

Zertifizierungsrichtlinie für Endnutzungszertifikate

Certification Practice Statement (CPS)

GB_BE-BTS4- Pfaffenbichler Franz Xaver, SDS1-Team

Kurzbeschreibung

Das Dokument beschreibt die Zertifizierungsrichtlinien für alle Zertifikate unter dem Zwischenzertifikat „Benutzer CA #“ (das betrifft Endnutzungszertifikate der Stadt Wien). # steht für die jeweilige CA Generation.

Klassifizierung

Vertraulichkeit der Unterlage siehe Fußzeile.

Inhalt

1. Einführung	10
1.1. Überblick	10
1.2. Dokumentenbezeichnung und Identifikation	10
1.3. Teilnehmende Parteien	10
1.3.1. Zertifizierungsdiensteanbieter (ZDA)	11
1.3.2. Registrierungsstelle (RA, Registration Authority)	11
1.3.3. Antragsteller (Zertifikatsinhaber)	11
1.3.4. Vertrauende Parteien	11
1.3.5. Weitere Teilnehmende des Vertrauensnetzwerks	11
1.4. Zertifikatsverwendung	12
1.4.1. Zulässige Zertifikatsverwendung	12
1.4.2. Ausgeschlossene Zertifikatsverwendung	12
1.5. Administration der Anwendungsvorgaben (Policy)	12
1.5.1. Verantwortliche Organisation für die Dokumentpflege	12
1.5.2. Kontaktperson	12
1.5.3. Die Vorgaben (Policy) verfassenden Personen	13
1.5.4. Prozeduren zur Freigabe der Vorgaben (Policy)	13
2. Veröffentlichung und Datenspeicherung	14
2.1. Datenspeicherung	14
2.2. Veröffentlichung der Zertifikatsinformationen	14
2.3. Zeitpunkt und Intervalle der Ausstellung	14
2.4. Zugriffslimitierungen der Datenspeicherung	14
3. Identifikation und Authentisierung	15
3.1. Benennungsmerkmale	15
3.1.1. Subjektidentifikation	15
3.1.2. Notwendigkeit für aussagekräftige Bezeichnungen	15

3.1.3.	Anonymität oder Pseudonymverwendung der Zertifikatsinhabenden Personen	15
3.1.4.	Regelungen zur Namensinterpretation	15
3.1.5.	Einzigartigkeit der Bezeichnungen	15
3.1.6.	Erkennbarkeit, Authentifizierung und die Rolle von Markenbezeichnungen	16
3.2.	Initiale Überprüfung der Identität	16
3.2.1.	Methode zum Beweis des Schlüsselbesitzes	16
3.2.2.	Authentisierung einer Juristischen Person.....	16
3.2.3.	Authentisierung einer natürlichen Person.....	16
3.2.4.	Nicht verifizierte Antragsinformationen.....	17
3.2.5.	Überprüfung der rechtmäßigen Antragsstellung	17
3.2.6.	Kriterien der Interoperabilität	17
3.3.	Identifikation und Authentisierung für Schlüsselwiederverwendung	17
3.3.1.	Identifikation und Authentisierung für Routine Schlüsselwiederverwendung	17
3.3.2.	Identifikation und Authentisierung für Routine Schlüsselwiederverwendung nach Widerruf	17
3.4.	Identifikation und Authentisierung für Sperr- bzw. Widerrufs Antrag	18
4.	Operative Vorgaben des Zertifikats-Lebenszyklus.....	19
4.1.	Zertifikatsantrag	19
4.1.1.	Wer kann einen Zertifikatsantrag stellen?	19
4.1.2.	Ausstellungsprozess und Verantwortlichkeiten	19
4.2.	Zertifikatsantragsfunktionen	19
4.2.1.	Identifikation und Authentisierung.....	19
4.2.2.	Akzeptieren oder Ablehnen eines Antrags	19
4.2.3.	Dauer der Abwicklung eines Antrags	20
4.3.	Zertifikatsausstellung.....	20
4.3.1.	Detailfunktionen der CA bei Ausstellung.....	20
4.3.2.	Benachrichtigung des Zertifikatsinhabers durch CA.....	20
4.4.	Erstmalige Zertifikatsnutzung	20
4.4.1.	Beidseitiges Einverständnis zur Zertifikatsnutzung.....	20
4.4.2.	Veröffentlichung der Zertifikate durch die CA	21
4.4.3.	Bekanntgabe der Veröffentlichung an andere Stellen.....	21
4.5.	Schlüsselpaar und Zertifikatsverwendung.....	21
4.5.1.	Schlüsselerzeugung und Zertifikatsgeltungsbereich des Antragstellenden Person	21
4.5.2.	Akzeptanz des Öffentlichen Schlüssels und komplementierender Zertifikatsverwendung	21
4.6.	Zertifikatserneuerung	21
4.6.1.	Umstände einer Zertifikatserneuerung.....	21
4.6.2.	Wer darf eine Zertifikatserneuerung beantragen?	22
4.6.3.	Abläufe der Zertifikatserneuerung	22
4.6.4.	Benachrichtigung der Antragstellenden Person über die Zertifikatserneuerung.....	22
4.6.5.	Einverständnis der Zertifikatserneuerung.....	22

4.6.6.	Veröffentlichung eines erneuerten Zertifikats durch die CA	22
4.6.7.	Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung	22
4.7.	Zertifikatserneuerung mit neuem Schlüsselpaar	22
4.7.1.	Umstände einer Schlüsselneugenerierung.....	22
4.7.2.	Wer darf eine Schlüsselneugenerierung beantragen?	23
4.7.3.	Abläufe der Schlüsselneugenerierung	23
4.7.4.	Benachrichtigung über die Neuausstellung	23
4.7.5.	Einverständnis der Neuausstellung mit neuem Schlüssel	23
4.7.6.	Veröffentlichung eines erneuerten Zertifikats durch die CA	23
4.7.7.	Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung	23
4.8.	Zertifikatsmodifikation	23
4.8.1.	Umstände einer Zertifikatsmodifikation	23
4.8.2.	Wer darf eine Zertifikatsmodifikation beantragen	23
4.8.3.	Abläufe zur Beantragung einer Zertifikatsmodifikation	24
4.8.4.	Benachrichtigung über die Zertifikatsneuausstellung	24
4.8.5.	Einverständniserklärung einer Neuausstellung.....	24
4.8.6.	Veröffentlichung eines modifizierten Zertifikats durch die CA	24
4.8.7.	Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung	24
4.9.	Zertifikatswiderruf und Sperre.....	24
4.9.1.	Umstände eines Widerrufs	24
4.9.2.	Wer kann einen Widerruf beantragen?	24
4.9.3.	Prozeduren der Widerrufsanhträge.....	25
4.9.4.	Durchführungszeit eines Widerrufs.....	25
4.9.5.	Zeitspanne der technischen Prozesse eines Widerrufs.....	25
4.9.6.	Zulässigkeit der Sperrinformationen für vertrauende Instanzen	25
4.9.7.	Sperrlisten Aktualisierungsfrequenz	26
4.9.8.	Maximale Latenz für Sperrlisten.....	26
4.9.9.	Online Widerruf- und Sperrprüfungs-Möglichkeiten	26
4.9.10.	Online Widerruf- und Sperrprüfungsvoraussetzungen	26
4.9.11.	Andere Möglichkeiten Sperrinformationen abzurufen.....	26
4.9.12.	Spezielle Vorgaben bei einer Kompromittierung einer Zertifikatserneuerung	26
4.9.13.	Umstände einer Sperre	26
4.9.14.	Wer kann eine Sperre beantragen?	26
4.9.15.	Abläufe zur Durchführung einer Sperre.....	27
4.9.16.	Begrenzungen der Sperrdauer	27
4.10.	Zertifikatsstatus Services	27
4.10.1.	Operative Eigenschaften	27
4.10.2.	Serviceverfügbarkeit	27
4.10.3.	Optionale erweiterte Services.....	27

4.11. Ablauf der Gültigkeit	27
4.12. Schlüssel hinterlegung und Wiederherstellung	27
4.12.1. Schlüssel hinterlegung und Wiederherstellungsvorgaben und Praktiken	28
4.12.2. Sitzungsschlüssel Aufbewahrung und Wiederherstellungsvorgaben und Praktiken	28
5. Liegenschaften, Management, und operative Kontrollen	29
5.1. Physikalische Kontrollen	29
5.1.1. Liegenschaft(en) und bauliche Maßnahmen	29
5.1.2. Physischer Zugang	29
5.1.3. Strom und Luftzirkulation	29
5.1.4. Wasserschäden	29
5.1.5. Brandvorbeugung und Brandbekämpfung	29
5.1.6. Datenspeicherung	30
5.1.7. Abfallentsorgung	30
5.1.8. Off-site Backup	30
5.2. Kontrollprozeduren	30
5.2.1. Vertrauenswürdige Rollen	30
5.2.2. Anzahl der Personen je Rollentätigkeit	31
5.2.3. Identifikation und Authentifizierung am System	31
5.2.4. Rollen mit getrennten Aufgaben	31
5.3. Personelle Kontrollen	31
5.3.1. Qualifikation, Erfahrung und Anforderungen an die Tauglichkeit der Rollen	31
5.3.2. Prozeduren zur Eignungsüberprüfung	32
5.3.3. Trainingsvorgaben	32
5.3.4. Weiterführende Trainings und Anforderungen der Fortbildung	32
5.3.5. Arbeitsaufgaben - Veränderungsanforderungen	32
5.3.6. Sanktionen für unautorisiertes Vorgehen	32
5.3.7. Anforderungen an Zulieferer und Vertragsparteien	32
5.3.8. Dokumentation für das Personal	32
5.4. Überwachungsprozeduren	33
5.4.1. Typen der aufzuzeichnenden Aktivitäten und Ereignisse	33
5.4.2. Intervalle der Logfile-Überprüfung	33
5.4.3. Aufbewahrung der Logfiles	33
5.4.4. Zugriffsschutz der Logfiles	33
5.4.5. Logfiles-Sicherungsprozeduren	33
5.4.6. Systemüberwachung	33
5.4.7. Automatische Benachrichtigungen über Ereigniseinträge	33
5.4.8. Verwundbarkeitseinschätzungen	34
5.5. Aufzeichnungsarchiv	34
5.5.1. Typen der zu archivierenden Daten	34

5.5.2.	Aktualisierungsintervalle der Archive und Überprüfung	34
5.5.3.	Schutz der Archivdaten	34
5.5.4.	Archiv-Sicherungsprozeduren	34
5.5.5.	Anforderung betreffend Zeitstempelverwendung	34
5.5.6.	Archiv-Sammel-Systeme	35
5.5.7.	Prozeduren zur Archiv-Verifikation	35
5.6.	Schlüsseltauschmechanismus	35
5.7.	Wiederherstellung nach Kompromittierung oder Disaster	35
5.7.1.	Notfallmaßnahmen und Kompromittierungsprozeduren	35
5.7.2.	Ausfall von Systemen, Software-Wiederherstellung und/oder korrumpierten Daten	35
5.7.3.	Kompromittierung privater Schlüssel der CA	36
5.7.4.	Fortführung des Betriebes nach Disaster	36
5.8.	Einstellung der CA oder RA Tätigkeit	36
6.	Technische Sicherheitskontrollen	37
6.1.	Schlüsselgenerierung und Installation	37
6.1.1.	Schlüsselgenerierung	37
6.1.2.	Übermittlung des Privaten Schlüssels an die Antragstellende Person	37
6.1.3.	Übermittlung des Öffentlichen Schlüssels an die Zertifizierungsinstanz	37
6.1.4.	Veröffentlichung der Öffentlichen Schlüssel an weitere Instanzen	37
6.1.5.	Schlüssellängen	38
6.1.6.	Schlüsselgenerierung, Schlüsselparameter und Qualitätssicherung	38
6.1.7.	Zwecke der Schlüsselverwendung (nach dem Standard X.509 v3 und entsprechender Feldbezeichnung)	38
6.2.	Schutz der privaten Schlüssel und Mechanismen zur korrekten Verwendung der kryptografischen Anwendungen	38
6.2.1.	Standards der Kryptografischen Module und deren Verwendung	38
6.2.2.	Generierung privater Schlüssel (n out of m) Mehrfach-Personen-Kontrolle	39
6.2.3.	Schlüsselhinterlegung des privaten Schlüssels	39
6.2.4.	Sicherung der privaten Schlüssel	39
6.2.5.	Archivierung der privaten Schlüssel	39
6.2.6.	Übermittlung privater Schlüssel in oder aus dem Kryptografischen Modul (HSM)	39
6.2.7.	Unterbringung der privaten Schlüssel im Kryptografischen Modul (HSM)	39
6.2.8.	Methode zur Aktivierung der privaten Schlüssel	39
6.2.9.	Methode zur Deaktivierung der privaten Schlüssel	40
6.2.10.	Methode der kontrollierten Zerstörung der privaten Schlüssel	40
6.2.11.	Einstufung der Sicherheit des kryptografischen Moduls (HSM)	40
6.3.	Weitere Aspekte des Schlüsselmanagements	40
6.3.1.	Archivierung der öffentlichen Schlüssel	40
6.3.2.	Zertifikatsgültigkeiten und operative Schlüsselverwendungszeiträume	40
6.4.	Aktivierungsdaten	40

