Ablaufbeschreibung und Nutzungsbedingungen für die Online-Schnittstelle des ITSG-Trust Centers (OSTC) ab Schnittstellen-Version 2.5

Stand der Spezifikation: Juli 2024

Version: 1.8

Herausgeber: ITSG GmbH

Redaktion: Informationstechnische Servicestelle der gesetzlichen Krankenversicherungen GmbH
Kaiserleistraße 10-16
63067 Offenbach

Inhaltsverzeichnis

Dokumentenreferenz

Nr.	Name des Dokumentes	Version	Datum
1	Datensatz- und Schemabeschreibung der OSTC über eXTra	2.2	2024
2	GI4X eXTra Profil	1.0.2	2010
3	Anlage 16 Security Schnittstelle für das Gesundheitswesen		2021
5	Anlage 8 Hypertext Transfer Protocol (http / https)		2016

1 Einleitung

1.1 Grundlagen

Dieses Dokument beschreibt die grundlegenden Anforderungen der OSTC Version 2.5.

Es werden die vier Phasen beim Datenaustausch mit der Online-Schnittstelle des ITSG-Trust Centers für die Online-Abwicklung von Zertifizierungsanträgen und Abruf von elektronischen Schlüssel sowie Schlüssellisten beschrieben.

1.2 Überblick

Zu beachten sind folgende Punkte in der OSTC-Version 2.5:

- Bei einem Erstantrag muss zuerst ein Antrag in der ITSG-Registrierungsstelle gestartet werden und es wird dazu eine eindeutige GUID-Nummer vergeben. Mit der GUID-Nummer führt der Antragsteller die weiteren Antragsschritte in der Kundensoftware mit OSTC-Unterstützung zur Schlüsselgenerierung aus und übermittelt die Antragsdaten mit dem Requestschlüssel und Hashcode über die OSTC. Für den Hashcode ist nur SHA256 zulässig.
- Bei einem Erstantrag werden nur die wesentlichen Antragsdaten zur Schlüsselgenerierung über die OSTC übermittelt. Alle weiteren Antragsdaten werden über die ITSG-Registrierungsstelle erfasst, ein schriftlicher Zertifizierungsantrag wird nicht mehr angefordert. Nur bei einem Online-Folgeantrag werden alle Antragsdaten über die OSTC übermittelt. Das bedeutet, dass in der Kundensoftware mit OSTC-Unterstützung jeweils für die Antragsvariante Erstantrag oder Online-Folgeantrag eine unterschiedliche Datenmenge erfasst wird, und es wird kein Zertifizierungsantrag mehr ausgedruckt.
- Bei einem Online-Folgeantrag ist eine erneute Authentifizierung über die ITSG-Registrierungsstelle nicht erforderlich, wenn der Ansprechpartner im Zertifikat unverändert bleibt. Für Teilnehmer, die eine Eigenerklärung als Meldestelle abgegeben haben und bei Anträgen von Datenannahmestellen, oder mit einer Test-Betriebsnummer ist die Antragsvariante Online-Folgeantrag nicht zulässig. In diesen Fällen ist eine erneute Authentifizierung über die ITSG-Registrierungsstelle ist bei jedem Antrag erforderlich.
- Im xml-Schema für die Antragsdaten sind die Elemente Erstantrag und Folgeantrag eingeführt worden. Es wird hierdurch immer die Art von dem zu übermittelten Antrag festgelegt. Der Erstantrag und Folgeantrag unterscheiden sich in den zu übermittelten Elementen. Durch die Aufteilung im xml-Schema in Erstantrag und Folgeantrag wurden zu den vorhandenen Simple types auch Complex types hinzugefügt.
- Das xml-Schema für die Übermittlung der eXTra-Nachricht mit den Antragsdaten ist auf die Zeichensätze I1 und U8 eingeschränkt. Der Zeichensatz wurde auf UTF-8 geändert, wobei es Einschränkungen der zulässigen Zeichen bei einzelnen Elementen gibt.
- Eine GUID-Nummer wird vom ITSG-Registrierungsportal vergeben und ermöglicht bei Erstantrag eine eindeutige Zusammenführung der Antragsdaten über die Kundensoftware und über das ITSG-Registrierungsportal. Das Element „GUID“ ist nur beim Erstantrag vorhanden.
- Bei der optionalen Rechnungsadresse gibt es Pflicht-Elemente mit zugeordneten Fehlercodes, dabei ist das Element Re_Email nur Bestandteil des Folgeantrages.

1.3 Weitere Spezifikationen und Standards

Folgende Spezifikationen oder Dokumente sind im Zusammenhang mit dieser Beschreibung zu beachten:

1. **Datensatz- und Schemabeschreibung der OSTC:**
   In diesem neuen Dokument werden die Datensätze und xml-Schemata für die OSTC-Version 2.5 detailliert mit allen Return- und Fehlercodes beschrieben.

2. **GI4X eXTra Profil:**
   Diese Spezifikation beschreibt zum eXTra-Standard die Profilierungs-Vorgaben in der GKV und ist für den xml-Datenaustausch zu beachten.

3. **Anlage 16 Security Schnittstelle für den Datenaustausch im Gesundheits- und Sozialwesen ab 2021.** In dem Dokument sind die notwendigen Mechanismen mit den kryptografischen Algorithmen niedergeschrieben.

4. **Anlage 8 Hypertext Transfer Protocol (http / https):**
   In dieser Spezifikation werden die Transportprotokolle http und https beschrieben.

1.4 Organisation

ITSG GmbH - Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GmbH

Kaiserleistraße 10-16
63067 Offenbach
Telefon: 069/8700358-0
E-Mail: tc-produktmanagement@itsg.de

2 Schnittstellen und Transport

2.1 Überblick

In der OSTC-Version 2.5 erfolgt der Datenaustausch gemäß dem GI4X eXTra-Standard der GKV. Dieser beschreibt eine einheitliche Transportschicht für xml-Dokumente. Zudem stellt eXTra bereits die Möglichkeiten der neuen Auftragsbestätigung des Antragstellers zur Verfügung.

Die Antragsdaten werden weiterhin in einer xml-Nutzdatendatei gespeichert, um bei Folgeanträgen eine Signatur mit dem bestehenden Zertifikat des Antragstellers auf File-Ebene zu ermöglichen. Die erzeugte xml-Nutzdatendatei wird dann als eXTra-Nachricht per https übermittelt. Die technischen Details sind in den folgenden Punkten und den zugeordneten xml-Schemata zu entnehmen.

Als wichtige Empfehlung soll bei Bedarf der Antragsstatus über eine Programmsicherung der Client-Software vor der abschließenden Auftragsbestätigung des Antragstellers nach folgenden Ablaufschritten erzeugt werden:

- Eine Beantragung wird durch den Antragsteller ausgelöst. Dabei muss der Antragsteller auf einen kostenpflichtigen Auftrag und auf die AGB's der ITSG im Client hingewiesen werden.
- Der Antragsteller erfasst die Antragsdaten im Client und generiert das Schlüsselpaar.
- Die Antragsdaten werden vom Client aufbereitet. Bei einem Folgeantrag werden die Antragsdaten signiert und verschlüsselt. Der Antrag wird an die OSTC übermittelt.
- Die Rückantwort der OSTC mit einer Auftragsnummer und einem Returncode sowie evtl. einem Fehlercode wird vom Client verarbeitet.

