

Seit 2023 gelten für Zertifizierungsanträge neue Anforderungen zur Identifizierung und Authentifizierung der Antragsteller beim ITSG-Trust Center.

## Voraussetzungen für eine Zertifizierung

- die Identifizierung und Authentifizierung der Antragsteller erfolgt über ein Online-Registrierungsportal des Trust Centers
- die Identifizierung der Kontaktperson erfolgt über ein Postident-Verfahren
- das Trust Center muss bei der Antragstellung durch geeignete Maßnahmen prüfen, ob die Betriebsnummer, gesonderte Absendernummer (z.B. A2345678), oder die Zahlstellenummer für Arbeitgeber, Absendernummer für Hochschulen (z.B. H2345678), oder das Institutionskennzeichen für Leistungserbringer dem Antragsteller zugeordnet werden darf. Dies erfolgt durch einen Freischaltcode, der postalisch an die in einem Verzeichnis hinterlegten Firmenadresse versendet wird.
- für den Hashcode des public Key im Requestschlüssel ist nur der Hashalgorithmus SHA256 zulässig
- Arbeitgeber, Leistungserbringer, oder Dienstleister (z.B. Rechenzentren), die mit dem für Ihre Betriebsnummer, gesonderte Absendernummer, oder Institutionskennzeichen ausgestellten Zertifikat Meldungen für weitere Nummern übertragen, gelten ab 2023 als Meldestelle.

Meldestellen, die für mehrere Betriebsnummern oder Institutionskennzeichen Daten übermitteln, müssen sich bei der Beantragung eines Zertifikates mit einer Eigenerklärung als Meldestelle registrieren. Eine nachträgliche Anmeldung als Meldestelle ist möglich. Das Formular zur Eigenerklärung für eine Meldestelle finden Sie hier zum [Download](#). Weitere Informationen zu Meldestelle finden Sie auf der Seite <https://www.itsg.de/produkte/trust-center/zertifikat-beantragen/> unter dem Punkt Preise.

Die Onlineschnittstelle des Trust Centers (OSTC) wird zur automatisierten Übermittlung der Antragsdaten und des Requestschlüssels mit dem Hashcode angeboten. Damit ist auch ein Online-Folgeantrag mit schnellerer Antragsabwicklung möglich. Die Nutzung der OSTC-Onlineschnittstelle setzt voraus, dass die verwendete Software die Onlineschnittstelle des Trust Centers unterstützt.

Bei Softwareprodukten ohne OSTC-Unterstützung muss der Requestschlüssel mit dem Hashcode vom Antragsteller manuell über das Upload-Portal auf der Seite <https://www.itsg-trust.de/zap/home> an das Trust Center übermittelt werden.

## Antragsvarianten und Voraussetzungen

Es gibt die drei grundlegenden Antragformen Erstantrag, erneuter Antrag und Online-Folgeantrag über die OSTC-Onlineschnittstelle des Trust Centers.

Bei Erstanträgen und erneuten Anträgen ist die Identifizierung und Authentifizierung der Antragsteller über das Trust Center-Registrierungsportal in einen Web-Browser durchzuführen. Eine Registrierung im Registrierungsportal ist ein einmaliger Vorgang pro Antrag und gilt nur für den jeweiligen Antrag. Die Registrierungsdaten werden aus datenschutzgründen nach einer Frist gelöscht. Zu beachten ist, dass eine Registrierung beim Trust Center nicht mit einer Registrierung beim SV-Meldeportal zu verwechseln ist und jeweils für eine abgeschlossene Registrierung eine Rechnung gestellt wird.

Die elektronischen Schlüssel werden bei allen Antragsvarianten in der verwendeten Entgeltabrechnungssoftware für Arbeitgeber, oder in der Abrechnungssoftware für Leistungserbringer, oder in einem separaten Verschlüsselungstool generiert. Bei einer Beantragung eines Zertifikats ist die Nummer (z.B. Betriebsnummer oder IK) in der jeweiligen Kundensoftware oder Verschlüsselungstool und bei einer Registrierung identisch anzugeben, denn eine Vermischung von Nummern oder ein Zahlendreher führt zu einem fehlerhaften Antrag.

- Erstanträge mit einer Registrierung im Registrierungsportal können ohne, oder zusätzlich mit der OSTC-Onlineschnittstelle durchgeführt werden und dies ist abhängig, ob die verwendete Kundensoftware die Onlineschnittstelle unterstützt.

