Vertrauensdiensteanbieter der Bundesagentur für Arbeit | 06.07.2023

Certificate Policy und Certification Practice Statement für qualifizierte Zertifikate der Bundesagentur für Arbeit

IT-Systemhaus

Inhaltsverzeichnis

Inhaltsverzeichnis 2

1 Einleitung 9

1.1 Überblick 9

1.2 Dokumentidentifikation 12

1.3 Teilnehmer des Dienstes 12

1.3.1 Zertifizierungsstellen (CA) und Zertifikatshierarchie 12

1.3.2 Registrierungsinstanzen 12

1.3.3 Antragsteller 12

1.3.3.1 Besteller (Subscriber) 12

1.3.3.2 Zertifikatsinhaber 12

1.3.4 Vertrauende Dritte (Relying Parties) 12

1.3.5 Weitere Teilnehmer 13

1.4 Anwendung von Zertifikaten 13

1.4.1 Zulässige Anwendung von Zertifikaten 13

1.4.2 Unzulässige Anwendung von Zertifikaten 13

1.5 Policy-Verwaltung 13

1.5.1 Organisation für die Verwaltung dieses Dokuments 13

1.5.2 Kontaktperson 13

1.5.3 Zuständigkeit für die Abnahme der CP 14

1.5.4 Abnahmeverfahren der CP 14

1.6 Definitionen und Abkürzungen 14

2 Veröffentlichung und Verzeichnisdienst 15

2.1 Verzeichnisdienste 15

2.2 Veröffentlichung von Zertifikatsinformationen 15

2.3 Häufigkeit und Zyklen für Veröffentlichungen 16

2.4 Zugriffskontrolle auf Verzeichnisse 16

3 Identifizierung und Authentisierung 17

3.1 Namensgebung 17

3.1.1 Namenstypen 17

3.1.2 Anforderungen an die Bedeutung von Namen 17

3.1.3 Anonymität und Pseudonyme für Zertifikatsinhaber 17

3.1.4 Regeln zur Interpretation verschiedener Namensformen 18

3.1.5 Eindeutigkeit von Namen 18

3.1.6 Erkennung, Authentisierung und Rolle von geschützten Namen 18

3.2 Erstmalige Identitätsprüfung 18

3.2.1 Methode zum Besitznachweis des privaten Schlüssels 18

3.2.2 Authentifizierung von Organisationen 18

3.2.3 Authentifizierung natürlicher Personen 18

3.2.4 Nicht verifizierte Teilnehmerinformationen 18

3.2.5 Überprüfung der Handlungsvollmacht 18

3.2.6 Kriterien für Zusammenwirkung 18

3.3 Identifizierung und Authentifizierung bei Schlüsselerneuerung 19
3.3.1 Identifizierung und Authentifizierung bei Routine-Schlüsselerneuerung 19
3.3.2 Identifizierung und Authentifizierung bei Schlüsselerneuerung nach Sperrung 19
3.4 Identifizierung und Authentifizierung beim Sperrantrag 19
3.5 Identifizierung und Authentifizierung beim Antrag auf Schlüsselwiederherstellung 19
4 Anforderungen an den Lebenszyklus des Zertifikats 20
4.1 Antragstellung für Zertifikate 20
4.1.1 Wer kann ein Zertifikat beantragen 20
4.1.2 Antragsprozess und Verantwortlichkeiten 20
4.2 Antragsbearbeitung 21
4.2.1 Durchführung der Identifikation und Authentifizierung 21
4.2.2 Annahme bzw. Ablehnung des Antrags 21
4.2.3 Fristen für die Antragsbearbeitung 21
4.3 Zertifikatserstellung 22
4.3.1 CA-Prozesse während der Zertifikatserstellung 22
4.3.2 Benachrichtigung des Zertifikatsinhabers über die Zertifikatserstellung 22
4.4 Zertifikatsannahme 22
4.4.1 Verfahren der Zertifikatsannahme 22
4.4.2 Veröffentlichung der Zertifikate durch den Zertifizierungsdienst 22
4.4.3 Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst 22
4.5 Nutzung des Schlüsselpaares und des Zertifikats 22
4.5.1 Nutzung durch den Zertifikatsinhaber 22
4.5.2 Nutzung durch vertrauende Dritte 23
4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Re-Zertifizierung) 23
4.6.1 Gründe für eine Zertifikatserneuerung 23
4.6.2 Wer kann eine Zertifikatserneuerung beantragen 23
4.6.3 Ablauf der Zertifikatserneuerung 23
4.6.4 Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung 23
4.6.5 Annahme einer Zertifikatserneuerung 24
4.6.6 Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst 24
4.6.7 Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst 24
4.7 Schlüssel- und Zertifikatserneuerung (Re-Key) 24
4.7.1 Gründe für eine Schlüssel- und Zertifikatserneuerung 24
4.7.2 Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen 24
4.7.3 Ablauf der Schlüssel- und Zertifikatserneuerung 24
4.7.4 Benachrichtigung des Zertifikatsinhabers nach Schlüssel- und Zertifikatserneuerung 25
4.7.5 Annahme der Schlüssel- und Zertifikatserneuerung 25
4.7.6 Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst 25
4.7.7 Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst 25
4.8 Zertifikatsmodifizierung 25
4.8.1 Gründe für eine Zertifikatsmodifizierung 25
4.8.2 Wer kann eine Zertifikatsmodifizierung beantragen 25

4.8.3 Ablauf der Zertifikatsmodifizierung 25
4.8.4 Benachrichtigung des Zertifikatsinhabers nach der Zertifikatsmodifizierung 25
4.8.5 Annahme der Zertifikatsmodifizierung 26
4.8.6 Veröffentlichung einer Zertifikatsmodifizierung durch den Zertifizierungsdienst ... 26
4.8.7 Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst 26
4.9 Sperrung und Suspendierungen von Zertifikaten 26
4.9.1 Gründe für eine Sperrung 26
4.9.2 Sperrberechtigte 26
4.9.3 Verfahren zur Sperrung 26
4.9.4 Fristen für die Beantragung einer Sperrung 27
4.9.5 Bearbeitungszeit für Anträge auf Sperrung 27
4.9.6 Prüfung des Zertifikatsstatus durch Dritte 27
4.9.7 Periode für die Erstellung der Sperrlisten 27
4.9.8 Maximale Latenz der Sperrlisten 27
4.9.9 Verfügbarkeit von Online-Sperrinformationen 28
4.9.10 Nutzung der Online-Sperrinformationen durch Dritte 28
4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen 28
4.9.12 Spezielle Anforderungen bei Kompromittierung privater Schlüssel 28
4.9.13 Gründe für die Suspendierung 28
4.9.14 Wer kann eine Suspendierung beantragen 28
4.9.15 Verfahren zur Suspendierung 28
4.9.16 Maximale Sperrdauer bei Suspendierung 28
4.10 Auskunftsdienste über den Zertifikatsstatus 28
4.10.1 Betriebseigenschaften 28
4.10.2 Verfügbarkeit 29
4.10.3 Optionale Funktionen 29
4.11 Ende der Nutzung (End of subscription) 29
4.12 Schlüsselhinterlegung und -wiederherstellung (Key Escrow und Recovery) 29
4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung 29
4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln 30
5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen 31
5.1 Infrastrukturelle Sicherheitsmaßnahmen 31
5.1.1 Lage und Konstruktion des Standortes 31
5.1.2 Zutrittskontrolle 31
5.1.3 Stromversorgung und Klimakontrolle 31
5.1.4 Schutz vor Wasserschäden 32
5.1.5 Brandschutz 32
5.1.6 Lagerung von Datenträgern 32
5.1.7 Entsorgung von Datenträgern 32
5.1.8 Ausgelagertes Backup 32
5.2 Organisatorische Sicherheitsmaßnahmen 32
5.2.1 Sicherheitskritische Rollen 32

5.2.2 Anzahl benötigter Personen bei sicherheitskritischen Aufgaben 32
5.2.3 Identifikation und Authentisierung von Rollen 32
5.2.4 Trennung von Rollen und Aufgaben 33
5.3 Personelle Sicherheitsmaßnahmen 33
5.3.1 Anforderungen an die Fachkunde und Erfahrung 33
5.3.2 Anforderungen an die Zuverlässigkeit 33
5.3.3 Anforderungen an die Schulung 33
5.3.4 Wiederholungen der Schulungen 33
5.3.5 Häufigkeit und Abfolge von Rollenwechsel 33
5.3.6 Sanktionen bei unzulässigen Handlungen 34
5.3.7 Vertragsbedingungen mit dem Personal beauftragter Dritter 34
5.3.8 An das Personal ausgehändigte Dokumente 34
5.4 Protokollierung sicherheitskritischer Ereignisse 34
5.4.1 Protokollierte Ereignisse 34
5.4.2 Auswertung von Protokolldaten 35
5.4.3 Aufbewahrungsfristen für Protokolldaten 35
5.4.4 Schutz der Protokolldaten 35
5.4.5 Sicherungsverfahren für Protokolldaten 35
5.4.6 Internes/externes Protokollierungssystem 35
5.4.7 Benachrichtigung des Auslösers eines Ereignisses 35
5.4.8 Schwachstellenbewertung 35
5.5 Archivierung von Protokolldaten 35
5.5.1 Arten von zu archivierenden Daten 36
5.5.2 Archivierungsfristen 36
5.5.3 Schutzvorkehrungen für das Archiv 36
5.5.4 Sicherungsverfahren für das Archiv 36
5.5.5 Anforderungen an den Zeitstempel der archivierten Daten 36
5.5.6 Internes oder externes Archivierungssystem 36
5.5.7 Verfahren zur Beschaffung und Verifizierung von Archivdaten 36
5.6 Schlüsselwechsel der Zertifizierungsinstanzen 36
5.7 Kompromittierung und Wiederherstellung (Disaster Recovery) 37
5.7.1 Prozeduren bei Sicherheitsvorfällen 37
5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen 37
5.7.3 Wiederherstellung nach Schlüsselkompromittierung 37
5.7.4 Aufrechterhaltung des Betriebs im Notfall 37
5.8 Einstellung der Tätigkeit 37
6 Technische Sicherheitsmaßnahmen 39
6.1 Erzeugung und Installation von Schlüsselpaaren 39
6.1.1 Erzeugung von Schlüsselpaaren 39
6.1.2 Übergabe privater Schlüssel an den Zertifikatsinhaber 39
6.1.3 Übergabe öffentlicher Schlüssel an den Zertifizierungsdiensteanbieter 39
6.1.4 Übergabe öffentlicher CA Schlüssel an Dritte (Relying Parties) 39
6.1.5 Schlüssellängen 39
6.1.6 Erzeugung und Prüfung der Schlüsselparameter 39

6.1.7 Verwendungszweck der Schlüssel 39
6.2 Schutz der privaten Schlüssel und der kryptographischen Module.....40
6.2.1 Standards für Schutzmechanismen und Bewertung der kryptographischen Module 40
6.2.2 Aufteilung der Kontrolle privater Schlüssel auf mehrere Personen 40
6.2.3 Treuhänderische Hinterlegung privater Schlüssel..... 40
6.2.4 Sicherung und Wiederherstellung privater Schlüssel 40
6.2.5 Archivierung privater Schlüssel..... 40
6.2.6 Transfer privater Schlüssel..... 40
6.2.7 Speicherung privater Schlüssel 40
6.2.8 Methoden zur Aktivierung privater Schlüssel..... 40
6.2.9 Methoden zur Deaktivierung privater Schlüssel..... 40
6.2.10 Methoden zur Vernichtung privater Schlüssel 41
6.2.11 Bewertung kryptographischer Module 41
6.3 Weitere Aspekte des Schlüsselmanagements 41
6.3.1 Archivierung öffentlicher Schlüssel 41
6.3.2 Verwendungsdauern von Zertifikaten und Schlüsselpaaren 41
6.4 Aktivierungsdaten.....41
6.4.1 Erzeugung und Installation von Aktivierungsdaten..... 41
6.4.2 Schutzmaßnahmen für Aktivierungsdaten..... 41
6.4.3 Weitere Aspekte zu Aktivierungsdaten..... 42
6.5 Sicherheitsbestimmungen für Computer 42
6.5.1 Spezifische Sicherheitsanforderungen für Computer 42
6.5.2 Bewertung der Computersicherheit..... 43
6.6 Technische Kontrollen des Software-Lebenszyklus 43
6.6.1 Systementwicklungsmaßnahmen 43
6.6.2 Sicherheitsmanagement 43
6.6.3 Bewertung der Maßnahmen zur Kontrolle des Lebenszyklus 43
6.7 Maßnahmen zur Netzwerksicherheit.....43
6.8 Zeitstempel 43
7 Profile 44
7.1 Zertifikatsprofile 44
7.1.1 Versionsnummer(n) 44
7.1.2 Zertifikatserweiterungen 44
7.1.3 Algorithmenbezeichner (OID) 44
7.1.4 Namensformen 44
7.1.5 Nutzung von Erweiterungen zu Namensbeschränkungen 45
7.1.6 Bezeichner für Zertifizierungsrichtlinien (OID) 45
7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen (Policy-Constraints) 45
7.1.8 Syntax und Semantik von Policy Qualifiern..... 45
7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (Certificate Policies) 45
7.2 Profil der Sperrlisten.....45
7.2.1 Versionsnummer(n) 45
7.2.2 Erweiterungen der Sperrlisten..... 45

7.3 OCSP-Profile 45
7.3.1 Versionsnummer(n) 45
7.3.2 OCSP-Erweiterungen 45
8 Revisionen und andere Bewertungen 47
8.1 Häufigkeiten von Revisionen 47
8.2 Identität und Qualifikation des Auditors 47
8.3 Beziehungen zwischen Auditor und zu untersuchender Partei 47
8.4 Umfang der Prüfungen 47
8.5 Maßnahmen bei Mängeln 48
8.6 Veröffentlichung der Ergebnisse 48
9 Weitere geschäftliche und rechtliche Regelungen 49
9.1 Gebühren 49
9.1.1 Gebühren für die Ausstellung oder Erneuerung von Zertifikaten 49
9.1.2 Gebühren für den Abruf von Zertifikaten 49
9.1.3 Gebühren für die Abfrage von Zertifikatsstatusinformationen 49
9.1.4 Gebühren für andere Dienstleistungen 49
9.1.5 Rückerstattungen 49
9.2 Finanzielle Verantwortung 49
9.2.1 Deckungsvorsorge 49
9.2.2 Weitere Vermögenswerte 49
9.2.3 Erweiterte Versicherung oder Garantie 49
9.3 Vertraulichkeit betrieblicher Informationen 49
9.3.1 Art der geheim zu haltenden Information 49
9.3.2 Öffentliche Informationen 50
9.3.3 Verantwortlichkeit für den Schutz von geheim zu haltender Information 50
9.4 Schutz personenbezogener Daten 50
9.4.1 Geheimhaltung 50
9.4.2 Vertraulich zu behandelnde Daten 50
9.4.3 Nicht vertraulich zu behandelnde Daten 50
9.4.4 Verantwortlichkeit für den Schutz privater Informationen 50
9.4.5 Einverständniserklärung zur Nutzung privater Informationen 50
9.4.6 Weitergabe von Informationen an Ermittlungsinstanzen oder Behörden 50
9.4.7 Sonstige Offenlegungsgründe 51
9.5 Geistiges Eigentum und dessen Rechte 51
9.6 Gewährleistung, Sorgfalts- und Mitwirkungspflichten 51
9.6.1 Verpflichtung der Zertifizierungsstelle 51
9.6.2 Verpflichtung der Registrierungsstelle 51
9.6.3 Verpflichtung des Antragstellers 51
9.6.4 Verpflichtung vertrauender Dritte 51
9.6.5 Verpflichtung weiterer Teilnehmer 51
9.7 Haftungsausschluss 51
9.8 Haftungsbegrenzungen 52
9.9 Schadensersatz 52

9.10 Gültigkeit der CP 52
9.10.1 Gültigkeitszeitraum 52
9.10.2 Vorzeitiger Ablauf der Gültigkeit 52
9.10.3 Konsequenzen des Ablaufs dieses Dokumentes 52
9.11 Individuelle Mitteilungen und Absprachen mit den Teilnehmern 52
9.12 Änderungen der Richtlinie 52
9.12.1 Verfahren für die Änderung 52
9.12.2 Benachrichtigungsverfahren und Veröffentlichungsperioden 52
9.12.3 Bedingungen für Änderungen der Objekt-Kennung (OID) 52
9.13 Schiedsverfahren 53
9.14 Geltende Gesetze 53
9.15 Konformität mit anwendbarem Recht 53
9.16 Sonstige Bestimmungen 53
9.16.1 Vollständigkeitsklausel 53
9.16.2 Abtretung der Rechte 53
9.16.3 Salvatorische Klausel 53
9.16.4 Vollstreckung (Anwaltskosten und Rechtsverzicht) 53
9.16.5 Höhere Gewalt (Force Majeure) 53
9.17 Andere Regelungen 53
9.17.1 Organisatorisch 53
9.17.2 Testmöglichkeiten 53
9.17.3 Menschen mit Behinderung 54
Abbildungsverzeichnis 55
Tabellenverzeichnis 56
Referenzen 57
Definitionen und Abkürzungen 59

1 Einleitung

1.1 Überblick

Die Bundesagentur für Arbeit (BA) hat seit dem 13.07.2017 für die Erstellung von qualifizierten Zertifikaten für elektronische Signaturen den Status eines qualifizierten Vertrauensdiensteanbieters im Sinne der [eIDAS].

Im Rahmen seiner Zertifizierungstätigkeit erstellt und verwaltet der qualifizierte Vertrauensdiensteanbieter der BA (VDA der BA) qualifizierte Zertifikate.

Der VDA der BA führt zu diesem Zweck folgende Prozesse durch:

- Registrierung natürlicher Personen
- Zertifikatserstellung
- Personalisierung, Ausgabe und Sperrung von Signaturkarten
- Veröffentlichung von Zertifikaten
- Sperrung von Zertifikaten einschließlich Bereitstellung des Sperrstatus.

Durch den VDA der BA ausgestellte Zertifikate können in zwei unterschiedliche Zertifikatshierarchien eingebunden sein.

- Die Legacy-Hierarchie.
- Die Standard-Hierarchie.

Die folgende Grafik zeigt die Legacy-Hierarchie:

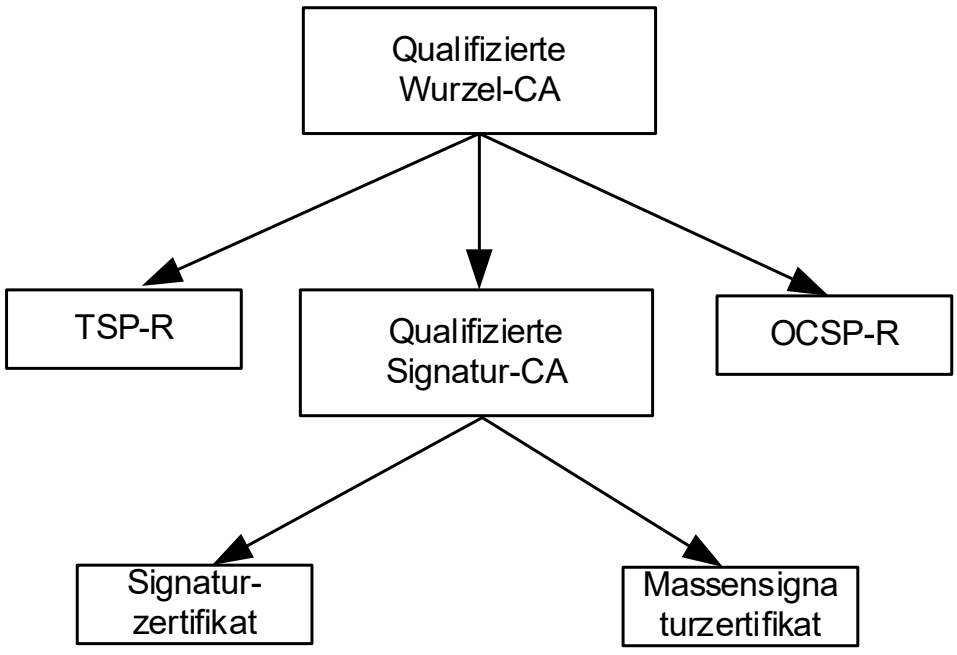
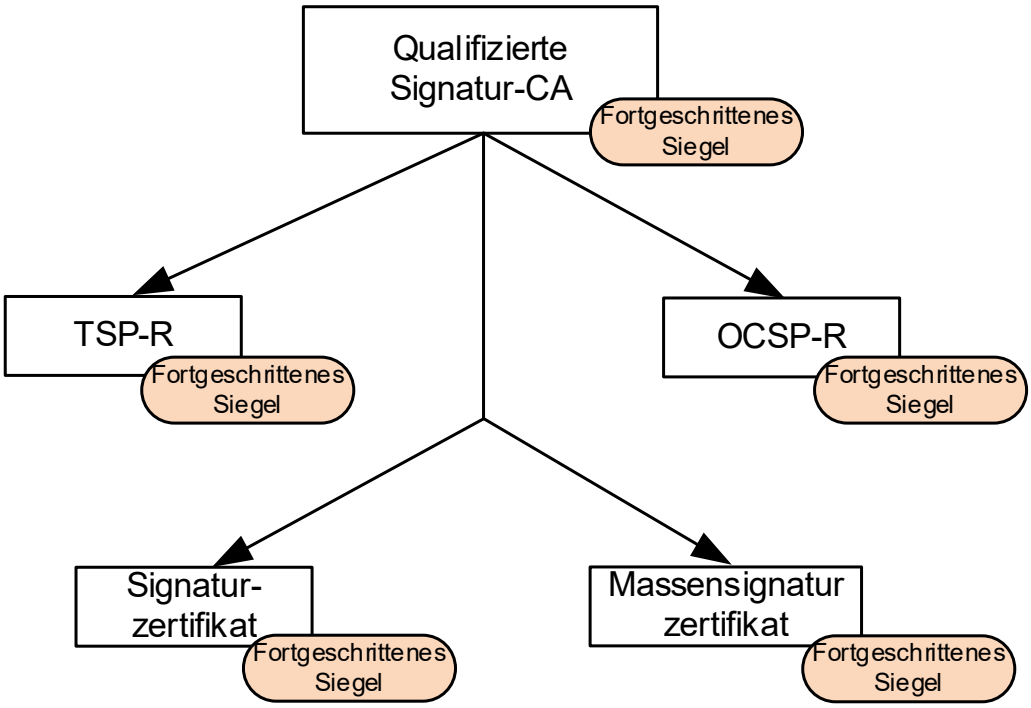


Abbildung 1 - qualifizierte Zertifikate in der Legacy-Hierarchie

Die beiden oberen Ebenen zeigen qualifizierte Zertifikate, die im Betrieb des Trustcenters (TCs) eingesetzt werden. Diese Zertifikate werden Dienstezertifikate genannt. Alle Zertifikate der Legacy-Hierarchie sind qualifizierte Zertifikate für elektronische Signaturen nach [eIDAS]. Sie enthalten eine qualifizierte elektronische Signatur des VDA der BA.

