CP/CPS – Stadt Zuerich CAs

Certificate Policy (CP) und Certification Practice Statement (CPS) der Certification Authorities (CA) der städtischen Public Key Infrastruktur (PKI)

Erstellerin
Stadt Zürich
Organisation und Informatik
Fachstelle Informationssicherheit
Albisriederstrasse 201
Postfach, 8022 Zürich

Tel. +41 44 412 91 11
Fax +41 44 412 93 85
www.stadt-zuerich.ch/oiz

Verfasser/in
P. Lips

Version
2.0

Versions-Nr.	Datum	Name	Tätigkeit
1.0	16.06.06	oizbae	Ersterstellung
2.0	18.06.13	oizlip	Zusammenfassung der CP/CPS aller städtischen CAs

Inhalt

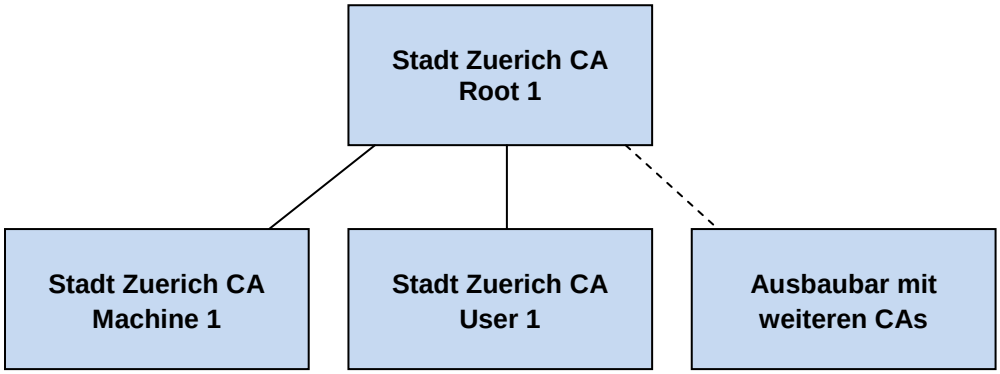
1 Einführung

1.1 Übersicht

1.1.1 CA Hierarchie

Die Organisation und Informatik (OIZ) ist als Informatik-Kompetenzzentrum der Stadt Zürich für IT-Basisdienstleistungen und departementsübergreifende IT-Projekte zuständig. Die zentrale städtische Public Key Infrastruktur (PKI) ist eine dieser IT-Basisdienstleistungen.

Die städtische PKI weist folgende zweistufige Hierarchie auf:



Die städtische PKI umfasst demnach aktuell drei CAs:

- Root CA: «Stadt Zuerich CA Root 1»
- Issuing CAs: «Stadt Zuerich CA Machine 1» und «Stadt Zuerich CA User 1»

Ein Ausbau mit weiteren Issuing CAs ist möglich.

1.1.2 Zertifikatsklassen und Zertifikatstypen

Die Stadtverwaltung Zürich lehnt sich bei den Zertifikatsklassen an die Bundesverwaltung an. Diese kennt vier Klassen von Zertifikaten mit unterschiedlichen Vertrauensniveaus:

Klasse	Registrierung	Ausgabeart	Funktion
A	Persönliche Identifikation	HW-Token	Rechtsgültige Signatur (ZertES)
B	Persönliche Identifikation	HW-Token	Signatur, Verschlüsselung, starke Authentisierung
C	Administrative Identifikation	Soft-Token	Signatur, Verschlüsselung, Authentisierung
D	Administrative Identifikation	Soft-Token	Authentisierung

Die Stadtverwaltung Zürich setzt dabei Zertifikate der Klasse C ein. Diese weisen zusammengefasst die folgenden Eigenschaften auf:

