Inhaltsverzeichnis

1 Allgemeines

Dieses Dokument zeigt auf, wie die EDV-Kommunikation zwischen der Eidgenössischen Zollverwaltung (EZV) und den am NCTS angeschlossenen Zollbeteiligten funktioniert.

Die Kommunikation basiert auf folgenden Standards:

UN/EDIFACT	United Nations Electronic Data Interchange for Administration, Commerce and Transport.
SMTP	Übermittlung der Meldungen via Internet

Übermittlung per Internet

1.1 Grundsätze

Übermittlungen via Internet sind hinsichtlich Datensicherheit und Datenschutz kritischer als solche mit X.400. Diesem Aspekt wurde durch folgende Maßnahmen Rechnung getragen:

- Die Übermittlungen **müssen** zumindest elektronisch **signiert** werden. Durch Verifizierung der elektronischen Signatur kann der Empfänger kontrollieren, ob die Meldung tatsächlich vom angegebenen Absender abgeschickt und unterwegs nicht verändert wurde.

- Auch mit einer Signatur wäre es jedoch mit einem gewissen Aufwand (d. h. entsprechendem Know-how und Zugriff auf Kommunikationsknoten) möglich, Daten während der Übermittlung abzufangen und dessen Inhalt auszuwerten. Falls der Zollbeteiligte es als notwendig erachtet, können darum zusätzlich zur Signatur die übermittelten Deklarationsdaten verschlüsselt werden.

- Jeder Zollbeteiligte muss eine Kontaktperson bezeichnen, die für die Kommunikation per Internet verantwortlich ist.

Die EZV kann die Einhaltung von Datenschutz und Datensicherheit nur für Tätigkeiten, Netzwerke, Hard- und Softwarekomponenten in ihrem Einflussbereich garantieren. Sie übernimmt keine Haftung für die Folgen von Datenmissbräuchen während der Datenübermittlung vom EDV-System des Zollbeteiligten zu demjenigen der Zollverwaltung und zurück.

1.2 Elektronische Signatur / Verschlüsselung

Es wird das sog. asymmetrische Signatur- resp. Verschlüsselungsverfahren mit S/MIME angewandt. In diesem Verfahren wird mit einem Schlüsselpaar gearbeitet.

Der Geheimschlüssel (Private Key) ist ein Unikat, d. h. es braucht nur ein Exemplar beim rechtmässigen Besitzer. Dieser Private Key wird zur Erzeugung einer elektronischen Signatur und zur Entschlüsselung von verschlüsselten Daten verwendet. **Er muss unbedingt geschützt (geheim gehalten) werden.**

Das Gegenstück zu diesem Geheimschlüssel ist der öffentliche Schlüssel (Public Key). Dieser Schlüssel ist im Prinzip jedermann zugänglich und dient zur Überprüfung der Echtheit einer elektronischen Signatur oder zur Verschlüsselung von Daten.

Das beschriebene Schlüsselpaar wird durch vertrauenswürdige Instanzen erzeugt (Zertifizierungsstelle = CA/Certification Authority). Für die Anwendung NCTS ist dies die Eidgenössische Zollverwaltung.

Das Schlüsselpaar wird per Email im PKCS#12-Format der für die Kommunikation verantwortlichen Kontaktperson des Zollbeteiligten zugestellt. Die dabei übermittelte Datei enthält neben dem persönlichen privaten und öffentlichen Schlüssel auch den öffentlichen (self signed) OZD CA-Schlüssel.

Die PKCS#12-Datei selbst ist durch ein Passwort geschützt. Das Passwort für den Zugriff wird dem Zollbeteiligten mit eingeschriebenem Brief zugestellt, damit sichergestellt werden kann, dass nur berechtige Anwender in den Besitz der Schlüssel gelangen.

Im NCTS wird pro Email-Adresse des Zollbeteiligten ein separates Schlüsselpaar (Zertifikat) erstellt. Dieses ist jedoch nur für eine beschränkte Zeit gültig (im NCTS mindestens ein Jahr, aber maximal zwei Jahre). 30 Tage vor Ablauf der Gültigkeitsfrist wird vom Zollcomputer automatisch ein neues Zertifikat (Folgezertifikat) erstellt und entweder der verantwortlichen Kontaktperson beim Zollbeteiligten (per signiertem E-Mail) oder analog der Deklarationsrückmeldungen direkt dem entsprechenden Produktionssystem zugestellt (wobei die Unterscheidung zwischen Deklarationsrückmeldung und Folgezertifikat aufgrund der «Content-Description» gemacht werden kann: beim Folgezertifikat lautet diese «NEW NCTS CERTIFICATES»).

