

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

In einer Einführungsphase wird ab Januar 2023 das neue Antragsverfahren parallel zum Altverfahren starten, so dass in 2023 nur diejenigen das neue Antragsverfahren durchlaufen müssen, die sich aktiv dafür entscheiden. Nach der Einführungsphase wird ab Mitte 2023 nur noch das neue Antragsverfahren unterstützt.

Voraussetzungen für eine Zertifizierung

Die wesentlichen Änderungen sind:

- schriftliche Zertifizierungsanträge werden nicht mehr unterstützt
- eine Übermittlung von Antragsdaten per Fax oder per E-Mail wird nicht mehr unterstützt
- für den Hashcode des Requestschlüssels ist nur noch der Hashalgorithmus SHA256 zulässig
- die Identifizierung und Authentifizierung der Antragsteller erfolgt über ein neues Online-Registrierungsportal
- die Identifizierung der Kontaktperson erfolgt über Postident-Verfahren
- das Trust Center muss durch geeignete Maßnahmen prüfen, ob die Betriebsnummer, gesonderte Absendernummer, Zahlstellennummer, Hochschulnummer oder das Institutionskennzeichen für Leistungserbringer dem Antragsteller zugeordnet werden darf. Dies erfolgt durch einen Freischaltcode, der postalisch an die in einem Verzeichnis hinterlegten Adresse versendet wird.
- Meldestellen, die für mehrere Betriebsnummern oder Institutionskennzeichen Daten übermitteln, müssen sich bei der Beantragung eines Zertifikates mit einer Eigenerklärung für eine Meldestelle anmelden. Eine nachträgliche Anmeldung als Meldestelle ist möglich. Das Formular zur Eigenerklärung für eine Meldestelle finden Sie hier zum [Download](#).

Die OSTC-Onlineschnittstelle des Trust Centers wird weiterhin zur automatisierten Übermittlung der Antragsdaten und des Requestschlüssels angeboten. Somit 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.

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 ITSG Registrierungsportal in einen Web-Browser durchzuführen. Die elektronischen Schlüssel werden dabei parallel in der verwendeten AG-Entgeltabrechnungssoftware, oder in der Abrechnungssoftware für Leistungserbringer, oder in einem separaten Verschlüsselungstool generiert.

- Erstanträge können ohne oder zusätzlich mit OSTC-Onlineschnittstelle durchgeführt werden und dies ist abhängig, ob die verwendete Software die Onlineschnittstelle unterstützt. Für einzelne Teilnehmergruppen sind Online-Anträge über die OSTC-Onlineschnittstelle nicht zulässig, z.B. Datenanahmestellen.
- Bei erneuten Anträgen erfolgt die Beantragung wie bei Erstanträgen, aber ohne OSTC-Onlineschnittstelle. Es wird vorausgesetzt, dass zuvor mindestens ein Zertifikat vom ITSG Trust Center beantragt wurde, oder wenn sich die Kontaktperson ändert.
- Bei einem Online-Folgeantrag über die OSTC-Onlineschnittstelle erfolgt die komplette Antragsabwicklung mit der verwendeten Software 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.

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 Erstantrag oder erneuter Antrag über das Trust Center Registrierungsportal durchzuführen.

Übersicht der Antragsdaten und Antragskomponenten

Die Antragsdaten umfassen folgende Daten:

- Betriebsnummer, Testbetriebsnummer, gesonderte Absendernummer, Hochschulnummer, Zahlstellennummer 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 Betriebsnummer, Testbetriebsnummer, gesonderte Absendernummer, Hochschulnummer, Zahlstellennummer oder Institutionskennzeichen
- optionale Rechnungsadresse für Zusendung einer Rechnung postalisch oder per E-Mail

weitere Antragskomponenten:

- SHA256-Hashcode des Requestschlüssel (z.B. pdf-Datei oder txt-Datei)
- Requestschlüsseldatei (z.B. 12345678.p10)
- optionale Eigenerklärung für Meldestellen (z.B. 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 Aktion erforderlich ist.