6.4.1.	Aktivierungsdaten Generierung und Installation	40
6.4.2.	Schutz der Aktivierungsdaten	41
6.4.3.	Weitere Aspekte der Verwendung von Aktivierungsdaten	41
6.5.	Computer Sicherheitsvorgaben	41
6.5.1.	Spezifische technische Anforderungen an Computersysteme	41
6.5.2.	Sicherheitseinstufung der Computer	41
6.6.	Technische Umgebungsparameter eines Systemzyklus	42
6.6.1.	Systemspezifische Entwicklungsumgebungen	42
6.6.2.	Verwaltung der Sicherheitsmaßnahmen	42
6.6.3.	Auflagen an die Verwaltung der Sicherheitsmaßnahmen	42
6.7.	Netzwerküberwachung	42
6.8.	Zeitstempeldienste	42
7.	Zertifikats-, CRL und OCSP Profile	43
7.1.	Zertifikatsprofil	43
7.1.1.	Versions Nummer	43
7.1.2.	Zertifikatserweiterungen	43
7.1.3.	Algorithmen Objekt Unterscheider	43
7.1.4.	Namensformen	44
7.1.5.	Namenseinschränkungen	44
7.1.6.	Anwendungsvorgaben Unterscheider	44
7.1.7.	Verwendung von die Anwendungsvorgaben einschränkende Erweiterungen	44
7.1.8.	Anwendungsvorgaben Syntax	44
7.1.9.	Verarbeitung von kritischen Anwendungsvorgaben Erweiterungen	44
7.2.	Sperrlisten Profil	44
7.2.1.	Versionsnummern	44
7.2.2.	Sperrlisten und Sperrlisten Erweiterungen	45
7.3.	OCSP Profil	45
7.3.1.	Unterstützte Versionen	45
7.3.2.	OCSP Erweiterung	45
8.	Entsprechungen von Audit und anderen Kontrollvorgaben	46
8.1.	Intervalle und Umstände von Überprüfungen	46
8.2.	Auswahl und Qualifikation der überprüfenden Stellen	46
8.3.	Abhängigkeiten der überprüfenden Stellen	46
8.4.	Themenbereiche einer Überprüfung (Mindestanforderungen)	46
8.5.	Maßnahmen im Falle von Mängelfeststellungen	47
8.6.	Kommunikation der Überprüfungsergebnisse	47
9.	Kommerzielle und gesetzliche Vorgaben	48
9.1.	Gebühren	48

9.1.1.	Gebühren zur Zertifikatsausstellung	48
9.1.2.	Zertifikatsverwendungsgebühren	48
9.1.3.	Gebühren zur Abfrage von Statusinformationen	48
9.1.4.	Sonstige Gebühren	48
9.1.5.	Refundierung von Gebühren	48
9.2.	Finanzielle Verantwortung	48
9.2.1.	Versicherungsschutz durch Dritte	48
9.2.2.	Weitere Regelungen	48
9.2.3.	Haftbarkeiten für weitere Zertifikatsteilnehmer	49
9.3.	Vertraulichkeitspflichten	49
9.3.1.	Geltungsbereich von vertraulichen Informationen	49
9.3.2.	Informationen die als nicht vertraulich gelten	49
9.3.3.	Verantwortung zum Schutz vertraulich geltender Daten	49
9.4.	Schutz persönlicher Informationen	49
9.4.1.	Datenschutzvorgaben	49
9.4.2.	Schützenswerte Daten	49
9.4.3.	Nichtschützenswerte Daten	49
9.4.4.	Verantwortungen zum Schutz der privaten Daten	50
9.4.5.	Zustimmungsvereinbarungen und Akzeptanz der Anwendungsvorgaben	50
9.4.6.	Einsichtsgewährung für allgemein überprüfende oder juristische Instanzen	50
9.4.7.	Weitere Umstände der Einsichtnahme	50
9.5.	Rechtswirksamkeit Geistiges Eigentum	50
9.6.	Vertretungsbefugnisse, Repräsentanzen und Garantien	50
9.6.1.	CA Repräsentanz und Garantien	50
9.6.2.	RA Repräsentanz und Garantien	51
9.6.3.	Zertifikatsinhaber Repräsentanz und Garantien	51
9.6.4.	Zustimmung Vertrauender Parteien des Zertifizierungsdienstes (Akzeptanzstellen)	51
9.6.5.	Weitere Regelungen	51
9.7.	Erklärungsbestimmungen	51
9.8.	Einschränkungen der Verantwortlichkeit	52
9.9.	Entschädigungen	52
9.10.	Inkrafttreten und Einstellung der Wirksamkeit der CPS	52
9.10.1.	Inkrafttreten	52
9.10.2.	Einstellung der Wirksamkeit	52
9.10.3.	Regelungen bei Einstellung der Wirksamkeit	52
9.10.4.	Effekte bei Einstellung der Wirksamkeit	52
9.11.	Individuelle Benachrichtigungen und Kommunikationsformen der Beteiligten	52
9.12.	Korrekturen	52
9.12.1.	Prozesse zur Einpflege von Korrekturen	52

9.12.2.	Bekanntmachungsmechanismen	53
9.12.3.	Umstände für eine Änderung der OID	53
9.13.	Schlichtungsbestimmungen	53
9.14.	Geltende Rechtslage	53
9.15.	Einhaltung der existierender Rechtslage	53
9.16.	Weitere Bestimmungen	53
9.16.1.	Allgemeine Vereinbarungen	53
9.16.2.	Zutreffende Aufgabenstellungen	53
9.16.3.	Salvatorische Klausel	53
9.16.4.	Klagbarkeit	54
9.16.5.	Höhere Gewalt	54
	Sonstige Bestimmungen	54
10. Anhang A	55
10.1.	Zertifikatsprofile	55
10.1.1.	Stadt Wien Root CA	55
10.1.2.	Stadt Wien Benutzer CA	57
10.1.3.	Benutzer Zertifikate	58
10.1.4.	Gemeinderat Zertifikate	60
11. Abkürzungsverzeichnis / Erläuterungen	63
12. Linkverzeichnis	64
13. Versionshistorie	64

1. Einführung

1.1. Überblick

Das Ziel dieses Dokuments ist es, die Anwendungsvorgaben für die vom Magistrat der Stadt Wien ausgestellten Zertifikate verbindlich zu beschreiben und im Sinne einer Zertifizierungsrichtlinie die Maßnahmen des sicheren und zuverlässigen Betriebes der technischen Einrichtung darzustellen.

Darunter fallen

- die Authentifizierung der Zertifikatsinhabende Personen
- die Identifikation derselben
- die technische Art und Weise wie diese durchgeführt wird
- ebenso die technischen Vorgaben, die zur sicheren Verwahrung und Anwendung der verwendeten Schlüssel zu verstehen sind
- wie die Widerrufe durchgeführt und die Sperrlisteninformationen systematisch abgerufen werden können.

Dieses Dokument soll zu einer transparenten und sicheren Anwendung aller involvierten Parteien beitragen und stellt die aktuell gültige Fassung der rechtlich verbindlichen Absichtserklärung des Magistrats der Stadt Wien dar.

Mit diesen Anwendungsvorgaben werden Varianten von Zertifikaten die zur Ausstellung gelangen beschrieben. Sofern nicht explizit in Identifikation, Mechanismus der Ausstellung, usw. unterschieden wird, gilt die beschriebene Regelung.

Die Beschreibungen in diesem Dokument entsprechen den Empfehlungen der IETF (Internet Engineering Task Force) RFC-3647 für die Dokumentation einer Zertifikatspolizze (Anwendungsvorgaben für ausstellende Personen, Zertifikatsinhabende Personen und alle akzeptierenden Parteien).

Anmerkung: Die Schlüsselwörter "MUSS", "DARF NICHT", "VERLANGT", "SOLLTE", "SOLLTE NICHT", "EMPFOHLEN", "KANN" und "OPTIONAL" sind wie in RFC 2119 der IETF zu interpretieren.

1.2. Dokumentenbezeichnung und Identifikation

Name: Zertifizierungsrichtlinie für Endnutzungszertifikate
(Certification Practice Statement)

Version: 1.0 - 31. Juli 2020

1.3. Teilnehmende Parteien

An dieser Stelle werden die einzelnen Teilnehmenden des Vertrauensnetzwerkes dargestellt und in den jeweiligen Rollen beschrieben. Es ergibt sich daraus ein Überblick über das gesamte System und den Kreis der Anwendenden.

1.3.1. Zertifizierungsdiensteanbieter (ZDA)

Der ZDA betreibt eine Zertifizierungsinstanz, deren Wurzelzertifikate öffentlich abgerufen werden. Dadurch können alle Zertifikate und darauf basierende Signaturen verifiziert werden. Die in diesem Dokument beschriebenen Zertifikate umfassen nach X.509 spezifizierte Zertifikate welche die folgenden erweiterten Schlüsselverwendungen enthalten:

- Client-Authentifizierung
- E-Mail-Sicherheit

Diese Zertifikate sind somit für einen sicheren Verbindungsaufbau bei sich gegenseitig authentifizierenden Systemen und zur Signatur von E-Mails geeignet.

1.3.2. Registrierungsstelle (RA, Registration Authority)

Der ZDA betreibt selbst eine Registrierungsstelle für die gegenständlichen Zertifikate. Diese ist in einer vom Betrieb des Zertifizierungsdienstes abgekoppelten Abteilung angesiedelt und agiert als eigene zu auditierende Organisationseinheit im Rahmen des Zertifizierungsdienstes.

Die RA identifiziert die einzelnen antragsstellenden Personen automatisch anhand der verwendeten Login Informationen und stellt die Zertifikate aus. Neben dem für die Zertifikatsinhabende Person selbständig durchführbaren Widerrufsdienst, werden durch die RA ebenfalls Sperren und Widerrufe durchgeführt.

Aktuell sind keine außerhalb des Magistrats der Stadt Wien autorisierten Registrierungsstellen aktiv.

1.3.3. Antragsteller (Zertifikatsinhaber)

Die zur Geltung kommenden Antragsstellenden Personen MÜSSEN juristische Personen sein, die in Form von natürlichen Personen die Anträge persönlich an die RA richten. D.h.: Es werden keine Maschinenzertifikate ausgestellt, die durch Automatismen vom Zertifizierungsdienst per Selbstabholung durchgeführt werden können.

Im Falle der positiven Erledigung der Identitätsüberprüfung und Zertifikatsausstellung wird aus der antragsstellenden Person eine Zertifikatsinhabende Person, der den gegenständlichen Anwendungsvorgaben unterliegt.

1.3.4. Vertrauende Parteien

Die Akzeptanz ist in keiner Weise auf Organisationen und Applikationen eingeschränkt.

1.3.5. Weitere Teilnehmende des Vertrauensnetzwerks

Derzeit gibt keinen weiteren Teilnahmekreis.

1.4. Zertifikatsverwendung

Die Verwendung der ausgestellten Zertifikate beschränkt sich auf die in den Zertifikaten beschriebenen Schlüsselverwendungen.

1.4.1. Zulässige Zertifikatsverwendung

Die damit erstellten Digitalen Signaturen sind ausschließlich als gültig anzusehen, wenn diese im Anwendungsumfeld der Stadt Wien durchgeführt wurden. Mit den zur Verfügung gestellten technischen Mitteln und unter Einhaltung der Arbeitsanweisungen der Stadt Wien sind die Signaturen und Kryptografischen Operationen von den Zertifikatsinhabenden Personen als gültig anzuerkennen.

Die Verwendung der zum Zertifikat gehörigen Schlüssel und das Vertrauen auf die Ausstellerinformationen sind ausschließlich für die Zertifikatsinhabende Person zulässig.

1.4.2. Ausgeschlossene Zertifikatsverwendung

Die Verwendung der Zertifikate für technische Operationen abseits der explizit aufgeführten Schlüsselverwendung ist nicht zulässig.

Zertifikate, deren Schlüssel in bzw. mit einem vermutlich kompromittierten System betrieben werden, DÜRFEN NICHT zur Anwendung gelangen.

In einem der Stadt Wien unbekannten und nicht explizit frei gegebenen Anwendungsumfeld sind die Signaturen und kryptografischen Operationen zu unterlassen und als ungültig anzusehen.

1.5. Administration der Anwendungsvorgaben (Policy)

Der Magistrat der Stadt Wien ist verantwortlich für die gegenständlichen Inhalte und deren Administration.

1.5.1. Verantwortliche Organisation für die Dokumentpflege

Dieses Dokument wird vom Magistrat der Stadt Wien aktuell gehalten und zur Verfügung gestellt.

1.5.2. Kontaktperson

Anfragen zum Dokument und die betreffenden Bereiche der Anwendungsvorgaben richten Sie bitte an:

Stadt Wien Trustcenter

E-Mail : ca@ma01.wien.gv.at

MA 01 - Wien Digital

Stadlauer Straße 54 und 56, 1220 Wien, Österreich

1.5.3. Die Vorgaben (Policy) verfassenden Personen

Der Magistrat der Stadt Wien und die rundQuadrat OG (in beratender Funktion) beschreiben den zur Anwendung kommenden Zertifizierungsdienst des Magistrats der Stadt Wien.

1.5.4. Prozeduren zur Freigabe der Vorgaben (Policy)

Die gegenständlichen Anwendungsvorgaben in Form dieses Dokuments werden in regelmäßigen Abständen kontrolliert und werden durch die internen Prozeduren, entsprechend dem ISMS (Informations-Sicherheits-Managements-Systems und dessen Policy) der Magistratsabteilung 01 der Stadt Wien (MA 01 - Wien Digital), freigegeben.

Die Policy für das ISMS der MA 01 - Wien Digital legt sicherheitsbezogene Ziele, Strategien, Verantwortlichkeiten und Methoden langfristig und verbindlich fest.

2. Veröffentlichung und Datenspeicherung

2.1. Datenspeicherung

Die von der beschriebenen PKI erzeugten und veröffentlichten Daten sind als Daten des Magistrats der Stadt Wien anzusehen und verlassen nicht deren Geltungsbereich. Diese Daten sind entsprechend der ISMS-Policy der MA 01 – Wien Digital, sicher verwahrt.

2.2. Veröffentlichung der Zertifikatsinformationen

Das Wurzelzertifikat und die Zertifikate der ausstellenden Zertifizierungsinstanzen, sowie die Sperrlisten und Zertifizierungsrichtlinien (CPS) des ZDA Magistrat der Stadt Wien kann auf den Seiten der Stadt Wien abgerufen werden.

Siehe : <https://www.wien.gv.at/kontakte/ma01/zertifikate.html>

Die ausgestellten Entitäten-Zertifikate (Endbenutzungszertifikate) werden ausschließlich in einem internen Verzeichnisdienst publiziert und verwaltet.

2.3. Zeitpunkt und Intervalle der Ausstellung

Zertifikate und Sperrlisten werden unmittelbar nach Ausstellung publiziert.

Die Sperrlisteninformationen werden einem Intervall von 1 Tag aktualisiert und sind 7 Tage gültig.

In den Sperrlisten (Certificate Revocation Lists) ist der Zeitpunkt der Gültigkeit der ausgestellten Sperrliste und der verbindliche Hinweis auf die nächste Sperrlistenaktualisierung enthalten.

2.4. Zugriffslimitierungen der Datenspeicherung

Da es sich um einen internen Nutzerkreis handelt sind die Endbenutzungszertifikate und die Sperrlisteninformation grundsätzlich nur innerhalb des Applikationsverbunds und somit innerhalb vertrauenswürdiger Netzwerkverbindungen abrufbar.

