



Version 1.0

1	Einleitung.....	3
1.1	Überblick.....	3
1.2	Identifikation des Dokuments .....	3
1.3	Beschreibung und Teilnehmer der PKI .....	3
1.3.1	Zertifizierungsstelle (certification authority) .....	3
1.3.2	Registrierungsstellen (Registration Authorities = RA) .....	4
1.3.3	Teilnehmer der Zertifizierungsinfrastruktur .....	4
1.4	Anwendungsbereich .....	4
1.4.1	Zulässige Nutzung der Zertifikate .....	5
1.4.2	Vertrauensstufen der Signaturzertifikate .....	5
1.4.3	Vertrauensstufen der Authentifizierungszertifikate .....	5
1.4.4	Vertrauensstufen der Verschlüsselungs- und Authentisierungszertifikate .....	6
1.5	Verwaltung der Zertifizierungsrichtlinie .....	6
1.5.1	Verwaltung dieses Dokuments .....	6
1.5.2	Kontakt:.....	6
1.6	Definitionen und Abkürzungen .....	6
2	Veröffentlichungen und Verzeichnisdienst .....	7
2.1	Verzeichnisdienst .....	7
2.2	Veröffentlichung von Informationen.....	7
2.3	Aktualisierung der Informationen.....	7
2.4	Zugang zu den Informationsdiensten .....	7
3	Identifizierung und Authentifizierung .....	8
3.1	Namen .....	8
3.2	Identitätsüberprüfung bei Neuantrag.....	8
3.2.1	Nachweis des Besitzes des privaten Schlüssels.....	9
3.2.2	Authentisierung einer Organisationseinheit.....	9
3.2.3	Authentisierung einer Person .....	9
3.2.4	Nicht überprüfte Informationen .....	9
3.2.5	Unterschriftslegimitation .....	9
3.2.6	Cross-Zertifizierung .....	9
3.3	Identifizierung und Authentifizierung bei einer Zertifikatserneuerung .....	9
3.4	Identifizierung und Authentifizierung bei einem Widerruf .....	9
4	Anforderung an den Lebenszyklus des Zertifikats .....	10
4.1	Zertifikatsantrag (Erstantrag).....	10
4.2	Bearbeitung von Zertifikaterstanträgen und Zertifikatserstellung.....	10
4.3	Zertifikatsausgabe .....	10
4.4	Zertifikatsakzeptanz.....	11
4.5	Verwendung des Schlüsselpaares und des Zertifikats .....	11
4.6	Zertifikatserneuerung / Rezertifizierung .....	11
4.7	Zertifikats-/ Schlüsselerneuerung.....	11
4.8	Zertifikatsmodifizierung.....	11
4.9	Sperrung von Zertifikaten .....	12
4.9.1	Gründe für eine Sperrung .....	12
4.9.2	Wer kann eine Sperrung veranlassen? .....	12
4.9.3	Prozess bei einer Sperrung .....	12
4.10	Dienst zur Statusabfrage von Zertifikaten.....	12
4.11	Austritt aus dem Zertifizierungsdienst.....	12
4.12	Schlüssel hinterlegung und -wiederherstellung .....	12
5	Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen .....	14
5.1	Infrastrukturelle Sicherheitsmaßnahmen.....	14
5.2	Organisatorische Sicherheitsmaßnahmen .....	14
5.3	Personelle Sicherheitsmaßnahmen .....	14
5.4	Sicherheitsüberwachung .....	15
5.5	Archivierung.....	15



.....

5.6	Schlüsselwechsel .....	15
5.7	Kompromittierung und Wiederherstellung .....	15
5.8	Einstellung des Betriebs .....	15
6	Technische Sicherheitsmaßnahmen .....	16
6.1	Schlüsselerzeugung und Installation .....	16
6.2	Schutz des privaten Schlüssels .....	16
6.3	Weitere Aspekte des Schlüsselmanagements .....	16
6.4	Aktivierungsdaten .....	16
6.5	Sicherheitsmaßnahmen für Computer .....	16
6.6	Lebenszyklus der Sicherheitsmaßnahmen .....	16
6.7	Sicherheitsmaßnahmen für das Netzwerk .....	16
6.8	Zeitstempel .....	16
7	Profile für Zertifikate, Widerruflisten und Online-Statusabfragen .....	17
7.1	Zertifikatprofile .....	18
7.1.1	Signaturzertifikat (bw-trust Basic-CA) .....	18
7.1.2	Verschlüsselungs- und Authentisierungszertifikat (bw-trust Basic-CA) .....	19
7.1.3	Zertifikat für Windows-Logon (bw-trust Basic-CA) .....	20
7.1.4	EFS-Zertifikat (bw-trust Basic-CA) .....	21
7.1.5	SSL-Server (bw-trust Basic-CA) .....	22
7.1.6	Zertifikat des Windows Domain Controllers (bw-trust Basic-CA) .....	23
7.1.7	IPSec-Zertifikat (bw-trust Basic-CA) .....	24
7.2	Weitere Profile .....	25
7.2.1	Sperrliste der bw-trust Basic-CA .....	25
8	Konformitätsprüfung .....	26
9	Rahmenvorschriften .....	27
9.1	Anerkennung der Richtlinie .....	27
9.2	Gebühren/Entgelte .....	27
9.3	Finanzielle Verantwortung .....	27
9.4	Vertraulichkeit von Geschäftsinformationen .....	27
9.5	Schutz personenbezogener Daten (Datenschutz) .....	27
9.6	Urheberrechte .....	27
9.7	Verpflichtungen .....	27
9.8	Gewährleistung .....	27
9.9	Haftungsbeschränkung .....	27
9.10	Haftungsfreistellung .....	27
9.11	Inkrafttreten und Aufhebung .....	27
9.12	Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern Kommunikationswege: Service Desk (nach ITIL) .....	27
9.13	Änderungen der Richtlinien .....	28
9.14	Konfliktbeilegung .....	28
9.15	Geltendes Recht .....	28
9.16	Konformität mit dem geltenden Recht .....	28
9.17	Weitere Regelungen .....	28



# 1 Einleitung

## 1.1 Überblick

Dieses Dokument enthält sowohl Certification Policy (CP) als auch Certificate Practise Statements (CPS) Inhalte.

Der Anhang enthält eine Überführung zur Referenzgliederung RFC 3647<sup>1</sup>, dem Nachfolger des RFC 2527.

Das vorliegende Dokument tritt zum 01.10.2007 in Kraft. Das Dokument wird laufend je nach Erfordernis aktualisiert. Dies ist durch den Dokumentverantwortliche sicherzustellen, siehe Kapitel 1.5.

## 1.2 Identifikation des Dokuments

Diese Richtlinie wird unter der OID 1.3.6.1.4.1.28259.1.1 geführt. Die übergeordnete OID ist der Organisationseinheit bw-trust CA zugeordnet (<http://www.iana.org/assignments/enterprise-numbers>). 28259

