Certificate Policy (CP)

für die
zertifikatsbasierte Schlüsselinfrastruktur
(Public Key Infrastructure - PKI)
des Trust-Centers
der Südwestfalen-IT

Erstellt durch:
Norbert Jung
Sonnenblumenallee 3
58675 Hemer

IHR KONTAKT

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

Inhalt Seite

Dokumentenhistorie:

Datum	Version	Änderungen	Autor
01.03.2005	0.1	Erster Entwurf	Marco Lazik
01.07.2005	0.2	Abschluss Diplomarbeit	Marco Lazik
30.01.2005	1.0	Überarbeitung für die Produktionsaufnahme	Peter Gittner (federführend)
31.01.2006	1.1	Anpassung des Layouts	Peter Gittner
11.05.2006	1.2	Überarbeitung, Kommentare des BSI	Norbert Jung
19.06.2006	1.2.1	4.2	Norbert Jung
05.02.2007	1.2.2	GFDL lizensiert	Norbert Jung
12.10.2007	1.3.0	POSTIDENT® BASIC	Norbert Jung
29.10.2007	1.4.0	Gruppenzertifikate	Norbert Jung
20.10.2009	1.4.1	Laufzeit max. 3 Jahre, Signaturkarte einbinden	Norbert Jung
17.12.2009	1.4.2	Kommentare BSI	Norbert Jung
07.04.2014	1.4.3	Anpassung wg. BSI [CP_Neu]	Norbert Jung
28.9.2017	1.5.0	Anpassung wg. SUB-CA, redaktionelle Änderungen	Norbert Jung
27.10.2017	1.5.1	redaktionelle Änderungen	Norbert Jung
24.01.2022	1.5.2	redaktionelle Anpassung auf SIT Südwestfalen-IT (SIT) als Rechtsnachfolger der KDVZ Citkomm	Norbert Jung

1. Einleitung

Die Südwestfalen-IT stellt die Dienstleistung eines Zertifizierungsdiensteanbieters der PKI-1-Verwaltung für Institutionen aus dem Bereich der öffentlichen Verwaltung zur Verfügung.
Die vorliegende Sicherheitsleitlinie (Policy) gilt nur für Zertifikate, die von der Südwestfalen-IT als Zertifizierungsdiensteanbieter der PKI-1-Verwaltung herausgegeben werden.
Die von der Südwestfalen-IT als Zertifizierungsdiensteanbieter der PKI-1-Verwaltung ausgegebenen Zertifikate dienen ausschließlich dem in dieser Policy angegebenem Zweck. Anderweitige Nutzungsarten erfordern eine Anpassung der Sicherheitsleitlinie.
Die vorliegende Sicherheitsleitlinie bildet den Rahmen für die Einschätzung der Vertrauenswürdigkeit der von der Südwestfalen-IT als Zertifizierungsdiensteanbieter für die PKI-1-Verwaltung ausgegebenen Zertifikate. Der Aufbau orientiert sich an der Sicherheitslinie der Wurzelzertifizierungsinstanz der Verwaltung [CPPCA] und lehnt sich damit an den Empfehlungen des RFC 3647 [RFC3647] an, welche das RFC 2527 [RFC2527] abgelöst hat.
Diese Sicherheitsleitlinie ist für alle beteiligten Personen des Zertifizierungsdiensteanbieters bindend und deren Anerkennung und Einhaltung Voraussetzung für die Erteilung eines Zertifikates.

2. Überblick

Die PKI der Südwestfalen-IT basiert auf den Festlegungen in dem Dokument „Technische Grundlagen der Wurzelzertifizierungsstelle Formate und Protokolle nach MTTv2, Version 2.0“. Dieses ermöglicht die Interoperabilität mit den internationalen Standards X.509, PKIX, PKCS, S/MIME und LDAP.

2.1. Zertifizierungshierarchie

Die Architektur der Südwestfalen-IT PKI wird im Folgenden dargelegt. Die CA der Südwestfalen-IT PKI-1-Verwaltung ist eine Hierarchieebene unter dem Wurzelzertifizierungsdiensteanbieter (nachfolgend auch: PCA) angesiedelt.
Als Zertifizierungsdiensteanbieter erhält die Südwestfalen-IT ein von der Wurzelzertifizierungsebene signiertes Zertifikat. Die Endanwender werden durch die Zertifizierungsstelle der Südwestfalen-IT eingebunden und bilden die unterste Ebene der Zertifizierungshierarchie.
Es werden auf Antrag Sub-CAs[1] von der CA der Südwestfalen-IT zertifiziert welche wiederum eine eigene Hierarchie innerhalb der Verwaltungs-PKI begründen.

2.2. SUB-CA

SUB-CA’s sind verpflichtet, eine eigene Policy vorzulegen und die Vorgaben der Wurzelzertifizierungsstelle (BSI) in den „Sicherheitsleitlinien der Wurzelzertifizierungsstelle der Verwaltung[2]“ gemachten Ausführungen umzusetzen.

Die Südwestfalen-IT betreibt im Rahmen ihrer PKI für die Ausstellung von Endbenutzerzertifikaten eine zweistufige Registrierungsstelle (Registration Authority: RA). Teilaufgaben der RA werden delegiert. Es existieren deshalb mehrere lokale Registrierungsstellen (Local Registration Authority: LRA). Jeder Kunde der Südwestfalen-IT aus der öffentlichen Verwaltung kann eine LRA-Instanz besitzen. Jede LRA kann mehrere, jedoch mindestens einen lokalen Ansprechpartner besitzen. Die Identifizierung und
Authentisierung der Endbenutzer[3] wird von der LRA durch die lokalen Ansprechpartner durchgeführt.
Die Schlüsselerzeugung der Zertifikatsnehmer erfolgt regelmäßig über den Browser auf den Client-Rechnern bei der Zertifikatsbeantragung. Der Zertifikatsnehmer wird bei der Beantragung des Zertifikats darauf hingewiesen, dass auf den Client-Rechnern eine Grundsicherheit durch den Einsatz eines Viren-Scanners gewährleistet sein muss.

[1] Sub-CA, Eine in der Hierarchie unter der Südwestfalen-IT CA angesiedelte CA
[2] Auch Ergänzungen und Änderungen dazu, Version 1.1 vom 29.1.2013, [siehe CP_Neu]
[3] Endbenutzer ist auch der Schlüsselverantwortliche im Fall von Gruppen-/Funktions-/Serverzertifikaten