- Bei erneuten Anträgen erfolgt die Beantragung wie bei Erstanträgen mit einer Registrierung ohne oder zusätzlich mit der OSTC-Onlineschnittstelle. Es wird vorausgesetzt, dass zuvor mindestens ein Zertifikat vom ITSG Trust Center beantragt wurde, oder wenn sich die Kontaktperson im Zertifikat ändert.
- Bei einem Online-Folgeantrag über die OSTC-Onlineschnittstelle erfolgt die komplette Antragsabwicklung mit der verwendeten Kundensoftware über die Onlineschnittstelle des Trust Centers ohne Registrierungsportal.  
Online-Folgeanträge über die OSTC-Onlineschnittstelle setzen voraus, dass ein noch gültiges Zertifikat vom ITSG Trust Center zur elektronischen Signatur der Antragsdaten verwendet wird und sich die Kontaktperson im gültigen Zertifikat auch für das neue Zertifikat nicht ändert.  
**Zu beachten:** Für einzelne Teilnehmergruppen sind Online-Folgeanträge nicht zulässig, z.B. Datenannahmestellen, Meldestellen und Anträge mit Testbetriebsnummern. Treffen die Voraussetzungen für einen Online-Folgeantrag nicht zu, dann ist ein erneuter Antrag über das Trust Center Registrierungsportal durchzuführen.

## Übersicht der Antragsdaten und Antragskomponenten

Die Antragsdaten umfassen folgende Daten:

- Betriebsnummer, Testbetriebsnummer, gesonderte Absendernummer (z.B. A2345678), Absendernummer für Hochschulen (z.B. H2345678), oder Zahlstellenummer für Arbeitgeber, oder Institutionskennzeichen für Leistungserbringer
- Vor- und Nachnamen der Kontaktperson gemäß Personalausweis oder Reisepass
- E-Mail-Adresse und Telefon-Nummer der Kontaktperson der Firma
- Firmennamen mit Firmenanschrift zur Nummer (z.B. Betriebsnummer, Institutionskennzeichen)
- optionale Rechnungsadresse für Zusendung einer Rechnung postalisch oder per E-Mail

Die Antragskomponenten sind:

- SHA256-Hashcode des public Key im Requestschlüssel als pdf-Datei
- Requestschlüsseldatei (z.B. 12345678.p10)
- optionale Eigenerklärung für Meldestellen als pdf-Datei

## Schritte zur Beantragung eines Zertifikats

Die nachfolgenden Schritte beschreiben eine Beantragung mit Ausgangssituation eines Erstantrags oder erneuten Antrags mit Identifizierung und Authentifizierung der Antragsteller über das Registrierungsportal. Eine Beantragung mit der Antragform Online-Folgeantrag ohne Registrierungsportal wird auch an den entsprechenden Schritten beschrieben, wo eine entsprechende Aktion erforderlich ist.

Eine ausführliche Beschreibung mit Screenshots zum Trust Center Registrierungsportal können Sie im Dokument „Informationen zum Trust Center Registrierungsportal“ auf unserer Web-Seite

<https://www.itsg.de/produkte/trust-center/unterlagen-download/> entnehmen.

### 1. Anmeldung am Registrierungsportal und Erfassung der Kontaktdaten

Erstanträge oder erneute Anträge mit einer Registrierung:

Das ITSG Registrierungsportal kann in einen Web-Browser über die Adresse <https://registrierungsportal.itsg.de> aufgerufen werden und es erscheint eine Anmeldemaske.

In der Anmeldemaske wählen Sie für einen neuen Vorgang den Knopf „Registrieren“ und für einen bestehenden Vorgang den Knopf „Anmelden“. Bitte die Anmeldeinformationen notieren, da man sich zur Durchführung der einzelnen

Schritte wiederholt anmelden muss. Es ist zu beachten, dass eine Registrierung im Registrierungsportal ein einmaliger Vorgang pro Antrag ist und Anmeldedaten einer zuvor abgeschlossenen Registrierungen nicht mehr existieren.

Bei jedem Erstantrag oder erneuten Antrag werden die Anmeldedaten für das Trust Center Registrierungsportal und Antragsdaten für ein Zertifikat von der Kontaktperson des Kunden im Registrierungsportal manuell erfasst.