2.2 eXTra-Schnittstelle

Der Datenaustausch zwischen Client und OSTC erfolgt über die eXTra Schnittstelle des ITSG-Trust Centers. Die verwendeten xml-Schemata basieren auf dem GI4X eXTra-Standard. Die detaillierte Beschreibung der xml-Schemata ist den Dokumenten „Datensatz- und Schemabeschreibung der OSTC“ und „Schnittstellenspezifikation_OSTC“ zu entnehmen.

2.2.1 Modellierung der eXTra-Nachrichten

Es wird nur die Transport-Ebene angewendet, eine zusätzliche Package-Ebene ist wegen einer Einzelbeantragung von Zertifikaten nicht erforderlich.

Für die eXTra-Nachrichten sind die Kommunikationsszenarien “request-with-response” und “request-with-acknowledgement” vorgesehen.

Für das Encoding der Daten in den eXTra-Nachrichten ist der Zeichensatz UTF-8 zu verwenden, nur für die xml-Datei mit den Antragsdaten muss das Encoding auf encoding=" UTF-8 " gesetzt werden.

In den eXTra-Nachrichten werden in den beiden Pflicht-Elementen „Sender/SenderID“ und „Receiver/ReceiverID“ jeweils die Betriebsnummer, Zahlstellenummer oder das IK des Antragstellers und der OSTC angegeben.

Für eine eindeutige Zuordnung der eXTra-Nachrichten wird in den Elementen „RequestDetails/RequestID“ und „ResponseDetails/ResponseID“ eine eindeutige Nachrichten-ID vergeben, bestehend aus der Sender-ID bzw. Receiver-ID mit Zeitstempel. Als Ausnahme wird nur im fehlerfreien Fall bei den Responses 1b und 2b die Auftragsnummer als eindeutige Nachrichten-ID direkt in der Nachricht vergeben, ansonsten im Fehlerfall die Receiver-ID mit Zeitstempel.

Gemäß KKS und den Schemata wird für die Übermittlung der eXTra-Nachrichten eine base64 kodierte xml-Nutzdatendatei erzeugt und in das eXTra-Element „TransportBody/Data“ kopiert. Für die Qualitätssicherung sollen die kodierten Antragsdaten wieder dekodiert werden. Dabei müssen die Daten identisch sein, um eine Abweichung speziell bei den Umlauten zu vermeiden.

Zusätzlich wird bei einem Folgeantrag die xml-Nutzdatendatei „Antragsdaten“ signiert und verschlüsselt. Zur Modellierung der verschlüsselten xml-Datei wird zusätzlich das optionale Element „TransportPlugins“ mit den Unterelementen verwendet.

2.2.2 Zugeordnete eXTra-Nachrichten

Für die komplette Antragsabwicklung sind folgende eXTra-Nachrichten zu verwenden:

1a) Request-Antrag (enthält „Antragsdaten“ mit p10-Requestdatei, bei Erstantrag nur p10-Requestdatei)
1b) Acknowledge-Antrag (enthält OSTC-Eingangs-Nr., Returncode sowie Fehlercode)

2a) Request-Auftrag (enthält Daten zur Auftragsbestätigung vom Antragsteller)
2b) Acknowledge-Auftrag (enthält Auftragsbestätigung von der OSTC)

3a) Request-Schlüsselanfragen (enthält Daten zur Abholung eines Zertifikats)
3b) Response-Schlüsselanfragen (enthält p7c-Zertifikatsdatei)

4a) Request-Listeanfragen (enthält Daten zur Abholung einer Schlüsselliste)
4b) Response-Listeanfragen (enthält Annahmeliste)

2.2.3 Zugeordnete URL’s

Die einzelnen eXTra-Nachrichten werden über den Webserver unter den folgenden URL’s ausgetauscht:

https://www.itsg-trust.de/ostcv25/antrag.php

Über diese URL werden die eXTra-Nachtichten (1a und 1b) zur Abwicklung der Online-Beantragung mit den Antragsdaten ausgetauscht.

https://www.itsg-trust.de/ostcv25/auftrag.php

Über diese URL werden die eXTra-Nachtichten (2a und 2b) zur Abwicklung der Auftragsbestätigung ausgetauscht.

https://www.itsg-trust.de/ostcv25/schluessel.php

Über diese URL werden die eXTra-Nachtichten (3a und 3b) zur Abholung eines Zertifikats ausgetauscht.

https://www.itsg-trust.de/ostcv25/liste.php

Über diese URL werden die eXTra-Nachtichten (4a und 4b) zur Abholung einer Schlüsselliste ausgetauscht.

2.3 https-Kommunikation

2.3.1 Überblick

Das OSTC-System basiert auf einem Webserver-Dienst, welcher auf Port 443 Anfragen per „POST- Methode“ unter dedizierten URL’s erwartet.

Der Datenaustausch einer Beantragung und die Abholung eines Zertifikats sowie einer Schlüsselliste erfolgt in vier getrennten https-Sessions. Es wird ein signiertes SSL-Zertifikat einer Root CA (z. B. Verisign oder andere) verwendet. Bei der Kommunikationsverbindung handelt es sich um eine einseitige https-Verbindung.

Erste https-Session:
Die Beantragung wird durch den Client initiiert und die Antragsdaten werden an die OSTC übermittelt. Der Client wartet dann auf die Rückantwort der OSTC. Die Daten werden direkt vom OSTC-System geprüft und das Ergebnis wird in Abhängigkeit der Datenqualität mit einer Auftragsnummer, einem Returncode oder eventuell mit einem Fehlercode an den Client zurückgemeldet. Für die weitere Bearbeitung wartet die OSTC auf die abschließende Auftragsbestätigung des Clients in der zweiten Session.

Zweite https-Session:
Nachdem als Empfehlung eine Programmsicherung vom Antragsstatus erzeugt wurde, übermittelt der Client eine abschließende Auftragsbestätigung an die OSTC und beendet somit die Beantragung.

Dritte https-Session:
Nach der Auftragsbestätigung und der erfolgreichen Eingangsprüfung wird der Antrag automatisch bearbeitet und das zugeordnete Zertifikat veröffentlicht. Die p7c-Responsedatei wird zur Abholung per eXTra-Nachtichten über die OSTC bereitgestellt.

Vierte https-Session:
Die Listen mit den öffentlichen Schlüsseln der Annahmestellen werden zur Abholung per eXTra-Nachtichten über die OSTC bereitgestellt.

2.3.2 Kommunikation

Die Kommunikation zwischen Client und OSTC basiert auf einem POST-Request ohne die Angabe von Namen-Wert-Paaren und ohne die Angabe von http-Argumenten in der URL.

Der https-Request und die https-Response müssen als Binary-Request ausgeführt werden, wobei der Request-Header lediglich die Attribute "Content-Type" und "Content-Length" enthalten muss. Der Request-Body enthält ausschließlich die zu übermittelnden Daten.