Funktion	Personenzertifikate – Verschlüsselung und Signatur von E-Mails – Benutzeranmeldung an Applikationen – Code-Signatur Maschinenzertifikate – SSL-Verschlüsselung (interne Verbindungen) – Client- und Server-Authentisierung (interne Geräte) Die Zertifikate werden normalerweise nur im Intranet genutzt.
Speichermedium	Die ausgestellten Zertifikate werden als Soft-Token im Benutzerprofil (Certificate Store) oder auf dem Client/Server gespeichert. Ausnahmen: CA-Zertifikate sind auf einem Hardware Security Modul gespeichert.
Qualität	Administrative Verfahren zur Zertifikatsausgabe: Es ist keine Überprüfung der Identität von Personen notwendig; die Zuweisung von Benutzern zur entsprechenden AD-Berechtigungsgruppe genügt in der Regel zum Bezug von Zertifikaten. Wenn immer möglich kommen Auto-Enrollment oder Self-Enrollment zum Einsatz. Personenzertifikate bestätigen somit, dass – der angegebene User und die E-Mail-Adresse im AD existiert. – sich der Benutzer erfolgreich am Active Directory angemeldet hat – der Besitzer des zugehörigen öffentlichen Schlüssels Zugriff auf diese E-Mail-Adresse hat. – die Zertifikate denselben Trustlevel haben wie die Windows-Authentisierung mit Username und Passwort. Für Maschinen gilt zusätzlich – der angegebene Domainname existiert. – die angegebene E-Mail Adresse existiert.

1.2 Name und Identifikation des Dokuments

Das vorliegende Dokument trägt die Bezeichnung «*Certificate Policy (CP) und Certification Practice Statement (CPS) der Certification Authorities (CA) der städtischen Public Key Infrastruktur*» (kurz: «CP/CPS – Stadt Zuerich CAs»).

Die Struktur des Dokuments entspricht dem RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

OID der CP/CPS: 1.3.6.1.4.1.13569.10.20.3.1.

1.3 PKI-Teilnehmer

1.3.1 Certification Authorities (CA)

Die städtische PKI besteht aus den folgenden CAs:

CA	Beschreibung	
Root CA	Bezeichnung	«Stadt Zuerich CA – Class C – Root 1»
	Zweck	Die städtische Root CA stellt Klasse C Zertifikate für alle untergeordneten Issuing CAs aus
	Namensraum	Die Root CA stellt Zertifikate für folgende Namenräume aus: – C = CH – O = Stadt Zuerich – E = pki@zuerich.ch
User CA	Bezeichnung	«Stadt Zuerich CA – Class C – User 1»
	Zweck	Die User CA stellt Zertifikate für Personen aus
	Namensraum	Zertifikate werden für die folgenden Namenräume ausgestellt: – C = CH – O = Stadt Zuerich – OU = Departement/Dienstabteilung (gemäss städtischen Namenskonventionen) – E = pki@zuerich.ch
Machine CA	Bezeichnung	«Stadt Zuerich CA – Class C – Machine 1»
	Zweck	Die Machine CA stellt Zertifikate für Geräte aus (Clients, Server, Netzwerkgeräte etc.)
	Namensraum	Zertifikate werden für die folgenden Namenräume ausgestellt: – C = CH – O = Stadt Zuerich oder Marketingnamen – OU = Departement/Dienstabteilung (gemäss städtischen Namenskonventionen) – E = pki@zuerich.ch

1.3.2 Registration Authorities (RA)

Für die Zertifikate der städtischen PKI sind wenn immer möglich Auto-Enrollment resp. Self-Enrollment vorgesehen. Ein persönliches Vorsprechen bei einer RA im Sinne einer organisatorischen Stelle ist nicht erforderlich.

Die Rolle der RA wird implizit durch das Active Directory (AD) und dessen Betreiber resp. durch [CA-ADMIN] und [IT-SEC] (siehe auch Kap. 1.6) wahrgenommen.