**Zu beachten:** Die Kontaktperson gibt in der Maske Ihren Vornamen und Nachnamen (ggf. auch Doppelnamen und Titel bei Nachname) gemäß Vorderseite Personalausweis, entsprechende amtliche Identitätskarte oder Reisepass vollständig an, z.B. Vorname: Erika Simone, Nachname: Dr. Mustermann.

Falls der Name unvollständig eingegeben wurde oder vom Ausweisdokument abweicht, führt dies zu einer Ablehnung im Registrierungsportal bei der Identitätsprüfung nach einem Postident-Verfahren.

Danach gibt die Kontaktperson ihre Firmenkontaktdaten an. Bei der Eingabe der E-Mail-Adresse ist auf die richtige Schreibweise zu achten, da sonst bei fehlerhaft erfasster Adresse eine Bestätigungsmail nicht erhalten wird und somit die Registrierung nicht fortgeführt werden kann.

## Online-Folgeanträge über die OSTC-Onlineschnittstelle:

Für Online-Anträge muss die verwendete Kundensoftware die OSTC-Onlineschnittstelle des ITSG-Trust Centers unterstützen und die Voraussetzungen für einen Online-Folgeantrag müssen erfüllt sein.

Bei einem Online-Folgeantrag über die OSTC-Onlineschnittstelle werden die kompletten Antragsdaten von der Kontaktperson des Kunden in der verwendeten Entgeltabrechnungssoftware für Arbeitgeber, oder in der Abrechnungssoftware für Leistungserbringer, oder in einem separaten Verschlüsselungstool bei Schritt 4 manuell erfasst.

## 2. Identifizierung der Kontaktperson

### Erstanträge oder erneute Anträge mit einer Registrierung:

Die Kontaktperson des Kunden, die eine Beantragung durchführt und auch im Zertifikat stehen soll, führt über das Registrierungsportal eine Identifizierung mit Postident-Verfahren durch. Zur Auswahl stehen folgende Ident Verfahren:

- Identifizierung in einer deutschen Postfiliale
- Identifizierung mit Online-Ausweisfunktion (eID)

Zu den Postident-Verfahren zeigen folgende Youtube-Erklärvideos die Durchführung:

[POSTIDENT durch Postfiliale - persönliche Identifikation vor Ort, einfach & schnell | Deutsche Post - YouTube](#)

[POSTIDENT durch Online-Ausweisfunktion \(eID\) per App | Deutsche Post - YouTube](#)

**Zu beachten:** Nach der Identifizierung mit einem Postident-Verfahren wird abschließend im Registrierungsportal die elektronische Rückmeldung vom Postident-System geprüft, ob Vornamen und Nachnamen (ggf. auch Doppelnamen und Titel bei Nachname) gemäß Vorderseite Personalausweis, entsprechende amtliche Identitätskarte oder Reisepass vollständig übereinstimmen.

War die Prüfung erfolgreich, können die weiteren Ablaufschritte durch die Kontaktperson fortgeführt werden.

War die Identifizierung nicht erfolgreich, wird der komplette Antragsvorgang im ITSG-Registrierungsportal als fehlerhaft beendet und ein neuer Vorgang kann gestartet werden.

Weitere Informationen zum Postident-Verfahren können Sie im Dokument „Informationen zum Postident-Verfahren beim ITSG Trust Center“ auf unserer Web-Seite

<https://www.itsg.de/produkte/trust-center/unterlagen-download/> entnehmen.

## Online-Folgeanträge über die OSTC-Onlineschnittstelle:

Für Online-Anträge muss die verwendete Software die OSTC-Onlineschnittstelle des ITSG-Trust Centers unterstützen und die Voraussetzungen für einen Online-Folgeantrag müssen erfüllt sein.

Die Kontaktperson des Kunden, der die Beantragung durchführt und auch im Zertifikat stehen soll, hat sich bei einem Erstantrag bereits authentifiziert. Bei einem Online-Folgeantrag gilt, dass sich die Kontaktperson im Zertifikat nicht ändern darf, sonst ist ein erneuter Antrag von einer neuen Kontaktperson über das ITSG Registrierungsportal durchzuführen und somit ist es kein Online-Folgeantrag mehr. Die nächste Aktion für diese Antragsform erfolgt bei Schritt 4.