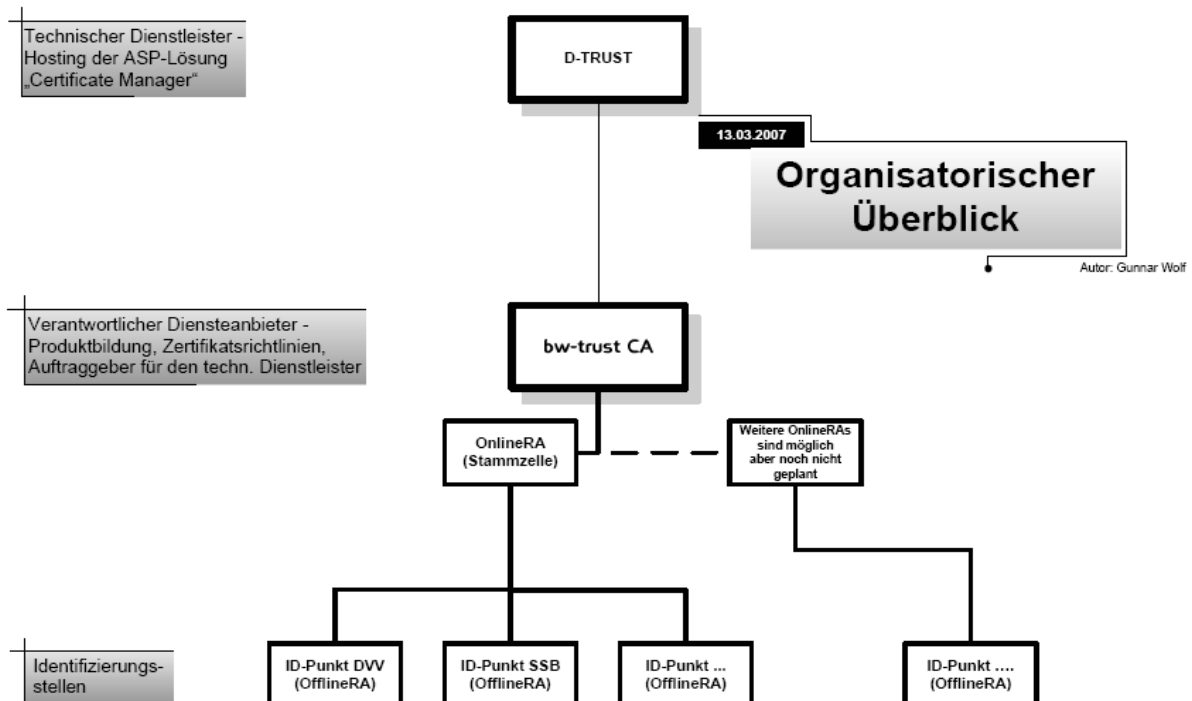
bw-trust CA  
Gunnar Wolf  
u10d001&stuttgart.de

## 1.3 Beschreibung und Teilnehmer der PKI

Die Landeshauptstadt Stuttgart betreibt unter dem Begriff bw-trust CA eine Einrichtung zur Ausstellung elektronischer Zertifikate für Identitäten der öffentlichen Verwaltung in Baden-Württemberg.

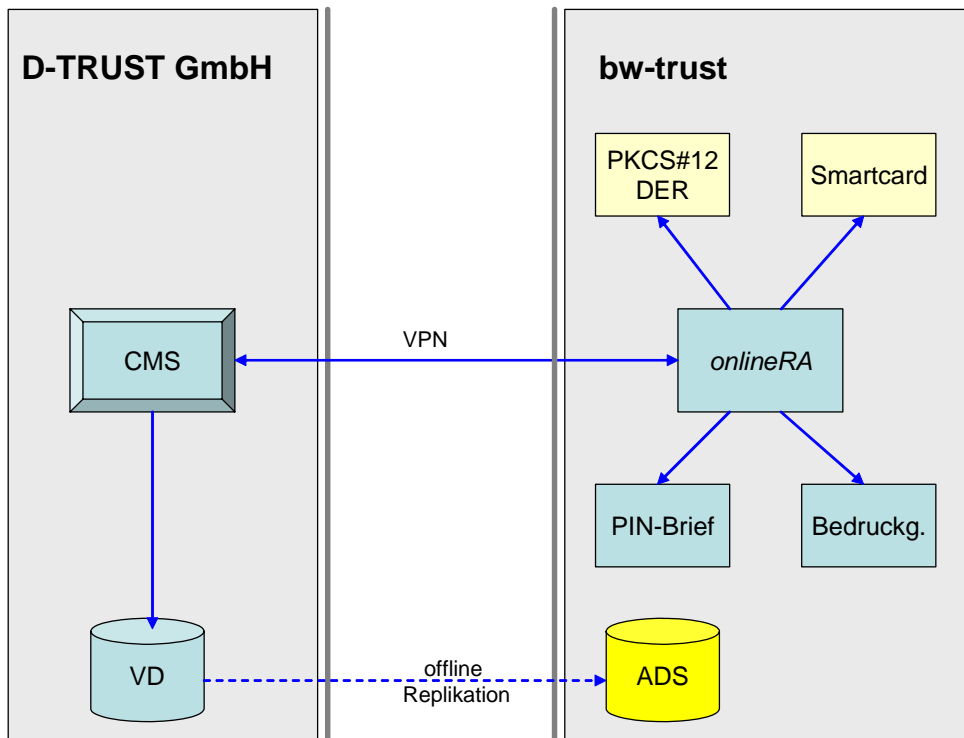
### 1.3.1 Zertifizierungsstelle (certification authority)

SubCAs sind derzeit nicht vorgesehen. Die Nutzung von Zertifikaten zur Erzeugung von weiteren Zertifikaten ist generell untersagt.



Zum Einsatz kommt eine Applikation (Certificate Management System) der Firma D-TRUST GmbH, in der die bw-trust CA abgebildet ist. Der Zugriff darauf wird mit der Hard-/Softwareumgebung der onlineRA über VPN-Tunnel realisiert.

<sup>1</sup> Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework



-----> = Option

### 1.3.2 Registrierungsstellen (Registration Authorities = RA)

Begriffsdefinition:

Die Einrichtung bw-trust CA betreibt mindestens eine onlineRA zur Registrierung der Antragsteller, mit deren Hilfe auch die Verarbeitung der Anträge in der CA durchgeführt wird. Sie besitzt die Berechtigung, Zertifikate für alle Organisationseinheiten der öffentlichen Verwaltung (inkl. Mehrheitsbeteiligungen) in Baden-Württemberg auszustellen. Weitere onlineRAs können beschränkt auf die Zuständigkeit bestimmter Organisationseinheiten aufgebaut werden.

Der ID-Punkt ist eine von der bw-trust CA autorisierte Identifizierungsstelle zur Prüfung der Antragsdaten inklusive Identitätsprüfung.

Die onlineRA kann auch die Aufgaben eines ID-Punktes wahrnehmen.

### 1.3.3 Teilnehmer der Zertifizierungsinfrastruktur

Teilnehmer an der Zertifizierungsinfrastruktur sind

-Nutzer in Form von

- Personen
- Pseudonymen
- Gruppen

-Maschinen, Komponenten und Anwendungen.

## 1.4 Anwendungsbereich

Zertifikate werden erstellt für Teilnehmer aus dem Bereich der öffentlichen Verwaltung inclusive der juristischen Personen mit Mehrheitsbeteiligung > 50 % der öffentlichen Hand.



### 1.4.1 Zulässige Nutzung der Zertifikate

Die Zertifikatsnutzung ist für folgende Anwendungsfälle erlaubt und vorgesehen:

#### Personenzertifikate

Produkt	qualifizierte Signatur	fortgeschrittene Signatur	Verschlüsselung Authentisierung	Windows-Domänen-Logon
<b>bw-trust ID-Card</b>		✓	✓	
<b>bw-trust ID-Card</b>		✓	✓	✓
<b>bw-trust ID-Card</b>				✓
<b>bw-trust PSE</b>		✓		
<b>bw-trust PSE</b>			✓	

#### Maschinenzertifikate

Produkt	EFS-Verschlüsselung	Maschinen-Authentisierung (SSL)	IPsec-Schlüssel	Windows-Domänen-Zertifikat
<b>bw-trust PSE</b>	✓			
<b>bw-trust DER oder PSE</b>		✓		
<b>bw-trust DER</b>			✓	
<b>bw-trust DER</b>				✓

### 1.4.2 Vertrauensstufen der Signaturzertifikate

Die bw-trust CA bietet die Ausstellung von Zertifikaten für die fortgeschrittene elektronische Signatur i.S. des Signaturgesetzes. Diese Zertifikate sind geeignet zur Absicherung von Prozessen des normalen und hohen Schutzbedarfs (ISO 27001 auf Basis von IT-Grundschutz), wenn der Antragsteller die dafür notwendigen weiteren Sicherheitsmaßnahmen realisiert hat.