Die Legacy-Hierarchie wird spätestens Ende 2023 außer Betrieb genommen. Die OCSP-Responder der Standard-Hierarchie beauskunften dann die Zertifikate der Legacy-Hierarchie. Neue Zertifikate gehören dann zu folgender Standard-Hierarchie:



Die beiden oberen Ebenen zeigen nach wie vor Zertifikate, die im Betrieb des Trustcenters (TCs) eingesetzt werden. Diese Zertifikate werden nach wie vor Dienstezertifikate genannt. Im Unterschied zur Legacy-Hierarchie handelt es sich um Zertifikate für elektronische Siegel nach [eIDAS]. Die qualifizierten Dienste (qualifizierte Signatur-CA, TSP-R, OCSP-R) werden also durch nicht qualifizierte Zertifikate für elektronische Siegel gekennzeichnet.

Alle Zertifikate der Standardhierarchie enthalten ein fortgeschrittenes elektronische Siegel des VDA der BA. OCSP-Auskünfte und Zeitstempel aus der Standard-Hierarchie enthalten ebenfalls ein fortgeschrittenes elektronisches Siegel des VDA der BA.

Qualifizierte Zertifikate für elektronische Signaturen werden ausschließlich für Benutzer, z. B. Mitarbeiter der BA, ausgestellt. Diese Zertifikate werden, je nach Ausprägung, Signaturzertifikate oder Massensignaturzertifikate genannt.

Das Schlüsselpaar für die Erstellung und Prüfung eines fortgeschrittenen elektronischen Siegels bzw. einer qualifizierten elektronischen Signatur wird in der sicheren Umgebung des VDA der BA unter Verwendung einer qualifizierten Siegel- bzw. Signaturerstellungseinheit im Sinne der [eIDAS] erzeugt.

Ein qualifiziertes Zertifikat wird zusammen mit dem zugehörigen Signaturschlüsselpaar auf einer Chipkarte an den Zertifikatsinhaber ausgeliefert. Der Zertifikatsinhaber ist also gleichzeitig Signaturschlüsselinhaber. Bei dieser Chipkarte handelt es sich um eine qualifizierte elektronische Signaturerstellungseinheit (QSCD) im Sinne der [eIDAS].

Chipkarten werden in folgenden technischen Ausprägungen vom VDA der BA erstellt und verwaltet:

- Einzelsignaturkarte: Sie enthält ein Signaturzertifikat und wird abhängig vom Benutzerkreis als digitale Dienstkarte (dDk) oder Mandanten-Signaturkarte bezeichnet. Digitale Dienstkarten werden an Mitarbeiter der BA sowie an Mitarbeiter der gemeinsamen Einrichtung nach dem Sozialgesetzbuch II (SGB II) ausgegeben. Die Ausgabe an Mitarbeiter einer gemeinsamen Einrichtung impliziert einen *vorausgehenden* Einkauf der entsprechenden Dienstleistung durch die gemeinsame Einrichtung bei der BA.

  Mandanten-Signaturkarten werden an Mitarbeiter von Institutionen (Mandanten) ausgegeben, die Signaturkarten für ihre Mitarbeiter beantragen. Dies impliziert eine *vorausgehende* vertragliche Vereinbarung zwischen der BA und der Institution. **Neue Mandanten-Signaturkarten werden seit 01.01.2022 nicht mehr ausgegeben.**

- Massensignaturkarte: Sie enthält ein Massensignaturzertifikat und wird abhängig vom Benutzerkreis schlicht als Massensignaturkarte (für Mitarbeiter der BA im SGB III) oder Mandanten-Massensignaturkarte bezeichnet. Massensignaturkarten ermöglichen die Erstellung mehrerer qualifizierter Signaturen nach einmaliger Aktivierung des privaten Schlüssels im Sinne von Abschnitt 6.2.8. Für die Mandanten-Massensignaturkarte ist eine *vorherige* vertragliche Vereinbarung zwischen der BA und der Institution erforderlich. **Neue Mandanten-Signaturkarten werden seit 01.01.2022 nicht mehr ausgegeben.**

Dienstezertifikate werden im Folgenden nur noch betrachtet, wenn sie in ihrer Funktion relevant sind. Beantragung, Erstellung usw. werden hier nicht beschrieben.

Einzelsignaturkarten enthalten zusätzlich die folgenden Schlüsselpaare und nicht qualifizierten Zertifikate:

- **Authentisierung:** Ein Schlüsselpaar sowie ein zugehöriges Zertifikat (Authentisierungszertifikat) für die Durchführung zertifikatsbasierter Authentisierung (z. B. Login an Systemen). Dieses Zertifikat ermöglicht zudem die fortgeschrittene Signatur.
- **Verschlüsselung:** Ein Schlüsselpaar sowie ein zugehöriges Zertifikat (Verschlüsselungszertifikat) für die Ver- und Entschlüsselung von Daten.

Massensignaturkarten enthalten zusätzlich ein Schlüsselpaar und ein zugehöriges nicht qualifiziertes Zertifikat (Authentisierungszertifikat), das ausschließlich für die Freischaltung der Massensignaturkarte im Sinne des Abschnittes 4.4.1 genutzt wird.

Die genannten nicht qualifizierten Zertifikate erstellt und verwaltet der VDA der BA in folgender Zertifizierungshierarchie:

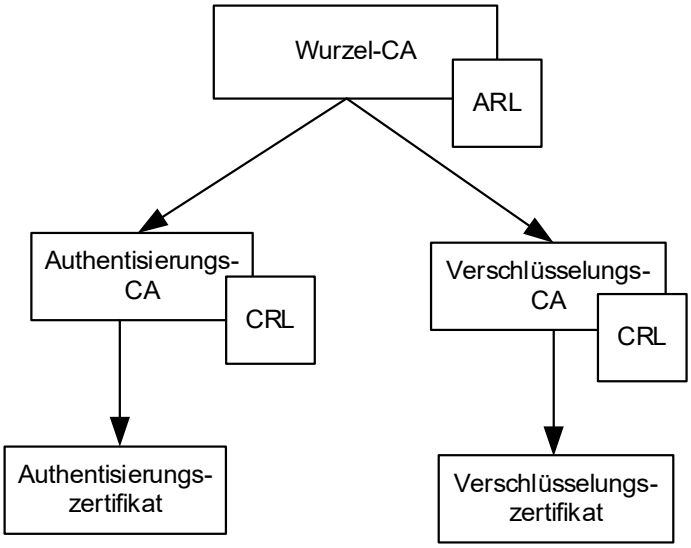


Abbildung 2 - nicht qualifizierte Zertifikate in der Zertifizierungshierarchie

Der Einfachheit halber wird vorliegendes Dokument als Certificate Policy (CP) bezeichnet, auch wenn es streng genommen die Kombination von Certificate Policy und Certification Practice Statement (CPS) für qualifizierte Zertifikate des VDA der BA ist. Die Dokumentstruktur orientiert sich am [RFC3647].

Die Zielsetzung einer Certificate Policy ist im [RFC3647] "Certificate Policy and Certification Practices Framework" ausführlich dargestellt. Inhaltlich basiert die Certificate Policy des VDA der BA zudem auf der ETSI-Policy [QCP-n-qscd], definiert aber z.T. schärfere Vorgaben. Die schärferen Vorgaben werden im vorliegenden Dokument an den relevanten Stellen explizit genannt.

Entsprechend den Vorgaben des [RFC3647] legt das Certification Practice Statement die Praktiken dar, die der VDA der BA bei der Beantragung, Generierung, Auslieferung und Verwaltung der Zertifikate

anwendet. Das vorliegende Dokument ermöglicht somit ebenfalls eine qualitative Einschätzung der Zertifizierungstätigkeit des VDA der BA.

Neben der Zertifizierungstätigkeit stellt der Vertrauensdiensteanbieter der BA auch qualifizierte Zeitstempel bereit. Sofern es nur seine Zertifizierungstätigkeit betrifft, wird der VDA der BA im vorliegenden Dokument auch als Zertifizierungsdiensteanbieter bezeichnet.

1.2 Dokumentidentifikation

Die Dokumentenbezeichnung lautet:

Certificate Policy und Certification Practice Statement für qualifizierte Zertifikate der Bundesagentur für Arbeit, Version: 5.1, Datum 06.07.2023

Das Dokument wird über folgenden Object Identifier (OID) referenziert: 1.3.6.1.4.1.21679.1.1.5.

Für die Referenzierung dieser Policy in Zertifikaten wird der obige Object Identifier im Zertifikat verwendet.

Bemerkung: Da es sich beim vorliegenden Dokument um eine Erweiterung der bisher unter dieser OID geführten „Certificate Policy der qualifizierten Signatur-CA der BA“ handelt, wurde der OID beibehalten.

1.3 Teilnehmer des Dienstes

1.3.1 Zertifizierungsstellen (CA) und Zertifikatshierarchie

Die Zertifizierungsstellen (CA) werden durch den VDA der BA betrieben. Sie erstellen die qualifizierten Zertifikate und Dienstezertifikate. Außerdem betreibt der VDA der BA einen Dienst zur sicheren Online-Abfrage von Informationen zum Sperrstatus dieser Zertifikate.

Zur Zertifizierungshierarchie vgl. Abschnitt 1.1.

1.3.2 Registrierungsinstanzen

Die Registrierung für Einzel- oder Massensignaturkarten wird in lokalen Registrierungsinstanzen (engl. Local Registration Authority, LRA) durchgeführt. Dort identifizieren die LRA-Registrare die Mitarbeiter, registrieren diese (Erfassung der notwendigen Daten) und beauftragen die Ausstellung entsprechender Zertifikate und Smartcards. Die LRA-Kartenausgeber händigen den Mitarbeitern (nach erneuter Identifizierung) gegen Unterschrift die Smartcard aus und veranlassen die Archivierung der entsprechenden Unterlagen.

1.3.3 Antragsteller

1.3.3.1 Besteller (Subscriber)

Abweichend von [QCP-n-qscd] können Besteller nur natürliche Personen sein. Sie sind nur in folgenden Fällen vom späteren Zertifikatsinhaber verschieden:

- Antragsteller für eine Massensignaturkarte ist ein zeichnungsbefugter Mitarbeiter, der von der Fachabteilung benannt wird, die für die Massensignaturanwendung zuständig ist.
- Mandanten-Signaturkarten bzw. -MSK werden von berechtigten Mitarbeitern des Mandanten beantragt. Neue Mandanten-Signaturkarten werden seit 01.01.2022 nicht mehr ausgegeben.

1.3.3.2 Zertifikatsinhaber

Abweichend von [QCP-n-qscd] können Zertifikatsinhaber nur natürliche Personen sein. Es handelt sich um Mitarbeiter der BA, einer gemeinsamen Einrichtung nach SGB II, die im Vorfeld die entsprechende Dienstleistung bei der BA eingekauft hat, oder des Mandanten.

1.3.4 Vertrauende Dritte (Relying Parties)

Empfänger qualifiziert elektronisch signierter Dokumente.

1.3.5 Weitere Teilnehmer

Keine.

1.4 Anwendung von Zertifikaten

1.4.1 Zulässige Anwendung von Zertifikaten

Die von der BA ausgegebenen qualifizierten Zertifikate und die entsprechenden Signaturschlüssel auf der dDk, MSK, Mandanten-Signaturkarte oder –MSK erfüllen die Anforderungen der [eIDAS] an qualifizierte Zertifikate für elektronische Signaturen, deren Signaturerstellungsdaten sich in einer qualifizierten elektronischen Signaturerstellungseinheit befinden. Die qualifizierten Zertifikate sind zur Nutzung wie in [QCP-n-qscd] beschrieben vorgesehen.

Das qualifizierte Signaturzertifikat einer dDk darf dabei ausschließlich für dienstliche Zwecke oder in der Kommunikation mit Behörden verwendet werden.

Die Anwendung des Signaturzertifikates einer MSK wird im Einsatzkonzept geregelt.

Für die Einschränkung der Anwendung von Signaturzertifikaten einer Mandanten-Signaturkarte oder –MSK gegenüber [QCP-n-qscd] ist der Mandant verantwortlich.

Bei der Nutzung der Zertifikate und Schlüsselpaare muss der Zertifikatsinhaber seine in der jeweiligen CP definierten Pflichten erfüllen.

Weitergehende Einschränkungen können sich aus mitgeltenden Dokumenten ergeben. In Frage kommen hier BA-interne Weisungen oder vertragliche Vereinbarungen, Gesamtkatalog der BA für gemeinsame Einrichtungen, Verwaltungsvereinbarung mit Mandanten.

1.4.2 Unzulässige Anwendung von Zertifikaten

Insbesondere gelten folgende Nutzungsbeschränkungen und -verbote:

- Mitarbeiterzertifikate und Mandanten-Zertifikate sind nicht zur Verwendung oder zum Weitervertrieb als Kontroll- oder Steuerungseinrichtung in gefährlichen Umgebungen oder für Verwendungszwecke, bei denen ein ausfallsicherer Betrieb erforderlich ist bzw. der Betrieb von nuklearen Einrichtungen, Flugzeugnavigations- oder Kommunikationssystemen, Luftverkehrs-Kontrollsystemen oder Waffenkontrollsystemen, wobei ein Ausfall direkt zum Tode, zu Personenschäden oder zu schweren Umweltschäden führen kann, vorgesehen oder darauf ausgelegt. Eine Verwendung zu solchen Zwecken wird ausdrücklich ausgeschlossen.
- Nach Ablauf der Gültigkeitsdauer oder Sperrung des Zertifikats dürfen die persönlichen Schlüssel nicht mehr zur Signierung verwendet werden.

1.5 Policy-Verwaltung

1.5.1 Organisation für die Verwaltung dieses Dokuments

Die Verwaltung des Dokuments erfolgt durch den VDA der BA. Informationen zur Änderung der Richtlinie finden Sie in Abschnitt 9.12. Für Kontaktinformationen zum VDA der BA siehe Abschnitt 1.5.2.

1.5.2 Kontaktperson

Die Revision und Freigabe des vorliegenden Dokuments unterliegt der ausschließlichen Verantwortung des VDA der BA.

Ansprechpartner für Fragen bezüglich dieser CP ist:

Bundesagentur für Arbeit
IT-Systemhaus
Vertrauensdiensteanbieter
Regensburger Straße 104
90478 Nürnberg
Internet: https://www.pki.arbeitsagentur.de
E-Mail: IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de

1.5.3 Zuständigkeit für die Abnahme der CP

Für die Verabschiedung dieser CP ist die VDA-Leitung zuständig. Zur Gültigkeit der CP siehe Abschnitt 9.10.

1.5.4 Abnahmeverfahren der CP

Die CP wird bei Bedarf durch den VDA der BA fortgeschrieben, vgl. Abschnitt 9.12. Nach einer Eignungsprüfung durch den Datenschutzbeauftragten und den Rechtsberater wird sie von der VDA-Leitung abgenommen.

1.6 Definitionen und Abkürzungen

Definitionen und Abkürzungen stehen am Ende des Dokumentes.

2 Veröffentlichung und Verzeichnisdienst

2.1 Verzeichnisdienste

Der VDA der BA betreibt die folgenden Verzeichnisdienste:

- Auf einer Webseite des VDA der BA werden Informationen des VDA wie Kontaktinformationen, CP und die Dienstezertifikate veröffentlicht. Die Webseite ist unter der URL

  https://www.pki.arbeitsagentur.de

  erreichbar.
- Über einen OCSP-Verzeichnisdienst kann der Status von qualifizierten Zertifikaten und Dienstezertifikaten abgerufen werden. Sofern der Zertifikatsinhaber zugestimmt hat, kann über den OCSP-Verzeichnisdienst auch das qualifizierte Zertifikat abgerufen werden. Die Verbindungsparameter des OCSP-Verzeichnisdienstes werden auf oben genannter Webseite veröffentlicht. Weitere Informationen zum OCSP-Verzeichnisdienst finden sich in Abschnitt 4.10.
- Über einen Verzeichnisdienst können die Zertifikate der qualifizierten Signatur-CAs abgerufen werden. Der zugehörige Abrufpfad ist ab 2023 in den Endbenutzerzertifikaten hinterlegt.

2.2 Veröffentlichung von Zertifikatsinformationen

Die folgende Tabelle gibt einen Überblick über die durch den VDA der BA im Zusammenhang mit der Ausstellung von qualifizierten Zertifikaten veröffentlichten Informationen sowie deren Veröffentlichungsort.

Zertifikatstyp	veröffentlicht in	Link
Qualifizierte Zertifikate und Dienstezertifikate	OCSP-Verzeichnis	http://ocsp.pki.arbeitsagentur.de/
Sperrstatusinformationen für qualifizierte Zertifikate und Dienstezertifikate	OCSP-Verzeichnis	http://ocsp.pki.arbeitsagentur.de/
Zertifikat und zugehöriger Hashwert (Fingerprint) der CA	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/
Signatur-CA-Zertifikate	LDAP/Web-Verzeichnis	Ab 2023 als AIA-Pfad im Endbenutzerzertifikat
Zertifikat und zugehöriger Hashwert (Fingerprint) des OCSP-Responders (Auskunftsdienst)	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/
Zertifikat und zugehöriger Hashwert (Fingerprint) des TSP-Responders (Zeitstempeldienst)	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/
CP für qualifizierte Zertifikate (vorliegendes Dokument)	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/
TSAPS	Web-Verzeichnis	https://www.pki.arbeitsagentur.de/

Tabelle 1 - Veröffentlichte Informationen

Das Sicherheitskonzept des VDA der BA sowie die technischen Spezifikationen, Betriebskonzepte und Arbeitsanweisungen enthalten vertrauliche Informationen und werden daher weder im Intranet noch im Internet veröffentlicht.

2.3 Häufigkeit und Zyklen für Veröffentlichungen

Vor der Verwendung des Signaturschlüsselpaares muss der Zertifikatsinhaber sein qualifiziertes Signaturzertifikat veröffentlichen. Die Veröffentlichung eines qualifizierten Signaturzertifikates wird vom Zertifikatsinhaber durch Aktivierung der übergebenen Smartcard ausgelöst.

Bei Sperrung eines qualifizierten Zertifikates wird dessen Sperrstatusinformation unverzüglich im OCSP-Verzeichnisdienst aktualisiert.

Die Veröffentlichung der CP für qualifizierte Zertifikate erfolgt jeweils nach der Freigabe der aktualisierten Version. Aktualisierungen der CP werden gemäß Kap. 9.12 veröffentlicht.

2.4 Zugriffskontrolle auf Verzeichnisse

Die im Internet veröffentlichte Information ist öffentlich zugänglich. Der Lesezugriff auf den Verzeichnisdienst ist also nicht beschränkt. Dagegen haben nur berechtigte Rollenträger oder Systeme Änderungsrechte für den Verzeichnisdienst.

