-1.0.2n-x64_86-win64.zip

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

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 Kommandozeile¹² 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 Datei `putty-0.70-installer.msi` (Windows Installer 32-bit) oder `putty-64bit-0.70-installer.msi` (Windows Installer 64-bit) herunter¹³ und führen die Installation aus.

¹² Hier als Beispiel für ein Debian System.

¹³ Verwenden Sie für den Download immer die aktuelle stabile Version.

5.2.4 Einrichtung der Übertragungsumgebung für Linux Systeme

Für die `sftp` Datenübertragung ist kein dedizierter Account auf dem Linux System notwendig. Es empfiehlt sich aber für die Datenübertragung einen entsprechenden User Space für die zu übertragenden Daten einzurichten¹⁴.

```
adduser <Userkennung>
```

Melden Sie sich unter der neu erzeugten Userkennung an und kopieren Sie die Datei `elster.pem` 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
```

5.3 PEM-Datei in das PPK-Format konvertieren

Unter Linux und Mac OS können Sie die PEM-Datei für den Verbindungsaufbau mit dem `sftp` Programm sofort verwenden. Die folgenden Schritte entfallen somit.

Sofern Sie für die Datenübertragung (vornehmlich unter Windows) die Programme `WinScp` oder `Filezilla` verwenden möchten, müssen Sie vorab die PEM-Datei in das PPK-Format konvertieren.

Voraussetzung dafür ist eine bestehende Putty Installation.

Öffnen Sie das Key Generator Programm `PuTTYgen.exe`

¹⁴ Für die Ausführung dieses Kommandos sind Rootrechte notwendig.

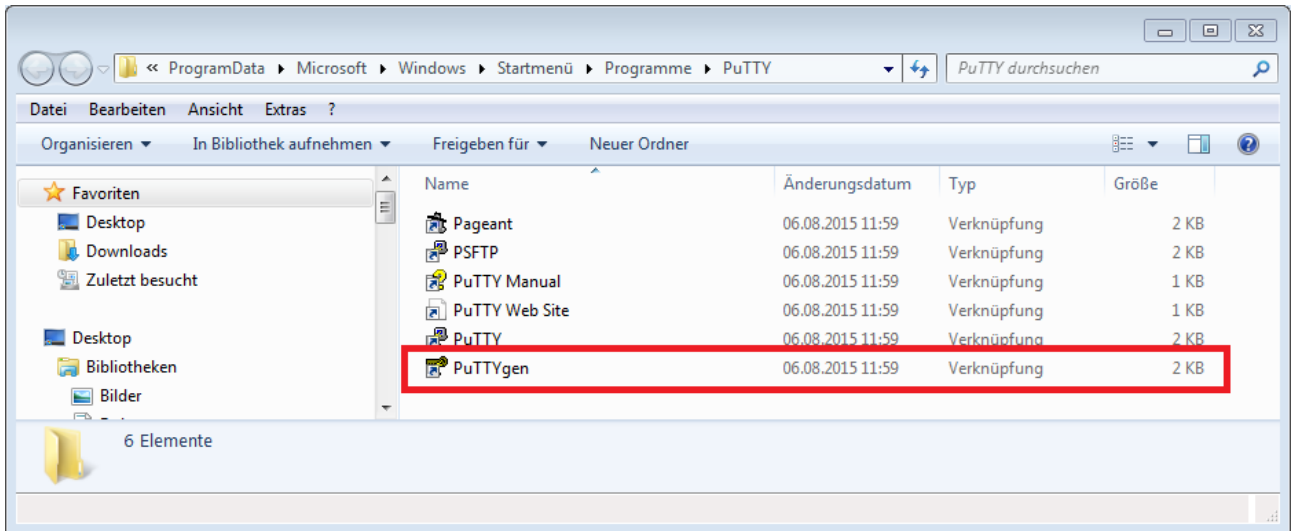


Abbildung 8: PuTTY Programmgruppe

Der PuTTY Key Generator startet.

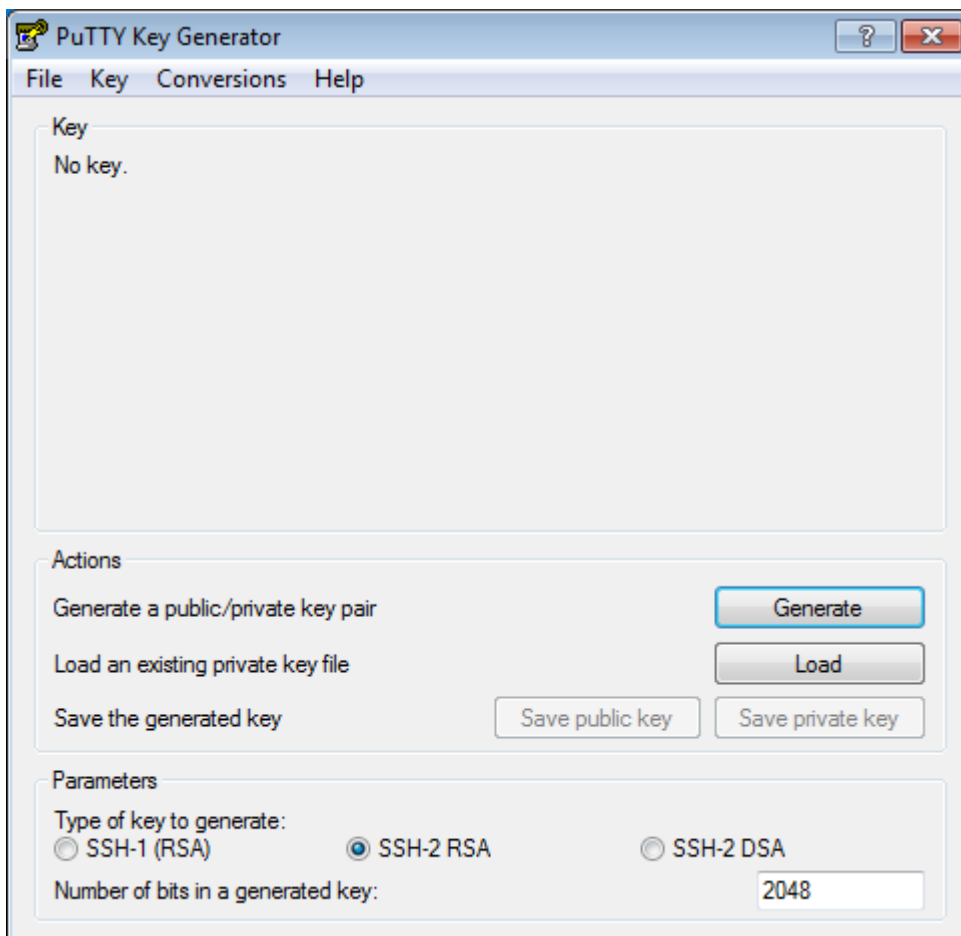


Abbildung 9: Key Generator Startseite

Klicken Sie auf „Load“ und wählen Sie die unter Kapitel 3.3 erzeugte PEM-Datei im Explorer aus.

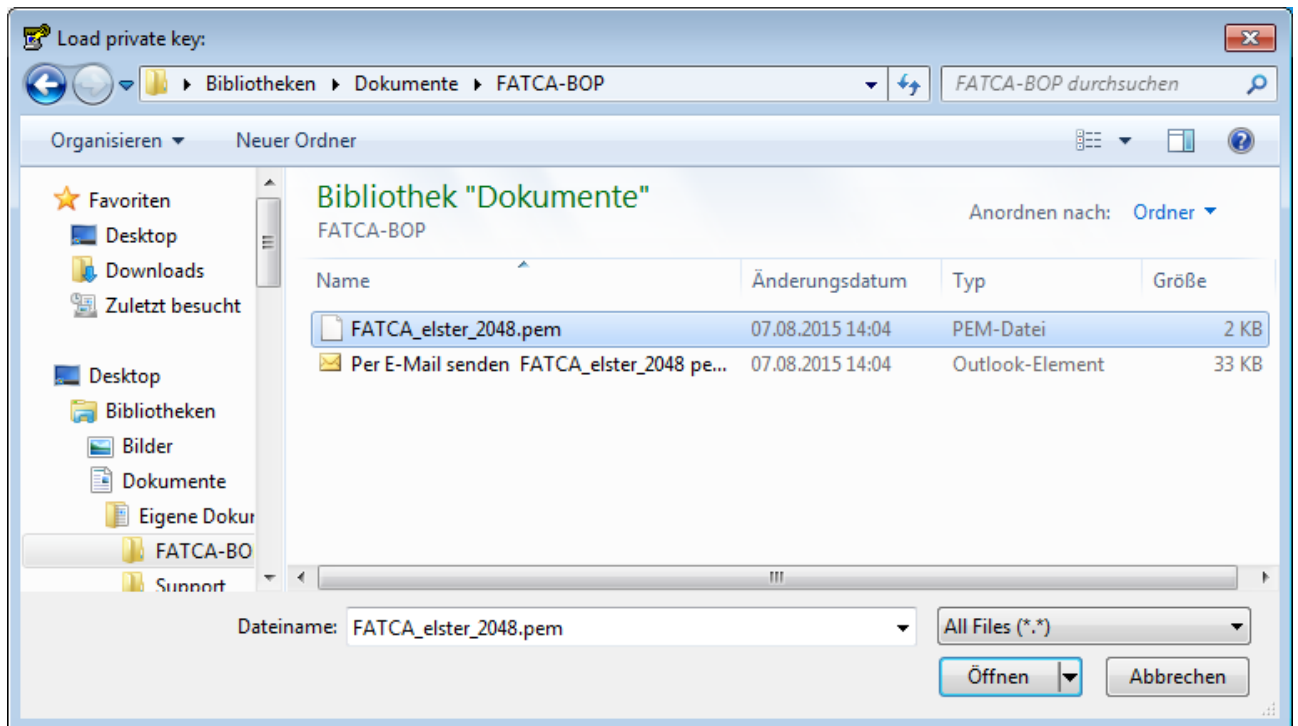


Abbildung 10: Auswahl der PEM-Datei

Die Nutzung der PEM-Datei wird durch die Eingabe der Passphrase¹⁵ freigeschaltet.

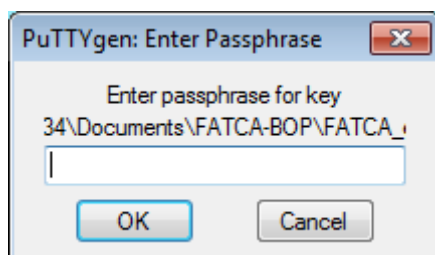



Abbildung 11: Eingabe der Passphrase zur Nutzungsfreischaltung

¹⁵ Das Passwort Ihres BOP-Zertifikates wird automatisch als Passphrase für Ihr ELMA5-Zertifikat verwendet..

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

6 Konventionen für Dateinamen

Jeder Datenupload auf den ELMA-Server besteht immer aus 2 Dateien (Datendatei und Signaturdatei). Die Datendatei enthält den durch das Fachverfahren spezifizierten Meldungsdatensatz. Über die zugehörige Signaturdatei wird die Authentizität des Senders und die Datenintegrität der Datendatei festgestellt.

Das zu übertragende Datenformat wird durch das Fachverfahren festgelegt und ist im jeweiligen Kommunikationshandbuch beschrieben.

Der globale Teil des Dateinamens besteht nur aus den **kleinen Buchstaben** [a-z] und den **Ziffern** [0-9]. Im speziellen Teil des Dateinamens (Dateiid) dürfen zusätzlich Buchstaben in Großschreibung verwendet werden [A-Z]. Die Verwendung von davon abweichenden Zeichen (öäüß 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 xml Suffix.

Dateinamen sind über **Zeit** und **Raum** eindeutig zu vergeben.

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.

