Allgemeine Vertragsbedingungen

V-PKI Trust-Center der Südwestfalen-IT

Erstellt durch:
Norbert Jung
Sonnenblumenallee 3
58675 Hemer

IHR KONTAKT

Auskunft erteilt:	Servicedesk
Durchwahl:	+49 271 30 321-0
Zentrale:	+49 271 30 321-0
Email:	servicedesk@sit.nrw

Inhalt Seite

1. Allgemeines ... 3

2. Leistungsbeschreibung ... 3

2.1. Allgemeines ... 3

2.2. Konformität und Standards ... 4

2.3. Beantragung ... 4

2.4. Widerruf und Sperrung von Zertifikaten ... 4

2.5. Technische Voraussetzungen ... 4

2.6. Support ... 5

2.7. Leistungsabgrenzung/ Mitwirkungspflichten ... 5

2.8. Lokale Registrierungsstelle ... 5

3. Kosten ... 5

4. Vertragliches ... 6

4.1. Laufzeit ... 6

5. Gültigkeit der allgemeinen Vertragsbedingungen ... 6

6. Salvatorische Klausel ... 6

1. Allgemeines

Die Südwestfalen-IT stellt die Dienstleistung eines Zertifizierungsdiensteanbieters unter der PKI-1-Verwaltung des BSI (**V-PKI**) für Mitarbeiter von Dienststellen aus dem Bereich der öffentlichen Verwaltung zur Verfügung.
Ebenso sind Dritte als mögliche Kunden angesprochen, die mit den genannten Dienststellen in regelmäßigem Kontakt stehen und Zertifikate im Rahmen ihrer Kommunikation mit diesen Dienststellen nutzen möchten. Die ausgestellten Zertifikate sind personalisiert.

Dritte im Sinne der Nutzungsbedingungen sind jedoch **nicht** Privatpersonen.

Die von der Certificate Authority (CA) der Südwestfalen-IT als Zertifizierungsdiensteanbieter innerhalb der V-PKI ausgegebenen Zertifikate dienen ausschließlich den in der veröffentlichten Policy (https://cas.citkomm.de/dokument/CertificatePolicy_aktuell.pdf) angegebenen Zwecken. Anderweitige Nutzungen bedingen eine gesonderte vertragliche Regelung mit der Südwestfalen-IT.

Alle Leistungen des Trust-Centers der Südwestfalen-IT sind verbindlich geregelt in der veröffentlichten Policy (https://cas.citkomm.de/dokument/CertificatePolicy_aktuell.pdf). Hierzu gehört insbesondere die sorgfältige Authentifizierung der Zertifikatsinhaber. Die Bedingungen der ausgestellten Zertifikate entsprechen der Stufe „fortgeschrittene Signatur". Durch die Südwestfalen-IT ausgestellte Zertifikate sind daher als vertrauenswürdig einzustufen.

Die Südwestfalen-IT ist als Zwischenzertifizierungsstelle zur V-PKI in einer dreistufigen Hierarchie eingebunden. Die oberste Stufe stellt das **BSI** (Bundesamt für Sicherheit in der Informationstechnik) als Wurzelzertifizierungsstelle dar. Die **Südwestfalen-IT**, als Zwischenzertifizierungsstelle, stellt die zweite Stufe der Hierarchie dar. Der **Zertifikatsnehmer** repräsentiert die dritte Stufe.

