Zertifizierungsrichtlinie / Certificate Policy

oesterreich.gv.at

Dokumentenverantwortliche: BMDW / BRZ GmbH
Version: 1.0
Datum: 11.02.2019

Versionshinweise

Version	Datum	Autor/in	Änderung
1.0	*11.02.2019*	*BMDW / BRZ GmbH*	*Initiale Version*

BRZ

Inhaltsverzeichnis

1. Einleitung 7

1.1 Überblick 7
1.2 Dokumentenname sowie Identifikation 8
1.3 Teilnehmende 8
1.3.1 Zertifizierungsstelle 8
1.3.2 Registrierungsstellen 9
1.3.3 Zertifikatsinhaber und Antragsteller (Subscribers) 10
1.3.4 Zertifikatsprüfer (Relying Parties) 10
1.3.5 Weitere Teilnehmende 10
1.4 Anwendungsbereich 11
1.4.1 Vorgesehene Anwendung von Zertifikaten 11
1.4.2 Nicht vorgesehene Anwendung von Zertifikaten 11
1.5 Verwaltung dieses Dokuments 12
1.5.1 Organisation die das Dokument administriert 12
1.5.2 Ansprechpartner und Kontaktstelle 12
1.6 Definitionen und Abkürzungen 12
1.6.1 Definitionen 13
1.6.2 Abkürzungen 15
1.7 Referenzdokumente 17

2. Veröffentlichungen und Verzeichnisdienst 20

2.1 Verzeichnisdienst 20
2.2 Veröffentlichungen 20
2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz) 21
2.4 Zugriffskontrolle zu den Verzeichnisdiensten 21

3. Identifizierung und Authentifizierung 23

3.1 Namensgebung 23
3.1.1 Namenstypen / Namensform 23
3.1.2 Aussagekraft von Namen 23
3.1.3 Anonymität und Pseudonyme 23
3.1.4 Regeln für die Interpretation der verschiedenen Namensformen 24
3.1.5 Eindeutigkeit der Namen 24
3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen 24
3.2 Identitätsprüfung bei Neuantrag 24
3.2.1 Nachweis des Besitzes eines privaten Schlüssels 24
3.2.2 Authentifizierung einer Organisation 25
3.2.3 Authentifizierung von natürlichen Personen 25
3.2.4 Nicht überprüfte Teilnehmerangaben 25
3.2.5 Überprüfung der Berechtigung 25
3.2.6 Kriterien für Zusammenarbeit 25
3.3 Identifizierung und Authentifizierung bei Zertifikatserneuerung mit Schlüsselwechsel 26
3.4 Identifizierung und Authentifizierung bei Widerruf und Sperranträgen 26

4. Anforderungen an den Lebenszyklus des Zertifikats 29

4.1 Beantragung eines Zertifikats 29

4.1.1 Wer kann ein Zertifikat beantragen 29
4.1.2 Verfahren und Verantwortung 30
4.2 Bearbeitung des Zertifikatsantrags 30
4.2.1 Durchführung der Identifizierung und Authentifizierung 30
4.2.2 Annahme oder Ablehnung des Zertifikatsantrags 30
4.2.3 Bearbeitungsdauer bei Zertifikatsanträgen 30
4.3 Erstellung des Zertifikats 31
4.3.1 Aufgaben der Zertifizierungsstelle 31
4.3.2 Benachrichtigung des Zertifikatsinhabers 31
4.4 Annahme des Zertifikats 31
4.4.1 Annahmeverfahren 31
4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle 32
4.4.3 Benachrichtigung weiterer Instanzen 32
4.5 Verwendung der Schlüssel und des Zertifikats 32
4.5.1 Verwendung der Schlüssel und des Zertifikats durch den Zertifikatsinhaber 33
4.5.2 Verwendung des Zertifikats durch Dritte 34
4.6 Zertifikatserneuerung (Re-Zertifizierung) 34
4.7 Schlüssel- und Zertifikatserneuerung (Re-key) 34
4.8 Zertifikatsmodifizierung 34
4.9 Widerruf und Sperrung (Suspendierung) von Zertifikaten 34
4.9.1 Widerrufsgründe 34
4.9.2 Wer kann einen Widerruf beantragen 35
4.9.3 Verfahren des Widerrufs 36
4.9.4 Fristen für den Zertifikatsinhaber 37
4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle 37
Die OESTERREICH.GV.AT-PKI führt den beantragten Widerruf eines betroffenen Zertifikats unverzüglich nach Eingang des Antrags durch. Der Widerruf wird so rasch wie möglich durchgeführt und ist innerhalb innerhalb eines Werktages wirksam. 37
4.9.6 Anforderungen zur Prüfung des Zertifikatsstatus durch eine Relying Party 37
4.9.7 Häufigkeit der Erstellung der CRL 37
4.9.8 Maximale Latenzzeit für Veröffentlichung von CRLs 37
4.9.9 Verfügbarkeit von Online-Statusabfragen (OCSP) 37
4.9.10 Anforderungen hinsichtlich der Online-Überprüfung 37
4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung 38
4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln 38
4.9.13 Gründe für eine Sperrung 38
4.9.14 Wer kann eine Sperrung beantragen 38
4.9.15 Verfahren der Sperrung 38
4.9.16 Maximale Dauer einer Sperrung 38
4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP) 38
4.10.1 Operative Merkmale 39
4.10.2 Verfügbarkeit des Dienstes 39
4.10.3 Optionale Merkmale 39
4.11 Beendigung des Vertragsverhältnisses 39

4.12 Schlüsselhinterlegung und –wiederherstellung 39
5. Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen 40
5.1 Infrastrukturelle Sicherheitsmaßnahmen 40
5.2 Organisatorische Sicherheitsmaßnahmen 40
5.3 Personelle Sicherheitsmaßnahmen 41
5.4 Protokollierung sicherheitskritischer Ereignisse 41
5.5 Archivierung 41
5.6 Schlüsselwechsel der Zertifizierungsstelle 41
5.7 Kompromittierung und Wiederherstellung 41
5.8 Einstellung des Betriebes 41
6. Technische Sicherheitsmaßnahmen 43
6.1 Generierung und Installation von Schlüsselpaaren 43
6.2 Schutz privater Schlüssel und Einsatz kryptografischer Module 43
6.3 Weitere Aspekte der Verwaltung von Schlüsselpaaren 43
6.4 Aktivierungsdaten 43
6.5 Sicherheitsmaßnahmen für Computer 44
6.6 Sicherheitsmaßnahmen für den Software-Lebenszyklus 44
6.7 Sicherheitsmaßnahmen für das Netzwerk 44
6.8 Zeitstempel 44
7. Zertifikatsprofil, Sperrlisten (CRL) und Online Statusabfragen (OCSP) 45
7.1 Zertifikatsprofil 45
7.1.1 Stamm 1 – SHA-384/ECDSA 46
7.2 Sperrlistenprofil (CRL) 47
7.2.1 Stamm 1 – SHA-384/ECDSA 47
7.3 OCSP-Request/Response Profil 48
8. Konformitätsprüfung (Compliance Audit, Assessments) 49
9. Andere geschäftliche und rechtliche Angelegenheiten 49
9.1 Gebühren 49
9.1.1 Gebühren für die Ausstellung, die Erneuerung oder den Widerruf von Zertifikaten 50
9.1.2 Gebühren für den Abruf bzw. den Zugriff auf Zertifikate 50
9.1.3 Gebühren für den Abruf bzw. den Zugriff auf Sperrlisten oder Statusinformationsdienste 50
9.1.4 Gebühren für weitere Dienstleistungen 50
9.2 Finanzielle Verantwortung 50
9.3 Vertraulichkeit von Geschäftsinformationen 50
9.4 Schutz personenbezogener Daten 50
9.5 Urheberrechte 51
9.6 Verpflichtungen 51
9.7 Gewährleistung 51
9.8 Haftungsbeschränkung 51
9.9 Haftungsfreistellung 51
9.10 Inkrafttreten und Aufhebung 51
9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmenden 52
9.12 Änderungen der Richtlinie 52

9.13 Konfliktbeilegung 52
9.14 Geltendes Recht 52
9.15 Konformität mit geltendem Recht 52
9.16 Allgemeine Bestimmungen 52
9.17 Andere Regelungen 52

1. Einleitung

1.1 Überblick

Die PKI[1] der Plattform OESTERREICH.GV.AT[2] ist ein geschlossenes System[3,4] und wird durch die Bundesrechenzentrum GmbH[5] (BRZ, BRZ GmbH) im eigenen, geschützten Rechenzentrum (Trustcenter, TC) redundant an zwei Standorten betrieben.

Das vorliegende Dokument repräsentiert die Zertifizierungsrichtlinie (d.h. englisch auch Certificate Policy[6] – CP) für die im BRZ betriebene PKI bzw. der Zertifizierungsstelle von OESTERREICH.GV.AT. Die Grundlage für die PKI ist die von der BRZ GmbH betriebene Plattform BRZ Trustcenter PKI. Auf deren Basis sind die prozeduralen sowie die operationellen Anforderungen an das Lifecycle-Management der OESTERREICH.GV.AT-PKI definiert.

Die BRZ GmbH fordert, dass sich Entitäten an diese CP halten, wenn diese digitalen Zertifikate innerhalb der PKI-Hierarchie von OESTERREICH.GV.AT (1) beantragen, (2) autorisieren, (3) erzeugen, (4) ausstellen, (5) ausliefern, (6) verwenden, (7) verwalten bzw. (8) widerrufen.

Die Gliederung dieser CP basiert auf dem anerkannten, internationalen Standard für die Erstellung von Zertifizierungsrichtlinien nach RFC[7] 3647[8] der Internet Engineering Task Force (IETF).

Policy Mapping wird nicht durchgeführt. Das bedeutet die Zuordnung von fremden Zertifizierungsrichtlinien (d.h.: die Anerkennung von CP oder CPS welche sich nicht im Einflussbereich von OESTERREICH.GV.AT befinden) wird nicht angewendet.

Im Bedarfsfall ist diese OESTERREICH.GV.AT-PKI CP anzupassen.

---

1 PKI – Public Key Infrastructure

2 Abrufbar: https://www.oesterreich.gv.at/

3 Anmerkung: Ein geschlossenes System im Sinne von Artikel 2 (2) eIDAS [eIDAS]

4 eIDAS – electronic IDentification, Authentication and trust Services

5 UID-Nummer: ATU41542700

6 Anmerkung: Die Bezeichnung wurde nach dem IETF-Standard RFC 3647 gewählt

7 RFC – Request for Comments

8 RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

1.2 Dokumentenname sowie Identifikation

Name des Dokuments	*Zertifizierungsrichtlinie / Certificate Policy für die PKI von oesterreich.gv.at*
Object Identifier OID[9,10]	1.2.40.0.10.1.1.13 (Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW).1
Version	1.0
Datum	11.02.2019

Die oben festgehaltene OID 1.2.40.0.10.1.1.13 und der damit verbundene, symbolische Bezeichner *„Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW)“* sind auf das BMDW registriert.

1.3 Teilnehmende

Dieser Abschnitt behandelt die PKI Beteiligten (d.h. Teilnehmende) für die Plattform OESTERREICH.GV.AT. Umfasst sind auch die Aufgaben der Teilnehmenden. Weitere Details sind in den folgenden Unterabschnitten verfügbar.

1.3.1 Zertifizierungsstelle

Der Begriff Zertifizierungsstelle (Certification Authority, CA) bezieht sich auf eine Einheit/Entität oder eine Organisation, welche für das (1) autorisieren, (2) erzeugen, (3) ausstellen, (4) ausliefern, (5) verwalten und/oder (6) widerrufen im Lebenszyklus eines Zertifikats verantwortlich ist. Dies gilt darüber hinaus auch für StammCAs (RootCA) und nachgeordnete AusstellerCAs (SubCA).

Die Ausstellung der kryptografisch geschützten Zertifikate erfolgt durch die jeweilige Zertifizierungsstelle im Trustcenter des BRZ.

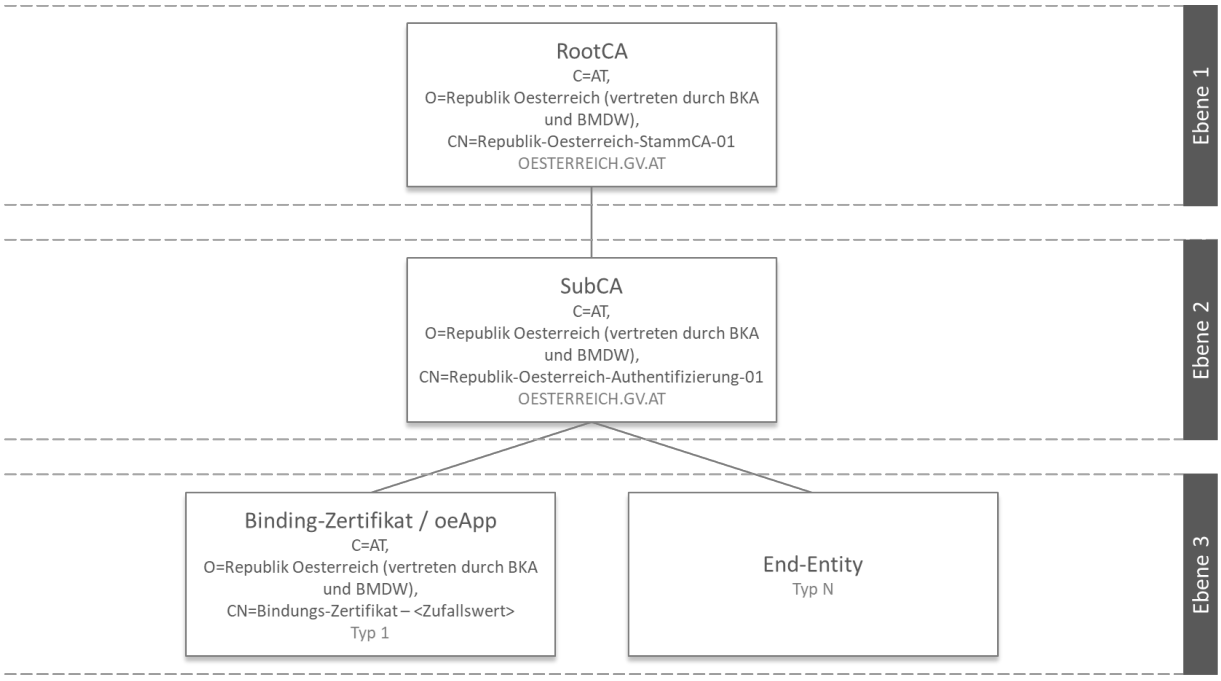
Eine 3-stufige Zertifikatshierarchie für die PKI der Plattform OESTERREICH.GV.AT ist umgesetzt. Die oberste Stufe (Ebene 1) bildet die RootCA. Auf der zweiten Stufe (Ebene 2) wird von der RootCA eine SubCA ausgestellt. Diese erstellt die Zertifikate für die End-Entities (EE) (Binding-Zertifikat für die oeAPP[11] in der Ebene 3).

