Dokumentation ELMA5-ZIVIT

Verfahren zur elektronischen Datenübertragung mit ELSTER Zertifikaten an das ZIVIT

Version:	**1.0**
Stand vom:	**21.12.2006**
Status:	**Entwurf – vorbehaltlich der Zustimmung des BSI**
Quelle:	**Programm-Dokumentation**
Copyright:	**© ZIVIT**

0 Copyright

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Im April 2006 stellte das Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT) erstmals ein Verfahren zur elektronischen Übertragung von Massendaten unter dem Namen mach5 vor. Hiermit wurde Großkunden die Möglichkeit zur Ablösung von Bandverfahren hin zu einem schnellen und kostengünstigen elektronischen Übertragungsverfahren ermöglicht. Nach der Startphase gingen von den Teilnehmern viele Wünsche und Vorschläge für den Ausbau des Verfahrens ein, die soweit möglich, sukzessive umgesetzt wurden. Eine wesentliche Neuerung ist dabei die Nutzung von Elster Software Zertifikaten, die ab dem ersten Quartal 2007 zur Verfügung steht. Diese evidente Produktfortschreibung soll auch im Verfahrensnamen reflektiert werden. Er wird daher ab dem 01.01.2007 von mach5 in ELMA5-ZIVIT geändert. Im weiteren Verlauf des Dokumentes wird aus Gründen der besseren Lesbarkeit die Kurzbezeichnung ELMA5 verwendet.

Mit ELMA5 können Daten zwischen beliebigen Endstellen und dem ZIVIT als Dienstleister für das Bundeszentralamt für Steuern (BZSt) übertragen werden.

2 Einführung

2.1 Zielgruppe, Voraussetzungen

Das Kommunikationsverfahren ELMA5 wurde für die Übertragung von Massendaten entwickelt. Es soll als Ersatz für die Versendung von Magnetbändern eingesetzt werden. Die Zielgruppe sind Großkunden, wie zum Beispiel Rechenzentren der Kreditwirtschaft.

Für die Übertragung von kleinen Datenbeständen stehen anderweitige etablierte Übertragungsmöglichkeiten zur Verfügung.

Für die Nutzung des ELMA5 Verfahrens ist eine Registrierung im BZSt-OnlinePortal (www.bzst.de) notwendig. Die Registrierung und Authentifizierung entspricht den aktuellen steuerlichen Vorschriften.

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 erhältlich. Ein flexibler Einsatz in unterschiedlichen Umgebungen ist somit gewährleistet. Im Standardfall kann eine Verbindung zum ZIVIT von einem Windows PC oder einer UNIX/Linux Maschine in wenigen Minuten hergestellt werden.

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

2.2 Quelle der Informationen

Dieses Dokument basiert auf den Vorschriften, die für steuerliche Verfahren beim ZIVIT und beim Bundeszentralamt für Steuern gelten. Darüber hinaus wurden Maßnahmen zur Sicherstellung von Datenschutz und IT Sicherheit entsprechend den Richtlinien der StDÜV und des BSI integriert.

2.3 Glossar

BSI	Bundesamt für Sicherheit in der Informationstechnik.
BZSt	Bundeszentralamt für Steuern.
BOP	BZSt Online-Portal
RSA	Authentifizierungsverfahren (Algorithmus von Rivest, Shamir und Adleman)
SFTP	SFTP ist die Abkürzung für "Secure File Transfer Program", einem interaktiven Dateitransferprogramm, mit dem der User vor dem eigentlichen Transfer Verzeichnisse und deren Inhalt auf dem Server einsehen und Kommandos auf dem Server ausführen kann.
SSH	SSH ist sowohl ein Programm als auch ein Netzwerkprotokoll, mit dessen Hilfe man Daten gesichert über das Internet zwischen Computer übertragen kann.
StDÜV	Steuerdatenübermittlungsverordnung.
ZIVIT	Zentrum für Informationsverarbeitung und Informationstechnik.

2.4 Ansprechpartner

Bei Fragen zum ELMA5 Verfahren wenden Sie sich bitte per Mail an:
onlineverfahren@steuerliches-info-center.de.

3 Beschreibung der ELMA5 Grundfunktionen

- Nutzung des Internets als Übertragungsmedium zwischen den sendenden Endstellen und den ZIVIT Server Systemen.
- Auslegung für Massendatenübertragung
- Nutzung von ELSTER Zertifikaten
- SSH Verschlüsselung mit zertifikatsbasierter Authentifizierung (RSA 1024 Bits / Protokoll Version 2 / Passphrase / 3DES für Entschlüsselung des privaten Schlüssels)
- Datensignatur
- Datenkompression (optional)
- Verwendung offener Standards
- Einfache Integration und Überwachung in Management-Systemen

3.1 Zulassung zum ELMA5 Übertragungsverfahren

ELMA5 ist für die Übertragung großer Datenmengen konzipiert. Es unterstützt diverse steuerliche Fachverfahren des BZSt. Die Registrierung der Teilnehmer für die einzelnen Fachverfahren erfolgt über das BZSt Online Portal (BOP). Hierbei erhält der Teilnehmer seine BZSt-Nummer. Entsprechende Hinweise zur Portal-Nutzung finden Sie auf der Internetseite des BZSt[1] unter den jeweiligen Fachverfahren.