1.3.3 Zertifikatsinhaber (Subscriber)

CA	Beschreibung
Root CA	Als Nutzer der Root CA gelten insbesondere die Verantwortlichen von untergeordneten CAs.
User CA	Nutzer der User CA sind Personen, insbesondere Mitarbeitende der Stadtverwaltung, die im Active Directory (AD) erfasst sind.
Machine CA	Nutzer der Machine CA sind technische User. Konkret handelt es sich um städtische Geräte (Clients, Server, Netzwerkgeräte etc.), Programme oder Dienste.

1.3.4 Externe Zertifikatsnutzer (Relying Parties)

Die städtische PKI wird hauptsächlich innerhalb der Stadtverwaltung genutzt.

Die Nutzung oder Verifikation städtischer Zertifikate durch externe Partner ist nach Installation der städtischen CA-Zertifikate möglich.

1.3.5 Weitere Teilnehmer

Keine.

1.4 Zertifikatsverwendung

Städtische Zertifikate dürfen für die in Kapitel 1.1.2 beschriebenen Einsatzgebiete verwendet werden. Andere Verwendungszwecke sind nicht zugelassen.

1.5 Verwaltung der Policy

1.5.1 Organisation der Dokumentenverwaltung

Für die Pflege des vorliegenden CP/CPS-Dokuments ist [IT-SEC] verantwortlich. Die CP/CPS wird im Einklang mit folgenden Regelungen gehalten:

- Handbuch Informationssicherheit der Stadt Zürich
- RFC 3647.

1.5.2 Kontaktstellen / Rollen

Kontaktstelle für dieses Dokument:

Stadt Zürich
Organisation und Informatik
Fachstelle Informationssicherheit
Albisriederstrasse 201 / Postfach
CH-8022 Zürich
Tel: +41 44 412 91 11
itsec@zuerich.ch

Die für Endbenutzer relevanten Kontaktstellen werden auf den in Kapitel 2 erwähnten Websites aufgeführt.

1.5.3 Genehmigungsverfahren

Anpassungen an diesem Dokument werden durch [IT-SEC] vorgenommen. Zusätzliche Informationen sind in Kap. 9.12 beschrieben.

1.6 Definitionen und Abkürzungen

In diesem Abschnitt werden einige wichtige Begriffe und Abkürzungen erklärt, die im Dokument verwendet werden. Die Begriffe sind aus Gründen der Verständlichkeit und Einhaltung der Standards teilweise in Englisch.

AD	Active Directory
[ADMIN]	Server- oder Netzwerkadministration/-Betrieb
Auto-Enrollment	Automatisierter Bezug von Zertifikaten (siehe auch Self-Enrollment)
CA	Certification Authority (Zertifizierungsstelle)
[CA-ADMIN]	CA-Administration/-Betrieb
CP	Certificate Policy Typischerweise bezeichnet die CP einen Satz von Regeln, die den Einsatz der Zertifikate für eine Organisation oder eine Klasse von Anwendungen beschreiben.
CPS	Certification Practice Statement (CPS) Die CPS ist eine detailliertere Beschreibung als die CP und beinhaltet zusätzlich die PKI-Prozesse.
CRL	Certificate Revocation List; Liste der zurückgezogenen Zertifikate
DN	Distinguished Name: Identifiziert den Eigner des Zertifikates
HSM	Hardware Security Modul (sicherer Hardware Schlüsselspeicher)
[HSM-ADMIN]	HSM-Administration/-Betrieb
[IT-SEC]	Fachstelle Informationssicherheit (Kontaktstelle für CP/CPS)
OCSP	Online Certificate Status Protocol
OID	Object Identifier; weltweit eindeutiger Identifikator für die Bezeichnung von Dokumenten/Objekten.
RA	Registration Authority (Registrierungsstelle)
SCEP	Simple Certificate Enrollment Protocol; unterstützt den automatisierten Bezug von Zertifikaten und CRL durch Geräte und Programme.
Self-Enrollment	Automatisierte Ausgabe von Zertifikaten aufgrund von Useranfragen (siehe auch Auto-Enrollment)
[SERVICEDESK]	Zentraler Service Desk von OIZ
[USER]	Im Active Directory erfasste Mitarbeitende
ZertES	Bundesgesetz zu qualifizierten Zertifikaten

2 Publikation und Verzeichnisdienste

2.1 Publikation von Informationen

Die Verantwortung für die Publikation von Zertifikaten, CRLs und zugehörigen Dokumenten liegt bei der OIZ.