### 1.4.3 Vertrauensstufen der Authentifizierungszertifikate

Die Vertrauensstufen unterscheiden sich nach der Art der Nutzung der Zertifikate. Wenn im Rahmen der automatisierten Verwendung die PIN einem Dienst übergeben wird bzw. der private Schlüssel ohne PIN-Schutz, verwendet werden kann, wird prinzipbedingt eine geringere Vertrauensstufe in Kauf genommen. In diesem Fall muss der erforderliche Schutz über die Rechteverwaltung der Produktumgebung gewährleistet werden.

Automatisierte Verwendung der Zertifikate bei

- Maschinen (SSL)
- IPsec-Netzverbindungen



Geschützte Verwendung der Zertifikate durch Eingabe einer PIN bei

- Personen, Pseudonymen, Gruppen
- Windows-Logon
- Preboot-Authentication

#### 1.4.4 Vertrauensstufen der Verschlüsselungs- und Authentisierungszertifikate

Diese Zertifikate sind geeignet zur Absicherung von Prozessen des normalen und hohen Schutzbedarfs (ISO 27001 auf Basis von IT-Grundschutz), wenn der Antragsteller die dafür notwendigen weiteren Sicherheitsmaßnahmen realisiert hat. Die bei der Verschlüsselung erreichte Vertrauensstufe hängt darüber hinaus von der Verwendung der Zertifikate im Rahmen von Anwendungen oder Produkten ab.

### 1.5 Verwaltung der Zertifizierungsrichtlinie

#### 1.5.1 Verwaltung dieses Dokuments

Dieses Dokument wird durch die Landeshauptstadt Stuttgart als Träger der Einrichtung „bw-trust CA“ veröffentlicht und gepflegt. Die Verwaltung dieser Einrichtung erfolgt durch die Abt. IuK des Haupt- und Personalamts.

Änderungen an diesem Dokument werden in einem internen Prozess (Arbeitsgruppe bw-trust) vorbereitet und durch eine formelle Freigabe des Trägers abgeschlossen. Sie treten mit der Veröffentlichung unter der Webadresse [www.bw-trust.de](http://www.bw-trust.de) in Kraft.

#### 1.5.2 Kontakt:

Postanschrift:

**bw trust CA**  
Landeshauptstadt Stuttgart  
Haupt- und Personalamt – Abt. IuK  
70173 Stuttgart

eMail:

[info@bw-trust.de](mailto:info@bw-trust.de)

Web:

[www.bw-trust.de](http://www.bw-trust.de)

Telefon:

0711-216-7325 oder -88 118

Telefax:

0711-216-957325 oder -953300

Hausadresse:

Eberhardstr. 6  
70178 Stuttgart

### 1.6 Definitionen und Abkürzungen

Hier werden keine Definitionen und Abkürzungen erläutert.



## 2 Veröffentlichungen und Verzeichnisdienst

### 2.1 Verzeichnisdienst

Der Verzeichnisdienst der bw-trust CA ist über eine ständig erreichbare *Adresse der D-Trust* (unter *ldap://directory.d-trust.net/ O=bw-trust%20Basic%20CA%20<Jahr>,C=DE*) erreichbar. Dabei wird der Begriff *<Jahr>* durch die jeweilige Jahreszahl ersetzt. Detaillierte Angaben sind dem Zertifikatsprofil zu entnehmen. Darunter können die Zertifikate der einzelnen Organisationseinheiten durch die Attribute *O=* bzw. *OU=* selektiert werden.

### 2.2 Veröffentlichung von Informationen

Diese Informationen werden über den zuvor beschriebenen Verzeichnisdienst bereitgestellt:

- Wurzelzertifikate der bw-trust Basic-CA
- Certificate Revocation Lists (CRL) der bw-trust Basic-CA

Darüber hinaus werden im Behördennetz Baden-Württembergs (LVN/KVN) per http-Protokoll die Wurzelzertifikate und die CRL unter <http://ca.bw-trust.de/cdp> veröffentlicht.

Darüber hinaus werden unter der Webadresse <http://ca.bw-trust.de> im Behördennetz Baden-Württemberg (KVN/LVN) verschiedene Informationen (Liste der ID-Punkte, Antragsformulare) zum Betrieb der CA veröffentlicht. Auch diese Zertifizierungsrichtlinie wird dort veröffentlicht.

### 2.3 Aktualisierung der Informationen

Zertifikate werden umgehend nach Ausstellung veröffentlicht. CRLs werden täglich aktualisiert.

### 2.4 Zugang zu den Informationsdiensten

Der Verzeichnisdienst im WWW ist generell für alle Nutzer erreichbar. Die Informationen im Behördennetz sind naturgemäß nur für deren Nutzer erreichbar.



### 3 Identifizierung und Authentifizierung

#### 3.1 Namen

Der Name der bw-trust Basic-CA wird in den Root-Zertifikaten gebildet aus dem Prefix „bw-trust Basic-CA“ und dem Zusatz des Ausstellungsjahrs des CA-Zertifikats (z.B. bw-trust Basic-CA 2007).

Die Teilnehmerzertifikate sind innerhalb der PKI durch den DN (distinguished name) eindeutig. Gegebenenfalls wird dies durch Zusätze im CN (common name) erreicht. Der DN enthält folgende Namenbestandteile:

c=de

O=[Name der juristischen Person]

OU1=[Organisationseinheit innerhalb der jur. Person]

OU2=[Organisationseinheit innerhalb der jur. Person] optional (nur bei Soft-PSE möglich)

CN= siehe nachfolgende Tabelle

Zertifikatstyp	Inhalt CN	Prüfung gegen	Subject Alternative Name
Natürliche Personen	[Titel] [Vorname] [Name]	Personalausweis oder Reisepass und Antragsunterlage	eMail-Adresse (SMTP)
Windows-Logon-Zertifikat	[Titel] [Vorname] [Name] des Zertifikatsinhabers lt. ActiveDirectory o.ä. Verzeichnisdienst	Antragsunterlage mit Angaben zur natürlichen Person	Universal Principal Name (UPN)
EFS-Zertifikat	[Titel] [Vorname] [Name] des Zertifikatsinhabers lt. ActiveDirectory o.ä. Verzeichnisdienst	Antragsunterlage mit Angaben zur natürlichen Person	eMail-Adresse (SMTP) der natürlichen Person
Pseudonyme	[Name]:PN	Antragsunterlage mit Angaben zur natürlichen Person	Optional: eMail-Adresse eines Posteingangsfachs
Gruppen	GRP:[Name]	Antragsunterlage mit Angaben zur Zusammensetzung der Gruppe und schlüsselverantwortlicher natürlichen Person	eMail-Adresse des Posteingangsfachs der Gruppe
Maschinen/ Netzkomponenten (SSL, IPsec)	[Name]	Antragsunterlage mit Angaben zur administrativen und schlüsselverantwortlichen natürlichen Person	Wenn nicht technisch anders gefordert = [Name]

Gruppennamen werden durch den Präfix GRP und Pseudonyme durch den Suffix PN gekennzeichnet.

Maschinen und Netzkomponenten sind mit dem in der benutzten Umgebung voll qualifizierenden Namen (FQDN) zu bezeichnen. Platzhalterzeichen wie „\*“ im Namen sind nicht zulässig. Die Domänenzugehörigkeit wird im Rahmen der Antragsbearbeitung auf Plausibilität geprüft.

#### 3.2 Identitätsüberprüfung bei Neuantrag

Für jedes Zertifikat ist der Schlüsselverantwortliche im Zertifikatsantrag zu benennen. Bei Personenzertifikaten ist dies der Inhaber des Zertifikats (Zertifikatsinhaber/ -nehmer). Bei Gruppen, Pseudonymen und Maschinen nimmt der Schlüsselverantwortliche alle Rechte und Pflichten des Zertifikatsinhabers wahr.



### 3.2.1 Nachweis des Besitzes des privaten Schlüssels

Selbsterstellte private Schlüssel sind nur für Zertifikate des Typs Maschinen/Netzkomponenten möglich. Der Besitz des Schlüssels ist bei der Beantragung zu versichern. Der Schlüsselverantwortliche übermittelt den Zertifikatsrequest im Format PKCS#10 an die OnlineRA.