Die BA hat entsprechende Sicherheitsmaßnahmen implementiert, um ein unbefugtes Ändern von Einträgen in den Verzeichnisdiensten zu verhindern.

3 Identifizierung und Authentisierung

3.1 Namensgebung

Es gelten die Regelungen des Standard [X509] bzw. seiner Profilierung in [RFC5280] bzw. dessen Profilierung in [COMPKI]. Aufgrund der Berücksichtigung von [COMPKI] sind die Anforderungen höher als in [QCP-n-qscd] beschrieben.

3.1.1 Namenstypen

Es gelten die Regelungen des Standard [X509] bzw. seiner Profilierung in [RFC5280] bzw. dessen Profilierung in [COMPKI]. Zertifikatsprofile finden sich in Abschnitt 7.1.

3.1.2 Anforderungen an die Bedeutung von Namen

Für das Feld `Subject` gelten zusätzlich folgende Festlegungen:

- Attribut `CountryName`: <DE>
- Attribut `Organization`: <Bundesagentur fuer Arbeit>
- Attribut `Surname`: <[Doktorgrad] Nachname des Zertifikatshalters wie im Ausweisdokument> für natürliche Personen. Ist der Doktorgrad im amtlichen Ausweisdokument vermerkt, kann er auf Wunsch des Antragstellers bei der Registrierung weggelassen werden. Ist der Doktorgrad im amtlichen Ausweisdokument nicht vermerkt, wird er bei der Registrierung nicht erfasst.
- Attribut `GivenName`: <Vorname des Zertifikathalters wie im Ausweisdokument> für natürliche Personen.
- Attribut `CommonName` (CN): <<Vorname> <Nachname>>, wobei Vorname identisch sein muss mit dem Attribut GivenName und Nachname identisch sein muss mit dem Attribut Surname (inkl. optionalem Doktorgrad). Ist ein cn in der oben genannten Form zu lang, so wird er auf die maximal zulässige Länge (64 Zeichen) gekürzt. Dabei werden zuerst die Titel und Vornamen gekürzt.

  Bei Massensignaturkarten oder Mandanten-Massensignaturkarten wird der CN im Einsatzkonzept der Massensignaturkarte bzw. durch den Mandanten festgelegt. Er enthält in jedem Fall ein Pseudonym, vgl. Abschnitt 3.1.3.
- Attribut `SerialNumber`: Der Wert wird vom VDA der BA generiert und bezeichnet den Zertifikatsinhaber eindeutig. Zu seiner Bestimmung werden Vorname, zweiter Vorname, Geburtsname, Geburtsort, Geburtsdatum des Zertifikatsinhabers benutzt.

3.1.3 Anonymität und Pseudonyme für Zertifikatsinhaber

Die Verwendung von Pseudonymen in Signaturzertifikaten wird nicht unterstützt. Der Pseudonymverzicht wird durch Unterschrift des Zertifikatsinhabers im Registrierungsprozess bestätigt.

Für die Dienstezertifikate werden, abhängig von der CA-Hierarchie, unterschiedliche Zertifikate eingesetzt:

- In der Legacy-Hierarchie werden für die benötigten qualifizierten Zertifikate der CA sowie des OCSP-Responder und des Zeitstempeldienstes (Dienstezertifikate) auf Mitarbeiter des Zertifizierungsdienstes (Rolle Sicherheitsoffizier) ausgestellte Zertifikate verwendet. Die Sicherheitsoffiziere können anhand des Attributes `SerialNumber` im Feld `Subject` des Dienstezertifikates identifiziert werden. Dienstezertifikate tragen ein Pseudonym im Attribut `CommonName` des `Subject`, das mit dem Suffix „:PN“ gekennzeichnet ist.
- In der Standard-Hierarchie werden für die benötigten Zertifikate der CA sowie des OCSP-Responder und des Zeitstempeldienstes (Dienstezertifikate) Zertifikate für elektronische Siegel eingesetzt. Dienstezertifikate tragen ein Pseudonym im Attribut CommonName des Subject, das mit dem Suffix „:PN“ gekennzeichnet ist.

Der Inhaber eines Massensignaturzertifikates kann anhand des Attributes `SerialNumber` im Feld `Subject` dieses Zertifikates identifiziert werden. Massensignaturzertifikate tragen ebenfalls ein Pseudonym im Attribut `CommonName` des `Subject`, das mit dem Suffix „:PN“ gekennzeichnet ist.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Es gelten die Regelungen des Standard [X509] bzw. seiner Profilierung in [RFC5280] bzw. dessen Profilierung in [COMPKI]. Aufgrund der Berücksichtigung von [COMPKI] sind die Anforderungen höher als in [QCP-n-qscd] beschrieben.

3.1.5 Eindeutigkeit von Namen

Qualifizierte Zertifikate können anhand des Attributes `SerialNumber` im Feld `Subject` eindeutig ihrem Inhaber zugeordnet werden. Aufgrund der Generierung der `SerialNumber`, vgl. Abschnitt 3.1.2, sind verschiedenen Personen verschiedene Werte der `SerialNumber` zugeordnet.

3.1.6 Erkennung, Authentisierung und Rolle von geschützten Namen

Der Wert des Feldes `Subject` in den ausgestellten Signaturzertifikaten ist im Wesentlichen identisch mit dem Namen des Zertifikatsinhabers in seinem Ausweis, also der Name einer natürlichen Person. Somit ist der Namensschutz gegeben.

Der Besteller einer Massensignaturkarte oder Mandaten-Massensignaturkarte ist hinsichtlich der Wahl des Pseudonyms für die Einhaltung von Namensrechten verantwortlich. Der Namensraum der verwendeten Pseudonyme in den Dienstezertifikaten wird vom Zertifizierungsdienst geprüft und freigegeben.

3.2 Erstmalige Identitätsprüfung

3.2.1 Methode zum Besitznachweis des privaten Schlüssels

Die Schlüsselpaare werden in der sicheren Umgebung des VDA der BA erzeugt. Daher ist kein Besitznachweis nötig.

3.2.2 Authentifizierung von Organisationen

Die Authentifizierung von Organisationen entfällt, da die BA keine Zertifikate für Organisationen ausstellt.

3.2.3 Authentifizierung natürlicher Personen

Bei der Registrierung für ein qualifiziertes Zertifikat muss sich der künftige Zertifikatsinhaber in der LRA persönlich durch einen gültigen amtlichen Ausweis sowie durch eine Gegenprobe der im Ausweis abgebildeten Unterschrift identifizieren. Zu den erhobenen Daten vergleiche Abschnitt 3.1.2.

Ein LRA-Rolleninhaber darf *nicht* seine eigene Identifikation durchführen.

Zur Referenzierung des verwendeten Ausweisdokumentes werden Ausweisnummer, der Typ des Ausweises und das Gültigkeitsdatum erhoben.

3.2.4 Nicht verifizierte Teilnehmerinformationen

Alle Informationen des Zertifikatsinhabers, die in das qualifizierte Zertifikat übernommen werden sollen, werden verifiziert.

3.2.5 Überprüfung der Handlungsvollmacht

Entfällt, da kein entsprechendes Attribut im Zertifikat aufgenommen wird.

3.2.6 Kriterien für Zusammenwirkung

Kriterien zur Zusammenwirkung entfallen.

3.3 Identifizierung und Authentifizierung bei Schlüsselerneuerung

3.3.1 Identifizierung und Authentifizierung bei Routine-Schlüsselerneuerung

Die routinemäßige Schlüsselerneuerung (d. h. Ausstellung eines neuen Zertifikates zu einem neuen Schlüssel kurz vor oder nach dem regulären Ablauf des alten Zertifikates) in einem automatisierten Prozess wird ausschließlich für dDk und bei unveränderten Stammdaten durchgeführt. Die Identifizierung und Authentisierung erfolgt erst bei der Übergabe der neuen Signaturkarte anhand eines gültigen Ausweisdokumentes. Sie entspricht dem Verfahren zur Zertifikatsannahme, vgl. Abschnitt 4.4.1, dient hier aber der Verifikation, dass sich die Stammdaten nicht geändert haben.

3.3.2 Identifizierung und Authentifizierung bei Schlüsselerneuerung nach Sperrung

Bei unveränderten Stammdaten erfolgt die Identifizierung und Authentifizierung bei einer Schlüsselerneuerung nach einer Sperrung (d. h. bei der Ausstellung eines neuen Zertifikates zu einem neuen Schlüssel nach einer Sperrung) erst bei der Übergabe der neuen Smartcard anhand eines gültigen Ausweisdokumentes. Sie entspricht dem Verfahren zur Zertifikatsannahme, vgl. Abschnitt 4.4.1, dient hier aber der Verifikation, dass sich die Stammdaten nicht geändert haben.

Bei geänderten Stammdaten ist eine Identifizierung nach Abschnitt 3.2 erforderlich.

3.4 Identifizierung und Authentifizierung beim Sperrantrag

Bezüglich der Identifizierung und Authentisierung beim Sperrantrag werden die folgenden Fälle unterschieden:

- Bei einer telefonischen Sperrung authentisiert sich der Beantragende durch seine E-Mail-Adresse und das Sperrpasswort, das er der Smartcard bei der Registrierung zugeordnet hat.
- Bei einer schriftlichen Sperrung authentisiert sich der Beantragende gegenüber dem Sperroperator durch die erforderlichen Daten auf dem Sperrantrag sowie durch seine eigenhändige Unterschrift.
- Bei der Durchführung einer Sperrung durch den Sperroperator Webportal oder dem LRA-Sperroperator authentisiert sich dieser mit seinem persönlichen Zertifikat gegenüber der Anwendung.

3.5 Identifizierung und Authentifizierung beim Antrag auf Schlüsselwiederherstellung

Es findet keine Schlüsselwiederherstellung für private Signaturschlüssel statt.

4 Anforderungen an den Lebenszyklus des Zertifikats

4.1 Antragstellung für Zertifikate

4.1.1 Wer kann ein Zertifikat beantragen

Die zulässigen Antragsteller sind in Abschnitt 1.3.3 aufgeführt.

4.1.2 Antragsprozess und Verantwortlichkeiten

Vor der Beantragung einer Mandanten-Signaturkarte oder Mandanten-Massensignaturkarte ist eine vertragliche Vereinbarung zwischen der BA und dem Mandanten erforderlich.

Zur Beantragung von Mandanten-Signaturkarten bzw. -MSK benennt der Mandant dem VDA der BA im Vorfeld berechtigte Mitarbeiter. Diese werden vom VDA der BA technisch berechtigt, die Bestellfunktion auf einer dedizierten Mandanten-Website zu nutzen. Im Zuge der Bestellung müssen die berechtigten Mitarbeiter folgende Stammdaten des künftigen Zertifikatsinhabers hinterlegen: Anrede, Vorname, Nachname, E-Mail-Adresse.

Vor der Beantragung einer dDk für einen Mitarbeiter einer gemeinsamen Einrichtung nach SGB II ist eine vertragliche Vereinbarung zwischen der BA und der gemeinsamen Einrichtung über die entsprechende Dienstleistung erforderlich.

Für Anträge durch Besteller nach 1.3.3.1 gilt:

- Zur Beantragung von Massensignaturkarten benennt die Fachabteilung, die für die Massensignaturanwendung zuständig ist, dem VDA der BA im Vorfeld die berechtigten Antragsteller. Unterschriftsberechtigte Mitarbeiter können eine MSK per Antragsformular bestellen. Die Liste der Unterschriftsberechtigten steht den LRA zur Verfügung. Bei der Registrierung wird überprüft, ob der Antragsteller in der Liste steht.
- Berechtigten Mitarbeitern des Mandanten steht eine Bestellfunktion auf einer Website zur Verfügung. Im Zuge der Bestellung müssen sie die Stammdaten des künftigen Zertifikatsinhabers hinterlegen.

Für Anträge durch Zertifikatsinhaber nach 1.3.3.2 gilt:

- Für Mitarbeiter der BA oder einer gemeinsamen Einrichtung nach SGB II mit vertraglicher Vereinbarung ist keine dedizierte Antragstellung erforderlich. Die Beantragung erfolgt implizit durch Aufnahme der Beschäftigung und ggf. Einkauf der entsprechenden Dienstleistung. Die Hinterlegung von Stammdaten des künftigen Zertifikatsinhabers erfolgt durch den Personalservice.
- Für Mitarbeiter des Mandanten ist nur Beantragung durch Besteller möglich.

In jedem Fall erfolgt die Einladung zur erstmaligen Identitätsprüfung nach 3.2 durch die zuständige LRA.

Als Teil der Einladung für eine dDk wird dem Zertifikatsinhaber eine Unterrichtung überlassen. Sie beschreibt:

- Funktionen der dDk
- Datenschutzregularien
- Registrierung, Kartenausgabe, Freischaltung, Sperrung
- Definition, Rechtswirkung, Erstellung, und (langfristige) Prüfung einer qualifizierten elektronischen Signatur
- Sicherheitshinweise für den Einsatz der dDk.

Für Mandanten-Signaturkarte und Mandanten–Massensignaturkarte existieren entsprechende Unterrichtungen, die dem Zertifikatsinhaber ebenfalls als Teil der Einladung überlassen werden.

Für die Massensignaturkarte existiert ebenfalls eine entsprechende Unterrichtung. Hier liegt es allerdings in der Verantwortung des Bestellers, dem Zertifikatsinhaber diese Unterrichtung vor der Registrierung zukommen zu lassen.

4.2 Antragsbearbeitung

4.2.1 Durchführung der Identifikation und Authentifizierung

Der künftige Zertifikatsinhaber wird von der zuständigen LRA zur Registrierung eingeladen. Für die Registrierung muss der Zertifikatsinhaber persönlich bei der zuständigen LRA erscheinen. Die Identifizierung erfolgt nach den Vorgaben zur erstmaligen Identitätsprüfung in Abschnitt 3.2. Der LRA-Registrar ruft den Stammdatensatz des künftigen Zertifikatsinhabers im Kartenmanagementsystem auf, prüft die vorhandenen Stammdaten und ergänzt diese anhand des Ausweisdokumentes. Anschließend erstellt er das Formular „Identitätsdaten“, in dem Vorname(n), Nachname, Geburtsdatum, Geburtsort, Staatsangehörigkeit des Zertifikatsinhabers sowie Art des vorgelegten Ausweisdokumentes, Ausweisnummer und dessen Ablaufdatum eingetragen werden. Die Richtigkeit dieser Daten bestätigen LRA-Registrar und Antragsteller mit ihrer Unterschrift auf dem Formular. Der ebenfalls ergänzte Geburtsname wird im System gespeichert.

Bei Beantragung einer MSK oder Mandanten-MSK wird diese Identifikation durch zwei LRA-Rolleninhaber im 4-Augen-Prinzip durchgeführt.

4.2.2 Annahme bzw. Ablehnung des Antrags

Anträge werden in folgenden Fällen abgelehnt:

- Der Antragsteller ist nicht berechtigt (siehe Abschnitt 4.1.1).
- Die notwendige vertragliche Vereinbarung bzw. der Einkauf der entsprechenden Dienstleistung fehlt (siehe Abschnitt 4.1.2).
- Der Zertifikatsinhaber kann nicht zweifelsfrei identifiziert werden oder es gibt Unstimmigkeiten bzgl. seiner Daten (siehe Abschnitt 4.2.1).
- Der künftige Inhaber eines Massensignaturzertifikates hat keine im Sinne des Abschnittes 4.4.1 freigeschaltete Einzelsignaturkarte.

Sofern der Antrag angenommen wird, führt der LRA-Registrar die folgenden Schritte aus:

- Ist der Zertifikatsinhaber Mitarbeiter der BA im Rechtskreis SGB III, erfasst er elektronisch Foto und Unterschrift
- Er fordert den Zertifikatsinhaber auf, ein Sperrpasswort zu vergeben (siehe Abschnitt 3.4).
- Er lässt sich vom Zertifikatsinhaber
    - die Kenntnisnahme der Unterrichtung (siehe Abschnitt 4.1.2),
    - Zustimmung zur Veröffentlichung des qualifizierten Zertifikates,
    - den Pseudonymverzicht nach Abschnitt 3.1.3 (nicht für MSK oder Mandanten-MSK),
    - die Zulässigkeit der amtsseitigen Sperrung

  bestätigen.
- Er signiert qualifiziert alle bisher erhobenen Daten. Damit wird der elektronische Registrierungsprozess abgeschlossen und ein Personalisierungsauftrag an das Trustcenter erstellt.
- Er legt die Registrierungsunterlagen in einer Registrierungsakte ab.
- Bei MSK oder Mandanten-MSK trägt der LRA-Registrar zusätzlich das auf dem Antragsformular notierte Pseudonym ein.

4.2.3 Fristen für die Antragsbearbeitung

Es werden keine Fristen für die Bearbeitung der Anträge festgelegt.

4.3 Zertifikatserstellung

4.3.1 CA-Prozesse während der Zertifikatserstellung

Nach erfolgreicher Registrierung wird auf einem zentralen System die Personalisierung der Smartcard durchgeführt. Dazu wird der Registrierungsdatensatz vom Registrierungssystem signiert an die CA übergeben. Bei erfolgreicher Signaturvalidierung wird anhand der im Registrierungsdatensatz enthaltenen Daten das entsprechende qualifizierte Zertifikat erzeugt und zusammen mit dem Schlüsselpaar auf der Smartcard gespeichert.

4.3.2 Benachrichtigung des Zertifikatsinhabers über die Zertifikatserstellung

Der Zertifikatsinhaber wird nach Eingang der Smartcard in der LRA vom LRA-Kartenausgeber benachrichtigt.

4.4 Zertifikatsannahme

4.4.1 Verfahren der Zertifikatsannahme

Das Signaturzertifikat wird mit der Smartcard in der LRA an den Zertifikatsinhaber ausgeliefert. Bei der Übergabe einer Smartcard erfolgt eine erneute Identifizierung anhand eines gültigen Ausweises wie bei der Registrierung, vgl. Abschnitt 3.2.3. Der Zertifikatsinhaber muss den Empfang schriftlich bestätigen. Dabei werden Typ, Nummer und Ablaufdatum des vorgelegten Ausweises festgehalten.

Die Ausgabe einer Massensignaturkarte oder Mandanten-Massensignaturkarte findet in der LRA im 4-Augen-Prinzip statt. Wenn der Antragsteller in der LRA erscheint, zieht der Kartenausgeber einen LRA-Registrar für den weiteren Ablauf hinzu.

Vor der Verwendung des Signaturschlüsselpaares muss der Zertifikatsinhaber die erhaltene Karte freischalten. Dabei muss er im ersten Schritt seine Signatur-PIN und ggf. Signatur-PUK[1] der Karte setzen (siehe Abschnitt 6.1.2). Im zweiten Schritt wird die Veröffentlichung seines qualifizierten Zertifikates angestoßen. Die dazu notwendige Software und ein geeignetes Kartenterminal sind auf den BA-Arbeitsplätzen und in der LRA vorhanden. Die Mitarbeiter der LRA unterstützen ihn auf Wunsch dabei.

4.4.2 Veröffentlichung der Zertifikate durch den Zertifizierungsdienst

Mit der Unterzeichnung der „Zustimmung zur Veröffentlichung“ erklärt der Zertifikatsinhaber sein Einverständnis zur Veröffentlichung seines qualifizierten Zertifikates. Im Zuge der Freischaltung der Smartcard wird das qualifizierte Zertifikat im Verzeichnis des Zertifizierungsdienstes veröffentlicht.

Details zur Veröffentlichung der Zertifikate finden sich in Abschnitt 2.2.

4.4.3 Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Falls notwendig wird die Aufsichtsstelle nach [eIDAS] über neue Dienstezertifikate informiert.

4.5 Nutzung des Schlüsselpaares und des Zertifikats

4.5.1 Nutzung durch den Zertifikatsinhaber

Es gelten die Bestimmungen wie in [QCP-n-qscd] clause 6.3.5 beschrieben.

Der Zertifikatsinhaber ist verpflichtet, seine Schlüsselpaare mit angemessener Sorgfalt zu nutzen. Generelle Hinweise dazu findet er in der Unterrichtung, vgl. 4.1.2. Insbesondere muss er sicherstellen, dass sein privater Schlüssel nicht ohne sein Wissen und nur in der von ihm gewünschten Weise

[1] Abhängig von der verwendeten QSCD

eingesetzt werden. Dazu hat er direkt im Anschluss an die Übergabe der Smartcard diese freizuschalten, also Signatur-PIN und ggf. die Signatur-PUK[2] mit nur ihm bekannten Werten[3] zu vergeben und die Veröffentlichung des qualifizierten Zertifikates anzustoßen. Die Nutzung des privaten Schlüssels ist erst möglich, nachdem der Zertifikatsinhaber die Smartcard freigeschaltet hat, vgl. Abschnitt 4.4. Damit erhält er die alleinige Kontrolle über seinen privaten Schlüssel. Zur Verwendung von Zertifikaten siehe Abschnitt 1.4.