In bestimmten Fällen können die Daten auch öffentlich gemacht werden. Diese werden gesondert gekennzeichnet und in Abstimmung mit den Nutzerkreisen ausgewählt.

Alle Daten werden entsprechend der ISMS-Policy der MA 01 - Wien Digital vor Zerstörung, Verlust und Manipulation geschützt.

3. Identifikation und Authentisierung

Der Magistrat der Stadt Wien identifiziert selbst, bzw. beruft sich auf innerhalb der Organisation gebräuchliche Identifizierungsmaßnahmen bei der Überprüfung der Antragstellenden Person. (Z.B.: Portalidentifikation)

3.1. Benennungsmerkmale

3.1.1. Subjektidentifikation

Alle Zertifikate MÜSSEN einen DN (Distinguished Name) entsprechend den X.500 Standards erhalten. Dieser DN ist innerhalb der ausstellenden Instanz und deren Hierarchie einmalig.

Die Subjektbezeichnung von allen Zertifikaten MUSS folgende Felder beinhalten:

- Common Name (CN)
- Organisation (O=Stadt Wien)
- Organizational Unit (OU=Abteilung)
- Country (C=AT)

3.1.2. Notwendigkeit für aussagekräftige Bezeichnungen

DN Bezeichnungen MÜSSEN eindeutig und erkennbar sein. Die Erkennbarkeit muss dahingehend gewährleistet sein, dass die Person bzw. die Organisation, oder deren Untereinheit, ableitbar ist.

3.1.3. Anonymität oder Pseudonymverwendung der Zertifikatsinhabenden Personen

Informationen der innehabenden Person dürfen nicht durch den Zertifizierungsdiensteanbietende Stelle anonymisiert werden, eine Verwendung eines Pseudonyms durch den Antragsstellende Person ist ausgeschlossen. Im Falle einer zu langen Bezeichnung DARF abgekürzt werden.

3.1.4. Regelungen zur Namensinterpretation

Keine.

3.1.5. Einzigartigkeit der Bezeichnungen

Grundsätzlich KANN ein und dieselbe Subjektbezeichnung in mehreren Zertifikaten verwendet werden und muss nicht einzigartig sein. Sofern eine Namensgleichheit gegeben ist, KANN ein eindeutiger Unterscheider für die Subjekterkennung verwendet werden. Dieser ist für alle weiteren und Folgezertifikate wiederzuverwenden.

Das Recht, die Durchführung einer Verwendung, und die Kontrolle über diese Unterscheider liegen bei der Registrierungsstelle des ZDA.

3.1.6. Erkennbarkeit, Authentifizierung und die Rolle von Markenbezeichnungen

Die Registrierungsstelle ist nicht verpflichtet, bei den übermittelten Nutzerdaten eine Kontrolle über etwaige Markenrechtsverletzungen durchzuführen.

Die Antragsstellenden Personen verpflichten sich zur rechtlich korrekten Verwendung der übermittelten Daten.

3.2. Initiale Überprüfung der Identität

Die erstmalige Überprüfung aller Antragsstellenden Personen wird durch die korrekte Autorisierung am Portal der Stadt Wien durchgeführt. Das Portal ist als eine vertrauenswürdige Applikation zu interpretieren.

3.2.1. Methode zum Beweis des Schlüsselbesitzes

Der Nachweis des Schlüsselbesitzes wird durch die technischen Eigenschaften der asymmetrischen Kryptographie bewiesen.

Durch die Beantragung eines Zertifikats mit gleichzeitiger Übermittlung eines PKCS#10 Antrags zeigt die Antragsstellende Person, dass er die Kontrolle über das Schlüsselpaar hat.

In jedem anderen Falle der Ausstellung wird ein vom ZDA in sicherer Umgebung generiertes Schlüsselpaar übermittelt. Dieses ist durch ein Passwort geschützt, das von der Antragsstellenden Person selbst gewählt wurde.

3.2.2. Authentisierung einer Juristischen Person

Kommt nicht zur Anwendung.

3.2.3. Authentisierung einer natürlichen Person

Die übermittelten Portaldaten werden verwendet um im Magistrat der Stadt Wien internen LDAP-Verzeichnis weitere Merkmale auszulesen. Diese Daten sind als vertrauenswürdig zu interpretieren.

Ein Datensatz der aus dem LDAP-Verzeichnis ausgelesenen Informationen wird in der RA-eigenen Datenbank zur Nachvollziehbarkeit abgelegt.

3.2.4. Nicht verifizierte Antragsinformationen

Inhalte werden ergänzend aus dem als vertrauenswürdig einzustufenden LDAP-Verzeichnis geholt und gelten als verifiziert. Da die Antragsstellenden Person keine Zertifikatsdaten selbst eingeben kann, gibt es keine „nicht verifizierten“ Informationen der Antragsstellenden Person.

3.2.5. Überprüfung der rechtmäßigen Antragsstellung

Da es sich um interne Endnutzungszertifikate handelt, kommt dieser Bereich nicht zur Anwendung.

3.2.6. Kriterien der Interoperabilität

In technischer Hinsicht handelt es sich zur Gänze um eine Infrastruktur entsprechend dem X.509 Standard und somit ist eine Kompatibilität mit allen Applikationen, die diesen Standard unterstützen, gewährleistet.

Die Zertifizierungsinstanzen sind in keiner Weise auf eine hierarchische Interoperabilität mit anderen Zertifizierungsdiensten ausgelegt. D.h.: Es gibt keine rechtliche und technische Verbindlichkeit zu anderen Zertifizierungsdiensten abseits des Magistrats der Stadt Wien.

3.3. Identifikation und Authentisierung für Schlüsselwiederverwendung

Für die Ausstellung eines Zertifikats ist die Generierung eines neuen Schlüsselpaares notwendig. Bereits zertifizierte Schlüssel DÜRFEN NICHT zur Zertifikatsausgabe verwendet werden.

Die eingesetzten technischen Prozeduren garantieren die Nicht-Ausstellung eines bereits zertifizierten Schlüssels.

3.3.1. Identifikation und Authentisierung für Routine Schlüsselwiederverwendung

Kommt nicht zur Anwendung.

3.3.2. Identifikation und Authentisierung für Routine Schlüsselwiederverwendung nach Widerruf

Kommt nicht zur Anwendung. Eine Neubeantragung mit einem neuen Schlüssel ist notwendig.

3.4. Identifikation und Authentisierung für Sperr- bzw. Widerrufs Antrag

Die Zertifikate können unter anderem von Zertifikatsinhabenden Personen und von der ausstellenden Instanz, in Form der RA, jederzeit ohne Angabe von Gründen widerrufen werden (Siehe 4.9.2).

Temporäre Sperren kommen nicht zur Anwendung.

Als Anlassfälle gelten eine konkrete oder vermutete Schlüsselkompromittierung, sowie das Einstellen der Verwendung der Schlüssel. In diesen Fällen MUSS ein Widerruf durchgeführt werden.

Eine entsprechende Webseite und eine E-Mailadresse stehen hierfür zur Verfügung. Eine weitere Authentisierung für den Widerruf ist nicht vorgesehen.

4. Operative Vorgaben des Zertifikats-Lebenszyklus

4.1. Zertifikatsantrag

4.1.1. Wer kann einen Zertifikatsantrag stellen?

Ausschließlich natürliche Personen, die im Rahmen des Portals eine existierende Authentifizierung besitzen und über die entsprechende Berechtigung zur Beantragung von Endnutzungszertifikaten verfügen.

4.1.2. Ausstellungsprozess und Verantwortlichkeiten

Nach der erfolgreichen Überprüfung der Antragstellenden Person durch die ROs (Registration Officers) wird der PKCS#10 Antrag an die CA (Certificate Authority) weitergereicht und unmittelbar das Zertifikat ausgestellt.

Im Falle, dass die Antragstellende Person selbst keine Schlüsselfunktionen im Rahmen der Applikation zur Verfügung hat, wird ein von der CA generiertes Schlüsselpaar erstellt und der Antragstellenden Person übermittelt. Hierzu wird ein PKCS#12 (Soft-Token) verwendet, der mit einem entsprechend der Passwort-Policy des Magistrats der Stadt Wien ausreichend langen und sicheren Passwort geschützt ist.

Die Ausstellung des Zertifikats obliegt dem Betreiber des Zertifizierungsdienstes (CA), das ist der Magistrat der Stadt Wien, vertreten durch die Magistratsabteilung 01 – Wien Digital.Identitätsfeststellung, Kontrolle über die Einhaltung der Abläufe und der Daten, sowie das Anstoßen der Generierung der Zertifikate bzw. der Soft-Token obliegt der Registrierungsstelle (RA).

Grundlegend ist eine Antragstellende Person in der Pflicht korrekte Daten anzugeben bzw. die aus Drittsystemen eingelesenen Daten zu kontrollieren. Zur Überprüfung der ihm übermittelten Zertifikate bzw. Soft-Token dienen die zur Verfügung gestellten Ausstellungszertifikate.

Sollte eine Antragstellende Person nicht die Korrektheit der ausgestellten Zertifikate verifizieren können, so ist dies umgehend der RA zu melden und ein neuer Antrag, sowie ein Widerruf der nicht korrekten Zertifikate durchzuführen.

4.2. Zertifikatsantragsfunktionen

4.2.1. Identifikation und Authentisierung

Die RA überprüfen die aus vertrauenswürdigen Quellen stammenden Inhalte der übermittelten Anträge auf eine grundsätzliche Vollständigkeit. Diese Prüfung erfolgt automatisch ohne Interaktion eines ROs.

4.2.2. Akzeptieren oder Ablehnen eines Antrags

Die RA überprüfen die aus vertrauenswürdigen Quellen stammenden Inhalte der übermittelten Anträge auf eine grundsätzliche Vollständigkeit. Diese Prüfung erfolgt automatisch ohne Interaktion eines ROs.

Für den Fall eines nicht korrekten Antrags wird dieser automatisch abgelehnt und die Antragstellende Person über den Umstand informiert.

4.2.3. Dauer der Abwicklung eines Antrags

Zertifikatsanträge werden automatisch abgearbeitet und innerhalb weniger Minuten ausgestellt.

Die Veröffentlichung der Zertifikate und die automatische Benachrichtigung des Antragstellenden Person mit weiteren Handlungsanweisungen erfolgt unmittelbar nach Ausstellung der Zertifikate.

4.3. Zertifikatsausstellung

4.3.1. Detailfunktionen der CA bei Ausstellung

Die CA überprüft die Korrektheit des Übermittlers anhand der verwendeten Authorisierungsdaten. In Folge wird der Zertifikatsantrag auf formale und technische Korrektheit überprüft. (Konkret die Einhaltung der PKCS#10 Formatierungen – falls vorhanden – und die Felderforderungen lt. X.509.) Ebenfalls stellt die CA die Einzigartigkeit des Schlüssels sicher.

4.3.2. Benachrichtigung des Zertifikatsinhabers durch CA

Die Kommunikation mit der Antragstellenden Person (und Zertifikatsinhabenden Person) erfolgt grundsätzlich durch die RA. Eine Benachrichtigung über die erfolgreiche Ausstellung wird automatisch von der CA versandt.

4.4. Erstmalige Zertifikatsnutzung

4.4.1. Beidseitiges Einverständnis zur Zertifikatsnutzung

Ein Antragstellende Person hat das Recht auf Ablehnung des ausgestellten Zertifikats. Dies kann aufgrund

- falscher Daten im Zertifikat;
- mangelnder Informationen seitens der RA;
- Änderung der Verhältnisse seitens des Antragstellenden Person seit Beantragung;
- oder eine vermutete Kompromittierung zurückzuführen sein.

In jedem Falle hat der Antragsstellende Person die Ablehnung vor der Inbetriebnahme und erstmaligen Nutzung der RA bekannt zu geben.

Mit einer Erstnutzung akzeptiert der Zertifikatsinhabende Person zur Gänze die Rechte und Pflichten entsprechend dieser und aller weiteren Nutzungsvereinbarungen für die Dauer der Gültigkeit.

4.4.2. Veröffentlichung der Zertifikate durch die CA

Alle Zertifikate werden im Magistrat der Stadt Wien internen LDAP-Verzeichnis publiziert. Hierzu haben nur separat berechnete Personen bzw. interne MitarbeiterInnen Zugriff.

4.4.3. Bekanntgabe der Veröffentlichung an andere Stellen

Kommt nicht zur Anwendung.

4.5. Schlüsselpaar und Zertifikatsverwendung

4.5.1. Schlüsselverwendung und Zertifikatsgeltungsbereich des Antragstellenden Person

Die Schlüsselverwendung ist eingeschränkt auf die Funktionen, die im Feld keyUsage und extendedKeyUsage entsprechend dem X.509 Standard vermerkt sind. Im Detail sind diese:

- keyUsage : DataEncipherment; KeyEncipherment; DigitalSignature
- extendedKeyUsage : Client-Authentication; E-Mail-Security

4.5.2. Akzeptanz des Öffentlichen Schlüssels und komplementierender Zertifikatsverwendung

Jede Person, die die Verwendung des Öffentlichen Schlüssels akzeptiert, hat sich über die korrekte Verwendung anhand der Zertifikatseinträge zur Schlüsselverwendung zu informieren und diese zu prüfen.

Weiters gilt es die Prüfdaten (öffentlicher Schlüssel) ausschließlich dann zu akzeptieren, wenn der Gültigkeitszeitraum (Ausgestellt am + Gültig bis) zum Prüfzeitpunkt korrekt und das Zertifikat nicht widerrufen oder gesperrt ist.

4.6. Zertifikatserneuerung

Eine Wiederverwendung des existierenden Schlüssels für eine Neuausstellung eines Zertifikates kommt nicht zur Anwendung.

4.6.1. Umstände einer Zertifikatserneuerung

Kommt nicht zur Anwendung.

4.6.2. Wer darf eine Zertifikatserneuerung beantragen?

Kommt nicht zur Anwendung.

4.6.3. Abläufe der Zertifikatserneuerung

Kommt nicht zur Anwendung.

4.6.4. Benachrichtigung der Antragstellenden Person über die Zertifikatserneuerung

Kommt nicht zur Anwendung.

4.6.5. Einverständnis der Zertifikatserneuerung

Kommt nicht zur Anwendung.