Die nachfolgende graphische Darstellung veranschaulicht die installierte Zertifikatshierarchie.

[9] OID – Object Identifier

[10] Anmerkung: Nach ASN.1 (Abstract Syntax Notation One)

[11] oeApp – ein über die Plattformen: (1) Apple® App Store® und (2) Google Play™ (Store) verfügbares Programm (App).



C – Land (Country)
O – Organisation (Organization)
CN – Gebräuchlicher Name (Common name)

AT – Ländercode für Österreich nach ISO 3166-1 alpha-2 [ISO 3166]
BKA – Bundeskanzleramt der Republik Österreich
BMDW – Bundesministerium für Digitalisierung und Wirtschaftsstandort
CA – Certification Authority

Abbildung 1: Graphische Darstellung der Zertifikatshierarchie für die PKI der Plattform OESTERREICH.GV.AT

Die BRZ GmbH stellt das RootCA-Zertifikat sowie das darunterliegende SubCA-Zertifikat aus. Bei den ausgestellten Zertifikaten in dieser Zertifikatshierarchie handelt es sich nicht um qualifizierte Endanwenderzertifikate.

Auch behält sich die BRZ GmbH vor in Abstimmung mit dem Auftraggeber (BMDW), weitere SubCA-Zertifikate (d.h. weitere CAs zur Ausstellung von End-Entity-Zertifikaten) in Abhängigkeit des Bedarfs für besondere Nutzungsszenarien auszustellen.

1.3.2 Registrierungsstellen

Die Registrierung erfolgt durch die Registrierungsstelle (Auto Enrollment Registration Authority, AERA) des Trustcenters in der BRZ GmbH und wird nicht an externe Services delegiert.

Die Authentifizierung von Teilnehmenden am Binding-Service für die Durchführung der Registrierung mit der AERA erfolgt auf die folgenden 2 Arten:

- Handy-Signatur (national)
- eIDAS[12] [eIDAS] (EU[13])

[12] eIDAS –electronic IDentification, Authentication and trust Services

[13] EU – Europäische Union

1.3.3 Zertifikatsinhaber und Antragsteller (Subscribers)

Bei einem Zertifikatsinhaber und/oder Antragsteller (Subscriber) handelt es sich um die End-Entity (siehe Abbildung 1), deren (1) Name oder (2) Identifier im Zertifikat enthalten ist und welche den eigenen Schlüssel und das damit verbundene Zertifikat nach dieser CP verwendet. Daher ist der Subscriber jene Hauptanwender-Entität, auf die das Zertifikat ausgestellt ist.

Der Zertifikatsinhaber (Subscriber):

- wird während der durchzuführenden Registrierung von der CA authentifiziert
- wird durch das erzeugte und ausgestellte Zertifikat identifiziert
- besitzt den im Zertifikat enthaltenen öffentlichen Schlüssel und ist dessen Eigentümer
- ist Besitzer und Eigentümer des privaten Schlüssels, welcher kryptografisch mit dem im Zertifikat gespeicherten öffentlichen Schlüssel verknüpft ist

Die Verpflichtungen der Zertifikatsinhaber (Subscriber) innerhalb der definierten CA-Hierarchie (siehe Abbildung 1) umfassen:

- geeignete Maßnahmen zu ergreifen, um den privaten Schlüssel vor Kompromittierung zu schützen
- unverzügliche Meldung über Verlust, Kompromittierung oder Beeinträchtigung privater Schlüssel oder nicht gegebener Korrektheit der gespeicherten Zertifikatinformationen zu machen

1.3.4 Zertifikatsprüfer (Relying Parties)

Bei Zertifikatsprüfern (Relying Parties) handelt es sich um Entitäten, welche der PKI vertrauen und damit den im Zertifikat gespeicherten Daten und deren Validität. Das bedeutet, es handelt sich um sogenannte *„Vertrauende Personen“* bzw. *„Vertrauende Systeme“* (z.B.: zentrale technische Komponenten von OESTERREICH.GV.AT).

Vertrauende Systeme (Technische Komponenten und Zertifikatsprüfer) sind:

- Identity Provider von OESTERREICH.GV.AT
- Service Provider von OESTERREICH.GV.AT

1.3.5 Weitere Teilnehmende

Bei sonstigen Teilnehmenden handelt es sich um die Empfänger bzw. Nutzer eines ausgestellten Zertifikats. Diese vertrauen dabei auf die Angemessenheit sowie die Korrektheit und die Zuverlässigkeit der im Zertifikat angegebenen Daten (z.B.: zur Überprüfung der Gültigkeit).

Darüber hinaus führt die BRZ GmbH keine Auslagerung von Funktionen und/oder Aufgaben an externe Organisationen durch. Das bedeutet, es gibt keine *„Delegated Third Party“* für den (1) Betrieb der CA-Infrastruktur, die (2) Prüfung, (3) Genehmigung, (4) Bearbeitung oder die (5) Verwaltung von Zertifikaten.

Aktuell sind alle Komponenten bzw. teilnehmenden Systeme im Bereich der OESTERREICH.GV.AT-PKI, in der Hoheit der BRZ GmbH.

Weitere BRZ-interne bzw. -externe Teilnehmer sind:

- Key Manager (Schlüsselträger) (intern)
- Sicherheitsadministratoren (intern)
- Validierungsstelle (intern)
- Informationsdienst (intern)
- Revisoren bzw. Auditoren (intern oder extern)

1.4 Anwendungsbereich

Die vorgesehenen Anwendungsmöglichkeiten der ausgestellten Zertifikate und der kryptografisch zugeordneten Schlüsselpaare sind in diesem Abschnitt der vorliegenden CP beschrieben.

Zu diesem Zweck hat die Zertifizierungsstelle sowohl Richtlinien als auch technische Einschränkungen definiert, um die geeigneten Verwendungszwecke für ausgestellte Zertifikate festzulegen. Darüber hinaus sind angemessene Kontrollmechanismen[14] installiert, um die Verwendung der ausgestellten Zertifikate für den beabsichtigten Zweck sicherzustellen.

1.4.1 Vorgesehene Anwendung von Zertifikaten

Die Zertifikate werden im Rahmen unterschiedlicher Anwendungen der Plattform OESTERREICH.GV.AT je nach Belegung der Attribute zur Schlüsselnutzung und den definierten Parametern der Zertifizierungsstelle eingesetzt.

Der Zertifikatsinhaber ist dafür verantwortlich, die Zertifikate so zu verwenden, dass deren Nutzung den anwendbaren rechtlichen Rahmenbedingungen entspricht. Insbesondere gilt dies auch für die Einhaltung von anwendbaren Ausfuhr- und/oder Einfuhrbestimmungen.

1.4.2 Nicht vorgesehene Anwendung von Zertifikaten

Die ausgestellten Zertifikate und damit verbundene, kryptografische Schlüssel sind ausschließlich für den unter Abschnitt 1.4.1 beschriebenen Anwendungskontext erlaubt. Darüber hinaus gehende Nutzung ist generell verboten.

Insbesondere sind die ausgestellten Zertifikate und damit verbundene, kryptografische Schlüssel nicht für die Verwendung oder zur Weitergabe vorgesehen, und/oder ausgelegt bzw. zugelassen für:

- die Erstellung qualifizierter elektronischer Signaturen oder solcher Siegel oder solcher Zeitstempel
- die Erstellung fortgeschrittener elektronischer Signaturen oder solcher Siegel oder solcher Zeitstempel
- die Anwendung im Bereich von Steuerungs- und Kontrolleinrichtungen in kritischen Umgebungen
- die Anwendung in Umgebungen, in denen schwerwiegende Schäden bei Menschen möglich sind

[14] Die installierten Kontrollmechanismen sind im Sicherheitskonzept von OESTERREICH.GV.AT und in den Betriebsdokumenten des Betreibers von OESTERREICH.GV.AT definiert.

Darüber hinaus sind die folgenden Anwendungsszenarien verboten:

- die Manipulation eines ausgestellten Zertifikats oder eines assoziierten kryptografischen Schlüssels
- die Nutzung eines ausgestellten Zertifikats für ein Man-in-the-Middle-Szenario (MitM) (z.B.: MitM-Angriff)
- die rechtswidrige Nutzung der Zertifikate
- die Nutzung der Zertifikate für rechtswidrige Handlungen

1.5 Verwaltung dieses Dokuments

1.5.1 Organisation die das Dokument administriert

Die vorliegende CP wird im Auftrag des BMDW[15] von der BRZ GmbH erstellt, herausgegeben und veröffentlicht. Die BRZ GmbH ist für die Pflege, Verwaltung, Organisation, Veröffentlichung und gegebenenfalls den Widerruf dieses Dokuments verantwortlich.

Diese CP ist zwischen dem BMDW und der BRZ GmbH abgestimmt.

Die Endverantwortung für die OESTERREICH.GV.AT-CP liegt beim BMDW als Auftraggeber.

1.5.2 Ansprechpartner und Kontaktstelle

Kontaktstelle für BürgerInnen und organisatorische Angelegenheiten

Serviceline-Telefonnummer	+43 1 71123 88 44 66

Technische Ansprechpartner für die PKI

Service Manager BRZ Trustcenter PKI Bundesrechenzentrum GmbH Hintere Zollamtsstrasse 4 1030 Wien	E-Mail: trustcenter@brz.gv.at

Die technische Verantwortung liegt bei der BRZ GmbH.

Endverantwortung für die Plattform OESTERREICH.GV.AT

Die Endverantwortung als Auftraggeber liegt beim Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW).

1.6 Definitionen und Abkürzungen

In diesem Abschnitt sind für die vorliegende CP relevante Definitionen, Abkürzungen und Akronyme festgelegt, um die Bedeutung dedizierter Fachbegriffe eindeutig festzulegen.

[15] BMDW – Bundesministerium für Digitalisierung und Wirtschaftsstandort

1.6.1 Definitionen

Access Management	Ein Webservice, um den Zugang zur Plattform OESTERREICH.GV.AT und insbesondere den Zugang zum Binding-Service (Binding-Service und User-Store) zu verwalten
Administrator	BenutzerIn mit erweiterten Rechten im Betriebssystem-Bereich oder Datenbank, jedoch ohne PKI-Aufgaben
AERA	Service zur automatischen Registrierung – Auto Enrollment Registration Authority (AERA)
Antragsteller	Eine Entität, die die PKI mittels Antrag auffordert ein Zertifikat auszustellen. Ein Antragsteller wird nach Erteilung des Zertifikats zum Zertifikatsinhaber.
Auftraggeber	Bundesministerium für Digitalisierung und Wirtschaftsstandort Stubenring 1 1010 Wien
Binding-Service	Ein Service • über welches Benutzer Binding-Zertifikate zur Authentifizierung am OESTERREICH.GV.AT-IDP[16] ausstellen lassen können und • für die Verwaltung von Binding-Zertifikaten
Binding-Zertifikate	End-Entity Zertifikate, welche zur Authentifizierung aus der oeApp an OESTERREICH.GV.AT genutzt werden.
BRZ.TC.PKI	Umfasst die Certification Authority (CA) und die Validation Authority (VA) des Trustcenters im BRZ
Certification Authority	Siehe Zertifizierungsstelle
Certificate Policy	Definiert die Entitäten einer PKI, die Rollen sowie deren Verantwortlichkeiten. (Das vorliegende Dokument ist eine CP).
Certification Practice Statement	Beschreibt die Vorgehensweise mit der eine CA digitale Zertifikate ausstellt und wartet. Die Bezeichnung wurde nach dem IETF-Standard RFC 3647 gewählt.
Certification Request Certificate Signing Request	Siehe Zertifikatsantrag
CRL[17] Distribution Service	Das Service bzw. System von dem eine Certificate Revocation List (CRL) heruntergeladen werden kann.
Key-Ceremony	Auditierbarer Prozess zur Verwaltung von kryptografischem Schlüsselmaterial. Alle Arbeitsschritte werden im 4-Augen-Prinzip durchgeführt und protokolliert