4.5.2 Nutzung durch vertrauende Dritte

Vertrauende Dritte sollten einem qualifizierten Zertifikat des Zertifizierungsdienstes der BA nur dann vertrauen, wenn

- dieses gültig und nicht gesperrt ist und
- dieses auf Basis der Dienstezertifikate des VDA der BA geprüft werden kann.

Zur Prüfung ist das Kettenmodell gemäß [COMPKI] SigG-Profile anzuwenden.

Vor dem Vertrauen auf ein qualifiziertes Zertifikat hat der vertrauende Dritte folgendes zu prüfen:

- den Sperrstatus des qualifizierten Zertifikats und aller darüber liegenden CA-Zertifikate der Zertifizierungskette im OCSP-Verzeichnisdienst: Falls eines der Zertifikate in der Zertifikatskette zum Zeitpunkt der jeweiligen Signaturerzeugung gesperrt war oder dessen Gültigkeit abgelaufen war, darf der Vertrauende Dritte auf das qualifizierte Zertifikat oder ein anderes gesperrtes qualifiziertes Zertifikat in der Zertifikatskette nicht vertrauen.
- die Eignung der Nutzung eines Zertifikats für einen bestimmten Zweck, der durch das vorliegende CP nicht verboten oder anderweitig beschränkt ist.
- die Nutzung des Zertifikats entspricht den im Zertifikat enthaltenen KeyUsage-Felderweiterungen.

Der vertrauende Dritte hat sich zudem regelmäßig auf der Webseite des Zertifizierungsdienstes, siehe Abschnitt 2.1, und bei der Aufsichtsstelle im Sinne der [eIDAS] zu informieren.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Re-Zertifizierung)

Bei der Zertifikatserneuerung unter Beibehaltung des alten Schlüssels handelt es sich um die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer, aber für den gleichen öffentlichen Schlüssel und sonst unveränderten Inhaltsdaten. In [RFC3647] wird dieser Vorgang „certificate renewal“ genannt.

4.6.1 Gründe für eine Zertifikatserneuerung

Zertifikatserneuerungen unter Beibehaltung des alten Schlüssels werden nicht durchgeführt.

4.6.2 Wer kann eine Zertifikatserneuerung beantragen

Zertifikatserneuerungen unter Beibehaltung des alten Schlüssels werden nicht durchgeführt.

4.6.3 Ablauf der Zertifikatserneuerung

Zertifikatserneuerungen unter Beibehaltung des alten Schlüssels werden nicht durchgeführt.

4.6.4 Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung

Zertifikatserneuerungen unter Beibehaltung des alten Schlüssels werden nicht durchgeführt.

---

[2] Abhängig von der verwendeten QSCD

[3] Die Vergabe unterschiedlicher Werte wird empfohlen.

4.6.5 Annahme einer Zertifikatserneuerung

Zertifikatserneuerungen unter Beibehaltung des alten Schlüssels werden nicht durchgeführt.

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst

Zertifikatserneuerungen unter Beibehaltung des alten Schlüssels werden nicht durchgeführt.

4.6.7 Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Zertifikatserneuerungen unter Beibehaltung des alten Schlüssels werden nicht durchgeführt.

4.7 Schlüssel- und Zertifikatserneuerung (Re-Key)

Bei der Schlüssel- und Zertifikatserneuerung handelt es sich um die Ersetzung eines Zertifikates durch ein Zertifikat mit neuer Gültigkeitsdauer und für einen neuen öffentlichen Schlüssel. In [RFC3647] wird dieser Vorgang „certificate re-key“ genannt.

4.7.1 Gründe für eine Schlüssel- und Zertifikatserneuerung

Die Smartcard und die darauf enthaltenen Zertifikate haben eine beschränkte Gültigkeitsdauer, vgl. Abschnitt 6.3.2. Nach Ablauf der Gültigkeitsdauer ist die Zuordnung des subject, vgl. Abschnitt 3.1.1, zum öffentlichen Schlüssel nicht mehr garantiert.

Nach Sperrung oder Ablauf der Gültigkeitsdauer eines qualifizierten Zertifikates ist die Erstellung einer gültigen qualifizierten elektronischen Signatur nicht mehr möglich. Verlust oder Defekt der Smartcard sind weitere Gründe.

4.7.2 Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen

- Für Massensignaturkarten oder Mandanten-Signaturkarten bzw. Mandaten–Massensignaturkarten erfolgt die Beantragung durch die in Abschnitt 1.3.3.1 genannten Besteller. Die folgenden Aufzählungspunkte sind für die genannten Kartentypen nicht anwendbar.
- Rechtzeitig vor Ablauf der Gültigkeitsdauer seines qualifizierten Zertifikates wird der Inhaber einer dDk entsprechend benachrichtigt. Der automatisierte Prozess erkennt geänderte Stammdaten und fordert den Inhaber zur Erstbeantragung nach Abschnitt 4.1.2 auf. Bei unveränderten Stammdaten wird in der Regel automatisch ein neues Signaturzertifikat beantragt und zusammen mit einer neuen Smartcard übergeben.
- Nach der Sperrung seines qualifizierten Zertifikates, Verlust oder Defekt der dDk kann der Zertifikatsinhaber selbst eine Erneuerung beantragen.

4.7.3 Ablauf der Schlüssel- und Zertifikatserneuerung

- Für Massensignaturkarten oder Mandanten-Signaturkarten bzw. Mandanten–Massensignaturkarten wird wie bei der Erstbeantragung vorgegangen, siehe Abschnitt 4.1.2. Die folgenden Aufzählungspunkte sind für die genannten Kartentypen nicht anwendbar.
- Rechtzeitig vor Ablauf der Gültigkeitsdauer seines qualifizierten Zertifikates wird der Inhaber einer dDk entsprechend benachrichtigt. Der automatisierte Prozess erkennt geänderte Stammdaten und fordert den Inhaber zur Erstbeantragung nach Abschnitt 4.1.2 auf. Bei unveränderten Stammdaten und falls der Inhaber nicht widerspricht, wird automatisch ein neues Signaturzertifikat beantragt, erstellt und als Teil einer neuen Smartcard an die LRA verschickt. Ein Widerspruchsgrund wäre etwa ein bevorstehendes

Ende des Beschäftigungsverhältnisses. Die Identifizierung wird wie in 3.3.1 beschrieben durchgeführt.

- Nach der Sperrung seines qualifizierten Zertifikates, Verlust oder Defekt der dDk, beantragt der Zertifikatsinhaber bei der LRA die Erneuerung des Zertifikates. Sofern sich seine Stammdaten gegenüber der erstmaligen Identitätsprüfung nicht geändert haben, veranlasst die LRA die Produktion einer neuen Smartcard, die an die LRA verschickt wird. Die Identifizierung wird wie in 3.3.2 beschrieben durchgeführt. Haben sich Vor- oder Nachname, E-Mail oder UPN des Zertifikatsinhabers geändert, ist wie bei der erstmaligen Antragstellung für Zertifikate nach Abschnitt 4.1.2 vorzugehen. Insbesondere ist eine Identifizierung nach Abschnitt 3.2 erforderlich.

4.7.4 Benachrichtigung des Zertifikatsinhabers nach Schlüssel- und Zertifikatserneuerung

Der Prozess der Benachrichtigung des Zertifikatsinhabers ist analog zum in Kapitel 4.3.2 beschriebenen Prozess bei der Erstausstellung.

4.7.5 Annahme der Schlüssel- und Zertifikatserneuerung

Der Prozess der Annahme ist analog zum in Abschnitt 4.4.1 beschriebenen Prozess bei der Erstausstellung. Im Rahmen der Annahme der Schlüssel- und Zertifikatserneuerung werden noch vorhandene ältere, gültige Karten des Zertifikatsinhabers durch die LRA gesperrt. Der Zertifikatsinhaber ist verpflichtet, ältere Karten der LRA vorzulegen, sofern sie noch vorhanden sind. Die Karten werden durch die LRA vernichtet. Andernfalls wird der Zertifikatsinhaber verpflichtet, die Karten selbst zu vernichten, falls er Zugriff darauf erlangt, z.B. die Karten wiederfindet.

4.7.6 Veröffentlichung einer Zertifikatserneuerung durch den Zertifizierungsdienst

Siehe Abschnitt 4.4.2.

4.7.7 Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Siehe Abschnitt 4.4.3.

4.8 Zertifikatsmodifizierung

Bei der Modifizierung eines Zertifikats handelt es sich um die Ersetzung eines Zertifikates durch ein Zertifikat mit veränderten Inhaltsdaten, aber für den gleichen öffentlichen Schlüssel und sonst unveränderter Gültigkeitsdauer. In [RFC3647] wird dieser Vorgang „certificate modification“ genannt.

4.8.1 Gründe für eine Zertifikatsmodifizierung

Modifizierungen von Zertifikaten werden nicht durchgeführt.

4.8.2 Wer kann eine Zertifikatsmodifizierung beantragen

Modifizierungen von Zertifikaten werden nicht durchgeführt.

4.8.3 Ablauf der Zertifikatsmodifizierung

Modifizierungen von Zertifikaten werden nicht durchgeführt.

4.8.4 Benachrichtigung des Zertifikatsinhabers nach der Zertifikatsmodifizierung

Modifizierungen von Zertifikaten werden nicht durchgeführt.

4.8.5 Annahme der Zertifikatsmodifizierung

Modifizierungen von Zertifikaten werden nicht durchgeführt.

4.8.6 Veröffentlichung einer Zertifikatsmodifizierung durch den Zertifizierungsdienst

Modifizierungen von Zertifikaten werden nicht durchgeführt.

4.8.7 Benachrichtigung weiterer Instanzen durch den Zertifizierungsdienst

Modifizierungen von Zertifikaten werden nicht durchgeführt.

4.9 Sperrung und Suspendierungen von Zertifikaten

4.9.1 Gründe für eine Sperrung

Ein qualifiziertes Zertifikat ist in den folgenden Fällen zu sperren:

- Wenn der Mitarbeiter aus dem Dienst der BA oder der gemeinsamen Einrichtung ausscheidet.
- Wenn die vertragliche Vereinbarung zwischen der BA und dem Mandanten endet, werden alle für den Mandanten ausgestellten qualifizierten Zertifikate gesperrt.
- Wenn die entsprechende Dienstleistungsvereinbarung zwischen gemeinsamer Einrichtung und der BA beendet wird, werden alle an die gE ausgegebenen dDk wieder eingezogen und die zugehörigen qualifizierten Zertifikate gesperrt.
- Wenn das qualifizierte Zertifikat aufgrund falscher Angaben ausgestellt wurde.
- Wenn der Zertifikatsinhaber seine privaten Schlüssel nicht mehr nutzen kann oder der Verdacht auf Kompromittierung besteht.
- Wenn der Verdacht besteht, dass die für die Erzeugung und Anwendung der privaten Schlüssel eingesetzten Algorithmen und Geräte keine ausreichende Sicherheit mehr bieten.
- Wenn ein Sperrberechtigter nach 4.9.2 es verlangt.

Bei der Sperrung der CA für qualifizierte Zertifikate werden die nachgeordneten Mitarbeiterzertifikate nur dann gesperrt, wenn der berechtigte Verdacht besteht, dass der private Schlüssel der CA, die das Zertifikat signiert hat, missbraucht wurde.

Wenn die BA ihre Zertifizierungsdienste einstellt, werden sämtliche von ihr ausgestellten Zertifikate gesperrt (siehe Abschnitt 5.8).

4.9.2 Sperrberechtigte

Die folgenden Stellen sind berechtigt, die Sperrung von qualifizierten Zertifikaten zu beantragen:

- Zertifikatsinhaber
- Besteller der MSK
- Berechtigte Mitarbeiter des Mandanten, sofern das mit dem VDA der BA vereinbart wurde
- amtsseitig durch Berechtigte, z.B. Personalservice der BA, wenn dienstliche oder gesetzliche Gründe dies erfordern
- die zuständige Aufsichtsstelle nach [eIDAS]
- VDA-Leitung, TC-Leitung.

4.9.3 Verfahren zur Sperrung

Es sind folgende Verfahren für die Sperrung von Zertifikaten definiert:

- **Telefonische Sperrung über die Sperrhotline**: Über die Sperrhotline können Smartcards durch den Zertifikatsinhaber telefonisch gesperrt werden. Der Anrufer nennt seine E-Mail-Adresse und das Sperrpasswort. Sind die Angaben korrekt, wird die Sperrung durchgeführt. Bei der Sperrung einer Smartcard werden alle zugeordneten Zertifikate gesperrt. Die Sperrung wird dem Zertifikatsinhaber umgehend bestätigt.
- Eine **Sperrung durch den LRA-Sperroperator** kann durch den Zertifikatsinhaber oder aus dienstlichen Gründen von Amts wegen beantragt werden. Der LRA-Sperroperator führt die Sperrung der Smartcard und der zugeordneten Zertifikate durch. Für die Sperrung durch den LRA-Sperroperator muss ein schriftlicher Sperrantrag vorgelegt werden.
- **Schriftlicher Sperrantrag**: Ein schriftlicher Sperrantrag für eine Smartcard kann per Post beim VDA der BA eingesendet werden. Der Antrag muss unterschrieben sein und den Namen des Karteninhabers bzw. des Zertifikatsinhabers, E-Mail-Adresse, sowie einen Sperrgrund enthalten. Der LRA-Sperroperator führt dann die Sperrung durch. Bei der Sperrung einer Smartcard werden ebenfalls alle zugeordneten Zertifikate gesperrt.
- **Sperrung von CA-Zertifikaten:** Die VDA-Leitung oder TC-Leitung stellt einen schriftlichen Sperrauftrag. Die Durchführung erfolgt im 4-Augen-Prinzip in der sicheren Umgebung des VDA der BA.
- **Massensperrung qualifizierter Zertifikate:** Die VDA-Leitung oder TC-Leitung stellt einen schriftlichen Sperrauftrag. Die Durchführung der Massensperrung erfolgt im 4-Augen-Prinzip in der sicheren Umgebung des VDA der BA. Die übrigen Zertifikate einer betroffenen Smartcard werden dabei nicht gesperrt.

In der folgenden Tabelle ist angegeben, über welche Kanäle Sperrberechtigte die Sperrung veranlassen können:

Antragsteller	Telefon (UHD)	Schriftlich	LRA
Inhaber	✓	✓	✓
Sperrung von Amts wegen		✓	✓
VDA der BA		✓	✓
BNetzA	✓	✓	

Tabelle 2 - Zuordnung der Sperrberechtigungen zu den Sperrmöglichkeiten

Die Identifizierung erfolgt wie in Abschnitt 3.4 beschrieben.

4.9.4 Fristen für die Beantragung einer Sperrung

Der Sperrberechtigte, vgl. Abschnitt 4.9.2, muss bei Vorliegen entsprechender Gründe unverzüglich die Sperrung initiieren.

4.9.5 Bearbeitungszeit für Anträge auf Sperrung

Die Sperrhotline ist permanent erreichbar, telefonische Sperranträge werden unmittelbar bearbeitet. Schriftliche Sperranträge werden innerhalb eines Arbeitstages nach Eingang bei der LRA bearbeitet.

4.9.6 Prüfung des Zertifikatsstatus durch Dritte

Vertrauende Dritte müssen bei der Prüfung von qualifizierten Zertifikaten den Sperrstatus über den OCSP-Verzeichnisdienst prüfen.

4.9.7 Periode für die Erstellung der Sperrlisten

Für qualifizierte Zertifikate werden keine Sperrlisten veröffentlicht.

4.9.8 Maximale Latenz der Sperrlisten

Für qualifizierte Zertifikate werden keine Sperrlisten veröffentlicht.

4.9.9 Verfügbarkeit von Online-Sperrinformationen

Der VDA der BA bietet den OCSP-Verzeichnisdienst für die Online-Prüfung von qualifizierten Zertifikaten an (siehe Abschnitt 2.1). Dieser ist hochverfügbar (24x7).

4.9.10 Nutzung der Online-Sperrinformationen durch Dritte

Vertrauende Dritte müssen bei der Prüfung von qualifizierten Zertifikaten den Sperrstatus über den OCSP-Verzeichnisdienst prüfen. Für die Verbindungsparameter siehe Abschnitt 2.

4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Der Inhaber einer Einzel- oder Massensignaturkarte wird per E-Mail über die Sperrung informiert.

4.9.12 Spezielle Anforderungen bei Kompromittierung privater Schlüssel

Keine.

4.9.13 Gründe für die Suspendierung

Eine Suspendierung (gemeint ist die Aussetzung im Sinne der [eIDAS], also der vorübergehende Verlust der Gültigkeit von ausgestellten qualifizierten Zertifikaten) wird nicht unterstützt. D. h., die Sperrung eines Zertifikates ist immer endgültig und kann nicht aufgehoben werden.

4.9.14 Wer kann eine Suspendierung beantragen

Es ist keine Suspendierung von qualifizierten Zertifikaten möglich, siehe Abschnitt 4.9.13.

4.9.15 Verfahren zur Suspendierung

Es ist keine Suspendierung von qualifizierten Zertifikaten möglich, siehe Abschnitt 4.9.13.

4.9.16 Maximale Sperrdauer bei Suspendierung

Es ist keine Suspendierung von qualifizierten Zertifikaten möglich, siehe Abschnitt 4.9.13.

4.10 Auskunftsdienste über den Zertifikatsstatus

Es gelten die Bestimmungen wie in [QCP-n-qscd] clause 6.3.10 beschrieben.

4.10.1 Betriebseigenschaften

Der Auskunftsdienst für den Sperrstatus qualifizierter Zertifikate basiert auf dem Online Certificate Status Protocol (OCSP).

Die Verbindungsparameter des OCSP-Verzeichnisdienstes werden auf der in Abschnitt 2.1 genannten Webseite veröffentlicht. Aktuell ist der OCSP-Verzeichnisdienst über die URL

http://ocsp.pki.arbeitsagentur.de

erreichbar.

Der OCSP-Verzeichnisdienst verwendet als Übertragungsprotokoll HTTP und implementiert das Online Certificate Status Protocol (OCSP) gemäß [RFC2560] und [COMPKI] mit den folgenden Eigenschaften:

- Die Anfragen (OCSP-Requests) müssen nicht signiert sein; signierte Anfragen werden jedoch auch unterstützt.
  - Die Hash-Werte in den Anfragen (Felder issuerNameHash und issuerKeyHash) müssen mit SHA-1 erstellt worden sein.
- Auskünfte des OCSP-Verzeichnisdienstes werden

- innerhalb der Legacy-Hierarchie mit einer qualifizierten elektronischen Signatur unterzeichnet.
- innerhalb der Standard-Hierarchie mit einem fortgeschrittenen elektronischen Siegel versiegelt.

- Das verwendete Dienstezertifikat und alle zugehörigen CA-Zertifikate der Hierarchie werden vom OCSP-Responder im Feld `certs` der `BasicResponse` der Antwort mitgeliefert.
- Das Feld `nextUpdate` in `SingleResponse` wird nicht verwendet.
- Sperrgründe werden nicht in der Antwort mitgegeben.
- Die unterstützten Erweiterungen sind in Abschnitt 7.3.2 angegeben.
- Statusinformationen zu einem qualifizierten Zertifikat werden über den Ablauf seiner Gültigkeitsdauer hinaus bereitgestellt, siehe dazu die Erweiterung ArchiveCutoff in Abschnitt 7.3.2.

4.10.2 Verfügbarkeit

Der OCSP-Verzeichnisdienst hat eine zugesicherte Verfügbarkeit von 99,80 Prozent.

4.10.3 Optionale Funktionen

Der OCSP-Verzeichnisdienst unterstützt die folgenden optionalen Funktionen:

- Eine Anfrage an den OCSP-Verzeichnisdienst für den Zertifikatsstatus kann die Erweiterung `Nonce` enthalten. Diese Extension dient der Vorbeugung gegen Angriffe durch Senden alter Antworten (Replay-Attacks). Der in der Anfrage übergebene Wert wird vom Auskunftsdienst in die Extension `Nonce` der Antwort kodiert.
- Eine Anfrage an den OCSP-Verzeichnisdienst kann für den Zertifikatsstatus die spezielle Erweiterung `RetrieveIfAllowed` aus dem SigG-Profile[4] von [COMPKI] enthalten. In diesem Fall kodiert der OCSP-Verzeichnisdienst das Zertifikat, dessen Status abgefragt wurde, gemäß dem SigG-Profile von [COMPKI] in die spezielle Erweiterung `RequestedCertificate` der Antwort.

4.11 Ende der Nutzung (End of subscription)

Die Nutzung des Dienstes endet, wenn

- der Zertifikatsinhaber aus dem Dienst der BA ausscheidet,
- das Arbeitsverhältnis des Zertifikatsinhabers als Mitarbeiter der gemeinsamen Einrichtung nach SGB II endet,
- das Dienstleitungsverhältnis zwischen der BA und der gemeinsamen Einrichtung nach SGB II beendet wird,
- das Dienstleitungsverhältnis zwischen der BA und dem Mandanten beendet wird.