Für Fehler in der https-Kommunikation wird auf https-Protokoll gemäß RFC 2818 verwiesen.

HTTP Digest Access Authentication:
Die Anmeldung an der OSTC erfolgt gemäß RFC 2617 HTTP Authentication

Inhalt des Request-Headers:
Content-Type: application/octet-stream
Content-Length: <Größe des https-body in Bytes)

Inhalt des Request-Bodys:
Der Inhalt des Request-Bodys ist das eXTra-Datenpaket.

3 Ablauf der Nachrichtenübermittlungen

In diesem Kapitel wird jeweils die Eingangsseite des Clients und der OSTC schematisch beschrieben.

Der Client des Antragstellers muss sich an der Schnittstelle mit den Zugangsdaten authentifizieren. Für die OSTC-Version 2.0 werden Zugangsdaten und eine Registration-ID dem Programmhersteller der Kommunikationssoftware nach einem Freigabetest ausgegeben.

Die Zugangsdaten der OSTC-Version 1.0 sind aufgrund der Inkompatibilität nicht zulässig. Der Antragsteller hat von dem Authentifizierungsvorgang keine unmittelbare Kenntnis.

3.1 Kommunikationsverlauf einer Beantragung

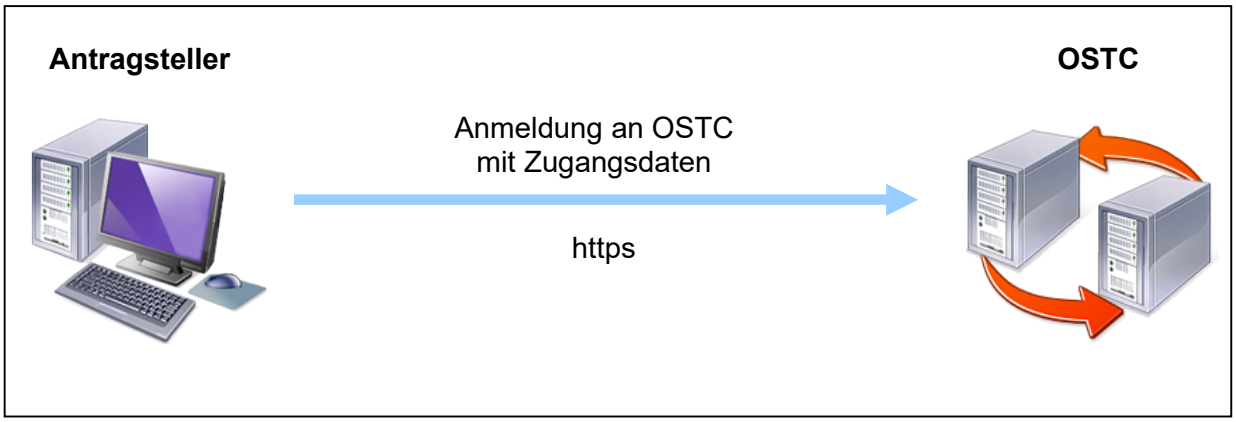
Zur Online-Beantragung eines Zertifikats muss der Antragsteller auf einen kostenpflichtigen Auftrag und auf die AGB's der ITSG im Client hingewiesen werden.

Erst mit der Zustimmung des Antragstellers wird die Beantragung über die Client-Software initiiert. Bei einem Erstantrag werden zunächst die Antragsdaten erfasst. Bei einem Folgeantrag werden die Antragsdaten aus dem Erstantrag übernommen, aber der Antragsteller soll mit einem Hinweis prüfen, ob die Adresse noch gültig ist.

3.1.1 Ablauf in der ersten https-Session

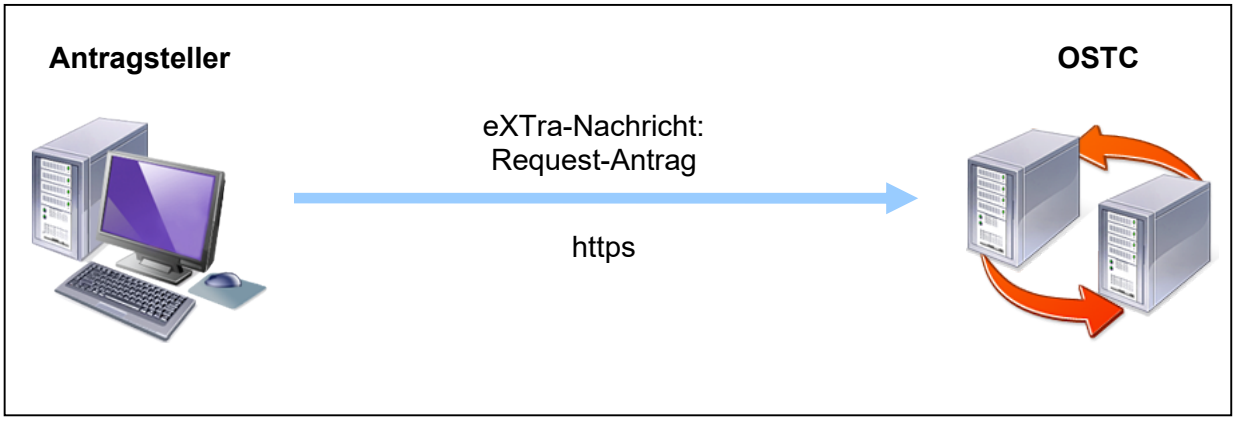
Der Client des Antragstellers muss sich an der Schnittstelle mit den Zugangsdaten authentifizieren. Für die OSTC-Version ab 2.0 werden Zugangsdaten und eine Registration-ID der zugelassenen Software dem Programmhersteller der Client-Software nach einem Freigabetest ausgegeben.

Schritt 1 – Anmeldung an der Schnittstelle:



Wenn die Zugangsdaten nicht verifiziert werden können, ist eine Anmeldung an der OSTC nicht möglich. Wurden die Zugangsdaten erfolgreich verifiziert, wird die verschlüsselte Verbindung aufgebaut.

Schritt 2 – Übermittlung der Antragsdaten an die OSTC:



Die Antragsdaten mit den base64-kodierten Daten des p10-Requestschlüssels werden in der xml-Nutzdatendatei „Antragsdaten“ gespeichert. Bei Erstantrag wird nur die p10-Requestdatei in der xml-Nutzdatendatei gespeichert. Das Datenformat der xml-Nutzdatendatei Antragsdaten“ wird gemäß xml-Schema in dem zugeordneten Dokument „Datensatz- und Schemabeschreibung der OSTC“ beschrieben.

Zur Legitimation bei Folgeanträgen werden die „Antragsdaten“ vom Antragsteller signiert und auch verschlüsselt. Dieser Vorgang wird von der jeweiligen Client-Software gemäß dem bestehenden Verfahren im Datenaustausch in der GKV durchgeführt. Somit ist eine einheitliche und erprobte Abwicklung gewährleistet. Details zu den Verfahren sind in den Dokumenten „Security Schnittstelle für das Gesundheitswesen“ und „Hinweise zur Security Schnittstelle für das Gesundheitswesen“ beschrieben. Die zu verwendende öffentliche Schlüssel der OSTC für die Verschlüsselung der Antragsdaten“ bei Folgeanträgen sind in den Annahmelisten enthalten.