Voraussetzung für die Freischaltung von ELMA5 und die Erteilung eines Zertifikates ist eine eingehende Prüfung durch den jeweiligen Fachbereich des BZSt. Der Teilnehmer muss sich für jedes Verfahren über das BOP explizit frei schalten, was eine separate Prüfung für das Fachverfahren bedingt.

Die bei der Registrierung im BOP vergebene BZSt-Nummer ist gleichzeitig die Senderkennung für den Zugang zum ELMA5 Kommunikationsserver und kann für alle auf den Teilnehmer zugelassenen Verfahren genutzt werden.

Im Anschluss kann die Übertragung mit den Zugangsdaten für das entsprechende Verfahren erfolgen.

[1] www.bzst.de

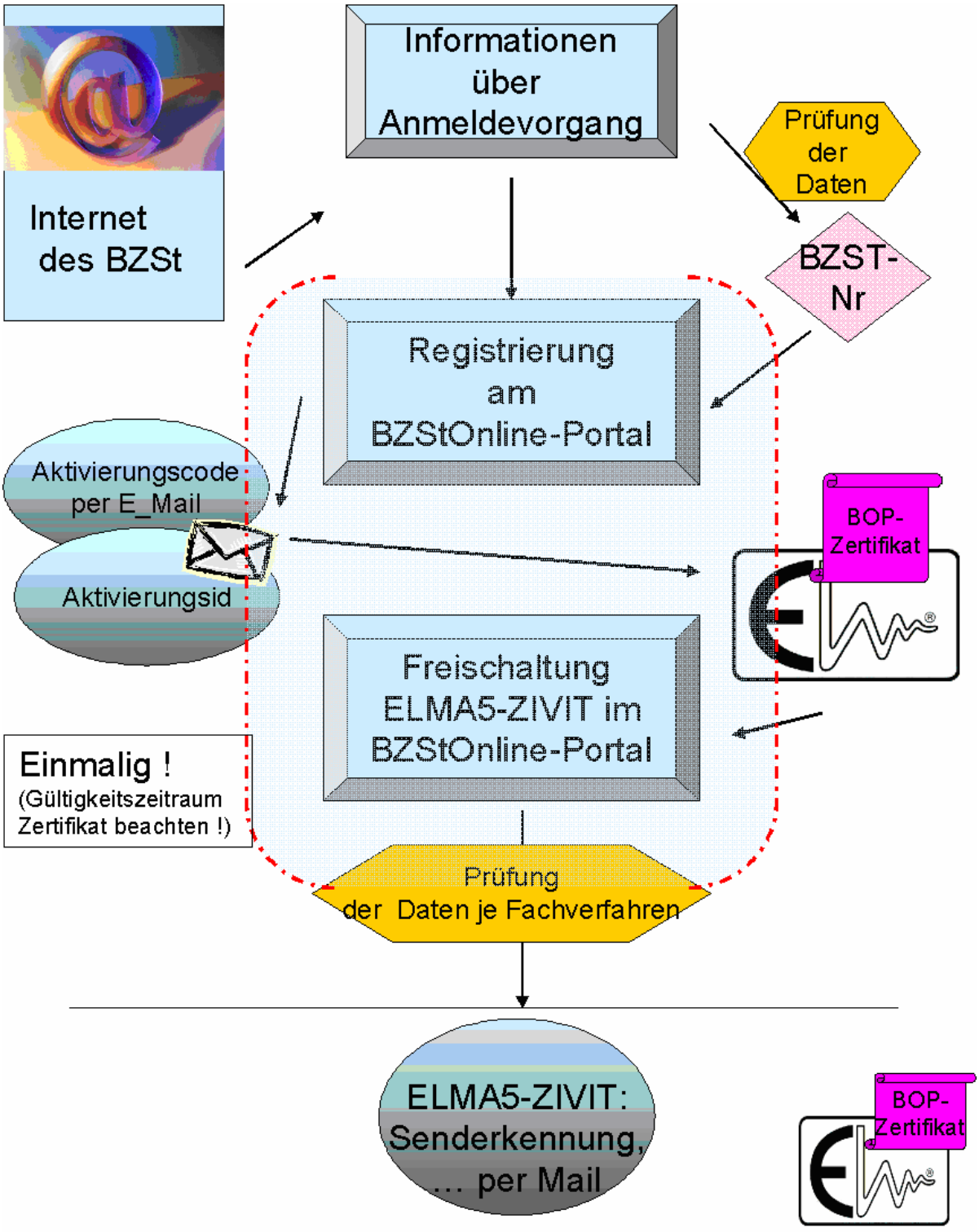

Abbildung 1: Schema Registrierung für das ELMA5-ZIVITVerfahren

3.2 Ablauf der Datenübertragung mit ELMA5

Der Benutzer erstellt mit seinen Backend-Systemen entsprechend der technischen Beschreibung des jeweiligen Fachverfahrens eine Datei mit den zu übertragenden Daten. Diese Datei ist vor der Übertragung mit dem privaten Schlüssel des Senders zu signieren. Dateien ohne Signatur werden im Rahmen der Signaturprüfung vom ELMA5-Kommunikationsserver für die Verarbeitung im jeweiligen Fachfachverfahren abgewiesen.

Der Benutzer meldet sich mit seiner BZSt-Nummer und seinem privaten Schlüssel unter Nutzung seiner Passphrase am ELMA5-Kommunikationsserver an. Nach erfolgreicher Anmeldung kann der Datentransfer automatisiert oder interaktiv (CLI oder GUI) erfolgen.