Bei Beendigung des Dienstleistungsverhältnisses werden alle Zertifikate der betroffenen Zertifikatsinhaber gesperrt. Die genauen Modalitäten werden zwischen den Vertragspartnern geregelt.

4.12 Schlüsselhinterlegung und -wiederherstellung (Key Escrow und Recovery)

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Eine treuhänderische Hinterlegung von privaten Signaturschlüsseln findet nicht statt.

[4] Zur Bezeichnung vgl. den zugehörigen Eintrag in Kapitel Definitionen und Abkürzungen am Ende des Dokumentes

4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Entfällt für qualifizierte Zertifikate.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

5.1.1 Lage und Konstruktion des Standortes

Die Vertrauensdienste werden an zwei räumlich getrennten Standorten betrieben:

- Der Hauptstandort - an diesem Standort wird die produktive Infrastruktur der Vertrauensdienste betrieben. Zusätzlich erfolgt hier die Kartenproduktion.
- Der Backupstandort - an diesem Standort wird die Backup-Infrastruktur der Vertrauensdienste betrieben. Bei Bedarf kann die Kartenproduktion hierher verlagert werden.
- In verschiedenen weiteren Liegenschaften der BA gibt es LRA-Räume zur Durchführung operativer Tätigkeiten des Zertifizierungsdienstes (Registrierung, Kartenausgabe, Sperrung).

An beiden Standorten gewährleisten bauliche Maßnahmen einen hohen Schutz gegen unbefugtes Eindringen, unbefugten Zutritt und Zugriff sowie unbefugte Einsichtnahme auf die sicherheitsrelevanten Einrichtungen des VDA der BA. Diese Maßnahmen sind im Sicherheitskonzept des VDA der BA dargelegt. Das Gebäude ist zum angrenzenden öffentlichen Bereich durch einen Perimeterschutz begrenzt (Hauptstandort) bzw. grenzt mit der einzigen Fensterfront an einen nicht frei zugänglichen Innenhof der Liegenschaft (Backupstandort). Beide Standorte verfügen über eine eigene Einbruchmeldeanlage (EMA), die von der Sicherheitszentrale am Hauptstandort auf Alarm- und Störmeldungen 7x24 überwacht wird. Die Sicherheitszentrale verständigt im Bedarfsfall die Polizei. Die einzelnen Räume beider Standorte werden mit Bewegungsmeldern überwacht. Der Hauptstandort unterliegt zusätzlich einer regelmäßigen Kontrolle durch den Sicherungsdienst. An beiden Standorten gibt es in den normal zugänglichen Lageplänen keine Hinweise auf die Räumlichkeiten des VDA der BA.

Die lokalen LRA-Räume folgen definierten Sicherheitsmaßnahmen. Sie sind in dedizierten Büroräumen untergebracht, verschlossen und gegen unbefugten Zutritt geschützt.

5.1.2 Zutrittskontrolle

In den beiden Standorten gewährleisten umfassende mehrstufige Maßnahmen zur Zutrittskontrolle einen hohen Schutz gegen unbefugtes Eindringen in die einzelnen Räume und unbefugten Zugriff auf die sicherheitskritischen Systeme und Daten. Diese Maßnahmen sind im Detail im Sicherheitskonzept des VDA der BA dargelegt. Zu beiden Standorten ist der Zutritt ausschließlich über eine alarmüberwachte Personenvereinzelungsschleuse (PVE) möglich. Zusätzlich zur PVE ist eine ständig verschlossene und überwachte Tür zur Flucht und Lieferung installiert. Alle Zutritte werden über eine eigene Zutrittskontrollanlage protokolliert. Die PVE sowie die Flucht- bzw. Liefertür werden videoüberwacht.

Der Zutritt zu einzelnen Räumen beider Standorte selbst, die jeweils in mehrere Zutrittszonen unterteilt sind, kann nur mit Hilfe eines Identifikationsmerkmalträgers (Zutrittskarte, Besitz und Wissen) erfolgen. Zutritt ist nur berechtigten Personen möglich, zu bestimmten Bereichen wird ein Zugang nur im 4-Augen-Prinzip je nach Rolle gewährt. Techniker- oder Besucherzutritte können nur in Begleitung autorisierter Rolleninhaber erfolgen.

Die lokalen Mitarbeiter in den verschiedenen Liegenschaften sind geschulte und vertrauenswürdige Rolleninhaber des VDA der BA. Nur sie haben uneingeschränkten Zutritt zu den lokalen LRA-Räumlichkeiten. Besucher und Techniker werden durch autorisierte Rolleninhaber begleitet.

Die Leitung des VDA der BA hat gegenüber allen Rolleninhabern des VDA der BA bzgl. ihrer Tätigkeiten innerhalb des VDA der BA fachliche Weisungsbefugnis.

5.1.3 Stromversorgung und Klimakontrolle

Die beiden Standorte des Vertrauensdienstes sind jeweils mit einer unterbrechungsfreien Stromversorgung und Schutzeinrichtungen gegen Überspannung ausgestattet. Am Hauptstandort

gewährleistet eine zweite Stromeinspeisung von einem redundanten Umspannwerk sowie eine automatische Umschaltung eine unabhängige und redundante Stromversorgung. Beide Standorte sind zusätzlich über dedizierte unterbrechungsfreie Stromversorgungen (USV) mit ausreichender Kapazität abgesichert.

Haupt- und Backupstandort sind mit eigenen, zentral überwachten redundanten Klimaanlagen ausgestattet.

5.1.4 Schutz vor Wasserschäden

Es befinden sich keine fließenden oder stehenden Gewässer in der räumlichen Nähe der beiden Standorte. Passiver Wasserschutz ist durch entsprechende Boden- und Rackbauweise sowie zusätzliche Wasserdetektion und automatische Abschaltung gewährleistet.

5.1.5 Brandschutz

An beiden Standorten wird der Brandschutz durch umfassende aktive, passive und organisatorische Maßnahmen realisiert. Diese sind im Sicherheitskonzept des VDA der BA dargelegt. Dazu gehören u.a. die Verwendung entsprechender Baumaterialien, die Aufteilung auf Brandabschnitte, die Brandfrüherkennung und –alarmierung über Rauchmelder sowie die ereignisgesteuerte Brandlöschung des jeweiligen Objektes. Die Überwachung erfolgt am ständig besetzten Hauptstandort. Zusätzlich wird die Feuerwehr im Zweischleifenprinzip alarmiert.

5.1.6 Lagerung von Datenträgern

Datenträger mit sicherheitskritischen Informationen werden in verschlossenen Behältnissen aufbewahrt. Datenträger mit besonders kritischen Informationen werden ausschließlich in Tresoren aufbewahrt.

5.1.7 Entsorgung von Datenträgern

Sämtliche für sicherheitskritische Systeme oder Informationen des VDA der BA genutzte Datenträger und Smartcards werden vor der Entsorgung sicher gelöscht oder physikalisch unbrauchbar gemacht. Papierdokumente, die vertrauliche Informationen enthalten, werden mindestens gemäß DIN 32757 Sicherheitsstufe 3 entsorgt.

5.1.8 Ausgelagertes Backup

An beiden Standorten wird regelmäßig ein Backup der Produktionsdaten durchgeführt. Die Datensicherung umfasst die Daten der Zertifizierungsprozesse, die Protokolldaten und weitere wichtige Daten. Die Backupdatenträger werden sicher aufbewahrt (siehe Abschnitt 5.1.6) und verlassen die gesicherten Bereiche nur unter Maßgabe gemäß Abschnitt 5.1.7.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitskritische Rollen

Sicherheitskritische Tätigkeiten im VDA der BA sind Rollen zugeordnet, die in einem internen Rollenkonzept beschrieben werden. Diese Tätigkeiten dürfen ausschließlich von Personen durchgeführt werden, die den entsprechenden Rollen zugewiesen sind. Die Anzahl der Rolleninhaber ist auf die notwendige Zahl beschränkt.

5.2.2 Anzahl benötigter Personen bei sicherheitskritischen Aufgaben

Besonders kritische Tätigkeiten werden ausschließlich unter Mitwirkung einer zweiten Person (4-Augen-Prinzip) durchgeführt.

5.2.3 Identifikation und Authentisierung von Rollen

Die Identifikation und Authentisierung der Rolleninhaber erfolgt beim Zutritt zu sicherheitsrelevanten Räumen durch eine Smartcard mit zugehöriger individueller PIN sowie beim Zugriff auf besonders sicherheitsrelevante Systeme mit Hilfe eines zwischen den jeweilig berechtigten Rolleninhabern

geteilten Passwortes. Für Systeme im Trustcenter, die keine Smartcard-Authentisierung unterstützen, erfolgt eine rollenspezifische Anmeldung über personalisierte Accounts mit Benutzername und Passwort. Eine Anmeldung mit administrativen Gruppenkonten ist nicht gestattet. Die Passwörter unterliegen einer Passwortpolicy.

5.2.4 Trennung von Rollen und Aufgaben

Grundsätzlich können Mitarbeiter des Vertrauensdienstes mehrere Rollen einnehmen. Für die Sicherheit ist es jedoch unerlässlich, gewisse Rollen personell zu trennen.

Dem Rollenkonzept liegen die folgenden Basisregeln und Rollenausschlüsse zugrunde:

- Leitende Rollen dürfen keine operativen oder administrativen Rollen übernehmen.
- Kontrollierende und beratende Rollen dürfen keine operativen oder administrativen Rollen übernehmen.
- Administrative Rollen dürfen keine operativen Rollen übernehmen.

Die Einhaltung der Rollenausschlüsse wird bei der Benennung der Rolleninhaber geprüft. Ein Rollenwechsel ist *nicht* möglich, wenn dadurch die Einhaltung des Rollenkonzeptes über die Zertifikatsprozesse gefährdet ist. Deshalb wird über den Rollenwechsel einer Person immer im Einzelfall entschieden und kann nur entgegen des Lebenszyklus einer Karte erfolgen. Sicherheitskritische Tätigkeiten werden im 4-Augen-Prinzip und durch die definierten Rolleninhaber unter Einhaltung der vorgegebenen Prozesse durchgeführt.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an die Fachkunde und Erfahrung

Der VDA der BA stellt durch geeignete Schulungen sicher, dass alle eingesetzten Rolleninhaber, so die Sicherheitsoffiziere, Systemadministratoren, Personalisierer, Registrare, Kartenausgeber, Sperroperatoren, Archivare und leitende Rollen die für ihre Aufgabe notwendige Fachkunde, Erfahrungen und Qualifikationen besitzen. Dies trifft sowohl auf alle BA-Angehörigen als auch auf von Vertragspartnern beauftragte und eingesetzte Mitarbeiter zu. Für alle Rollen gibt es Vertreter.

5.3.2 Anforderungen an die Zuverlässigkeit

Der VDA der BA stellt sicher, dass in den Vertrauensdiensten eingesetztes Personal die für einen sicheren Betrieb notwendige Zuverlässigkeit besitzt. Alle Rolleninhaber mit Ausnahme der Archivare müssen sich vor Übernahme einer Rolle gemäß §9 Abs. 1 Ziffer 3 Sicherheitsüberprüfungsgesetz (SÜG) einer erweiterten Sicherheitsüberprüfung im Bereich Sabotageschutz unterziehen. Die Sicherheitsüberprüfung ohne Beanstandung ist auch Voraussetzung für den Einsatz von beauftragten Mitarbeitern externer Vertragspartner. Die Archivare benötigen vor der Übernahme einer Rolle ein aktuelles Führungszeugnis nach § 30 Abs. 1 und 5 des Bundeszentralregistergesetzes.

5.3.3 Anforderungen an die Schulung

Die für die Vertrauensdienste eingesetzten Rolleninhaber werden vor Aufnahme der Tätigkeit ausreichend zu IT-Sicherheit und Fachkunde über rollenspezifische Schulungsmodule geschult und Sicherheitsbelehrungen durchgeführt. Diese Schulungen werden dokumentiert.

5.3.4 Wiederholungen der Schulungen

Der VDA der BA ordnet Wiederholungsschulungen für das in den Vertrauensdiensten eingesetzte Personal bei Bedarf dann an, wenn der Eindruck entsteht, dass die Fachkunde eines Rolleninhabers für seine Aufgabe nicht mehr ausreichend ist. Dies kann z. B. im Rahmen eines Audits festgestellt werden. Die Schulungsinhalte werden regelmäßig auf ihre Aktualität überprüft. Hinsichtlich IT-Sicherheit erfolgen jährlich dokumentierte Belehrungs- und Sensibilisierungsmaßnahmen.

5.3.5 Häufigkeit und Abfolge von Rollenwechsel

Ein regelmäßiger Rollenwechsel findet nicht statt.

5.3.6 Sanktionen bei unzulässigen Handlungen

Sollte ein Rolleninhaber die Anweisungen und Vorschriften verletzen oder sollten auffallend häufig Fehler auftreten, werden Maßnahmen zur zukünftigen Verhinderung ergriffen. Dies beinhaltet gegebenenfalls auch den Entzug, die Suspendierung oder die Änderung seiner Rollen, Aufgaben und Zugriffsrechte. In schweren Fällen kann dies auch arbeits- und strafrechtliche Maßnahmen beinhalten.

5.3.7 Vertragsbedingungen mit dem Personal beauftragter Dritter

Für das Personal beauftragter Dritter, sofern sie eine Rolle im Zertifizierungsdienst einnehmen, gelten dieselben Anforderungen an Zuverlässigkeit und Fachkunde wie für internes Personal.

5.3.8 An das Personal ausgehändigte Dokumente

Mitarbeitern der Vertrauensdienste werden die folgenden Dokumente zur Verfügung gestellt, sofern sie zur Durchführung der Tätigkeiten oder zur Einhaltung von Anweisungen oder gesetzlichen Vorschriften notwendig sind:

- Informationen zu den relevanten Gesetzen und Verordnungen, insbesondere zur elektronischen Signatur und zum Datenschutz
- Interne Betriebskonzepte und Handlungsanweisungen der Zertifizierungsdienste
- Betriebshandbücher der Systeme und Software
- Relevante technische Normen
- Rollenspezifische Schulungsunterlagen.

5.4 Protokollierung sicherheitskritischer Ereignisse

5.4.1 Protokollierte Ereignisse

Sicherheitsrelevante Ereignisse werden von den IT-Systemen elektronisch protokolliert:

- Ereignisse im Lebenszyklus der Zertifikate, dDk (z. B. Registrierung, Kartenausgabe, Generierung von Schlüsseln und Zertifikaten, Ausstellen und Veröffentlichen von Zertifikaten, Personalisierung, Sperranfragen und Sperrungen),
- Ereignisse im Lebenszyklus der Hardware-Sicherheitsmodule der Vertrauensdienste (z. B. Initialisierung und Konfiguration eines HSM, Schlüsselgenerierung, Schlüsselbackup und -wiederherstellung, Löschen von Schlüsseln), Änderungen der Policy,
- Sicherheitsrelevante Systemereignisse und Fehlermeldungen der kritischen Systeme, Firewall und Router,
- Bei Systemen, die auf die gesetzliche Zeit angewiesen sind, alle zeitbezogenen Ereignisse wie die Synchronisierung der Uhren oder Fehler beim Bezug der aktuellen Zeit,
- Zutritte zu den Räumlichkeiten,
- Sicherheitskritische Ereignisse der Zutrittskontrollanlagen,
- Zuweisung und Entzug von Rollen,
- Ausgestellte qualifizierte Zeitstempel,
- Start und Stopp von Systemen, Hardwarefehler, Abstürze.

Zu jedem Ereignis werden dabei die folgenden Daten erfasst:

- Zeitpunkt (Datum und Uhrzeit),
- Art des Ereignisses,
- Ursprung des Ereignisses (z. B. System, Ort, Benutzer).

Neben der elektronischen erfolgt auch eine nicht-technische Protokollierung. Dabei werden Protokolle der sicherheitsrelevanten internen Prozeduren und Prozesse angefertigt. Darüber hinaus werden u. a. folgende Registrierungsdaten erfasst und signiert aufbewahrt:

  - Nummer und Art des Identifizierungsdokumentes

- GID (unique identifier)
- Anrede
- Nachname
- Akad. Grad
- Namensvorsatz
- 1. Vorname
- 2. Vorname
- Geburtsdatum
- Geburtsort
- Geburtsname
- Zeitpunkt der Registrierung
- Einverständniserklärung zur Zertifikatsveröffentlichung.

5.4.2 Auswertung von Protokolldaten

Alle Protokolldaten werden regelmäßig und zusätzlich bei Verdacht auf Unregelmäßigkeiten umgehend überprüft.

Die Monitoringsysteme bereiten die gesammelten Protokolldaten durch Konsolidierung und Korrelationen auf, zeigen die Ergebnisse den verantwortlichen Rolleninhabern an und führen gegebenenfalls eine Alarmierung durch.

5.4.3 Aufbewahrungsfristen für Protokolldaten

Protokolldaten, die den Lebenszyklus der qualifizierten Zertifikate dokumentieren, werden vom VDA der BA entsprechend §16 Abs. 4 [VDG] für die gesamte Zeit seines Betriebs aufbewahrt.

5.4.4 Schutz der Protokolldaten

Alle Protokolldaten werden durch die Zugriffskontrollmechanismen der speichernden Systeme vor unbefugtem Zugriff und vor Manipulation geschützt.

5.4.5 Sicherungsverfahren für Protokolldaten

Alle elektronischen Protokolldaten werden im Rahmen der Sicherung der Produktivsysteme der Zertifizierungsdienste regelmäßig gesichert.

5.4.6 Internes/externes Protokollierungssystem

Die Protokollierung erfolgt durch interne Systeme des VDA der BA.

5.4.7 Benachrichtigung des Auslösers eines Ereignisses

Eine Benachrichtigung erfolgt ggf. im Rahmen der Untersuchung außergewöhnlicher Ereignisse.

5.4.8 Schwachstellenbewertung

Evtl. Schwachstellen werden durch permanente Überwachung und durch Sicherheits-Audits durch den Beauftragten für IT-Sicherheit und regelmäßig im Rahmen von Schwachstellentests durch externe Auditoren bewertet.

5.5 Archivierung von Protokolldaten

Die Archivierung relevanter Daten erfolgt in Übereinstimmung mit Artikel 24 Absatz 2 Buchstabe h) der [eIDAS] sowie §16 Abs. 4 [VDG] . Archivierte Daten werden vor unbefugter Einsichtnahme, Manipulation und Vernichtung geschützt.

5.5.1 Arten von zu archivierenden Daten

Siehe Abschnitt 5.4.1.

5.5.2 Archivierungsfristen

Die Protokolldaten, die den Lebenszyklus der qualifizierten Zertifikate dokumentieren, werden vom VDA der BA entsprechend §16 Abs. 4 [VDG] für die gesamte Zeit seines Betriebs aufbewahrt.

5.5.3 Schutzvorkehrungen für das Archiv

Papierdokumente werden im Archiv des Zertifizierungsdienstes archiviert. Für dieses sind ausreichende Schutzmaßnahmen implementiert, die im Sicherheitskonzept des VDA der BA detailliert beschrieben sind.

Elektronische Daten werden durch die Speicherung in den Produktiv-Systemen und ihren Backups archiviert. Für die archivierten elektronischen Daten sind daher die entsprechenden Schutzmaßnahmen (siehe Abschnitte 5.1, 5.2.2 und 5.2.3) wirksam.

5.5.4 Sicherungsverfahren für das Archiv

Archivierte Papierdokumente werden nicht zu Zwecken der Datensicherung kopiert.

Archivierte elektronische Daten werden im Rahmen der Datensicherung der Systeme gesichert.

5.5.5 Anforderungen an den Zeitstempel der archivierten Daten

Archivierte elektronische Daten werden mit einer Zeitangabe versehen.

Elektronische Dokumente, die im Zuge der

- erstmaligen Identitätsprüfung
- Zertifikatsannahme
- Bearbeitung einer schriftlichen Sperrung

erstellt werden, tragen einen qualifizierten elektronischen Zeitstempel.

Die Zeitangabe zu anderen archivierten elektronischen Daten entspricht der Systemzeit zur Erstellung der Daten, vgl. Abschnitt 6.8.

5.5.6 Internes oder externes Archivierungssystem

Die Archivierung erfolgt durch interne Systeme und im zentralen Archiv des Vertrauensdienstes.

5.5.7 Verfahren zur Beschaffung und Verifizierung von Archivdaten

Im Sicherheitskonzept des VDA der BA sind die Vorgaben für die Beschaffung von Archivdaten festgelegt. Insbesondere werden von Papierdokumenten nur Kopien herausgegeben.