Die Informationen werden auf den folgenden beiden Webseiten im Intranet der Stadt resp. im Internet publiziert:

Website	Inhalt

Intranet: http://pki.intra.stzh.ch	– Übersicht der PKI Umgebung
	– Dokumente:
	  – Nutzungsrichtlinien
	  – Städtische Rechtsgrundlagen
	  – Beschreibungen, Anleitungen
	– Zertifikatsmanagement:
	  – Link auf die Zertifikat-Antragsseiten
	– Kontaktstellen

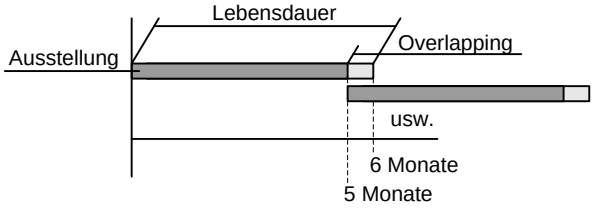
Internet: http://pki.stzh.ch	– Dokumente:
	  – Aktuelle Version der CP/CPS
	– Zertifikatsmanagement:
	  – Zertifikate der CAs
	  – CRL (Zertifikatssperrlisten)
	– Kontaktstellen

2.2 Publikationsintervalle

Für die CAs der städtischen PKI gelten die folgenden Publikationsintervalle:

2.2.1 Root CA

CRL
– Aktualisierung des CRL-Verzeichnisses: Bei Publikation neuer CRL
– Ausstellung der CRL: Alle 5 Monate
– Lebensdauer der CRL: 6 Monate
– Overlapping der CRL: 1 Monat
– Delta CRL: Nein

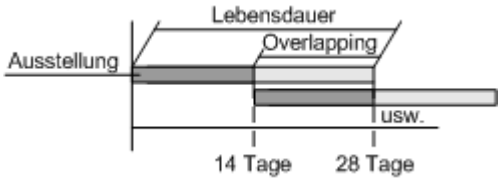


– CRL-Veröffentlichungspunkt: http://pki.stzh.ch/pki/crl/

CA-Zertifikat
– Publikation manuell

2.2.2 User CA

CRL
– Aktualisierung des CRL-Verzeichnisses: Täglich
– Ausstellung der CRL: Alle 14 Tage
– Lebensdauer der CRL: 28 Tage
– Overlapping der CRL: 14 Tage
– Delta CRL: Nein

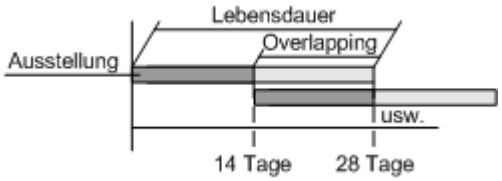


– CRL-Veröffentlichungspunkt:
  – Primär: http://pki.stzh.ch/pki/crl/
  – Sekundär: ldap:/// (Standard AD-Integration)

CA-Zertifikat
– Publikation manuell

2.2.3 Machine CA

CRL
– Aktualisierung des CRL-Verzeichnisses: Täglich
– Ausstellung der CRL: Alle 14 Tage
– Lebensdauer der CRL: 28 Tage
– Overlapping der CRL: 14 Tage
– Delta CRL: Nein



– CRL-Veröffentlichungspunkt:
  – Primär: http://pki.stzh.ch/pki/crl/
  – Sekundär: ldap:/// (Standard AD-Integration)

CA-Zertifikat
– Publikation manuell

2.3 Zugriffsschutz auf Verzeichnisse

Die oben genannten Webseiten sind für städtische Mitarbeitende und im Auftragsverhältnis stehende externe Mitarbeitende im Züri-Netz lesend zugänglich.