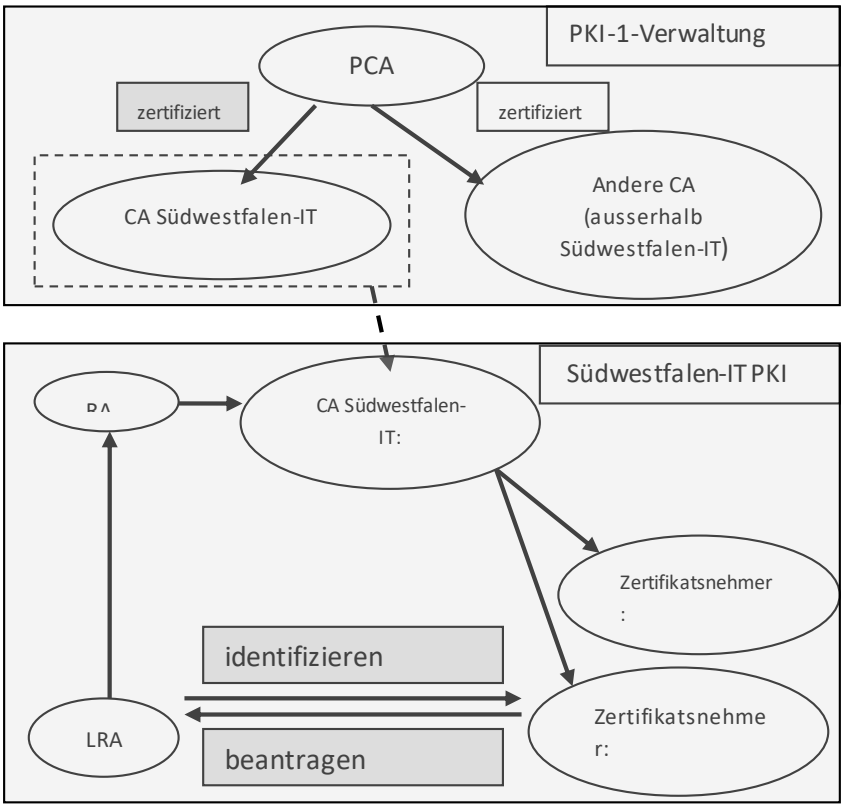

Abbildung 1: Zertifizierungshierarchie

Eine Kreuzzertifizierung[4] mit anderen CAs ist nach der PKI-1-Verwaltungspolicy [CPPCA] nicht erlaubt. Eine Kreuzzertifizierung darf nur von der PCA-1-Verwaltung vorgenommen werden, untere Hierarchieebenen werden somit gleichzeitig mit kreuzzertifiziert

2.3. Verzeichnisdienst (LDAP)

Die Südwestfalen-IT stellt die von ihr ausgestellten Zertifikate und Sperrlisten mittels eines öffentlichen LDAP-Dienstes bereit. Die hohe Verfügbarkeit wird durch die Südwestfalen-IT sichergestellt. Der Verzeichnisdienst ist aus dem Internet über die URL **http://cas.citkomm.de** erreichbar.

2.4. Kosten

Der Zertifizierungsdienst wird Kunden der Südwestfalen-IT aus der öffentlichen Verwaltung und deren Mitarbeitern zur Verfügung gestellt. Ebenso werden Dritte zertifiziert, die mit den Verwaltungen zur Aufgabenerfüllung elektronisch kommunizieren. Kosten für die Ausstellung von Zertifikaten werden über Kundenverträge geregelt.

2.5. Anwendungsbereich

Der Zertifizierungsdienst erstellt auf Antrag Zertifikate für die Mitarbeiter aus der öffentlichen Verwaltung als Kunde der Südwestfalen-IT. Voraussetzung für die Erstellung eines Zertifikates ist die Anerkennung und die Einhaltung der Verpflichtungen dieser Policy.

[4] Kopplung zweier unabhängiger Infrastrukturen mittels gegenseitiger Zertifizierung

Die erstellten Zertifikate dienen im Rahmen dieser Sicherheitsrichtlinie der Verschlüsselung und Signierung, der Authentisierung sowie der Nutzung in den folgenden Bereichen:

- der digitalen Signatur / Verschlüsselung von Emails,
- der digitalen Signatur / Verschlüsselung von Dokumenten,
- der Authentisierung von Online-Verbindungen,
- der Authentisierung von Personen gegenüber Systemen,
- der Authentisierung von Personengruppen gegenüber Systemen,
- der Authentisierung von Personen
- der Authentisierung von IT-Prozessen und Programm-Code

2.6. Personelle Unterstützung

Die folgenden Angaben geben den Stand vom 29.09.2017 wieder.

2.7. Organisationsstruktur

Der Dienst zur Zertifizierung wird durch die Südwestfalen-IT betrieben.

2.8. Ansprechstelle des Zertifizierungsdiensteanbieters

Südwestfalen-IT
Abteilung Trust-Center
Sonnenblumenallee 3
58675 Hemer
Call-Center der Südwestfalen-IT:
Tel.: +49 271 30 321-0, E-Mail: pki@sit.nrw

3. Allgemeine Bestimmungen

Der Zertifizierungsdiensteanbieter Südwestfalen-IT übernimmt die folgenden Verpflichtungen.

1. Der Zertifizierungsdiensteanbieter Südwestfalen-IT vereinbart mit der Wurzelzertifizierungsstelle, nachfolgend auch PCA der Verwaltung (PCA-1-Verwaltung) genannt, einen innerhalb der PKI eindeutigen Namen. Der vereinbarte Name ist für jedes durch die PCA der Verwaltung ausgestellte Zertifikat eindeutig und folgt dem in der Certification Practice Statement (CPS) [CPS] beschriebenen Namenskonzept.
2. Die Südwestfalen-IT verpflichtet sich zur Einhaltung und Erfüllung der in den Sicherheitsleitlinien der PKI-1-Verwaltung und der in den Sicherheitsleitlinien der Südwestfalen-IT gestellten Anforderungen.
3. Sobald der Zertifizierungsdiensteanbieter erkennt, dass er die in den Sicherheitsleitlinien des Wurzelzertifizierungsdienstes und/oder der Selbsterklärung [selbsterkl] aufgestellten Anforderungen nicht mehr erfüllt, ist er verpflichtet, dieses unverzüglich und schriftlich der PCA der Verwaltung mitzuteilen.
4. Erkennt die PCA der Verwaltung, dass die in den Sicherheitsleitlinien der Wurzelzertifizierungsstelle und/oder der Selbsterklärung aufgestellten Anforderungen von der Zertifizierungsstelle nicht mehr erfüllt werden, verpflichtet sich die Südwestfalen-IT, innerhalb von zwei Wochen nach einer schriftlichen Aufforderung eine schriftliche Stellungnahme abzugeben.
5. Die Südwestfalen-IT verpflichtet sich, auf Verlangen Aufzeichnungen und Unterlagen, auch in elektronischer Form, zur Prüfung vorzulegen und auf Verlangen der PCA der Verwaltung die unterzeichnete Selbsterklärung zu erneuern. Kommt die Südwestfalen-IT diesem nicht innerhalb zwei Wochen nach, ist die PCA der Verwaltung berechtigt, das CA-Zertifikat zu sperren.
6. Die Südwestfalen-IT stellt sicher, dass das CA-Schlüsselpaar in einer gesicherten Umgebung kryptographisch geeignet erzeugt wird.
7. Die Südwestfalen-IT verpflichtet sich, diese Policy einzuhalten.

8. Die Südwestfalen-IT stellt einen Sperrdienst zur Verfügung.
9. Die Südwestfalen-IT verpflichtet sich, die Komponenten und Verfahren für alle eingebundenen Systemkomponenten technisch aktuell zu halten.

3.1. Verpflichtungen des Zertifikatnehmers[5]

Die Zertifikatsnehmer sind verpflichtet,

1. die Richtigkeit und Vollständigkeit der angegebenen Daten bei der Beantragung sicherzustellen,
2. die Verfahren zur Identifizierung und Authentisierung der in den Sicherheitsleitlinien ausgegebenen Leitlinien einzuhalten,
3. den privaten Schlüssel zu schützen; d.h. ihn vor dem Zugriff durch unberechtigte Personen zu schützen und eine Weitergabe des Schlüssels nur im Falle eines Gruppen- oder Serverzertifikates vorzunehmen,
4. die Sperrung des Zertifikats bei einer Kompromittierung oder des Verdachts einer Kompromittierung unverzüglich zu veranlassen,
5. die Zertifikate nur dieser Policy entsprechend zu nutzen. Entscheidend ist die Policy zum Zeitpunkt der Zertifikatserstellung.