5.6 Schlüsselwechsel der Zertifizierungsinstanzen

Ein Schlüsselwechsel einer Zertifizierungsinstanz (CA) erfolgt in folgenden Fällen:

- Die Schlüsselpaare, die der VDA der BA zur Erbringung seiner Zertifizierungsdienste einsetzt, besitzen eine beschränkte Gültigkeitsdauer, die im zugeordneten Zertifikat angegeben ist. Sie werden rechtzeitig vor Ablauf ihrer Gültigkeit gewechselt.
- Es besteht der Verdacht, dass der private Schlüssel einer Zertifizierungsinstanz kompromittiert wurde.
- Die dem Schlüsselpaar zugeordneten Algorithmen oder die verwendete Schlüssellänge bieten nach aktuellem Wissensstand für die vorgesehene Nutzungsdauer keine ausreichende Sicherheit.[5]

[5] Die Eignung der kryptographischen Algorithmen und Parameter werden regelmäßig geprüft und überwacht.

- Im qualifizierten Bereich zusätzlich, wenn der private Schlüssel, z. B. aufgrund eines Signaturkartendefektes, nicht mehr nutzbar ist.

Bei diesen Schlüsselwechseln erfolgt im qualifizierten Bereich eine Sperrung des Zertifikates der Zertifizierungsinstanz (CA-Zertifikat). Der alte private Schlüssel wird sicher vernichtet (siehe Abschnitt 6.2.10).

Gegebenenfalls wird das Zertifikat zum neuen Schlüsselpaar wie in Abschnitt 2.2 beschrieben veröffentlicht.

5.7 Kompromittierung und Wiederherstellung (Disaster Recovery)

5.7.1 Prozeduren bei Sicherheitsvorfällen

Es existiert ein Notfallkonzept, in dem die Prozesse, Prozeduren und Verantwortlichkeiten bei Notfällen geregelt sind. Zielsetzung dieser Notfallprozeduren ist die Minimierung von Ausfällen der Zertifizierungsdienstleistungen bei gleichzeitiger Aufrechterhaltung der Sicherheit. Die Ursachen des Vorfalls werden nach Wiederherstellung des Regelbetriebes analysiert und beseitigt.

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen

Nach einer vermuteten oder tatsächlichen Kompromittierung von Ressourcen, Software oder Daten finden die Notfallprozeduren Anwendung (siehe Abschnitt 5.7.1).

5.7.3 Wiederherstellung nach Schlüsselkompromittierung

Im Falle der Kompromittierung oder vermuteten Kompromittierung von privaten Schlüsseln der Vertrauensdienste wird das jeweilige Zertifikat sofort gesperrt (ausgenommen ein Wurzelzertifikat). Gleichzeitig werden alle mit Hilfe dieses privaten Schlüssels seit der vermuteten Kompromittierung ausgestellten Zertifikate gesperrt.

Sofern der Verdacht besteht, dass die für die Erzeugung und Anwendung des privaten Schlüssels eingesetzten Algorithmen, Parameter oder Geräte unsicher sind, wird eine entsprechende Untersuchung durchgeführt.

Der VDA der BA stellt Informationen für betroffene Antragsteller nach 1.3.3 und Vertrauende Dritte nach 1.3.4 bereit. Die Meldepflichten des VDA der BA gemäß [eIDAS] bleiben davon unberührt.

Für den Schlüsselwechsel der Zertifizierungsinstanz siehe Abschnitt 5.6.

5.7.4 Aufrechterhaltung des Betriebs im Notfall

Im Notfall wird durch die Infrastruktur am zweiten Standort (siehe Abschnitt 5.1.1) ein Notbetrieb sichergestellt. Die Maßnahmen zur Wiederherstellung des Normalbetriebes sind in einem Notfallkonzept geregelt.

Das Notfallkonzept wird stets aktuell gehalten und durch regelmäßige Notfallübungen überprüft.

5.8 Einstellung der Tätigkeit

Der VDA der BA verfügt über einen fortlaufend aktualisierten Beendigungsplan. Im Falle der endgültigen Einstellung einzelner oder aller Zertifizierungsdienste werden im Rahmen eines Beendigungsplanes u. a. folgende Maßnahmen ergriffen:

- Die Antragsteller nach Abschnitt 1.3.3 und Vertrauende Dritte nach Abschnitt 1.3.4 werden von der Einstellung der Zertifizierungsdienste, soweit möglich, mindestens zwei Monate im Voraus informiert.
- Die Aufsichtsstelle nach [eIDAS] wird informiert.
- Alle ausgestellten noch gültigen Zertifikate werden gesperrt.
- Alle nicht mehr benötigten privaten Schlüssel der Zertifizierungsdienste werden vernichtet (siehe Abschnitt 6.2.10).

- Die nach Artikel 24 [eIDAS] geforderte Nachprüfbarkeit ausgestellter qualifizierter Zertifikate über den Zeitraum der Gültigkeit hinaus wird sichergestellt.

6 Technische Sicherheitsmaßnahmen

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Das Signaturschlüsselpaar für die Erstellung und Prüfung einer qualifizierten elektronischen Signatur wird innerhalb der sicheren Umgebung des VDA der BA von der jeweiligen QSCD generiert.

Schlüsselpaare für die qualifizierten Dienste des VDA der BA werden innerhalb der sicheren Umgebung des VDA der BA von der jeweiligen QSCD generiert.

6.1.2 Übergabe privater Schlüssel an den Zertifikatsinhaber

Die Übergabe des privaten Schlüssels für Signaturerstellung an den Zertifikatsinhaber erfolgt durch Übergabe der entsprechenden Smartcard durch einen Kartenausgeber in der LRA. Die Übergabe erfolgt persönlich unter Gegenprüfung eines gültigen amtlichen Ausweisdokumentes. Der Zertifikatsinhaber muss den Empfang schriftlich bestätigen, vgl. Abschnitt 4.4.1.

Private Schlüssel der qualifizierten Dienste des VDA der BA werden nicht übergeben sondern verbleiben innerhalb der sicheren Umgebung des VDA der BA, vgl. 6.2.2.

6.1.3 Übergabe öffentlicher Schlüssel an den Zertifizierungsdienste-anbieter

Wird vom VDA der BA nicht unterstützt.

6.1.4 Übergabe öffentlicher CA Schlüssel an Dritte (Relying Parties)

Die öffentlichen Schlüssel werden als Teil des zugehörigen Zertifikates veröffentlicht, vgl. Abschnitt 2.

6.1.5 Schlüssellängen

Durch den VDA der BA neu ausgestellte Zertifikate nutzen RSA mit mindestens 3072 Bit Moduluslänge.

6.1.6 Erzeugung und Prüfung der Schlüsselparameter

Die Eignung der kryptographischen Algorithmen und Parameter wird vom Management ständig überwacht. Wenn notwendig werden die Schlüssellängen rechtzeitig angepasst, um die Sicherheit der Zertifizierungsdienste, der Zertifikate und der dafür zulässigen Anwendungen (siehe Abschnitt 1.4.1) zu gewährleisten.

Basis für geeignete Algorithmen und Parameter der qualifizierten Zertifikate und Schlüssel sind die Empfehlungen der Aufsichtsstelle nach [eIDAS].

6.1.7 Verwendungszweck der Schlüssel

Die genaue Bezeichnung des Verwendungszweckes des Schlüssels ist schlüsselabhängig und wird in der Zertifikatserweiterung KeyUsage bzw. ExtendedKeyUsage vermerkt (siehe Abschnitt 7.1.2). Es gilt:

- Die Schlüsselpaare der Zertifikatsinhaber dürfen ausschließlich zu den in Abschnitt 1.4 genannten Zwecken verwendet werden.
- Die privaten Schlüssel der CAs werden ausschließlich im Zuge der Erstellung von Zertifikaten und Sperrlisten verwendet.
- Die privaten Schlüssel des OCSP-Verzeichnisdienstes werden ausschließlich im Zuge der Erstellung von OCSP-Antworten verwendet.
- Die privaten Schlüssel des Zeitstempeldienstes werden ausschließlich im Zuge der Erstellung von Zeitstempeln verwendet.

6.2 Schutz der privaten Schlüssel und der kryptographischen Module

6.2.1 Standards für Schutzmechanismen und Bewertung der kryptographischen Module

Bei den Signaturkarten handelt es sich um eine qualifizierte elektronische Signaturerstellungseinheiten (QSCD) im Sinne der [eIDAS]. In der Standard-Hierarchie werden für die qualifizierten Dienste (qualifizierte Signatur-CA, TSP-R, OCSP-R) qualifizierte elektronische Siegelerstellungseinheiten im Sinne der [eIDAS] in Form von Hardware-Sicherheitsmodulen (HSM) verwendet.

6.2.2 Aufteilung der Kontrolle privater Schlüssel auf mehrere Personen

Bei privaten Schlüsseln auf Signaturkarten findet keine Aufteilung statt. Die privaten Schlüssel der qualifizierten Vertrauensdienste stehen unter Kontrolle der Sicherheitsoffiziere des VDA der BA.

6.2.3 Treuhänderische Hinterlegung privater Schlüssel

Eine treuhänderische Hinterlegung der privaten Schlüssel findet nicht statt.

6.2.4 Sicherung und Wiederherstellung privater Schlüssel

Sicherung und Wiederherstellung der privaten Schlüssel in Signaturkarten finden nicht statt.

Private Schlüssel der qualifizierten Dienste, wenn diese in einem HSM gespeichert sind, werden gesichert.

6.2.5 Archivierung privater Schlüssel

Eine Archivierung privater Schlüssel findet nicht statt.

6.2.6 Transfer privater Schlüssel

Ein Transfer wird nicht durchgeführt. Die privaten Schlüssel werden durch die qualifizierte elektronische Signaturerstellungseinheit erzeugt und können nicht ausgelesen werden.

6.2.7 Speicherung privater Schlüssel

Die privaten Schlüssel sind innerhalb der qualifizierten elektronischen Signaturerstellungseinheit so gespeichert, dass sie nicht ausgelesen werden können.

6.2.8 Methoden zur Aktivierung privater Schlüssel

Die Anwendung eines privaten Schlüssels einer Smartcard erfordert die Eingabe einer durch den Zertifikatsinhaber selber vergebenen PIN.

Einzelsignaturkarten erlauben nach der Aktivierung eine einmalige Signaturerstellung.

Massensignaturkarten und Mandanten-Massensignaturkarten erlauben nach der Aktivierung bis zur Deaktivierung nach 6.2.9 die Erstellung einer unbegrenzten Anzahl von Signaturen.

Die Aktivierung privater Schlüssel der qualifizierten Dienste erfolgt ausschließlich unter Mitwirkung mehrerer berechtigter Mitarbeiter, ausschließlich im Rahmen festgelegter Prozeduren und in der vorgesehenen sicheren Umgebung.

6.2.9 Methoden zur Deaktivierung privater Schlüssel

Private Schlüssel auf den Smartcards sind deaktiviert, solange keine Aktivierung mit einer PIN erfolgt ist. Der qualifizierte Signaturschlüssel einer Einzelsignaturkarte wird nach einmaliger Anwendung automatisch deaktiviert. Massensignaturkarten und Mandanten-Massensignaturkarten werden

deaktiviert, indem sie aus dem Kartenleser entfernt werden oder der Prozess, der auf die Karten zugreift, beendet wird.

Private Schlüssel in HSM sind deaktiviert, solange keine Aktivierung über den Sicherheitsmechanismus des HSM erfolgt ist. Diese erfolgt ausschließlich unter Mitwirkung von mindestens zwei berechtigten Mitarbeitern.

6.2.10 Methoden zur Vernichtung privater Schlüssel

Private Schlüssel der qualifizierten Dienste werden entweder durch einen sicheren Löschmechanismus des Hardware-Sicherheitsmoduls oder durch physikalische Zerstörung der Dienstekarte vernichtet. Zertifikatsinhaber haben gesperrte oder abgelaufene Smartcards (soweit noch verfügbar) durch Zerstören des Chips zu vernichten. Dies kann auch in der LRA erfolgen.

6.2.11 Bewertung kryptographischer Module

Siehe Abschnitt 6.2.1.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel werden mit den qualifizierten Zertifikaten vom VDA der BA entsprechend §16 Abs. 4 [VDG] für die gesamte Zeit seines Betriebs aufbewahrt.

6.3.2 Verwendungsdauern von Zertifikaten und Schlüsselpaaren

Die Dienstezertifikate des VDA der BA waren in der Legacy-Hierarchie fünf Jahre gültig. In der Standard-Hierarchie gelten Zertifikate der Signatur-CA für acht Jahre, Zertifikate der OCSP- und TSP-Responder sieben Jahre.

Signaturzertifikate oder Massensignaturzertifikate sind ab dem 01.07.2022 drei Jahre gültig. Davor waren sie fünf Jahre gültig.

Private Schlüssel der qualifizierten Dienste werden nach Ablauf ihres Zertifikates nicht mehr verwendet (siehe Abschnitt 6.2.10).

Die Eignung der kryptographischen Algorithmen und Parameter wird vom Management ständig überwacht. Wenn sich herausstellt, dass ein Algorithmus oder die entsprechende Schlüssellänge über die Gültigkeitsdauer des Zertifikates hinweg keine ausreichende Sicherheit mehr bietet, wird rechtzeitig der Wechsel der betroffenen Schlüsselpaare veranlasst, vgl. Abschnitt 5.6.

6.4 Aktivierungsdaten

Die Nutzung des privaten Schlüssels ist durch die zugehörige PIN geschützt.

6.4.1 Erzeugung und Installation von Aktivierungsdaten

Die PINs der Smartcard (siehe Abschnitt 6.4.2) werden vom Zertifikatsinhaber bei der Freischaltung der Karte (siehe Abschnittes 4.4.1) vergeben. Die Freischaltung kann erst nach der Ausgabe (siehe Abschnitt 6.1.2) der Karte an den Inhaber erfolgen.

Im Trustcenter wird die PIN einer Chipkarte, die zur Aktivierung des eingesetzten HSM genutzt wird, im Rahmen des Initialisierungsprozesses durch den Inhaber der Chipkarte vergeben.

6.4.2 Schutzmaßnahmen für Aktivierungsdaten

Die PINs der Smartcards werden unter anderem durch die folgenden Maßnahmen geschützt:

- Nach drei aufeinanderfolgenden fehlerhaften Eingaben einer PIN werden die entsprechenden privaten Schlüssel für die Benutzung gesperrt.
- Jeder PIN kann eine PUK zugeordnet sein, mit der die privaten Schlüssel wieder entsperrt werden können.

- Die PINs und PUKs können nicht aus den Karten ausgelesen werden.
- Ist der Signatur-PIN keine PUK zugeordnet[6], kann die Signatur-PIN nach drei aufeinanderfolgenden fehlerhaften Eingaben nicht mehr genutzt werden.
- Die Signatur-PIN und die ggf. zugeordnete[6] PUK können nur nach Eingabe des aktuellen Wertes geändert werden.
- Bei der Übergabe einer dDk oder Gästekarte muss der Karteninhaber die Karte freischalten (siehe Abschnitt 4.4.1) und dabei die PINs und PUK der Karte frei vergeben. Eine Nutzung der privaten Schlüssel ist erst nach Vergabe der PIN und der ggf. zugeordneten[6] PUK und Freischaltung der Karte möglich.
- Die Signatur-PIN-Vergabe im Rahmen der Freischaltung im Sinne des Abschnitts 4.4.1 ist nur möglich, wenn noch keine PIN gesetzt wurde. Dadurch kann der Zertifikatsinhaber prüfen, dass eine PIN nicht schon vergeben und die Signaturkarte evtl. benutzt wurde.
- Für Massensignaturkarte, Mandanten-Signaturkarte und Mandanten–Massensignaturkarte liegt es in der Verantwortung des Bestellers, für angemessene Sicherheitsmaßnahmen zu sorgen.
- Eine Speicherung der PINs und PUKs durch den VDA der BA findet nicht statt.

Die PINs zum Aktivieren der privaten Schlüssel der qualifizierten Dienste werden durch die folgenden organisatorischen Maßnahmen geschützt:

- Die Mitarbeiter sind verpflichtet, PINs vertraulich zu behandeln.
- Falls einem Mitarbeiter seine Rolle entzogen wird, wird ihm auch der Zugriff auf die ihm zugeordneten Smartcards entzogen.

6.4.3 Weitere Aspekte zu Aktivierungsdaten

Bei Smartcards sind der Wert für die maximale Anzahl der Fehlbedienungen sowie die Länge von PIN und PUK fest vorgegeben.

6.5 Sicherheitsbestimmungen für Computer

6.5.1 Spezifische Sicherheitsanforderungen für Computer

Auf den für die Erbringung der qualifizierten Dienste notwendigen Systemen sowie auf den Systemen, die dem Schutz der Einrichtungen der qualifizierten Dienste dienen, sind alle notwendigen und anwendbaren Sicherheitsmaßnahmen der IT-Grundschutzkataloge umgesetzt. Zusätzlich werden die folgenden Maßnahmen zur Computersicherheit umgesetzt:

- Die zentralen IT-Systeme sind in verschlossenen Technikschränken untergebracht, die nur im 4-Augen-Prinzip geöffnet werden können.
- Die Vergabe und Kontrolle von Zugriffs- und Zutrittsrechten erfolgt rollenbasiert.
- Die sicherheitskritischen Systeme sind mit Siegeln versehen.
- Die Administration der zentralen Systeme wird protokolliert.
- Die Sicherheit der zentralen Systeme und die dafür eingesetzten Maßnahmen werden durch ein Monitoringsystem automatisch überwacht (siehe Abschnitt 5.4).
- Die Sicherheit der Systeme und die dafür eingesetzten Maßnahmen sind Gegenstand der regelmäßigen Audits (siehe Kapitel 8).
- In dem Rechenzentrum (RZ) befinden sich nur Systeme, welche durch den VDA der BA betrieben werden.
- Nicht benötigte Dienste sind deaktiviert.

[6] Abhängig von der verwendeten QSCD

6.5.2 Bewertung der Computersicherheit

Für die QSCD wurde eine formale Evaluierung der Systemsicherheit nach den Common Criteria for Information Technology Security Evaluation (CC) durchgeführt.

Darüber hinaus wurde im Sicherheitskonzept des VDA der BA eine Bedrohungs- und Risikoanalyse durchgeführt, die die Wirksamkeit aller getroffenen Maßnahmen untersucht.

6.6 Technische Kontrollen des Software-Lebenszyklus

Der VDA der BA stellt sicher, dass die für die Zertifizierungsdienste eingesetzte Software in einer Weise entwickelt, getestet, ausgeliefert, installiert, konfiguriert, betrieben und gewartet wird, so dass ihre Authentizität, Integrität, und bestimmungsgemäßen Funktionsfähigkeit sichergestellt ist.

6.6.1 Systementwicklungsmaßnahmen

Änderungen an Software oder Konfiguration werden in einem Versionskontrollsystem mit persönlichem Login nachgehalten. Programmpakete werden vom Releasemanagement kryptographisch signiert. Änderungen an Software oder Konfiguration werden zunächst in einer Testumgebung und im Erfolgsfall anschließend in einer Referenzumgebung der Produktion erprobt. Softwareänderungen in der Produktion sind nur unter Verwendung des PIN-gesicherten Installationsmediums und nach Freigabe durch die TC-Leitung möglich.

6.6.2 Sicherheitsmanagement

Im Sicherheitskonzept des VDA der BA sind die Verantwortlichkeiten und Prozesse des Sicherheitsmanagements definiert.

6.6.3 Bewertung der Maßnahmen zur Kontrolle des Lebenszyklus

Im Sicherheitskonzept des VDA der BA wurde eine Bedrohungs- und Risikoanalyse durchgeführt, welche die Wirksamkeit aller getroffenen Maßnahmen untersucht.

6.7 Maßnahmen zur Netzwerksicherheit

In den für die Erbringung der Zertifizierungsdienste notwendigen Netzwerken sind alle erforderlichen Sicherheitsmaßnahmen implementiert. Dazu zählen:

- Die Aufteilung in verschiedene Netzwerksegmente und die Beschränkung und Überwachung der Kommunikation durch Firewalls.
- Sämtliche Kommunikationsverbindungen zwischen Systemen unterschiedlicher Netzwerksegmente sind durch kryptographische Mechanismen gesichert.
- Die Sicherheit der Netzwerke und die dafür eingesetzten Maßnahmen sind Gegenstand der regelmäßigen Audits (siehe Kapitel 8).

6.8 Zeitstempel

Die von den Systemen der Zertifizierungsdienste protokollierten Daten (siehe Abschnitt 5.4.1) werden mit Zeitangaben versehen. Die Systemzeiten sind synchronisiert. Eine kryptographische Sicherung der Zeitangaben in den Protokolldaten findet nicht statt.

7 Profile

7.1 Zertifikatsprofile

7.1.1 Versionsnummer(n)

Die qualifizierten Zertifikate und Dienstezertifikate entsprechen dem Standard [X509] Version 3 bzw. seiner Profilierung in [RFC5280]. Sie erfüllen zudem die Anforderungen von [eIDAS]. Qualifizierte Zertifikate genügen zudem dem SigG-Profile von Common PKI[COMPKI].