### 3.2.2 Authentisierung einer Organisationseinheit

Die Identität und Bezeichnung einer Organisationseinheit ist durch deren Leiter per Unterschrift mit Dienstsiegel bzw. Firmenstempel zu bescheinigen.

### 3.2.3 Authentisierung einer Person

Die Identität einer natürlichen Person wird durch einen amtlichen Personalausweis oder Reisepass nachgewiesen. Dies erfolgt bei einem von bw-trust registrierten ID-Punkt oder in einer OnlineRA selbst. Der Umfang der Prüfung ist in der Tabelle in Abschnitt 3.1 dargestellt.

Die Zugehörigkeit einer natürlichen Person zu einer Organisationseinheit wird im Zertifikatsantrag durch den Leiter der Organisationseinheit bestätigt.

Im Antragsformular wird vermerkt, gegen welches Ausweisdokument die Authentisierung erfolgt ist.

### 3.2.4 Nicht überprüfte Informationen

Außer den Angaben in Abschnitt 3.2.2 und 3.2.3 werden keine weitere Informationen überprüft.

### 3.2.5 Unterschriftslegimitation

Für die Legitimation des Leiters einer Organisationseinheit reicht die Verwendung des Dienstsiegels bzw. Firmenstempels aus.

### 3.2.6 Cross-Zertifizierung

Cross-Zertifizierungen werden nur mit CAs der öffentlichen Verwaltung vorgenommen.

## 3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

Die Erneuerung eines Zertifikats kann vom Zertifikatsinhaber auch in elektronischer Form beantragt werden. Der Schlüsselverantwortliche kann die Erneuerung bzw. Verlängerung elektronisch beantragen, wenn er sich auf die Benachrichtigung über den bevorstehenden Ablauf der Gültigkeit bezieht.

## 3.4 Identifizierung und Authentifizierung bei einem Widerruf

Das Verfahren zur Sperrung ist in Kap 4.9 beschrieben.



## 4 Anforderung an den Lebenszyklus des Zertifikats

Die gewählte Gliederungsvariante erfordert nun Fallunterscheidungen innerhalb der Prozessbeschreibungen, sofern je nach Profil andere Regelungen notwendig sind.

### 4.1 Zertifikatsantrag (Erstantrag)

#### Prozessablauf:

1. Die Bedarfsstelle (Person, Gruppen-Handlungsbevollmächtigter, Serveradministrator) beantragt über das in elektronischer Form bereitgestellte Formular ein Zertifikat und gibt die notwendigen Daten ein.
2. Das Formular wird ausgedruckt. Dieses wird zum Leiter der Organisationseinheit (OU) weitergeleitet, von diesem mit dem Dienstsiegel / Firmenstempel versehen und unterschrieben.
3. Der Antragsteller geht zum ID-Punkt und gibt den Antrag ab.

Es wird vorausgesetzt, dass die Berechtigung zur Antragsstellung vorliegt, wenn ein unterschriebener und gesigelter Antrag der Organisation etc. vorgelegt wird. Identifizierung der natürlichen Person siehe Kapitel. 3.2.

Der Antrag auf ein Maschinenzertifikat (PKCS#10-Request) kann elektronisch gestellt werden, wenn der Antragsteller ein Schlüsselverantwortlicher mit persönlich zugeordnetem Zertifikat ist. Ferner muss beim ersten Antrag auf ein Maschinenzertifikat der Leiter der Organisationseinheit (OU) dem Schlüsselverantwortlichen schriftlich und mit Dienstsiegel / Firmenstempel das Recht zur Beantragung von Maschinenzertifikaten für eine konkrete Domäne bescheinigen.

### 4.2 Bearbeitung von Zertifikaterstanträgen und Zertifikatserstellung

#### Prozessablauf:

1. Beim ID-Punkt wird die Identität des Antragstellers (gem. Kapitel 3.2) sowie die in Papierform vorgelegten Zertifikatsanträge geprüft (Vollständigkeit und Plausibilität).
2. Wenn die Prüfung positiv abgeschlossen ist, werden die Daten vom ID-Punkt elektronisch erfasst bzw. zur Weiterverarbeitung an die onlineRA freigegeben.
3. Anschließend werden die Daten durch die onlineRA in das Certificate Management System importiert und die Zertifikatserstellung wird vorgenommen.

### 4.3 Zertifikatsausgabe

#### Prozessablauf:

1. Die OnlineRA übermittelt die erstellten Zertifikate und die PIN-Briefe an den ID-Punkt.
  - a. Bei SmartCards und PIN-Briefen per getrennter Post.
  - b. Bei Soft-PSE per eMail. Der PIN-Brief wird auf getrenntem Weg versandt. Bei Maschinenzertifikaten ist kein PIN-Brief erforderlich.
2. Der ID-Punkt gibt die Zertifikate und die PIN-Briefe entweder persönlich oder auf postalisch getrennten Wegen an die Bedarfsstelle aus.  
Dabei ist zu beachten, dass der Empfang der Zertifikate bestätigt wurde, bevor die PIN-Briefe versandt werden.
3. Das Antragsformular mit der dokumentierten Zertifikatsausgabe wird im ID-Punkt mit den zum Fall gehörigen Unterlagen archiviert.



#### 4.4 Zertifikatsakzeptanz

Die Akzeptanz eines Zertifikats erfolgt implizit durch Nutzung desselben. Der Zertifikatsinhaber ist verpflichtet, die Korrektheit des eigenen Zertifikats sowie des Zertifikats der Zertifizierungsstelle nach Erhalt unverzüglich zu überprüfen. Nach einem Zeitraum von 14 Tagen gilt es als akzeptiert. Fehlerhaft ausgestellte Zertifikate werden von der onlineRA widerrufen.

#### 4.5 Verwendung des Schlüsselpaares und des Zertifikats

Wer Zertifikate der bw-trust im Rahmen einer Signatur erhält oder zur Ver- und Entschlüsselung nutzt, oder im Rahmen dieser Richtlinie verwendet, muss

- den korrekten Einsatz gem. dem Schlüsselverwendungszweck (Key-Usages und Extended-Key-Usages) prüfen
- die aktuellen Statusinformationen aus der gültigen Sperrliste einbeziehen.

Ein Basiswissen zum Umgang mit Zertifikaten wird in den Organisationen und bei den Beteiligten vorausgesetzt.

Der private Schlüssel muss geschützt aufbewahrt werden. Eine PIN darf unautorisierten Personen nicht zugänglich gemacht werden..

#### 4.6 Zertifikatserneuerung / Rezertifizierung

Unter Zertifikatserneuerung / Rezertifizierung wird die Bereitstellung eines neuen Zertifikats unter Verwendung des zuvor verwendeten Schlüsselpaares verstanden (wenn die Schlüssellänge nach geltender Vorgabe der Bundesnetzagentur noch ausreichend ist und die Antragstellerdaten unverändert gültig sind). Eine Zertifikatserneuerung / Rezertifizierung kann nur für Zertifikate auf SmartCards durchgeführt werden.

##### Prozessablauf:

1. Vier Wochen vor Ablauf des Zertifikats erhält der Schlüsselverantwortliche eine Benachrichtigung mit dem Hinweis auf die Möglichkeit der Zertifikatserneuerung / Rezertifizierung.
2. Der Schlüsselverantwortliche sendet im Verlauf dieser vier Wochen den Antrag mit Signatur per Mail und die SmartCard per Post an den ID-Punkt. Dabei bestätigt er die Richtigkeit / weitere Gültigkeit aller Angaben.  
Alternativ kann der Antrag auch in Papierform gestellt werden, dann muss der Antragsteller persönlich mit gültigem Ausweis und SmartCard beim ID-Punkt erscheinen (vgl. Kapitel 4.1 und 3.2).
3. Der ID-Punkt prüft den Antrag gem. Kapitel 4.2 und leitet ihn an die onlineRA weiter. Fortsetzung des Prozesses erfolgt wie in Punkt 4.3 dargestellt.

