

Leistungsbeschreibung für Dienstleistungen des Trust Centers der ITSG GmbH

1. Geltung und Änderung der AGB

Die ITSG erbringt Trust Center-Dienstleistungen für ihre Vertragspartner (Kunden) aufgrund der nachfolgenden Leistungsbeschreibung. Allen Vertragsabschlüssen der ITSG liegen, sofern nicht ausdrücklich anders vereinbart, die Allgemeinen Geschäftsbedingungen der ITSG (im folgenden AGB genannt) www.itsg.de/agb zugrunde.

Änderungen der AGB werden mit der Erteilung eines neuen Zertifikates wirksam. Ändert die ITSG die AGB, so kann der Kunde innerhalb eines Monats nach Zugang der Änderungsmitteilung kündigen. Der Vertrag endet in diesem Fall mit dem Ablauf der Gültigkeitsdauer des Zertifikats (s. Ziffer 3) oder der Sperrung des Zertifikats (s. Ziffer 6). Die ITSG weist den Kunden auf dieses Kündigungsrecht hin.

2. Vertragsschluss

In Abänderung der Ziffer 2 der AGB gelten die nachfolgenden Regelungen:

Der Vertrag kommt entweder aufgrund einer Online-Registrierung oder einer elektronischen Beantragung über die Online-Schnittstelle des Trust Centers in Verbindung mit einer vom Trust Center zugelassenen Software zustande.

Der Kunde stellt zur Beantragung einen öffentlichen Schlüssel bereit, den das Trust Center mittels Zertifikats authentifiziert. Damit sich das Trust Center von der Authentizität des öffentlichen Kundenschlüssels überzeugen kann, hat der Kunde dem Antrag einen Ausdruck des Schlüssels (Hash-Wert oder Fingerprint des Schlüssels) beizufügen. Detaillierte Informationen zu den Teilnehmerschlüsseln sind im Dokument „Security Schnittstelle für das Gesundheits- und Sozialwesen“ beschrieben.

Das Trust Center muss durch geeignete Maßnahmen prüfen, ob die Betriebsnummer, Absendernummer, oder Zahlstellennummer dem Antragsteller zugeordnet werden darf. Dies erfolgt durch einen Freischaltcode, der postalisch an die in der Betriebsstättendatei der Bundesagentur für Arbeit oder in den Verzeichnissen für Absendernummern und Zahlstellennummern hinterlegte Adresse versendet wird.

Auch im Leistungserbringerverfahren erfolgt eine Prüfung auf Zuordnung zum Institutionskennzeichen (IK) mit einem Freischaltcode, der postalisch an die in dem Verzeichnis der ArGe IK hinterlegte Adresse versendet wird.

Die Identität des vom Kunden benannten Ansprechpartners muss bei der Antragstellung nachgewiesen werden. Bei einer Online-Registrierung erfolgt die Identitätsprüfung mit einem Postident-Verfahren. Bei reiner elektronischer Beantragung ist eine elektronische Signatur mit einem gültigen Zertifikat über die Online-Schnittstelle des Trust Centers bereit zu stellen. Das Trust Center ist berechtigt, die Prüfung der Identität des Ansprechpartners durch Registrierungsstellen (z. B. Verwaltungsstellen der Gesetzlichen Krankenversicherung) durchführen zu lassen. Eine Überprüfung der vom Kunden genannten Firmendaten (z. B. Firmenname oder Anschrift) erfolgt nicht.

Die ITSG behält sich vor, nicht abgeschlossene Anträge nach einer Frist von 120 Tagen, beginnend nach dem letzten Kontakt mit dem Kunden, alle eingesendeten Antragsinformationen fachgerecht zu vernichten.

3. Gültigkeitsdauer von Zertifikaten

Sofern nicht Rechtsvorschriften zwingend andere Fristen vorschreiben, beträgt die Gültigkeitsdauer der Zertifikate

- ⇒ 3 Jahre für alle Teilnehmer des Datenaustausches mit Arbeitgebern
- ⇒ 3 Jahre für alle Teilnehmer des Datenaustausches mit Leistungserbringern
(einzelabgebende Leistungserbringer, Annahmestellen der GKV, Krankenkassen und deren
Verwaltungsstellen, kommerzielle Abgabestellen (Rechenzentren), Krankenhäuser und stationäre
Reha-Einrichtungen)

Bei der Erteilung von Zertifikaten für andere als die hier aufgeführten Gruppen wird, das Trust Center die Gültigkeitsdauer rechtzeitig festlegen und in geeigneter Weise bekanntgeben. Mit dem Ablauf der Gültigkeitsdauer des Zertifikates erlischt die Authentifikation des öffentlichen Schlüssels.