Die Daten werden zunächst im Eingangsverzeichnis des ELMA5-Kommunikationsservers abgelegt. Nach Abschluss des Datentransfers ist die Verbindung durch den Sender zu beenden.

Sämtliche Zugangs- und Datenübertragungsaktivitäten werden durch das ZIVIT protokolliert.

Die in das Verzeichnis `/upload` vom Sender eingestellten Daten werden formal geprüft. Dies beinhaltet die Validierung der Signatur, der Datenintegrität und die Zulassung für das jeweilige Fachverfahren. In. Abhängigkeit vom Fachverfahren sind weitergehende formale Prüfungen vor die Verarbeitung geschaltet. Nach einer erfolgreichen Eingangsprüfung werden die Daten an das betreffende Fachverfahren weitergeleitet. Für Daten, die diesen Kriterien nicht entsprechen, wird der Sender über den Grund der Ablehnung per Mail informiert. Danach werden die abgewiesenen Daten protokolliert und gelöscht. Die inhaltliche Datenprüfung erfolgt im nachfolgenden Fachverfahren. Der Sender erhält zum Zeitpunkt der Datenübergabe an das Fachverfahren und nach Einstellung der Protokolldatei eine Mail an seine bei der Registrierung angegebene technische Mailadresse. Nähere Details sind in den Dokumenten zu den entsprechenden Fachverfahren enthalten.

Die Protokolldateien werden dem Teilnehmer in seinem Abholverzeichnis `/download` zur Verfügung gestellt. Der Nutzer wird über das Vorliegen einer ihn betreffenden Information per Mail informiert.

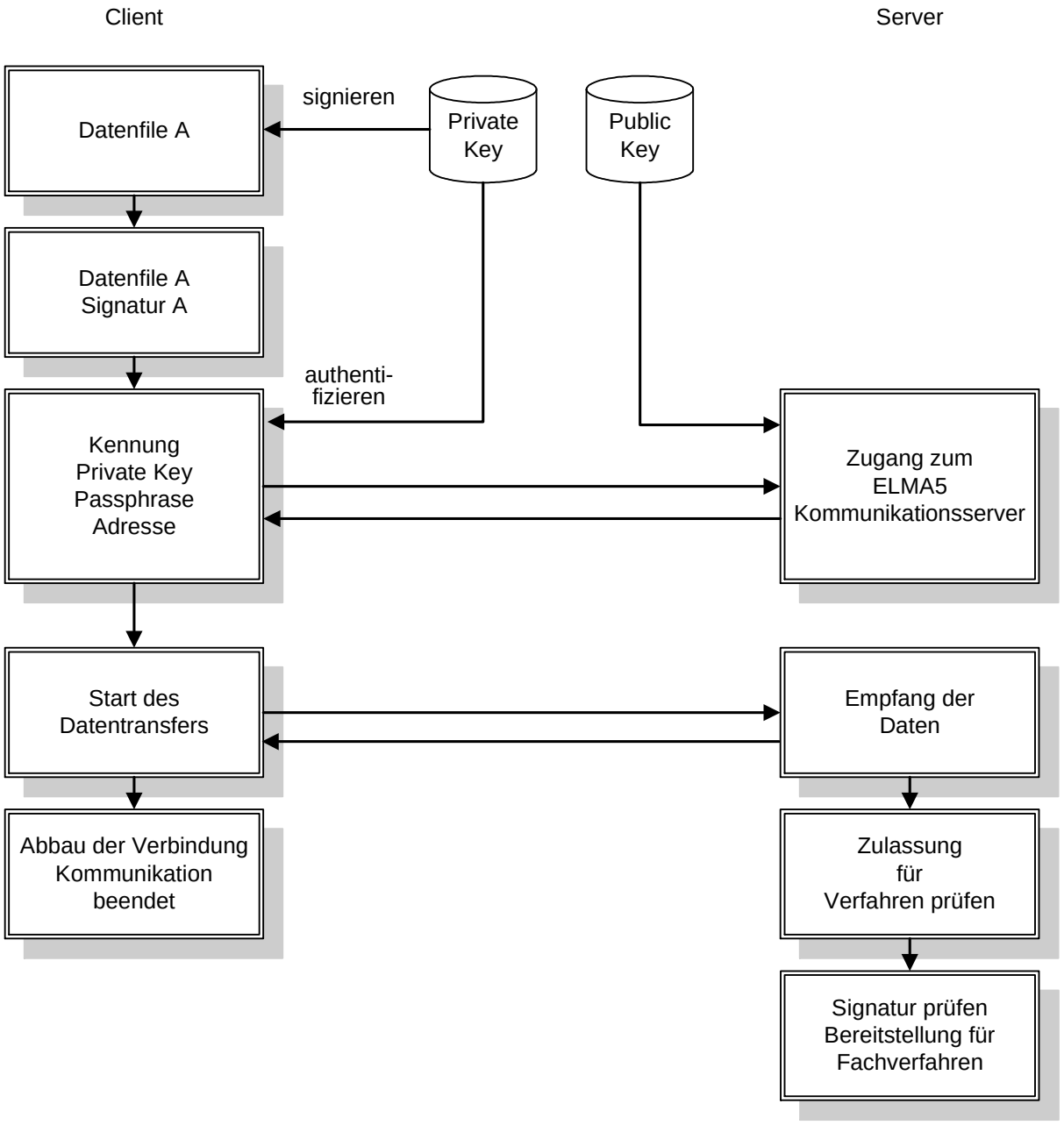

Abbildung 2: Schema Ablauf der Datenübertragung

4 Technische Voraussetzungen für die Nutzung der Kommunikationsschnittstelle

4.1 Systemvoraussetzungen für den Hardware-Einsatz

Die Systemvoraussetzungen für die Nutzung des ELMA5 Kommunikationsservers 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.