[16] IDP – Identity Provider

[17] CRL – Certificate Revocation List

Man-in-the-Middle	Ist eine Angriffsart auf Computer-Systeme wobei der Angreifer zwischen zwei Kommunikationspartnern angesiedelt ist und sowohl Zugang als auch die Kontrolle über den Datenverkehr hat.
OCSP[18] Responder	Ein Online-Service, das OCSP-Responses nach IETF RFC 6960 [RFC 6960] erstellt
oeApp	Eine über die Plattformen: (1) Apple® App Store® und (2) Google Play™ (Store) verfügbare App für die Nutzung der Online-Plattform OESTERREICH.GV.AT
Repository	Ein Verzeichnis oder ein Archiv zur Speicherung und Beschreibung von digitalen Inhalten (z.B.: der Ort, an dem unter anderem das CP gespeichert ist und dort öffentlich abrufbar ist)
RootCA	Siehe *StammCA*
Secure Element	Ein Chip in einem Computer/Gerät als sicherer Speicher um schützenswerte, asymmetrische Schlüsselpaare und PKI Zertifikate zu hinterlegen.
SSL[19]/TLS[20]	Secure Socket Layer/Transport Layer Security [RFC 5246] ist ein Verfahren für die sichere Übertragung von Daten über ein Netzwerk
SSO	Single-Sign-On – nach einmaliger Authentifizierung ist die Nutzung aller verbundenen Services ohne weitere Authentifizierung möglich.
StammCA	Ist die oberste Zertifizierungsstelle, die ihren öffentlichen Schlüssel in einem selbst-signierten Zertifikat, das zur Zertifikatsprüfung als Vertrauensanker dient, publiziert
Trustcenter (TC)	Ist eine unabhängige sowie vertrauenswürdige Institution, welche die Vergabe von Zertifikaten und die Hinterlegung digitaler Schlüssel sowie digitaler Signaturen durchführt. Der Begriff Trustcenter wird daher häufig als Synonym für Zertifizierungsstelle benutzt.
UI	User-Interface, eine Benutzerschnittstelle für die Nutzung bzw. Interaktion zwischen BenutzerIn und Gerät
Validation Authority	Ist ein Überbegriff für *OCSP Responder* und *CRL Distribution Service*

[18] OCSP – Online Certificate Status Protocol

[19] SSL – Secure Sockets Layer

[20] TLS – Transport Layer Security

Vertrauensanker	(engl. Trust Anchor) In den Einstellungen der Software eines Zertifikatsprüfers als vertrauenswürdig markiertes Zertifikat; die Zertifikatsprüfsoftware wird jedes Zertifikat dieser Zertifizierungsstelle sowie in der Hierarchie darunterliegender Zertifizierungsstellen als vertrauenswürdig einstufen
Zertifikatsantrag	(engl. Certification / Certificate Signing Request) bezeichnet sowohl ein Datenformat, das den öffentlichen Schlüssel enthält, für den ein Zertifikat ausgestellt werden soll, als auch den organisatorischen Ablauf zur Beantragung eines Zertifikats
Zertifikatsinhaber	eine Entität, die im Eigentum und im Besitz eines Zertifikats ist nachdem ein Antrag zur Ausstellung eines Zertifikats genehmigt wurde. Zusammenhang zu Antragsteller siehe bitte *„Antragsteller“*
Zertifizierungsdienst	Siehe *Zertifizierungsstelle*
Zertifizierungsdienste-anbieter	Siehe *Zertifizierungsstelle*
Zertifizierungsinstanz	Ist das IT-System, das eine Zertifizierungsstelle betreibt, um Zertifikate auszustellen
Zertifizierungsstelle	(engl. Certification Authority) ist die organisatorische Einheit, die eine Zertifizierungsinstanz betreibt und Zertifikate ausstellt

1.6.2 Abkürzungen

AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation One
BMDW	Bundesministerium für Digitalisierung und Wirtschaftsstandort
BKA	Bundeskanzleramt
BRZ	Bundesrechenzentrum
BRZ GmbH	Bundesrechenzentrum GmbH
CA	Certification Authority (Zertifizierungsstelle)
CA Administrator	Certification-Authority-Administrator
CC	Common Criteria
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement

CR bzw. CSR	Certification Request bzw. Certificate Signing Request
CRL	Certificate Revocation List
DN	Distinguished Name
EAL	Evaluation Assurance Level
ECC	Ellipitic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
eIDAS	electronic IDentification, Authentication and trust Services
eID	elektronischer Identitätsnachweis
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
GmbH	Gesellschaft mit beschränkter Haftung
HSM	Hardware Security Module
HTTPS	Hyper Text Transfer Protocol gesichert mit SSL/TLS
IDP	Identity Provider
IDS	Intrusion Detection System
ISO	International Organization for Standardization
KM	Key Manager
MitM	Man-in-the-Middle
MOA	Module für Online Applikationen
MOA-ID	Module für Online Applikationen – Identifikation
LDAP	Lightweight Directory Access Protocol
O	Organisation
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PKIX	Public Key Infrastruktur X.509
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SAML	Security Assertion Markup Language
SM	Service Manager
SSO	System Security Officer
SSL	Secure Socket Layer
TC	Trustcenter

TLS	Transport Layer Security
UID	Umsatzsteuer-Identifikationsnummer
USV	Unterbrechungsfreie Stromversorgung
VDA	Vertrauensdiensteanbieter

1.7 Referenzdokumente

[AT-SPG]	Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG). https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792. Republik Österreich.
[BRZ ASRL TC]	BRZ Trustcenter – Allgemeine Sicherheitsrichtlinie. V1.1, 01.05.2016. Bundesrechenzentrum GmbH.
[BRZ SRL IT-Services]	Sicherheitsrichtlinie – IT-Services. V3.0, 31.03.2016. Bundesrechenzentrum GmbH.
[CPS]	Ausführungsbestimmungen / Certification Practice Statement – oe.gv.at . V1.0, 11.02.2019. Bundesrechenzentrum GmbH.
[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. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=DE Europäischen Union.
[ENISA]	Algorithms, Key Sizes and Parameters Report – 2013. V1.0, 10.2013. European Union Agency for Network and Information Security.
[ECRYPT]	ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012). 09.2012. European Network of Excellence in Cryptology II.
[ISO 3166]	Codes for the representation of names of countries and their subdivisions – Part 1: Country codes. 11.2013. International Organization for Standardization.

[RFC 822]	Standard for the format of ARPA internet text messages. https://www.ietf.org/rfc/rfc0822. 06.1999. Internet Engineering Task Force.
[RFC 6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. https://tools.ietf.org/html/rfc6960. 06.2013. Internet Engineering Task Force.
[RFC 3629]	UTF-8, a transformation format of ISO 10646. https://tools.ietf.org/html/rfc3629. 11.2003. Internet Engineering Task Force.
[RFC 3647]	Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework. https://tools.ietf.org/html/rfc3647. 11.2003. Internet Engineering Task Force.
[RFC 4514]	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names. https://tools.ietf.org/html/rfc4514. 06.2006. Internet Engineering Task Force.
[RFC 4519]	Lightweight Directory Access Protocol (LDAP): Schema for User Applications. https://tools.ietf.org/html/rfc4519. 06.2006. Internet Engineering Task Force.
[RFC 5246]	The Transport Layer Security (TLS) Protocol Version 1.2. https://tools.ietf.org/html/rfc5246. 08.2008. Internet Engineering Task Force.
[RFC 5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://tools.ietf.org/html/rfc5280. 08.2008. Internet Engineering Task Force.
[RFC 6090]	Fundamental Elliptic Curve Cryptography Algorithms. https://tools.ietf.org/html/rfc6090. 02.2011. Internet Engineering Task Force.

[RFC 8422]	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier. https://tools.ietf.org/html/rfc8422. 08.2018. Internet Engineering Task Force.
[SEC-OEGVAT]	Sicherheitskonzept – OESTERREICH.GV.AT Plattform in der geltenden Fassung. Bundesrechenzentrum GmbH.
[SEC-FACILITY]	Sicherheitsrichtlinie Facility Services V3.0., 31.03.2016 Bundesrechenzentrum GmbH.
[X.500]	Information Technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services. ISO/IEC 9594-1:2005. 2005. International Organization for Standardization.
[X.509]	Information Technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services. ISO/IEC 9594-1:2005. 2005. International Organization for Standardization.
[X.680]	Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation. 10.2008. International Telecommunication Union.

2. Veröffentlichungen und Verzeichnisdienst

Dieser Abschnitt behandelt Repositories, die notwendig sind um die relevanten Informationen zugänglich zu machen. Gleichzeitig erfolgt hier eine Abgrenzung zu nicht öffentlich zugänglichen Dokumentationen.

2.1 Verzeichnisdienst

Zur Prüfung des Zertifikatsstatus und für die öffentliche Bereitstellung von Statusinformationen der ausgegebenen Zertifikate wird ein

- OCSP[21]-Responder[22]

betrieben.

Zugriff auf den Auskunftsdienst, um den Status von Zertifikaten zu überprüfen, ist mit den folgenden Optionen möglich:

- Online Certificate Status Protocol (OCSP)

Die OCSP-Signer-Zertifikate sind über das Internet abrufbar.

Das BRZ betreibt keinen zentralen Verzeichnisdienst (z.B.: LDAP[23]-Verzeichnisdienst).

2.2 Veröffentlichungen

Sämtliche relevanten Informationen werden auf https://www.oesterreich.gv.at online in einem webbasierten Repository zum Abruf bereitgestellt.

Die veröffentlichten Daten umfassen:

- Nutzungsbedingungen
- Certificate Policy (CP)
- Erklärungen zum Widerrufsverfahren
- RootCA-Zertifikat (inkl. Fingerprint)
- SubCA-Zertifikate (inkl. Fingerprint)
- Widerrufsinformationen (OCSP-Auskünfte)

Die vorliegende Certificate Policy (CP) ist öffentlich unter https://www.oesterreich.gv.at/app-digitales-amt/sicherheitsinformationen abrufbar.

Das mit diesem CP verbundene Certification Practice Statement (CPS) [CPS] für die Plattform OESTERREICH.GV.AT von der Republik Österreich ist nicht öffentlich abrufbar. Nach einer Zustimmung des Auftraggebers (BMDW) können nicht öffentlich abrufbare Dokumente (z.B.: das CPS [CPS]) an Dritte weitergegeben werden.

---

[21] OCSP – Online Certificate Status Protocol

[22] Abrufbar: http://ocsp.oesterreich.gv.at/ocsp

[23] LDAP – Lightweight Directory Access Protocol

Darüber hinaus veröffentlichen die PKI-Beteiligten (siehe Abschnitt 1.3) neben den RootCA- und SubCA-Zertifikaten OCSP-Auskünfte unter https://ocsp.oesterreich.gv.at/ocsp.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Unmittelbar nach der erfolgten Freigabe von erstellten Dokumenten oder nach der abgeschlossenen Freigabe von durchgeführten Änderungen findet die Veröffentlichung statt.

Versionierung bei Änderungen, Ergänzungen oder Korrekturen

Wird eine Änderung durchgeführt, so ist eine neue Version zu erstellen und daher die Versionsnummer schrittweise zu erhöhen, um inhaltliche Änderungen nachvollziehen zu können. Eine bloße Unterscheidung anhand des Datums der Veröffentlichung ist nicht zulässig.

Gültigkeit und Anwendungsbereich

Neue Versionen sind sofort nach der Veröffentlichung für alle im Abschnitt 1.3 beschriebenen Teilnehmenden gültig. Eine nicht mehr aktuelle Version ist demnach sofort ungültig. Die Verantwortung zur Berücksichtigung einer aktualisierten Version liegt bei den Teilnehmenden.

Änderungen an der CP und deren Aktualisierung

Diese CP [CP] ist mindestens einmal jährlich einem Review zu unterziehen. Bei Änderungen der im CP [CP] festgelegten Beschreibungen, Definitionen, Erklärungen, Maßnahmen oder Prozesse ist das Dokument zeitgerecht zu aktualisieren.

Veröffentlichung von Zertifikaten

Die Veröffentlichung eines Zertifikats erfolgt, nachdem das Zertifikat erstellt wurde. Jede Änderung des Zertifikatsstatus wird in den Statusinformationen veröffentlicht.

Generell gilt, dass sowohl die RootCA-Zertifikate, als auch die SubCA-Zertifikate nach der Erstellung öffentlich verfügbar sind.

Veröffentlichung von Sperrinformationen bzw. Statusinformationen

Eine Aktualisierung der öffentlich zugänglichen Sperrinformationen für RootCA-Zertifikate und für SubCA-Zertifikate wird nach jeder Änderung durchgeführt.

2.4 Zugriffskontrolle zu den Verzeichnisdiensten

Die BRZ GmbH betreibt ausschließlich einen Auskunftsdienst (OCSP) und keinen Verzeichnisdienst (z.B.: LDAP-Verzeichnisdienst) um Widerrufsinformationen zu veröffentlichen.

Zugriff auf den Auskunftsdienst

Der Abruf von Daten des Auskunftsdienstes, um den Zertifikatsstatus zu erhalten, ist ausschließlich mit lesendem Zugriff möglich. Die BRZ GmbH kann bei Bedarf Mengenbeschränkungen definieren und umsetzen.

Schutz vor Manipulation und Modifikation

Der Auskunftsdienst ist vor unbefugter Manipulation bzw. Veränderung geschützt.

3. Identifizierung und Authentifizierung

3.1 Namensgebung

3.1.1 Namenstypen / Namensform

Die OESTERREICH.GV.AT-PKI stellt Zertifikate ausschließlich nach dem X.509-Standard [X.509] aus.

In der OESTERREICH.GV.AT-PKI wird eine eindeutige Namenshierarchie angewendet. Alle von der OESTERREICH.GV.AT-PKI erstellten Zertifikate enthalten daher eindeutige Namen. Diese eindeutigen Namen sind konform zur Standard-Serie X.500 [X.500].

CA-Zertifikate müssen Zertifikate erzeugen (generieren) und signieren, welche einen zum X.500-Standard [X.500] kompatiblen, eindeutig definierten Namen (Distinguished name, DN) in den Feldern Aussteller und Betreff enthalten.

Die folgende Tabelle beschreibt das anzuwendende Schema für die verwendeten Attribute:

SubjectDN	
commonName (CN)	*Bindungs-Zertifikat – < Zufallswert>*
organizationName (O)	*Republik Oesterreich (vertreten durch BKA und BMDW)*
countryName (C)	*AT*

Tabelle 1: Anzuwendendes Schema für verwendete Attribute | SubjectDN

Ein DN entspricht dem oben beschriebenen Schema. Die festgelegte Reihenfolge dieser genannten Attribute muss eingehalten werden. Die Bedeutung der beschriebenen Attribute wird in Abschnitt 7.1 genauer erklärt.

Die Pflicht-Attribute *„C“* und *„O“* müssen exakt einmal angegeben werden.