4.6.6. Veröffentlichung eines erneuerten Zertifikats durch die CA

Kommt nicht zur Anwendung.

4.6.7. Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung

Kommt nicht zur Anwendung.

4.7. Zertifikatserneuerung mit neuem Schlüsselpaar

Es sind keine Automatismen implementiert, die eine Zertifikatserneuerung mit einem neuen Schlüsselpaar durchführen.

Die Zertifikatsinhabenden Person werden automatisch informiert, dass der Gültigkeitszeitraum demnächst beendet ist. Die Informationen werden 60 Tage vor Ablauf und 30 Tage vor Ablauf versendet.

D.h.: Eine Zertifikatserneuerung ist einem Neuantrag gleichgestellt und kommt somit im gegenständlichen Sinn des Abschnitts nicht zur Geltung (siehe 4.1).

4.7.1. Umstände einer Schlüsselneugenerierung

Kommt nicht zur Anwendung.

4.7.2. Wer darf eine Schlüsselneugenerierung beantragen?

Kommt nicht zur Anwendung.

4.7.3. Abläufe der Schlüsselneugenerierung

Kommt nicht zur Anwendung.

4.7.4. Benachrichtigung über die Neuausstellung

Kommt nicht zur Anwendung.

4.7.5. Einverständnis der Neuausstellung mit neuem Schlüssel

Kommt nicht zur Anwendung.

4.7.6. Veröffentlichung eines erneuerten Zertifikats durch die CA

Kommt nicht zur Anwendung.

4.7.7. Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung

Kommt nicht zur Anwendung.

4.8. Zertifikatsmodifikation

Eine Zertifikatsmodifikation bedeutet die Neuausstellung eines neuen Zertifikats auf Basis des existierenden öffentlichen Schlüssels.

Aus Sicherheitsgründen ist dies bei vorliegender Regelung nicht zulässig.

4.8.1. Umstände einer Zertifikatsmodifikation

Eine Zertifikatsmodifikation ist nicht zulässig. (Siehe 4.8).

4.8.2. Wer darf eine Zertifikatsmodifikation beantragen

Eine Zertifikatsmodifikation ist nicht zulässig. (Siehe 4.8).

4.8.3. Abläufe zur Beantragung einer Zertifikatsmodifikation

Eine Zertifikatsmodifikation ist nicht zulässig. (Siehe 4.8).

4.8.4. Benachrichtigung über die Zertifikatsneuausstellung

Kommt nicht zur Anwendung.

4.8.5. Einverständniserklärung einer Neuausstellung

Kommt nicht zur Anwendung.

4.8.6. Veröffentlichung eines modifizierten Zertifikats durch die CA

Kommt nicht zur Anwendung.

4.8.7. Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung

Kommt nicht zur Anwendung.

4.9. Zertifikatswiderruf und Sperre

4.9.1. Umstände eines Widerrufs

Zertifikate müssen widerrufen werden, wenn:

- ein Informationsbestandteil nicht mehr zutreffend ist;
- der private Schlüssel kompromittiert wurde;
- ein Verdacht besteht, dass der private Schlüssel kompromittiert wurde;
- der private Schlüssel verloren wurde, bzw. die Kontrolle über die Anwendung des privaten Schlüssels nicht mehr möglich ist;
- der Schlüssel und das Zertifikat für einen Zweck verwendet wurden, der nicht Bestandteil der Zertifizierungsrichtlinie und/oder der Anwendungsvorgaben ist;
- bei Einstellung des Zertifizierungsdienstes.

4.9.2. Wer kann einen Widerruf beantragen?

Ein Widerruf kann initiiert werden durch:

- Magistrat der Stadt Wien als ausstellende Instanz
- Registrierungsstelle

- Zertifikatsinhabende Person
- Personen mit entsprechender Berechtigung zur Administration von Server- und Client Zertifikaten (Portal-Gruppe)

4.9.3. Prozeduren der Widerrufsansträge

Ein Widerruf kann direkt an die Registrierungsstelle gemeldet werden. Dies kann per Web-Applikation oder E-Mail an ca@ma01.wien.gv.at durchgeführt werden.

Für die Durchführung ist der Name der Zertifikatsinhabenden Person und der CN (Common Name), oder die Seriennummer des Zertifikats notwendig.

Alle Zertifikatsinhabenden Personen haben ebenfalls die Möglichkeit über die Webseite, die auch zur Abholung des Zertifikats dient, den Widerruf selbständig zu beantragen. Die Protokolldaten werden archiviert.

4.9.4. Durchführungszeit eines Widerrufs

Eine Zertifikatsinhabende Person MUSS den Widerruf unmittelbar nach Erkennen der Notwendigkeit beantragen.

Die eingerichtete Webseite übermittelt den Widerrufsanspruch unmittelbar an die RA. Im Falle eines Widerrufs durch die Registrierungsstelle ist ein RO im Rahmen der Normalarbeitszeit dazu angehalten, den Widerruf unmittelbar nach Bekanntgabe durchzuführen.

Eine Reaktionszeit seitens der Registrierungsstelle wird mit 1 Werktag garantiert.

4.9.5. Zeitspanne der technischen Prozesse eines Widerrufs

Die Ausstellende Instanz führt die Widerrufe unmittelbar durch. Die Publikation der Sperrlisten wird in den vordefinierten Intervallen durchgeführt. (Siehe 4.9.7)

Im Falle der Veröffentlichung der Sperrliste (CRL) auf den Webseiten des Portals kann es zu einigen Minuten Verzögerung kommen.

4.9.6. Zulässigkeit der Sperrinformationen für vertrauende Instanzen

Grundsätzlich gilt, dass vertrauende Instanzen die Verpflichtung haben die Sperrinformationen gegen eine gültige Sperrliste (CRL), oder den Online-Dienst (OCSP) zu prüfen.

Für den Fall, dass eine solche nicht verfügbar ist, sind die gegenständlichen Vereinbarungen der Verbindlichkeiten seitens der Zertifizierungsdiensteanbietende Stelle und der Zertifikatsinhabenden Person für die vertrauenden Instanzen nicht gültig.

In besonderen Fällen, in denen keine, bzw. nicht regelmäßig Sperrinformationen als CRL verfügbar sind und auch mittels OCSP-Anfragen keine Prüfung stattfinden kann, ist die Verwendung von "Blacklisting"

innerhalb einer Applikation zulässig. Diese besonderen Fälle bedürfen immer einer separaten Regelung abseits dieser Vereinbarung.

4.9.7. Sperrlisten Aktualisierungsfrequenz

Sperrlisten werden täglich ausgestellt und haben eine Gültigkeitsdauer von 7 Tagen.

4.9.8. Maximale Latenz für Sperrlisten

Die maximale Latenz beträgt 10min.

4.9.9. Online Widerruf- und Sperrprüfungs-Möglichkeiten

Der ZDA bietet einen OCSP-Dienst an (Online-Certificate-Status-Protocol).

4.9.10. Online Widerruf- und Sperrprüfungsvoraussetzungen

Grundsätzlich gibt es keine besonderen Voraussetzungen.

Die Adresse für den OCSP-Dienst lautet: <http://ocsp.wien.gv.at/ocsp/>

Die Applikationen müssen entsprechende technische Mittel verfügbar haben, um eine OCSP-Anfrage absetzen und die Antwort korrekt interpretieren zu können. Dies liegt nicht im Verantwortungsbereich des Zertifizierungsdienstes.

4.9.11. Andere Möglichkeiten Sperrinformationen abzurufen.

Kommt nicht zur Anwendung.

4.9.12. Spezielle Vorgaben bei einer Kompromittierung einer Zertifikatserneuerung

Zertifikatserneuerung wird nicht unterstützt.

4.9.13. Umstände einer Sperre

Temporäre Sperren werden nicht unterstützt.

4.9.14. Wer kann eine Sperre beantragen?

Temporäre Sperren werden nicht unterstützt.

4.9.15. Abläufe zur Durchführung einer Sperre

Temporäre Sperren werden nicht unterstützt.

4.9.16. Begrenzungen der Sperrdauer

Temporäre Sperren werden nicht unterstützt.

4.10. Zertifikatsstatus Services

4.10.1. Operative Eigenschaften

Der Zertifikatsstatus ist anhand einer Interpretation der zugehörigen Sperrliste möglich. Weiters wird ein OCSP-Service angeboten: <http://ocsp.wien.gv.at/ocsp/>

4.10.2. Serviceverfügbarkeit

Die Sperrlistenverfügbarkeit ist redundant auf den Webseiten der Stadt Wien publiziert.

<https://www.wien.gv.at/kontakte/ma01/zertifikate.html>

Der Magistrat der Stadt Wien garantiert eine Verfügbarkeit von 99.7% im Zeitraum eines Jahres. Das Prüfen des Zertifikatsstatus ist 24 h x 7 Tage möglich.

4.10.3. Optionale erweiterte Services

Kommen nicht zur Anwendung.

4.11. Ablauf der Gültigkeit

Eine Zertifikatsinhabende Person kann zu jedem Zeitpunkt der Gültigkeit das Zertifikat widerrufen und somit die Gültigkeit beenden (siehe 4.9).

Ansonsten endet die Gültigkeit mit der beim Ausstellungszeitpunkt festgelegten Dauer der Gültigkeit.

4.12. Schlüsselhinterlegung und Wiederherstellung

Kommt nicht zur Anwendung.

4.12.1. Schlüssel hinterlegung und Wiederherstellungsvorgaben und Praktiken

Kommt nicht zur Anwendung.

4.12.2. Sitzungsschlüssel Aufbewahrung und Wiederherstellungsvorgaben und Praktiken

Kommt nicht zur Anwendung.

5. Liegenschaften, Management, und operative Kontrollen

5.1. Physikalische Kontrollen

Der Magistrat der Stadt Wien implementiert geeignete physische Sicherheitskontrollen, um den Zugriff zu Hard- und Software, die zum Betrieb des Zertifizierungsdienstes eingesetzt wird, zu regeln.

5.1.1. Liegenschaft(en) und bauliche Maßnahmen

Die Komponenten des Zertifizierungsdienstes sind in einem sicheren Rechenzentrum am Organisationssitz in Wien (Österreich) untergebracht.

5.1.2. Physischer Zugang

Ausschließlich autorisierte Personen haben physischen Zugang zum Rechenzentrum. Jeder Zugang wird protokolliert. Die Regelungen der Zugangseinschränkungen und der Durchführung werden regelmäßig auditiert. Die Ergebnisse der Audits werden entsprechend des ISMS zur Steuerung und Regelung der Sicherheit weitergeleitet.

Der Zugang ist durch personalisierte Zutrittskarten (Angestelltenausweise) auch technisch abgesichert.

5.1.3. Strom und Luftzirkulation

Alle kritischen Komponenten sind mit einer unterbrechungsfreien Stromversorgung verbunden. Im Falle eines Netzausfalls stehen die verfügbaren Generatoren für den Notbetrieb zur Verfügung. Die Räumlichkeiten sind außerdem mit einer Klimaanlage ausgestattet.

Im Falle des Totalausfalls gelten die allgemeinen Auflagen für das Rechenzentrum, um die Systeme kontrolliert abzuschalten.

5.1.4. Wasserschäden

Das Rechenzentrum ist vor Wasserschäden baulich geschützt.

5.1.5. Brandvorbeugung und Brandbekämpfung

Es sind entsprechend der behördlichen Auflagen und entsprechend den Qualitätssicherungen zum Betrieb eines Datenzentrums Feuermelder und automatische Löschsysteeme verfügbar.

5.1.6. Datenspeicherung

Alle Daten, die zum Betrieb des Zertifizierungsdienstes verarbeitet werden, werden gespeichert und archiviert. Die Speicherung (Backups) erfolgt im selben Rechenzentrum. Die Archivierung erfolgt auf getrennten Systemen und kann in gesonderten Liegenschaften erfolgen.

5.1.7. Abfallentsorgung

Alle in Papier und auf Dauerspeichermedien verfügbaren Daten werden gesichert und kontrolliert entsprechend den internen ISMS-Vorgaben entsorgt.

Digitale Speichermedien werden sicher überschrieben oder gelöscht (Wiping). Papier wird geschreddert und in verschlossenen Müllsystemen entsorgt.

5.1.8. Off-site Backup

Alle off-site Lokationen für die Datenspeicherung und Archivierung haben einen angemessenen physischen Schutz und lassen nur befugten Zugriff entsprechend der Rollenentsprechung zu.

Diese stehen während der Bürozeiten zur Verfügung.

5.2. Kontrollprozeduren

5.2.1. Vertrauenswürdige Rollen

Um sicherzustellen, dass keine Einzelperson den Zertifizierungsdienst kompromittieren kann, gibt es eine Rollenverteilung mit getrennten Kompetenzen und Aufgabenstellungen. Diese ergänzen einander in den logischen Abfolgen.

Diese Rollen sind:

System Admin (SA)

ist verantwortlich für das grundsätzliche Funktionieren der physischen Entität, also der Hard- und Software, mit der die CA betrieben wird. Der Zugriff ist auf die Software-Ebene beschränkt. Es gibt keine Möglichkeit der Manipulation der logischen Konfiguration des CA-Systems.

Registration Officer (RO)

ist verantwortlich für die Identifizierung/Verifikation der Antragsdaten und für das nachvollziehbare Zustandekommen der erfolgreichen Ausstellung und Übermittlung des Zertifikats. ROs sind ebenfalls Kontaktstelle für die Sperre und den Widerruf, sofern dieser nicht automatisch erfolgt, bzw. erfolgen kann.

Security Officer (SO)

die Hauptverantwortlichen innerhalb der CA – konfigurieren und steuern die logischen Instanzen der PKI. Sie generieren die Schlüssel und setzen die Formate, Publikationsparameter fest.

5.2.2. Anzahl der Personen je Rollentätigkeit

Mindestens 2 Personen werden pro Rolle geschult und mit den Systemen und der Rolle vertraut gemacht, so dass etwaige Ausfälle keine systematischen Engpässe verursachen. Für den Fall eines bleibenden oder langfristigen Ausfalls werden zusätzliche Personen ausgebildet und am System berechtigt, die Rolle einzunehmen.

Für die gegenständlichen Zertifizierungsinstanzen ist kein Vieraugen-Prinzip eingerichtet. Die einzelnen Arbeitsmaßnahmen müssen vollständig entsprechend der Vorgaben protokolliert werden. Dies gilt für jede einzelne Rolle.