1. Anmeldung am Registrierungsportal und Erfassung der Kontaktdaten

Erstanträge oder erneute Anträge ohne OSTC-Onlineschnittstelle:

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 Anmeldedaten notieren, da man sich zur Durchführung der einzelnen Schritte wiederholt anmelden muss.

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

Online-Folgeanträge über die OSTC-Onlineschnittstelle:

Für Online-Anträge muss die verwendete Software die OSTC-Onlineschnittstelle des ITSG-Trust Centers unterstützen.

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

2. Identifizierung der Kontaktperson

Erstanträge oder erneute Anträge ohne OSTC-Onlineschnittstelle:

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

- 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](#)

Nach erfolgreicher Identifizierung mit einem Postident-Verfahren 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 in 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.

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

Das Trust Center muss durch geeignete Maßnahmen die Firmendaten prüfen, ob die Betriebsnummer, Absendernummer, Zahlstellenummer, Hochschulnummer 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 Hochschulnummern und die Zahlstellennummern werden von der ITSG verwaltet.

Der Kontaktperson wird entsprechend der eingegebenen Daten die zugordnete Firmenadresse des Kunden angezeigt. Eine Aktualisierung der Firmenadresse ist im ITSG-Registrierungsportal nicht gestattet und muss bei Bedarf auf separaten Weg der jeweiligen Vergabestelle mitgeteilt werden und der Antrag wird bis zur Klärung und Aktualisierung angehalten.

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 Requestsschlüssels postalisch gesendet.

4. Erfassung der Schlüsseldaten und Generierung der Kundenschlüssel

Erstanträge oder erneute Anträge ohne OSTC-Onlineschnittstelle:

Es wird nun eine GUID-Vorgangsnummer vergeben, die als Referenz zwischen den Antragsdaten im Registrierungsportal und Ihren Schlüsseldaten aus Ihrem System 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 angeboten.

Nachdem alle Antragsdaten im Registrierungsportal erfasst wurden, ist es zur Durchführung dieses Schrittes erforderlich, dass zunächst als Zwischenschritt in der verwendeten AG-Entgeltabrechnungssoftware, 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.

Dazu sind in der separaten Software oder im 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 diese Software oder Verschlüsselungstool führen entweder Sie als Kontaktperson oder eine andere berechtigte Person (z.B. Administrator) dies durch.

Die zu verwendeten Schlüsseldaten umfassen folgende Daten und müssen mit den Antragsdaten im Registrierungsportal übereinstimmen:

- Betriebsnummer, Absendernummer, Zahlstellennummer, Hochschulnummer 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, Absendernummer, Zahlstellennummer, Hochschulnummer oder Institutionskennzeichen ist nicht zulässig. Zulässig sind zusätzliche Angaben im Firmennamen, wie z.B. Ort, Bundesland, oder Name des Dienstleisters, bei dem das Zertifikat im Einsatz ist. Der eigentliche Firmenname darf dabei nur ergänzt werden.

Beim Firmennamen sind 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.

Zu beachten: Die GUID-Vorgangsnummer ist nicht Bestandteil der Schlüsseldaten für das Zertifikat und ist nur als Referenz zusätzlich zu den Schlüsseldaten in der Software oder im Verschlüsselungstool zu erfassen, damit somit ein Bezug zum Vorgang im Registrierungsportal für den Zertifizierungsantrag besteht. Wie zuvor bei den Antragsvarianten beschrieben, gilt dies nur für die Antragformen Erstantrag und erneuter Antrag, nicht aber für Online-Folgeantrag über die OSTC-Onlineschnittstelle des Trust Centers.

Es wird ein manuelles Kopieren und Einfügen der langen GUID-Vorgangsnummer empfohlen, um Schreibfehler oder Zeichendreher zu vermeiden.