Das Attribut *„OU“* wird nicht angegeben für:

- RootCA / StammCA
- SubCA / AusstellerCA
- Binding-Zertifikat der oeApp

3.1.2 Aussagekraft von Namen

Der festgelegte Distinguished Name (DN) muss den Zertifikatsinhaber eindeutig identifizieren und aussagekräftig sein.

Der DN muss sowohl die (1) Entität (d.h. Gerät, Organisation, Person, Objekt), für die das Zertifikat ausgestellt wurde, als auch für die (2) Entität, die der Aussteller des Zertifikats ist, eindeutig identifizieren.

3.1.3 Anonymität und Pseudonyme

Anonyme oder pseudonyme Zertifikatsdaten sind nicht verboten. Ein erstelltes Pseudonym ist dem festgelegten Zertifikatsinhaber (authentifiziert nach Abschnitt 3.2.3) eindeutig zugeordnet.

Die Ausstellung anonymer Zertifikate ist verboten.

3.1.4 Regeln für die Interpretation der verschiedenen Namensformen

Nicht anwendbar.

3.1.5 Eindeutigkeit der Namen

Der CN muss für die folgenden Zertifikate offenkundig eindeutig sein:

- RootCA / StammCA
- SubCA / AusstellerCA
- Binding-Zertifikat / oeApp

Das bedeutet, der DN eines Zertifikatinhabers muss derart unzweifelhaft eindeutig sein und darf daher auch nicht an unterschiedliche Zertifikatinhaber vergeben werden.

3.1.6 Erkennung, Authentifizierung und Funktion von Warenzeichen

Da sich die jeweiligen CN eines ausgestellten Zertifikats nicht direkt auf eine natürliche Person bezieht, ist eine Anerkennung von Warenzeichen potentiell relevant. Es liegt daher ausschließlich in der alleinigen Verantwortung des Teilnehmenden, dass die Namenswahl keine Markenrechte, Warenzeichen oder ähnliche Schutzrechte verletzt. Die OESTERREICH.GT.AT PKI und/oder die BRZ GmbH als Betreiberin sind nicht verpflichtet, diese Rechte zu überprüfen.

Wird die BRZ GmbH über eine solche Verletzung derartiger Schutzrechte informiert, wird das betroffene Zertifikat widerrufen und der Nutzer informiert.

3.2 Identitätsprüfung bei Neuantrag

Der Zertifikatsnehmer muss bei einem Neuauftrag gegenüber der Zertifizierungsstelle nachweisen, dass er im Besitz des privaten Schlüssels ist, der dem zu zertifizierenden öffentlichen Schlüssel zugeordnet ist, indem der im Zertifikatantrag enthaltene Certificate Signing Request (CSR) mit dem privaten Schlüssel signiert und an die CA übermittelt wird. Die CA muss die Gültigkeit der Signatur überprüfen.

Die Identitätsprüfung von Neuanträgen erfolgt automatisch durch die AERA.

Die bei der Antragsstellung durchgeführten Überprüfungen basieren auf der Grundlage des nicht öffentlich verfügbaren Sicherheitskonzepts der Plattform OESTERREICH.GV.AT [SEC-OEGVAT] und sind in der vorliegenden CP definiert.

3.2.1 Nachweis des Besitzes eines privaten Schlüssels

Bei der Antragstellung ist es notwendig nachzuweisen, dass der Zertifikatsinhaber im Besitz des privaten Schlüssels ist.

Zu diesem Zweck umfasst der Registrierungs- und/oder der Ausstellungsprozess ein Verfahren, bei dem der Antragsteller den Besitz des privaten Schlüssels durch Verwendung eines mit dem

privaten Schlüssel der OESTERREICH.GV.AT-App selbst signierten PKCS[24]#10[25]-konformen Certificate Signing Requests (CSR) der den öffentlichen Schlüssel der OESTERREICH.GV.AT-App enthält, nachweist. Der CSR wird geschützt über https[26] (TLS) an das Binding-Service übermittelt.

3.2.2 Authentifizierung einer Organisation

Jede Organisation, die an der OESTERREICH.GV.AT-PKI teilnimmt, hat einen Vertrag mit dem Auftraggeber (BMDW) abgeschlossen. Vor Vertragsschluss werden die von der Organisation gemachten Angaben vom Auftraggeber (BMDW) durch eine Prüfung von geeigneten Evidenz-Unterlagen verifiziert. Dies kann vom Auftraggeber delegiert werden.

3.2.3 Authentifizierung von natürlichen Personen

Die Authentifizierung von natürlichen Personen im Rahmen von Zertifikatsausstellungsprozessen erfolgt durch einen Vertrauensdiensteanbieter (VDA) und die am Smartphone installierte VDA-Komponente.

Die Authentifizierung erfolgt nicht direkt an der OESTERREICH.GV.AT-PKI. Die Authentifizierung findet am Binding-Service statt und zwischen der OESTERREICH.GV.AT-PKI und dem Binding-Service besteht eine Vertrauensbeziehung.

3.2.4 Nicht überprüfte Teilnehmerangaben

Alle Teilnehmerangaben werden überprüft. Neben Validierungen aus den Abschnitten 3.2.2 und 3.2.3 erfolgen keine weiteren und daher darüber hinausgehenden Überprüfungen.

3.2.5 Überprüfung der Berechtigung

Berechtigungsprüfungen für Benutzer

Die Validierung und die Autorisierung der Berechtigungen finden im Binding-Service durch ein geeignetes Verfahren statt. Das bedeutet, jeder erfolgreich am Binding-Service authentifizierte Benutzer darf einen CSR erstellen und an das Binding-Service übermitteln. Das Binding-Service übermittelt den CSR danach an die AERA.

Berechtigungsprüfungen bei Stellvertretungen

Stellvertretungen sind im Bereich der OESTERREICH.GV.AT-PKI nicht möglich.

3.2.6 Kriterien für Zusammenarbeit

Eine Zusammenarbeit mit externen PKIs ist zum derzeitigen Zeitpunkt nicht vorgesehen. Das bedeutet, die Betreiber der OESTERREICH.GV.AT-PKI führen keine Kreuzzertifizierungen (auch: „Cross-Zertifizierungen) durch. Daher werden andere Zertifizierungsstellen von der

[24] PKCS – Public Key Cryptography Standard

[25] PKCS#10 – Certification Request Standard (d.h. ein potentielles Schema für einen Zertifikatsantrag an eine Certification Authority)

[26] https – Hypertext Transfer Protocol Secure

OESTERREICH.GV.AT-PKI nicht anerkannt, wodurch eine technische Vernetzung mit anderen Zertifizierungsstellen nicht vorgesehen ist.

Sollten vor Inbetriebnahme der OESTERREICH.GV.AT-PKI Cross-Zertifizierungen bestehen, sind diese vor der Inbetriebnahme der OESTERREICH.GV.AT-PKI zwischen der (1) BRZ GmbH (Service Manager, System Security Officer) und dem (2) Auftraggeber (BMDW) abzustimmen bzw. zu bereinigen.

Die Kontaktaufnahme für Angelegenheiten, die im Rahmen der vorliegenden CP zu behandeln sind, ist ausschließlich über folgende Optionen möglich:

Technischer Kontakt

BRZ GmbH

Organisatorischer Kontakt[27]

Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW)

3.3 Identifizierung und Authentifizierung bei Zertifikatserneuerung mit Schlüsselwechsel

Bei einer Zertifikatserneuerung mit einem Schlüsselwechsel handelt es sich um eine erneute Ausstellung von Zertifikaten und erneute Generierung der damit assoziierten Schlüssel für den jeweils gleichen Zertifikatseigentümer. Dies ist etwa nach Ablauf der Gültigkeit eines Zertifikats oder bei Änderung der Daten bei Zertifikatsinhabern möglich.

Die Schlüsselerneuerung für ein ausgestelltes Zertifikat oder für widerrufene Zertifikate ist nicht möglich.

3.4 Identifizierung und Authentifizierung bei Widerruf und Sperranträgen

Ausschließlich autorisierte Entitäten (z.B.: Geräte, Organisationen, Personen, PKI) können einen Widerruf von Zertifikaten veranlassen. Autorisiert sind entweder Zertifikatsinhaber oder berechtigte Dritte. Diese Entitäten können Zertifikate widerrufen.

Ein Widerruf ist manuell oder automatisch möglich:

Manuell

- durch den Benutzer (d.h. Zertifikatsinhaber) über die App/Web-Oberfläche[28]
- durch Erstellen eines Widerrufantrags durch den Benutzer in der OESTERREICH.GV.AT-App (oeApp)

Automatisch

- bei erkennen eines gerooteten[29] Geräts

---

[27] Anmerkung: Die Endverantwortung für OESTERREICH.GV.AT liegt beim Auftraggeber (BMDW)

[28] Abrufbar: https://www.oesterreich.gv.at

- durch Zeitablauf des qualifizierten Zertifikats beim VDA
- nach Widerruf oder Sperre[30] eines qualifizierten Signaturzertifikats[31] von einem Benutzer durch den VDA
- durch Zeitablauf des Binding-Zertifikats
- bei definierten Fehlerfällen (z.B.: Fehler beim Aufbringen des Zertifikats im Client)

Überprüfung des aktuellen Zertifikatsstatus

Der Status eines Zertifikats (d.h.: abrufen von solchen Statusinformation) kann mit einem Auskunftsdienst über OCSP öffentlich[32] abgefragt und überprüft werden.

Auswirkungen von Widerrufen auf Zertifikate

Ein Widerruf führt zu einem dauerhaften und nicht umkehrbaren Entzug der Gültigkeit eines Zertifikats.

Temporäre Sperren von OESTERREICH.GV.AT-Zertifikaten

Eine zeitlich begrenzte Sperre (d.h. temporärer Widerruf) von RootCA-Zertifikaten, von SubCA-Zertifikaten und von Binding-Zertifikaten der OESTERREICH.GV.AT-PKI ist nicht möglich.

Temporäre Sperren von Zertfikaten bei VDAs

Nachdem ein qualifiziertes Signatur-Zertifikat beim VDA gesperrt oder widerrufen wurde (z.B.: durch den Zertifikatsinhaber) wird anschließend jedes damit erzeugte Binding-Zertifikat (z.B.: auf mehreren Smartphones, Tablet-Computern) automatisch widerrufen und dieses Zertifikat ist daher dauerhaft sowie nicht umkehrbar ungültig. Danach ist gegebenenfalls ein neues Binding-Zertifikat zu beantragen.

Protokollierung von Widerrufen

Ein Widerruf wird protokolliert und beim Betreiber von OESTERREICH.GV.AT gespeichert.

Authentisierung bei Widerrufen

Die Authentisierung eines durchzuführenden Widerrufs hat in geeigneter Art und Weise zu erfolgen.

Kontaktstellen für Widerrufe von OESTERREICH.GV.AT-Zertifikaten

Für den Widerruf von Zertifikaten zu nützende Kontaktdetails sind:

---

[29] Rooten – Manipulieren (z.B.: nicht-autorisiertes entfernen von Einschränkungen, modifizieren des Betriebssystems) der beschränkten Rechte eines Geräts, um die größt-moglichen erweiterten Berechtigungen (z.B.: Administrator-Rechte) zu erhalten. Rooten wird oft auch als jailbreaken (vom Begriff Jailbreak) bezeichnet.

[30] Sperre – temporärer Widerruf eines Zertifikats. Manche VDAs bieten diese Möglichkeit an.

[31] Anmerkung: Dieses qualifizierte Signaturzertifikat wird durch den VDA verwaltet und liegt nicht im Einflussbereich von OESTERREICH.GV.AT.

[32] Abrufbar: http://ocsp.oesterreich.gv.at/ocsp

Online-Plattform für Widerrufe

https://www.oesterreich.gv.at

Programmverwaltung der digitalen Vertriebsplattformen

- Apple® App Store®
- Google Play™ (Store)

4. Anforderungen an den Lebenszyklus des Zertifikats

Dieser Abschnitt behandelt die betrieblichen (operationellen) Anforderungen im Lebenszyklus von Zertifikaten.

Antragsteller (später Zertifikatsinhaber) führen einen Registrierungsprozess durch, der die folgenden Anforderungen inkludiert:

- Erzeugen eines kryptografischen Schlüsselpaares
- Ausliefern des erzeugten öffentlichen Schlüssels der kryptografisch mit dem korrespondierenden privaten Schlüssel verbunden ist
- Akzeptieren der Nutzungsbedingungen für Antragsteller / Zertifikatsinhaber

Die nachfolgenden operationellen Anforderungen sind für den Lebenszyklus von Zertifikaten anwendbar.

4.1 Beantragung eines Zertifikats

Dieser Abschnitt behandelt die Anforderungen an den Prozess zur Beauftragung von Zertifikaten. Der Prozess findet zwischen der App und dem Binding-Service statt.

4.1.1 Wer kann ein Zertifikat beantragen

Ausschließlich Nutzer von OESTERREICH.GV.AT assoziierten Apps (intern) welche entweder die dafür erforderliche iOS[33] App oder die Android[34] App auf ihrem Gerät installiert haben, können ein Zertifikat beantragen.

Zwischen den mit OESTERREICH.GV.AT assoziierten Apps (intern) und dem Binding-Service der OESTERREICH.GV.AT-PKI besteht eine authentifizierte Verbindung, wenn sich der Benutzer beim VDA authentifiziert hat. Die Verbindung über das Internet wird über TLS (Transport Layer Security) geschützt.

Das Binding-Service prüft die Gültigkeit der Zertifikatsanforderungen (national und eIDAS [eIDAS]) für die OESTERREICH.GV.AT-PKI. Details sind im nicht öffentlichen Sicherheitskonzept der OESTERREICH.GV.AT-PKI [SEC-OEGVAT] beschrieben.

Das Binding-Service prüft die Key Attestation[35] Elemente der Entität, die ein Zertifikat anfordert, um der CA kryptografisch nachzuweisen, dass der zur Zertifikatsanforderung gehörende private Schlüssel in einem Secure Element auf dem Smartphone geschützt ist.