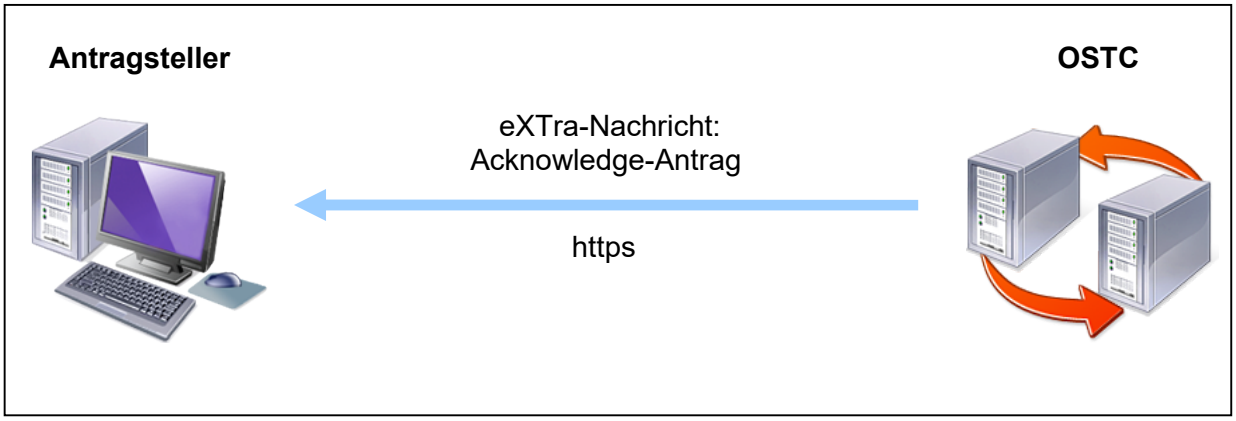
Das Trust Center verwendet für die OSTC die folgende IK- bzw. Betriebsnummer:

Verfahren	BN / IK	Kassenart	Name
Arbeitgeber	BN 17046976	ITSG	ITSG GmbH Trust Center
Leistungserbringer	IK 660640162	ITSG	ITSG GmbH Trust Center

Bei Folgeanträgen muss das optionale Element „TransportPlugins“ verwendet werden, da die „Antragsdaten“ signiert und verschlüsselt sind. Die fertigen „Antragsdaten“ werden für die Übermittlung base64 kodiert und dann im Data-Element des Transportbodies eingebunden.

Für die Art der Kommunikation wird das Szenario “request-with-acknowledgement” verwendet, da von der OSTC eine Auftragsnummer und keine Nutzdaten erwartet werden.

Schritt 3 – Übermittlung der Rückantwort der OSTC:



Jeder Online-Folgeantrag, der durch die OSTC erfolgreich angenommen wird, erhält von der OSTC ein „Acknowledgement“ mit den entsprechenden Return- oder Fehlercodes, diese sind in dem Dokument „Datensatz- und Schemabeschreibung der OSTC“ beschrieben. Bei Erstantrag erfolgt kein Acknowledgement für die übermittelte p10-Requestdatei. Die Rückantwort wird innerhalb der https-Session an den Client geliefert.

Daten der OSTC-Rückantwort
Jeder erfolgreich geprüfte Antrag wird mit einer Eingangsnummer belegt. Somit enthalten die xml-Elemente der Rückantwort die folgenden Inhalte:

- OSTC-Version (default)
- Returncode (immer!)
- Fehlercode (nur bei Fehler)
- Eingangsnummer (bei erfolgreich geprüftem Antrag)

Bei einem Fehler aus der Prüfung wird im Element „Report“ die Rückantwort „Error“ erstellt. Der Returncode und mögliche Fehlercodes aus der Überprüfung der Antragsdaten werden von der OSTC im Element „ResponseDetails/Code“ zurückgemeldet. Zusätzlich wird der Status im Element „Text“ mit OK oder Fehler signalisiert. Eine Fehlertextausgabe erfolgt nicht und ist bei Bedarf im Client umzusetzen.

Die Eingangsnummer wird bei erfolgreich geprüften Daten für den Antrag im Element „Response-ID“ übermittelt.

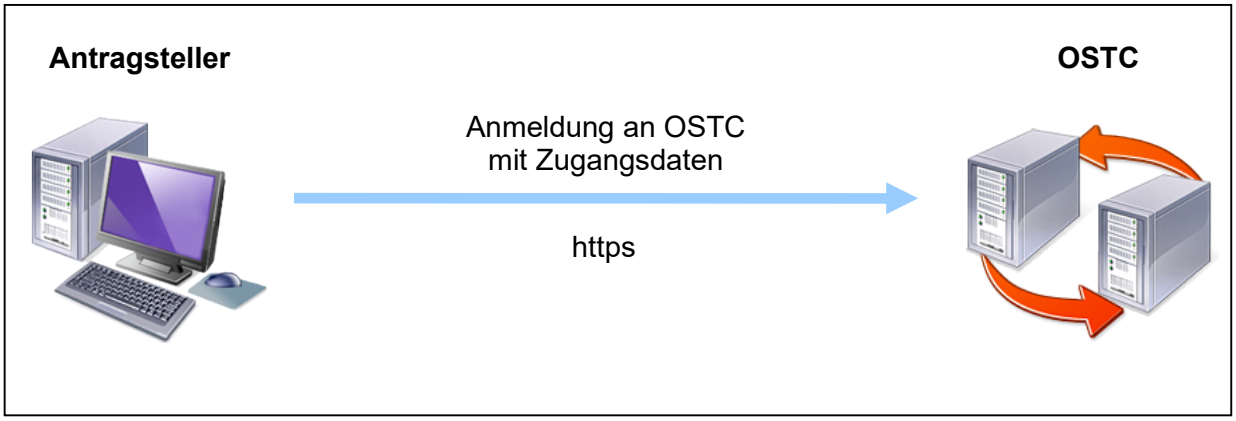
3.1.2 Ablauf in der zweiten https-Session

Der Antragsteller muss den kostenpflichtigen Auftrag bei der ITSG explizit bestätigen, dazu übermittelt der Client nach einer erneuten Anmeldung die Auftragsbestätigung des Antragstellers.

Nach den Verarbeitungsschritten des Clients erfolgt zeitversetzt die Auftragsbestätigung des Antragsstellers.