Durch die Beantragung der Sperrung eines Zertifikats durch den Zertifikatsnehmer entstehen für den Zertifikatsnehmer keine Kosten.

3.2. Vertraulichkeit

Alle Dokumente unterliegen der Vertraulichkeit. Die Sicherheitsleitlinie ist zur Veröffentlichung freigegeben.

3.3. Gültigkeitsdauer

Endbenutzerzertifikate besitzen regelmäßig eine Gültigkeitsdauer von drei Jahren. Laufzeiten von ein- oder zwei Jahren möglich.
Nachgeordnete Zertifizerungsstellenzertifikate (SUB-CA's) besitzen eine max. Gültigkeit von 6 Jahren.
Zertifikate werden nach dem Ablauf ihrer Gültigkeitsdauer nicht erneuert. Es ist notwendig, ein neues Zertifikat zu beantragen.

3.4. Signaturkarten

3.4.1. Kooperation TeleSec

Die Südwestfalen-IT bietet ihren Kunden die Möglichkeit, Signaturkarten (PKS) zu erwerben. Diese Signaturkarten tragen ein qualifiziertes Zertifikat der
T-Systems International GmbH [TeleSec] und bei Bedarf ein weiteres fortgeschrittenes Zertifikat der V-PKI der Südwestfalen-IT.
Für die Beantragung und Nutzung der Qualifizierten Signatur auf dieser Signaturkarte gelten die Bestimmungen und Ausführungen der T-Systems International GmbH.

3.4.2. Beantragung von Signaturkarten

[5] Endbenutzer, für die personenbezogene Zertifikate ausgestellt werden, Schlüsselverantwortliche, für die Gruppen-/Funktions- oder Server-Zertifikate ausgestellt werden,
Nachgeordnete Zertifizierungsstellen, für die SUB-CA Zertifikate ausgestellt werden.

Die Beantragung von Signaturkarten geschieht über das Portal der V-PKI der Südwestfalen-IT. Nachdem die Daten für ein Fortgeschrittenes Zertifikat der
V-PKI erfasst worden sind, wird der Dialog zur Eingabe weiterer Daten für das Qualifizierte Zertifikat automatisiert fortgeführt.
Der Prozess der Beantragung und die Verifizierung des Antragstellers und dessen Antragsdaten entspricht dabei der Standardprozedur der TeleSec für die Beantragung von Signaturkarten.
Die Südwestfalen-IT ist durch die TeleSec für diesen Workflow autorisiert und ist Registrierungsstelle der TeleSec mit der **RM-Nummer A.01.24**.

4. Identifizierung und Authentisierung

Die von der Südwestfalen-IT ausgestellten Zertifikate sind als vertrauenswürdig einzustufen. Diese Vertrauenswürdigkeit basiert auf der grundsätzlichen Art der Überprüfung der Inhalte und der Identitätsfeststellung.
Die Sicherheit der Verschlüsselung ist unter anderem von den eingesetzten Algorithmen, Zertifikaten und Produkten abhängig.
Für die Einstufung der Vertrauenswürdigkeit des Zertifizierungs-Dienstanbieters ist die Verbindlichkeit der durch die Zertifikate gemachten Aussagen bedeutsam. Die eindeutige Zuordnung eines Zertifikats zum Zertifikatsinhaber ist dabei von entscheidender Bedeutung.

Es bestehen zwingend bindende Vorschriften zur Identifizierung von Zertifikatsnehmern.

4.1. Beantragung

Jede Beantragung eines Zertifikats wird im Grundsatz wie eine Erstbeantragung behandelt. Eine Verlängerung der ausgestellten Zertifikate ist nicht vorgesehen.

4.1.1. Identifizierung und Authentifizierung einer natürlichen Person

Antragsteller müssen durch ihre zuständige LRA[6](Local Registration Authority) zweifelsfrei identifiziert und authentifiziert werden. Die LRA überprüft dazu die übermittelten Daten auf Korrektheit und Vollständigkeit. Zur Authentifizierung muss die LRA den Antragsteller erstmalig durch persönliches Erscheinen identifizieren und anhand eines gültigen amtlichen Ausweises authentifizieren.
Die Identifikation und Authentifizierung bei einer Erstbeantragung ist auf Antrag des Antragstellers auch durch den POSTIDENT ® Dienst BASIC der Deutsche POST AG [Postident] möglich. Ebenso wird die Möglichkeit eingeräumt, für Antragsteller aus der öffentlichen Verwaltung das BehördenIdent durch eine Siegelführende Person zu nutzen.
Wird ein Folgeantrag für ein Zertifikat **durch und für dieselbe** Person oder **für denselben Zweck** vor Ablauf einer Gültigkeitsperiode gestellt, kann der LRA / RA eine elektronisch signierte Mail dieser Person zur Authentifizierung akzeptieren.
Anschließend wird der Antrag zur weiteren Bearbeitung freigegeben.

4.1.2. Weitere benötigte Dokumente

Jede LRA ist berechtigt, weitere Dokumente zur zweifelsfreien Identifizierung und/oder Authentisierung vom Antragsteller zu verlangen.

4.1.3. Identifizierung und Authentifizierung einer juristischen Person

Es ist nicht vorgesehen, Zertifikate an juristische Personen zu vergeben.

[6] LRA im genannten Sinne ist im Einzelfall auch die RA des Zertifizierungsdienste -Anbieters

4.1.4. Anforderungen an den CA-Namensraum

Der zugeordnete CA-Namensraum für den Südwestfalen-IT Zertifizierungsdiensteanbieter wird in [CPS] beschrieben.

Die CA-Namensraumvergabe des Zertifizierungsdiensteanbieters Südwestfalen-IT erfüllt die vom BSI in [Namreg] gestellten Anforderungen.

Der Common Name (CN) des Zertifizierungsdiensteanbieters Südwestfalen-IT ist für jedes von der Wurzelzertifizierungsstelle für die Südwestfalen-IT ausgestellte Zertifikat innerhalb der PKI der Südwestfalen-IT eindeutig und folgt dem im CPS [CPS] definierten Namenskonzept.

4.1.5. Anforderungen an den Teilnehmer-Namensraum

Der zugeordnete Namensraum für Zertifikate des Zertifizierungsdiensteanbieters Südwestfalen-IT wird in [CPS] beschrieben.
Der enthaltene Teilnehmer-Namensraum wird in Absprache mit der PCA der Verwaltung vereinbart.

Die Teilnehmer-Namensraumvergabe des Zertifizierungsdiensteanbieters Südwestfalen-IT für Endbenutzer erfüllt die vom BSI in [Namreg] gestellten Anforderungen.
Für den Fall, das Zertifikate für Personengruppen, Funktionen oder automatisierte IT-Prozesse ausgestellt werden, gelten die entsprechenden Vorgaben des BSI in [Namreg] und darüber hinaus die weitergehenden Regelungen des BSI in [GRP] und [CP_Neu].

4.1.6. Eindeutigkeit des Namens von Endbenutzerzertifikaten

Der Zertifizierungsdiensteanbieter Südwestfalen-IT stellt sicher, dass für jeden Zertifikatsnehmer ein eindeutiger Name verwendet wird. Bei Namensdoppelung wird über die Einträge in das CN-Feld sichergestellt, dass die Eindeutigkeit gegeben ist. Gruppenzertifikate und Zertifikate für Funktionen oder automatisierte IT-Prozesse werden zudem eindeutig durch das Kürzel **GRP:** (**neu FKT:**) im CN-Feld gekennzeichnet.