---

[33] iOS® – Apple® Betriebssystemplattform für mobile Endgeräte; Nutzung des Cisco® Trademarks IOS® unter Lizenz

[34] Android – Betriebssystemplattform für mobile Endgeräte

[35] Key Attestation – Die Key Attestation (Android) überprüft die Extensions (d.h. Erweiterungen), die im ersten Zertifikat der Zertifikatskette im hardwaregestützten Keystore eines Geräts angezeigt werden.

4.1.2 Verfahren und Verantwortung

Verantwortungen der Antragsteller

Der Antragsteller zur Erstellung eines Zertifikats ist dazu verpflichtet, ausschließlich aktuelle und korrekte Informationen in den CSR einzubringen.

Bevor ein Binding-Zertifikat erzeugt werden kann, ist ein Durchlaufen eines Registrierungsprozesses (z.B.: ausgestellte Bürgerkarte, ausgestellte Handy-Signatur) bei einem VDA oder das Vorhandensein einer eIDAS-konformen [eIDAS] eID erforderlich.

Verantwortungen der OESTERREICH.GV.AT-PKI

Bevor ein Zertifikat erzeugt werden kann, muss die RootCA vom Antragsteller einen Zertifikatsauftrag und die Zustimmung zu den vertraglich vereinbarten Bestimmungen erhalten.

4.2 Bearbeitung des Zertifikatsantrags

Dieser Abschnitt behandelt die Anforderungen zur Bearbeitung eines Zertifikatsantrags durch die OESTERREICH.GV.AT-PKI.

4.2.1 Durchführung der Identifizierung und Authentifizierung

Der Antragsteller ist dazu verpflichtet, alle notwendigen Informationen, um ein Zertifikat zu erstellen und/oder welche in der vorliegenden CP gefordert werden, in geeigneter Form zur Verfügung zu stellen.

Wenn nicht alle notwendigen Daten und Angaben enthalten sind, wird kein Binding-Zertifikat ausgestellt und dem Benutzer eine Fehlermeldung angezeigt.

4.2.2 Annahme oder Ablehnung des Zertifikatsantrags

Die Schlüsselerstellung für die Binding-Zertifikate erfolgt in jedem Fall innerhalb des Secure-Elements auf den Geräten der Antragsteller. Nachdem der Schlüssel erstellt wurde, wird das Zertifikat an die App des Benutzers übermittelt, darin gespeichert und im User Store gespeichert.

Treten bei der Identitätsprüfung oder bei der Korrektheitsprüfung der vom Antragsteller angegebenen Daten Unstimmigkeiten auf, die nicht zeitnah und restlos auszuräumen sind, wird der Zertifikatsantrag abgelehnt. Das bedeutet, Zertifikatsanträge werden von der OESTERREICH.GV.AT-PKI abgelehnt, wenn nicht alle Anforderungen der vorherigen Kapitel erfüllt sind. Der Antragsteller muss über die Ablehnungsgründe informiert werden (z.B.: über eine Nachricht in der App).

4.2.3 Bearbeitungsdauer bei Zertifikatsanträgen

Alle an der Bearbeitung von Zertifikatsanträgen beteiligten Entitäten unternehmen, wirtschaftlich und technisch angemessene Anstrengungen, um sicherzustellen, dass übermittelte sowie korrekte Zertifikatsanträge (CSR) rechtzeitig bearbeitet werden. Die Identität wird entweder durch einen

VDA festgestellt, durch Anwendung Handy-Signatur oder mittels einer unterstützten eIDAS-konformen [eIDAS] ausländischen eID[36] für nicht-österreichische EU-BürgerInnen.

Korrekte Zertifizierungsanträge (Certificate Signing Requests – CSRs) werden innerhalb eines wirtschaftlich angemessenen Zeitrahmens bearbeitet. Die OESTERREICH.GV.AT CA ist nicht für Verzögerungen verantwortlich, die vom Antragsteller oder von Ereignissen außerhalb der Kontrolle der CA ausgelöst werden.

Die Bearbeitungsdauer ist wegen der automatischen Verarbeitung und Erzeugung der Binding-Zertifikate ausreichend kurz. Damit ist die Umsetzung der in der OESTERREICH.GV.AT-PKI geforderten Binding-Prozesse möglich.

4.3 Erstellung des Zertifikats

Dieser Abschnitt behandelt die Generierung eines Zertifikats nach der erfolgreich durchgeführten Überprüfung des übermittelten CSRs durch die OESTERREICH.GV.AT-PKI.

4.3.1 Aufgaben der Zertifizierungsstelle

Um einen korrekten Zertifikatsantrag abzuschließen und ein Zertifikat zu erstellen wird auf dem Gerät des Benutzers, im Secure Element ein kryptografisch verknüpftes Schlüsselpaar erzeugt. Mit dem privaten Schlüssel wird ein erstellter CSR signiert. Dieser enthält den öffentlichen Schlüssel. Der CSR wird an das Binding-Service übermittelt.

Die PKI nimmt CSRs entgegen und prüft die Signatur der CSRs mit dem öffentlichen Schlüssel aus dem CSR. Danach generiert die PKI das Zertifikat, welches den öffentlichen Schlüssel aus dem CSR und die Identitätsinformationen des Antragstellers beinhaltet.

Die (1) OESTERREICH.GV.AT-PKI, dem (2) Binding-Service und der (3) Identity-Provider (IdP) protokollieren und archivieren die Daten für die Zertifikatsbeantragung. Die detaillierten Abläufe sind im Sicherheitskonzept [SEC-OEGVAT] der OESTERREICH.GV.AT-PKI beschrieben.

4.3.2 Benachrichtigung des Zertifikatsinhabers

Der Antragsteller (d.h. Zertifikatsnehmer) wird von der OESTERREICH.GV.AT-PKI über die abgeschlossene Ausstellung des Zertifikats informiert.

4.4 Annahme des Zertifikats

4.4.1 Annahmeverfahren

Der Antragsteller (bzw. Zertifikatsnehmer) nimmt das von der OESTERREICH.GV.AT-PKI generierte Zertifikat an und bestätigt im Rahmen der Übergabe automatisch den Empfang sowie die Akzeptanz des Zertifikats.

Zertifikate sind nach den folgenden Prozessschritten:

[36] eID – elektronische Identität

Gültig

- nach Übermitteln einer Empfangsbestätigung

Ungültig

- nach Verstreichen der Frist um eine Empfangsbestätigung zu übermitteln oder das Zertifikat zu nutzen

Die Annahme eines erstellten Zertifikats erfolgt durch die vom Antragsteller (bzw. Zertifikatsnehmer) übermittelte Empfangsbestätigung (d.h. Erklärung zur Annahme). Das Binding-Service protokolliert die übertragene Empfangsbestätigung in Kombination mit allen während der Antragstellung übermittelten Daten des Antragstellers. Übermittelt der Antragsteller (bzw. Zertifikatsnehmer) keine Bestätigung für das erstellte Zertifikat an die OESTERREICH.GV.AT-PKI innerhalb von 6 Stunden, führt die OESTERREICH.GV.AT-PKI aus Sicherheitsgründen einen automatischen Widerruf des ausgestellten Zertifikats durch. Ein Widerruf ist nicht umkehrbar und somit dauerhaft. Daraus folgt, dass das Zertifikat ungültig ist. Dieser Vorgang wird protokolliert.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

RootCA-Zertifikate

Die durch die OESTERREICH.GV.AT-PKI erzeugten RootCA-Zertifikate sind über das Repository der Webseite[37] öffentlich zugänglich. Der Übertragungsweg ist mittels Transport Layer Security (TLS) gesichert.

SubCA-Zertifikate

Die durch die OESTERREICH.GV.AT-PKI erzeugten SubCA-Zertifikate sind über das Repository der Webseite[38] öffentlich zugänglich. Der Übertragungsweg ist mittels Transport Layer Security (TLS) gesichert.

Binding-Zertifikate

Die OESTERREICH.GV.AT-PKI veröffentlicht Binding-Zertifikate nicht.

4.4.3 Benachrichtigung weiterer Instanzen

Die Benachrichtigung weiterer Instanzen ist nicht erforderlich.

4.5 Verwendung der Schlüssel und des Zertifikats

Die im Rahmen dieser CP ausgestellten Zertifikate werden ausschließlich als Binding-Zertifikate für Apps welche mit OESTERREICH.GV.AT assoziiert sind erstellt. Diese Zertifikate dürfen nur für Client-TLS-Authentisierungen der oeApps im Zusammenhang mit der Plattform OESTERREICH.GV.AT verwendet werden.

[37] Abrufbar: https://www.oesterreich.gv.at/app-digitales-amt/sicherheitsinformationen

[38] Abrufbar: https://www.oesterreich.gv.at/app-digitales-amt/sicherheitsinformationen

Die detaillierten Anwendungsszenarien (Verbindungsaufbau, Prüfen des Widerrufsstatus, etc.) sind im Sicherheitskonzept von OESTERREICH.GV.AT [SEC-OEGVAT] beschrieben.

4.5.1 Verwendung der Schlüssel und des Zertifikats durch den Zertifikatsinhaber

Der Zertifikatsinhaber ist zur Einhaltung der Nutzungsbedingungen von OESTERREICH.GV.AT verpflichtet. Die Nutzungsbedingungen sind öffentlich abrufbar[39].

Der Zertifikatsinhaber darf den privaten Schlüssel und/oder das Zertifikat ausschließlich für den festgelegten Zweck verwenden (Siehe Abschnitt 1.4.1).

Der private Schlüssel ist vom Zertifikatsinhaber geheim zu halten sowie die unbefugte Verwendung durch bzw. die Weitergabe an Dritte zu verhindern. Diese Geheimhaltungsverpflichtung der vom Zertifikatsinhaber gespeicherten Daten besteht über die Gültigkeit des ausgestellten Zertifikats hinaus.

Manipulationen am erstellen Zertifikat sind nicht erlaubt und führen zu einem Widerruf.

Die Verpflichtungen des Zertifikatsinhabers sind:

Einhaltung von Restriktionen der Nutzung

- Einhalten der Beschränkungen zur Verwendung des eigenen privaten Schlüssels
- Einhalten der in den Nutzungsbedingungen definierten Regelungen zur Schlüsselverwendung und zur Verwendung der ausgestellten Zertifikate

Benachrichtigungen an den Betreiber von OESTERREICH.GV.AT

- Eindeutig referenzierbare Daten an den Betreiber von OESTERREICH.GV.AT übermitteln
- Unverzüglich den Betreiber von OESTERREICH.GV.AT benachrichtigen, falls die Angaben im Zertifikat nicht oder nicht mehr den aktuellen Tatsachen entsprechen
- Unverzüglich den Betreiber von OESTERREICH.GV.AT benachrichtigen, falls der Verdacht besteht, dass das Zertifikat und/oder das Schlüsselmaterial kompromittiert wurde
- Unverzüglich den Betreiber von OESTERREICH.GV.AT benachrichtigen, wenn Schlüsselmaterial kompromittiert wird oder verloren geht
- Unverzüglich den Betreiber von OESTERREICH.GV.AT benachrichtigen, wenn das Schlüsselmaterial nicht mehr alleinig vom Zertifikatsinhaber kontrolliert wird (z.B.: nicht mehr geheim gehalten werden kann)

Auslösen eines Widerrufs

- Unverzüglich den Widerruf des betroffenen Zertifikats in der OESTERREICH.GV.AT-App (oeAPP) zu initiieren, wenn der eigene private Schlüssel kompromittiert ist (oder der Verdacht darauf besteht) oder das Zertifikat nicht länger benötigt wird

Bei Fehlverhalten des Zertifikatsinhabers behält sich OESTERREICH.GV.AT vor, das betroffene Zertifikat zu widerrufen. Darüber wird der Zertifikatsinhaber informiert.

[39] Abrufbar: https://www.oesterreich.gv.at/app-digitales-amt/nutzungsbedingungen

4.5.2 Verwendung des Zertifikats durch Dritte

Berechtigte Dritte können Zertifikate dauerhaft widerrufen.

Die Nutzung eines Zertifikats durch Dritte und/oder die Weitergabe an Dritte sind nicht erlaubt.

Bei OESTERREICH.GV.AT-Apps (oeAPPs), welche von Zertifikatsinhabern auf Geräten installiert wurden und das Schlüsselmaterial sowie die Zertifikate enthalten, handelt es sich nicht um Dritte.

4.6 Zertifikatserneuerung (Re-Zertifizierung)

Eine Zertifikatserneuerung (Re-Zertifizierung) wird nicht durchgeführt.

4.7 Schlüssel- und Zertifikatserneuerung (Re-key)

Erneuerungen von Schlüsseln und/oder Zertifikaten werden nicht durchgeführt.

4.8 Zertifikatsmodifizierung

Modifizierungen von Zertifikaten werden nicht durchgeführt.

4.9 Widerruf und Sperrung (Suspendierung) von Zertifikaten

Die OESTERREICH.GV.AT-PKI schreibt ein einstufiges Widerrufskonzept vor. Ein Widerruf führt zu einem dauerhaften und nicht umkehrbaren Entzug der Gültigkeit eines erstellten Zertifikats. Widerrufe sind durchführbar.

Zeitlich beschränkte Sperren und die damit verbundene erneute Aktivierung von gesperrten Zertifikaten (RootCA, SubCA, End-Entity) sind nicht möglich. Das bedeutet Sperren (d.h. zeitlich begrenzte Suspendierungen bzw. temporäre Widerrufe) von Zertifikaten werden durch die OESTERREICH.GV.AT-PKI daher auch nicht durchgeführt.

4.9.1 Widerrufsgründe

Tritt zumindest einer der nachfolgenden Gründe ein, oder lässt sich ein Verdacht darauf nicht zuverlässig widerlegen, wird der Widerruf eines ausgestellten Zertifikats durchgeführt.