Während der Eingangsprüfung wird über die Eingangsdatei ein Hash gebildet, welcher zusammen mit dem Dateinamen gespeichert wird. Bei einer Abweisung ist daher immer ein neuer Dateiname zu bilden und im Datensatz mindestens ein Zeichen zu ändern. So erkennt die ELMA-Prüfung, dass es sich bei der Datenlieferung nicht um eine versehentliche Doppellieferung handelt.

6.1 Namenskonventionen für die Datendatei

Der Aufbau des Dateinamens besteht aus folgenden Teilen:


m5_<pb>_<ssssssssss>_<aaaaaaaa>_<DateiId>.xml

Beispiel für eine CRS Datendatei:

m5_cs_bz123456789_1234567890_sparkohl0001.xml

Feldname	Anzahl Zeichen	Inhalt / Erläuterung	Bemerkungen
----------	----------------	----------------------	-------------

m5	2	ELMA-Dateikennung konstant	- Konstant für alle Verfahren
_	1	Unterstrich - konstant	
<pb>	2	Produktbezeichnung 2-stellig, alphanumerisch, wird vom Fachverfahren vorgegeben	Beispiel: cs (CRS), fc (FATCA)
_	1	Unterstrich - konstant	
<sssssssssss>	11	Alphanumerische BZSt- Nummer des Senders. Diese wurde während der Registrierung im BZStOnline-Portal vergeben.	Ist benutzerabhängig und beginnt mit bz oder bx. Es folgen 9 Ziffern. Beispiel: bz123456789 Wichtig: Kleinschreibung beachten!
_	1	Unterstrich - konstant	
<aaaaaaaaaaa>	10	Account-ID des verwendeten Zertifikats	10-stellige Zahl. Ihre AccountID wird Ihnen im privaten Bereich des BOP-Portalkontos unter „Mein BOP“ -> „Mein Benutzerkonto“ als „Benutzerkonto-ID“ angezeigt.
_	1	Unterstrich - konstant	
<Dateild>	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, A-Z, 0- 9] enthalten. Es sind keine Sonderzeichen oder Unterstriche () erlaubt. Eine naheliegende Option für Dienstleister ist die Codierung des FI, in dessen Auftrag die Datendatei erstellt wird.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

.	1	Punkt – konstant Trennung Präfix.Suffix	
xml	3	Suffix - konstant	

Tabelle 1: Aufbau Dateinamen bei Lieferung

6.2 Namenskonvention für die Signaturdatei

Zu jeder Datendatei gehört eine korrespondierende Signaturdatei. Der Name der Signaturdatei besteht aus dem Namen der Sendedatei, wobei dieser um den Suffix `.sig` erweitert wird.

`m5_<pb>_<ssssssssss>_<aaaaaaaa>_<DateiId>.xml.sig`

6.3 Namenskonvention für die Rückmeldedatei

Rückmeldungen erfolgen (sofern das Fachverfahren solche unterstützt) auf elektronischem Wege. Die Dateien basieren auf den Dateinamen der Meldung und werden im `/download` Verzeichnis des Kommunikationsservers zur Verfügung gestellt. Der Empfänger wird über die Existenz einer Rückmeldung per E-Mail informiert. Es obliegt ihm, die Rückmeldung auf sein System zu laden und zu verarbeiten.

Die Rückmeldedatei (Antwortdatei / Ergebnisdatei) entspricht den Namenskonventionen der Sendedatei. Sie wird im „download“ Verzeichnis eingestellt und der Dateiname als Rückmeldung durch Ergänzung einer UUID vor dem Punkt kenntlich gemacht. Für jede Rückmeldedatei wird eine eindeutige UUID vergeben.


`m5_<pb>_<ssssssssss>_<aaaaaaaa>_<DateiId>_<uiuiuiui-
uiui-
uiui-
uiui-
uiuiuiuiui>.xml`

Beispiel einer CRS Rückmeldedatei:

`m5_cs_bz123456789_1234567890_name0001_da5b42ce-9d27-4255-920e-1a089ee0ec8.xml`

7 Bereitstellung der zu übertragenden Dateien