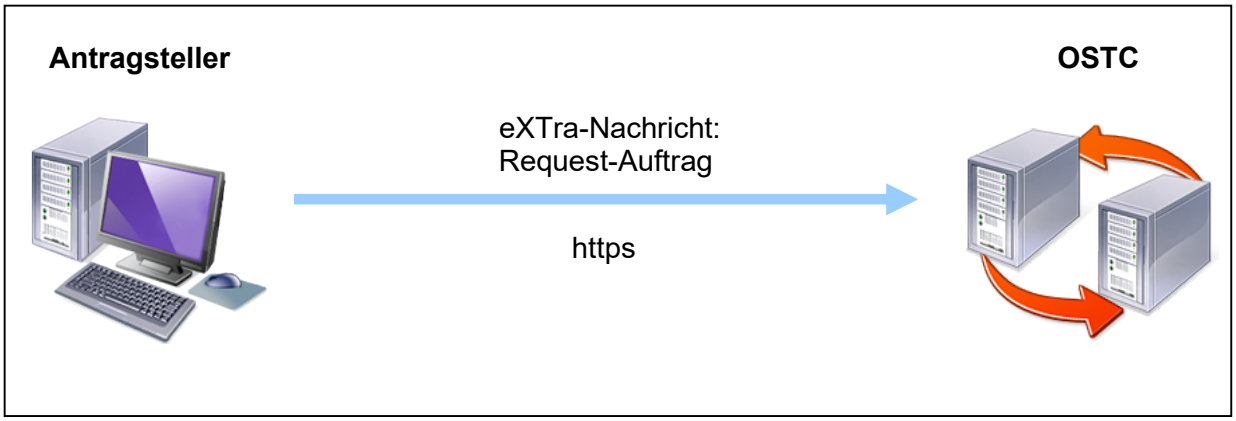
Eine empfohlene Sicherung nach der erfolgreichen Beantragung mit einer Auftragsnummer soll es den Antragsteller z. B. nach einem Systemabsturz ermöglichen, den Antragsstatus mit dem privaten Schlüssel wiederherstellen zu können, um somit eine weitere kostenpflichtige Beantragung zu vermeiden.

In dieser neuen Session muss sich der Client wieder an der Schnittstelle anmelden.
Schritt 1 – Anmeldung an der Schnittstelle:



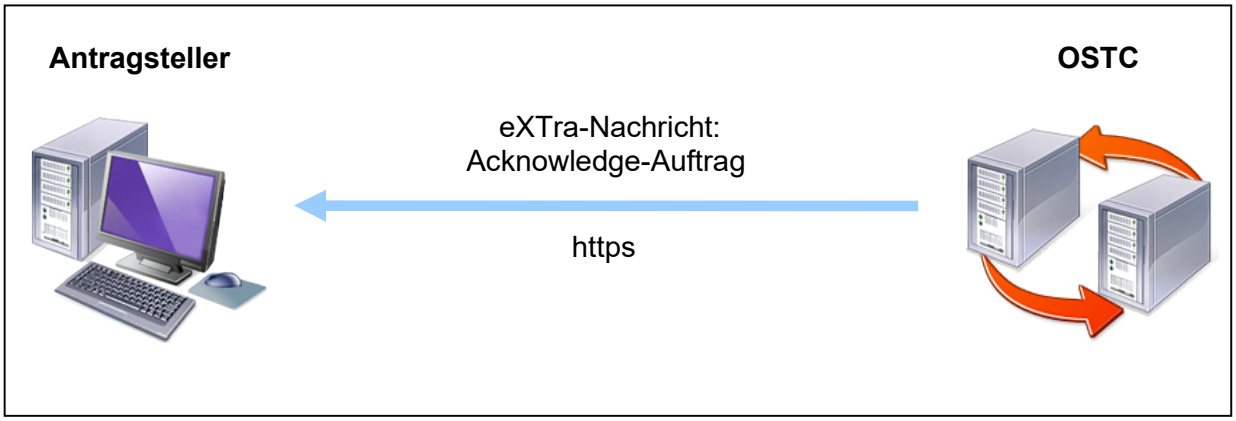
Die Verifizierung der Zugangsdaten ist mit dem Ablauf in der ersten https-Session identisch.

Schritt 2 – Übermittlung der Auftragsbestätigung des Antragstellers:



Der Client übermittelt nach der erneuten Anmeldung die Auftragsbestätigung des Antragstellers. Hierzu werden die xml-Nutzdaten mit den Auftragsdaten base64 kodiert und dann im Data-Element des Transportbodies eingebunden. Für die Art der Kommunikation wird hier das Szenario “request-with-acknowledgement” verwendet, da von der OSTC nur eine Empfangsbestätigung und keine Nutzdaten erwartet werden.

Schritt 3 – Übermittlung der OSTC-Bestätigung:



Abschließend sendet die OSTC ein „Acknowledgement“ als Empfangsbestätigung.
Nach dem das OSTC-System die Auftragsbestätigung des Antragstellers verarbeitet hat, erfolgt die weitere Bearbeitung des Antrags und die Erstellung des Zertifikats im Trust Center.

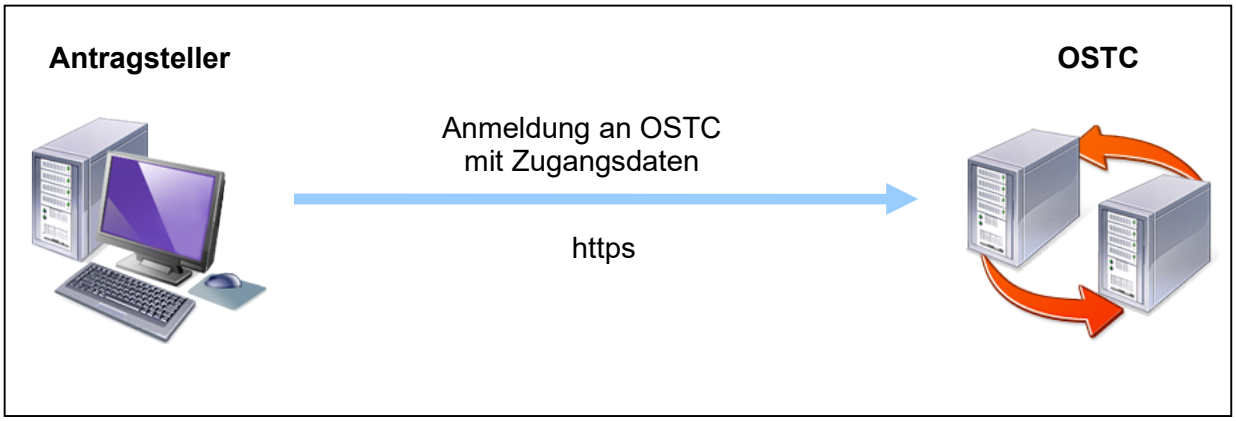
3.2 Bereitstellung der Zertifikate und Schlüssellisten

3.2.1 Ablauf in der dritten https-Session

Nach dem das OSTC-System die Auftragsbestätigung des Antragstellers verarbeitet hat, erfolgt die weitere Bearbeitung des Antrags und die Erstellung des Zertifikats im Trust Center.