#### 4.7 Zertifikats-/ Schlüsselerneuerung

Mit Zertifikats-/ Schlüsselerneuerung ist die erneute Ausstellung eines Zertifikats mit geänderten Schlüsseldaten und unverändert gültigen Antragstellerdaten gemeint.

Abgelaufene oder gesperrte Zertifikate müssen neu beantragt werden (Prozess wie in Punkt 4.1 ff dargestellt).

#### 4.8 Zertifikatsmodifizierung

Unter Zertifikatsmodifizierung wird die Bereitstellung eines neuen Zertifikats mit geänderten Zertifikatsinhalten verstanden. Vor Auslieferung des neuen Zertifikats wird automatisch durch die onlineRA das bisherige widerrufen.



.....

Eine Modifizierung ist nicht vorgesehen, es muss ein neuer Antrag (Prozess vgl. Punkt 4.1 ff) gestellt werden.

## 4.9 Sperrung von Zertifikaten

### 4.9.1 Gründe für eine Sperrung

Zertifikate müssen von der zuständigen Zertifizierungsstelle unverzüglich widerrufen werden, wenn mindestens einer der folgenden Gründe bekannt wird:

- Ein Zertifikat enthält Angaben, die nicht mehr gültig sind (z. B. wenn sich die Identität des Schlüsselverantwortlichen geändert hat)
- Der private Schlüssel des Schlüsselverantwortlichen wurde geändert oder kompromittiert
- Der Schlüsselverantwortliche hat seine Berechtigungsgrundlage verloren (z. B. bei Verlassen der Organisationseinheit bzw. Organisation oder bei Änderung der Aufgaben)
- Der Schlüsselverantwortliche hält die Zertifizierungsrichtlinie nicht ein

Zertifikate können darüber hinaus widerrufen werden, wenn

- die onlineRA oder die ID-Punkte die Zertifizierungsrichtlinie nicht einhalten
- der Zertifizierungsbetrieb von bw-trust eingestellt wird
- der onlineRA bei der Erstellung des Zertifikats ein Fehler unterlaufen ist

### 4.9.2 Wer kann eine Sperrung veranlassen?

Sperrberechtigt sind:

- der Zertifikatsinhaber bzw. der Schlüsselverantwortliche
- der Leiter der Organisationseinheit
- der ID-Punkt
- die onlineRA.

### 4.9.3 Prozess bei einer Sperrung

Die Sperrung erfolgt durch Mitteilung folgender Angaben:

- Name des Sperrantragstellers
- Name des Zertifikatsinhabers bzw. des Schlüsselverantwortlichen
- Seriennummer des Zertifikats, hilfsweise den Zertifikatstyp
- Sperrpasswort

an die Hotline der D-Trust. Diese ist erreichbar unter der Telefonnummer 0 30 / 25 93 91 - 6 02 (besetzt von Mo-Fr 09:00 – 17:00 Uhr, außer an bundeseinheitlichen Feiertagen) oder per Mail an [sperr@bw-trust.net](mailto:sperr@bw-trust.net)

Eine aktualisierte CRL wird im Rahmen des Betriebsablaufs unmittelbar nach einer Sperrung ausgestellt und veröffentlicht.

## 4.10 Dienst zur Statusabfrage von Zertifikaten

Die CRL wird in Verzeichnisdiensten der D-Trust und der bw-trust (vgl. Kapitel 2.1 und 2.2) zur Verfügung gestellt. Es wird keine weitere Überprüfungsmöglichkeit zur Verfügung gestellt.

## 4.11 Austritt aus dem Zertifizierungsdienst

Der Austritt aus dem Zertifizierungsdienst erfolgt mit Sperrung des Zertifikats oder mit Ablauf seiner Gültigkeit. Damit enden die vertraglichen Hauptleistungspflichten.

## 4.12 Schlüsselhinterlegung und -wiederherstellung

Es werden nur Schlüssel für Authentifizierungs- und Verschlüsselungszertifikate in Form von Soft-PSEs hinterlegt. Ein Antrag auf Schlüsselwiederherstellung kann für diese Zertifikate gestellt werden.

Prozess:



- Der Antrag auf Schlüsselwiederherstellung muss vom Schlüsselverantwortlichen an die onlineRA weitergeleitet werden.  
Folgendes muss enthalten sein:
  - Name des Schlüsselverantwortlichen
  - Seriennummer des Zertifikats
  - Sperrpasswort
- Der Antrag kann per E-Mail eingereicht werden und muss elektronisch signiert sein. Alternativ kann er auch in Papierform, mit Dienstsiegel / Firmenstempel und Unterschrift gestellt werden.
- Die onlineRA überprüft den Antrag auf Korrektheit und übermittelt das hinterlegte Zertifikat wie unter Ziffer 4.3 beschrieben.



## 5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb einer PKI.

### 5.1 Infrastrukturelle Sicherheitsmaßnahmen

Die ID-Punkte bestehen aus einem Standard-Büroarbeitsplatz mit IT-Ausstattung, einem Besucherplatz für eine diskrete Beratung sowie einem verschließbaren Aktenschrank und einem Aktenvernichter.

Die onlineRA befindet sich in den Räumen der bw-trust-CA bei der Landeshauptstadt Stuttgart, Eberhardstraße 6, 70173 Stuttgart. Das Büro und die darin betriebenen Komponenten sind im zutrittsgeschützten Bereich der Abteilung Informations- und Kommunikationstechnik untergebracht. Zum Einsatz kommt Hard- und Software der Firma D-TRUST, die über einen VPN-Tunnel mit dem Zertifikatsserver der Firma D-Trust verbunden ist. Das Equipment kann nur von dafür zugelassenen Personen in Betrieb genommen werden. Weitere Komponenten sind ein verschließbarer Aktenschrank, ein Aktenvernichter sowie ein Tresor.

Der Betrieb der Zertifizierungstechnik erfolgt durch Firma D-TRUST in Berlin, Kommandantenstraße 15, 10969 Berlin, innerhalb der für die Ausstellung qualifizierter Zertifikate mit Anbieterakkreditierung nach Signaturgesetz geprüften Sicherheitsumgebung. Die Zertifizierungstechnik der bw-trust-CA sowie deren Backups sind in versiegelten Serverschränken untergebracht, welche wiederum in biometrisch zutrittskontrollierten Räumen des D-Trust-Trustcenters aufgestellt sind. Die Überwachung der Sicherheit erfolgt entsprechend dem TÜV-geprüften Sicherheitskonzept des Trustcenters.

### 5.2 Organisatorische Sicherheitsmaßnahmen

Die für den Betrieb der CA zugelassenen Mitarbeiter werden durch Firma D-TRUST im Umgang mit der Infrastruktur und der ordnungsgemäßen Identifizierung der Antragsteller sowie der Dokumentation der Prozesse geschult. Die Mitarbeiter werden mit einem RA-Officer-Zertifikat ausgestattet, mit dem die Inbetriebnahme der Zertifizierungstechnik möglich ist.

Die für die Registrierung der Antragsteller zugelassenen Mitarbeiter (ID-Punkt-Mitarbeiter) werden in der Handhabung der Zertifikatsanträge und der ordnungsgemäßen Identifizierung der Antragsteller sowie der Dokumentation der Prozesse geschult.

### 5.3 Personelle Sicherheitsmaßnahmen

Folgende Rollen sind definiert:

- onlineRA-Mitarbeiter
- ID-Punkt-Mitarbeiter.

Anforderungen an den ID-Punkt-Mitarbeiter:

- Abgeschlossene Ausbildung in einem Verwaltungsberuf oder vergleichbare Qualifikation.
- Mitarbeiter sind kontinuierlich mit der Verwaltung verbunden.
- Polizeiliches Führungszeugnis ohne Einträge und nicht älter als drei Monate
- Schulung in der Handhabung der Zertifikatsanträge und der ordnungsgemäßen Identifizierung der Antragsteller sowie der Dokumentation der Prozesse

Anforderungen an den onlineRA-Mitarbeiter:

Es gelten die gleichen Anforderungen wie bei ID-Punkt-Mitarbeitern. Darüber hinaus muss die Schulung der onlineRA-Mitarbeiter durch D-TRUST erfolgen.