Die vom Sender eingestellten Dateien (Datendatei und Signaturdatei) werden vor der Weiterleitung an das zugehörige Fachverfahren gegen das folgende Regelwerk geprüft. Die Dateien werden von der ELMA-Massendatenschnittstelle geprüft und nur bei Erfüllung aller Prüfpunkte akzeptiert.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

7.1 Prüfung der XML-Datendatei

Prüfen Sie vor der Signaturerstellung und Übertragung der Datendatei die folgenden Punkte auf ihre Validität:

7.1.1 UTF-8 Kodierung

Für die Erstellung der XML-Datei ist die UTF-8 Kodierung ohne BOM¹⁶ zu verwenden. Abweichende Kodierungen werden nicht unterstützt und führen zu einer ganzheitlichen Abweisung.

Es wird empfohlen, nur die üblicherweise in Namens- und Adressdaten enthaltenden Zeichen der UTF-8 Kodierung zu nutzen¹⁷. 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](#) herangezogen werden.

7.1.2 XSD-Schema Validierung

Die XML-Datendatei ist vor der Versendung gegen das vom Fachverfahren zur Verfügung gestellte aktuelle XSD Schema zu validieren.

Dabei sind folgende Punkte zu beachten:

- Die „Namespace“-Einsetzungen müssen korrekt sein.
- Für jeden Namespace-Prefix muss das `xmlns:prefix` Attribut einmalig vorhanden sein.
- Das `xsi:schemaLocation` Attribut muss einmalig vorhanden sein.
- Das Erstellungsdatum im ELMA-Header ist mit dem Tagesdatum des voraussichtlichen Datei-Uploads zu füllen.


7.1.3 Unzulässige Zeichen und Beschränkungen

Die nachfolgend dargestellten Zeichen sind als Inhalt in einem Feld unzulässig. Sie führen zur Abweisung der eingereichten Lieferung.

Zeichen	Englische Beschreibung	Deutsche Beschreibung
'	Apostrophe	Apostroph

¹⁶ Als Byte Order Mark wird das Unicode Zeichen U+FEFF verwendet.

¹⁷ Je nach dem gewählten Fachverfahren können die zu verwendenden Zeichen eingeschränkt sein.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

--	Double Dash	Doppelter Trennstrich
#	Hash	Doppelkreuz
&	Ampersand	Kaufmännisches Und
<	Less Than	Kleiner als
"	Quotation Mark	Anführungszeichen
>	Greater Than	Größer als

Tabelle 2: Übersicht unzulässiger Zeichen

ELMA nimmt Daten gemäß UTF-8 grundsätzlich ohne Einschränkung an.

In den ELMA Elementen (ELMAxx, ELMAKOM, ELMAHeader, ELMAVerfahren) werden keine Ersetzungszeichen benötigt. Die Verwendung würde zu einer Abweisung führen.

Im XML sind Markierungen erlaubt. Sie werden aber herausgefiltert. Demnach führt auch "`<![CDATA[[]]>`" oder "`<![CDATA[[]]>`-" zur Ablehnung, weil die Zeichenkette "--" im XML enthalten ist.

7.1.4 Dateigrößenbeschränkung

Die zu übermittelnde Datendatei darf bis zu 100 MB groß sein. Eine Überschreitung dieser Maximalgröße kann zu einer Dateiabweisung führen. Davon abweichende Regelungen sind fachverfahrensspezifisch hinterlegt.

7.1.5 Aufbau ELMAKOM-Header

Der Aufbau der XML-Struktur besteht aus einem Root-Element (welches vom Namen abweichend benannt sein kann). Dieses Element stellt den Wurzelknoten für die gesamte zu übertragende Datei da.

Danach folgt der ELMAKOM-Abschnitt. Dieser beinhaltet die Teile ELMAHeader und ELMAVerfahren. Der ELMAHeader enthält alle Informationen des Senders für die Fachverfahrens- und Sender-Zuordnung. Unter ELMAVerfahren befinden sich die fachverfahrensspezifischen Inhalte. Die Beschreibung der Struktur ist nicht Bestandteil dieser Dokumentation. Hier wird auf das jeweilige Fachverfahren verwiesen.

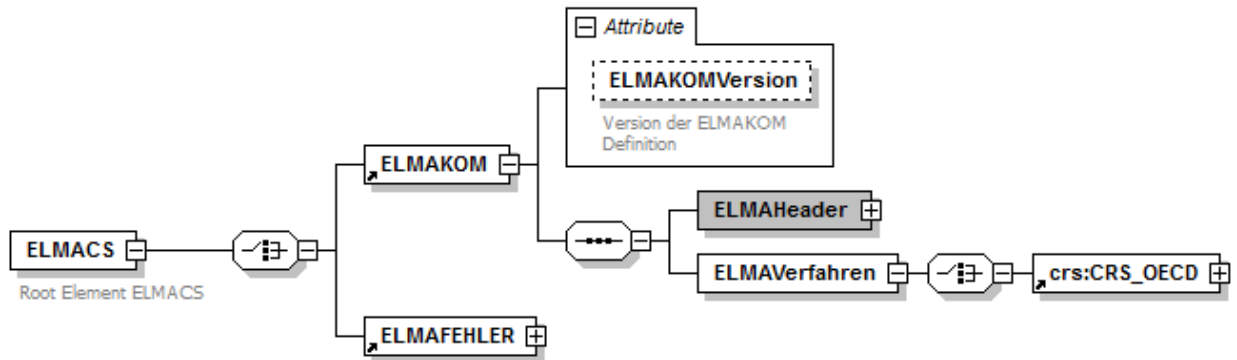