Zertifikatsinhaber verursachen Widerrufe

- Wenn der Zertifikatsinhaber dies wünscht
- Ableben des Zertifikatsinhabers mit der frühesten Wirksamkeit nachdem OESTERREICH.GV.AT davon Kenntnis erlangt
- OESTERREICH.GV.AT-Bindung wird widerrufen
- VDA-Bindung wird widerrufen
- Das qualifizierte Signatur-Zertifikat beim VDA wird widerrufen

Verletzung der Validität von Zertifikaten oder der Konformität zu Anforderungen

- Die Gültigkeit des ausgestellten Zertifikats ist abgelaufen
- Die Gültigkeit der VDA-Bindung ist abgelaufen
- Die Gültigkeit des ausgestellten, qualifizierten Signaturzertifikats beim VDA ist abgelaufen

- Die im Zertifikat enthaltenen Angaben sind nicht oder nicht mehr aktuell (d.h. ungültig)
- Wenn ein Gerät, auf dem Schlüsselmaterial gespeichert wird, gerootet wird und daher das Betriebssystem nicht mehr konform zum für die Plattform OESTERREICH.GV.AT erstellten Sicherheitskonzept [SEC-OEGVAT] ist
- Die Inhalte oder das technische Format des erstellten Zertifikats stellen ein Risiko für vertrauende Dritte dar

Veränderungen beim Schlüsselmaterial und bei Zertifikaten

- Wenn ein neues Zertifikat erstellt wird
- Das Schlüsselmaterial kann nicht mehr geheim gehalten werden
- Das Schlüsselmaterial ist kompromittiert (z.B.: manipuliert)
- Das Schlüsselmaterial geht verloren oder wurde gestohlen (z.B.: Smartphone verloren/gestohlen)
- Erstelltes Schlüsselmaterial und/oder angewendete Algorithmen bzw. Parameter (z.B.: Schlüssellänge) entsprechen nicht dem aktuellen Stand der Technik

Vertragliche Basis, Rechtsgrundlage sowie Missbrauch und Verstöße

- Widersprechen gegen die Nutzungsbedingungen von OESTERREICH.GV.AT
- Die vorliegende CP oder das CPS [CPS] der OESTERREICH.GV.AT-PKI verlangt einen Widerruf
- Rechtsgrundlagen bzw. Rechtsnormen (z.B.: Gesetze, Verordnungen) fordern einen Widerruf
- Missbräuchliche Verwendung des Schlüsselmaterials und/oder des Zertifikats durch Zertifikatsinhabers und/oder Dritte (z.B.: Rechtswidrigkeit, Verstoß gegen die vorliegende CP bzw. gegen das CPS [CPS])
- Verstoß des Zertifikatsinhabers bzw. eines autorisierten Dritten gegen die vorliegende CP oder das CPS [CPS]
- Verstoß des Zertifikatsinhabers bzw. eines autorisierten Dritten gegen die Nutzungsbedingungen von OESTERREICH.GV.AT

OESTERREICH.GV.AT-App (oeAPP)

- Die OESTERREICH.GV.AT-App (oeAPP) wird neu installiert nachdem diese von einem Gerät entfernt wurde. Das alte Binding-Zertifikat der zuvor entfernten App wird widerrufen.

Da eine Sperre von Zertifikaten und/oder Schlüsselmaterial bei Verdachtsmomenten nicht möglich ist, führen die oben aufgelisteten Gründe auch bei den jeweiligen Verdachtsmomenten zu einem nicht umkehrbaren Widerruf des betroffenen Zertifikats.

4.9.2 Wer kann einen Widerruf beantragen

Widerrufe können entweder manuell oder automatisch durchgeführt werden. Einen Widerruf können die folgenden natürlichen Personen beantragen:

Manueller Widerruf

- Generell der Zertifikatsinhaber oder autorisierte Dritte (z.B.: Familienangehörige bei Ableben des Zertifikatsinhabers)
- Der Zertifikatsinhaber oder autorisierte Dritte widerrufen aus der OESTERREICH.GV.AT-App die für diese App relevanten Zertifikate
- Der Zertifikatsinhaber oder autorisierte Dritte (z.B.: Familienangehörige) widerrufen aus der OESTERREICH.GV.AT-App Zertifikate von beliebigen (assoziierten) Geräten bzw. Apps
- Der Zertifikatsinhaber oder autorisierte Dritte widerrufen ein (oder mehrere) Zertifikat(e) über die Browser-Oberfläche der Web-Plattform OESTERREICH.GV.AT-App von beliebigen (assoziierten) Geräten bzw. Apps
- Personen, welche die Identität bzw. die Berechtigung eines Zertifikatsnehmers bei der Zertifikatsbeantragung bestätigt haben, können einen Widerruf durchführen, wenn der Zertifikatsnehmer nicht mehr berechtigt ist, das Zertifikat zu verwenden

Automatischer Widerruf

- Generell die OESTERREICH.GV.AT-PKI selbst (z.B.: die OESTERREICH.GV.AT-App (oeAPP) erstellt einen Widerrufsantrag, wenn ein Android-Gerät gerootet wird und die SubCA führt diesen Widerrufsantrag aus)
- Generell die OESTERREICH.GV.AT-App (oeAPP) selbst
- Generell der VDA selbst (z.B.: indirekt über den Widerruf des qualifizierten Signaturzertifikats, welcher den automatischen Widerruf des Binding-Zertifikats auslöst)
- Bei einem Sicherheitsvorfall widerrufen die OESTERREICH.GV.AT-PKI und/oder der VDA alle betroffenen Zertifikate
- Die OESTERREICH.GV.AT-App (oeAPP) bei Entfernung der App von einem Gerät
- Die OESTERREICH.GV.AT-PKI bei einer Neuausstellung eines Zertifikats
- Wenn die Annahme eines erstellten Zertifikats nicht bestätigt wird

Technisch durchgeführt wird ein Widerruf unabhängig vom Antrag entweder vom VDA und/oder von der OESTERREICH.GV.AT-PKI.

4.9.3 Verfahren des Widerrufs

Der Widerruf eines ausgestellten Zertifikats ist mit den folgenden gängigen Kommunikationsmethoden möglich:

- Elektronischer Widerrufsworkflow über OESTERREICH.GV.AT-Web
- OESTERREICH.GV.AT-App (oeAPP)

Der Antragsteller muss sich durch geeignete Form authentifizieren und eine Identifizierung ermöglichen.

Die OESTERREICH.GV.AT-PKI führt den beantragten Widerruf des betroffenen Zertifikats an der relevanten CA durch. Der Zertifikatsinhaber wird über den durchgeführten Widerruf des Zertifikats unterrichtet.

4.9.4 Fristen für den Zertifikatsinhaber

Zertifikatsinhaber und/oder autorisierte Dritte sind dazu verpflichtet, unmittelbar nachdem die Kenntnis über den (oder die) zum Widerruf führenden Gründe erlangt wird, den Widerruf des betroffenen Zertifikats über ein gängiges Kommunikationsmedium (Siehe 4.9.3) zu beantragen.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Die OESTERREICH.GV.AT-PKI führt den beantragten Widerruf eines betroffenen Zertifikats unverzüglich nach Eingang des Antrags durch. Der Widerruf wird so rasch wie möglich durchgeführt und ist innerhalb eines Werktages wirksam.

4.9.6 Anforderungen zur Prüfung des Zertifikatsstatus durch eine Relying Party

Gültigkeitsprüfung mittels OCSP

Die Prüfung des Zertifikatsstatus kann mithilfe des OCSP-Responders erfolgen. Widerrufsinformationen werden daher mittels Auskunftsdienst (OCSP) veröffentlicht, wodurch eine Gültigkeitsprüfung aller in der OESTERREICH.GV.AT-PKI-Hierarchie (Siehe Abbildung 1) ausgestellten Zertifikate durchführbar ist. Um die Gültigkeit eines Zertifikats zu überprüfen, muss der Zertifikatsnutzer eine Anfrage an den OCSP-Responder stellen.

Gültigkeitsprüfung mittels CRL

Eine Überprüfung der Zertifikatsgültigkeit mittels CRL ist nicht durchführbar.

4.9.7 Häufigkeit der Erstellung der CRL

Nicht anwendbar (siehe: 4.9.6).

4.9.8 Maximale Latenzzeit für Veröffentlichung von CRLs

Nicht anwendbar (siehe: 4.9.6).

4.9.9 Verfügbarkeit von Online-Statusabfragen (OCSP)

Sperrinformationen (bzw. Widerrufsinformationen[41]) werden für die Zertifikatsnutzer online über das Internet mittels OCSP-Responder nach RFC 6960 bereitgestellt[42]. Darin sind alle von der OESTERREICH.GV.AT-Zertifizierungsstelle widerrufenen Zertifikate enthalten.

Das OCSP ist grundsätzlich 7x24x365 über das Internet erreichbar.

Erstellte OCSP-Antworten sind höchstens 1 (eine) Stunde gültig.

4.9.10 Anforderungen hinsichtlich der Online-Überprüfung

Im Rahmen der wirtschaftlich vernünftigen Möglichkeiten bietet OESTERREICH.GV.AT sowohl Onlinedienste über das Internet als auch die Verfahren für Menschen mit Behinderungen nach dem aktuellen Stand der Technik verfügbar an.

---

[41] Anmerkung: eine zeitlich begrenzte Sperre ist nicht möglich (Siehe: 3.4)

[42] Abrufbar: https://ocsp.oesterreich.gv.at/ocsp

Die RootCA aktualisiert die OCSP-Datenbank zumindest einmal jährlich oder nach einem Widerruf innerhalb von 24 Stunden.

4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung

Nicht anwendbar.

4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln

Bei (dem Verdacht) einer Kompromittierung eines privaten Schlüssels ist das davon betroffene Zertifikat so schnell wie möglich bzw. spätestens innerhalb von einem Werktag nach der Bekanntgabe zu widerrufen.

Der betroffene Schlüssel darf nicht mehr verwendet werden.

Weitere Details zu Anforderungen bei Kompromittierungen von privaten Schlüsseln über (1) Verpflichtungen der Zertifikatsinhaber (siehe: 1.3.3), zur (2) Verwendung der Schlüssel und des Zertifikats (siehe: 4.5.1) sowie zu (3) Widerrufsgründen (siehe: 4.9.1).

4.9.13 Gründe für eine Sperrung

Nicht anwendbar.

4.9.14 Wer kann eine Sperrung beantragen

Nicht anwendbar.

4.9.15 Verfahren der Sperrung

Nicht anwendbar.

4.9.16 Maximale Dauer einer Sperrung

Nicht anwendbar.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Alle CAs (Siehe Abbildung 1) ermöglichen OCSP-Abfragen. Diese sind ausschließlich über OCSP-Responder durchführbar.

Das Zertifikat des OCSP-Responders wird mit dem gleichen Schlüssel der CA signiert, der auch für die Signatur der Endbenutzerzertifikate verwendet wird. OCSP-Zertifikate für OCSP-Responder werden in jedem Fall ausschließlich von der CA erstellt, welche das End-Entity-Zertifikat ausgestellt hat. Daher wird in jedem Fall das gleiche Zertifikat für die Signatur der OCSP-Response verwendet, das auch für die Signierung der End-Entity-Zertifikate verwendet wird, für die der OCSP-Responder Widerrufsstatusinformationen zur Verfügung stellt.

Der OCSP-Responder beantwortet nur Anfragen für Zertifikate, welche von der OESTERREICH.GV.AT-PKI erstellt wurden. Derartige Anfragen werden protokolliert und gespeichert.

Die versendete OCSP-Antwort wird mit dem kryptografischen Algorithmus `ecdsa-with-SHA384` unter Verwendung der Kurve `NIST P-384` nach RFC 8422 [RFC 8422] elektronisch signiert.

4.10.1 Operative Merkmale

Der Online-Dienst zur Überprüfung des Zertifikatsstatus basiert auf einem OCSP-Responder. Damit erhalten Anfragende eine Auskunft über die Gültigkeit von ausgegebenen Zertifikaten vom OCSP-Responder.

4.10.2 Verfügbarkeit des Dienstes

Das OCSP ist grundsätzlich 7x24x365 über das Internet erreichbar.

Die zu erwartende Antwortzeit soll 5 Sekunden nicht überschreiten. Daher müssen ausreichende Kapazitäten zur Verfügung gestellt werden, so dass diese Antwortzeit unter betriebsüblichen Bedingungen einzuhalten ist.

4.10.3 Optionale Merkmale

Nicht anwendbar.

4.11 Beendigung des Vertragsverhältnisses

Die Beendigung eines Vertragsverhältnisses erfolgt durch Deinstallation oder zurücksetzen der OESTERREICH.GV.AT-App (oeApp).

4.12 Schlüsselhinterlegung und –wiederherstellung

Sowohl eine Schlüsselhinterlegung als auch eine Wiederherstellung sind nicht möglich. Liegen Gründe vor, die eine Wiederherstellung erfordern, ist eine neue Erstellung des Schlüsselmaterials sowie des assoziierten Zertifikats notwendig.

5. Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

Die Infrastruktur der OESTERREICH.GV.AT-PKI ist in einem geschützten Raum des BRZ Trustcenters untergebracht.

Alle Prozesse für die Beantragung, die Erzeugung, den Betrieb bzw. die Nutzung sowie den Widerruf während des gesamten Lebenszyklus von Zertifikaten betriebenen CAs sind definiert und dokumentiert. Ein unabhängiges Audit wurde durchgeführt.

Fachkundig qualifiziertes, geschultes und sicherheitsüberprüftes Personal arbeitet im Betrieb des Trustcenters.

Zum Schutz der (1) Vertraulichkeit, der (2) Integrität und der (3) Verfügbarkeit von Zertifikatsdaten sowie des Zertifikatsmanagements-Prozesses hat die BRZ GmbH im Rahmen des Sicherheitskonzepts eine *„BRZ Trustcenter – Allgemeine Sicherheitsrichtlinie“* [BRZ ASRL TC] und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] entwickelt, definiert und eingeführt. Dieses Sicherheitskonzept wird regelmäßig gewartet. Es umfasst Anforderungen an die administrativen, die baulichen, die infrastrukturellen, die organisatorischen sowie die personellen Sicherheitsmaßnahmen und ist nicht öffentlich abrufbar.