.....

Beim Betrieb der technischen Komponenten der bw-trust CA bei D-Trust kommt ein Rollenmodell zur Anwendung, das sicherstellt, dass sämtliche Aktionen im Vier-Augen-Modus ablaufen.

#### **5.4 Sicherheitsüberwachung**

Die Überwachung der festgelegten Sicherheitsmaßnahmen obliegt der in der Landeshauptstadt Stuttgart für die IT-Sicherheit und den Datenschutz zuständigen Organisationseinheit.

#### **5.5 Archivierung**

Die Antragsunterlagen werden bei den ID-Punkten, bei denen die Antragstellung erfolgt ist, für die Dauer von sechs Jahren archiviert.

Bei SmartCard-basierten Zertifikaten wird eine Mehrfertigung des PIN-Briefs im verschlossenen Umschlag bei der onlineRA archiviert.

#### **5.6 Schlüsselwechsel**

Das Ausstellerzertifikat der bw-trust-CA wird alle drei Jahre erneuert.

Die Schlüssel der bw-trust Basic-CA werden in einem HSM durch darin implementierte Schlüsselerzeugungsroutinen generiert und gespeichert. Das Schlüsselmaterial wird in verschlüsselter Form über spezielle Smartcards in ein Backup-HSM übertragen, um bei einem eventuellen Ausfall des HSM eine schnelle Wiederinbetriebnahme der CA zu ermöglichen.

#### **5.7 Kompromittierung und Wiederherstellung**

Sollte das Ausstellerzertifikat kompromittiert worden sein, muss ein Schlüsselwechsel vorgenommen werden und alle ausgestellten Zertifikate müssen gesperrt werden.

Die Wiederherstellung des Ausstellerzertifikates kann durch einen Reimport des gesicherten Schlüsselmaterials in den HSM erfolgen.

#### **5.8 Einstellung des Betriebs**

Falls der Betrieb von bw-trust Basic CA eingestellt wird, so wird dies den Teilnehmern rechtzeitig vorher mitgeteilt werden. Eine Migration zu einer Nachfolgelösung wird unterstützt. Bei Betriebsende werden alle Zertifikate gesperrt. Der Verzeichnisdienst wird bis zum Ablauf der Zertifikatsgültigkeit aufrechterhalten.



## 6 Technische Sicherheitsmaßnahmen

### 6.1 Schlüsselerzeugung und Installation

Die Schlüsselerzeugung für die CA findet in einem FIPS 140-2 Level 2-konformen HSM (Eracom ProtectServer Orange) nach den anwendbaren Vorgaben des Sicherheitskonzepts der Fa. D-TRUST in deren Räumen statt. Dasselbe gilt für die Ablage und den Schutz des Schlüsselmaterials im Certificate Management System.<sup>2</sup>

Das Schlüsselmaterial auf Smartcards wird während der Vorphysisierung auf der Karte selbst erzeugt und bis zur Endpersonalisierung durch Sicherheitsanker geschützt.

Das Schlüsselmaterial von Soft-PSEs wird innerhalb der Clientkomponente des Certificate Management Systems (onlineRA) erzeugt und durch eine PKCS#12-Datei passwortgeschützt.

### 6.2 Schutz des privaten Schlüssels

Siehe Fußnote<sup>3</sup>

### 6.3 Weitere Aspekte des Schlüsselmanagements

Alle von der bw-trust CA produzierten öffentlichen Schlüssel werden in Form der erstellten Zertifikate im Verzeichnisdienst gespeichert. Maschinenzertifikate und solche, deren Veröffentlichung vom Antragsteller nicht gewünscht ist, werden nicht öffentlich zugänglich geführt. Die veröffentlichten Zertifikate bleiben bis zum Ende der Gültigkeit und danach noch mindestens ein Jahr abrufbar.

Die Gültigkeitsdauer der Schlüssel und Zertifikate beträgt einheitlich drei Jahre und ist dem Zertifikat zu entnehmen.

### 6.4 Aktivierungsdaten

Der Zugang zum HSM ist im Sicherheitskonzept<sup>4</sup> der D-TRUST geregelt.

### 6.5 Sicherheitsmaßnahmen für Computer

Die für den Zertifizierungsbetrieb eingesetzten Computer, Netze und Komponenten wurden durch die von der Bundesnetzagentur anerkannte Prüf- und Bestätigungsstelle „TÜV Informationstechnik GmbH“ geprüft.

### 6.6 Lebenszyklus der Sicherheitsmaßnahmen

Das Sicherheitskonzept der D-TRUST sieht regelmäßige Auswertungen von Logfiles auf Regelverletzungen, Angriffsversuche und andere Vorfälle vor und beinhaltet eine Risikoanalyse.

### 6.7 Sicherheitsmaßnahmen für das Netzwerk

In diesem Zusammenhang ist mit Netzwerk die Verbindung der onlineRA zum Trustcenter von D-Trust gemeint. Diese Verbindung ist in Form eines VPN-Tunnels realisiert.

### 6.8 Zeitstempel

Ein Zeitstempeldienst wird nicht bereitgestellt.

<sup>2</sup> Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D-TRUST GmbH -qualifizierter Betrieb-

<sup>3</sup> Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D-TRUST GmbH -qualifizierter Betrieb-

<sup>4</sup> Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D-TRUST GmbH -qualifizierter Betrieb-



## 7 Profile für Zertifikate, Widerrufslisten und Online-Statusabfragen

Die PKI basiert auf den ISIS-MTT Spezifikationen der T7 und der TeleTrust Deutschland e.V in der Version 1.1 [1]. Damit wird die Interoperabilität zu international verbreiteten Standards wie X.509, PKIX, S/MIME und LDAP ermöglicht.

Für die Richtlinie der bw-trust Basic-CA wird folgende OID verwendet: 1.3.6.1.4.1.28259.1.1 (Registriert bei IANA - Internet Assigned Numbers Authority)

### Übersicht der vorgesehenen Verwendungen:

Produkt	qualifizierte Signatur	fortgeschrittene Signatur	Verschlüsselung Authentisierung	Windows-Domänen-Logon	Gültigkeit
<b>bw-trust ID-Card</b>		✓	✓		3 Jahre
<b>bw-trust ID-Card</b>		✓	✓	✓	3 Jahre
<b>bw-trust ID-Card</b>				✓	3 Jahre
<b>bw-trust PSE</b>		✓			3 Jahre
<b>bw-trust PSE</b>			✓		3 Jahre

Produkt	EFS-Verschlüsselung	Maschinen-Authentisierung (SSL)	IPsec-Schlüssel	Windows-Domänen-Zertifikat	Gültigkeit
<b>bw-trust PSE</b>	✓				3 Jahre
<b>bw-trust DER oder PSE</b>		✓			3 Jahre
<b>bw-trust DER oder PSE</b>			✓		3 Jahre
<b>bw-trust DER</b>				✓	5 Jahre



## 7.1 Zertifikatprofile

### 7.1.1 Signaturzertifikat (bw-trust Basic-CA)

Zertifikatsfeld	Inhalt
serialNumber	<serialNumber>
signatureAlgorithm	sha1WithRSAEncryption
issuer	CN = bw-trust Basic-CA <Jahr> O = bw-trust CA C = DE
validity	notBefore: (UTCTime) <notBefore> GMT notAfter: (UTCTime) <notBefore + 3 Jahre> GMT
subject	serialNumber = <subjectSerialNumber> <sup>1</sup> CN = <"Titel Vorname Name" des Zertifikatsinhabers> <sup>2</sup> OU = <Abteilung1> OU = <Abteilung2> <sup>3</sup> O = <Organisation> C = DE
subjectPublicKeyInfo	keyLength: 2048 Bit publicKeyAlgorithm: rsaEncryption
basicConstraints	critical: cA = false
keyUsage	critical: nonRepudiation, digitalSignature
extendedKeyUsage	emailProtection
authorityKeyIdentifier	keyID: ... (20 byte)
subjectKeyIdentifier	... (20 byte)
certificatePolicies	1.3.6.1.4.1.28259.1.1
subjectAlternativeName	email:<E-Mailadresse des Zertifikatsinhabers>
cRLDistributionPoints	URI:ldap://directory.d-trust.net/CN=bw-trust%20Basic-CA%20<Jahr>,O=bw-trust%20CA,C=DE?certificaterevocationlist?base? objectClass=crlDistributionPoint URI:http://ca.bw-trust.de/cdp/bw-trust%20Basic-CA%20<Jahr>.crl <sup>4</sup>

<sup>1</sup> wird durch D-TRUST vergeben (wird zur Unterscheidung der PIN-Briefe benötigt)

<sup>2</sup> Markierung von Gruppenzertifikaten durch Präfix "GRP:" erfolgt durch den Mitarbeiter der *onlineRA* (sofern nicht per XML definiert), Suffix für Pseudonyme ":PN" wird automatisch angehängen

<sup>3</sup> nur im Soft-PSE, falls angegeben

<sup>4</sup> Dieser CDP wird nicht durch D-TRUST verwaltet.