4.2 Systemvoraussetzungen für den Software-Einsatz

Für die Linux Betriebssystem Derivate (Suse, RedHat, Fedora, Debian) werden in der Regel die OpenSSH Module standardmäßig bei der Grundinstallation mit installiert. Die Nutzung der SSH Programme `sftp` und von `openssl` ist somit sofort nach der Grundkonfiguration möglich. Das gleiche gilt auch für die UNIX Derivate HP-UX, AIX und andere.

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

4.3 Internetanbindung und Bandbreite

Für die ELMA5 Kommunikation mit dem ZIVIT 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 clientseitig die Verwendung einer Datenkompression möglich. Der Kompressionslevel ist auf die Leistungsfähigkeit der Hardware abzustimmen.

4.4 Firewall Konfiguration

Bei der Verwendung einer Firewall ist beim Sender die Freischaltung der ZIVIT IP-Adresse und des Ports 22 zu konfigurieren.

4.5 Identifizierung, Verbindung

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

Der Austausch der RSA Public Keys erfolgt nach Überprüfung der Identität des Teilnehmers zwischen diesem und dem ZIVIT.

Die Verbindung besteht nur während der Datenübertragung und wird danach abgebaut.

Die RSA Zertifikate unterliegen den Richtlinien eines strukturierten Rechenzentrum Betriebes.

4.6 Verfügbarkeit - Failover

Der ELMA5-Kommunikationskomponente des ZIVIT ist redundant ausgelegt. Eine Hochverfügbarkeit wird jedoch nicht garantiert. Durch planmäßige Wartungsarbeiten[2] oder Betriebsstörungen kann es zu temporären Einschränkungen[3] 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.

4.7 Verfahrensaufnahme

Das ELMA5-Verfahren steht ab 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 Internetseite des BZSt.

[2] Planmäßige Wartungsarbeiten werden bekannt gegeben.

[3] Eine Ausfallzeit von max. 3 Stunden wird als verfahrensunkritisch betrachtet.

5 Technische Beschreibung der Kommunikation

5.1 Grundlagen

Als SSH (Secure Shell) werden Protokolle und eine Sammlung von Anwendungen bezeichnet, die SSH implementieren. OpenSSH wird vom OpenBSD Projekt gepflegt und weiterentwickelt[4]. Die Protokolle werden in den Internet- Drafts der IETF Working Group Secure Shell (secsh)[5] definiert.

Beginnend mit der Authentifizierung werden bei Verwendung von SFTP alle Daten bidirektional mit dem RSA Algorithmus kryptographisch verschlüsselt übertragen. Das Mitlesen von Passwörtern und Daten ist für unberechtigte Dritte nicht möglich.

ELMA5 verwendet Public Key Authentifizierung und Version 2 des SSH Protokolls.

Für die Übertragung ist nur sftp zugelassen.

5.2 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 Datei mit dem X.509 Zertifikat enthält zusätzlich den privaten Schlüssel. Dieser wird sowohl für die Signatur der zu übertragenden Dateien als auch für die Verschlüsselung bei der Datenübertragung verwendet. 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.

5.3 Username und Passwort Authentifikation

Die Anmeldung mit Username und Passwort ist am ELMA5-Kommunikationserver nicht möglich.

[4] http://www.openssh.org/

[5] http://www.ietf.org/html.charters/secsh-charter.html

5.4 Registrierungsdaten

Die Nutzung des Datenübertragungsverfahrens ELMA5 setzt eine Registrierung im BOP für ein steuerliches Fachverfahren voraus.

- Anmeldung für das jeweilige Fachverfahren.
- Freischaltung für dieses Fachverfahren nach Prüfung der dort geltenden Voraussetzungen. Per Mail erhält der dann Teilnehmer:
  - IP-Adresse des ELMA5 Kommunikationsservers.
- Das Elster-Zertifikat ist aus technischen Gründen für die Nutzung von ELMA5 durch den Teilnehmer zu konvertieren. Nähere Informationen erhalten Sie über den in der Freischaltungsmail enthaltenen Link.

5.5 Signatur der zu übertragenden Dateien

Jede Datei **muss** vor der Übertragung vom Versender mit seinem privaten Schlüssel signiert werden. Eine vorhandene Signatur wird vom ZIVIT nach Erhalt der Datei überprüft. Sendedateien ohne korrespondierende Signaturdatei werden nicht zur Verarbeitung zugelassen.

5.6 Datenübertragung unter Linux / UNIX

5.6.1 Prüfung der Registrierungsdaten und Einrichtung der Übertragungsumgebung

Für die Datenübertragung per sftp ist kein dedizierter Account notwendig. Es empfiehlt sich aber einen eigenen Account für die Datenübertragung und einen entsprechenden User Space für die zu übertragenden Daten einzurichten.

```
adduser[6] <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
```

5.6.2 Erstellung der Signaturdatei

Auf Linux Systemen kann für die Erstellung der Signaturdatei das OpenSSL[7] Command Line Tool verwendet werden.

```
openssl dgst –md5 –binary –out <Dateiname-mit-Suffix>.sig \[8]
            –sign ~/.ssh/elster.pem <Dateiname-mit-Suffix>

Enter pass phrase for key: <Passphrase>
```

5.6.3 Datenübertragung per `sftp`

Die Optionen und Parameter zur Verwendung des sftp Programms sind vielfältig. Eine ausführliche Beschreibung kann auf Linux Systemen mit dem Befehl `man sftp` angezeigt werden. Der gesamte Übertragungsvorgang kann in einer Batchdatei festgelegt und automatisiert ausgeführt werden.