Anschrift des Zertifizierungsdiensteanbieters:

Südwestfalen-IT
Trust-Center
Sonnenblumenallee 3
58675 Hemer
Tel.- Hotline: 0271 303210
Fax: 0271 303211010
E-Mail: pki@sit.nrw

Link zur Beantragung eines Zertifikats: https://cas.citkomm.de/html/main.php

2. Leistungsbeschreibung

2.1. Allgemeines

1. Die Südwestfalen-IT stellt Zertifikate aus für die Nutzung
    a. der digitalen Signatur / Verschlüsselung von E-Mails,
    b. der digitalen Signatur / Verschlüsselung von Dokumenten,
    c. der Authentisierung von Online-Verbindungen,
    d. der Authentisierung von Personen gegenüber Systemen,
    e. der Authentisierung von Personen.
2. Die Südwestfalen-IT unterhält einen Verzeichnisdienst (LDAP) im Internet und veröffentlicht die durch die Südwestfalen-IT ausgestellten Zertifikate
3. Die Zertifikate haben eine Laufzeit von drei Jahren. Die Laufzeit eines Zertifikats ist nicht verlängerbar. Folgezertifikate sind durch Neuantrag zu generieren.

4. Die Bedingungen zur Ausstellung und zum Betrieb der Certificate Authority (CA) der Südwestfalen-IT und den unter der CA ausgestellten Zertifikaten sind in den Sicherheitsleitlinien (Certificate Policy) verbindlich dokumentiert. Die Sicherheitsleitlinien sind unter https://cas.citkomm.de abrufbar.

2.2. Konformität und Standards

1. Die Zertifikate sind interoperabel mit den internationalen Standards X.509, PKIX, PKCS, S/MIME und LDAP und entsprechen den Anforderungen an fortgeschrittene Signaturen nach dem Signaturgesetz.
2. Die Südwestfalen-IT stellt sicher, dass jedes Zertifikat durch eine eindeutige Kennung im Common Name (CN) des Zertifikats gekennzeichnet ist.

2.3. Beantragung

1. Die Beantragung eines Zertifikates erfolgt von einem Internet-fähigen PC über das Online-Antragsverfahren der SIT-CA. Die gesamte weitere technische Beantragung und Verwaltung von Zertifikaten erfolgt automatisiert über das Web-Portal und E-Mail.
2. Die Überprüfung der Identität des Antragstellers sowie dessen Angaben im Zertifikatsantrag werden durch die Südwestfalen-IT oder eine von ihr akkreditierte lokale Registrierungsstelle (LRA) vorgenommen. Ferner kann gegen Aufpreis das POSTIDENT®-Verfahren der Deutschen Post AG sowie das BehördenIDENT-Verfahren zur Identitätsfeststellung genutzt werden. Eine persönliche Vorstellung ist zwingend erforderlich.
3. Die Registrierungsstelle der Südwestfalen-IT oder die zuständige LRA stellen sicher, dass die im Zertifikat enthaltenen Angaben zum Namen, Vornamen, Dienststelle und E-Mail sowie der öffentliche Teil eines Schlüsselpaares, der im Browser des Antragstellers erzeugt wurde, zum Zeitpunkt der Beantragung eines Zertifikates zum Antragsteller gehören.
4. Zertifikate werden nicht auf juristische Personen ausgestellt. Gleichwohl ist die Ausstellung von nicht personenbezogenen Gruppenzertifikaten möglich. (s.o.)
5. Bei der Ausstellung von Gruppenzertifikaten ist eine schlüsselverantwortliche Person zu benennen und bei der Beantragung anzugeben. Zertifikate für Gruppen oder Server werden nicht im Standard-Online-Dialog durch den Endbenutzer beantragt. Der erweiterte Online-Dialog für die Beantragung wird bei Bedarf durch die Südwestfalen-IT bereitgestellt.
6. Zertifikate werden nicht auf Pseudonyme ausgestellt.
7. Der Antragsteller erhält an die im Zertifikat angegebene E-Mail-Adresse eine E-Mail mit den notwendigen Angaben zur Installation und Aktivierung seines ausgestellten Zertifikats.