Abbildung 14: Beispiel mit ELMACS als Root-Element für das CRS-Fachverfahren

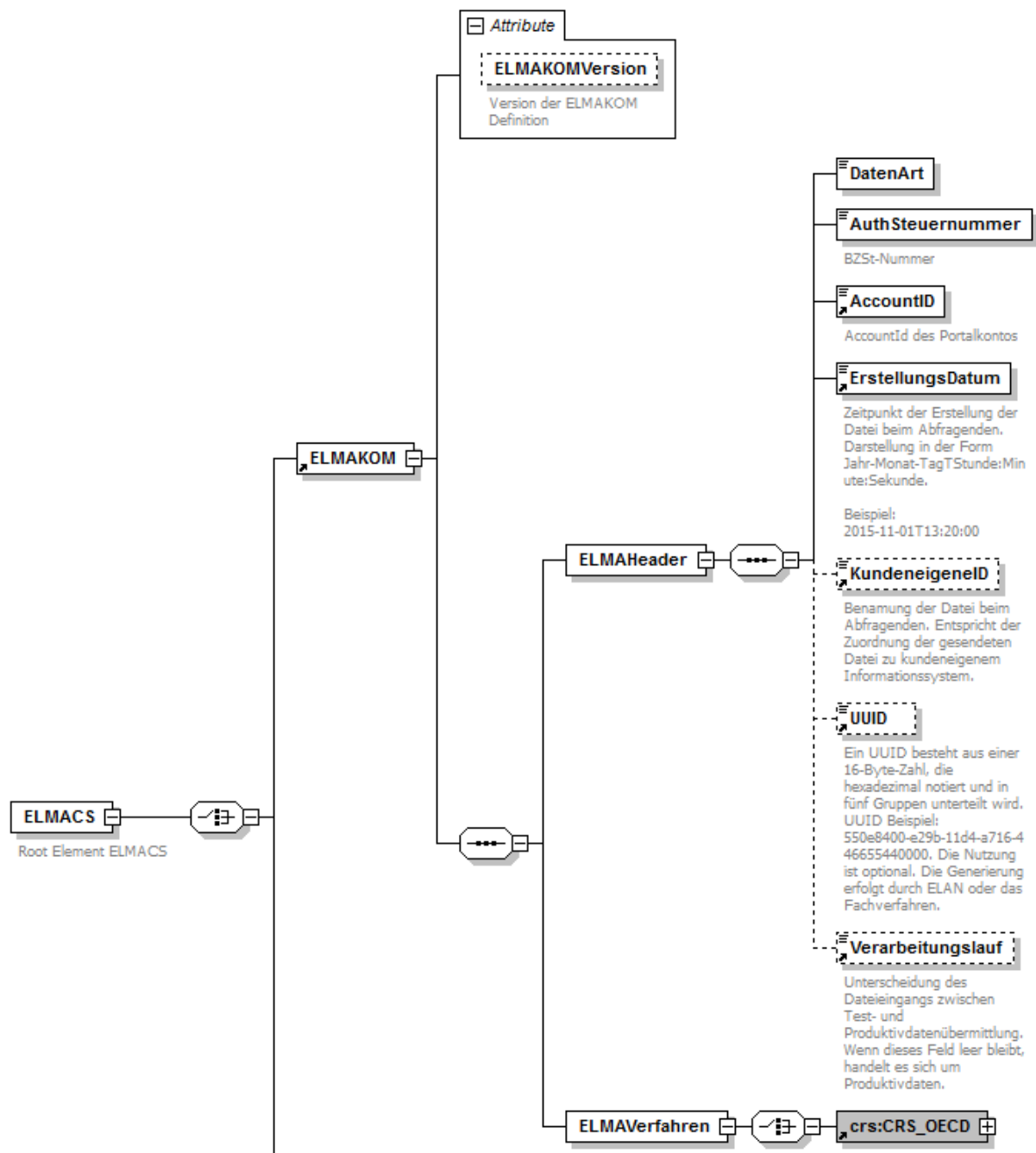



Abbildung 15: Aufbau des ELMAHeader

Nachfolgende Tabelle beschreibt die Befüllung des ELMAKOMHeaders.

Feldname	Anzahl Zeichen	Typ	M/ Muss K/ Kann	Inhalt / Erläuterung	Bemerkungen
ELMAKOMVersion	1		K	1	Siehe Vorgabe des Fachverfahrens
DatenArt	10		M	%	Siehe Vorgabe des Fachverfahrens. Für CRS → CRS_ELMA
AuthSteuernummer	11	an	M	Die verwendete BZSt-Nummer	Ist benutzerabhängig. Beginnt mit BZ oder BX gefolgt von 9 Ziffern. Beispiel: „BZ123456789“ Wichtig: Großschreibung beachten!
AccountID	10	an	M	Die verwendete AccountID des Anwenders	10-stellige Zahl. Die AccountID wird im privaten Bereich des BOP-Portalkontos unter „Mein BOP“ -> „Mein Benutzerkonto“ als „Benutzerkonto-ID“ angezeigt.
ErstellungsDatum	19	An	M	Tagesdatum des Dateiuploads der Dateien	Dieses Feld ist mit dem Erstellungsdatum zu füllen. Die Übertragungszeit wird nur informationshalber genutzt. Format:Jahr-Monat-TagTStunde:Minute:Sekunde Beispiel: 2014-12-31T13:20:00
KundeneigenelD	12	an	K		Kann für die Zuordnung der gesendeten Datei zum kundeneigenen Informationssystem verwendet werden. <u>Dieses Feld muss genau 12 Zeichen enthalten.</u> Eine Abweichung führt zu einer Abweisung.
UUID	36	an	K	Kennzeichnung	Ein UUID besteht aus einer 16-

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

				der Datenlieferung	Byte-Zahl, die hexadezimal notiert und in fünf Gruppen unterteilt wird. UUID Beispiel: 550e8400-e29b-11d4-a716-446655440000
Verarbeitungslauf	ENUM		K	PRODUKTION SLAUF oder TESTLAUF	Unterscheidung des Dateneingangs zwischen Test- und Produktivdatenübermittlung. Bei einem leeren Feld handelt es sich immer um Produktionsdaten.

Tabelle 3: Inhalt ELANKOMHeader

7.2 Signaturdatei erstellen

Zu jeder Datendatei muss eine korrespondierende Signaturdatei erstellt und übermittelt werden. Die Signatur bezieht sich nur auf den Inhalt der Datendatei. Eine Änderung im Namen der Datendatei bedingt keine neue Signaturdatei.

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

Im Rahmen der Anpassung an die neuesten BSI Sicherheitsstandards muss zur Erstellung der Signaturdatei ab Dezember 2018, spätestens September 2019, als Signaturverfahren RSASSA-PSS¹⁸ mit folgenden Parametern verwendet werden:

Hashverfahren: SHA-256

Mask Generation Function: MGF1 mit SHA-256 Länge des Salts: 32 Byte Trailer Field: 0xBC

Die Umstellung der Signaturverfahren erfolgt stufenweise. Ab September 2019 ist zwingend das Signaturverfahren RSASSA-PSS mit dem Hashverfahren SHA-256 zu nutzen. Einlieferungen nach dem bisherigen Signaturverfahren (RSASSA-PKCS1-v1_5 mit SHA-512) werden ab diesem Zeitpunkt abgewiesen. Wir empfehlen daher eine frühzeitige Umstellung des Signaturverfahrens.

7.2.1 Signaturdatei unter Linux erstellen

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

¹⁸ RSASSA-PSS ist in PKCS #1 ab Version 2.1 standardisiert. Die aktuelle Version 2.2 finden Sie in RFC 8017 unter <https://tools.ietf.org/html/rfc8017>

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 dgst -sha256 -binary -out <Dateiname-mit-Suffix>.sig \19  
  
-sigopt rsa_padding_mode:pss  
  
-sigopt rsa_pss_saltlen:-1  
  
-sign ~20/.ssh/elster.pem <Dateiname-mit-Suffix>
```