Auf das Publikationsverzeichnis haben nur [CA-ADMIN] Schreibrechte.

3 Identifikation und Authentisierung

In den folgenden Abschnitten werden die Prozesse für die Identifikation und Authentisierung der CA-Nutzer beschrieben.

3.1 Namensgebung

Die städtischen CAs verfügen über eigene ausgeprägte Prozesse. Diese gewährleisten, dass

- die Identität der Nutzer für den in dieser CP/CPS vorgesehenen Verwendungszweck hinreichend festgestellt wurde
- die Zertifikate eine gültige E-Mail-Adresse beinhalten
- die Namensgebung den städtischen Richtlinien entspricht.

Die Namen von CAs der städtischen PKI werden wie folgt gebildet:

«Stadt Zuerich CA – Class C – [Typ] [Laufnummer]»

- Typ: Root, User, Machine;
- Laufnummer: 1, 2, …

3.1.1 Root CA

Namensarten	Die Root CA «Stadt Zuerich CA – Class C – Root 1» stellt Zertifikate für untergeordnete CAs aus. Der Subject Name der ausgegebenen Zertifikate entspricht X.500 Distinguished Names (DN). Die folgenden Felder werden verlangt: CN = Name der untergeordneten CA. Beispiele: «Stadt Zuerich CA – Class C – Machine 1» und «Stadt Zuerich CA – Class C – User 1» E = E-Mail-Adresse der zuständigen Organisation: p-ki@zuerich.ch
Aussagekräftige Namen	Die nach obigen Regeln erstellten Benennungen sind selbstredend.
Anonymisierung oder Pseudonymisierung	Die CA erstellt städtische Zertifikate. Eine Anonymisierung bzw. Pseudonymisierung ist nicht notwendig.
Regeln für die Auslegung unterschiedlicher Namensarten	Nicht anwendbar.
Eindeutigkeit von Namen	Die Namen müssen eindeutig sein, dies muss bei der Ausgabe eines neuen Zertifikats gewährleistet werden.
Erkennung, Authentisierung und Rolle von Marken	Nicht anwendbar.

3.1.2 User CA

Namensarten	Die User CA «Stadt Zuerich CA – Class C – User 1» stellt Zertifikate für Benutzer aus. Der Subject Name der ausgegebenen Zertifikate entspricht X.500 Distinguished Names (DN). Die folgenden Felder werden verlangt: CN = User-Name aus dem AD E = E-Mail-Adresse aus dem AD
Aussagekräftige Namen	Die nach obigen Regeln erstellten Benennungen sind selbstredend.
Anonymisierung oder Pseudonymisierung	Die CA erstellt städtische Zertifikate. Eine Anonymisierung bzw. Pseudonymisierung ist nicht notwendig.
Regeln für die Auslegung unterschiedlicher Namensarten	Nicht anwendbar.
Eindeutigkeit von Namen	Die Namen müssen eindeutig sein, dies muss bei der Ausgabe eines neuen Zertifikats gewährleistet werden.
Erkennung, Authentisierung und Rolle von Marken	Nicht anwendbar.