2.4. Widerruf und Sperrung von Zertifikaten

1. Ein Zertifikat kann auf Antrag durch die Südwestfalen-IT gesperrt werden.
2. Eine Sperrung kann telefonisch, per E-Mail oder per Fax an den Kundenservice der Südwestfalen-IT beantragt werden. Die Berechtigung zur Beantragung einer Sperrung ist bei dem Sperrauftrag zu belegen.
3. Die Südwestfalen-IT erstellt Sperrlisten (certificate revocation list) für widerrufene Zertifikate und veröffentlicht diese über den Verzeichnisdienst im Internet.
4. Die Südwestfalen-IT als CA sperrt ein Zertifikat bei begründetem Verdacht des Missbrauchs.
5. Ein gesperrtes Zertifikat kann nicht wieder entsperrt werden.
6. Der Zertifikatseigner verpflichtet sich, bei Verlust, Diebstahl oder Bruch der Verschlüsselung seines Zertifikates unverzüglich den Sachverhalt anzuzeigen und das Zertifikat sperren zu lassen.
7. Die Südwestfalen-IT als CA verpflichtet sich, bei Verlust, Diebstahl oder Bruch der Verschlüsselung des CA-Zertifikates unverzüglich den Sachverhalt anzuzeigen und alle mit diesem CA-Zertifikat ausgestellten Zertifikate sperren zu lassen.

2.5. Technische Voraussetzungen

1. Für die Beantragung eines Zertifikats sind ein Internetzugang und ein Browser notwendig.

2. Das Schlüsselpaar wird beim Antragsverfahren aus dem betreffenden Browser generiert und im lokalen Zertifikatsspeicher des angemeldeten Benutzers auf dem PC hinterlegt. Der öffentliche Teil des Schlüssels wird über das Antragsverfahren zur Zertifizierungsstelle der Südwestfalen-IT übertragen und dort weiterverarbeitet. Nach erfolgreicher Ausstellung wird dem Anwender der zertifizierte öffentliche Teil zum Download angeboten. Die Zusammenführung des Antrags mit dem durch die Südwestfalen-IT erteilten Zertifikat muss auf demselben PC und unter demselben Benutzerprofil wie die Antragsstellung erfolgen.
3. Die Südwestfalen-IT testet die Kompatibilität gängiger Produkte mit den ausgestellten Zertifikaten.

2.6. Support

1. Die Südwestfalen-IT stellt einen Second Level Support über das UHD der Südwestfalen-IT zur Verfügung. Zugangsberechtigt für den Support sind die als LRA benannten Personen oder benannte IT-Verantwortliche des Kunden.

2.7. Leistungsabgrenzung/ Mitwirkungspflichten

1. Der Anwender ist zu einer sorgfältigen Beantragung verpflichtet. Eine Veränderung der Zertifikatsinhalte ist nach der Zertifikatserstellung nur durch Sperrung des Zertifikates und kostenpflichtige Neuausstellung möglich.
2. Die verantwortliche Nutzung und der Schutz gegen Missbrauch des Zertifikates liegen in der ausschließlichen Verantwortung des Kunden.
3. Die Erstellung einer Sicherheitskopie des Zertifikates inkl. des privaten Schlüssels und deren Verwahrung liegt in der ausschließlichen Verantwortung des Kunden
4. Die Südwestfalen-IT speichert keinerlei Zertifikatskopien und unterhält auch keine Wiederherstellungsmechanismen, um gelöschte oder beschädigte private Schlüssel wiederherzustellen. Dokumente, die mit einem solchen Schlüssel verschlüsselt wurden, können nicht mehr entschlüsselt werden.
5. Der Antragsteller ist verpflichtet, einen neuen, kostenpflichtigen Zertifikatsantrag zu stellen, wenn der private Schlüssel nicht mit dem ausgestellten Zertifikat zusammengeführt werden kann. Dieser Umstand ist anzuzeigen. Das betroffene Zertifikat ist zu sperren.