Enter pass phrase for key: <Passphrase>

Nach Eingabe der Passphrase wird die Signaturdatei erstellt.

7.2.2 Signaturdatei unter Windows erstellen

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


Wechseln Sie in das Verzeichnis der Datendatei. Die `elster.pem` Schlüsseldatei muss im selben Verzeichnis liegen. Andernfalls ist diese im folgenden Aufruf mit einer Pfadangabe zu versehen. Führen Sie im Kommandozeilen-Fenster die folgende Kommandozeile aus. Substituieren Sie [Pfadangabe] durch das Installationsverzeichnis der `openssl.exe` Datei.

```
[Pfadangabe]\openssl.exe dgst -sha256 -binary \21  
  
-out <Dateiname-mit-Suffix>.sig  
  
-sigopt rsa_padding_mode:pss  
  
-sigopt rsa_pss_saltlen:-1  
  
-sign elster.pem <Dateiname-mit-Suffix>
```

¹⁹ Das Zeichen „\¹⁹“ stellt die Fortsetzung der Eingabe in einer neuen Zeile dar. Wird die Eingabe nicht in einer neuen Zeile fortgesetzt, kann dies entfallen.

²⁰ Das Zeichen „~“ referenziert das Home-Verzeichnis des Anwenders. Hier kann auch der komplette Pfad angegeben werden.

²¹ Das Zeichen „\²¹“ stellt die Fortsetzung der Eingabe in einer neuen Zeile dar. Wird die Eingabe nicht in einer neuen Zeile fortgesetzt, kann dies entfallen.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

Enter pass phrase for key: <Passphrase>

Nach Eingabe der Passphrase wird die Signaturdatei erstellt.

8 Übertragung Daten- und Signatur-Datei an die ELMA-Massendatenschnittstelle

8.1 Aufbau der Verbindung

Die Einlieferung einer ELMA-Datei erfolgt über eine Rechner-zu-Rechner-Kopplung per SFTP. Der zu verwendende DNS-Name ist: **elma5p.bfinv.de** (IP-Adresse: 80.245.147.91)

Es ist zu beachten, dass zur Konfiguration der Serververbindung nur dieser DNS-Name zu verwenden ist und nicht die resultierende IP-Adresse. Das BZSt behält sich vor, die IP-Adresse jederzeit ohne Vorankündigung zu ändern.

Als Benutzername ist Ihre BZ-Nummer in der Form „bz123456789“ (klein geschriebenes „bz“) und als Passwort die Passphrase²² anzugeben. Zudem ist darauf zu achten, dass das Zertifikat aus Kapitel 5.2.4 bzw. 5.3 im SFTP-Programm hinterlegt ist.


8.2 Ablauf der Datenübertragung

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.

Es ist immer zuerst die Datendatei und anschließend die korrespondierende Signaturdatei in das „upload“- Verzeichnis auf dem ELMA- Server einzustellen.

²² Das Passwort Ihres BOP-Zertifikates wird automatisch als Passphrase für Ihr ELMA5-Zertifikat verwendet.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

8.3 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.