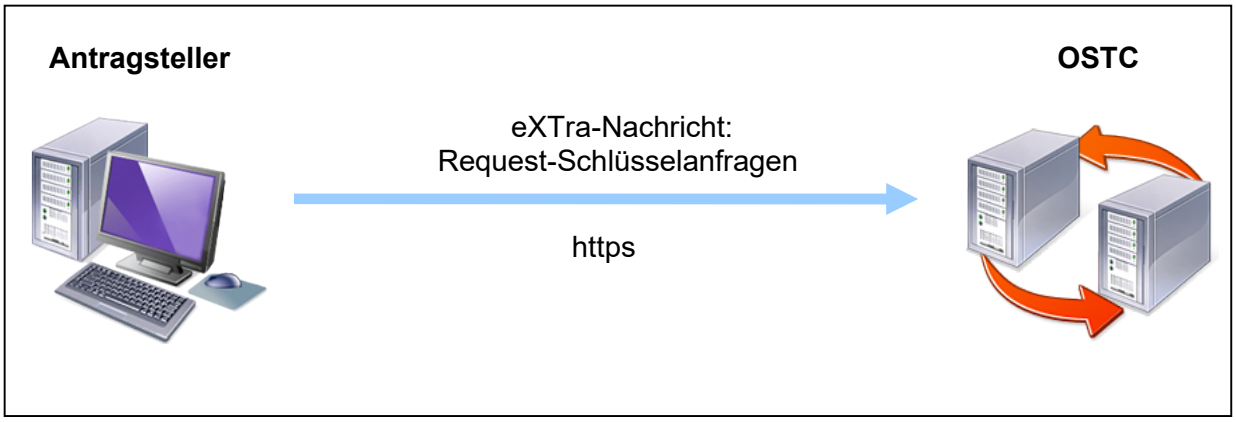
Die Zertifikate werden zur Abholung per eXTra-Nachtichten über die OSTC bereitgestellt. Mit der Eingangsnummer und der IK oder Betriebsnummer kann der Antragsteller sein Zertifikat nach Bereitstellung direkt über den Client anfragen.

Schritt 1 – Anmeldung an der Schnittstelle:



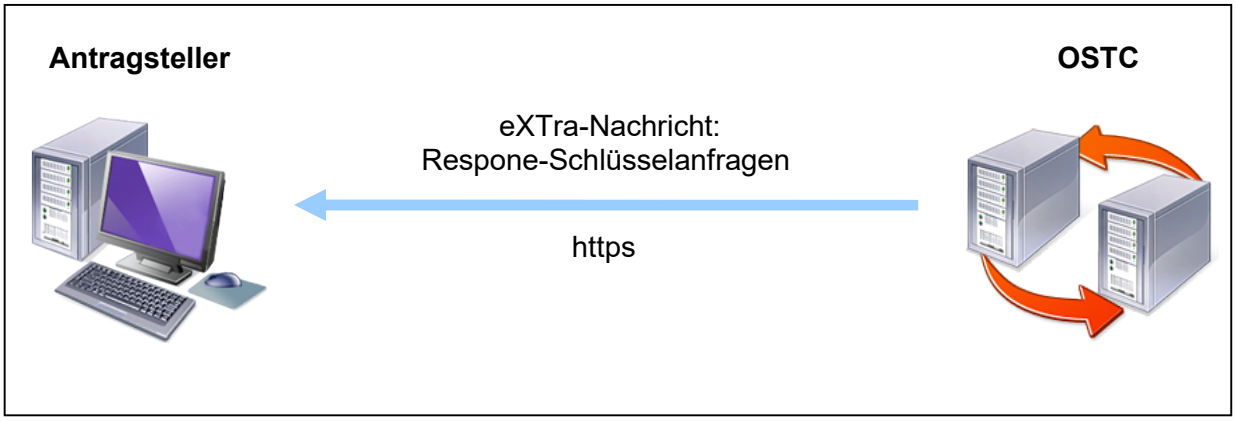
Die Verifizierung der Zugangsdaten ist mit dem Ablauf in der ersten https-Session identisch.

Schritt 2 – Übermittlung der Zertifikatsanfrage des Antragstellers:



Der Client übermittelt nach der erneuten Anmeldung die Anfrage zur Abholung eines Zertifikats des Antragstellers. Hierzu werden die xml-Nutzdaten mit den Zertifikatsdaten base64 kodiert und dann im Data-Element des Transportbodies eingebunden. Für die Art der Kommunikation wird hier das Szenario “request-with-response” verwendet.

Schritt 3 – Übermittlung des Zertifikats:

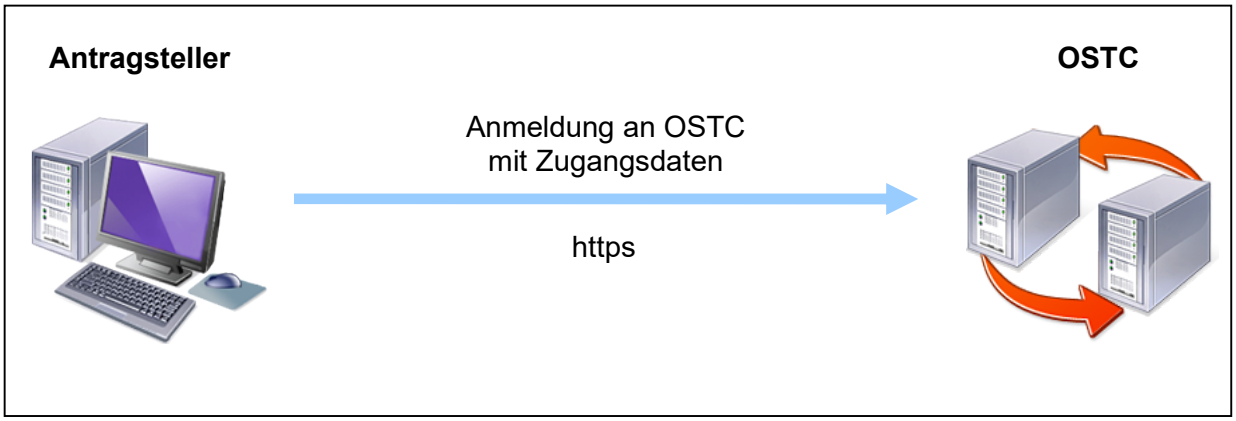


Nach Prüfung der Eingangsnummer und der IK oder Betriebsnummer werden die Daten der p7c-Responsedatei für die Übermittlung base64 kodiert und dann im Data-Element des Transportbodies eingebunden. Abschließend sendet die OSTC den „Response“ an den Client.

3.2.2 Ablauf in der vierten https-Session

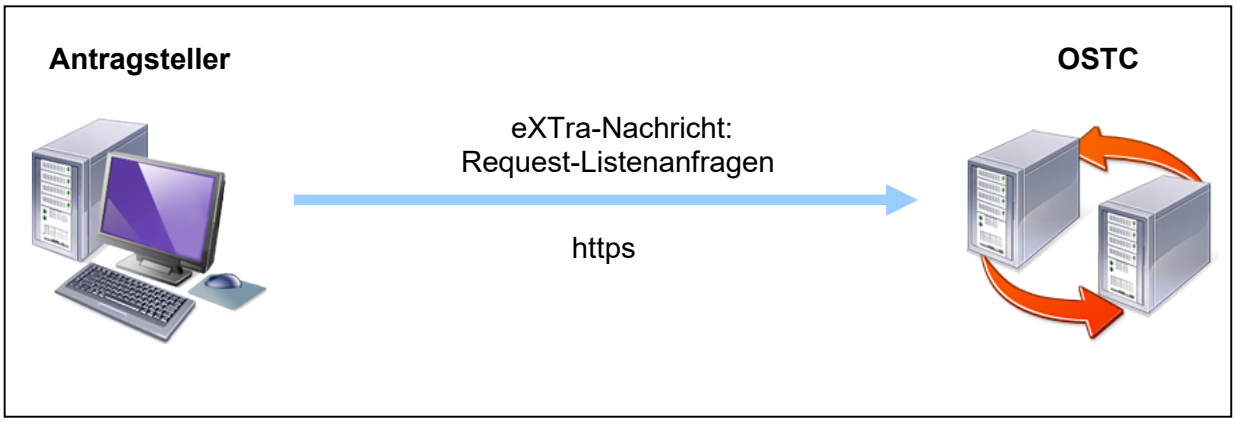
Die Schlüssellisten werden zur Abholung per eXTra-Nachtichten über die OSTC bereit gestellt. Der Antragsteller kann direkt über den Client eine Schlüsselliste anfragen.