Das Folgezertifikat kann nach der Installation sofort angewendet werden. Im Zollsystem wird nach dem Eingang der ersten Deklaration, die mit dem neuen Zertifikat verarbeitet wurde, das bisherige Zertifikat durch das Folgezertifikat ersetzt. Zwar können bis zum Ablauf des ersetzten Zertifikates eingehende Deklarationen, die noch mit diesem Zertifikat signiert / verschlüsselt wurden, verarbeitet werden; die Rückmeldungen werden aber mit dem neuen Zertifikat signiert / verschlüsselt. Andererseits ist es auch möglich, dass für eine kurze Zeit beim EDV-System des Zollbeteiligten Deklarationsrückmeldungen eingehen, die mit unterschiedlichen Zertifikaten signiert / verschlüsselt wurden, d. h. es werden je nach Rückmeldungen verschiedene Zertifikate für die Prüfung der Signatur bzw. der für die Entschlüsselung der Daten benötigt. Dieses Problem kann beim Zollbeteiligten mit einer Historisierung der Zertifikate gelöst werden. Eine andere Möglichkeit wäre, das Folgezertifikat erst zu aktivieren, wenn die Rückmeldungen aller mit dem alten Zertifikat verarbeiteten Deklarationen wieder beim EDV-System eingetroffen sind.

1.2.1 Technische Beschreibung «Signatur»

Verarbeitet und verschickt werden S/MIME-signierte Meldungen:

Envelope MIME-Attribute	MIME-Version: 1.0 Content-Type: multipart/signed; protocol= "application/x-pkcs7-signature"; micalg=sha1
Attachment MIME-Attribute (Deklaration, Rückmeldung)	Content-Type: application/octet-stream Content-Transfer-Encoding: base64
Attachment MIME-Attribute (Signatur)	Content-Type: application/x-pkcs7-signature; Name= "smime.p7s" Content-Transfer-Encoding: base64 Content-Disposition: attachment; filename="smime.p7s“

Jede signierte Meldung muss das Zertifikat des Absenders enthalten (multipart/signed und application/x-pkcs-signature MIME-Format).

1.2.2 Verschlüsselung

Technische Beschreibung für signierte und verschlüsselte Übermittlungen

Envelope MIME-Attribute	MIME-Version: 1.0 Content-Type: application/x-pkcs7-mime; name="smime.p7m" Content-Disposition: attachment; filename="smime.p7m" Content-Transfer-Encoding: base64

Schlüsselaustausch für verschlüsselte Meldungen

Für die Verschlüsselung wird der öffentliche Schlüssel des Kommunikationspartners benötigt. Bei der erstmaligen Vergabe der Schlüssel ist die Direktion EZV als Aussteller der Schlüssel bereits im Besitz des entsprechenden öffentlichen Schlüssels der Zollbeteiligten.

Der öffentliche Schlüssel der Direktion EZV wird als Zertifikat in einem signierten E-Mail an den Systemverantwortlichen des Zollbeteiligten übermittelt. Sofern dieser das Direktion EZV CA-Zertifikat installiert hat (aus der vorgängig verschickten PKCS#12-Datei), kann er die Korrektheit dieses Zertifikates überprüfen und es danach für die Verschlüsselung von Deklarationsmeldungen einsetzen.

1.3 Standards

Eingesetzte Software (auf Seiten der Zollverwaltung)	OpenSSL
Mailformat	MIME 1.0
Secure Mailformat	S/MIME 2
Zertifikatsformat	X509v3
Zertifikatsaustausch	PKCS#12
Meldungssyntax	PKCS#7

1.4 E-Mail-Adressen Zollcomputer

- Testsystem:
  - transit@nctstest.ezv.admin.ch
  - autoanswer.transit@nctstest.ezv.admin.ch
- Produktionssystem
  - transit@ncts.ezv.admin.ch
  - autoanswer.transit@ncts.ezv.admin.ch

1.5 Fehlerbehandlung von signierten oder verschlüsselten Deklarationen

Ist eine Deklaration vom Sicherheitsstandpunkt korrekt, wird sie der Anwendung NCTS zur weiteren Behandlung übergeben. Kann eine Meldung hingegen nicht entschlüsselt oder verifiziert werden, wird mit einer Delivery Status Notification DSN geantwortet.