4.1.7. Nachweis des Besitzes des Schlüsselpaares

Der Antragssteller hat die Sorgfaltspflicht, angemessene Sicherheitsmaßnahmen zu treffen, den privaten Schlüssel seines Zertifikats sowie eine ggf. vorhandene Signaturkarte vor Missbrauch zu schützen.

4.2. Sperrantrag

Die Beantragung zum Sperren eines Zertifikats kann über verschiedene Wege erfolgen. Gegenüber der Südwestfalen-IT besitzt nur die Abteilung, repräsentiert durch die LRA, Berechtigung, einen Antrag zur Sperrung eines Zertifikats zu stellen.
Zertifikatsinhaber haben für die Sperrung ihres Zertifikats die zuständige LRA zu informieren, bei Nichterreichbarkeit auch direkt die RA der Südwestfalen-IT.
Zur Beantragung einer Sperrung durch die LRA dient das für LRA's eingerichtete Web-Interface.
Dadurch wird die RA des Zertifizierungsdiensteanbieters Südwestfalen-IT informiert, die RA kann die Sperreinträge einsehen und die Sperrung veranlassen.

Die RA ist verpflichtet, die Wahrhaftigkeit eines Sperrantrages geeignet zu überprüfen.

Mögliche Übermittlungsmethoden eines Sperrantrages gegenüber den RA`s:[7]

- Telefon
- signierte Email

Folgende Angaben sind zur Beantragung einer Sperrung durch die LRA notwendig:

- Anmeldepasswort des LRA am Web-Interface für LRA
- Name und Telefon des Beantragenden der Sperrung [8]
- Name des Zertifikatsinhabers / Schlüsselverantwortlichen
- Kommune (Stadt/Verwaltung) / Abteilung (Dienststelle) des Zertifikatinhabers
- Seriennummer des Zertifikats
- Begründung für die Sperrung [9]

Nach erfolgter Sperrung versendet die RA eine Mitteilung an folgenden Personenkreis:

- Zertifikatsinhaber / Schlüsselverantwortlichen
- Zuständige LRA

4.3. Wiederausstellen nach Sperrung

Nach der Sperrung eines Zertifikats muss ein neues Zertifikat beantragt werden. Ein Wiederaufleben der Gültigkeit ist nicht möglich.
Eine erneute Beantragung zur Erteilung eines Zertifikats erfolgt auf dieselbe Art wie bei der erstmaligen Beantragung.

5. Ablauforganisation

5.1. Zertifikatsbeantragung

5.1.1. Standardantragsweg

Zertifikatsnehmer beantragen ihr Zertifikat beim Zertifizierungs-Dienstanbieter Südwestfalen-IT.
Die Beantragung von Endbenutzerzertifikaten erfolgt über das im Internet verfügbare Webfrontend.
Für die Beantragung sind folgende personenbezogene Daten anzugeben:

- Räumliche Ordnung
- Organisationseinheit I
- Organisationseinheit II / Gruppe / Funktion
- Name, Vorname
- Email-Adresse.

Die Räumliche Ordnung ist für die Beantragung notwendig, aber kein Bestandteil des Zertifikats.

Der Antrag wird durch die zuständige LRA nach erfolgreicher Identifikation, nach Kapitel 3.1, verifiziert. Bei erfolgreicher Verifizierung wird der Antrag in elektronischer Form an den RA-Operator weitergeleitet. Der RA-Operator hat die Berechtigung, den verifizierten Antrag zur Zertifizierung an die CA weiterzuleiten.

5.1.2. Zertifikatsbeantragung eines Zertifizierungsstellenzertifikats

Für die Beantragung eines Zertifizierungsstellenzertifikats (SUB-CA) muss ein Certificate Signing Request (CSR) im festgelegten Format und mit festgelegten Inhalten bereitgestellt werden.

[7] sowohl LRA als auch RA
[8] Für notwendige Rückfragen durch den RA
[9] Die Angabe von Sperrgründen ist freigestellt

5.2. Ausstellung eines Zertifikats

Die Zertifizierungsstelle der Südwestfalen-IT erzeugt beim Vorliegen eines vollständigen und geprüften Antrags und nach erfolgter Identifizierung und Authentisierung ein den Daten des Antragstellers entsprechendes Zertifikat.
Der dazu vorliegende Zertifikats-Antrag (Certificate Signing Request) muss durch die RA freigegeben und über ein portables Speichermedium an den CA-Operator übergeben werden.
Die Zertifizierungsstelle behält sich vor, bei dem Wechsel des Zertifikats des Zertifizierungsdiensteanbieters neue Zertifikate für die Teilnehmer auszustellen.

5.3. Akzeptanz des Zertifikats

Erzeugte Endbenutzerzertifikate werden über den Verzeichnisdienst gemäß Kapitel 1.1.3 veröffentlicht. Zertifizierungsstellenzertifikate (SUB-CA) werden über die Webseite zur Beantragung von Zertifikaten http://cas.citkomm.de/ veröffentlicht.
Der Antragsteller erhält nach der erfolgreichen Erzeugung seines Zertifikats eine E-Mail mit einem vorhandenen Link zum Download des Zertifikats.
Der Zertifikatsnehmer ist verpflichtet, das für ihn ausgestellte Zertifikat sofort nach Erhalt auf Richtigkeit der Angaben zu überprüfen und bei Nichtakzeptanz umgehend einen der folgenden Ansprechpartner zu informieren:

- Die eigene, zuständige LRA
- Den RA-Operator des Zertifizierungsdiensteanbieters Südwestfalen-IT
- Das Callcenter der Südwestfalen-IT

5.4. Sperrung von Zertifikaten

5.4.1. Sperrgründe

Ein Zertifikat muss aus folgenden Gründen gesperrt werden:

- Nichtakzeptanz des Zertifikats durch den Antragsteller.
- Die Angaben im ausgestellten Zertifikat entsprechen nicht oder nicht mehr der Realität.
- Schwächen im verwendeten Kryptoalgorithmus werden bekannt.
- Die eingesetzte Hard- und Software weist Sicherheitsrisiken auf.
- Der Zertifizierungsdiensteanbieter stellt seinen Betrieb ein.
- Kompromittierung oder Verlust des privaten Schlüssels.
- Der Zertifikatsnehmer verlässt das Unternehmen.

5.4.2. Zeitdauer zwischen Sperrantrag und Sperrung

Die Zertifizierungsstelle sperrt bei Vorliegen eines gültigen Sperrantrags das Endbenutzerzertifikat unmittelbar, jedoch spätestens am nächsten Arbeitstag.

5.4.3. Ausstellen von Sperrlisten

Bei der Sperrung eines Zertifikats wird die Sperrliste auf dem Verzeichnisdienst umgehend aktualisiert.

5.4.4. Bekanntgabe von Sperrungen

Die aktuelle Sperrliste wird vom Zertifizierungsdiensteanbieter über das Webfrontend veröffentlicht und nach der Sperrung eines Zertifikats aktualisiert.

5.4.5. Kompromittierung des geheimen Schlüssels

Bei der Feststellung einer Kompromittierung des privaten Schlüssels eines Zertifikats ist das Zertifikat unverzüglich zu sperren. Der Inhaber des Zertifikats ist verpflichtet, entsprechende Schritte einzuleiten.
Sollte der geheime Schlüssel des Zertifizierungsdiensteanbieters Südwestfalen-IT oder einer nachgeordneten Zertifizierungsstelle (SUB-CA) kompromittiert werden, ist das Zertifikat des Zertifizierungsdiensteanbieters und vorher alle nachgeordneten Zertifikate zu sperren.