5.2.3. Identifikation und Authentifizierung am System

Jede Person erhält ein auf Smartcard-basiertes Zertifikat, mit dem gegenüber dem System eine Autorisierung durchgeführt wird.

Für die Schlüsselgenerierung an den Hardware-Security-Modulen sind den Personen in der Rolle eines Security-Officer separate Authentifizierungs-Token übergeben worden.

5.2.4. Rollen mit getrennten Aufgaben

Es sind abseits der bereits definierten Rollen keine Rollen definiert, die in sich weiterer Unterscheidungen und Aufgabentrennungen, bedürfen.

Es gibt keine Person, die mehr als eine Rolle einnehmen darf.

5.3. Personelle Kontrollen

Entsprechend der allgemeinen Auflagen für die Beschäftigung beim Magistrat der Stadt Wien entspricht jede Person, die eine Rolle für den Zertifizierungsdienst einnimmt, einem vereidigten Beschäftigungsverhältnis.

Die Personen sind ausreichend über die Systeme und die Tragweite ihrer Verantwortung geschult und informiert.

5.3.1. Qualifikation, Erfahrung und Anforderungen an die Tauglichkeit der Rollen

Entsprechend der allgemeinen Vorgaben zur Beschäftigung des Magistrat der Stadt Wien gibt es eine gesicherte Ausbildung an den Systemen. Die Mindestvorgaben werden von den leitenden Personen des Rechenzentrums und den Systemverantwortlichen innerhalb der Organisation definiert und kontrolliert.

5.3.2. Prozeduren zur Eignungsüberprüfung

Abseits der fachlichen Entsprechung, die durch die Standardprozeduren zur Einstellung (HR) definiert und kontrolliert wird, wird entsprechend der verwaltungsrechtlichen Vorgaben für jede Person vor der Einstellung der Hintergrund geprüft. Im Falle einer Nicht-Entsprechung wird diese Person nicht beschäftigt und somit auch gesichert nicht mit einer Rolle betreffend des Zertifizierungsdienstes betraut.

Externe Personen nehmen keine betriebliche Rolle innerhalb des Zertifizierungsdienstes ein.

5.3.3. Trainingsvorgaben

Alle Personen erhalten entsprechend ihrer Rolle Training an den Systemen und in ihren Tätigkeiten.

Insbesondere erhalten sie Sicherheitsinformationen betreffend die Funktionsweisen von PKI-Systemen.

5.3.4. Weiterführende Trainings und Anforderungen der Fortbildung

Es gibt kontinuierliche Informationen betreffend Veränderungen an den Systemen und/oder den Policy-Vorgaben.

Für grundsätzliche Veränderungen oder Arbeitsweisen werden weitere Trainings und Schulungen abgehalten.

5.3.5. Arbeitsaufgaben - Veränderungsanforderungen

Für die gegenständliche Zertifizierungsrichtlinie gibt es keine besonderen Anforderungen an die Personen zur regelmäßigen Veränderung der Aufgabenstellung.

5.3.6. Sanktionen für unautorisiertes Vorgehen

Entsprechend dem Vertrag zur Beschäftigung und innerhalb des Dienstrechts des Magistrats der Stadt Wien sind disziplinarische Maßnahmen definiert, für den Fall eines unautorisierten Verhaltens.

5.3.7. Anforderungen an Zulieferer und Vertragsparteien

Vertragsparteien, die für das System und den Zertifizierungsdienst benötigt werden, werden denselben Hintergrundüberprüfungen unterzogen.

Ein entsprechender Vertrag mit Vertraulichkeitsvereinbarung und Strafmaßnahmen MUSS vorliegen.

5.3.8. Dokumentation für das Personal

Es stehen detaillierte fachliche Schulungs- und Trainingsunterlagen zur Verfügung. Allen Beteiligten stehen Unterlagen zur Bedienung des Systems für Ihre jeweiligen Aufgaben zur Verfügung.

Entsprechend der Kontroll- und Protokollierungsmaßnahmen sind schematische Vorlagen bereitgestellt.

5.4. Überwachungsprozeduren

5.4.1. Typen der aufzuzeichnenden Aktivitäten und Ereignisse

Alle Ereignisse betreffend Konfiguration, Schlüsselgenerierung und Arbeiten am Zertifikatsmanagement innerhalb des Zertifizierungsdienstes sind zu protokollieren – sowohl als systematisches Logging, als auch als Protokoll der handelnden Personen.

Aus den Aufzeichnungen muss eine erkennbare nachvollziehbare Handlung abgeleitet und entsprechend einer Risikoeinschätzung interpretiert werden können.

5.4.2. Intervalle der Logfile-Überprüfung

Die System-Logfiles werden mindestens 2 mal jährlich analysiert und ausgewertet.

5.4.3. Aufbewahrung der Logfiles

Die Logfiles werden zumindest 7 Jahre archiviert.

5.4.4. Zugriffsschutz der Logfiles

Alle Systemprotokolldaten sind durch den generellen Systemzugriff geschützt. Nur berechtigte Personen (Systemadmins und Security-Officer) haben Zugriff.

5.4.5. Logfiles-Sicherungsprozeduren

Die Systemdaten werden täglich gesichert. Die Sicherungen sind vor Manipulation geschützt.

5.4.6. Systemüberwachung

Das Protokollierungssystem ist integrativer Bestandteil des CA-Systems und startet und stoppt mit demselben.

Ohne erfolgreiche Inbetriebnahme des Protokollierungssystems sind keine Ausstellungen, oder Veränderungen mit bzw. am CA-System möglich.

5.4.7. Automatische Benachrichtigungen über Ereigniseinträge

Aktuell sind keine automatischen Benachrichtigungen für einzelne Ereigniseinträge definiert und konfiguriert.

5.4.8. Verwundbarkeitseinschätzungen

Bedrohungs- und Risikoeinschätzungen, sind wiederkehrende Maßnahmen für den Zertifizierungsdienst. Diese inkludieren die Ausstattung, die physische Lokation die Aufzeichnungsmaßnahmen, die Software, das Personal, etc.

Die Vorgaben kommen aus den allgemeinen ISMS-Anforderungen. Die ISMS-Steuerung übernimmt das ISMS-Sicherheitsmanagement-Team der MA 01 - Wien Digital.

Generell erstellte Risikoeinschätzungen werden regelmäßig hinterfragt und zeitgemäß adaptiert, um sowohl die technische und organisatorische, wie auch die wirtschaftliche Gefährdung stetig auf einem akzeptablen Niveau zu halten.

5.5. Aufzeichnungsarchiv

Für den gegenständlichen Zertifizierungsdienst werden Archivaufzeichnungen 7 Jahre vorgehalten.

Die Daten sind vor Zugriff geschützt.

5.5.1. Typen der zu archivierenden Daten

Alle Protokolle und Logfiles zur Ausstellung von Zertifikaten werden archiviert.

5.5.2. Aktualisierungsintervalle der Archive und Überprüfung

Die System-Logfiles werden mindestens zweimal jährlich analysiert und ausgewertet.

5.5.3. Schutz der Archivdaten

Die Archivdaten können nur von Auditoren und Systemadmins abgerufen werden.

5.5.4. Archiv-Sicherungsprozeduren

Es gelten die allgemeinen Vorgaben für den sicheren Betrieb.

5.5.5. Anforderung betreffend Zeitstempelverwendung

Derzeit werden keine gesicherten Zeitstempeldienste innerhalb der Archivierung verwendet.

5.5.6. Archiv-Sammel-Systeme

Die betroffenen Systemdaten unterliegen keiner speziellen Richtlinie zur gesammelten Ablageordnung.

5.5.7. Prozeduren zur Archiv-Verifikation

Die archivierten Daten gelten im Allgemeinen als vertrauenswürdig für den vorliegenden Zertifizierungsdienst und werden gepaart mit den physischen Aufzeichnungen (Papierprotokollen) interpretiert.

5.6. Schlüsseltauschmechanismus

Es gibt kein automatisiertes Schlüsselmanagement. Alle Schlüssel müssen rechtzeitig von autorisiertem Personal generiert und in Betrieb genommen werden.

Für jeden neu zu verwendenden Schlüssel werden neue Generationen von Zertifikaten ausgerollt. Die Generation der Schlüssel ist aus dem Zertifikat erkenn- und interpretierbar.

Alte Schlüssel werden falls möglich zur Ausstellung von Sperrinformationen verwendet, bis alle damit ausgestellten Zertifikate widerrufen oder abgelaufen sind.

5.7. Wiederherstellung nach Kompromittierung oder Disaster

Es existieren klare Vorgaben für die Handlungen im Falle einer Kompromittierung oder eines Totalausfalls (Disaster). Es existieren weiters Notfallprozeduren, die eine rasche Wiederherstellung eines sicheren und ungestörten Betriebes gewährleisten.

5.7.1. Notfallmaßnahmen und Kompromittierungsprozeduren

Die Handlungsanweisungen sind vertraulich und nur befugten Personen innerhalb der Betreiberorganisation bekannt. Die Steuerung und Aktuell-Haltung obliegt dem IT-Service Continuity Management des Magistrats der Stadt Wien.

5.7.2. Ausfall von Systemen, Software-Wiederherstellung und/oder korruptierten Daten

Im Falle eines Totalausfalls werden die Systeme innerhalb der kürzest möglichen Zeit wiederhergestellt und eine neue Generation von Schlüsseln und Zertifikaten ausgerollt.

Die anwendenden und inhabenden Personen von ausgestellten und vom Ausfall betroffenen Zertifikaten und Sperrlistenabrufen werden umgehend vom Ausfall informiert und erhalten klare Informationen über die Wiederherstellung und Zurverfügungstellung von neuen Zertifikaten und Sperrlisten.

5.7.3. Kompromittierung privater Schlüssel der CA

Im Falle einer Schlüsselkompromittierung oder des Verdachts einer Kompromittierung wird die Ausstellung von Zertifikaten und Sperrlisten sofort gestoppt und der Zugriff auf die Systeme unterbunden.

In Folge werden alle verfügbaren Daten analysiert, im Falle eines verdachtsfreien Analyseergebnisses, wird der Betrieb wieder hergestellt.

Für den Fall einer tatsächlichen Kompromittierung werden unmittelbar alle Nutzende Personen informiert, die ausgerollten Zertifikate gesperrt und Arbeiten angestrebt, um eine rasche Wiederherstellung eines gesicherten Betriebs zu gewährleisten.

Den betroffenen anwendenden Personen werden so rasch als möglich neue Zertifikate zur Verfügung gestellt.

5.7.4. Fortführung des Betriebes nach Disaster

Dem Betrieb steht ein Ausfallsrechenzentrum zum sicheren Fortführen der Zertifizierungsinstanz im Falle eines Disasters zur Verfügung.

Die Informationen zum Betrieb sind als vertraulich eingestuft und werden an dieser Stelle nicht veröffentlicht, sind aber von der Betriebsführung für Berechtigte im notwendigen Umfang weiterzugeben.

5.8. Einstellung der CA oder RA Tätigkeit

Für den Fall einer Einstellung der CA-Tätigkeit, und im gegenständlichen Fall des Zertifizierungsdienstes somit auch der RA-Tätigkeit, werden alle Nutzenden Personen in einem ausreichend definierten Zeitraum vorab informiert.

Alle Zertifikate werden vor Einstellung der Tätigkeit widerrufen.

6. Technische Sicherheitskontrollen

Alle privaten CA-Schlüssel (ausgenommen der Test- und Administrations-CA) sind gesichert in der Verwendung innerhalb des HSM (Hardware-Security-Moduls). Das HSM entspricht zumindest den FIPS-140-2 Level 3 und/oder Common Criteria EAL 4 Standards.

Der Zugriff in der Verwendung des HSM ist limitiert auf die Security Officer (SO) der vorliegenden CPS. Die Absicherung erfolgt durch gesicherte Verwendungs-Codes, entsprechend der Zertifizierung des HSM.

6.1. Schlüsselgenerierung und Installation

6.1.1. Schlüsselgenerierung

Alle CA-Schlüssel werden innerhalb des HSM und mit als sicher geltenden Algorithmen erzeugt.

Schlüssel der Zertifikatsantragstellenden Person werden entweder von den Antragsstellenden Personen an den Zielsystemen erzeugt, oder von der CA in Software produziert. (Siehe Appendix A)

6.1.2. Übermittlung des Privaten Schlüssels an die Antragstellende Person

Im Fall der CA-seitigen Generierung des Schlüsselpaares wird der PKCS#12-Container mit einem Aktivierungs-PIN an den Antragstellende Person übermittelt.

Im Falle einer Selbstgenerierung im Zielsystem ist der Private Schlüssel keines Transports ausgesetzt. (Details siehe Appendix A)

6.1.3. Übermittlung des Öffentlichen Schlüssels an die Zertifizierungsinstanz

Der öffentliche Schlüssel wird entweder von der CA gemeinsam mit dem privaten Schlüssel erzeugt und in Form des PKCS#12-Containers an die Antragstellende Person übermittelt, oder im Falle der Selbstgenerierung von der Antragstellenden Person zur Aufnahme ins Zertifikate gesichert übermittelt.

(Details siehe Appendix A)

6.1.4. Veröffentlichung der Öffentlichen Schlüssel an weitere Instanzen

Alle öffentlichen Schlüssel werden in Form der gültigen Zertifikate im LDAP Verzeichnisdienst des Betreibers publiziert und zur Verfügung gestellt.

Weiteren Nutzern werden die Zertifikate auf Anfrage und im Falle der korrekten Überprüfung der Anfragegestattung übermittelt.

6.1.5. Schlüssellängen

Die Länge der Schlüssel ist im Appendix A definiert. Im Allgemeinen gilt eine Schlüssellänge für die ausstellenden Instanzen (die CA Schlüssel) von 4096 bit RSA und für alle Antragstellenden Personen eine Länge von 2048 bit RSA als Mindestlänge.

6.1.6. Schlüsselgenerierung, Schlüsselparameter und Qualitätssicherung

Die CA-Schlüssel werden innerhalb der HSM-Module generiert, wodurch die korrekte Generierung gewährleistet wird.

Die Antragsdaten werden mit entsprechender Software an den Zielsystemen generiert. Von der CA erzeugte Schlüssel sind seitens der korrekten Kryptobibliotheken der Herstellfirma gesichert.

Im Zweifelsfalle obliegt es der RA-Instanz die Schlüssel auf Korrektheit zu prüfen.