Schritt 1 – Anmeldung an der Schnittstelle:



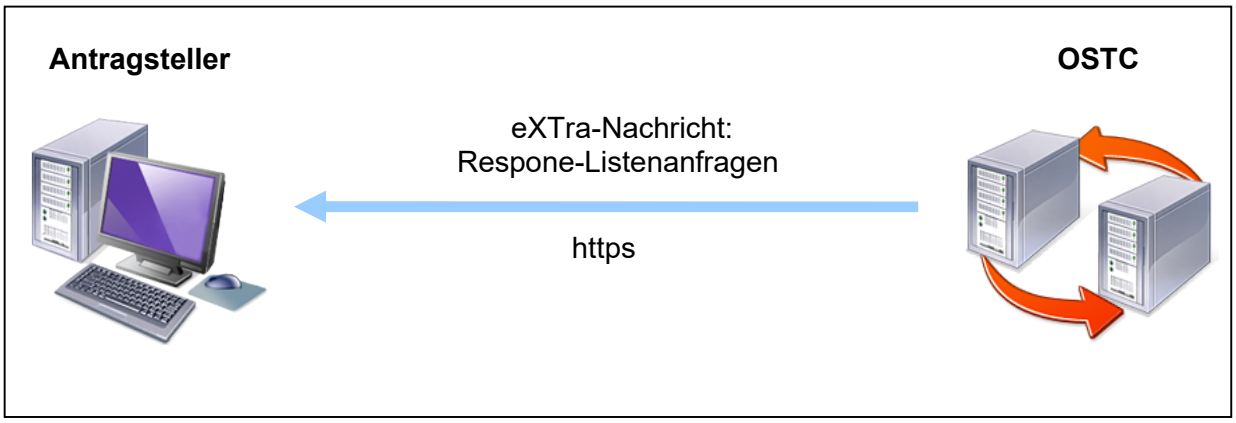
Die Verifizierung der Zugangsdaten ist mit dem Ablauf in der ersten https-Session identisch.

Schritt 2 – Übermittlung der Listeanfrage des Antragstellers:



Der Client übermittelt nach der erneuten Anmeldung die Anfrage zur Abholung einer Schlüsselliste. Hierzu werden die xml-Nutzdaten mit den Listedaten base64 kodiert und dann im Data-Element des Transportbodies eingebunden. Für die Art der Kommunikation wird hier das Szenario “request-with-response” verwendet.

Schritt 3 – Übermittlung der Schlüsselliste:



Nach Prüfung der angefragten Schlüsselliste werden die base64 kodierten Schlüsseldaten der Annahmeliste im Data-Element des Transportbodies eingebunden. Abschließend sendet die OSTC den „Response“ an den Client.

Nach dem Importieren der Schlüsseldaten vom Trust Center wird eine zweite Programmsicherung der Client-Software mit dem abgeschlossenen Antragsstatus empfohlen. Diese wichtige Sicherung soll es den Antragsteller bei einer Neuinstallation ermöglichen, den abgeschlossenen Antragsstatus mit dem privaten Schlüssel, dem Zertifikat und den Annahmeschlüssel wiederherstellen zu können. Ohne Programmsicherung kann der Status mit dem privaten Schlüssel und dem Zertifikat nicht mehr hergestellt werden und eine erneute kostenpflichtige Beantragung wäre erforderlich.

4 Verarbeitung von Erstanträgen und Online-Folgeanträgen

4.1 Erstanträge

Bei einem Erstantrag wird die xml-Nutzdatendatei „Antragsdaten“ nur mit der p10-Requestdatei ohne weitere Antragsdaten unverschlüsselt über die OSTC übermittelt, da der Antragsteller über kein gültiges zugeordnetes Zertifikat vom Trust Center verfügt. In diesem Fall wird der Zertifizierungsantrag und die Authentifizierung über ein separates Antragsportal der ITSG abgewickelt.

4.2 Online-Folgeanträge

Die übermittelte xml-Nutzdatendatei „Antragsdaten“ muss mit einem gültigen Zertifikat des Antragsstellers gemäß Punkt 3.1.1 verschlüsselt sein. Ein Zertifikat mit einer anderen IK- oder Betriebsnummer bzw. mit fremdem Schlüssel ist nicht zulässig. Die IK- bzw. Betriebsnummer muss für das Zertifikat mit dem Erstantrag bzw. dem vorangegangenen Antrag identisch sein. Für Teilnehmer, die eine Eigenerklärung als Meldestelle abgegeben haben und bei Anträgen von Datenannahmestellen, oder mit einer Test-Betriebsnummer ist die Antragsvariante Online-Folgeantrag nicht zulässig. In diesen Fällen ist eine erneute Authentifizierung über die ITSG-Registrierungsstelle bei jedem Antrag erforderlich.

4.3 Nicht eindeutig qualifizierbare Folgeanträge

Eine Bearbeitung eines Online-Folgeantrags kann nicht erfolgen, wenn der elektronische Abgleich der IK- oder Betriebsnummer nicht eindeutig vorgenommen werden kann, da z. B. kein gültiges Zertifikat seitens des Antragstellers vorliegt. Bei einer fehlerhaften Datenverschlüsselung kann der Antrag nicht weiter bearbeitet werden und es wird der zugeordnete Fehlercode zurückgegeben.

4.4 Doppelte Anträge

Die Schnittstelle prüft, ob innerhalb von 24 Stunden mehrere Anträge von einem Antragsteller (gleiche IK oder BN) eingesendet werden. Falls zu einer IK- oder Betriebsnummer mehrere Anträge innerhalb dieses Zeitraums abgegeben werden, erfolgt bereits bei der Abgabe eine Ablehnung. Eine erneute Antragstellung ist erst nach 24 Stunden möglich. Hiermit soll vermieden werden, dass ein Antragsteller nicht einfach mehrere kostenpflichtige Anträge direkt hintereinander senden kann.

5 Nutzungsbedingungen für die OSTC Version 2.5

5.1 Anmeldeformular

Dieses Anmeldeformular dient zur Anforderung einer Anmeldekennung für die OSTC des ITSG-Trust Centers für Softwarehäuser.