5.4.6. Suspendierung

Die Suspendierung[10] von Zertifikaten ist nicht vorgesehen.

5.5. Beweissicherung und Protokollierung

Detaillierte Ausführungen zur Durchführung von Archivierung, Beweissicherung, Protokollierung und zugeordneten Rechten von auszuführenden Personenkreisen werden in dem CPS [CPS] definiert. Außerdem werden Angaben zu Zeiträumen gemacht, für die eine Datensicherung und Protokollierung gewährleistet werden muss.

5.6. Schlüsselwechselmanagement

Endbenutzerzertifikate des Zertifizierungsdiensteanbieters Südwestfalen-IT sind auf eine max. Gültigkeit von drei Jahren beschränkt.
Zertifizierungsstellenzertifikate (SUB-CA's) des Zertifizierungsdiensteanbieters Südwestfalen-IT haben eine max. Gültigkeit von 6 Jahren.
Eine Verlängerung der Gültigkeit von Zertifikaten nach Ablauf der Nutzungsdauer ist nicht vorgesehen. Nutzer müssen ggf. vor Ablauf der Gültigkeitsdauer neue Zertifikate beantragen. 30 Tage vor Ablauf der Gültigkeit des Zertifikats werden Nutzer per Email über das weitere Vorgehen informiert.
Rechtzeitig vor Ablauf des Zertifikats des Zertifizierungsdiensteanbieters beantragt und erhält der Zertifizierungsdiensteanbieter Südwestfalen-IT ein neues Zertifikat von der Wurzelzertifizierungsstelle. Zertifizierungsstellen-Zertifikate (CA-Zertifikate) besitzen eine Gültigkeit von max. 6 Jahren. Es ist möglich, dass der Zertifizierungsdiensteanbieter vor dem Ablauf der Gültigkeit ein neues CA-Zertifikat der PCA der Verwaltung bekommt (ältere CA-Zertifikate verlieren damit nicht ihre Gültigkeit). Dadurch kann der Zertifizierungsdiensteanbieter mehrere gültige Zertifikate besitzen.

5.7. Kompromittierung und Wiederherstellung

Der Zertifizierungsdiensteanbieter Südwestfalen-IT verfügt über ein Konzept zur Wiederherstellung eines ordnungsgemäßen Betriebs nach Notfällen und/oder Katastrophen [CPS].
Somit ist eine Wiederherstellung in angemessener Zeit möglich. Als Notfall werden unter anderem die Kompromittierung des privaten Schlüssels des Zertifizierungsdiensteanbieters Südwestfalen-IT, das Bekannt werden von Schwachstellen in den verwendeten kryptographischen Verfahren und die Nichtverfügbarkeit der Sperrlisten angesehen.
Das Konzept unterliegt einer ständigen Pflege und Aktualisierung.

5.8. Betriebseinstellung / Betriebsaufgabe

Die Einstellung des Betriebs des Zertifizierungsdienstes der Südwestfalen-IT ist anzukündigen. Hierfür gelten folgende Regelungen:

- Der Zertifizierungsdiensteanbieter kann den Betrieb mit einer Ankündigungsfrist von drei Monaten ohne Angabe von Gründen einstellen.
- Die Ankündigung muss schriftlich erfolgen.

[10] Aussetzung der Gültigkeit eines Zertifikats über einen definierten Zeitraum

- Die Ankündigung ist zu veröffentlichen.
- Die Veröffentlichung geschieht durch eine Mitteilung an den Wurzelzertifizierungsdiensteanbieter und per Email an die Zertifikatenutzer.
- Die Art und Weise der Einstellung ist mit dem Wurzelzertifizierungs-Dienstanbieter vertraglich geregelt.

Alle vom Zertifizierungsdiensteanbieter Südwestfalen-IT ausgestellten Zertifikate werden zum Zeitpunkt der Einstellung des Betriebs ungültig. Zertifikate, deren Gültigkeit formal über den Zeitpunkt der Betriebseinstellung Gültigkeit haben, werden mit Zeitpunkt der Betriebseinstellung gesperrt.
Nach erfolgter Ankündigung zur Einstellung des Betriebs werden neue Zertifikate für Endbenutzer nur noch mit einer Gültigkeit bis zum Ende des Betriebs ausgestellt.

6. Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

Die Umsetzung der Anforderungen des Wurzelzertifizierungsdiensteanbieter bezüglich der infrastrukturellen, organisatorischen und personellen Sicherheitsmaßnahmen sind im CPS [CPS] dargelegt. Die dokumentierten Sicherheitsmaßnahmen entsprechen dem Niveau des IT-Grundschutzhandbuchs [IT-Grund].
Das in Form des CPS [CPS] vorliegende Sicherheitskonzept kann bei Bedarf von dem Wurzelzertifizierungsdiensteanbieter eingesehen werden.

6.1. Infrastrukturelle Maßnahmen

6.1.1. Lage des Zertifizierungsanbieters

Der Dienst zur Zertifizierung erfolgt bei der Südwestfalen-IT.

Südwestfalen-IT
Sonnenblumenallee 3
58675 Hemer

Callcenter der Südwestfalen-IT
Tel.: +49 271 30 321-0
Email: pki@sit.nrw

6.1.2. Zutritt zur Südwestfalen-IT

Das Gebäude der Südwestfalen-IT verfügt über ein Zutrittskontroll- und Überwachungssystem.
Betriebsfremden wird der Zugang erst nach Ausweisung und Angabe der zu besuchenden Person gestattet. Der Besucher erhält einen speziell gekennzeichneten Besucherausweis, welcher offen und sichtbar getragen werden muss. Die besuchte Person muss seinen Besucher während des gesamten Aufenthalts begleiten und am Ende des Besuchs persönlich zum Ausgang geleiten.
Die besuchte Person muss den Besuch am Ende mit Uhrzeit quittieren.

6.1.3. Stromversorgung und Klimatechnik

Der technisch-infrastrukturelle Standort der Südwestfalen-IT verfügt über eine für den Notfall abgesicherte Lüftungsanlage. Für den Fall eines Stromausfalls sind die Systeme mit einer unterbrechungsfreien Stromversorgung (USV) ausgestattet. Die Ausfallsicherheit ist so gewährleistet.

6.1.4. Brandschutz

Der Zertifizierungsdiensteanbieter Südwestfalen-IT verfügt über eine Feuermeldeanlage und entsprechender Infrastruktur, die zur Vorsorge und Bekämpfung von Bränden dient[11]. Die regelmäßige Wartung der Brandmelde- und Löschanlagen ist vertraglich mit dem Hersteller geregelt.
Die Brandmelde- und Löschanlagen stehen in direktem Kontakt mit der lokalen Berufsfeuerwehr.

6.1.5. Besonders schützenswerte Objekte

Für besonders schützenswerte Objekte der Public Key Infrastruktur existieren spezielle Konzepte zur Sicherung, Wiederherstellung, Archivierung und Vernichtung.
Diese Objekte sind:

- Privater Schlüssel des Zertifizierungsdiensteanbieters
- Protokolldateien

6.2. Organisatorische Maßnahmen

Durch entsprechende Regelungen und Maßnahmen des Zertifizierungsdiensteanbieter Südwestfalen-IT wird nur ausgewählten Personenkreisen der Zugang zu technischen Räumen gewährt und die notwendigen Berechtigungen erteilt.
Dieses Rollenkonzept in [CPS] regelt Zuständigkeiten und kontrolliert Interessenskonflikte.