3.1.3 Machine CA

Namensarten	Die Machine CA «Stadt Zuerich CA – Class C – Machine 1» stellt Zertifikate für Geräte (Server, Clients, Router, etc.) aus. Der Subject Name der ausgegebenen Zertifikate entspricht X.500 Distinguished Names (DN). Die folgenden Felder werden verlangt: CN = Domainname des Geräts E = E-Mail-Adresse der zuständigen Organisation: p-ki@zuerich.ch
Aussagekräftige Namen	Die nach obigen Regeln erstellten Benennungen sind selbstredend.
Anonymisierung oder Pseudonymisierung	Die CA erstellt städtische Zertifikate. Eine Anonymisierung bzw. Pseudonymisierung ist nicht notwendig.
Regeln für die Auslegung unterschiedlicher Namensarten	Nicht anwendbar.
Eindeutigkeit von Namen	Die Namen müssen eindeutig sein, dies muss bei der Ausgabe eines neuen Zertifikats gewährleistet werden.
Erkennung, Authentisierung und Rolle von Marken	Nicht anwendbar.

3.2 Anträge für Zertifikatsausstellung

3.2.1 Root CA

Notwendige Credentials	Antragsteller mit Projektantrag für die Implementation einer neuen Issuing CA.
Authentizitätsprüfung der Credentials	– Vier-Augen-Prinzip auf Basis Split-Passwort. – Anwesenheit von [CA-ADMIN] und [IT-SEC].
Enrollment	Das Enrollment erfolgt manuell durch den [CA-ADMIN] an der Konsole. Der Antrag wird von der CA auf Hold gesetzt. Die Ausstellung des Zertifikates erfolgt unter Berücksichtigung des Vier-Augen-Prinzips manuell.
Authentizitätsprüfung der untergeordneten CA	Die Root CA stellt ausschliesslich Zertifikate für untergeordnete CAs aus. Die Authentizität des Zertifikatsantrags (CSR) dieser CAs wird durch [CA-ADMIN] und [IT-SEC] überprüft.

3.2.2 User CA

Notwendige Credentials	User Account im AD oder bestehendes gültiges Zertifikat.
Authentizitätsprüfung der Credentials	– Die User-CA kennt ausschliesslich ein Self-Enrollment sowie ein Auto-Enrollment für [USER], die bereits im städtischen AD integriert sind. – Die OIZ ist zuständig für die Struktur des AD. Sie eröffnet, mutiert und löscht OUs. – Die Dienstabteilungen sind verantwortlich für die Vollständigkeit und Korrektheit ihrer eigenen Userdaten (User, E-Mail-Adressen, andere Attribute). Da eben diese Informationen für die Zertifikate verwendet werden, liegt die Verantwortung für die Attribute bei der D/DA.
Enrollment	– Grundsätzlich Self-Enrollment. – Auto-Enrollment bei der ersten User Anmeldung (falls in Zertifikatsvorlage definiert)
Authentizitätsprüfung der Person	Die Person wird bei Eintritt in die D/DA durch das zuständige HR bzw. den Linienvorgesetzten identifiziert.

3.2.3 Machine CA

Notwendige Credentials	User oder Computer Account im AD, über welchen ein Zertifikat beantragt wird. Der Computer Account muss Mitglied in der Domäne und der entsprechenden AD-Gruppe sein.
Authentizitätsprüfung der Credentials	– Bei Enrollment durch [USER]: Username/Passwort. – Die Dienstabteilungen sind verantwortlich für die Vollständigkeit und Korrektheit ihrer eigenen Userdaten (User, E-Mail-Adressen, andere Attribute). Da eben diese Informationen für die Zertifikate verwendet werden, liegt die Verantwortung für die Attribute bei der D/DA. – Bei maschinellem Enrollment: Vorweisen eines gültigen Zertifikates.
Enrollment	Self-Enrollment (über offizielle Website, MMC oder SCEP).

Authentizitätsprüfung der Person	– Bei Enrollment durch [USER]: Die Person wird bei Eintritt in die D/DA durch das HR bzw. den Linienvorgesetzten identifiziert. – Bei maschinellem Enrollment: nicht anwendbar.