Bereits vor Ablauf der Gültigkeitsdauer des Zertifikats wird das Trust Center auf Antrag ein neues Zertifikat erzeugen. Für dieses neue Zertifikat muss der Kunde einen neuen öffentlichen Schlüssel und die Antragsunterlagen bereitstellen, die gemäß Ziff. 2 neu zu generieren sind.

4. Leistungen des Trust Centers, Leistungsstörungen

Das Trust Center registriert jeden Kunden unter einem eindeutigen Namen, prüft die Eindeutigkeit seines öffentlichen Schlüssels und bestätigt die Zuordnung des Schlüssels zum Kunden durch ein Zertifikat. In Ausnahmefällen kann auch die Schlüsselgenerierung durch das Trust Center erfolgen. Die Zertifikate werden in öffentlichen Verzeichnissen bereitgestellt, sodass die Zertifikate aller Teilnehmer abgerufen werden können, soweit die technischen Voraussetzungen hierfür beim Kunden gegeben sind. Soweit der Kunde bereits vor Ablauf der Gültigkeit ein neues Zertifikat beantragt, wird unabhängig von der Gültigkeit des bestehenden Zertifikats das Neue an dem Tag der Erstellung veröffentlicht. Nach Ablauf ihrer Gültigkeit werden Zertifikate aus den öffentlichen Verzeichnissen entfernt.

Für seine Kunden stellt das Trust Center bei Bedarf auch die öffentlichen Schlüssel von Kommunikationspartnern bereit, deren Zertifizierung durch andere Trust Center vorgenommen wurde, sofern die Voraussetzungen hierfür gegeben sind.

Neben den gültigen Zertifikaten stellt das Trust Center in den öffentlichen Schlüsselverzeichnissen auch Sperrlisten bereit, in denen sämtliche gesperrte Zertifikate enthalten sind, solange die im Zertifikat ausgewiesene Gültigkeitsdauer noch nicht abgelaufen ist. Diese Sperrlisten werden mindestens einmal monatlich herausgegeben und enthalten neben den gesperrten Zertifikaten auch eine Information über den spätesten Ausgabetag der nächsten Sperrliste. Gesperrte Zertifikate werden darüber hinaus unverzüglich aus den anderen Teilen der öffentlichen Schlüsselverzeichnisse entfernt.

Die öffentlichen Schlüsselverzeichnisse sind grundsätzlich 24 Stunden, 7 Tage die Woche verfügbar. Die Überwachung der Funktionalität und die Behebung von Fehlern erfolgt jedoch nur während der normalen Servicezeiten des Rechenzentrums. Zeitweise Störungen der Abrufbarkeit von Zertifikaten und Sperrlisten können sich aus Gründen höherer Gewalt oder erforderlicher Maßnahmen (z. B. Reparaturen) ergeben. Dies gilt auch für Störungen im Bereich der Fernmeldeanlagen der Deutschen Telekom AG. Das Trust Center wird alle zumutbaren Anstrengungen unternehmen, Störungen baldmöglichst zu beheben.

5. Pflichten des Kunden

Jeder Kunde ist selbst dafür verantwortlich, dass sein privater Schlüssel vor Missbrauch durch Unbefugte geschützt wird. Der Schlüssel ist durch ein Passwort oder eine persönliche Identifikationsnummer (PIN) zu sichern, die nur dem Kunden bekannt sein darf.

Bei Preisgabe oder Verdacht der Preisgabe von Passwort oder PIN sind diese unverzüglich zu ändern; bei Kompromittierung des privaten Schlüssels ist unverzüglich die Sperrung des Zertifikats zu veranlassen.

Der Kunde hat unverzüglich jede Änderung seines Namens, seiner Firma, seines Wohn- oder Geschäftssitzes bzw. seiner Rechnungsanschrift, seiner Rechtsform und seines Identifikationskennzeichens mitzuteilen. Diese Pflicht endet nach der vollständigen Zahlung der Rechnung der ITSG. Änderungen der Betriebsnummer oder des Institutionskennzeichens sowie das Ausscheiden des verantwortlichen Ansprechpartners sind während der gesamten Gültigkeit des Zertifikats unverzüglich schriftlich anzuzeigen.