6.1.7. Zwecke der Schlüsselverwendung (nach dem Standard X.509 v3 und entsprechender Feldbezeichnung)

CA-Schlüssel sind definiert und gekennzeichnet, um Zertifikate auszustellen und Sperrlisten (CRLs und OCSP-Anfragen) zu signieren.

Nutzungszertifikate sind entsprechend der vorliegenden CPS gekennzeichnet. Siehe Details in Appendix A.

6.2. Schutz der privaten Schlüssel und Mechanismen zur korrekten Verwendung der kryptografischen Anwendungen

Alle Beteiligten sind dazu angehalten alle erforderlichen Maßnahmen zum Schutz der privaten Schlüssel einzuhalten. Entsprechend der gegenständlichen Richtlinie (CPS) gilt dies für den Verlust, die Zerstörung und die unbefugte Verwendung des privaten Schlüssels.

Die Sicherungen beinhalten angemessene Aufbewahrung und die Verwendung von sicheren Passwörtern und Aktivierungs-Codes (PIN).

6.2.1. Standards der Kryptografischen Module und deren Verwendung

Alle CA-Schlüssel sind geschützt innerhalb des Hardware-Security-Moduls (HSM), das den Sicherheitsanforderungen von FIPS-140-2 Level 3 und/oder Common Criteria EAL 4 entspricht.

6.2.2. Generierung privater Schlüssel (n out of m) Mehrfach-Personen-Kontrolle

CA Schlüssel der vorliegenden Zertifizierungsinstanz können von einem SO (Security Officer) zur Verwendung gebracht, innerhalb der CA Software zur Verwendung markiert werden.

6.2.3. Schlüsselhinterlegung des privaten Schlüssels

Private Schlüssel werden nicht hinterlegt.

6.2.4. Sicherung der privaten Schlüssel

Eine Sicherung der privaten Schlüssel des HSM erfolgt in gesicherter und kontrollierter Weise in Form eines geklonten HSM und nie in einer Form, in der die Schlüssel kompromittiert werden können. Die Schlüssel verlassen also nie die gesicherte Umgebung.

Anwendenden Personen ist es gestattet Sicherungen der privaten Schlüssel vorzunehmen, sofern die Sicherungen nachweislich vor unbefugter Verwendung sicher verwahrt werden. Zumindest im selben Ausmaß wie die aktiven Schlüssel.

6.2.5. Archivierung der privaten Schlüssel

Die privaten Schlüssel werden nicht archiviert. Die gesicherte Zerstörung der Schlüssel muss im Beisein der Zertifikatsinhabenden Person erfolgen. Dies gilt auch für Schlüssel von abgelaufenen Zertifikaten.

6.2.6. Übermittlung privater Schlüssel in oder aus dem Kryptografischen Modul (HSM)

Die CA-Schlüssel werden immer im HSM generiert und verlassen nie das Modul.

6.2.7. Unterbringung der privaten Schlüssel im Kryptografischen Modul (HSM)

Die privaten Schlüssel werden entsprechend den Sicherheitsvorgaben der Herstellfirma und somit entsprechend den Zertifizierungsvorgaben der Sicherheitsüberprüfenden Instanz (Common Criteria und/oder FIPS Evaluatoren) verwendet und abgelegt.

6.2.8. Methode zur Aktivierung der privaten Schlüssel

Die privaten Schlüssel benötigen zur Aktivierung immer einen, der Zertifizierung des Moduls entsprechenden, Aktivierungs-Mechanismus.

6.2.9. Methode zur Deaktivierung der privaten Schlüssel

Wenn die CA-Software aktiv ist, gelten die Schlüssel als aktiviert. Im Falle eines Neustarts der CA müssen die Schlüssel separat aktiviert werden.

Die Schlüssel können gesondert von SOs deaktiviert werden.

6.2.10. Methode der kontrollierten Zerstörung der privaten Schlüssel

Private Schlüssel der CA werden nach Ablauf der Verwendungsperiode zerstört. Dies gilt auch für alle Sicherungskopien.

Dies wird entsprechend den Herstellvorgaben durchgeführt und protokolliert.

6.2.11. Einstufung der Sicherheit des kryptografischen Moduls (HSM)

Das HSM entspricht nachweislich den Anforderungen von FIPS-140-2 Level 3 und/oder Common Criteria EAL 4.

6.3. Weitere Aspekte des Schlüsselmanagements

6.3.1. Archivierung der öffentlichen Schlüssel

Öffentliche Schlüssel werden ausschließlich in Form der Zertifikate abgelegt und aufbewahrt.

6.3.2. Zertifikatsgültigkeiten und operative Schlüsselverwendungszeiträume

Siehe Appendix A – generell gilt:

Für CA-Zertifikate gelten die folgenden Maximalzeiträume der Gültigkeit:

- Root CA: 20 Jahre
- Issuing CA: 10 Jahre

6.4. Aktivierungsdaten

6.4.1. Aktivierungsdaten Generierung und Installation

Als Aktivierungsdaten gelten einzigartige Codes, die zur Verwendung des Schlüssels angewandt werden müssen. Diese Aktivierungsdaten dürfen ausschließlich den Zertifikatsinhabenden Personen bekannt sein.

Den Antragstellenden Personen wird ein geeignetes Werkzeug zur Generierung angeboten und zur Verfügung gestellt, um sichere Codes zu erzeugen.

Für die Inbetriebnahme und Installation gibt es keine gesonderten Vorgaben seitens der CPS. Für den Fall entsprechender Server-oder Applikationspolicies gilt es diesen zu entsprechen, um die sichere Verwendung zu garantieren.

6.4.2. Schutz der Aktivierungsdaten

Aktivierungsdaten, sofern diese übermittelt werden müssen, unterliegen besonderer Schutzmaßnahmen und sind immer ausreichend kryptografisch zu schützen.

Sie sollten bestenfalls nie aufgezeichnet werden und dürfen keinesfalls mit anderen Personen geteilt werden.

6.4.3. Weitere Aspekte der Verwendung von Aktivierungsdaten

Die Unterbringung und Aktivierung der Schlüssel muss sicherstellen, dass die Aktivierungsdaten benötigt werden. Schlüssel ohne Aktivierungsdaten dürfen nicht zur erfolgreichen Installation führen. Diese gelten automatisch als kompromittiert und die Zertifikate sind zu widerrufen.

6.5. Computer Sicherheitsvorgaben

6.5.1. Spezifische technische Anforderungen an Computersysteme

Die Sicherheit der eingesetzten Systeme erreicht das notwendige Sicherheitsniveau ausschließlich durch eine Kombination von Maßnahmen auf Hardware-, Software- und organisatorischer Ebene.

Dazu zählen unter anderem (nicht vollständige Aufzählung der beim Betreiber getroffenen Maßnahmen):

- TLS gesicherte Verbindungen zu allen Web-basierten Services
- Virenschutz auf allen betroffenen Systemen
- Geregelte und eingeschränkte Netzwerkverbindungen
- PKI basierende Authentifizierungen für SO und RO
- Netzwerküberwachungssysteme

Eine vollständige Maßnahmenübersicht wird im Rahmen des ISMS geregelt.

6.5.2. Sicherheitseinstufung der Computer

Es werden alle betroffenen und zum Einsatz kommenden Endgeräte entsprechend der internen Regelungen zur Serversicherheit betrieben und überwacht.

6.6. Technische Umgebungsparameter eines Systemzyklus

Ein Systemzyklus ist die Dauer des Einsatzes einer bestimmten in Betrieb genommenen Konfiguration aus Hard- und Software. Sofern zulässig werden nur Updates und Wartungsarbeiten vorgenommen.

Für den Fall von gravierenden Umbauten ist der Zyklus beendet und eine als neu geltende Kombination von Hard- und Software bildet einen neuen Systemzyklus. Dies ist unabhängig von der Verwendung der Schlüssel, Zertifikate und sonstigen zeitlich limitierten Bereichen zu interpretieren.

6.6.1. Systemspezifische Entwicklungsumgebungen

Die verwendeten Software-Produkte, im Speziellen die PKI-Komponenten, sind Open Source und werden von externen Projekten und/oder Organisationen verwaltet.

Neuerungen werden geprüft und kontrolliert zur Anwendung eingebracht.

6.6.2. Verwaltung der Sicherheitsmaßnahmen

Der Betreiber verfolgt alle technischen Entwicklungen der zum Einsatz gelangenden Produkte. Parallel dazu wird proaktiv eine Technologiebeobachtung des Marktes betrieben, um die notwendige Reaktionszeit im Bedrohungsfalle möglichst kurz zu halten.

6.6.3. Auflagen an die Verwaltung der Sicherheitsmaßnahmen

Alle Auflagen und Kontrollen werden im Rahmen des ISMS der MA 01 - Wien Digital gesteuert.

6.7. Netzwerküberwachung

Der gesamte Zugriff auf die CA-Umgebung via Netzwerke ist geschützt und überwacht sowie mittels Firewalls und Routenfilterung limitiert. Die aktiven Verbindungen sind limitiert auf die Systemadministration und bedürfen spezifischer Zugriffspoints.

6.8. Zeitstempeldienste

Zeitstempeldienste kommen nicht zur Anwendung.

7. Zertifikats-, CRL und OCSP Profile

7.1. Zertifikatsprofil

Alle von dem Zertifizierungsdienst ausgestellten Zertifikate entsprechen dem RFC 5280 und sind X.509 Version 3 Zertifikate.

Detaillierte Informationen zu Ausprägungen der einzelnen Zertifikatsprofile sind im Anhang A zu finden.

7.1.1. Versions Nummer

Zertifikate werden ausschließlich im Format X.509 Version 3 ausgestellt.

7.1.2. Zertifikatserweiterungen

Folgende Zertifikatserweiterungen werden im Rahmen des ZDA für Wurzel-, Ausstellungs- und Endnutzungszertifikate verwendet. Hierbei bedeutet „x“, dass eine Erweiterung in einem Zertifikat enthalten ist und „optional“, dass sie Abhängig vom Zertifikatsprofil verwendet werden kann:

Erweiterung	Zertifikatstyp			Kritisch ja/nein
	Wurzel	Ausstellung	Endnutzungsgr	
Subject Key Identifier	X	X	X	NEIN
Basic Constraints	X	X	X	JA
Key Usage	X	X	X	JA
Authority Key Identifier		X	X	NEIN
Enhanced Key Usage			X	NEIN
Subject Alternative Name			Optional	NEIN
Certificate Policies			X	NEIN
CRL Distribution Points		X	X	NEIN
Authority Information Access			X	NEIN

7.1.3. Algorithmen Objekt Unterscheider

Die verwendeten Algorithmen Objekt Unterscheider (algorithm object identifier) entsprechen den in RFC 3279 ("Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile") angegebenen.

Der verwendete Signaturalgorithmus ist sha256WithRSAEncryption (1.2.840.113549.1.1.11).

7.1.4. Namensformen

Siehe 3.1.1

7.1.5. Namenseinschränkungen

Siehe 3.1.1

7.1.6. Anwendungsvorgaben Unterscheider

Diese Zertifizierungsrichtlinie hat folgenden Unterscheider (OID):

1.2.40.0.11.6.1.1.0.1

7.1.7. Verwendung von die Anwendungsvorgaben einschränkende Erweiterungen

Es werden keine, die Anwendungsvorgaben einschränkende Erweiterungen im Zertifikat verwendet.

7.1.8. Anwendungsvorgaben Syntax

Zertifikate, die entsprechend dieser Zertifizierungsrichtlinie ausgestellt wurden, enthalten den in 7.1.6 angegebenen Unterscheider (OID) in der dafür vorgesehen Erweiterung des Zertifikats.

7.1.9. Verarbeitung von kritischen Anwendungsvorgaben Erweiterungen

Keine Vorgaben.

7.2. Sperrlisten Profil

Sperrlisten (Certificate Revocation Lists – CRL) werden im Format X.509 Version 2 in Übereinstimmung mit dem RFC 5280 ausgestellt. Es werden ausschließlich gesamte Sperrlisten ausgestellt, Delta-Sperrlisten werden nicht verwendet.

7.2.1. Versionsnummern

Sperrlisten werden ausschließlich im Format X.509 Version 2 ausgestellt.

7.2.2. Sperrlisten und Sperrlisten Erweiterungen

Die URL zu der Sperrliste ist in der Zertifikatserweiterung CRLDistributionPoints enthalten.

In allen Sperrlisten werden die als nicht kritisch markierten Erweiterungen authorityKeyIdentifier und CRLNumber verwendet.

Für die Einträge in einer Sperrliste wird die als nicht kritisch markierte Erweiterung reasonCode verwendet.

7.3. OCSP Profil

Das Online Certificate Status Protokoll Service ist entsprechend Punkt 4.10 verfügbar.

7.3.1. Unterstützte Versionen

Das OCSP Service unterstützt Version 1 des OCSP-Protokolls entsprechend dessen Definition im Standard RFC 2560.

7.3.2. OCSP Erweiterung

Die URL zum OCSP Dienst ist in der Zertifikatserweiterung authorityKeyIdentifier enthalten.

8. Entsprechungen von Audit und anderen Kontrollvorgaben

Generell gilt, dass es sich bei dem gegenständlichen Zertifizierungsdienst um keine öffentlichen Zertifikate handelt und somit keinen spezifischen externen Auflagen oder Gesetzgebungen entsprochen werden muss.

Alle Entsprechungen basieren auf interne Richtlinien und werden innerhalb des ISMS der MA 01 - Wien Digital definiert und gesteuert.

8.1. Intervalle und Umstände von Überprüfungen

Ein externes Audit wird im Falle einer als relevant eingestufte Änderung am System, oder ansonsten mindestens einmal jährlich durchgeführt.

Die Sicherheitsentsprechungen, also die Auditziele, werden im ISMS der MA 01 - Wien Digital vorgegeben und die Ergebnisse in weiteren Maßnahmen verwaltet.

8.2. Auswahl und Qualifikation der überprüfenden Stellen

Die Überprüfungen werden durch Unternehmen, die unter anderem im Bereich von Einsatz und Verwendung von PKI-Komponenten und Risikodarstellungen qualifiziert sind, durchgeführt.

8.3. Abhängigkeiten der überprüfenden Stellen

Die überprüfende Stelle müssen in jeder Form unabhängig vom Betreiber agieren und Schlussfolgerungen ziehen können.