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Alle umgesetzten infrastrukturellen Sicherheitsmaßnahmen sind im nicht öffentlich zugänglichen Certification Practice Statement [CPS] der OESTERREICH.GV.AT-PKI sowie im Dokument *„BRZ Trustcenter Allgemeine Sicherheitsrichtlinie“* [BRZ ASRL TC] und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] detailliert beschrieben.

Darüber hinaus gehende Details zum physischen Zugang zum Rechenzentrum des Trustcenters der BRZ GmbH in dem die OESTERREICH.GV.AT-PKI betrieben wird, sind in dem Dokument *„Sicherheitsrichtlinie Facility Services 3.0 der BRZ GmbH“* geregelt.

5.2 Organisatorische Sicherheitsmaßnahmen

Die OESTERREICH.GV.AT-PKI wird im Trustcenter der BRZ GmbH betrieben. Daher wendet die OESTERREICH.GV.AT-PKI Personal- und Managementpraktiken an, welche die Vertrauenswürdigkeit und das notwendige Fachwissen der Mitarbeiter sowie die zufriedenstellende Erfüllung ihrer zugewiesenen Aufgaben mit angemessener Sicherheit gewährleisten.

Die BRZ GmbH besitzt von jedem im Bereich der OESTERREICH.GV.AT-PKI tätigen Mitarbeiter der sicherheitskritische Rollen übernimmt, eine unterschriebene Erklärung darüber, dass für die jeweilige Rolle zugrundeliegende Sicherheitsdokumente bekannt sind und eingehalten werden.

Die BRZ GmbH stellt sicher, dass alle Aktivitäten in Bezug auf die OESTERREICH.GV.AT-PKI dem betroffenen System und der verantwortlichen Person zuzuordnen sind, welche die zugehörige Aktion ausführt.

Die BRZ GmbH implementiert das 4-Augenprinzip (auch bekannt als „Dualkontrolle“) für die Erfüllung kritischer Aufgaben im Bereich der OESTERREICH.GV.AT-PKI.

5.3 Personelle Sicherheitsmaßnahmen

Die umgesetzten personellen Sicherheitsmaßnahmen sind im nicht öffentlich zugänglichen Certification Practice Statement [CPS] der OESTERREICH.GV.AT-PKI sowie im Dokument *„BRZ Trustcenter Allgemeine Sicherheitsrichtlinie“* [BRZ ASRL TC] und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] detailliert beschrieben.

5.4 Protokollierung sicherheitskritischer Ereignisse

Die umgesetzten Methoden, Prozeduren und Techniken für die Protokollierung von Ereignissen sowie insbesondere für die Protokollierung von sicherheitskritischen Ereignissen sind im nicht öffentlich zugänglichen Certification Practice Statement [CPS] der OESTERREICH.GV.AT-PKI sowie im Dokument *„BRZ Trustcenter Allgemeine Sicherheitsrichtlinie“* [BRZ ASRL TC] und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] detailliert beschrieben.

5.5 Archivierung

Die umgesetzten Methoden, Prozeduren und Techniken für die Archivierung von Daten bzw. Dokumenten (z.B.: elektronisch oder papiergebunden) sind im nicht öffentlich zugänglichen Certification Practice Statement [CPS] der OESTERREICH.GV.AT-PKI sowie im Dokument *„BRZ Trustcenter Allgemeine Sicherheitsrichtlinie“* [BRZ ASRL TC] und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] detailliert beschrieben.

5.6 Schlüsselwechsel der Zertifizierungsstelle

Der Schlüsselwechsel der Zertifizierungsstelle erfolgt unter den gleichen Bedingungen wie die erstmalige Erstellung der Schlüssel (siehe: Abschnitt 6).

5.7 Kompromittierung und Wiederherstellung

Die allgemeinen Disaster-Recovery-Maßnahmen sind im nicht öffentlich zugänglichen Dokument *„BRZ Trustcenter – Allgemeine Sicherheitsrichtlinie“* [BRZ ASRL TC] und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] definiert.

5.8 Einstellung des Betriebes

Die allgemeinen Anforderungen, um die Einstellung des Betriebs handzuhaben, sind im nicht öffentlich zugänglichen Dokument *„BRZ Trustcenter – Allgemeine Sicherheitsrichtlinie“* [BRZ ASRL TC] und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] beschrieben.

Eine beabsichtigte Beendigung des Betriebs der OESTERREICH.GV.AT-PKI im BRZ Trustcenter wird frühzeitig zwischen dem Auftraggeber (BMDW) und dem BRZ Trustcenter vereinbart.

Bevor der Betrieb eines Systems beendet werden kann, wird gewährleistet, dass das BRZ Trustcenter

a. alle im Betrieb notwendigen Daten der zu beendenden OESTERREICH.GV.AT-PKI in die Verantwortung des Auftraggebers (BMDW) übergibt,
b. private Schlüssel in der Verantwortung des BRZ Trustcenters zerstört oder deren weitere Verwendung sicher unterbindet.

Diese Aufgaben werden unter Einhaltung des 4-Augen-Prinzips (auch *„Dualkontrolle“*) durchgeführt.

6. Technische Sicherheitsmaßnahmen

Die OESTERREICH.GV.AT-PKI befindet sich im Trustcenter der BRZ GmbH. Die detaillierten technischen Sicherheitsmaßnahmen sind im nicht öffentlich zugänglichen Dokument [BRZ ASRL TC] und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] spezifiziert.

6.1 Generierung und Installation von Schlüsselpaaren

Ergänzende Anforderungen zu den Vorgaben aus der [BRZ ASRL TC] bzw. der und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] an die OESTERREICH.GV.AT-CA:

Die Ausstellung und der Widerruf von Endanwender-Zertifikaten kann von einem Mitarbeiter der Registrierungsstelle nicht durchgeführt werden, da dies nur mittels automatisierter Prozesse vorgesehen ist. Die Einhaltung eines 4-Augen-Prinzips ist hierfür daher nicht notwendig.

Weitere Details über die umgesetzten Methoden, Prozeduren und Techniken für die Erzeugung und die Installation von Schlüsselpaaren sind im nicht öffentlich zugänglichen Certification Practice Statement [CPS] der OESTERREICH.GV.AT-PKI sowie im Dokument *„BRZ Trustcenter Allgemeine Sicherheitsrichtlinie“* [BRZ ASRL TC] und im Sicherheitskonzept für die OESTERREICH.GV.AT-PKI [SEC-OEGVAT] detailliert beschrieben.

6.2 Schutz privater Schlüssel und Einsatz kryptografischer Module

Die im HSM gespeicherten, privaten Schlüssel der RootCA sowie der SubCA (d.h. AusstellerCA) der OESTERREICH.GV.AT-PKI dürfen den Einflussbereich des Administrators der Appliance bzw. den Einflussbereich der BRZ GmbH niemals verlassen.

a. die Datenträger der Appliance müssen gemäß den internen Sicherheitsrichtlinien zur Nutzung von Datenträgern ([BRZ SRL Server Services] Maßnahme SGL.003.BM) gehandhabt werden,
b. Backups von Konfigurationen dürfen den privaten Schlüssel nicht enthalten und
c. eine Vernichtung des privaten Schlüssels muss stets protokolliert durchgeführt werden.

6.3 Weitere Aspekte der Verwaltung von Schlüsselpaaren

Die allgemeinen Aspekte für die Verwaltung von Schlüsselpaaren sind im nicht öffentlich zugänglichen Certification Practice Statement [CPS] der OESTERREICH.GV.AT-PKI definiert.

6.4 Aktivierungsdaten

Detaillierte Beschreibungen über die Aktivierungsdaten sind im nicht öffentlich zugänglichen Certification Practice Statement [CPS] der OESTERREICH.GV.AT-PKI beschrieben.

6.5 Sicherheitsmaßnahmen für Computer

Details über die umgesetzten Methoden, Prozeduren und Techniken der installierten Sicherheitsmaßnahmen für Computer-Systeme sind im nicht öffentlich zugänglichen Certification Practice Statement [CPS] der OESTERREICH.GV.AT-PKI beschrieben.

6.6 Sicherheitsmaßnahmen für den Software-Lebenszyklus

Details über die Sicherheitsmaßnahmen für den Software-Lebenszyklus sind im nicht öffentlich zugänglichen Certification Practice Statement [CPS] der OESTERREICH.GV.AT-PKI beschrieben.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Der Datenverkehr ist auf das für die Funktionen notwendige Maß zu beschränken.

Die Systeme im BRZ Trustcenter werden entweder offline betrieben oder mittels Firewall gegen unberechtigte Zugriffe geschützt. Die Verbindung von sicherheitskritischen Systemen erfolgt mit TLS authentisiert und verschlüsselt.

Online-Systeme (z.B.: OCSP-Responder, Verzeichnisdienst) sind von den internen Netzen durch Firewalls getrennt.

Sensible Daten und Dokumente, die über ungesicherte Netzwerke übertragen werden, werden durch ein vom System Security Officer genehmigtes Verschlüsselungsverfahren geschützt.
Kritische Systeme werden in eigenen virtuellen Netzen und geschützt durch Firewalls betrieben.

6.8 Zeitstempel

Datums- und Zeitinformationen werden aus zuverlässigen Zeitquellen abgeleitet. Bei Bedarf findet eine manuelle Kontrolle bzw. eine notwendige Korrektur statt.

Details über Datums- und Zeitinformationen sowie Beschreibungen der verwendeten Systeme sind im nicht-öffentlich zugänglichen CPS [CPS] beschrieben.

7. Zertifikatsprofil, Sperrlisten (CRL) und Online Statusabfragen (OCSP)

Folgende Tabellen zeigen eine Zusammenfassung der detaillierten Beschreibungen in [BRZ CA Profile].

In Fällen von Widersprüchen zwischen den Tabellen und [BRZ CA Profile] gilt die Information aus diesem Kapitel.

Für diesen Abschnitt gelten folgende Abkürzungen:

OEGV SCA	OESTERREICH.GV.AT StammCA (RootCA)
OEGV SCA OCSP	OESTERREICH.GV.AT StammCA (RootCA) OCSP Signer
OEGV ACA	OESTERREICH.GV.AT Authentifzierung (SubCA)
OEGV ACA OCSP	OESTERREICH.GV.AT Authentifzierung (SubCA) OCSP Signer
OEGV OEAPP CLIENT	OESTERREICH.GV.AT oeAPP TLS-Client

7.1 Zertifikatsprofil

Der Aufbau der erstellten und ausgegebenen Zertifikate basiert auf dem internationalen Standard X.509 [X.509]. Die nachfolgende Tabelle beschreibt die relevanten Zertifikatsfelder und erklärt deren Bedeutung:

Es wird 1 Stamm (SHA-384/ECDSA[43]) analog zur BRZ CA definiert. Das Zertifikatsprofil ist in folgender Tabelle zusammengefasst:

[43] ECDSA – Elliptic Curve Digital Signature Algorithm

7.1.1 Stamm 1 – SHA-384/ECDSA

Verwendetes Zertifikatsprofil

Die Seriennummern für die von den CAs (RootCA, SubCA) der OESTERREICH.GV.AT-erstellten Zertifikate werden mit kryptografisch sicheren Zufallszahlengeneratoren erstellt. Jede generierte Seriennummer ist größer als 0 (null) und muss mindestens 60 bit Länge besitzen und die Quelle basiert auf einem kryptografisch sicheren Zufallsgenerator und ist für jeden Aussteller einmalig sowie eineindeutig[44].

	OEGVAT PKI RootCA (SHA-384/ECDSA) (OEGV SCA)	**OEGVAT PKI RootCA OCSP Signer (OEGV SCA OCSP)**	**OEGVAT PKI SubCA (SHA-384/ECDSA) (OEGV ACA)**	**OEGVAT PKI SubCA OCSP Signer (OEGV ACA OCSP)**	**OEGVAT PKI EndEntity (OEGV OEAPP CLIENT)**
Verwendung	CA-Zertifikat	Signatur von OCSP Responses	CA-Zertifikat	Signatur von OCSP Responses	End-Entity-Zertifikat
Version	v3	v3	v3	v3	v3
SerialNumber	60 bit, Zufallszahl	60 bit, Zufallszahl	60 bit, Zufallszahl	60 bit, Zufallszahl	60 bit, Zufallszahl
Signaturalgorithmus	ecdsa-with-SHA384 (1.2.840.10045.4.3.3)	ecdsa-with-SHA384 (1.2.840.10045.4.3.3)	ecdsa-with-SHA384 (1.2.840.10045.4.3.3)	ecdsa-with-SHA384 (1.2.840.10045.4.3.3)	ecdsa-with-SHA384 (1.2.840.10045.4.3.3)
Aussteller	siehe Antragsteller	OEGV SCA	OEGV SCA	OEGV ACA	OEGV ACA
Gültigkeitsdauer	12 Jahre (4 382 Tage) (ASN.1 UTCTime)	15 Monate (458 Tage) (ASN.1 UTCTime)	12 Jahre (4 382 Tage) 31.12.2031 (ANS.1 UTCTime)	7 Tage (ASN.1 UTCTime)	oeAPP: maximal 6 Monate (183 Tage) (ASN.1 UTCTime)
Verwendungsdauer	7 Jahre für die Ausstellung von SubCA-Zertifikaten 12 Jahre für die Ausstellung von OCSP-Signer-Zertifikaten	1 Jahr	7 Jahre für die Ausstellung von Binding-Zertifikaten 12 Jahre für die Ausstellung von OCSP-Signer-Zertifikaten	1 Tag	Maximal 6 Monate für Handy-Signatur Authentifizierung Maximal 3 Monate für eIDAS (EU) Authentifizierung

[44] eineindeutig – eine bijektive Funktion d.h.: eine umkehrbar eindeutige Funktion