### **3. Überprüfung der Firmendaten**

#### Erstanträge oder erneute Anträge mit einer Registrierung:

Das Trust Center muss durch geeignete Maßnahmen die Firmendaten prüfen, ob die Betriebsnummer, gesonderte Absendernummer, oder Zahlstellennummer für Arbeitgeber, Absendernummer für Hochschulen, oder Institutionskennzeichen für Leistungserbringer dem Antragsteller zugeordnet werden darf. Dies erfolgt durch einen Freischaltcode, der postalisch an die in einem Verzeichnis hinterlegten Adresse versendet wird. Die hinterlegte Adresse stammt aus dem aktuellen Verzeichnis der ArGe IK für Institutionskennzeichen und der aktuellen Betriebsstättendatei der Bundesagentur für Arbeit für Betriebsnummern. Die gesonderten Absendernummern inklusive der Absendernummern für Hochschulen und die Zahlstellennummern werden von der ITSG verwaltet.

Der Kontaktperson wird entsprechend der eingegebenen Nummer (z.B. Betriebsnummer, Institutionskennzeichen) die zugeordnete Firmenadresse des Kunden angezeigt. Die Kontaktperson hat die Möglichkeit seinen Namen und z.B. Abteilung zur angezeigten Firmenadresse manuell hinzuzufügen, damit eine gezielte Zusendung eines Freischaltungsbriefs an die Kontaktperson möglich ist. An die zugeordnete Firmenadresse wird ein Freischaltcode und der SHA256-Hashcode des Requestschlüssels postalisch gesendet.

**Zu beachten:** Ist die angezeigte Firmenadresse im Registrierungsportal nicht korrekt, so ist eine Änderung der Firmendaten durch die ITSG GmbH nicht gestattet. Die Kontaktperson muss dann der zuständigen Vergabestelle die aktuellen Firmendaten des Unternehmens mitteilen. Dabei ist nur die Aktualisierung der Firmenadresse des zur Nummer (z.B. Betriebsnummer, Institutionskennzeichen) zugeordneten Antragstellers zulässig (z.B. nach Umzug), nicht aber eine abweichende Adresse der berechtigten Kontaktperson für die Registrierung, z.B. eines beauftragten Dienstleisters, oder eine private Adresse. Bis zur Aktualisierung der Firmendaten kann die Registrierung nicht fortgeführt werden. Auf die Dauer der Aktualisierung bei der externen Vergabestelle hat die ITSG GmbH keinen Einfluss. Die Kontaktperson soll sich danach wieder am Registrierungsportal anmelden, um die automatische Aktualisierung der Firmendaten zu überprüfen. Eine gesonderte Mitteilung über die Aktualisierung, z.B. per E-Mail, erfolgt nicht.

### **4. Erfassung der Schlüsseldaten und Generierung der Kundenschlüssel**

Die Schlüsseldaten für das Zertifikat umfassen folgende Daten und müssen mit den Antragsdaten im Registrierungsportal übereinstimmen:

- Betriebsnummer, gesonderte Absendernummer, oder Zahlstellennummer für Arbeitgeber, Absendernummer für Hochschulen, oder Institutionskennzeichen für Leistungserbringer
- Firmenname
- Name der Kontaktperson

**WICHTIG:** Schlüsseldaten, die nicht mit den Antragsdaten im Registrierungsportal übereinstimmen, führen zu einem fehlerhaften Zertifizierungsantrag. Ein anderer Firmenname, abweichend vom Inhaber der Betriebsnummer, gesonderte Absendernummer, Zahlstellennummer, Absendernummer für Hochschulen, oder Institutionskennzeichen ist nicht zulässig. Zulässig sind zusätzliche Angaben im Firmennamen, wie z.B. Ort, Bundesland, oder Name des Dienstleisters, sowie Bezeichnung der Dienstleistung, bei dem das Zertifikat im Einsatz ist. Der eigentliche Firmenname darf dabei nur ergänzt werden, z.B. Erika Mustermann Physiopraxis.

Bei dem Beispiel ist die Angabe Physiopraxis nur eine Ergänzung des Firmennamen als Bezeichnung der Dienstleistung.

Beim Firmennamen sind max. 80 Zeichen zulässig und bei längeren Firmennamen kann die offizielle Kurzbezeichnung (z.B. ITSG GmbH) verwendet werden, oder der Firmenname kann sinnvoll gekürzt werden (z.B. Informationstechnische Servicestelle der Gesetzl. Krankenversich. GmbH).