3.3 Anträge für Zertifikatserneuerung

3.3.1 Root CA

Notwendige Credentials	Anwesenheit von [CA-ADMIN] und [IT-SEC].
Authentizitätsprüfung der Credentials	Vier-Augen-Prinzip auf Basis Split Passwort
Enrollment	Das Enrollment erfolgt manuell durch den [CA-ADMIN] an der Konsole. Der Antrag wird von der CA auf Hold gesetzt. Die Ausstellung des Zertifikates erfolgt manuell unter Berücksichtigung des Vier-Augen-Prinzips
Authentizitätsprüfung der untergeordneten CA	Die Authentizität des Zertifikatsantrags (CSR) dieser CA wird durch [CA-ADMIN] und [IT-SEC] überprüft.

3.3.2 User CA

Notwendige Credentials	User Account im AD und bestehendes gültiges Zertifikat.
Enrollment	– Verschlüsselungs-Zertifikate: Self-Enrollment mittels Auto-Enrollment, MMC oder Website – Signatur-Zertifikate: Self-Enrollment mittels Auto-Enrollment, MMC oder Website

3.3.3 Machine CA

Notwendige Credentials	User Account im AD und bestehendes gültiges Zertifikat.
Enrollment	– Self-Enrollment via MMC als [USER] (lokaler Admin) – Auto-Enrollment im Computer-Account Kontext – Bei Web-Enrollment (z.B. SSL) Prozess analog Erstausstellung

3.4 Anträge für Zertifikatsrevokation

3.4.1 Root CA

Notwendige Credentials	Verifikation Antrag/Antragsteller Anwesenheit von [IT-SEC] und [CA-ADMIN].
Authentizitätsprüfung der Credentials	Vier-Augen-Prinzip auf Basis Split-Passwort.
Revokation	Revokation unter Berücksichtigung des Vier-Augen-Prinzips mit Hilfe der beiden Split Keys.

3.4.2 User CA

Authentizitätsprüfung der Person (inkl. Ablauf)	– [USER] kontaktiert [SERVICEDESK] im Falle von Key-Verlust (inkl. Key-Beschädigung) – SERVICEDESK] erstellt einen Incident z.H. [CA-ADMIN] – [CA-ADMIN] revoziert Zertifikat nach Rücksprache mit [USER] und erfolgreicher Identifizierung
Das Ticket muss folgende Informationen beinhalten	– Benutzername – Zeit des Anrufs – Erreichbarkeit via E-Mail/Telefon – Angaben über Zertifikat, das gesperrt werden muss – Grund der Sperrung, z.B. Key Kompromittierung (Verlust des Schlüssels), Auflösung des Arbeitsverhältnis – Das Ticket wird [CA-ADMIN] zugewiesen.

3.4.3 Machine CA

Authentizitätsprüfung der Person (inkl. Ablauf)	– Bei Diebstahl/Verlust eines Clients: [USER] kontaktiert [SERVICEDESK] im Falle eines Schlüsselverlusts – Bei Kompromittierung eines Serverzertifikats: [ADMIN] kontaktiert den [SERVICEDESK] – [SERVICEDESK] erstellt einen Incident z.H. [CA-ADMIN] – [CA-ADMIN] revoziert Zertifikat nach Rücksprache mit [USER] oder [ADMIN]
Das Ticket muss folgende Informationen beinhalten	– Benutzername – Zeit des Anrufs – Erreichbarkeit via E-Mail/Telefon – Bezeichnung des betroffenen Geräts – Angaben über Zertifikat, das gesperrt werden muss – Grund der Sperrung: Diebstahl, etc.

3.5 Anträge für Key Recovery

3.5.1 Root CA

Nicht anwendbar. Die Root CA macht kein Key Backup.