Es besteht generell die Hol-Schuld für alle vom Trust Center veröffentlichten Verzeichnisse, die für den verschlüsselten Datenaustausch benötigt werden.

6. Sperrung von Zertifikaten

Das Trust Center kann von ihm ausgegebene Zertifikate sperren, wenn

- ⇒ der Kunde dies beantragt. Der Zeitpunkt der Sperrung wird durch das Trust Center festgelegt. Die Sperrung zu einem gewünschten Termin kann das Trust Center nicht berücksichtigen;
- ⇒ es davon Kenntnis erlangt, dass das Zertifikat unrichtige oder nicht mehr zutreffende Angaben enthält, z. B. Zuteilung einer neuen Betriebsnummer bzw. Identifikationskennzeichen oder Ausscheiden des vom Kunden benannten Ansprechpartners;
- ⇒ es davon Kenntnis erlangt, dass der Kunde bei Antragstellung unrichtige oder falsche Angaben (z. B. falsche Betriebsnummer) gemacht hat;
- ⇒ Tatsachen die Annahme rechtfertigen, dass das Zertifikat gefälscht ist oder nicht hinreichend fälschungssicher ist;
- ⇒ der begründete Verdacht besteht, dass der private Schlüssel des Teilnehmers kompromittiert ist (z.B. eine entsprechende Mitteilung des Kunden);
- ⇒ ein Dritter, der am Datenaustausch beteiligt ist, eine Kompromittierung eines Kunden mitteilt, behält sich das Trust Center die unverzügliche Sperrung vor. Das Trust Center wird sich im Regelfall vor der Sperrung um eine Klärung mit dem Kunden bemühen;
- ⇒ der Kunde mit der Zahlung der Vergütung für die Zertifizierung trotz Mahnung im Rückstand ist.

Die Aufhebung einer Sperrung ist nicht möglich. Der Kunde kann jedoch ein neues Zertifikat beantragen, sofern das Trust Center das Vertragsverhältnis nicht aus wichtigem Grund kündigt. Soweit das Trust Center den Grund für die Sperrung zu vertreten hat, wird das neue Zertifikat kostenfrei generiert und bereitgestellt. Eine Erstattung von Vergütungen des Kunden (auch anteilig) erfolgt bei berechtigter Sperrung nicht.

7. Dauer des Vertragsverhältnisses, Kündigung

Der Vertrag wird auf unbestimmte Zeit geschlossen und kann von beiden Vertragspartnern jederzeit schriftlich zum Ende der Gültigkeitsdauer des Zertifikats gekündigt werden.

Das Recht zur fristlosen Kündigung bleibt unberührt. Für das Trust Center liegt ein wichtiger Grund insbesondere dann vor, wenn der Teilnehmer mit Zahlung der Rechnungsbeträge in Verzug ist oder wiederholt seine Pflichten aus Ziffer 5 verletzt.

Eine Erstattung von Vergütungen des Kunden (auch anteilig) erfolgt nicht.

8. Vergütung, Zahlungen

Die Leistungen des Trust Centers werden dem Kunden zu den bei der Antragstellung bekannt gegebenen Tarifen in Rechnung gestellt. Im Übrigen gelten die Ziffer 5.1, 5.2 und 5.3 der AGB der ITSG.

Bei einer nachträglichen Änderung der Rechnungsadresse erhebt die ITSG eine pauschale Servicegebühr gemäß der veröffentlichten Preisliste.

9. Vertraulichkeit

Die dem Trust Center zum Zwecke der Zertifizierung übermittelten Daten des Teilnehmers werden vertraulich behandelt; davon ausgenommen sind die in Zertifikaten bzw. öffentlichen Verzeichnissen enthaltenen Informationen über den Teilnehmer.

10. Haftung

Die Haftung wegen Verletzung von Pflichten dieses Vertrags richtet sich in Abweichung Ziffer 8 der AGB nach folgenden Bestimmungen:

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 jedoch bis zu 5.000,00 € je Schadenfall.

11. Gerichtsstand

Gerichtsstand ist der Sitz der ITSG GmbH 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.

12. Schlussbestimmungen

Ist eine der Regelungen nichtig, so bleiben die übrigen Bestimmungen gültig. Die Parteien verpflichten sich, unverzüglich die nichtige Bestimmung durch eine ihrer wirtschaftlich möglichst nahekommenen, rechtlich zulässigen Bestimmung zu ersetzen.