In einer Requestdatei kann das Trust Center aus technischen Gründen für Firmennamen und Namen der Kontaktperson keine Umlaute und nur folgende Sonderzeichen maschinell verarbeiten: Leerzeichen, /, Minus, Punkt und (Klammer). Umlaute (ä, ö, ü etc.) oder weitere Sonderzeichen (ß, +, &, Semikolon, Unterstrich, Komma, \, Anführungszeichen, § etc.) sind nicht zulässig.

#### Erstanträge oder erneute Anträge mit einer Registrierung:

Es wird nun in der Registrierung eine GUID-Vorgangsnummer vergeben, die als Referenz zwischen den Antragsdaten im Registrierungsportal und Ihren Schlüsseldaten aus der Kundensoftware verwendet wird. Da die eindeutige GUID aus 36 Zeichen besteht, wird für die Übernahme der GUID ein manuelles Kopieren und Einfügen der Zeichen empfohlen, um Schreibfehler oder Zeichendreher zu vermeiden. Die GUID-Vorgangsnummer wird dazu als pdf-Dokument oder zum Kopieren in die Zwischenablage angeboten.

Nachdem alle Antragsdaten im Registrierungsportal erfasst wurden, ist zur Durchführung dieses Schrittes erforderlich, dass zunächst als Zwischenschritt in der verwendeten Entgeltabrechnungssoftware für Arbeitgeber, oder in der Abrechnungssoftware für Leistungserbringer, oder in einem separaten Verschlüsselungstool ein elektronisches Zertifikat beim ITSG Trust Center beantragt wird. Dies kann nicht im Registrierungsportal geschehen, da hier nur die Identifizierung und Authentifizierung der Antragsteller erfolgt und das Trust Center nicht die privaten Schlüssel verwaltet.

Dazu sind in der Kundensoftware oder in einem Verschlüsselungstool die Schlüsseldaten zur Generierung der Kundenschlüssel (private Key und public Key) manuell zu erfassen und ein Zertifikat zu beantragen.

In Abhängigkeit des Zugriffs auf die Kundensoftware oder Verschlüsselungstool führen entweder die Kontaktperson oder eine andere berechtigte Person (z.B. Administrator) dies durch.

**Zu beachten:** Die GUID-Vorgangsnummer ist nicht Bestandteil der Schlüsseldaten für das Zertifikat und ist nur als Referenz zusätzlich zu den Schlüsseldaten in der Kundensoftware oder in einem Verschlüsselungstool mit OSTC-Unterstützung zu erfassen, damit somit ein Bezug zum Vorgang im Registrierungsportal für den Zertifizierungsantrag besteht. Es wird ein manuelles Kopieren und Einfügen der langen GUID empfohlen, um ein Schreibfehler oder Zeichendreher zu vermeiden.

Unterstützt die verwendete Kundensoftware nicht die OSTC-Onlineschnittstelle des Trust Centers, dann ist die GUID nicht zwingend mit den Schlüsseldaten in der verwendeten Software zu erfassen und die GUID wird dann zur manuellen Übermittlung der Requestdatei und Hashcode an das Trust Center benötigt (siehe Punkt 5).

Nach Eingabe der Schlüsseldaten erfolgt die automatische Erzeugung der Schlüssel mit dem SHA256-Hashcode des Schlüssels zur Zertifizierung über die verwendete Kundensoftware, oder über ein separates Verschlüsselungstool.

Der SHA256-Hashcode des generierten Requestschlüssels soll von der verwendeten Software in eine Datei gespeichert werden (pdf-Datei), um bei einem nachfolgenden Antragsschritt den Hashcode durch die Kontaktperson auf Übereinstimmung zu prüfen (Beispielsauszug eines Hashcodes: E1D07A4B.....FC781).

Die pdf-Datei mit dem SHA256-Hashcode muss für eine eindeutige Zuordnung folgende Angaben enthalten:

- Betriebsnummer, gesonderte Absendernummer, oder Zahlstellennummer für Arbeitgeber, Absendernummer für Hochschulen, oder Institutionskennzeichen für Leistungserbringer
- Firmenname
- Name der Kontaktperson
- Hashcode des public Key im Requestschlüssel (SHA256 Hash-Algorithmus)
- Unterschrift der Kontaktperson (Vorgabe gemäß Security-Schnittstelle Kapitel 5.5)

## Alle Antragsformen mit OSTC-Onlineschnittstelle:

Für Online-Anträge muss die verwendete Software die OSTC-Onlineschnittstelle des ITSG-Trust Centers unterstützen und die Voraussetzungen für einen Online-Folgeantrag müssen erfüllt sein.