## 7.1.2 Verschlüsselungs- und Authentisierungszertifikat (bw-trust Basic-CA)

Zertifikatsfeld	Inhalt
serialNumber	<serialNumber>
signatureAlgorithm	sha1WithRSAEncryption
issuer	CN = bw-trust Basic-CA <Jahr> O = bw-trust CA C = DE
validity	notBefore: (UTCTime) <notBefore> GMT notAfter: (UTCTime) <notBefore + 3 Jahre> GMT
subject	serialNumber = <subjectSerialNumber> <sup>1</sup> CN = <"Titel Vorname Name" des Zertifikatsinhabers> <sup>2</sup> OU = <Abteilung1> OU = <Abteilung2> <sup>3</sup> O = <Organisation> C = DE
subjectPublicKeyInfo	keyLength: 2048 Bit publicKeyAlgorithm: rsaEncryption
basicConstraints	critical: cA = false
keyUsage	critical: digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage	clientAuthentication, emailProtection
authorityKeyIdentifier	keyID: ... (20 byte)
subjectKeyIdentifier	... (20 byte)
certificatePolicies	1.3.6.1.4.1.28259.1.1
subjectAlternativeName	email:<E-Mailadresse des Zertifikatsinhabers>
cRLDistributionPoints	URI:ldap://directory.d-trust.net/CN=bw-trust%20Basic-CA%20<Jahr>,O=bw-trust%20CA,C=DE?certificateRevocationList?base?objectClass=crlDistributionPoint URI:http://ca.bw-trust.de/cdp/bw-trust%20Basic-CA%20<Jahr>.crl <sup>4</sup>

<sup>1</sup> wird durch D-TRUST vergeben (wird zur Unterscheidung der PIN-Briefe benötigt)

<sup>2</sup> Markierung von Gruppenzertifikaten durch Präfix "GRP:" erfolgt durch Mitarbeiter der *onlineRA* (sofern nicht per XML definiert), Suffix für Pseudonyme ":PN" wird automatisch angehängen

<sup>3</sup> nur im Soft-PSE, falls angegeben

<sup>4</sup> Dieser CDP wird nicht durch D-TRUST verwaltet.



7.1.3 Zertifikat für Windows-Logon (bw-trust Basic-CA)

Zertifikatsfeld	Inhalt
serialNumber	<serialNumber>
signatureAlgorithm	sha1WithRSAEncryption
issuer	CN = bw-trust Basic-CA <Jahr> O = bw-trust CA C = DE
validity	notBefore: (UTCTime) <notBefore> GMT notAfter: (UTCTime) <notBefore + 3 Jahre> GMT
subject	serialNumber = <subjectSerialNumber> <sup>1</sup> CN = <Name des Zertifikatsinhabers wie in AD> OU = <Abteilung> O = <Organisation> C = DE
subjectPublicKeyInfo	keyLength: 2048 Bit publicKeyAlgorithm: rsaEncryption
basicConstraints	critical: cA = false
keyUsage	critical: digitalSignature, keyEncipherment
extendedKeyUsage	clientAuthentication, smartcardLogon (1.3.6.1.4.1.311.20.2.2)
authorityKeyIdentifier	keyID: ... (20 byte)
subjectKeyIdentifier	... (20 byte)
certificatePolicies	1.3.6.1.4.1.28259.1.1
subjectAlternativeName	otherName: UPN:<UPN des Zertifikatinhabers> (1.3.6.1.4.1.311.20.2.3)
cRLDistributionPoints	URI:ldap://directory.d-trust.net/CN=bw-trust%20Basic-CA%20<Jahr>,O=bw-trust%20CA,C=DE?certificaterevocationlist?base?objectClass=crlDistributionPoint URI:http://ca.bw-trust.de/cdp/bw-trust%20Basic-CA%20<Jahr>.crl <sup>2</sup>

<sup>1</sup> wird durch D-TRUST vergeben (wird zur Unterscheidung der PIN-Briefe benötigt)

<sup>2</sup> Dieser CDP wird nicht durch D-TRUST verwaltet.



## 7.1.4 EFS-Zertifikat (bw-trust Basic-CA)

Zertifikatsfeld	Inhalt
serialNumber	<serialNumber>
signatureAlgorithm	sha1WithRSAEncryption
issuer	CN = bw-trust Basic-CA <Jahr> O = bw-trust CA C = DE
validity	notBefore: (UTCTime) <notBefore> GMT notAfter: (UTCTime) <notBefore + 3 Jahre> GMT
subject	serialNumber = <subjectSerialNumber> <sup>1</sup> CN = <Name des Zertifikatsinhabers wie in AD> OU = <Abteilung> O = <Organisation> C = DE
subjectPublicKeyInfo	keyLength: 2048 Bit publicKeyAlgorithm: rsaEncryption
basicConstraints	critical: cA = false
keyUsage	critical: digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage	emailProtection , encryptedFileSystem (1.3.6.1.4.1.311.10.3.4), eFSFileRecovery (1.3.6.1.4.1.311.10.3.4.1)
authorityKeyIdentifier	keyID: ... (20 byte)
subjectKeyIdentifier	... (20 byte)
certificatePolicies	1.3.6.1.4.1.28259.1.1
subjectAlternativeName	email:<E-Mailadresse des Zertifikatinhabers>
cRLDistributionPoints	URI:ldap://directory.d-trust.net/CN=bw-trust%20Basic-CA%20<Jahr>,O=bw-trust%20CA,C=DE?certificaterevocationlist?base? objectClass=crlDistributionPoint URI:http://ca.bw-trust.de/cdp/bw-trust%20Basic-CA%20<Jahr>.crl <sup>2</sup>

<sup>1</sup> wird durch D-TRUST vergeben (wird zur Unterscheidung der PIN-Briefe benötigt)

<sup>2</sup> Dieser CDP wird nicht durch D-TRUST verwaltet.



7.1.5 SSL-Server (bw-trust Basic-CA)

Zertifikatsfeld	Inhalt
serialNumber	<serialNumber>
signatureAlgorithm	sha1WithRSAEncryption
issuer	CN = bw-trust Basic-CA <Jahr> O = bw-trust CA C = DE
validity	notBefore: (UTCTime) <notBefore> GMT notAfter: (UTCTime) <notBefore + 3 Jahre> GMT
subject	CN = <DNS-Name des Servers> OU = <Abteilung> O = <Organisation> C = DE
subjectPublicKeyInfo	keyLength: 2048 Bit publicKeyAlgorithm: rsaEncryption
basicConstraints	critical: cA = false
keyUsage	critical: digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage	clientAuthentication, serverAuthentication
authorityKeyIdentifier	keyID: ... (20 byte)
subjectKeyIdentifier	... (20 byte)
certificatePolicies	1.3.6.1.4.1.28259.1.1
subjectAlternativeName	email:<E-Mailadresse des Schlüsselerantwortlichen>
cRLDistributionPoints	URI:ldap://directory.d-trust.net/CN=bw-trust%20Basic-CA%20<Jahr>,O=bw-trust%20CA,C=DE?certificaterevocationlist?base? objectClass=crlDistributionPoint URI:http://ca.bw-trust.de/cdp/bw-trust%20Basic-CA%20<Jahr>.crl <sup>1</sup>

<sup>1</sup> Dieser CDP wird nicht durch D-TRUST verwaltet.