8.4. Themenbereiche einer Überprüfung (Mindestanforderungen)

Die Überprüfungen und die Risikoeinschätzungen entsprechen den Empfehlungen des BSI IT-Grundschutzhandbuches und den stets aktuellen Vorgaben der ETSI und RFC Standards.

Beispielhafte Themenbereiche sind:

- Sicherheitsvorgaben und Steuerungsmaßnahmen
- Physische Sicherheitsvorkehrungen
- Technologische Evaluation
- Vertraulichkeits- und Geheimhaltungsmaßnahmen
- Service-Level-Entsprechungen
- Einhaltung der Anwendungsvorgaben (Im Speziellen der ISMS-Policies zum sicheren Betrieb von Servern und Applikationen)

8.5. Maßnahmen im Falle von Mängelfeststellungen

Die Maßnahmen werden im Rahmen des ISMS der MA 01 - Wien Digital beschlossen und kommen umgehend zur Anwendung.

8.6. Kommunikation der Überprüfungsergebnisse

Die Ergebnisse werden ausschließlich an den Betreiber übergeben. Dieser definiert je nach Bedarf gesonderte Kommunikationsmaßnahmen, u.a. auf Basis der Vorschläge der überprüfenden Stelle.

9. Kommerzielle und gesetzliche Vorgaben

9.1. Gebühren

Beim gegenständlichen Zertifizierungsdienst kommen keine Zertifikatsgebühren zur Anwendung.

9.1.1. Gebühren zur Zertifikatsausstellung

Keine Anwendung.

9.1.2. Zertifikatsverwendungsgebühren

Keine Anwendung.

9.1.3. Gebühren zur Abfrage von Statusinformationen

Keine Anwendung.

9.1.4. Sonstige Gebühren

Keine Anwendung.

9.1.5. Refundierung von Gebühren

Keine Anwendung.

9.2. Finanzielle Verantwortung

Es gibt keine Anforderungen an die kommerzielle Haftbarkeit des Betreibers für den gegenständlichen Zertifizierungsdienst und keine gesonderten Regelungen innerhalb des Betreibers.

9.2.1. Versicherungsschutz durch Dritte

Keine Anwendung.

9.2.2. Weitere Regelungen

Keine Anwendung.

9.2.3. Haftbarkeiten für weitere Zertifikatsteilnehmer

Keine Regelung.

9.3. Vertraulichkeitspflichten

9.3.1. Geltungsbereich von vertraulichen Informationen

Jede Information über Personen oder Organisationen in Verbindung mit dem Zertifizierungsdienst gilt als vertraulich, sofern diese nicht explizit in gesonderten Regelungen anders definiert ist.

Alle Informationen werden nur in Rücksprache und mit Zustimmung der betroffenen Personen oder Organisationen weitergegeben.

9.3.2. Informationen die als nicht vertraulich gelten

Jede Information, die in Form eines Zertifikats veröffentlicht wird, gilt als nicht vertraulich.

9.3.3. Verantwortung zum Schutz vertraulich geltender Daten

Alle beschäftigten Personen im Rahmen des Zertifizierungsdienstes des Betreibers sind dazu angehalten, die vertrauenswürdigen Daten der Nutzer zu schützen und Verstöße umgehend dem Betreiber bekannt zu geben.

9.4. Schutz persönlicher Informationen

9.4.1. Datenschutzvorgaben

Alle beschäftigten Personen des Betreibers unterliegen den allgemeinen Datenschutzvorgaben des Betreibers.

9.4.2. Schützenswerte Daten

Alle Informationen, die nicht in Zertifikaten Verwendung finden, sind besonderen Schutzes würdig. Dazu zählen insbesondere potentielle Aktivierungsdaten.

9.4.3. Nichtschützenswerte Daten

Alle Informationen, die in Zertifikaten Verwendung finden und publiziert werden, bedürfen keines besonderen Schutzes

9.4.4. Verantwortungen zum Schutz der privaten Daten

Insbesondere die Aktivierungsdaten und die privaten Schlüssel sind von allen Beteiligten und allen betroffenen Entitäten dieser Zertifizierungsrichtlinie geheim zuhalten.

9.4.5. Zustimmungsvereinbarungen und Akzeptanz der Anwendungsvorgaben

Mit der Verwendung des Zertifikats (und der privaten Schlüssel) akzeptiert die Zertifikatsinhabende Person alle in dieser Richtlinie auferlegten Pflichten und erhält alle definierten Rechte.

Es existiert keine gesonderte Zustimmungsnötigkeit in schriftlicher oder anders nachweisbarer Form.

9.4.6. Einsichtsgewährung für allgemein überprüfende oder juristische Instanzen

Im Allgemeinen gilt keine Einsicht für Dritte, außer per gesetzlicher Befugnis. Auditoren wird die statistische Auswertung gestattet. Gesammelte Daten sind nach Abschluss des Audits kontrolliert zu vernichten.

9.4.7. Weitere Umstände der Einsichtnahme

Keine Anwendung.

9.5. Rechtswirksamkeit Geistiges Eigentum

Alle Rechtsansprüche, die ableitbar aus den produzierten Zertifikaten und den systemrelevanten Dokumentationen entstehen, liegen ausschließlich beim Betreiber, dem Magistrat der Stadt Wien.

Die Rechte am Zertifikat und an der Verwendung der Schlüssel liegen bei der Zertifikatsinhabenden Person.

9.6. Vertretungsbefugnisse, Repräsentanzen und Garantien

9.6.1. CA Repräsentanz und Garantien

Der CA-Betreiber garantiert, sich zur Gänze an die selbst auferlegten Vorgaben und Pflichten in gegenständlichem Dokument zu halten.

Es wird garantiert, dass nach bestem Wissen und Gewissen die Zertifikatsinformationen stets geprüft und zutreffend für den Zeitpunkt der Ausstellung gültig sind.

Weiters wird garantiert, dass stets an der Sicherstellung eines gesicherten und sicheren Betriebes des Zertifizierungsdienstes gearbeitet und dieser überwacht, kontrolliert und gesteuert wird.

9.6.2. RA Repräsentanz und Garantien

In gegenständlichem Fall ist die CA auch RA. Die getrennt voneinander agierenden Personen (SO, RO) unterliegen denselben Auflagen, Rechten und Pflichten.

9.6.3. Zertifikatsinhaber Repräsentanz und Garantien

Zertifikatsinhabende Personen gewährleisten:

- Den Schutz des privaten Schlüssels.
- Alle Angaben die zur Aufnahme ins Zertifikat führen sind Wahrheitsgemäß.
- Alle Informationen sind für die Gültigkeitsdauer des Zertifikats zutreffend.
- Das Zertifikat wird ausschließlich entsprechend der vorliegenden CPS verwendet.
- Im Falle, dass die Daten des Zertifikats sich ändern oder der Schlüssel kompromittiert wird, wird eine sofortige Sperre und/oder ein Widerruf veranlasst.

9.6.4. Zustimmung Vertrauender Parteien des Zertifizierungsdienstes (Akzeptanzstellen)

Akzeptanzstellen garantieren...:

- die zum Einsatz kommenden kryptografischen Mechanismen stets zu kontrollieren (also z.B.: jede Signatur technisch zu prüfen) und die Gültigkeit der Zertifikate stets zu überprüfen.
- , dass die Akzeptanz einer technischen Operation eines Schlüssels und des dazugehörigen Zertifikats zur Gänze der Akzeptanzstelle obliegt.

9.6.5. Weitere Regelungen

Alle involvierten Parteien stimmen den vorliegenden Regelungen zu und garantieren die Einhaltung der Rechte und Pflichten.

9.7. Erklärungsbestimmungen

Alle Vertragsvereinbarungen betreffend den Zertifizierungsdienst müssen einen Hinweis auf die betreffende Zertifizierungsrichtlinie beinhalten.

9.8. Einschränkungen der Verantwortlichkeit

Die Verantwortung ist auf die direkt in Zusammenhang mit dieser CPS stehenden Bestandteile eingeschränkt.

9.9. Entschädigungen

Keine Anwendung.

9.10. Inkrafttreten und Einstellung der Wirksamkeit der CPS

9.10.1. Inkrafttreten

Diese Richtlinie wird wirksam mit Ausstellung des ersten Zertifikats basierend auf den gegenständlichen Anwendungsvorgaben.

9.10.2. Einstellung der Wirksamkeit

Diese CPS ist gültig, bis ein Ersatz durch eine neue Version definiert und veröffentlicht wird.

9.10.3. Regelungen bei Einstellung der Wirksamkeit

Keine gesonderten Regelungen.

9.10.4. Effekte bei Einstellung der Wirksamkeit

Die Einstellung der Wirksamkeit hat keinen Einfluss auf die Regelungen des geistigen Eigentums.

9.11. Individuelle Benachrichtigungen und Kommunikationsformen der Beteiligten

Es gibt keine Einschränkungen, sofern alle Beteiligten ihr Einverständnis bekunden.

9.12. Korrekturen

9.12.1. Prozesse zur Einpflege von Korrekturen

Die Veröffentlichung von Korrekturen zu diesem Dokument erfolgt nach der Dokumentenlenkung der MA 01.

Bei jeder Fassung wird eine Liste an relevanten Änderungen angeführt.

9.12.2. Bekanntmachungsmechanismen

Keine gesonderten Regelungen.

9.12.3. Umstände für eine Änderung der OID

Im Falle einer Veränderung der die Sicherheit betreffenden Vorgaben oder der zum Einsatz kommenden Technik muss eine neue OID das Dokument erkennbar als neu ausweisen. Dies muss in den Zertifikaten erkennbar sein.

9.13. Schlichtungsbestimmungen

Keine gesonderten Regelungen.

9.14. Geltende Rechtslage

Es gibt keine zutreffenden übergeordneten Gesetzgebungen.

9.15. Einhaltung der existierender Rechtslage

Dieses Dokument hat keine gesetzlichen Vorgaben.

9.16. Weitere Bestimmungen

9.16.1. Allgemeine Vereinbarungen

Keine Anwendung.

9.16.2. Zutreffende Aufgabenstellungen

Keine Anwendung.

9.16.3. Salvatorische Klausel

Jedwede Bestimmung dieses Dokuments, sofern als nicht zutreffend, nicht geeignet, oder widersinnig reklamiert, beeinflusst nicht die weiteren Bestimmungen der Vereinbarungen dieses Dokuments.

9.16.4. Klagbarkeit

Keine Anwendung.

9.16.5. Höhere Gewalt

Der Betreiber kann nicht für Ereignisse außerhalb seiner unmittelbaren Kontrolle haftbar gemacht werden.

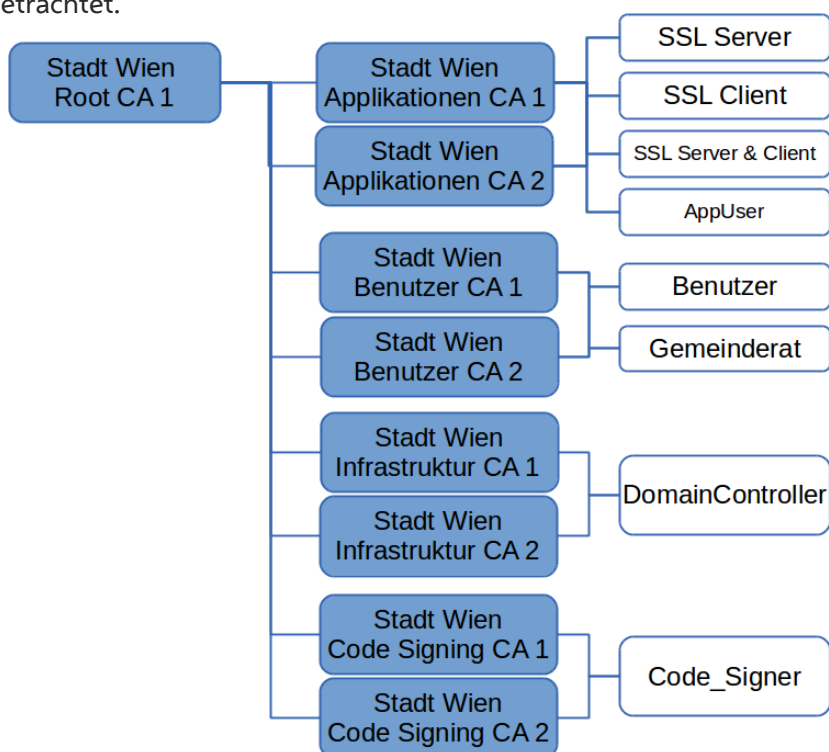
Sonstige Bestimmungen

Keine.

10. Anhang A

10.1. Zertifikatsprofile

Entsprechend der folgenden Darstellung der Zertifikats-Hierarchie des ZDA gibt es ein Wurzelzertifikat, mehrere Ausstellungszertifikate und unter jedem Ausstellungszertifikat ein oder mehrere Zertifikatsprofile. Im Zuge dieser Zertifizierungsrichtlinie werden nur Zertifikate unter der „Stadt Wien Benutzer CA“ betrachtet.