---

[6] Hierfür sind Rootrechte notwendig.

[7] http://www.openssl.org

[8] Der Backslash ist optional und dient hier nur der besseren Lesbarkeit.

5.7 Datenübertragung unter Windows

Im Folgenden werden die wichtigsten Voraussetzungen, Konfigurationen und Kommandos zur Bedienung der PuTTY Suite[9] dokumentiert. PuTTY ist eine Windowsportierung der OpenSSH Programme. Weiterhin wird das Open Source Programm `winscp3.exe` vorgestellt, das es jedem Windowsnutzer ermöglicht, SCP/SFTP über eine komfortable graphische Oberfläche zu bedienen. WinSCP bedient sich teilweise der PuTTY Programme. Diese werden standardmäßig unter `C:\Programme\WinSCP3\PuTTY` installiert.

5.7.1 Konvertierung des OpenSSH Private Key mit PuTTY

Der OpenSSH Private Key ist vor der Windows Nutzung in einen PuTTY Key zu konvertieren.

```
puttygen elster.pem -o elster.ppk
```

Abbildung 3: PuTTY Programmgruppe

Aus der PuTTY Programmgruppe den Key Generator `puttygen` auswählen.

[9] http://www.chiark.greenend.org.uk/~sgtatham/putty/

Abbildung 4: PuTTY Key Generator: Laden des Private Key

Nach dem Drücken der „Load“ Taste ist der Pfad und der Dateiname für `elster.pem` auszuwählen. Die Verwendung wird durch Eingabe der Passphrase frei geschaltet.

Abbildung 5: PuTTYgen: Eingabe der Passphrase

Abbildung 6: PuTTYgen Notice

Abbildung 7: PuTTY Key Generator: Speichern des konvertierten Private Key

Der konvertierte Private Key ist mit “Save private key” unter `elster.ppk` im Dateisystem zu sichern.

5.7.2 Erstellung der Signaturdatei

Für den Einsatz unter Microsoft Windows steht eine OpenSSL Implementierung[10] zur Verfügung. OpenSSL kann nach dem Download des Tools aus der Command Line Shell gestartet werden. Je nach Installationspfad und gesetzter PATH Variable muss der Programmaufruf ggf. mit einem voran gestellten absoluten Pfadnamen erfolgen. Für den privaten Schlüssel sind entsprechende Sicherheitsvorkehrungen gegen den unbefugten Zugriff durchzuführen. Es empfiehlt sich, die Zugriffsrechte auf den privaten Schlüssel Anwender bezogen zu setzen.

```
openssl dgst –md5 –binary –out <Dateiname-mit-Suffix>.sig
            –sign elster.pem <Dateiname-mit-Suffix>

Enter pass phrase for key: <Passphrase>
```

5.7.3 Datenübertragung per `psftp`

[10] http://www.ca.uni-tuebingen.de/anleit/opensslbin.zip

Der Ablauf der zu übertragenden Dateien kann z. B. durch die Datei `batchdatei.bat` gesteuert werden.

Beispiel für `batchdatei.bat`:

```
put *
get upload/*
rm upload/*
exit
```

Die Datenübertragung der Dateien kann z.B. mit folgendem CLI Befehl erfolgen.

```
psftp –b batchdatei -i elster.ppk  <BZSt-Nummer>@<IP-Adresse>
```

5.7.4 Datenübertragung mit dem Programm `WinSCP`

Mit dem Programm WinSCP kann der Datentransfer Skript gesteuert oder interaktiv durchgeführt werden. Der Datentransfers ist komfortabel per Drag and Drop über das Windows GUI möglich. Für die Darstellung kann zwischen Norton Commander und Windows Explorer gewählt werden. Das Programm wird standardmäßig Im Verzeichnis `C:\Programme\WinSCP3` installiert.