6.3. Personelle Maßnahmen

Rollen, Berechtigungen und Zuständigkeiten unterliegen bestimmten Anforderungsprofilen.
Jede mit einer Aufgabe vertraute Person muss den jeweiligen Anforderungskriterien seiner Rolle nachweislich entsprechen. Das Rollenkonzept und die erforderlichen Anforderungskriterien sind im CPS [CPS] beschrieben.

7. Technische Sicherheitsmaßnahmen

Alle technischen Sicherheitsmaßnahmen sind detailliert in dem CPS [CPS] des Zertifizierungsdiensteanbieters beschrieben und werden von der PKI der Südwestfalen-IT umgesetzt.
Das Niveau entspricht mindestens den im IT-Grundschutzhandbuch [IT-Grund] beschriebenen Maßnahmen.

7.1. Schlüsselmanagement

7.1.1. Schlüsselgenerierung

Die kryptographisch hinreichend sicheren privaten Schlüssel des Zertifizierungsdiensteanbieters Südwestfalen-IT werden in dem von der Wurzelzertifizierungsstelle vorgegebenen Format in einer sicheren Umgebung erstellt.
Die kryptographisch hinreichend sicheren privaten Schlüssel für Endanwender werden im Browser eines Antragstellers generiert. Auf besondere Anforderung ist die Generierung des privaten Schlüssels für Endbenutzerzertifikate zentral beim Zertifizierungsdiensteanbieter möglich.
Die Südwestfalen-IT verpflichtet sich durch Vertragsabschluss mit der Wurzelzertifizierungsstelle, die Schlüsselpaargenerierung für die CA des Zertifizierungsdiensteanbieters Südwestfalen-IT, sowie zentral generierte Schlüssel für Endbenutzerzertifikate, nach dem aktuellen Stand der Technik und unter Einhaltung des Vier-Augen-Prinzips durchzuführen.

7.1.2. Übergabe der öffentlichen Schlüssel und Zertifikate

Die öffentlichen Schlüssel des Zertifizierungsdiensteanbieters werden der Wurzelzertifizierungsstelle in dem von der Wurzelzertifizierungsstelle vorgegebenem Format übergeben. Der öffentliche Schlüssel wird durch den

[11] Brand und Katastrophenschutzordnung der Südwestfalen-IT, Feuerwehrplan nach DIN 14095; Stand 2002

Wurzelzertifizierungsdiensteanbieter signiert. Die erstmalige Übergabe muss persönlich durch den gesetzlichen Vertreter der Südwestfalen-IT oder dessen Beauftragten erfolgen; ansonsten ist auch Briefpost zulässig.
Die zentral oder dezentral erzeugten, öffentlichen Schlüssel für Anwenderzertifikate werden auf elektronischem Wege in eine interne Datenbank geschrieben und nach erfolgreicher Verifizierung über ein portables Speichermedium zur CA überführt und durch die CA der Südwestfalen-IT signiert.
Ausgestellte Zertifikate werden in den öffentlichen Verzeichnisdienst überführt und der Inhaber wird per Email informiert.

7.1.3. Kryptoalgorithmen, Schlüssellängen, Parametergenerierung

Die Umsetzung der aktuellen Empfehlungen des BSI – „Geeignete Kryptoalgorithmen gemäß § 17 Abs. 2 SigV" - wird innerhalb der PKI angestrebt.

7.1.4. Schlüsselnutzung

Der private Schlüssel des Zertifizierungsdiensteanbieters Südwestfalen-IT wird ausschließlich zur Signierung der Schlüssel der Endanwender, der Schlüssel der RA und der zu veröffentlichenden Zertifikatssperrlisten genutzt.

7.2. Schutz des geheimen Schlüssels

7.2.1. Schutz des geheimen Schlüssels für Endanwender

Anwender haben eine spezielle Sorgfaltspflicht, den eigenen privaten Schlüssel zu schützen. Dies gilt auch für private Schlüssel von abgelaufenen oder gesperrten Zertifikaten.

7.2.2. Schlüsselteilung

Ist nicht vorgesehen.

7.2.3. Key Escrow

Ist nicht vorgesehen.

7.2.4. Backup privater Schlüssel

Die privaten Schlüssel des Zertifizierungsdiensteanbieters Südwestfalen-IT sind über ein Backupverfahren unter der strengen Einhaltung des Vier-Augen-Prinzips wieder herstellbar.

Für sämtliche private Schlüssel der Anwender ist seitens des Zertifizierungsdiensteanbieters kein Backup-Verfahren vorgesehen. Im Falle des Verlustes oder der Kompromittierung des privaten Schlüssels der Endanwender wird das Endanwenderzertifikat auf Antrag gesperrt. Die Endanwender sind auf die Notwendigkeit der Sicherung des privaten Schlüssels hingewiesen worden.

7.2.5. Archivierung privater Schlüssel

Die Archivierung des privaten Schlüssels der Südwestfalen-IT CA erfolgt bis zum Ablauf der Gültigkeit des Zertifikats.

Für Zertifikatsnehmer ist seitens der Südwestfalen-IT keine Archivierung des privaten Schlüssels vorgesehen. Es wird jedoch empfohlen, dass Kunden der Südwestfalen-IT die privaten Schlüssel der Zertifikatsnehmer archivieren.

7.2.6. Schlüsselinstallation und Aktivierung, dezentral

Der Zugriff auf den privaten Schlüssel des Zertifizierungsdiensteanbieters Südwestfalen-IT kann nur unter Einhaltung des Vier-Augen-Prinzips erfolgen. Weitere Aspekte zur Aktivierung des privaten Schlüssels des Zertifizierungsdiensteanbieters Südwestfalen-IT sind durch den Zertifizierungsdiensteanbieter Südwestfalen-IT geregelt.
Die Installation und Aktivierung der Benutzerzertifikate aus **dezentral** erzeugten Anträgen erfolgt über den Link in der dem Zertifikatsnehmer zugesandten Email.

7.2.7. Schlüsselinstallation und Aktivierung, zentral

Die Schlüssel der V-PKI Zertifikate in Verbindung mit einer Signaturkarte werden zentral aus den Antragsdaten in der Südwestfalen-IT erzeugt. Auf die Signaturkarte werden die damit erzeugten V-PKI-Zertifikate in der Form PKCS#12 (persönlicher Datenaustausch) aufgebracht und den Antragstellern zur Verfügung gestellt. Nach der Installation sind die V-PKI-Zertifikate für den Antragsteller nur über seine persönliche Signaturkarte nutzbar.

7.2.8. Schlüsselvernichtung

Der Zertifizierungsdiensteanbieter Südwestfalen-IT ist selbst für die Vernichtung der eigenen Schlüssel verantwortlich.

Nach Ablauf oder Sperrung eines Endbenutzerzertifikats ist es nicht notwendig, den privaten Schlüssel des Zertifikatsnehmers zu vernichten.

7.3. Weitere Aspekte des Schlüsselmanagements

7.3.1. Archivierung öffentlicher Schlüssel

Die öffentlichen Schlüssel des Zertifizierungsdiensteanbieters Südwestfalen-IT werden während ihrer Gültigkeit und darüber hinaus archiviert. Ein öffentlicher Zugriff auf den öffentlichen Schlüssel der CA des Zertifizierungsdienstanbieters der Südwestfalen-IT ist während der Gültigkeit und darüber hinaus möglich.