7.1.2 Zertifikatserweiterungen

Zertifikate aus der Standard- oder Legacy-Hierarchie, vgl. Abschnitt 1.1, enthalten folgende nicht-kritische Erweiterungen:

- AuthorityKeyIdentifier (nicht im Zertifikat der qualifizierten Wurzel-CA)
- SubjectKeyIdentifier
- CertificatePolicies
- AuthorityInfoAccess (nicht in selbstsignierten CA-Zertifikaten)
- ExtendedKeyUsage (nur OCSP)
- QCStatement: Abweichend von [ETSI-POLQ], clause 6.6.1 a) werden in qualifizierten Zertifikaten für elektronische Signaturen nur esi4-qcStatement-1 und esi4-qcStatement-4 aus [ETSI-QCST] eingetragen. Ein PKI Disclosure Statement ist nach [eIDAS] nicht notwendig und wird nicht eingetragen. Handelt es sich bei einem Dienstezertifikat um ein Zertifikat für elektronische Siegel, wird nur esi4-qcStatement-6 mit dem QC type identifier id-etsi-qct-eseal eingetragen. Diese Siegelzertifikate sind *nicht* qualifiziert.

und folgende kritische Erweiterungen:

- KeyUsage
  - selbstsignierte CA-Zertifikate: `keyCertSign, CRLSign.`
  - Qualifizierte Signatur-CA-Zertifikate der Legacy-Hierarchie: `keyCertSign`
  - Signatur- und Massensignaturzertifikate: `nonRepudiation`
- BasicConstraints
- ExtendedKeyUsage (nur TSP)

7.1.3 Algorithmenbezeichner (OID)

Die verwendeten Algorithmenbezeichner entsprechen den gängigen Standards.

7.1.4 Namensformen

Es gelten die Regelungen des Standard [X509] bzw. seiner Profilierung in [RFC5280] bzw. für qualifizierte Zertifikate dessen Profilierung in [COMPKI].

Für das Feld `Issuer` gelten zusätzlich folgende Festlegungen:

- Attribut `CountryName`: <DE>
- Attribut `Organization`: <Bundesagentur fuer Arbeit>
- Attribut `CommonName` (CN): Der Common Name der CA-Zertifikate ist nach dem folgenden Schema aufgebaut: <Präfix>-<Bezeichner>-CA-<lfd Nummer>:PN
  - Dienstezertifikate der qualifizierten Dienste nutzen das Präfix BA-QC, andernfalls ist das Präfix BA.
  - Der Bezeichner ist ein eindeutiger Namensbestandteil, der die Nutzung der CA andeuten soll.
  - Allen CA folgt danach der Kennzeichner „CA“.

- Die laufende Nummer wird für jeden Namen beginnend mit „1“ fortlaufend ganzzahlig geführt. Abschließend erfolgt die Kennzeichnung des CN als Pseudonym gemäß [COMPKI].

  Beispiel: CN=BA-QC-Wurzel-CA-1:PN; Es handelt sich um den Common Name des Dienstezertifikats eines qualifizierten Dienstes (BA-QC), genauer der Wurzel-CA (Bezeichner), mit der laufenden Nummer 1.

7.1.5 Nutzung von Erweiterungen zu Namensbeschränkungen

Erweiterungen zur Namensbeschränkung werden nicht verwendet.

7.1.6 Bezeichner für Zertifizierungsrichtlinien (OID)

Die folgende OID wird in der Erweiterung certificatePolicy für die Referenzierung der CP für qualifizierte Zertifikate verwendet:

- CP der qualifizierten Zertifikate: 1.3.6.1.4.1.21679.1.1.5

Vgl. Abschnitt 1.2.

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen (Policy-Constraints)

Erweiterungen zur Richtlinienbeschränkungen werden nicht verwendet.

7.1.8 Syntax und Semantik von Policy Qualifiern

Richtlinien-Qualifier in der Erweiterung Certificate Policies werden nicht verwendet.

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (Certificate Policies)

Die Erweiterungen für Zertifizierungsrichtlinien in den Zertifikaten sind nicht kritisch.

7.2 Profil der Sperrlisten

Für qualifizierte Zertifikate werden keine Sperrlisten veröffentlicht.

7.2.1 Versionsnummer(n)

Entfällt.

7.2.2 Erweiterungen der Sperrlisten

Entfällt.

7.3 OCSP-Profile

7.3.1 Versionsnummer(n)

Der OCSP-Verzeichnisdienst der BA unterstützt OCSP nach [RFC2560]. Zusätzlich werden Erweiterungen von Common PKI [COMPKI] verwendet.

7.3.2 OCSP-Erweiterungen

Der OCSP-Verzeichnisdienst unterstützt bei Anfragen die in der folgenden Tabelle angegebenen Erweiterungen:

Erweiterungen	Inhalt
Nonce	Wert, der die Antwort kryptographisch an die Anfrage bindet (optional)
AcceptableResponses	id-pkix-ocsp-basic
ServiceLocator	Wird vom OCSP-Responder nicht ausgewertet

Tabelle 3 - Zulässige Erweiterungen der OCSP-Anfragen

In den Antworten verwendet der OCSP-Verzeichnisdienst die in der folgenden Tabelle angegebenen Erweiterungen:

Erweiterungen	Inhalt
Nonce	Gleicher Wert wie in der Anfrage. Nicht existent, falls in Anfrage nicht vorhanden.
ArchiveCutoff	Wie in [RFC2560] beschrieben. Das Aufbewahrungsintervall beträgt 10950 Tage.
CertHash	Bei Status good oder revoked wird der SHA-1 Hash-Wert des Zertifikats eingetragen.
RequestedCertificate	Enthält das Zertifikat, falls RetrieveIfAllowed bei der Anfrage gesetzt war.

Tabelle 4 - Erweiterungen der OCSP-Antworten

8 Revisionen und andere Bewertungen

Die BA führt selbst regelmäßig interne Audits durch, um die Einhaltung der Sicherheitsmaßnahmen sicherzustellen. Neben internen, selbst durchgeführten Audits werden auch externe Prüfungen gemäß [eIDAS] Artikel 20 von einer unabhängigen Konformitätsbewertungsstelle durchgeführt.

8.1 Häufigkeiten von Revisionen

Interne Revisionen bzw. Audits werden regelmäßig nach einem Auditplan sowie bei Bedarf nach sicherheitskritischen Vorfällen durchgeführt. Dazu gehören insbesondere monatliche Schwachstellenscans aus dem Netz der BA sowie mindestens jährliche PEN-Tests.

Mindestens alle 24 Monate werden Prüfungen gemäß [eIDAS] Artikel 20 von einer unabhängigen Konformitätsbewertungsstelle durchgeführt.

Die Aufsichtsstelle nach [eIDAS] kann jederzeit eine Überprüfung vornehmen oder durch eine unabhängige Konformitätsbewertungsstelle vornehmen lassen.

8.2 Identität und Qualifikation des Auditors

Der Beauftragte für IT-Sicherheit ist verantwortlich für die Prüfung der IT-Sicherheit innerhalb des VDA der BA. Zu seinen Aufgaben gehören:

- Initiierung regelmäßiger Prüfungen
- Überprüfung, ob das interne Kontrollsystem wirksam ist.

Der Beauftragte für IT-Sicherheit des IT-Systemhauses ist verantwortlich für die Überprüfung der Sicherheit des Vertrauensdienstes im laufenden Betrieb. Der Beauftragte für IT-Sicherheit im IT-Systemhaus besitzt umfangreiche Kompetenz und Erfahrung im Bereich Informationssicherheit, PKI und bezüglich der relevanten Gesetzgebung (vor allem zur elektronischen Signatur und zum Datenschutz).

Der Schwachstellenscan wird durch den Bereich Cert-BA im IT-Systemhaus durchgeführt, der über angemessene Expertise verfügt.

Die Durchführung des PEN-Tests wird von der BA an einen externen Dienstleister vergeben.

Unabhängige Konformitätsbewertungsstellen sind gemäß [eIDAS] Artikel 3 Satz 1 Nr. 18 akkreditiert.

8.3 Beziehungen zwischen Auditor und zu untersuchender Partei

Der interne Auditor ist ein Mitarbeiter der BA. Das Rollenkonzept des VDA der BA stellt sicher, dass der Auditor in keiner Weise an der Administration oder dem Betrieb der Zertifizierungsdienste beteiligt ist. Außerdem ist der Auditor weder direkt noch indirekt vom Zertifizierungsdienst der BA oder seinen Mitarbeitern abhängig.

Der beauftragte PEN-Tester und die Konformitätsbewertungsstelle stehen in vertraglicher Beziehung zur BA, haben aber keine Berührungspunkte mit Aufbau oder Betrieb der Vertrauensdienste.

8.4 Umfang der Prüfungen

Das Ziel der Audits ist die Überprüfung der Umsetzung der definierten Sicherheitsmaßnahmen. Die Prüfungen werden nach Kontrollplänen durchgeführt und umfassen insbesondere die folgenden Bereiche:

- Konfiguration der sicherheitskritischen Systeme,
- Log-Daten sicherheitskritischer Systeme,
- Protokolle sicherheitskritischer Prozeduren (z. B. Prozeduren der Schlüsselerzeugung, Notfallprozeduren, Updaten der Systeme),

- Dokumentation der personellen Sicherheitsmaßnahmen (z. B. Schulungsnachweise, Dienstpläne),
- Dokumentation zu Prozeduren und Systemen (z. B. Notfallpläne, Systemhandbücher),
- Schlüssel sowie Authentisierungs-Chipkarten (z. B. für die Zugangskontrolle oder den Zugriff auf Signaturkarten und Hardware-Sicherheitsmodule),
- Archivdaten,
- Einrichtungen zur baulichen und physikalischen Sicherheit (z. B. Zutrittskontrolle, Brandschutz, Klimatisierung).

Die Grundlage für die externen Prüfungen bildet das Sicherheitskonzept des VDA der BA.

8.5 Maßnahmen bei Mängeln

Festgestellte Mängel werden je nach Schwere und Dringlichkeit im Rahmen des definierten Schwachstellenmanagements betrachtet und entsprechend behandelt. Schwerwiegende Mängel werden an das Security-Management der BA gemeldet.

Die Meldepflichten und Maßnahmen der [eIDAS] bleiben davon unberührt.

8.6 Veröffentlichung der Ergebnisse

Die Ergebnisse werden in einem Audit-Bericht dokumentiert. Sie werden nicht veröffentlicht.

Das Ergebnis einer regelmäßigen ([eIDAS] Artikel 20) oder von der Aufsichtsstelle nach [eIDAS] angeordneten Prüfung wird der Aufsichtsstelle zur Verfügung gestellt.

Meldepflichten des VDA der BA gemäß [eIDAS] bleiben davon unberührt.

9 Weitere geschäftliche und rechtliche Regelungen

9.1 Gebühren

Die Dienstleistungen des Zertifizierungsdienstes sind für Mitarbeiter der BA im Rechtskreis SGB III gebührenfrei.

Werden die Dienstleistungen von einem anderen als dem in Satz 1 genannten Antragsteller, vgl. Abschnitt 1.3.3, in Anspruch genommen, gelten die Regelungen der folgenden Absätze.

9.1.1 Gebühren für die Ausstellung oder Erneuerung von Zertifikaten

Gemeinsame Einrichtungen nach SGB II, die für ihre Mitarbeiter auf Basis § 50 Abs. 3 SGB II die dDk eingekauft haben, müssen die dafür vereinbarten Gebühren zur Aufwandsentschädigung entrichten.

Mandanten müssen für die Ausstellung der Signaturkarten für ihre Mitarbeiter die vertraglich vereinbarten Gebühren zur Aufwandentschädigung entrichten.

9.1.2 Gebühren für den Abruf von Zertifikaten

Derzeit erhebt die BA für den Abruf von Zertifikaten über die in 2.1 genannten Verzeichnisdienste keine Gebühren.

9.1.3 Gebühren für die Abfrage von Zertifikatsstatusinformationen

Die BA erhebt für den Abruf von Zertifikatsstatusinformationen über OCSP keine Gebühren.

9.1.4 Gebühren für andere Dienstleistungen

Für den Betrieb des Zertifizierungsdienstes wird von den Antragstellern eine vertraglich vereinbarte Gebühr über den Gültigkeitszeitraum des Zertifikats erhoben.

9.1.5 Rückerstattungen

Eine Rückerstattung rechtmäßig erhobener Gebühren erfolgt nicht. Eine Rückerstattung ist nur bei vertraglicher Vereinbarung möglich. Für die gemeinsamen Einrichtungen ist die Regelung zur Rückerstattung Bestandteil der eingekauften Dienstleistung.

9.2 Finanzielle Verantwortung

9.2.1 Deckungsvorsorge

Der VDA der BA verfügt über die erforderliche Deckungsvorsorge in Form einer Versicherung gemäß §2 [VDV].

9.2.2 Weitere Vermögenswerte

Keine weiteren Vermögenswerte.

9.2.3 Erweiterte Versicherung oder Garantie

Aufgrund der Zuschusspflicht des Bundes aus § 365 SGB III kann eine Insolvenz des VDA der BA nicht eintreten.

9.3 Vertraulichkeit betrieblicher Informationen

9.3.1 Art der geheim zu haltenden Information

Als vertraulich gelten alle betrieblichen Informationen, die nicht von der BA über die Verzeichnisdienste oder über ihre Web-Seiten veröffentlicht werden.

9.3.2 Öffentliche Informationen

Als öffentlich gelten alle Informationen in den ausgestellten und veröffentlichten Zertifikaten, die Sperrinformationen sowie alle veröffentlichten CPS/CP-Versionen.

9.3.3 Verantwortlichkeit für den Schutz von geheim zu haltender Information

Der VDA der BA sichert die in Abschnitt 9.3.1 genannten vertraulichen Informationen vor Manipulation und unbefugter Kenntnisnahme durch Dritte.

9.4 Schutz personenbezogener Daten

9.4.1 Geheimhaltung

Der VDA der BA beachtet die gesetzlichen Anforderungen zur Geheimhaltung von vertraulichen Daten, insbesondere die des Bundesdatenschutzgesetzes sowie weiterer Datenschutzvorschriften, u.a. der EU-Datenschutz-Grundverordnung. Die BA trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten dürfen im Rahmen der Diensterbringung an Dritte nur im Rahmen vertraglicher Regelungen weitergegeben werden, wenn vom Dritten zuvor eine Vertraulichkeitserklärung unterzeichnet wurde, in der dieser die mit der Aufgabe betrauten Mitarbeiter zur Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet hat.

9.4.2 Vertraulich zu behandelnde Daten

Als vertraulich gelten alle personenbezogenen Daten, die nicht Bestandteil eines Zertifikats sind.

9.4.3 Nicht vertraulich zu behandelnde Daten

Alle im Zertifikat enthaltenen Informationen gelten als nicht vertraulich.

9.4.4 Verantwortlichkeit für den Schutz privater Informationen

Der VDA der BA wird die Daten des Zertifikatsinhabers, soweit sie in personenbezogener Form vorliegen, unter Einhaltung der einschlägigen Bestimmungen der Datenschutzvorschriften behandeln (siehe auch 9.4.1).

9.4.5 Einverständniserklärung zur Nutzung privater Informationen

Soweit erforderlich, erteilt der Antragsteller sein Einverständnis, dass seine personenbezogenen Daten zum Zweck der Diensterbringung auf Basis der geltenden Gesetze verarbeitet werden dürfen.

9.4.6 Weitergabe von Informationen an Ermittlungsinstanzen oder Behörden

Es gelten die Vorschriften des §8 [VDG], insbesondere die Absätze

(2) Der Vertrauensdiensteanbieter darf personenbezogene Daten einer Person, die Vertrauensdienste nutzt, den zuständigen Stellen übermitteln,

1. soweit die zuständigen Stellen die Übermittlung nach Maßgabe der hierfür geltenden Bestimmungen verlangen, da die Übermittlung erforderlich ist,

a) für die Verfolgung von Straftaten oder Ordnungswidrigkeiten,

b) zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder

c) für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden,

oder

2. soweit Gerichte die Übermittlung im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.
   Die Berechtigung zur Datenübermittlung nach Satz 1 Nummer 1 gilt nicht, soweit sie durch andere Gesetze ausdrücklich ausgeschlossen ist.

(3) Die Vertrauensdiensteanbieter haben die Übermittlung zu dokumentieren. Die Dokumentation ist zwölf Monate aufzubewahren.

(5) Die allgemeinen Datenschutzanforderungen bleiben unberührt.

9.4.7 Sonstige Offenlegungsgründe

Keine weiteren Offenlegungsgründe.

9.5 Geistiges Eigentum und dessen Rechte

Bestand und Inhalt von Urheber- und sonstigen Immaterialgüterrechten richten sich nach den allgemeinen gesetzlichen Vorschriften.

9.6 Gewährleistung, Sorgfalts- und Mitwirkungspflichten

9.6.1 Verpflichtung der Zertifizierungsstelle

Der VDA der BA sichert zu, dass die von ihm erzeugten Zertifikate alle Anforderungen der vorliegenden CP erfüllen.

9.6.2 Verpflichtung der Registrierungsstelle

Die LRAs sind verpflichtet, gemäß der vorliegenden CP zu handeln.

9.6.3 Verpflichtung des Antragstellers

Der Antragsteller, siehe Abschnitt 1.3.3, hat insbesondere folgende Pflichten:

- Die Zertifikate sind nur bestimmungsgemäß und nicht missbräuchlich zu benutzen.
- Der dem qualifizierten Zertifikat zugeordnete private Schlüssel und seine Aktivierungsdaten sind geheim zu halten und sicher vor unbefugten Zugriffen aufzubewahren.
- Mängel, Schäden oder sonstige Störungen sind unverzüglich der Registrierungsstelle des Zertifizierungsdienstes der BA anzuzeigen.
- Bei Verlust oder Verdacht der Kompromittierung eines privaten Schlüssels ist unverzüglich eine Sperrung des entsprechenden Zertifikates zu veranlassen.
- Er hat die Hinweise in der Unterrichtung zu beachten.
- Er hat sich über Aktualisierung der CP zu informieren, siehe Abschnitt 9.12.2.

9.6.4 Verpflichtung vertrauender Dritte

Vertrauende Dritte sind dazu verpflichtet, gemäß den in Abschnitt 4.5.2 und Abschnitt 4.9.6 beschriebenen Regeln vorzugehen.

9.6.5 Verpflichtung weiterer Teilnehmer

Keine Verpflichtungen für andere Teilnehmer.

9.7 Haftungsausschluss

Der VDA der BA übernimmt trotz Umsetzung aller erforderlichen Sicherheitsmaßnahmen keine Gewähr dafür, dass die Datenverarbeitungssysteme ohne Unterbrechung betriebsbereit sind und fehlerfrei arbeiten.

Datenverluste in Folge technischer Störungen und die Kenntnisnahme vertraulicher Daten durch unberechtigte Eingriffe sind auch bei Beachtung der erforderlichen Sorgfalt nie völlig auszuschließen.

9.8 Haftungsbegrenzungen

Die Haftung des VDA der BA richtet sich nach den jeweiligen gesetzlichen Bestimmungen, insbesondere § 10 Vertrauensdienstegesetz [VDG] sowie §2 Vertrauensdiensteverordnung [VDV], sowie den Schadensersatzregelungen des Allgemeinen Bürgerlichen Gesetzbuches.

9.9 Schadensersatz

Siehe 9.8.

9.10 Gültigkeit der CP

9.10.1 Gültigkeitszeitraum

Die vorliegende CP ist ab dem 06.07.2023 gültig. Die Gültigkeit endet spätestens mit der Einstellung der Tätigkeit des VDA der BA (siehe Abschnitt 5.8).

9.10.2 Vorzeitiger Ablauf der Gültigkeit

Die Gültigkeit dieser CP endet vorzeitig mit der Veröffentlichung einer neuen Version.

9.10.3 Konsequenzen des Ablaufs dieses Dokumentes

Die Teilnehmer sind bis zum Ende der Nutzung (End of subscription) siehe 4.11, oder der Einstellung der Tätigkeit, siehe 5.8, an die Bestimmungen der dann gültigen Version der CP gebunden.

9.11 Individuelle Mitteilungen und Absprachen mit den Teilnehmern

Für individuelle Mitteilungen und Absprachen mit den Teilnehmern werden die jeweils gültigen Kontaktinformationen und Kommunikationswege (E-Mail, Telefon, Post, etc.) genutzt.

9.12 Änderungen der Richtlinie

9.12.1 Verfahren für die Änderung

Für die Pflege der CP ist ein interner Prozess mit einer entsprechenden Rolle auf Managementebene definiert. Durch diesen wird sichergestellt, dass die CP stets die aktuellen Praktiken der Zertifizierungsdienste der BA wiedergibt.

Bei einer Aktualisierung der CP wird nur dann die volle Versionsnummer erhöht, wenn sicherheitsrelevante Veränderungen der beschriebenen Praktiken vorgenommen wurden. Die Entscheidung über die Erhöhung der vollen Versionsnummer ist Teil des Prozesses zur Aktualisierung der CP.

9.12.2 Benachrichtigungsverfahren und Veröffentlichungsperioden

Eine Aktualisierung der CP wird auf der Webseite des VDA der BA, siehe Abschnitt 2.1, bekannt gegeben.