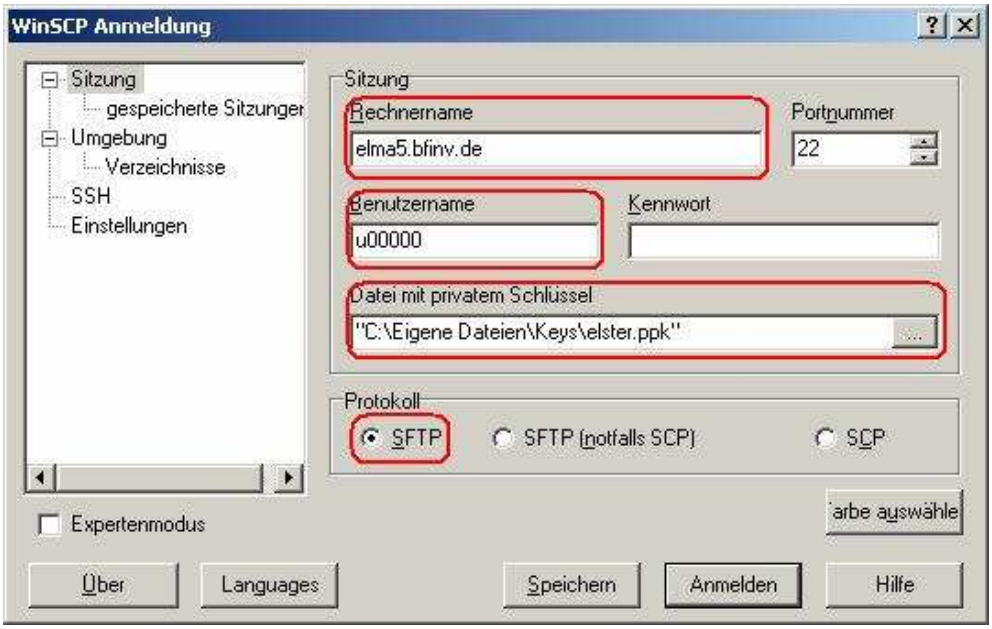

Abbildung 8: WinSCP Anmeldung – Sitzung

Der Rechnername, die Benutzerkennung (BZSt-Nummer) und der Pfad zur privaten Schlüsseldatei sind im Anmeldungsdialog zu setzen. Als Protokoll wird nur SFTP unterstützt.

Abbildung 9: WinSCP Anmeldung - Verzeichnisse

Das Upload Verzeichnis oder auch ein lokales Verzeichnis kann auf Wunsch permanent vor eingestellt werden.

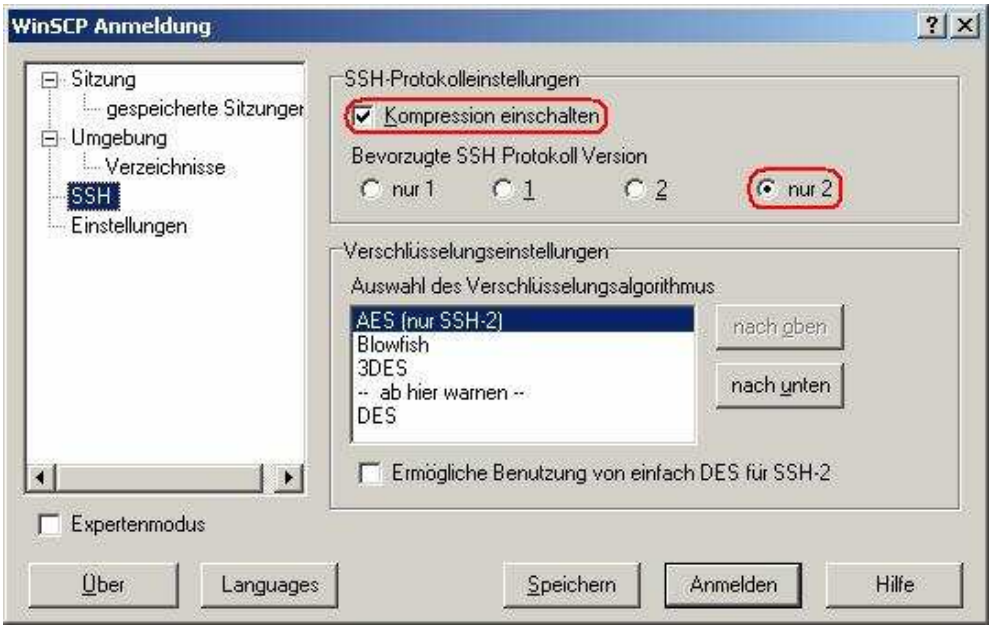

Abbildung 10: WinSCP Anmeldung - SSH

Es wird nur das SSH Protokoll Version 2 unterstützt. Die Kompression kann optional für die Übertragung großer Datenvolumen eingeschaltet werden.

Abbildung 11: WinSCP Anmeldung - Einstellungen

Die Benutzerschnittstelle ist vom Erscheinungsbild konfigurierbar. Eine einfache, übersichtliche und schnelle Dateiauswahl kann durch Voreinstellung der Norton Commander Ansicht erreicht werden. Hier wird im linken Fenster das Filesystem des lokalen Rechners und auf der rechten Seite das Filesystem des ELMA5-Kommunikationsservers abgebildet. Durch einfaches Drag und Drop lassen sich die zu übertragenden Files transferieren.

Bei Auswahl der Windows Explorer Benutzerschnittstelle als Voreinstellung werden die Files des Zielsystems in einem Fenster angezeigt. Der Komfort und die Interagilität sind dabei eingeschränkt.

Abbildung 12: WinSCP Authentifizierungsbanner

Die Datenschutzerklärung wird während der Anmeldung angezeigt.

Abbildung 13: WinSCP: Eingabe der Passphrase

Nach der Eingabe der Passphrase können Sie die Dateien per Drag and Drop transferieren.

Das Programm bietet sehr viele Optionen, bis hin zum automatischen Abgleich von Verzeichnissen bei Änderung. Feste Profile können gespeichert und als Icon vom Desktop gestartet werden, so dass lediglich noch die Passphrase eingegeben werden muss.