Bei einem Online-Antrag über die OSTC-Onlineschnittstelle werden alle erforderlichen Antragsdaten auch für die Generierung der Kundenschlüssel (private Key und public Key) in der verwendeten Entgeltabrechnungssoftware für Arbeitgeber, oder in der Abrechnungssoftware für Leistungserbringer, oder in einem separaten Verschlüsselungstool manuell erfasst.

Nach Eingabe der Antragsdaten erfolgt die automatische Erzeugung der Schlüssel mit dem SHA256-Hashcode des Schlüssels zur Zertifizierung über die verwendete Software, oder über ein separates Verschlüsselungstool.

Die Verwendung einer GUID-Vorgangsnummer aus einer Registrierung gilt nicht für Online-Folgeanträge ohne Registrierung.

## **5. Übermittlung der Requestdatei und Hashcode zur Zertifizierung sowie Eigenerklärung**

### Erstanträge oder erneute Anträge ohne OSTC-Onlineschnittstelle:

Wenn die verwendete Software die OSTC-Onlineschnittstelle nicht unterstützt, dann sind die Dateien aus Punkt 2 mit der Requestdatei (z. B. 12345678.p10) und dem SHA256-Hashcode (pdf-Datei mit Unterschrift) manuell an das Trust Center zu übertragen.

Optional kann eine Eigenerklärung für eine Meldestelle (pdf-Datei mit Unterschrift und Firmenstempel) übermittelt werden.

Die Übermittlung der Requestdatei mit dem Hashcode muss vom Antragsteller manuell über das Upload-Portal auf der Seite <https://www.itsg-trust.de/zap/home> an das Trust Center übermittelt werden. Zur eindeutigen Zuordnung der Dateien ist noch die GUID-Vorgangsnummer aus dem Registrierungsportal anzugeben. Es wird ein manuelles Kopieren und Einfügen der langen GUID empfohlen, um Schreibfehler oder Zeichendreher zu vermeiden.

### Alle Antragsformen mit OSTC-Onlineschnittstelle:

Für Online-Anträge muss die verwendete Kundensoftware die OSTC-Onlineschnittstelle des ITSG-Trust Centers unterstützen und die Voraussetzungen für einen Online-Folgeantrag müssen erfüllt sein.

Bei einem Online-Antrag über die OSTC-Onlineschnittstelle werden alle erforderlichen Antragsdaten und Komponenten (ohne Eigenerklärung) über die Onlineschnittstelle übermittelt. Der Antragsteller erhält eine Online-Auftragsnummer vom OSTC-System zurück, wenn kein Fehler festgestellt wird.

Optional kann eine Eigenerklärung einer Meldestelle (pdf-Datei mit Unterschrift und Firmenstempel) separat übermittelt werden. Meldestellen müssen ab 2023 mit jedem Zertifizierungsantrag eine Eigenerklärung abgeben. Über einen Browser ruft die Kontaktperson die Web-Adresse <https://www.itsg-trust.de/zap/upload-self-declaration> auf und kann auf der Seite die Eigenerklärung hochladen.

## **6. Kostenpflichtige Beauftragung oder Storno der Zertifizierung**

Die Preisliste und AGB's der ITSG werden im Internet auf der Seite <https://www.itsg.de/produkte/trust-center/zertifikat-beantragen/> veröffentlicht.

### Erstanträge oder erneute Anträge:

Nach Erhalt des Freischaltungsbriefs vergleicht die Kontaktperson den SHA256-Hashcode auf dem Brief mit dem auf dem Kundenrechner gespeicherten Hashcode visuell auf Übereinstimmung.