## 7.1.6 Zertifikat des Windows Domain Controllers (bw-trust Basic-CA)

Zertifikatsfeld	Inhalt
serialNumber	<serialNumber>
signatureAlgorithm	sha1WithRSAEncryption
issuer	CN = bw-trust Basic-CA <Jahr> O = bw-trust CA C = DE
validity	notBefore: (UTCTime) <notBefore> GMT notAfter: (UTCTime) <notBefore + 3 Jahre> GMT
subject	CN = <Name des Domänencontrollers> OU = <Abteilung> DC = <DC(s)>
subjectPublicKeyInfo	keyLength: 2048 Bit publicKeyAlgorithm: rsaEncryption
basicConstraints	critical: cA = false
keyUsage	critical: digitalSignature, keyEncipherment
extendedKeyUsage	clientAuthentication, serverAuthentication
authorityKeyIdentifier	keyID: ... (20 byte)
subjectKeyIdentifier	... (20 byte)
certificatePolicies	1.3.6.1.4.1.28259.1.1
subjectAlternativeName	otherName: <GUID> (1.3.6.1.4.1.311.25.1) DNS: <DNS-Name des Domänencontrollers>
Certificate Template Name (1.3.6.1.4.1.311.20.2)	DomainController
cRLDistributionPoints	URI:ldap://directory.d-trust.net/CN=bw-trust%20Basic-CA%20<Jahr>,O=bw-trust%20CA,C=DE?certificaterevocationlist?base?objectClass=crlDistributionPoint URI:http://ca.bw-trust.de/cdp/bw-trust%20Basic-CA%20<Jahr>.crl <sup>1</sup>

<sup>1</sup> Dieser CDP wird nicht durch D-TRUST verwaltet.



7.1.7 IPSec-Zertifikat (bw-trust Basic-CA)

Zertifikatsfeld	Inhalt
serialNumber	<serialNumber>
signatureAlgorithm	sha1WithRSAEncryption
issuer	CN = bw-trust Basic-CA <Jahr> O = bw-trust CA C = DE
validity	notBefore: (UTCTime) <notBefore> GMT notAfter: (UTCTime) <notBefore + 1 Jahre> GMT
subject	CN = <DNS des Servers> OU = <Abteilung> O = <Organisation> C = DE
subjectPublicKeyInfo	keyLength: 2048 Bit publicKeyAlgorithm: rsaEncryption
basicConstraints	cA = false
keyUsage	critical: digitalSignature
extendedKeyUsage	IPSec Intermediate System Usage (1.3.6.1.5.5.8.2.2)
authorityKeyIdentifier	keyID: ... (20 byte)
subjectKeyIdentifier	... (20 byte)
certificatePolicies	1.3.6.1.4.1.28259.1.1
subjectAlternativeName	<DNS-Name des Servers>
cRLDistributionPoints	URI:ldap://directory.d-trust.net/CN=bw-trust%20Basic-CA%20<Jahr>,O=bw-trust%20CA,C=DE?certificaterevocationlist?base?objectClass=crlDistributionPoint URI:http://ca.bw-trust.de/cdp/bw-trust%20Basic-CA%20<Jahr>.crl <sup>1</sup>



## 7.2 Weitere Profile

### 7.2.1 Sperrliste der bw-trust Basic-CA

Feld	Inhalt
version	2
signatureAlgorithm	sha1WithRSAEncryption
issuer	CN = bw-trust Basic-CA <Jahr> O = bw-trust CA C = DE
validity	lastUpdate: (UTCTime) <lastUpdate> GMT nextUpdate: (UTCTime) <lastUpdate + 5 Tage> GMT
authorityKeyIdentifier	keyID: ... (20 byte)
cRLNumber	< lfd. Nummer der CRL >
Liste gesperrter Zertifikate	revocationDate: (UTCTime) <revocationDate> GMT reasonCode: <cRLReasonCode>



## 8 Konformitätsprüfung

Dieses Kapitel bekommt erst Relevanz, wenn weitere Zertifizierungsstellen innerhalb der bw-trust Basic CA Struktur implementiert werden sollen. Zunächst werden dazu keine Aussagen getroffen.



## 9 Rahmenvorschriften

### 9.1 Anerkennung der Richtlinie

Diese Richtlinie wurde von der Landeshauptstadt Stuttgart als Träger der Einrichtung bw-trust CA mit Unterstützung der Firma D-TRUST als Dienstleister der PKI erstellt.

Alle weiteren PKI Teilnehmer erkennen die Richtlinie mit dem Zertifikatsantrag an (Teil des Auftrags).

### 9.2 Gebühren/Entgelte

Die aktuellen Entgelte für die Erstellung von Zertifikaten durch die bw-trust CA sind auf deren Webseiten in den Behördennetzen Baden-Württembergs unter <http://ca.bw-trust.de> abrufbar.

### 9.3 Finanzielle Verantwortung

Keine Regelungen erforderlich.

### 9.4 Vertraulichkeit von Geschäftsinformationen

Keine Regelungen erforderlich.

### 9.5 Schutz personenbezogener Daten (Datenschutz)

Die Landeshauptstadt Stuttgart als Träger der Einrichtung bw-trust CA hat ein IT-Sicherheitskonzept nach IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) erstellt.

### 9.6 Urheberrechte

Keine Regelungen erforderlich.

### 9.7 Verpflichtungen

Soweit nicht ausdrücklich zugesichert räumt bw-trust keine Garantien ein und macht keine Zusicherungen im Rechtssinn. bw-trust sorgt für die Identifizierung der Antragsteller und Schlüsselverantwortlichen gemäß dieser Richtlinie und die Zuordenbarkeit des öffentlichen Schlüssels zum Zertifikatsinhaber bzw. Schlüsselverantwortlichen. Die Korrektheit der Angaben im Zertifikat wird gewährleistet.

Die bw-trust-CA stellt sicher, dass ein in Zertifikaten verwendeter Name (*DistinguishedName*) des Zertifikatsinhabers (Feld *subject*) innerhalb der bw-trust-CA und über den Lebenszyklus des Zertifikats hinaus stets eindeutig ist.

### 9.8 Gewährleistung

Keine Regelungen erforderlich.

### 9.9 Haftungsbeschränkung

Keine Regelungen erforderlich.

### 9.10 Haftungsfreistellung

Keine Regelungen erforderlich.

### 9.11 Inkrafttreten und Aufhebung

Siehe Kap. 1.1

### 9.12 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern Kommunikationswege: Service Desk (nach ITIL)



.....

Mitteilungen der bw-trust CA an die Zertifikatsinhaber bzw. Schlüsselverantwortlichen werden an die letzte in den Unterlagen der bw-trust verzeichnete eMail-Adresse versendet.

### **9.13 Änderungen der Richtlinien**

Nachträge zu dieser Richtlinie werden in dieses Dokument eingearbeitet und unter derselben OID veröffentlicht. Auf den Webseiten der bw-trust-CA wird auf die erfolgten Änderungen zeitnah unter „Meldungen“ hingewiesen.

### **9.14 Konfliktbeilegung**

Keine Regelungen erforderlich.

### **9.15 Geltendes Recht**

Geltendes deutsches Recht wurde beachtet. Sofern geltendes Recht gegen Passagen dieser Richtlinie sprechen wird die Richtlinie entsprechend geändert, zudem gilt Absatz 9.16.

### **9.16 Konformität mit dem geltenden Recht**

Sofern aufgrund einer Gesetzesänderung eine Passage dieser Richtlinie ungültig wird, so bleibt der Rest weiterhin in Kraft.

### **9.17 Weitere Regelungen**

Direkte Absprachen zwischen den PKI Teilnehmern sind ungültig.

**>>> Ende des Dokuments <<<**