9.12.3 Bedingungen für Änderungen der Objekt-Kennung (OID)

Die Entscheidung über die Zuweisung einer neuen OID ist Teil des Prozesses zur Aktualisierung der CP. Bei Ergänzungen oder Modifikationen der CP entscheidet der VDA der BA, ob sich daraus signifikante Änderungen der Sicherheit des Vertrauensdienstes, der Rechte und Pflichten der Teilnehmer oder der Anwendbarkeit der Zertifikate ergeben, die eine Änderung der OID bedingen.

9.13 Schiedsverfahren

Die Aufsichtsstelle nach [eIDAS], derzeit Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, kann zur Beilegung telekommunikationsrechtlicher Streitigkeiten einen einvernehmlichen Einigungsversuch vor einer Gütestelle (Mediationsverfahren) gemäß § 124 TKG vorschlagen.

9.14 Geltende Gesetze

Es gilt deutsches Recht.

9.15 Konformität mit anwendbarem Recht

Für Streitigkeiten aus dieser CP gilt – soweit gesetzlich zulässig – als Gerichtsstand Nürnberg.

9.16 Sonstige Bestimmungen

9.16.1 Vollständigkeitsklausel

Alle in vorliegender CP enthaltenen Regelungen gelten zwischen dem VDA der BA und den Teilnehmern. Mündliche Vereinbarungen bzw. Nebenabreden bestehen nicht.

9.16.2 Abtretung der Rechte

Entfällt.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser CP unwirksam sein oder Lücken enthalten, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.

Anstelle der unwirksamen Bestimmung gilt die wirksame Bestimmung als vereinbart, welche der ursprünglich gewollten am nächsten kommt.

9.16.4 Vollstreckung (Anwaltskosten und Rechtsverzicht)

Entfällt.

9.16.5 Höhere Gewalt (Force Majeure)

Entfällt.

9.17 Andere Regelungen

9.17.1 Organisatorisch

Keine

9.17.2 Testmöglichkeiten

Der VDA der BA stellt Antragstellern im Sinne von Abschnitt 1.3.3 Testzertifikate auf Signaturkarten zur Verfügung.

Die Dienstezertifikate der Testsysteme sind am Namensschema des Common Name (CN) der ausstellenden CA-Zertifikate erkennbar:

EDST-Test-BA-QC-<Bezeichner>-CA-<lfd Nummer>:PN

<Bezeichner> ist ein eindeutiger Namensbestandteil, der die Nutzung der CA andeuten soll. Die laufende Nummer wird für jeden Namen beginnend mit „1“ fortlaufend ganzzahlig geführt. Abschließend erfolgt die Kennzeichnung des CN als Pseudonym gemäß Common PKI [COMPKI].

Der Präfix „EDST-Test-BA-QC“ wird verwendet, um durch den Namen den nicht qualifizierten Charakter des entsprechenden Dienstes hervorzuheben.

Beispiel:

CN=EDST-Test-BA-QC-Signatur-CA-5:PN

9.17.3 Menschen mit Behinderung

Der VDA der BA beachtet die gesetzlichen Anforderungen zur Barrierefreiheit, insbesondere das Behindertengleichstellungsgesetz und die barrierefreie Informationstechnikverordnung.

Abbildungsverzeichnis

Abbildung 1 - qualifizierte Zertifikate in der Legacy-Hierarchie 9
Abbildung 2 - nicht qualifizierte Zertifikate in der Zertifizierungshierarchie 11

Tabellenverzeichnis

Tabelle 1 - Veröffentlichte Informationen 15
Tabelle 2 - Zuordnung der Sperrberechtigungen zu den Sperrmöglichkeiten 27
Tabelle 3 - Zulässige Erweiterungen der OCSP-Anfragen 46
Tabelle 4 - Erweiterungen der OCSP-Antworten 46

Referenzen

Bezeichner	Dokument
[RFC5280]	RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
[eIDAS]	VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[ETSI-TSP]	ETSI TS 101 861: Time stamping profile, European Telecommunications Standards Institute, Version 1.2.1, März 2003
[ETSI-POLQ]	ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. Version 2.1.1, Februar 2016
[ETSI-QCST]	ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements V2.1.1, Februar 2016
[QCP-n-qscd]	Certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; OID 0.4.0.194112.1.2 Definiert in [ETSI-POLQ]
[RFC3647]	RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, IETF Network Working Group, November 2003
[RFC2560]	RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP, IETF Network Working Group, Juni 1999
[RFC2251]	RFC 2251: Lightweight Directory Access Protocol (v3), IETF Network Working Group, Dezember 1997
[RFC3161]	RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), IETF Network Working Group, August 2001
[COMPKI]	Common PKI Specifications for Interoperable PKI Applications from T7 and Teletrust V2.0, January20th, 2009, http://www.t7ev.org/common-pki.html
[ISISMTT1]	Common ISIS-MTT Specifications for Interoperable PKI Applications - Core Parts, T7 e. V. i. G. and TeleTrusT e. V., Version 1.1, März 2004
[ISISMTTb]	Common ISIS-MTT Specifications for Interoperable PKI Applications - Optional Profile: SigG-Profile, T7 e. V. i. G. and TeleTrusT e. V., Version 1.1, März 2004
[X509]	ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, International Telecommunication Union, August 2005 (äquivalent zu ISO/IEC 9594-8)
[FIPS140]	FIPS PUB 140-1: Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), Januar 1994
[PKCS1]	PKCS#1: RSA Cryptography Standard, RSA Laboratories, Version 2.1, Juni 2002
[SÜG]	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz – SÜG) vom 20. April 1994 (BGBl. I S. 867), zuletzt geändert durch Art. 20 V v. 19.06.2020 I 1328

Bezeichner	Dokument
[VDG]	Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist In Kraft getreten am 29.7.2017.
[VDV]	Vertrauensdiensteverordnung vom 15. Februar 2019 BGBl. I 2019 S. 114 ausgegeben am 27. Februar 2019. In Kraft getreten am 28.2.2019.

Definitionen und Abkürzungen

Begriff	Erläuterung
Aktivierungsdaten	Vertrauliche Daten, mit denen sich ein legitimierter Nutzer eines privaten Schlüssels gegenüber dem System, das den Schlüssel speichert, (z. B. einer Chipkarte) authentisiert und somit den Schlüssel aktiviert. Üblicherweise werden PINs und Passwörter als Aktivierungsdaten verwendet.
ARL	Authority Revocation List – Sperrliste für CA-Zertifikate
ASCII	American Standard Code for Information Interchange – Standard für einen Zeichensatz
ASN.1	Abstract Syntax Notation - Beschreibungssprache für Daten, wird z. B. von X.509 verwendet
Asymmetrische Kryptoverfahren	Kryptografische Verfahren, die auf zwei verschiedenen Schlüsseln basieren, wobei einer öffentlich und einer privat (geheim) ist. Dadurch ist es möglich, dass jemand mit dem öffentlichen Schlüssel eine Nachricht verschlüsselt, die nur der Besitzer des geheimen Schlüssels wieder entschlüsseln kann. Damit ist das Problem des Austausches und des Verteilens von geheimen symmetrischen Schlüsseln beseitigt, und es sind Verfahren wie die digitale Signatur möglich.
Authentisierung, Authentifizierung	Vorgang des Nachweises der Authentizität durch kryptografische Verfahren. Durch ein festgelegtes Verfahren wird festgestellt, ob jemand wirklich derjenige ist, der er vorgibt zu sein, bzw. dass die Daten wirklich von einer bestimmten Person stammen. Authentisierung bezeichnet dabei den Nachweis, Authentifizierung die Prüfung dieses Nachweises.
Authentisierungszertifikat	Zertifikat zu einem Schlüsselpaar (z.B. auf einer digitalen Dienstkarte oder Gästekarte), mit dem eine sichere Authentisierung (z. B. für einen Smartcard-Logon oder an einem Web-Portal) durchgeführt werden kann.
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. Die BNetzA ist nach dem [VDG] die zuständige Aufsichtsbehörde.
Certification Authority (CA)	Englischer Begriff für eine Zertifizierungsinstanz
Certificate Policy (CP)	Gesamtheit der Regeln und Vorgaben, die die Anwendbarkeit eines Zertifikatstyps festlegen. Auf Deutsch etwa „Zertifizierungsrichtlinie“
Certification Practice Statement (CPS)	Darlegung der Praktiken, die ein Zertifizierungsdienst bei der Ausgabe der Zertifikate anwendet.
Certificate Revocation List (CRL)	Certificate Revocation List - englischer Begriff für Zertifikats-Sperrliste.
Common Criteria (CC)	Internationaler Standard zur Bewertung der Informationssicherheit von Produkten und Systemen. CC unterscheidet verschiedene Evaluation Assurance Levels (EAL), die festlegen, was und wie geprüft wird. Die Prüfung erfolgt immer gegen die Sicherheitsvorgaben oder ein Schutzprofil (Protection Profile).
DCF77	Von der Physikalisch-Technische Bundesanstalt auf 77,5 kHz ausgestrahltes Funksignal, das in Deutschland die „gesetzliche Zeit“ verbreitet.

Begriff	Erläuterung
Delta-CRL	Inkrementelle Sperrliste, d. h. Sperrliste, die nur jene Sperrinformationen enthält, die sich seit der Veröffentlichung der letzten vollständigen Sperrliste geändert haben.
digitale Dienstkarte (dDk)	Als Chipkarte realisierter Ausweis für interne Mitarbeiter der BA. Die dDk enthält Schlüsselpaare zur Erzeugung von Signaturen, zur Authentisierung und zur Verschlüsselung. Die dDken sind sichere Signaturerstellungs-einheiten.
digitale Signatur	Mit asymmetrischen Kryptoverfahren berechnete Daten, die mit anderen elektronischen Daten logisch verknüpft sind, und mit denen sich deren Authentizität und Integrität prüfen lassen. Die Sicherheit einer digitalen Signatur hängt dabei von den verwendeten Parametern des Kryptoverfahrens, der Geheimhaltung des privaten Schlüssels und der Zuordnung des öffentlichen Schlüssels zum Signator (z. B. durch ein Zertifikat) ab.
DistinguishedName (DN)	Namensform nach X.501. Ein DN besteht aus verschiedenen Attributen und entsprechenden Werten und soll eine Entität eindeutig kennzeichnen. Häufig genutzte Attribute sind CommonName (cn), Organization (o) und Country (c).
DNS-Name	Eindeutiger Name eines Systems, über das dieses in einem Netzwerk adressiert werden kann
Elektronische Signatur	Daten, die mit anderen elektronischen Daten logisch verknüpft sind, und mit denen sich deren Authentizität und Integrität prüfen lassen. D.h., mittels einer elektronischen Signatur kann sowohl die Unverfälschtheit einer Nachricht als auch der Unterzeichner eines elektronischen Dokumentes verifiziert werden. Die sicherste bekannte Ausprägung einer elektronischen Signatur ist die qualifizierte digitale Signatur.
Gästekarte	Als Smartcard realisierter Ausweis für externe Mitarbeiter der BA. Die Gästekarte enthält Schlüsselpaare zur Authentisierung und zur Verschlüsselung.
Hardware Sicherheitsmodul (HSM)	Gerät zur sicheren Speicherung und Anwendung kryptographischer Schlüssel. Im Unterschied zu Smartcards besitzen HSMs meist eine eigene Stromversorgung und implementieren oft aufwendige Sicherheitsmechanismen wie ein sicheres Key Backup von Schlüsseln, die Protokollierung sicherheitsrelevanter Ereignisse oder ein rollenbasiertes Zugriffskonzept.
HTTP	Hypertext Transfer Protocol – besonders im Internet verbreitetes Kommunikationsprotokoll.
Kartenausgeber	Rolle im VDA der BA, der u.a. die dDk oder Gästekarte an die Mitarbeiter ausgibt.
Karteninhaber	Person, für den eine dDk oder Gästekarte ausgestellt wurde.
Kartenpersonalisierung	Dienst innerhalb des VDA der BA, der die dDk oder Gästekarte personalisiert.
LDAP	Lightweight Directory Access Protocol – von der IETF standardisiertes Protokoll zum Zugriff auf Verzeichnisse.
Local Registration Authority (LRA)	In den Dienststellen der BA eingerichtete lokale Registrierungsstellen. Diese sind u.a. für die Ausgabe der Mitarbeiterzertifikate zuständig.

Begriff	Erläuterung
= Lokale Registrierungsstelle	
Mandanten-Signaturkarte	Signaturkarten, die an Mitarbeiter des Mandanten ausgegeben werden. Sie enthalten ein Schlüsselpaar sowie ein zugehöriges Zertifikat (Signaturschlüsselzertifikat) für die Erzeugung bzw. Verifizierung qualifizierter elektronischer Signaturen.
Mandanten-Zertifikat	Qualifiziertes Zertifikat auf der Mandanten-Signaturkarte
Massensignatur	Eine Massensignatur beschreibt hier eine Betriebsart von Chipkarten mit einmaliger PIN-Eingabe mehrere Signaturen durchzuführen. Eine erneute PIN-Eingabe wird erst nach Beendigung der logischen Verbindung zwischen Karte und System notwendig. Massensignaturen werden in speziell dafür vorgesehenen Anwendungen durch Massensignaturkarten durchgeführt.
Massensignaturkarte (MSK)	Die Massensignaturkarte erlaubt die mehrfache qualifizierte Signatur nach Eingabe der Signatur-PIN. Die MSK darf nur in geschützten Umgebungen eingesetzt werden.
Mitarbeiterzertifikat	Oberbegriff für das auf der dDk oder Gästekarte enthaltene qualifizierte Zertifikat, Authentisierungszertifikat oder Verschlüsselungszertifikat.
Object Identifier (OID)	Weltweit eindeutiger, hierarchisch ausgebauter, numerischer Bezeichner
OCSP	Online Certificate Status Protocol – Von der IETF standardisiertes Protokoll zur Online-Abfrage von Statusinformationen von Zertifikaten
OCSP-Responder	Server, der einen OCSP-Verzeichnisdienst implementiert
OCSP-Verzeichnisdienst	Verzeichnisdienst, der Zertifikate und ihren aktuellen Sperrstatus über das OCSP-Protokoll bereitstellt
Öffentlicher Schlüssel	Nicht-geheimer Teil eines Schlüsselpaares bei asymmetrischen Schlüsselpaaren
OID	Object Identifier
Personalisierung	Vorgang der Zuordnung einer Karte zu einer Person. Dies kann einerseits durch die physikalische Personalisierung (z. B. Hochprägung, Lasergravur) oder auch durch die elektrische Personalisierung (d. h. Laden der personenbezogenen Daten in den Speicher der Chipkarte) geschehen.
PIN	Personal Identification Number - Geheimzahl zur Authentisierung eines Individuums z. B. gegenüber einer Chipkarte
PKI	Public Key-Infrastruktur - technisches Umfeld für den Einsatz asymmetrischer Kryptoverfahren. Eine PKI basiert üblicherweise auf Zertifikaten und einer Zertifizierungshierarchie. Wichtige Komponenten einer PKI sind daher die Zertifizierungsinstanzen, Registrierungsinstanzen und Verzeichnisdienste. Darüber hinaus umfasst die PKI aber auch die Teilnehmer (Anwender), dezentrale Komponenten wie z. B. Client-Komponenten zur Speicherung und Anwendung der Schlüssel und Zertifikate sowie umfassende technische und organisatorische Prozesse.
Privater Schlüssel	Geheimer Teil eines Schlüsselpaares bei asymmetrischen Schlüsselpaaren

Begriff	Erläuterung
PSE	Personal Security Environment – Speicher für kryptographische Schlüssel. Ein PSE kann als Hardware (z.B. Smartcard) oder als verschlüsselte Datei (Soft-PSE) realisiert sein.
PUK	PIN Unblocking Key - Code zur Re-Aktivierung einer gesperrten PIN, dabei wird der Fehlbedienungszähler wieder auf 0 gesetzt.
QSCD	Qualified Signature Creation Device - eine qualifizierte elektronische Signaturerstellungseinheit im Sinne der [eIDAS].
Registrar (LRA-Registrar)	Rolle im VDA der BA, der die Registrierung der Mitarbeiter durchführt.
Registrierungsinstanz (engl. Registration Authority, RA)	Stelle eines Zertifizierungsdienstes, die die Anträge zur Ausstellung oder Sperrung von Zertifikaten erfasst und die Antragsteller identifiziert werden.
RFC	Request for Comment - Dokumententyp der Internet Engineering Task Force (IETF), in der diese Standards vorschlägt und veröffentlicht
RSA	Asymmetrisches Kryptoverfahren für Verschlüsselung und digitale Signatur, benannt nach Rivest, Shamir, Adleman
SGB	Sozialgesetzbuch
SHA-1	Vom US-amerikanischen Standardisierungsinstitut normierte Hashfunktion mit 160 Bit langen Ausgabewerten.
SigG-Profile	Bezeichnung des Part 9 der Spezifikation [COMPKI]. Der Terminus SigG ist fester Bestandteil des Dokumentnamens. SigG (Signaturgesetz) ist seit dem 29.07.2017 außer Kraft.
Smartcard	Einzelsignaturkarte, MSK, Gästekarte werden unter dem Begriff Smartcard zusammengefasst
Sperrliste	Liste, in der ein Anbieter eines Zertifizierungsdienstes die Sperrinformation der von ihm ausgestellten und noch nicht abgelaufenen Zertifikate veröffentlicht.
Sperroperator (LRA-Sperroperator)	Rolle im VDA der BA, der die Sperrung von Mitarbeiterzertifikaten in einer LRA durchführt.
Sperrstatus	Status eines Zertifikates bzgl. Sperrung
TS	Technical Standard - Bezeichnung für technische Standards bei ETSI
TSP	Time Stamp Protokoll - Protokoll zur Anforderung und Ausgabe eines Zeitstempels.
VDA	Vertrauensdiensteanbieter (hier: der Bundesagentur für Arbeit) gemäß [eIDAS]
Verschlüsselungszertifikat	Zertifikat zu einem Schlüsselpaar (z. B. auf einer digitalen Dienstkarte oder Gästekarte), dass eine verschlüsselte Kommunikation ermöglicht
Verzeichnisdienst	In einer PKI, der Dienst über den Zertifikate oder Informationen zu Zertifikaten (z. B. Sperrinformationen) oder der PKI abgerufen werden können.
Wurzel-CA	Oberste Zertifizierungsinstanz einer Zertifizierungshierarchie. Das Zertifikat der Wurzel-CA wird von ihr selbst signiert und muss den Teilnehmern der PKI auf eine vertrauenswürdige Weise (z. B. offline) zugänglich gemacht werden.

Begriff	Erläuterung
X.509	Von der ITU definierter Standard, der unter anderem die heute überwiegend verwendeten Datenformate für Zertifikate und Sperrlisten definiert.
Zeitstempel	Elektronische Bestätigung, dass gewisse Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Ein Zeitstempel enthält üblicherweise eine digitale Signatur über die mit der aktuellen Zeitinformation versehenen vorgelegten Daten.
Zeitstempeldienst	Dienst, der Zeitstempel ausstellt
Zertifikat	Eine elektronische Bescheinigung, mit der ein öffentlicher Schlüssel dem Zertifikatsinhaber zugeordnet wird und dessen Identität bestätigt wird. Ein Zertifikat enthält Angaben zum Inhaber, zum Aussteller und zur Nutzung des Zertifikates sowie den öffentlichen Schlüssel des Inhabers. Außerdem enthält das Zertifikat eine digitale Signatur, welche die Authentizität und Integrität der im Zertifikat enthaltenen Daten sicherstellt.
Zertifikatsinhaber/Zertifikatsnehmer	Entität, für die das Zertifikat ausgestellt wird. Der Zertifikatsinhaber ist im Zertifikat als "CN" eingetragen.
Zertifizierungsdienst	Dienst, der Zertifikate ausstellt oder andere Dienstleistungen im Zusammenhang mit Zertifikaten erbringt, beispielsweise Verzeichnisdienste, Zeitstempeldienste, Schlüsselhinterlegungsdienste.
Zertifizierungshierarchie	Hierarchisch geordnete Struktur bestehend aus den Zertifizierungsinstanzen und den von ihnen ausgestellten Zertifikaten. Auf der untersten Hierarchie-Ebene stehen die Zertifikate der Endanwender. Unter jeder Zertifizierungsinstanz hängen an entsprechenden Ästen die Entitäten, für die sie Zertifikate ausstellen. Die oberste(n) Zertifizierungsinstanz(en) nennt man Wurzel-CA(s).
Zertifizierungsinstanz	Logische Einheit eines Zertifizierungsdienstes zur Ausstellung (Signierung) von Zertifikaten. Jeder Zertifizierungsinstanz sind jeweils ein oder mehrere Schlüsselpaare zur Signierung der Zertifikate zugeordnet.
Zertifizierungsstelle	Zertifizierungsdienstleister, der Zertifikate ausstellt