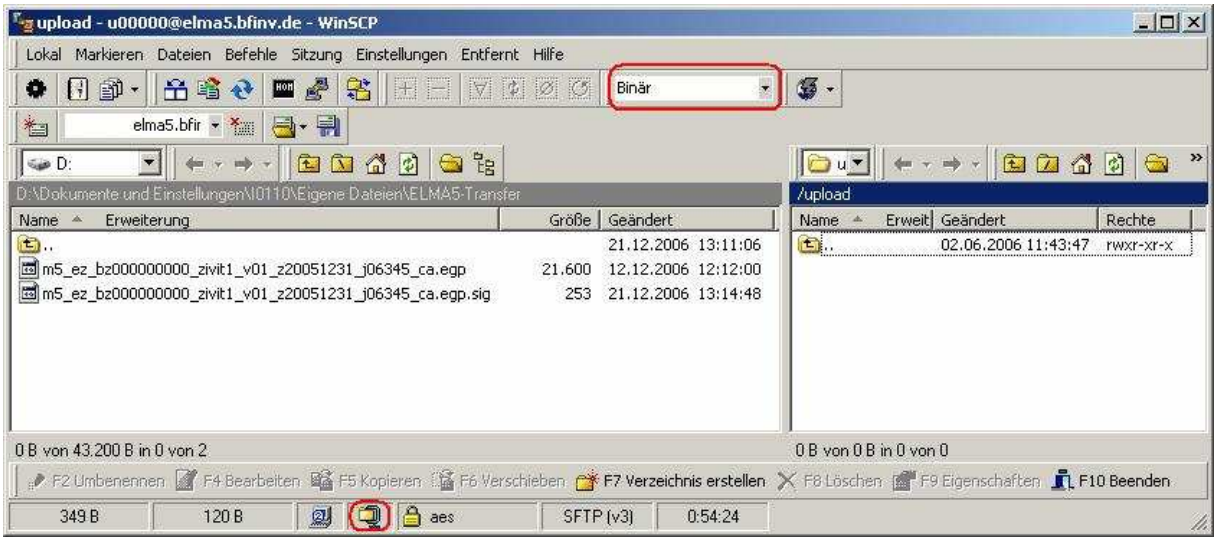

Abbildung 14: WinSCP Ansicht - Norton Commander

Abbildung 15: WinSCP Ansicht – Windows Explorer

6 Namenskonventionen

6.1 Namenskonvention für die Sendedatei

m5_<pb>_<sssssssssss>_<ppp><xxx>_v<xx>_z<yyyymmdd>_<s><yyddd>_<c><x>.<f><v><l>

- ELMA5-ZIVIT-Dateikennung

- Produktbezeichnung <pb>
  2-stellig, alphanumerisch, wird jeweils vom Fachverfahren vorgegeben

- BZSt-Nummer <sssssssssss>
  11-stellig, alphanumerisch, wird bei der Anmeldung im BOP vergeben.
  Die beiden führenden Buchstaben (bz oder bx) sind in Kleinschreibung zu verwenden!

- Übertragungsprozess-ID <ppp>
  3-stellig, alphanumerisch, wird vom Sender frei vergeben
  (z. B. Backend 1 = b01, Backend 2 = b02)

- Lieferanten-ID <xxx>
  3-stellig, alphanumerisch, wird vom Sender frei vergeben
  (z. B. ext. Lieferant A=l01, int. Lieferant B=l02)

- Datensatz Version v<xx>
  2-stellig, numerisch
  (Vorgabe v01)

- Ende Sammelzeitraum z<yyyymmdd>
  (z. B. 20051231)

- Gewünschte Verarbeitungssequenz <s><yyddd>
  Verarbeitungssequenz + julianischer Kalender
  d = tägliche Verarbeitung
  w = wöchentliche Verarbeitung
  m = monatliche Verarbeitung
  q = quartalsweise Verarbeitung
  h = halbjährliche Verarbeitung
  j = jährliche Verarbeitung

- Codepage <c>
  a = keine Angabe
  b = IBM-273
  c = IBM-850

e = EBCDIC 273 oder EBCDIC 1141

Bei Verwendung der EBCDIC Codepage darf nur der unten dargestellte reduzierte Zeichensatz verwendet werden.

	-0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-A	-B	-C	-D	-E	-F
0-																
1-																
2-																
3-																
4-	sp										Ä	.		(	+	
5-	&										Ü			)	;	
6-	-	/									ö	,		_		
7-											:					
8-		a	b	c	d	e	f	g	h	i						
9-		j	k	l	m	n	o	p	q	r						
A-		ß	s	t	u	v	w	x	y	z						
B-																
C-	ä	A	B	C	D	E	F	G	H	I						
D-	ü	J	K	L	M	N	O	P	Q	R						
E-	Ö		S	T	U	V	W	X	Y	Z						
F-	0	1	2	3	4	5	6	7	8	9						
	-0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-A	-B	-C	-D	-E	-F

- Verarbeitungsart <x>
  a – k = Reihenfolge der tägliche Datenversorgung, beginnend mit „a“
  l = Datenversorgung „Fusionsbestand“
  m – z = Datenversorgung für weitere Sonderläufe (noch nicht definiert)

- „.“ Trennung Präfix.Suffix

- Funktionstyp <f>
  e = Einzeldatei-Übertragung
  m = Sammel-Übertragung

- Verarbeitungstyp <v>
  g = Gesamtbestand (Gesamtversorgung)
  i = Increment (Deltaversorgung)
  f = Fusion Alt-/Neudatei (Fusionsvorgang)
  a = Alt-/Neu-/Änderungsdatei (Restrukturierung)
  m = Migration (z. B. Wechsel operatives System)
  b = Begleitschein

- Verarbeitungslauf <l>
  v = Vorlauf
  t = Testlauf
  p = Produktionslauf
  k = Korrekturlauf

n = Nachlauf

6.2 Namenskonvention für die Signaturdatei

m5_<pb>_<sssssssssss>_<ppp><xxx>_v<xx>_z<yyyymmdd>_<s><yyddd>_<c><x>.<f><v><l>**.sig**

Zu jeder Sendedatei gehört eine Signaturdatei. Der Name der Sendedatei wird um den Suffix `.sig` erweitert.