Mögliche Fehlermeldungen	Ursache
Decoding failed (5.7.5)	falsches Zertifikat für die Verschlüsselung verwendet
Verification failed (5.7.7)	Ursache: Meldung falsch signiert
Wrong edi content (5.5.0)	Message-Inhalt beginnt nicht mit der EDI-Initialisierungssequenz
Smpt_mime_xxx: not allowed / supported for … (5.5.0)	verwendete Sicherheitsstufe (signiert/signiert und verschlüsselt) stimmt nicht mit Konfiguration überein
Illegal padding inside the string (5.5.0)	höchstwahrscheinlich falsche MIME base64 Encoding
Illegal character found in input (5.5.0)	höchstwahrscheinlich falsche MIME base64 Encoding

1.6 Testszenarien für SW-Hersteller

Bevor ein SW-Hersteller mit dem Test-System der Direktion EZV testet, sollte er vorgängig im Selbsttest prüfen, ob er eine an sich selbst adressierte signierte / verschlüsselte Meldung erfolgreich versendet und anschliessend erfolgreich entschlüsselt werden kann.

Für die Tests können bei der Direktion EZV Testzertifikate verlangt werden, welche 5 Jahre gültig sind.

2 Implementierung

2.1 Allgemeines

Diese Lösung kann für eine ganze Applikation oder Teile davon benutzt werden:

- Transit und Ausfuhr (NCTS): Deklarationen und Rückmeldungen
- Transit (NCTS): VD und Suchverfahren

Es ist also möglich, verschiedene E-Mail-Adressen für die Kommunikation mit dem EZV-System zu benutzen.

2.2 Einschränkungen

Die Deklarationen und Rückmeldungen in NCTS müssen mindestens signiert sein (ähnlich wie Ein- und Ausfuhr). Siehe auch Punkt 4.1.

Das Versenden des VBD oder den Stammdateien bleibt vorläufig ohne Zertifikat und Verschlüsselung. Es ist aber möglich die gleiche Adresse, wie Deklarationen und Rückmeldungen für NCTS, zu benutzen.

3 Antragsformulare

3.1 Antragsformular für Test-/Produktionsbetrieb

Das Antragsformular befindet sich unter:

http://www.ezv.admin.ch/zollanmeldung/05042/05048/index.html?lang=de

Darin muss der Zollbeteiligte unter anderem Angaben machen über:

- Spediteur- und Deklarantendaten
- VBD: Angabe der E-Mail-Adresse
- Allgemeine Angaben
- Etc.

Das Antragsformular enthält zudem Bestimmungen für den NCTS-Betrieb.

3.2 Antrag für Deklarations-Übermittlungen via Internet

Dieses Formular befindet sich auf der Internet-Seite der EZV, an folgender Adresse:

http://www.ezv.admin.ch/zollanmeldung/05042/05048/index.html?lang=de

3.2.1 Allgemeines

Vermerken Sie zuerst, ob die nachfolgenden Angaben für:

- Den Produktionsbetrieb
- Den Testbetrieb
- Oder für beides

verwendet werden sollen.

3.2.2 Punkt 1.1

Angaben zur Person und Firma, welche für die Internet-Konfiguration des Kunden verantwortlich ist.

3.2.3 Punkt 1.2

Angaben zum Kunden (Zollpartner).

Wichtig ist anzugeben, wohin die Folgezertifikate übermittelt werden sollen.

3.2.4 Punkt 1.3

Hier muss der Zollpartner unter Angabe des Spediteurs vermerken, für welche Verkehrsart (Einfuhr, Ausfuhr, Transit) die Angaben verwendet werden sollen. Er kann dabei eine oder mehrere Verkehrsarten angeben.

Arbeitet ein Zollpartner mit mehreren Spediteurnummer aber nur einer E-Mail-Adresse, kann er im Antrag gleichzeitig mehrere Spediteurnummern angeben.