8.4 Umbenennung der Dateien

Beim Upload der Datei- und Signaturdatei 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

Erst nach einem erfolgreichen Transfer auf den ELMA Server sind die 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.

8.5 Abholung Rückmeldedatei

Die Rückmeldedateien stehen im „download“-Verzeichnis auf dem ELMA Server zur Abholung bereit.


Der Verbindungsaufbau und der Datentransfer erfolgt wie unter Kapitel 8.1 und 8.2 beschrieben. Es ändert 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 Bereitstellung²³ automatisiert gelöscht. Dies gilt unabhängig davon, ob die Datei zuvor bereits abgerufen wurde. Eine erneute Wiederherstellung der Datei ist nicht möglich.

9 ELMA Eingangsprüfungen

Nach der Dateieinlieferung in das Upload-Verzeichnis werden formale Prüfungen vorgenommen.

In der Regel erfolgen diese Prüfungen zeitversetzt, also nicht unmittelbar nach dem Upload.

²³ Ab dem Tag der E-Mailversendung.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

Falls eine der nachfolgenden Prüfungen nicht erfolgreich ist, wird diese abgebrochen, die betroffene Datei im Upload-Verzeichnis gelöscht und vollständig abgewiesen. Der Sender der Datei erhält – wenn möglich – eine E-Mail mit der Fehlermeldung an die im Portalkonto zur BZSt-Nummer hinterlegte Adresse.

9.1 Allgemeine formale Vorprüfung

- Ist eine Datendatei und eine Signaturdatei mit gleichlautenden Dateinamen im Namenteil vor dem Suffix vorhanden?
- Entsprechen beide Dateinamen (Daten- und Signaturdatei) Aufbau und Schreibweise der Namenskonvention?
- Wurde die Signaturdatei mit dem zur *Account-ID* (Benutzerkonto-ID) gehörigen Zertifikat erstellt?
- Ist die Signaturdatei 256 Byte groß?
- War die Signaturprüfung erfolgreich?
- Ist die einzelne Datendatei oder die einzelne Signaturdatei älter als 10 Tage?
- Wurde zu einem früheren Zeitpunkt bereits eine Datei gleichen Namens gesendet? (Dies ist nicht zulässig.)
- Diese Prüfung erfolgt auch für Dateinamen von bereits abgewiesenen Dateien. Nach der Abweisung einer Lieferung ist daher sowohl der Dateiname als auch der Dateiinhalt zwingend zu verändern. Der Dateninhalt der XML-Datendatei kann durch ein zusätzliches Leerzeichen an entsprechender Stelle geändert werden.
- Wurde zu einem früheren Zeitpunkt für die *Account-ID* bereits eine Datei mit komplett identischem Inhalt gesendet? (Dies ist nicht zulässig.)
- Diese Prüfung erfolgt auch für bereits abgewiesene Dateien. Nach der Abweisung einer Lieferung ist daher sowohl der Dateiname als auch der Dateiinhalt zwingend zu verändern.

9.2 Erweiterte Vorprüfung für XML-Datenlieferungen

9.2.1 Liste der möglichen ELMA Fehlercodes und deren Bedeutung

Nach der Einstellung der XML-Datenlieferung und der Signaturdatei in das „upload“-Verzeichnis wird während des ELMA Verarbeitungslaufes im korrespondierenden „download“-Verzeichnis eine Datei mit dem für die Datenlieferung verwendeten Dateinamen und dem zur Dateilieferung gehörenden Fehlercode eingestellt. Zusätzlich wird eine E-Mail an die im Portalkonto zur BZSt-Nummer gehörende AccountID hinterlegte E-Mail Adresse versendet.

Für die E-Mail Betreffzeile wird folgender Eintrag verwendet:

ELMA5- Verarbeitungsstatus: DATEINAME

oder

Verarbeitungsstatus: DATEINAME

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


FehlerID in der XML Datei	Bedeutung	E-Mail Text
8000	Datei wurde 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.

Die FehlerID 8000 ist eine Ausnahme, da sie eigentlich keinen Fehler bedeutet. In diesem Fall wurde die Datenlieferung durch die ELMA-Schnittstelle angenommen und zur Prüfung an das Fachverfahren übergeben.

Nachfolgend werden die möglichen ELMA Fehlercodes und deren Bedeutung dargestellt.

FehlerID in der XML Datei	Fehlerfall	E-Mail Text
8001	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	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	Dateiname nicht korrekt	Wir haben Ihre im Betreff genannte Datei erhalten. Der Dateiname entspricht leider nicht den Namenskonventionen. Die Datei wurde abgewiesen.
8004	Falsche BZSt Nummer	Wir haben Ihre im Betreff genannte Datei

	verwendet	erhalten. Die BZSt-Nummer im Dateinamen entspricht leider nicht Ihrer Senderkennung. Die Datei wurde abgewiesen.
8005	Signatur-Datei fehlt	Wir haben Ihre im Betreff genannte Datei erhalten. Leider fehlt die zugehörige Signaturdatei. Die Datei wurde abgewiesen.
8006	Signaturprüfung fehlgeschlagen	Wir haben Ihre im Betreff genannte Datei erhalten. Die Signaturprüfung ist leider fehlgeschlagen.
8007	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 www.bzst.bund.de . Die Datei wurde abgewiesen.
8008	Keine ELMA5 Freischaltung für das Verfahren vorhanden	Wir haben Ihre im Betreff genannte Datei erhalten. Es besteht keine Freischaltung für das gewünschte Fachverfahren. Die Datei wurde abgewiesen.
8009	Portalkonto 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 www.bzst.bund.de . Die Datei wurde abgewiesen.
8009	ELANNutzer gesperrt	Wir haben Ihre im Betreff genannte Datei erhalten. Ihre BZSt-Nummer bzw. Ihr

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------


			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 www.bzst.bund.de . Die Datei wurde abgewiesen.
8010	Dateiname verwendet	bereits	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 übermittelt	bereits	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	Headerdaten = Dateiname		Wir haben Ihre im Betreff genannte Datei erhalten. Die BZSt Nummer und/oder die AccountID sind im Dateinamen und im ELMA-Header der Datei unterschiedlich. Die Datei wird nicht verarbeitet und abgewiesen.
8013	Testlauf verwendet		Wir haben Ihre im Betreff genannte Lieferung erhalten. Der verwendete Verarbeitungslauf ist ungültig. Daher wurde die Lieferung abgewiesen. Für FATCA derzeit nicht relevant.