7.3.2. Nutzungsdauer für öffentliche und private Schlüssel

Die max. Nutzungsdauer für Endbenutzerzertifikate beträgt drei Jahre. Eine Re-Zertifizierung von Zertifikaten ist nicht vorgesehen.
Die Signaturprüfschlüssel (öffentliche Schlüssel) können zur Signaturprüfung und die Entschlüsselungsschlüssel (private Schlüssel) können zur Entschlüsselung zeitlich unbegrenzt genutzt werden.
Schlüssel von Zertifizierungsstellenzertifikaten (SUB-CA's) sind max. 6 Jahre
gültig und dürfen nach Ablauf der Gültigkeit nicht mehr genutzt werden.

8. Profile für Zertifikate und Sperrlisten (CRLs)

Das Profil des Zertifikats des Zertifizierungsdiensteanbieters Südwestfalen-IT sowie die Zertifikate der Endbenutzer entsprechen den Vorgaben der PCA [FormProt].

Das Profil der Sperrlisten des Zertifizierungsdiensteanbieters Südwestfalen-IT entspricht den Vorgaben der PCA [FormProt].

Regelungen bezüglich der Vergabe von Namen sind geregelt und entsprechen den Vorgaben der PCA [Namreg].

9. Änderung und Anerkennung dieser Certificate Policy

9.1. Änderungen

Der Zertifizierungsdiensteanbieter Südwestfalen-IT ist verantwortlich, diese Policy auf einem ständig aktuellen Stand zu halten. Berechtigungen zur Änderung und entsprechender Umsetzung dieser Policy sind geregelt.

9.2. Anerkennung

Der Zertifizierungsdiensteanbieter Südwestfalen-IT verpflichtet sich zur Anerkennung dieser Policy.
Die Nutzer von Zertifikaten der V-PKI verpflichten sich mit der Beantragung ihres Zertifikats zur Anerkennung dieser Policy.

Mit der Anerkennung dieser Policy entstehen für den Zertifikatsnehmer Verpflichtungen, welche der Zertifikatsnehmer einzuhalten und umzusetzen hat.
Eine Nichtanerkennung dieser Policy oder eine Nichterfüllung der Pflichten führt zur Sperrung des Zertifikats des Nutzers.

10. Glossar

Authentisierung
Nachweis der behaupteten Identität des Zertifikatinhabers.

Authentifizierung
Prüfung der behaupteten Identität des Zertifikatinhabers

BSI
Abkürzung für "Bundesamt für Sicherheit in der Informationstechnik"

BehördenIdent

Eine Siegelführende Person in einer öffentlichen Verwaltung
stellt die Identität eines Antragstellers anhand eines gültigen Ausweispapieres
zweifelsfrei fest und bestätigt dies durch Ausstellung einer „öffentlichen Urkunde“
mit seinem Dienstsiegel.

CA-Zertifikat
Ein von der → PCA ausgestelltes Zertifikat für → Zertifizierungsstellen. Mit dem CA-Zertifikat kann eine → CA weitere Zertifikate ausstellen.

Certification Policy (CP)
engl. für → Sicherheitsleitlinien

Certificate Revocation List (CRL)
Die Sperrliste enthält die Sperrinformationen über Endbenutzer- Zertifikate.

Certification Authority (CA)
engl. für → Zertifizierungsstelle

Common Name (CN)
Ein Attributtyp, der verwendet wird, um Namen von Personen / Gruppen / Diensten innerhalb eines → DN zu definieren.

Distiguished Name (DN)
Gibt die Position eines Objekts in Verzeichnisdienst an.

Endbenutzer

Eine natürliche Person, ein DV-Dienst, eine Personengruppe, welche die unterste Hierarchieebene darstellt und Zertifikate nutzt.

Gültigkeit

Definiert einen Zeitraum, über welchen ein ausgestelltes Zertifikat sinnesgemäß genutzt werden darf.

IETF

Internet Engineering Task Force (www.ietf.org). Gremium, das Internetstandards entwickelt.

Key Escrow

engl. → Schlüsselhinterlegung

Maßnahme, um beispielsweise ein Mitlesen verschlüsselter Nachrichten durch staatliche Stellen zu ermöglichen.

Kreuzzertifizierung

Kopplung zweier unabhängiger Infrastrukturen mittels gegenseitiger Zertifizierung.

LDAP Data Interchange Format

Standarisiertes Verfahren zum Austausch von Daten oder Strukturen in LDAP-fähigen Verzeichnissen, RFC 2849.

Lokale Registrierungsstelle (LRA: Local Registration Authority)

Bildet die persönliche und organisatorische Schnittstelle zwischen den Endanwendern und der PKI. LRA ist Teil der → RA

Öffentlicher Schlüssel

Öffentlicher Anteil des Schlüsselpaares. Mit diesem Schlüssel verschlüsselte Daten können nur mit dem dazugehörigen privaten Schlüssel entschlüsselt werden.

MIME

Multi Purpose Internet Mail Extensions (RFC 2045 - 2049) Standard für das Format von Emails. MIME definiert, wie Texte mit internationalen Character-Sets oder Binärdateien als Anhang von EMails verwendet werden.

Policy Certificate Authority (PCA)

Wurzelzertifizierungsstelle der → PKI-1-Verwaltung. Von ihr können Zertifizierungsstellen von Bund, Ländern und Kommunen → CA- Zertifikate ausgestellt bekommen.

PKI-1-Verwaltung

→ V-PKI

Policy

hier: → Sicherheitsleitlinien

Public Key
engl. → öffentlicher Schlüssel

Private Key
engl. → privater Schlüssel

Privater Schlüssel
Nicht öffentlicher Anteil des Schlüsselpaares. Mit diesem Schlüssel können die mit dem dazugehörigen → öffentlichen Schlüssel verschlüsselten Texte entschlüsselt werden.

Public Key Infrastruktur (PKI)
Ein System, das die Vertrauensbeziehungen unter Nutzung der Public-Key-Technologie verwaltet. Aufgabe der PKI ist es zu gewährleisten, dass digitale Zertifikate und Zertifizierungsbehörden validiert und als vertrauenswürdig angesehen werden.

RA (Registration Authority)
Registrierungsstelle welche die Angaben zum Zertifikatsantrag prüft

RFC (Request for Comments)
Spezifikationen, Vorschläge, Ideen und Richtlinien, das Internet betreffend, werden in Form von so genannten RFCs veröffentlicht. Seit 1989 ist die Struktur und der Aufbau von RFCs durch die RFC 1111 geregelt.

S/MIME
Secure MIME. Erweiterung des MIME-Standards für Mailverschlüsselung und digitale Unterschriften (RFC 2633).

Sicherheitsleitlinien
Leitlinien für das Ausstellen, Sperren, Erneuern und Anwenden von Zertifikaten durch die Zertifizierungsstelle.

Sub-CA
Eine der CA untergeordnete Zertifizierungsstelle welche wiederum Zertifikate ausstellen darf.

Suspendierung
Aussetzung der Gültigkeit eines Zertifikats über einen definierten Zeitraum.

Verwaltungs-PKI (V-PKI)
Allgemeine Beschreibung für die gesamte PKI des Bundes. Sowohl die PCA, als auch alle angeschlossenen →Zertifizierungsstellen sind Teilnehmer der V-PKI.

Wurzelzertifizierungsstelle
Oberste Vertrauensinstanz einer →PKI.

Zertifikat

Bestandteil eines digitalen Zertifikats sind der öffentliche Schlüssel und Angaben zur Person (Name), welche im Besitz des korrespondierenden privaten Schlüssels ist. Ein Zertifikat wird von einer vertrauenswürdigen Zertifizierungsstelle nach sorgfältiger Überprüfung digital signiert.