Stimmt der SHA256-Hashcode auf dem Freischaltbrief mit dem Hashcode auf dem Kundenrechner überein, dann kann die Kontaktperson mit dem zugesendeten Freischaltcode die Registrierung abschließen und somit einen kostenpflichtigen Auftrag erteilen. Mit der Beauftragung erfolgt die Zertifizierung als kostenpflichtige Dienstleistung der ITSG. Nur während einer nicht abgeschlossenen Registrierung kann der Antragsteller den Vorgang im Registrierungsportal über den blauen Hilfebutton stornieren. Danach ist ein Storno nur bei fehlerhaften Anträgen möglich, da im Fehlerfall ohne Fehlerkorrektur kein Zertifikat erstellt wird.

Bei nicht Übereinstimmung des Hashcodes ist eine Klärung entweder mit dem zuständigen Software-Support oder mit dem Systemadministrator erforderlich, um einen fehlerhaften Antrag zu vermeiden (z. B. wurden in der Zwischenzeit nochmals Schlüssel generiert). Der Antrag wird in bis zur Klärung und Aktualisierung angehalten und weitere Schritte sind dann mit der ITSG-Hotline abzustimmen.

#### Alle Antragsformen mit OSTC-Onlineschnittstelle:

Bei einem Online-Antrag über die OSTC-Onlineschnittstelle bestätigt der Antragsteller während der Beantragung in der verwendeten Software, dass er die AGB's der ITSG zur Kenntnis genommen hat und eine kostenpflichtige Dienstleistung der Zertifizierung beauftragt. Ohne abschließende OSTC-Auftragsbestätigung über die Kundensoftware wird der Antrag nicht weiter bearbeitet. Der Antragsteller kann den Auftrag stornieren, in dem er keine abschließende Auftragsbestätigung aus der Kundensoftware über die OSTC sendet, da somit kein Zertifikat erstellt wird. Mit einer OSTC-Auftragsbestätigung ist ein Storno bei Online-Folgeantrag nicht mehr möglich.

## **7. Zertifizierung, Bereitstellung und Veröffentlichung**

Die übermittelte Requestdatei wird im Trust Center bei der Eingangsprüfung mit dem Hashcode gemäß Antragsdaten verglichen. Werden bei der Prüfung der Requestdatei und Antragsdaten keine Fehler festgestellt, dann erfolgt die Zertifizierung der Requestdatei durch das Trust Center jeweils an einem Werktag.

Vor der Bereitstellung der Zertifikatsdatei an den Antragsteller veröffentlicht das Trust Center den zertifizierten öffentlichen Schlüssel in den öffentlichen Schlüsselverzeichnissen für die Teilnehmer am elektronischen Datenaustausch im Internet: [www.trustcenter.info](http://www.trustcenter.info)

Das Trust Center stellt dem Antragsteller die zertifizierte Requestdatei (z. B. 12345678.p7c) als Zertifikat wie folgt bereit:

#### Alle Antragsformen ohne OSTC-Onlineschnittstelle:

- Zertifikatsdatei zum Download über die Online-Antragsverfolgung auf der Seite <https://www.itsg-trust.de/all/oav.php>
- per E-Mail an die E-Mail-Adresse der Kontaktperson

#### Alle Antragsformen mit OSTC-Onlineschnittstelle:

Die Bereitstellung der Zertifikatsdatei erfolgt direkt online zur Abholung über die OSTC-Onlineschnittstelle. Eine E-Mail an die Kontaktperson kann dabei zur Kenntnis genommen werden. Die Kontaktperson führt die Funktion zur Abholung der Zertifikatsdatei in der in der verwendeten Entgeltabrechnungssoftware für Arbeitgeber, oder in der Abrechnungssoftware für Leistungserbringer, oder in einem separaten Verschlüsselungstool durch.

## **8. Rechnung und Zustellung**

Nach der Bereitstellung und Veröffentlichung der Zertifikate erhalten die Antragsteller eine Rechnung von der ITSG. Für eine Registrierung als Meldestelle wird ab 2024 eine Registrierungsgebühr berechnet. Die Rechnungen werden üblicherweise im Folgemonat nach Erstellung des Zertifikats versendet.

Die Rechnungen werden gemäß den Antragsdaten entweder an die Firmenadresse, oder an eine optionale Rechnungsadresse, oder optionale E-Mail-Adresse versendet.

Das Zertifikat ist bereits nach der Bereitstellung vor dem Rechnungsversand im elektronischen Datenaustauschverfahren gültig. Die Preisliste wird im Internet auf der Seite [www.trustcenter.info](http://www.trustcenter.info) veröffentlicht.