6.3 Namenskonvention für die Rücksendedatei

m5_<pb>_<sssssssssss>_<ppp><xxx>_v<xx>_z<yyyymmdd>_<s><yyddd>_<c><x>.<f><v><l>

- ELMA5-ZIVIT-Dateikennung
- Produktbezeichnung <pb>
  2-stellig, alphanumerisch, wird jeweils vom Fachverfahren vorgegeben
- Rückmelder BZSt-Nummer <sssssssssss>
  11-stellig, alphanumerisch, wird bei der Anmeldung im BOP vergeben
- Rückmelder Übertragungsprozess-ID <ppp>
  3-stellig, alphanumerisch
  (z. B. Backend 1 = b01, Backend 2 = b02)
- Rückmelder Lieferanten-ID <xxx>
  3-stellig, alphanumerisch,
  (z. B. ext. Lieferant A=l01, int. Lieferant B=l02)
- Datensatz Version v<xx>
  2-stellig, numerisch
  (Vorgabe v01)
- Rückmelder Ende Sammelzeitraum z<yyyymmdd>
  (z. B. 20051231)
- Gewünschte Verarbeitungssequenz <s><yyddd>
  Verarbeitungssequenz + julianischer Kalender
  d = tägliche Verarbeitung
  w = wöchentliche Verarbeitung
  m = monatliche Verarbeitung

q = quartalsweise Verarbeitung
h = halbjährliche Verarbeitung
j = jährliche Verarbeitung

- Codepage
  a = keine Angabe
  b = IBM-273
  c = IBM-850
  e = EBCDIC 273 oder EBCDIC 1141

  Bei Verwendung der EBCDIC Codepage darf nur der unter 6.1 dargestellte reduzierte Zeichensatz verwendet werden.
- Verarbeitungsart <x>
  a – k = Reihenfolge der täglichen Datenversorgung, beginnend mit „A“
  l = Datenversorgung „Fusionsbestand“
  m – z = Datenversorgung für weitere Sonderläufe (noch nicht definiert)
- „.“ Trennung Präfix.Suffix
- Funktionstyp <f>
  e = Einzeldatei-Übertragung
  m = Sammel-Übertragung
- Verarbeitungstyp <v>
  r = Rückmeldung ZIVIT
- Verarbeitungslauf <l>
  v = Vorlauf
  t = Testlauf
  p = Produktionslauf
  k = Korrekturlauf
  n = Nachlauf

6.4 Erläuterungen zu den Namenskonventionen

Gewünschte Verarbeitungssequenz <s><yyddd> – Verarbeitungssequenz + julianischer Kalender:

- Kennbuchstabe für die Verarbeitungssequenz <s>.
- Verarbeitung Jahreszahl, 2-stellig, numerisch, aufsteigend, ab 04 <yy>.
- julianischer Kalendertag, 3-stellig, numerisch <ddd>.

- Vorgabe des gewünschten Verarbeitungstages, kann gleich oder größer dem Datum der Aufbereitung nach der Tagesendverarbeitung durch den Lieferanten sein.
- Anmerkungen:
  An Samstagen, Sonntagen und bundeseinheitlichen Feiertagen werden normalerweise keine Dateien durch die Lieferanten an den RZ-Betreiber gesendet bzw. verarbeitet, da hierfür bisher an diesen Tagen keine fachliche Notwendigkeit besteht.
  D.h., diese Daten werden ggf. am 1. Werktag / Woche – oder später - inkl. der Änderungen des (der) Tage(s) in einer Datei gespeichert und als eine Datei versendet.

6.5 Rückmeldungen / Protokolldateien

Rückmeldungen erfolgen (wenn das Fachverfahren solche verwendet) auf elektronischem Wege. Die Dateinamen basieren auf den Dateinamen der Meldung und werden im `/upload` Verzeichnis des Kommunikationsservers zur Verfügung gestellt. Der Empfänger wird über das Vorliegen einer Rückantwort per Mail informiert. Es obliegt ihm, die Rückmeldung auf sein System zu laden und zu verarbeiten.

7 Information der Verfahrensteilnehmer

7.1 Beeinträchtigung von Sicherheitsrelevanten Komponenten

Sollten sich für das vom BZSt eingesetzte ELMA5-ZIVIT-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 zu Behebung der Schwachstelle in Betracht kommen. Alle ELMA5-Verfahrensteilnehmer sind dem BZSt mit den vollständigen Kontaktdaten bekannt. Sie werden in einem solchen Fall umgehend per 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.

7.2 Beeinträchtigung durch Wartungsarbeiten oder Betriebsstörungen

Die Verfahrensteilnehmer werden über geplante Wartungsarbeiten mit Einschränkung der Erreichbarkeit des ELMA5-Kommunikationsservers per Mail informiert, sofern die Ausfallzeit voraussichtlich länger als 3 Stunden dauert.

Bei Betriebsstörungen, für die eine Ausfallzeit von mehr als 3 Stunden absehbar ist, wird ebenfalls eine entsprechende Information der Verfahrensteilnehmer durchgeführt, sofern die operativen Systeme eine Information per Mail zulassen.