Zertifizierungsdiensteanbieter
Stellt den Dienst für Endanwender zur Verfügung, digitale Zertifikate und entsprechende Sperrlisten zu erstellen. Ein Zertifizierungsdiensteanbieter kann auch weitere Dienste wie einen Registrierungs- und Verzeichnisdienst ausstellen.

Zugang
Mit dem Zugang wird der physikalische Zugang zu den Systemen der → PKI beschrieben.

Zugriff
Mit dem Zugriff wird der logische Zugriff auf der Betriebssystemebene der → PKI beschrieben.

Zutritt
Mit dem Zutritt wird der Zutritt zur technischen Infrastruktur der Südwestfalen-IT beschrieben.

X.509
Weit verbreiteter Standard für digitale Zertifikate. Das Format verlangt gewisse Standardinformationen, z.B. eine Email-Adresse, die den Inhaber des Zertifikats identifiziert.

11. Referenzen

[CPS] Lazik, Marco (2005), Certification Practice Statement, Iserlohn: SÜDWESTFALEN-IT Citkomm in der jeweils aktuellen Version

[CPPCA] Schmidt, Andreas (09.01.2003), Sicherheitsleitlinien der Wurzelzertifizieungsinstanz, Bonn: BSI Version 3.2

[CP_Neu] Ergänzungen und Änderungen zu den „Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung; Version 3.2 vom 09.01.2003; Stand: Version 1.1 vom 29.01.2013

[FormProt] BSI (25.11.2002 a), Zertifizierungsinfrastruktur für die PKI-1-Verwaltung: Technische Grundlagen der Wurzelzertifizierungsstelle, Formate und Protokolle nach MTTv2, Bonn: BSI Version 2.0

[GRP] Regelungen für Gruppenzertifikate, Bundesamt für Sicherheit in der Informationstechnik, Version 1.3 vom 10.12.2002

[IT-Grund] BSI (November 2004) *IT-Grundschutzhandbuch*, BSI: Bonn http://www.bsi.de/gshb/deutsch/index.htm (01.02.2005)

[Namreg] BSI (25.11.2002 b), Zertifizierungsinfrastruktur für die PKI-1-Verwaltung: Namensregeln und Formate, Bonn: BSI

[Postident] Deutsche Post AG Zentrale, Produktmanagement, Zusatz und Spezialleistungen BRIEF, 53250 Bonn, Stand 03/2007, Mat.-Nr. 675-201-121,
Hier: Postident BASIC

[RFC2314] Kaliski, B. (März 1998), PKCS#10: Certification Request Syntax, Network Working Group: RFC 2314
ftp://ftp.rfc-editor.org/in-notes/rfc2314.txt (02.04.2005)
(Version 1.5)

[RFC2527] S. Chokhani & W. Fork (1999), *Network Working Group: RFC 2527*
ftp://ftp.rfc-editor.org/in-notes/rfc2527.txt (21.02.2005)

[RFC3647] S. Chokhani et al. (2003), Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group: RFC 3647
ftp://ftp.rfc-editor.org/in-notes/rfc3647.txt (01.04.2005)

[Selbsterkl] BSI, Selbsterklärung der Zertifizierungsstelle
Version 3.00

[SigG] Der Bundespräsident Johannes Rau et al. (21.05.2001), "Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften", *Bundesgesetzblatt Jahrgang 2001 Teil 1 Nr. 22,* Bonn: Bundesanzeiger Verlagsges.mbH, 867 - 884

[SigV] Der Bundeskanzler Gerhard Schröder, Der Bundesminister für Wirtschaft und Technologie Müller (16.11.2001), "Verordnung zur elektronischen Signatur (Signaturverordnung - SigV)", *Bundesgesetzblatt Jahrgang 2001 Teil 1 Nr. 59,* Bonn: Bundesanzeiger Verlagsges.mbH, 3074 – 3084

[TeleSec] T-Systems International GmbH, Trust Center Services, Untere Industriestr. 20, D-57250 Netphen, E-Mail: info@t-systems.com

GNU Free Documentation

GNU Free Documentation License
Version {+1.2, November 2002+}

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other {+functional and useful+} document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative

works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other {+work, in any medium,+} that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. {+Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein.+} The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". {+You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.+}

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. {+(Thus,+} if the Document is in part a

textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. {+If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.+}

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A {+Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A+} "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, {+that is suitable for revising the document+} straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose {+markup, or absence of markup,+} has been {+arranged+} to thwart or discourage subsequent modification by readers is not Transparent. {+An image format is not Transparent if used for any substantial amount of text.+} A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML

or XML using a publicly available DTD, and standard-conforming simple {+HTML, PostScript or PDF+} designed for human modification. {+Examples of transparent image formats include PNG, XCF and JPG.+} Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated {+HTML, PostScript or PDF+} produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

{+A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.+}

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies {+(or copies in media that commonly have printed covers)+} of the {+Document,+} numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location {+from+} which the general network-using public has access to download using public-standard network {+protocols a complete Transparent copy of the Document, free of added material.+} If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified

Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has {+fewer+} than {+five), unless they release you from this requirement.+}

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section {+Entitled+} "History", {+Preserve+} its {+Title,+} and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section {+Entitled+} "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. {+For+} any section {+Entitled+} "Acknowledgements" or "Dedications", {+Preserve+} the {+Title of the section,+} and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers

or the equivalent are not considered part of the section titles.

M. Delete any section {+Entitled+} "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section {+to be Entitled+} "Endorsements" or to conflict in title with any Invariant Section.

{+O. Preserve any Warranty Disclaimers.+}

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section {+Entitled+} "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license {+notice, and that you preserve all their Warranty Disclaimers.+}

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections {+Entitled+} "History" in the various original documents, forming one section {+Entitled+} "History"; likewise combine any sections {+Entitled+} "Acknowledgements", and any sections {+Entitled+} "Dedications". You must delete all sections {+Entitled "Endorsements".+}

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, {+is called an "aggregate" if+} the copyright {+resulting from+} the compilation is {+not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included+} an {+aggregate,+} this License does not apply to the other works {+in+} the {+aggregate which+} are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one {+half+} of the entire aggregate, the Document's Cover Texts may be placed on covers that {+bracket+} the Document within the {+aggregate, or the electronic equivalent of covers if the Document is in electronic form.+} Otherwise they must appear on {+printed+} covers {+that bracket+} the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a

translation of this {+License, and all the license notices in the Document, and any Warrany Disclaimers,+} provided that you also include the original English version of this {+License and the original versions of those notices and disclaimers.+} In case of a disagreement between the translation and the original version of this {+License or a notice or disclaimer,+} the original version will prevail.

{+If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.+}

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this

License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright (c) YEAR YOUR NAME.
> Permission is granted to copy, distribute and/or modify this document
> under the terms of the GNU Free Documentation License, Version {+1.2+}
> or any later version published by the Free Software Foundation;
> with {+no+} Invariant {+Sections, no+} Front-Cover {+Texts,+} and {+no+} Back-Cover {+Texts.+}
> A copy of the license is included in the section entitled "GNU
> Free Documentation License".

If you have Invariant Sections, Front-Cover {+Texts and Back-Cover+} Texts, {+replace the "with...Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the+}
> Front-Cover Texts being {+LIST, and with the+} Back-Cover {+Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.+}

If your document contains nontrivial examples of program code, we

recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.