Unterstützt die verwendete Software nicht die OSTC-Onlineschnittstelle des Trust Centers, dann ist die GUID-Vorgangsnummer nicht zwingend mit den Schlüsseldaten in der verwendeten Software zu erfassen und die GUID wird dann zur manuellen Übermittlung der Requestdatei und Hashcode 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 Software, oder über ein separates Verschlüsselungstool. Der SHA256-Hashcode des generierten Requestschlüssels soll von der verwendeten Software in eine Datei gespeichert werden (z. B. pdf-Datei, txt-Datei), um bei einem nachfolgenden Antragschritt den Hashcode durch die Kontaktperson auf Übereinstimmung zu prüfen (Beispielsauszug eines Hashcodes: E1D07A4B.....FC781).

Online-Folgeanträge über die OSTC-Onlineschnittstelle:

Für Online-Anträge muss die verwendete Software die OSTC-Onlineschnittstelle des ITSG-Trust Centers unterstützen.

Bei einem Online-Folgeantrag über die OSTC-Onlineschnittstelle werden alle erforderlichen Antragsdaten auch für die Generierung der Kundenschlüssel (private Key und public Key) in der verwendeten AG-Entgeltabrechnungssoftware, 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.

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 (z. B. pdf, txt) manuell an das Trust Center zu übertragen.

Optional kann eine Eigenerklärung für eine Meldestelle (z.B. pdf-Datei) übermittelt werden.

Eine Übermittlung per Fax oder per E-Mail wird nicht mehr unterstützt, daher wird nun ein Upload-Portal angeboten. Über einen Browser ruft die Kontaktperson die Web-Adresse www.itsg-trust.de/zap auf und kann auf der Seite die drei Dateien hochladen. 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.

Online-Folgeanträge über die OSTC-Onlineschnittstelle:

Für Online-Anträge muss die verwendete Software die OSTC-Onlineschnittstelle des ITSG-Trust Centers unterstützen.

Bei einem Online-Folgeantrag über die OSTC-Onlineschnittstelle werden alle erforderlichen Antragsdaten und Komponenten (ohne Eigenerklärung) über die Onlineschnittstelle übermittelt. Der Kunde erhält eine Online-Auftragsnummer vom OSTC-System zurück.

Optional kann eine Eigenerklärung einer Meldestelle (z.B. pdf-Datei) separat übermittelt werden. Meldestellen müssen ab Mitte 2023 mit jedem Zertifizierungsantrag eine Eigenerklärung abgeben. Über einen Browser ruft die Kontaktperson die Web-Adresse www.itsg-trust.de/zap auf und kann auf der Seite die Eigenerklärung hochladen.

6. Kostenpflichtige Beauftragung der Zertifizierung

Die Preisliste und AGB's der ITSG werden im Internet auf der Seite www.trustcenter.info veröffentlicht.

Erstanträge oder erneute Anträge ohne OSTC-Onlineschnittstelle:

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 Freischaltungsbrief mit dem Hashcode auf dem Kundenrechner überein, dann kann die Kontaktperson mit dem zugesendeten Freischaltcode die abschließende Beauftragung im Registrierungsportal aktivieren. Mit der Beauftragung erfolgt die Zertifizierung als kostenpflichtige Dienstleistung der ITSG.

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.

Online-Folgeanträge über die OSTC-Onlineschnittstelle:

Bei einem Online-Folgeantrag 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 die abschließende Auftragsbestätigung wird der Antrag nicht weiterbearbeitet.

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

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

Erstanträge oder Online-Folgeanträge über die OSTC-Onlineschnittstelle:

Die Bereitstellung der Zertifikatsdatei erfolgt direkt online zur Abholung über die OSTC-Onlineschnittstelle. Die Kontaktperson führt dazu die Funktion zur Abholung der Zertifikatsdatei in der in der verwendeten AG-Entgeltabrechnungssoftware, oder in der Abrechnungssoftware für Leistungserbringer, oder in einem separaten Verschlüsselungstool durch.

Alle Antragsformen:

- Zertifikatsdatei zum Download über die Online-Antragsverfolgung im Internet: www.trustcenter.info
- per E-Mail an die E-Mail-Adresse der Kontaktperson

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 in 2023 eine Registrierungsgebühr berechnet. Die Rechnungen werden jeweils in der ersten Monatshälfte für Zertifizierungen aus dem Vormonat erstellt und 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 veröffentlicht.