10.1.1. Stadt Wien Root CA

Stadt Wien Root CA	
Identifizierung & Authentifizierung	
Bei CA Zertifikaten gibt es keine Identifizierung oder Authentifizierung.	
Registrierungsprozess	
Bei CA Zertifikaten gibt es keine Registrierung	
Schlüssel Parameter	
Algorithmus	RSA
Schlüssel Generierung	innerhalb eines HSMs durch 2 Security Officer
Schlüssellänge	4096 bit

Schlüsselverwendung	CertificateSigning, CRLSigning	
Übermittlung des privaten Schlüssels	-	
Übermittlung des öffentlichen Schlüssels	-	
Zertifikats-Generierung		
Wurzelzertifikate sind selbst signiert und werden durch 2 Security Officer generiert.		
Gültigkeit	20 Jahre	
Zertifikats-Übermittlung		
CA Zertifikate werden auf der Webseite des ZDAs veröffentlicht.		
Zertifikats-Inhalt		
Feld	Inhalt	Wert
Version	3	Fix
Serien Nummer	Eindeutige Nummer	generiert
Signaturalgorithmus	SHA256withRSAEncryption	Fix
Ausstellende Instanz		
Common Name (CN)	Name und Generation	"Stadt Wien Root CA #"
Organisation (O)	"Stadt Wien"	Fix
Country (C)	"AT"	Fix
Antragstellende Instanz		
Common Name (CN)	Name und Generation	"Stadt Wien Root CA #"
Organisation (O)	"Stadt Wien"	Fix
Country (C)	"AT"	Fix
Erweiterungen		
KeyUsage	CertSign, CRLSign	Fix
Enhanced Key	Keine	
Thumbprint Algorithms	SHA1	berechnet
Thumbprint	Hash-Wert	berechnet
Subject Key Identifier	Schlüssel Identifikation	generiert

10.1.2. Stadt Wien Benutzer CA

Stadt Wien Benutzer CA		
Identifizierung & Authentifizierung		
Bei CA Zertifikaten gibt es keine Identifizierung oder Authentifizierung.		
Registrierungs-Prozess		
Bei CA Zertifikaten gibt es keine Registrierung		
Schlüssel Parameter		
Algorithmus	RSA	
Schlüssel Generierung	innerhalb eines HSMs durch 2 Security Officer	
Schlüssellänge	4096 bit	
Schlüsselverwendung	CertificateSigning, CRLSigning	
Übermittlung des privaten Schlüssels	-	
Übermittlung des öffentlichen Schlüssels	-	
Zertifikats-Generierung		
Werden von der Root CA ausgestellt und durch 2 Security Officer generiert.		
Gültigkeit	10 Jahre	
Zertifikats-Übermittlung		
CA Zertifikate werden auf der Webseite des ZDAs veröffentlicht.		
Zertifikats-Inhalt		
Feld	Inhalt	Wert
Version	3	Fix
Serien Nummer	Eindeutige Nummer	generiert
Signaturalgorithmus	SHA256withRSAEncryption	Fix
Ausstellende Instanz		
Common Name (CN)	Name und Generation	“Stadt Wien Benutzer CA #“
Organisation (O)	“Stadt Wien“	Fix
Country (C)	“AT“	Fix
Antragstellende Instanz		
Common Name (CN)	Name und Generation	“Stadt Wien

		Benutzer CA #"
Organisation (O)	"Stadt Wien"	Fix
Country (C)	"AT"	Fix
Erweiterungen		
KeyUsage	CertSign, CRLSign	Fix
Enhanced Key	Keine	
Thumbprint Algorithms	SHA1	berechnet
Thumbprint	Hash-Wert	berechnet
Subject Key Identifier	Schlüssel Identifikation	Generiert
Authority Key Identifier	Schlüssel Identifikation	Subject Key Identifier des Wurzelzertifikats

10.1.3. Benutzer Zertifikate

Benutzer Zertifikate	
Identifizierung & Authentifizierung	
<p>Die Antragstellung erfolgt über eine gesicherte Webapplikation, welche nur für ausgewählte und berechnigte Personen zugänglich ist. Die Identifizierung erfolgt über ein der Applikation vorgeschaltetes Sicherheitsportal, am dem sich die Antragstellende Person mit Anmeldenamen und Passwort authentifiziert.</p>	
Registrierungs-Prozess	
<p>Die Antragstellende Person füllt in einer gesicherten Webapplikation ein webbasiertes Antragsformular aus, welches neben den Kontaktdaten auch die Zertifikatsinformation und einen Zertifikatsantrag im PKCS#10 Format (entfällt bei der Schlüsselgenerierung durch die CA) enthält. Hierbei werden alle für das Zertifikat relevanten Daten aus Drittsystemen vorausgefüllt und sind für die Antragstellende Person nicht änderbar.</p> <p>Der Antrag wird nach dem Absenden automatisch von der RA Software auf formale Korrektheit und Vollständigkeit überprüft. Sind alle Angaben korrekt, wird der Antrag automatisch an die CA weitergereicht, welche automatisch (ohne weitere Genehmigung eines ROs) das Zertifikat ausstellt.</p> <p>Die Antragstellende Person erhält daraufhin die Information per E-Mail, dass ihr Zertifikat über die gesicherte Webapplikation abgeholt werden kann.</p>	
Schlüssel Parameter	
Algorithmus	RSA
Schlüssel Generierung	Durch den Antragstellende Person oder durch die CA
Schlüssellänge	2048 / 4096 bit

Schlüsselverwendung	DigitalSignature, NonRepudiation, KeyEncipherment	
Erweiterte Schlüsselverwendung	Client-Authentication, E-Mail-Security	
Übermittlung des privaten Schlüssels	<p>Im Fall der Generierung des Schlüssels durch die CA wird der</p> <p>private Schlüssel der Antragstellenden Person in Form einer PKCS#12</p> <p>Datei über die Antrags-Webseite zu Verfügung gestellt. Für den Download ist das bei der Antragstellung vom Antragstellenden Person selbst gewählte Passwort notwendig, mit welchem auch der private Schlüssel innerhalb der PKCS#12 Datei geschützt ist.</p>	
Übermittlung des öffentlichen Schlüssels	<p>Im Fall der Generierung des Schlüssels durch die Antragstellenden Person wird der CA der öffentliche Schlüssel über die Antrags-Webseite in Form eines PKCS#10 Antrags übermittelt.</p> <p>Im Fall der Generierung des Schlüssels durch die CA wird der Antragstellenden Person der öffentliche Schlüssel in Form des ausgestellten Zertifikats gemeinsam mit dem privaten Schlüssel übermittelt.</p>	
Zertifikats-Generierung		
Alle Nutzungszertifikate werden von der „Stadt Wien Benutzer CA #“ ausgestellt.		
Gültigkeit	5 Jahre	
Zertifikats-Übermittlung		
Die Zertifikate können durch die Antragstellende Person über die Antrags-Webseite heruntergeladen werden.		
Zertifikats-Inhalt		
Feld	Inhalt	Wert
Version	3	Fix
Serien Nummer	Eindeutige Nummer	generiert
Signaturalgorithmus	SHA256withRSAEncryption	Fix
Ausstellende Instanz		
Common Name (CN)	Name des Ausstellenden Persons („#“ gibt die Generation an)	“Stadt Wien Benutzer CA #“
Organisation (O)	“Stadt Wien“	Fix
Country (C)	“AT“	Fix

Antragstellende Instanz		
Common Name (CN)	Name der Antragstellenden Person	Aus Drittsystem (nicht editierbar)
Organisational Unit (OU)	Abteilung / Applikationsbetreiber	Aus Drittsystem (nicht editierbar)
Organisation (O)	"Stadt Wien"	Fix
Country (C)	"AT"	Fix
Erweiterungen		
KeyUsage	DigSig, NonRep, KeyEnc	Fix
Enhanced Key Usage	ClientAuth, E-Mail-Sec	Fix
Thumbprint Algorithms	SHA1	berechnet
Thumbprint	Hash-Wert	berechnet
Subject Key Identifier	Schlüssel Identifikation	generiert
Authority Key Identifier	Schlüssel Identifikation	Subjekt Key Identifier der Ausstellungs-CA

10.1.4. Gemeinderat Zertifikate

Gemeinderat Zertifikate
Identifizierung & Authentifizierung
Die Antragstellung erfolgt über eine gesicherte Webapplikation welche nur für ausgewählte und berechnigte Personen zugänglich ist. Die Identifizierung erfolgt über ein, der Applikation vorgeschaltetes, Sicherheitsportal wo sich die Antragstellende Person mit Anmeldeamen und Passwort authentifiziert.
Registrierungs-Prozess
<p>Die Antragstellende Person füllt in einer gesicherten Webapplikation ein webbasiertes Antragsformular aus, welches neben den Kontaktdaten auch die Zertifikatsinformation und einen Zertifikatsantrag im PKCS#10 Format (entfällt bei der Schlüsselgenerierung durch die CA) enthält. Hierbei werden alle für das Zertifikat relevanten Daten aus Drittsystemen vorausgefüllt und sind für die Antragstellende Person nicht änderbar.</p> <p>Der Antrag wird nach dem Absenden von einem Registration Officer begutachtet. Dieser prüft neben der allgemeinen Plausibilität und Vollständigkeit, die enthaltenen Domain-Namen gegen eine Whitelist von zulässigen Domains.</p> <p>Sind alle Angaben korrekt, genehmigt der Registration Officer den Zertifikatsantrag, wodurch die eigentliche Zertifikatsausstellung ausgelöst wird.</p>

Die Antragstellende Person erhält daraufhin die Information per E-Mail, dass sein Zertifikat über die gesicherte Webapplikation abgeholt werden kann.		
Schlüssel Parameter		
Algorithmus	RSA	
Schlüssel Generierung	Durch die CA	
Schlüssellänge	2048 / 4096 bit	
Schlüsselverwendung	DigitalSignature, NonRepudiation, KeyEncipherment	
Erweiterte Schlüsselverwendung	Client-Authentication	
Übermittlung des privaten Schlüssels	<p>Im Fall der Generierung des Schlüssels durch die CA wird der</p> <p>private Schlüssel der Antragstellenden Person in Form einer PKCS#12</p> <p>Datei über die Antrags-Webseite zur Verfügung gestellt. Für den Download ist das bei der Antragstellung von der Antragstellenden Person selbst gewählte Passwort notwendig, mit welchem auch der private Schlüssel innerhalb der PKCS#12 Datei geschützt ist.</p>	
Übermittlung des öffentlichen Schlüssels	<p>Im Fall der Generierung des Schlüssels durch die Antragstellende Person wird der CA der öffentliche Schlüssel über die Antrags-Webseite in Form eines PKCS#10 Antrags übermittelt.</p> <p>Im Fall der Generierung des Schlüssels durch die CA wird der Antragstellende Person der öffentliche Schlüssel in Form des ausgestellten Zertifikats gemeinsam mit dem privaten Schlüssel übermittelt.</p>	
Zertifikats-Generierung		
Alle Endnutzungszertifikate werden von der „Stadt Wien Benutzer CA #“ ausgestellt.		
Gültigkeit	5 Jahre, jedoch maximal bis zum Ende der nächsten Legislaturperiode (aktuell 31.10.2020)	
Zertifikats-Übermittlung		
Die Zertifikate können durch die Antragstellende Person über die Antrags-Webseite heruntergeladen werden.		
Zertifikats-Inhalt		
Feld	Inhalt	Wert
Version	3	Fix
Serien Nummer	Eindeutige Nummer	generiert

Signaturalgorithmus	SHA256withRSAEncryption	Fix
Ausstellende Instanz		
Common Name (CN)	Name der Ausstellenden Person („#“ gibt die Generation an)	“Stadt Wien Benutzer CA #“
Organisation (O)	“Stadt Wien”	Fix
Country (C)	“AT”	Fix
Antragstellende Instanz		
Common Name (CN)	Name der Antragstellenden Person	Frei wählbar
Organisational Unit (OU)	Gemeinderats-Klub Ein Wert aus Auswahl: KSP, KGR, KNE, KVP, KFP, MA 01	DropDown
Organisation (O)	“Stadt Wien”	Fix
Country (C)	“AT”	Fix
Erweiterungen		
KeyUsage	DigSig, NonRep, KeyEnc	Fix
Enhanced Key Usage	ClientAuth	Fix
Thumbprint Algorithms	SHA1	berechnet
Thumbprint	Hash-Wert	berechnet
Subject Key Identifier	Schlüssel Identifikation	generiert
Authority Key Identifier	Schlüssel Identifikation	Subjekt Key Identifier der Ausstellungs- CA

11. Abkürzungsverzeichnis / Erläuterungen

Kurzform / Begriff	Erklärung
[Frei verfügbar]	Vertraulichkeitsstufe: Frei verfügbar
C	Country
CA	Certificate Authority
CN	Common Name
CPS	Certification Practice Statement
CRL	Certificate Revocation List
d.h.	das heißt
DN	Distinguished Name
etc.	et cetera
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISMS	Information Security Management System
LDAP	Lightweight Directory Access Protocol
MA	Magistratsabteilung
min.	Minuten
Nr.	Nummer
Nr.	Nummer
O	Organisation
OCSP	Online Certificate Status Protocol
OE	Organisationseinheit
OID	Object Identifier
OU	Organisational Unit
PIN	Persönliche Identifikationsnummer
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
POL	Abkürzung für Policy (= Dokumentenart)
RA	Registration Authority
RO	Registration Officer
RSA	Random sequential adsorption
SA	System Admin

Kurzform / Begriff	Erklärung
SO	Security Officer
u.a.	unter anderem
z.B.	zum Beispiel
ZDA	Zertifizierungsdiensteanbietende Stelle

12. Linkverzeichnis

Beschreibung	Link
OCSP Dienst	http://ocsp.wien.gv.at/ocsp/
RFC-3647	https://www.ietf.org/rfc/rfc3647.txt
ZDA Magistrat der Stadt Wien	https://www.wien.gv.at/kontakte/ma01/zertifikate.html

13. Versionshistorie

V1.0.0 – SDS1-Team – Pfaffenbichler Franz Xaver		gültig: ab 28.01.2021
Änderungen: Erstversion		
Überprüft von	SEC-TL – Steiner Wolfgang, GAT1-TL – Schifferl Peter, Management Board – TeilnehmerInnen	
Freigabe am	28.01.2021 durch AL – Nabicht Werner	

Übersicht – Dokumentendaten	
Titel	Zertifizierungsrichtlinie für Endnutzungszertifikate
Untertitel	Certification Practice Statement (CPS)
Klassifizierungsstufe	[Frei verfügbar]
Gültigkeitszeitraum	Gültig ab Freigabe bis siehe ASP
Inhaltlich überprüft von	SEC-TL – Steiner Wolfgang, GAT1-TL – Schifferl Peter, Management Board – TeilnehmerInnen
Freigabestatus	Freigegeben am 28.01.2021 durch AL – Nabicht Werner
Ersetzt	–
AutorIn	SDS1-Team – Pfaffenbichler Franz Xaver
Version erstellt von	-
Beiträge von	SEC-TL – Steiner Wolfgang
Verantwortliche OE	GB_BE-BTS4
Änderungsberechtigt	BTS3-Team, BTS4-Team
Dokumentenkenzeichnung Themenkreis-Dokumentenart- LfdNr-Kurzbezeichnung (Betreff)- Version	ITSM-POL-7-CPS_BenutzerCA-V1.0.0
Ablageort	https://www.wien.gv.at/kontakte/ma01/pdf/zertifizierungsrichtlinie-benutzer.pdf ELAK: 1161396-2020-1
Vorlagenversion	MGMTS-VOR-Dokument-Lang-V3.1.1