Tabelle 4: Liste der möglichen ELMA Fehlercodes

9.2.2 Prüfung auf Schemakonformität

- Ist die XML-Datei gegen das XSD-Schema des entsprechenden Fachverfahrens validierbar?

Ist diese Prüfung nicht erfolgreich, so wird eine Antwortdatei mit ELMAFEHLER, Fehler-ID = 8001 (Schema Fehler) erzeugt und im download-Verzeichnis auf dem ELMA Server

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

bereitgestellt.

Diesbezüglich erhält der Sender der Datei eine E-Mail. Diese wird an die zur BZSt-Nummer im Portalkonto hinterlegte E-Mail-Adresse gesendet.

9.2.3 Prüfung des XML-Rahmens

- Wurde die UTF-8 Zeichenkodierung verwendet?
- Wurde die Datei ohne Byte Order Mark²⁴ (BOM) erstellt?

Ist mindestens eine dieser Prüfungen nicht erfolgreich, so wird eine Antwortdatei mit ELMAFEHLER, Fehler-ID = 8002 (Codepage Fehler) erzeugt und im download-Verzeichnis auf dem ELMA Server bereitgestellt.

Diesbezüglich erhält der Sender der Datei eine E-Mail. Diese wird an die zur BZSt-Nummer im Portalkonto hinterlegte E-Mail-Adresse gesendet.

9.2.4 Prüfung der Berechtigung

- Ist die im Dateinamen verwendete BZSt-Nummer mit der im Feld `ELMAHeader->AuthSteuernummer` eingetragenen Information innerhalb der Datei identisch?
- Wurde die BZSt- Nummer innerhalb der Datei in Großbuchstaben und im Dateinamen in Kleinbuchstaben verwendet?
- Kann die BZSt-Nummer dem Sender zugeordnet werden?
- Ist die im Dateinamen verwendete `AccountID` mit der im Feld `ELMAHeader->AccountID` eingetragenen Information innerhalb der Datei identisch?
- Kann die `AccountID` dem Sender zugeordnet werden (Signaturprüfung)?
- Ist die BZSt-Nummer des Senders gesperrt oder für das Fachverfahren stillgelegt?
- Ist die `AccountID` des Senders für Fachverfahren gesperrt?

Ist mindestens eine dieser Prüfungen nicht erfolgreich, so wird eine ELMAFEHLER Rückmeldedatei mit entsprechender FehlerID erzeugt und im download-Verzeichnis auf dem ELMA Server bereitgestellt.

Diesbezüglich erhält der Sender der Datei eine E-Mail. Diese wird an die zur BZSt-Nummer im Portalkonto hinterlegte E-Mail-Adresse gesendet.

²⁴ Die Bytesequenz EF BB BF ist am Dateianfang nicht erlaubt und führt zu einer Abweisung.

9.3 ELMA Prüfungen erfolgreich absolviert

Sofern die ELMA Prüfungen alle erfolgreich absolviert wurden, wird die eingereichte Datei für das jeweilige Fachverfahren eingestellt und im upload-Verzeichnis gelöscht.

Der Portalkontoinhaber erhält eine E-Mail an die im Portalkonto hinterlegte E-Mail Adresse. Mit dieser wird er darüber informiert, dass seine Datei im ELMA upload-Verzeichnis eingegangen ist und nach einer erfolgreichen Vorprüfung (ohne Fehler) an das gewünschte Fachverfahren zur Bearbeitung überstellt wurde.

Vom jeweiligen Fachverfahren kann der Portalkontoinhaber nach Dateieingang zusätzlich eine E-Mail an die im Portalkonto hinterlegte E-Mailadresse erhalten (abhängig vom Verfahren). Mit dieser wird er darüber informiert, dass seine Datei bei der Verarbeitung des Fachverfahrens eingegangen ist.

9.4 Abfolge der ELMA Dateiprüfung

Die Prüfungen durch die ELMA-Massendatenschnittstelle kann die Abweisung der Datendatei und der Signaturdatei bedeuten. In diesem Fall wird der Fehlergrund vom ELMA Server durch eine E-Mail an die im Portalkonto hinterlegte E-Mailadresse versendet. Der Sender der Daten erhält nach Abschluss der Verarbeitung in jedem Fall eine FehlerXML Antwortdatei in sein Downloadverzeichnis eingestellt. Der Dateiname entspricht dem Namen der Sendedatei. Über die in der Datei enthaltene FehlerID kann eine Analyse der Ursache im Abweisungsfall durchgeführt werden.

Die ELMA Prüfabfolge und die möglichen resultierenden Fehler sind in der folgenden Tabelle zusammen mit Lösungshinweisen beschrieben.

Lfd. Nr.	Was wird geprüft?	Hinweise	FehlerID
1	Entspricht der Name der Signaturdatei dem Namen der Datendatei plus dem Dateianhang (Suffix) „.sig“? Ist die Größe der Signaturdatei = 256 Byte? Wurde die Signatur mit dem zur AccountID gehörenden Zertifikat erstellt?		8005
2	Handelt es sich bei der XML-	Informationen zur UTF-8 Zeichencodierung	8002


	<p>Datei um eine UTF-8- und Validierung finden Sie unter der URL: konforme Datei ohne Byte https://www.w3.org/International/questions/qa-validator-charset-check.de. Order Mark (BOM)?</p> <p>Öffnen Sie die Datei in einem Hex-Editor und entfernen Sie ggf. am Anfang der Datei die Bytesequenz EF BB BF, da die Verwendung von Byte Order Mark nicht unterstützt wird.</p>	
3	<p>Konnte die XML-Datendatei gegen das verfahrensspezifische Schema validiert werden?</p>	8001
4	<p>Entspricht der Dateiname den Konventionen?</p> <p><i>m5_xx_{a-z0-9}{11}_{09}{10}_{a-z0-9}{1,12}.xml</i></p> <p>Wobei xx dem jeweiligen Verfahrenskennzeichen entspricht.</p>	8003
5	<p>Entspricht die im Dateinamen verwendete BZSt-Nummer dem Namen des ELMA-Home Verzeichnisses?</p>	8004
6	<p>Sind die BZSt-Nr. und die AccountID im Dateinamen mit den Einträgen im ELMA-Header der Datendatei identisch?</p>	8012
7	<p>Wurde die Signatur mit dem zugehörigen Zertifikat erstellt?</p>	8006
8	<p>Wurde zu einem früheren Zeitpunkt bereits eine Datei gleichen Namens in die</p>	8010

²⁵ Ab Dezember 2018 sind Signaturen sowohl mit sha512 als auch sha256 zulässig. Ab August 2019 sind nur noch Dateieinlieferungen mit einer Signatur nach RSASSA-PSS mit SHA-256 erlaubt.