	OEGVAT PKI RootCA (SHA-384/ECDSA) (OEGV SCA)	OEGVAT PKI RootCA OCSP Signer (OEGV SCA OCSP)	OEGVAT PKI SubCA (SHA-384/ECDSA) (OEGV ACA)	OEGVAT PKI SubCA OCSP Signer (OEGV ACA OCSP)	OEGVAT PKI EndEntity (OEGV OEAPP CLIENT)
Antragsteller **(s. *Abschnitt 3.1*)**	CN=Republik-Oesterreich-StammCA-01 O=Republik Oesterreich (vertreten durch BKA und BMDW) C=AT alle RDN: ASN.1 PrintableString	CN=Republik-Oesterreich-StammCA-01-OCSP-Responder O=Republik Oesterreich (vertreten durch BKA und BMDW) C=AT alle RDN: ASN.1 PrintableString	CN=Republik-Oesterreich-Authentifizierung-01 O=Republik Oesterreich (vertreten durch BKA und BMDW) C=AT alle RDN: ASN.1 PrintableString	CN=Republik-Oesterreich-Authentifizierung-OCSP-01-Responder -01 O=Republik Oesterreich (vertreten durch BKA und BMDW) C=AT alle RDN: ASN.1 PrintableString	Siehe Abschnitt 3.1.1 alle RDN: ASN.1 PrintableString wenn ausreichend; UTF8String sonst
Öffentlicher Schlüssel	ECDSA 384 Bit NIST-Kurve P-384 OID 1.2.840.10045.2.1 (id-ecPublicKey) AlgorithmIdentifier-Feld: secp384r1 1.3.132.0.34	ECDSA 384 Bit NIST-Kurve P-384 OID 1.2.840.10045.2.1 (id-ecPublicKey) AlgorithmIdentifier-Feld: secp384r1 1.3.132.0.34	ECDSA 384 Bit NIST-Kurve P-384 OID 1.2.840.10045.2.1 (id-ecPublicKey) AlgorithmIdentifier-Feld: secp384r1 1.3.132.0.34	ECDSA 384 Bit NIST-Kurve P-384 OID 1.2.840.10045.2.1 (id-ecPublicKey) AlgorithmIdentifier-Feld: secp384r1 1.3.132.0.34	ECDSA 256 Bit, NIST-Kurve P-256 OID 1.2.840.10045.2.1 (id-ecPublicKey) AlgorithmIdentifier-Feld: secp256r1 1.2.840.10045.3.1.7
Zertifikatserweiterungen					
Zertifizierungsrichtlinie (CertificatePolicies)	non-critical 1.2.40.0.10.1.13.1	non-critical 1.2.40.0.10.1.13.1	non-critical 1.2.40.0.10.1.13.1	non-critical 1.2.40.0.10.1.13.1	non-critical 1.2.40.0.10.1.13.1
Basiseinschränkungen (BasicConstraints)	critical cA=true; pathLength nicht limitiert	nicht vorhanden	critical cA=true; pathLength nicht limitiert	nicht vorhanden	nicht vorhanden
Schlüsselkennung des Antragstellers (SubjectKey Identifier)	non-critical	non-critical	non-critical	non-critical	non-critical
Schlüsselkennung des Ausstellers (AuthorityKey Identifier)	non-critical mit Attribut `keyIdentifier`	non-critical mit Attribut `keyIdentifier`	non-critical mit Attribut `keyIdentifier`	non-critical mit Attribut `keyIdentifier`	non-critical mit Attribut `keyIdentifier`
Key Usage	critical keyCertSign,	critical digitalSignature	critical keyCertSign	critical digitalSignature	critical OEAPP CLIENT: digitalSignature
Extended Key Usage	nicht vorhanden	critical id-kp-OCSPSigning	nicht vorhanden	critical id-kp-OCSPSigning	critical OEAPP CLIENT: id-kp-clientAuth
CRL Distribution Points	nicht vorhanden	nicht vorhanden	nicht vorhanden	nicht vorhanden	nicht vorhanden
Authority Information Access	nicht vorhanden	nicht vorhanden	non-critical `accessMethod id-ad-ocsp (http)`	nicht vorhanden	non-critical `accessMethod id-ad-ocsp (http)`
NoCheck	nicht vorhanden	non-critical	nicht vorhanden	non-critical	nicht vorhanden
Alternativer Antragstellername (SubjectAlternative Name)	nicht vorhanden	nicht vorhanden	nicht vorhanden	nicht vorhanden	non-critical OEAPP CLIENT (optional) dNSName, iPAddress, rfc822Name

7.2 Sperrlistenprofil (CRL)

7.2.1 Stamm 1 – SHA-384/ECDSA

Nicht anwendbar.

7.3 OCSP-Request/Response Profil

Der OCSP Responder berücksichtigt die Vorgaben von [IETF RFC6960]. Das Zertifikat des OCSP-Responders wird von der jeweiligen CA (d.h. RootCA, SubCA) ausgestellt, welche die OCSP-Information bereitstellt. Das bedeutet, dass das Zertifikat des OCSP-Responders mit demselben Schlüssel signiert wird, mit dem auch die End-Entity-Zertifikate unterzeichnet werden, für welche der OCSP-Responder die notwendigen Widerrufsstatusinformationen über das Internet bereitstellt.

Der `OCSPRequest` MUSS vom Client NICHT signiert werden. Eine etwaige im `OCSPRequest` enthaltene Signatur wird vom OCSP-Responder nicht geprüft.

Ein `OCSPRequest` DARF AUSSCHLIEßLICH den Status von Zertifikaten einer CA abfragen. Die `OCSPResponse` wird in Folge vom zugehörigen OCSP-Signer dieser CA laut folgenden Tabellen signiert:

	OEGVAT PKI **RootCA OCSP- Response**
Signaturalgorithmus	**ecdsa-with-SHA384** **(1.2.840.10045.4.3.3)**

	OEGVAT PKI **SubCA OCSP- Response**
Signaturalgorithmus	**ecdsa-with-SHA384** **(1.2.840.10045.4.3.3)**

8. Konformitätsprüfung (Compliance Audit, Assessments)

Audits werden für regelmäßige Überprüfungen auf die Einhaltung der sich aus den rechtlichen Rahmenbedingungen, relevanten internationalen Standards durchgeführt. Durchgeführt werden diese im Einklang mit dem Dokument *„BRZ Trustcenter Allgemeine Sicherheitsrichtlinie“* [BRZ ASRL TC], nach der vorliegenden CP sowie dem nicht öffentlich zugänglichen CPS [CPS].

Durchführung von internen Audits

Interne Audits zur Qualitätssicherung finden im Trustcenter der BRZ GmbH jährlich nach Abstimmung mit dem Auftraggeber (BMDW) statt.

Durchführung von externen Audits

Externe Audits werden in Abstimmung mit dem Auftraggeber (BMDW) durchgeführt.

Aufzeichnungen und Protokollierungen für Überprüfungen

Der sichere Betrieb der Systeme im BRZ Trustcenter wird ergänzt durch die vollständige Aufzeichnung aller sicherheitsrelevanten Aktivitäten – inklusive dem zugehörigen Zeitpunkt und involvierten Personen in elektronischen und papierbasierten Protokollen.

Der durch die Protokollierung erzeugte Audit Trail ist geeignet für nachträgliche Compliance Audits der Systeme. Diese Audits dienen der Überprüfung der definierten Zertifizierungs- und Sicherheitsrichtlinien bzw. dem Sicherheitskonzept von OESTERREICH.GV.AT und der Integrität der betroffenen kryptografischen Objekte.

Regelmäßige Überprüfungen finden jährlich statt.

Ad-hoc-Überprüfungen werden bei Bedarf (z.B.: bei gravierenden technischen Änderungen) angeordnet.

Die Behebung von Mängeln erfolgt risikobasiert oder zeitnah.

9. Andere geschäftliche und rechtliche Angelegenheiten

9.1 Gebühren

Gebühren zwischen Auftraggeber (BMDW) und BRZ GmbH

Gebühren und/oder Honorare zwischen Auftraggeber (BMDW) und dem BRZ Trustcenter sind in den zugrundeliegenden Projekt- und Betriebsvereinbarungen definiert.

Gebühren für Antragsteller, Zertifikatsnehmer und End-Entities

Die Gebühren sind in diesem Abschnitt und in den folgenden Unterabschnitten sowie in den Nutzungsbedingungen[45] von OESTERREICH.GV.AT festgelegt.

Darüber hinaus gibt es keine weiteren Vereinbarungen über Gebühren.

9.1.1 Gebühren für die Ausstellung, die Erneuerung oder den Widerruf von Zertifikaten

Nicht anwendbar.

9.1.2 Gebühren für den Abruf bzw. den Zugriff auf Zertifikate

Nicht anwendbar.

9.1.3 Gebühren für den Abruf bzw. den Zugriff auf Sperrlisten oder Statusinformationsdienste

Nicht anwendbar.

9.1.4 Gebühren für weitere Dienstleistungen

Nicht anwendbar.

9.2 Finanzielle Verantwortung

Finanzielle Aspekte zwischen Auftraggeber und dem BRZ Trustcenter sind in den zugrundeliegenden Projekt- und Betriebsverträgen definiert. Darüber hinaus gibt es keine weiteren Vereinbarungen.

Risiken, welche aus der Haftung für die CA der OESTERREICH.GV.AT-PKI entstehen, sind im Betriebsvertrag zwischen der BRZ GmbH und dem Auftraggeber (BMDW) definiert.

9.3 Vertraulichkeit von Geschäftsinformationen

Die OESTERREICH.GV.AT-PKI wird im BRZ Trustcenter betrieben und stellt Binding-Zertifikate aus.

Die Binding-Zertifikate enthalten keine personenbezogenen Daten.

9.4 Schutz personenbezogener Daten

Die Erfassung, die Verarbeitung, die Speicherung, die Übertragung und die Löschung von personenbezogenen Daten unterliegt den geltenden Datenschutzbestimmungen[46,47].

Darüber hinaus hat die OESTERREICH.GV.AT-PKI ein Datenschutzkonzept definiert.

---

[45] Abrufbar: https://www.oesterreich.gv.at/ app-digitales-amt/nutzungsbedingungen

[46] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)

[47] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Alle Informationen und Daten, die in erstellten und ausgegebenen (i.e. veröffentlichten) Zertifikaten bzw. Sperrlisten explizit (z.B. E-Mail-Adresse) oder implizit (z.B. Zertifizierungsdaten) angegeben und daher enthalten sind oder eine Ableitung möglich ist, sind nicht vertraulich.

9.5 Urheberrechte

Die vorliegende CP ist urheberrechtlich geschützt. Daher ist eine Verwendung von (z.B.: ausgewählten) Textteilen, enthaltenen Abbildungen oder Abschnitten ausnahmslos nur nach ausdrücklicher schriftlicher Einverständniserklärung durch die OESTERREICH.GV.AT-PKI (z.B.: durch den Auftraggeber, BMDW) erlaubt.

Die OESTERREICH.GV.AT-PKI überträgt die Nutzungsrechte für die ausgestellten und die ausgegebenen Binding-Zertifikate an die End-Entities.

9.6 Verpflichtungen

Keine weiteren Verpflichtungen definiert.

9.7 Gewährleistung

Regelungen über die Gewährleistung sind in den Nutzungsbedingungen definiert.

9.8 Haftungsbeschränkung

Generelle Informationen zur Haftung sowie über relevante Haftungsbeschränkungen sind in den Nutzungsbedingungen definiert. Die Nutzungsbedingungen[48] sind auf der Webseite[49] von OESTERREICH.GV.AT abrufbar.

9.9 Haftungsfreistellung

Nicht anwendbar.

9.10 Inkrafttreten und Aufhebung

Eine neue Version dieser CP tritt unmittelbar nach der Freigabe durch den Auftraggeber in Kraft und hebt eine vorherige Version unverzüglich auf.

Diese CP ist öffentlich und über eine TLS geschützte Verbindung über das Internet verfügbar[50].

Eine Aufhebung einer CP ist ausschließlich durch die Freigabe einer neuen Version oder nach Beendigung des Service der OESTERREICH.GV.AT-PKI möglich.

---

[48] Abrufbar: https://www.oesterreich.gv.at/ app-digitales-amt/nutzungsbedingungen

[49] Abrufbar: https://www.oesterreich.gv.at

[50] Abrufbar: https://www.oesterreich.gv.at/ app-digitales-amt/sicherheitsinformationen

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmenden

Rechtlich bindende Kommunikation MUSS schriftlich (z.B. per E-Mail, per Brief) erfolgen und der Empfang MUSS vom Kommunikationspartner schriftlich bestätigt werden. Kommunikation sicherheitskritischer Informationen MUSS bei elektronischer Übertragung verschlüsselt erfolgen.

9.12 Änderungen der Richtlinie

Diese CP wird aktualisiert, wenn technische, organisatorische oder rechtliche Anforderungen oder darauf basierende Änderungen dies erfordern.

9.13 Konfliktbeilegung

Sämtliche Beschwerden, Konflikte oder über die Einhaltung und die damit verbundene Umsetzung der Certificate Policy sind an die BRZ GmbH in schriftlicher Form zu übermitteln.

9.14 Geltendes Recht

Der Gerichtsstand ist Wien/Österreich. Es gilt ausnahmslos österreichisches Recht.

9.15 Konformität mit geltendem Recht

Nicht anwendbar.

9.16 Allgemeine Bestimmungen

Die OESTERREICH.GV.AT-PKI stellt sicher, dass dem Zertifikatsinhaber alle sich aus den in dieser CP aufgelisteten Anforderungen in geeigneter Form zur Kenntnis gebracht werden und die Erfüllung dieser Vereinbarungen vertraglich festgelegt wird.

Die OESTERREICH.GV.AT-PKI ist für die Einhaltung aller in diesem Dokument beschriebenen Prozesse, Methoden und Verfahren zuständig und dafür verantwortlich.

9.17 Andere Regelungen

Wenn Teile dieser CP unwirksam oder undurchführbar sind, unzutreffend sind, ungültig oder sich rechtliche Bestimmungen (z.B.: Verordnungen oder Gesetze) ändern, welche die Teile dieser CP betreffen, bleiben die anderen Teile dieser CP in Kraft.

Darüber hinaus sind keine anderen Regelungen festgelegt.