Empfänger

ITSG-Trust Center
Elektronischer Datenaustausch
Kaiserleistraße 10-16
63067 Offenbach

Angaben zum Unternehmen (Nutzer)

Name der Firma: _____

Straße und Haus-Nr.: _____

Postleitzahl und Ort: _____ _____

Angaben zum Ansprechpartner

Ansprechpartner: _____

E-Mail-Adresse: _____

Telefon-Nummer: _____

Angaben zur Softwareapplikation (Allgemeine Informationen über das Softwareprodukt, welches die Online-Schnittstelle unterstützt)

Name der Applikation: _____

Softwareversion: _____

Wir fordern eine Anmeldekennung gemäß der aktuellen Beschreibung für die Online-Schnittstelle des ITSG-Trust Centers an.

_____ _____
(Datum) (Unterschrift)

Mit der nachfolgenden Unterschrift bestätigen wir, dass wir
- die besonderen Nutzungsbedingungen für die Online-Schnittstelle unter Punkt 5.2
- die AGB der ITSG unter www.itsg.de

zur Kenntnis genommen haben.

_____ _____
(Datum) (Unterschrift)

Senden Sie das vollständig ausgefüllte Anmeldeformular per E-Mail an
tc-produktmanagement@itsg.de

5.2 Besondere Nutzungsbedingungen

5.2.1 Geltungsreihenfolge

Für die Nutzung der Online-Schnittstelle gelten in folgender Reihenfolge:

- schriftliche Vereinbarungen im Einzelfall
- diese Besonderen Nutzungsbedingungen

Es gelten die Nutzungsbedingungen und Geschäftsbedingungen in der jeweiligen Fassung bei Vertragsabschluss.

5.2.2 Vertragsschluss, Schriftform

Der Vertrag über die Nutzung der Online-Schnittstelle des ITSG-Trust Centers kommt mit der Annahme des unterzeichneten Anmeldeformulars durch die ITSG zustande. Der Vertrag und eventuelle Änderungen unterliegen der Schriftform. Als Schriftform gilt auch Telefax.

5.2.3 Leistung der ITSG

Die ITSG stellt dem Nutzer kostenfrei eine Online-Schnittstelle zur Verfügung. Die Online-Schnittstelle ermöglicht die elektronische Abgabe von Anträgen auf Zertifizierung beim ITSG-Trust Center. Jeder Abgabevorgang muss eine Identifizierung der Softwareapplikation beinhalten. Jede Applikation erhält durch die ITSG einen Benutzernamen mit einem Passwort und eine RegistrationID zugeteilt.

Der Anwender kann Anträge auf Zertifizierung über die dafür vorgesehene Online-Schnittstelle des Trust Centers durchführen. Die Daten des Anwenders werden bei der Übertragung verschlüsselt übertragen.

Die Schnittstelle stellt die ITSG nicht permanent ohne Unterbrechungen zur Verfügung. Unterbrechungen können sich insbesondere ergeben durch

- Wartungsarbeiten und Störungsbehebungen
- die technische Umsetzung von Verbesserungen
- Änderungen der Inhalte

5.2.4 Haftung der ITSG

Die Haftung der ITSG gegenüber ihren Kunden - gleich aus welchem Rechtsgrund - ist mit Ausnahme der Verletzung wesentlicher Vertragspflichten beschränkt auf die Fälle des Vorsatzes und der groben Fahrlässigkeit der gesetzlichen Vertreter, Mitarbeiter und Erfüllungsgehilfen der ITSG. Soweit wesentliche Vertragspflichten verletzt werden, haftet die ITSG auch für leicht fahrlässig verursachte Schäden höchstens bis zu 5.000,00 € je Schadenfall.

5.2.5 Anmeldung und Angaben des Nutzers

Der Nutzer bestätigt mit der Unterzeichnung, dass die vor und bei Vertragsschluss gemachten Angaben über seine Person und vergleichbare vertragsrelevante Umstände vollständig und richtig sind. Der Nutzer verpflichtet sich, die ITSG jeweils unverzüglich über Änderungen dieser Umstände zu unterrichten. Auf entsprechende Anfrage der ITSG hat der Benutzer die Daten zu bestätigen.

5.2.6 Allgemeine Nutzung der Online-Schnittstelle

Der Benutzer darf den Service nur in der von der ITSG vertraglich und technisch vorgegebenen Weise nutzen und in der angegebenen Softwareapplikation müssen die technischen Abläufe gemäß den zugeordneten Spezifikationen und Dokumentationen durchgeführt werden. Ein Eingriff in die technischen Abläufe über die bloße Nutzung hinaus (Manipulation) ist untersagt. Die Anzeige von Meldungen zu Return- und Fehlercodes obliegt dem Nutzer.

5.2.7 Pflichten des Nutzers

Der Nutzer sichert zu, dass er in der angegebenen Softwareapplikation eine Sicherheitsabfrage für eine kostenpflichtige Beantragung eines Zertifikats mit einem Hinweis auf die AGB der ITSG über die Web-Seite www.itsg.de und die Leistungsbeschreibung des ITSG-Trust Centers über die Web-Seite www.trustcenter.info verbindlich einpflegen wird, damit ein Antragsteller davon Kenntnis nehmen kann und somit eine versehentliche Beantragung nicht möglich ist.

Direkt bei der Antraggenerierung werden nicht zulässige Angaben und Zeichen gemäß den Vorgaben des Trust Centers von der Softwareapplikation geprüft und abgewiesen, damit eine fehlerhafte Beantragung vermieden wird. Der Antragsteller wird bei einem Folgeantrag auf die Prüfung seiner aktuellen Adresse hingewiesen, um bei einem Umzug die neue Adresse anzugeben und somit nicht zustellbare Rechnungen zu vermeiden

5.2.8 Wichtige Hinweise

Im Falle einer Einschränkung zur Nutzung der Online-Schnittstelle, z. B. durch eine Firewall, soll der Antragsteller alternativ einen Zertifizierungsantrag ohne OSTC-Anbindung aus der Softwareapplikation generieren können. Diese Vorgabe ist für die Antragsteller wichtig, damit stets die Möglichkeit einer Beantragung ohne Supportaufwand gegeben ist, unabhängig der Beantragungsart.

5.2.9 Kündigung / Einstellung der Dienste

Die Vereinbarung kann mit einer Frist von 2 Wochen zum Monatsende gekündigt werden.
Die ITSG hat das Recht zur außerordentlichen Kündigung und sofortiger Sperrung der Schnittstelle insbesondere

- wenn der Nutzer seine Daten trotz zweifacher Aufforderung nicht bestätigt
- der Nutzer die Schnittstelle in schwerwiegender Weise manipuliert.

5.2.10 Gerichtsstand

Der Gerichtsstand richtet sich nach dem Sitz der ITSG in Offenbach, soweit der Kunde Vollkaufmann ist und der Vertrag zum Betrieb seines Handelsgewerbes gehört. Die ITSG kann ihre Ansprüche auch bei den Gerichten des allgemeinen Gerichtsstandes des Kunden geltend machen. Ein etwaiger ausschließlicher Gerichtsstand bleibt unberührt.