2.8. Lokale Registrierungsstelle

1. Die Südwestfalen-IT stellt eine Registrierungsstelle (Registration Authority – RA) zur Verfügung, um Antragsteller für Zertifikate zu authentifizieren. Die Identitätsprüfung ist kostenfrei, sofern sie in den Räumen der Südwestfalen-IT erfolgt. Für eine Authentifizierung beim Kunden wird ein Vor-Ort-Einsatz gegen eine Aufwandspauschale angeboten. Ein pauschalierter Vor-Ort-Einsatz ist jeweils auf die Dauer der effektiven Authentifizierung beschränkt.
2. Als weitere Option kann der Identifikationsdienst POSTIDENT® der Deutschen Post AG genutzt werden, bei dem sich der Anwender bei einer Postfiliale persönlich vorstellt und über Ausweisvorlage seine Identität bestätigen lässt. Ebenfalls möglich ist die Nutzung des BehördenIDENT-Verfahrens.
3. Kundenverwaltungen können auf Wunsch die Funktion einer lokalen Registrierungsstelle (LRA) gegenüber Antragstellern übernehmen. Hierzu sind der Abschluss und die Einhaltung eines entsprechenden Akkreditierungsvertrages mit der Südwestfalen-IT erforderlich. Zusätzlich ist eine kostenpflichtige Einweisung der die Aufgaben wahrnehmenden Personen obligatorisch.

3. Kosten

1. Je Zertifikatsausstellung wird ein einmaliges Entgelt gemäß der jeweils aktuellen Preisliste erhoben.
2. Zusätzliche Entgelte fallen im Einzelfall für die Authentifizierung von Antragstellern Vor-Ort, mittels POSTIDENT® Dienst, BehördenIDENT, Zertifikatsgenerierung durch die Südwestfalen-IT, Unterweisung der LRA, First Level Support sowie ggf. sonstiger Dienstleistungen gemäß der aktuellen Preisliste an.

3. Die Kostenpflicht entsteht mit der Freigabe eines Antrags durch eine LRA. Sofern POSTIDENT® oder BehördenIDENT genutzt wird, entsteht die Kostenpflicht mit Nutzung dieses Verfahrens.
4. Die Abrechnung der erbrachten Leistungen erfolgt spätestens jährlich, je nach Anzahl der beantragten Zertifikate.

4. Vertragliches

4.1. Laufzeit

1. Die Vertragslaufzeit ist regelmäßig an die Laufzeit des Zertifikates gebunden. Sie endet automatisch mit Ablauf des Zertifikates.
2. Der User wird per E-Mail rechtzeitig vor Laufzeitende seines Zertifikates über das bevorstehende Laufzeitende informiert. Die E-Mail wird an die im Zertifikatsantrag hinterlegte E-Mail-Adresse gesandt.

5. Gültigkeit der allgemeinen Vertragsbedingungen

Es gilt die jeweils aktuelle Fassung der Vertragsbestimmungen. Die SIT ist berechtigt, einseitig ohne vorherige Konsultation der Kunden und Nutzer der PKI neue Prozesse, Inhalte, Betriebs-, Service- oder Supportzeiten zum Bestandteil dieser Bestimmungen zu machen. Dies kann z.B. aus technischen Gründen erforderlich werden. Sofern und sobald neue Regelungen erforderlich werden, gelten diese ab Veröffentlichung auf dieser Seite und ersetzen die in diesem Dokument dargestellten.

6. Salvatorische Klausel

Rechte und Pflichten aus dieser Absichtserklärung werden durch Formumwandlung bzw. Neustrukturierungen der Betriebsorganisation der Parteien, auch wenn diese zur Ausgliederung von Betriebsteilen oder zur Schaffung neuer Rechtspersönlichkeiten führen, nicht berührt.

Sollte eine Regelung dieser Bestimmungen unwirksam sein, wird die Wirksamkeit der übrigen Regelungen dadurch nicht berührt. Die Parteien werden die unwirksame Regelung unverzüglich durch eine solche wirksame ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Regelung am nächsten kommt.

Auf diese Bestimmungen findet deutsches Recht Anwendung. Gerichtsstand ist das für die SIT zuständige Gericht.