	Produktions- oder Testumgebung gesendet?	Dateiname und der Dateinhalt (z.B. durch Einfügen eines Leerzeichens) zu ändern.	
9	Wurde zu einem früheren Zeitpunkt für diese BZSt-Nr. und AccountID bereits eine Datei mit identischem Inhalt in die Produktions- oder Testumgebung eingestellt?	Für jede Datenlieferung wird ein Hashcode gebildet und gespeichert. Über den Hashcode wird die Doppellieferung von bereits verarbeiteten Lieferungen (diese könnten auch unter einem anderen Dateinamen eingeliefert worden sein) ausgeschlossen. Diese Prüfung erfolgt auch für bereits abgewiesene Dateien. Nach der Abweisung einer Lieferung ist daher sowohl der Dateiname als auch der Dateinhalt (z.B. durch Einfügen eines Leerzeichens) zwingend zu verändern.	8011
10	Ist die BZSt-Nr im BZSt gesperrt oder stillgelegt worden?	Kontaktaufnahme mit dem Fachbereich im BZSt.	8009
11	Ist die AccountID im BZSt gesperrt oder stillgelegt worden?	Kontaktaufnahme mit dem Fachbereich im BZSt.	8009
12	Ist die verwendete AccountID im BZSt für die Dateiübertragung an das Fachverfahren freigeschaltet?	Eine Beschreibung für die Anmeldung zur ELMA5 Nutzung finden Sie im Kommunikationshandbuch Teil 1.	8007
13	Ist für die verwendete AccountID eine gültige fachverfahrensbezogene Freischaltung ELMA5 Freischaltung vorhanden?	Eine Beschreibung der fachverfahrensbezogenen Freischaltung finden Sie im Kommunikationshandbuch Teil 1.	8008
14	Alle ELMA5 Vorprüfungen wurden erfolgreich durchlaufen. Die Datei wurde zur fachlichen Prüfung an das Fachverfahren weitergeleitet.		8000

Tabelle 5: Abfolge der ELMA Prüfungen und deren Fehlercodes

Weitere Hinweise zu möglichen Fehlergründen:

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

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 Dateiinhalt in mehrere Einzeldateien aufteilen. Diese müssen jeweils das vollständige XML-Schema enthalten. Zu jeder Datei ist eine zugehörige Signaturdatei zu erstellen.

Tabelle 6: Weitere ELMA Fehlergründe


10 Abgrenzung zum XML-Upload über BOP

Neben der bisher beschriebenen Datenübermittlung über die SFTP-Verbindung gibt es in einzelnen Verfahren die Möglichkeit, eine XML-Datendatei über den Upload-Client im BZStOnline-Portal an das BZSt zu übertragen.

Um den Upload über das BOP nutzen zu können, sind die Kapitel 3.1 (Registrierung im BZStOnline-Portal), 3.2 (Freischaltung zur Teilnahme am ELMA-Verfahren), 6.1 (Namenskonventionen für die Datendatei), 6.3 (Namenskonvention für die Rückmeldedatei), 7.1 (Prüfung der XML-Datendatei) und 9 (ELMA-Eingangsprüfung) dieses KHBs und ggfs. verfahrensspezifische Besonderheiten für den XML-Upload zu beachten.

Eine kurze Benutzeranleitung über den eigentlichen Upload der Datendatei über das BOP finden Sie im BOP unter "Formulare & Leistungen"/"Versand von Massendaten (ELMA5)" nach Auswahl des betreffenden Fachverfahrens. Bitte beachten Sie, dass für den Upload von XML-Dateien die Einbindung des BOP-Zertifikats im Browser erforderlich ist.

Die Rückmeldungen zu einer über das BOP übertragenen Datei sind nicht im BOP-Postfach 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)"/"Abholung von ELMA5-Protokollen“.

	Kommunikationshandbuch Teil 3a - CRS: Datenübermittlung an das BZSt über die ELMA-Massendatenschnittstelle	Version:1.6 Stand: 17.06.2019
---	---	----------------------------------

11 Information der Verfahrensteilnehmer

11.1 Beeinträchtigung von Sicherheitsrelevanten Komponenten

Sollten sich für das vom BZSt eingesetzte ELMA-Verfahren Hinweise auf Schwachstellen im Protokoll, der Konfiguration oder einzelnen Komponenten ergeben, so werden diese nach Vorliegen eines Patches oder Workarounds unverzüglich behoben. Im Falle eines evidenten Sicherheitsproblems kann auch eine Verfahrensabschaltung bis zur Behebung der Schwachstelle in Betracht kommen. Alle ELMA-Verfahrensteilnehmer sind dem BZSt mit den vollständigen Kontaktdaten bekannt. Sie werden in einem solchen Fall umgehend per E-Mail über Art, Umfang und Schwere des vorliegenden Problems informiert.

Wegen der Vielzahl der clientseitig einsetzbaren Produkte obliegt es den Sendestellen in den einschlägigen Foren die Sicherheitshinweise zu der von ihnen eingesetzten Software auszuwerten und eventuell durch neue Versionen oder Updates die Betriebssicherheit zu gewährleisten.

12 Abkürzungsverzeichnis

Das Abkürzungsverzeichnis finden Sie im Kommunikationshandbuch – [Glossar und Abkürzungsverzeichnis](#)²⁶.

13 Glossar

Das Glossar finden Sie im Kommunikationshandbuch – [Glossar und Abkürzungsverzeichnis](#).

14 Referenzdokumente / Verweise

<u>Nr.</u>	<u>Titel</u>	<u>Ablageort / URL</u>
1	BZStOnlinePortal	www.elsteronline.de/bportal ²⁷

15 Anhänge

Nr.	Titel	Ablageort/URL
1	Kommunikationshandbuch Teile 0,1, 2, 3a, 3b, 4	Kommunikationshandbuch ²⁸

Tabelle 7: Anhänge

²⁶http://www.bzst.de/SharedDocs/Downloads/DE/CRS/crs_khb_Glossar_1_0.html;jsessionid=67119673D9CB630DE1BD290E360BCD08.live6831?nn=78976

²⁷ <https://www.elster.de/bportal/start>

²⁸ http://www.bzst.de/DE/Unternehmen/Intern_Informationsaustausch/CommonReportingStandard/Handbuecher/handbuecher_node.html;jsessionid=67119673D9CB630DE1BD290E360BCD08.live6831#js-toc-entry1