3.5.2 User CA

Notwendige Credentials	User Account im AD, bereits ausgestellte Verschlüsselungszertifikate
Authentizitätsprüfung der Credentials	Implizit durch AD
Authentizitätsprüfung der Person (inkl. Ablauf)	– [USER] kontaktiert [SERVICEDESK] im Falle eines Key-Verlusts inkl. Key-Beschädigung – [SERVICEDESK] macht Incident mit Angaben über betroffenes Verschlüsselungszertifikat (Serienummer) – [CA-ADMIN] exportiert den betroffenen – mit Key Recovery Agent verschlüsselten – Schlüssel aus der Datenbank (Key Recovery 1. Teil) – [IT-SEC] entschlüsselt den verschlüsselten Schlüssel (mit Key Recovery Agent Client und zugehörigem Passwort), stellt ihn als passwortgeschützte PKCS#12-Datei dem [USER] zu und löscht die Datei anschliessend (Key Recovery 2. Teil) – [IT-SEC] stellt [SERVICEDESK] das Passwort für den Key Import bei [USER] zu – [SERVICEDESK] kontaktiert [USER], um den wiederhergestellten Schlüssel im Postfach von [USER] mit Hilfe des Passworts zu entschlüsseln und ins Profil zu importieren; [USER] kann alle Aktionen mit verfolgen.

3.5.3 Machine CA

Die Machine CA macht kein Key Backup. Jedoch können Zertifikate, die per Web-Enrollment ausgestellt wurden, ab PFX-Datei im Zertifikatarchiv wiederhergestellt werden. Archivierte PFX-Dateien werden nur der ursprünglichen antragstellenden Person oder deren Nachfolge zugestellt.

4 Betriebsanforderungen

4.1 Zertifikatsantrag

4.1.1 Root CA

Wer kann einen Zertifikatsantrag einreichen?	Anträge für eine Zertifikatsignierung von Issuing CAs dürfen ausschliesslich durch [IT-SEC] und [CA-ADMIN] im Team (Vier-Augen-Prinzip) erstellt werden.
Enrollment Prozess und Verantwortungen	Ablauf Enrollment (der gesamte Ablauf wird mittels Screendumps dokumentiert): – Untergeordnete CA: Der Zertifikatsantrag wird auf der untergeordneten CA erstellt. – Root CA: Einloggen durch [CA-ADMIN] auf der Root CA. – Root CA: [CA-ADMIN] und [IT-SEC] reichen den Antrag mittels mmc ein und erzeugen das Zertifikat. – Untergeordnete CA: Import des Zertifikates. – Speichern des Zertifikates der Schlüssel als PKCS#12 File auf 2 CDs (Sicherstellung/ Verschlüsselung mit Split Passwort). Es werden neue Passwörter definiert. – Sicherstellung jeweils einer CD in den beiden Safes von [CA-ADMIN] und [IT-SEC].

4.1.2 User CA

Wer kann einen Zertifikatsantrag einreichen?	Alle [USER] mit einem AD Account dürfen Anträge stellen.
Enrollment Prozess und Verantwortungen	– Anträge erfolgen über Self-Enrollment oder Auto-Enrollment. – CA-Service überprüft, ob der Antrag alle notwendigen Informationen für die entsprechende Zertifikatsvorlage enthält und ob der Antragssteller Mitglied in der für den Zertifikatsbezug berechtigten AD-Gruppe ist. – Schlägt eine Überprüfung fehl, wird der Antrag abgelehnt und in der CA-Datenbank archiviert.

4.1.3 Machine CA

Wer kann einen Zertifikatsantrag einreichen?	Anträge dürfen durch – [CA-ADMIN] aufgrund eines vorliegenden AD Accounts – [USER] und Computer mit einem AD-Account gestellt werden.
Enrollment Prozess und Verantwortungen	– Anträge erfolgen über die PKI-Website, Self-Enrollment oder Auto-Enrollment. – CA-Service überprüft, ob der Antrag alle notwendigen Informationen für die entsprechende Zertifikatsvorlage enthält und ob der Antragssteller Mitglied in der für den Zertifikatsbezug berechtigten AD-Gruppe ist. – Schlägt eine Überprüfung fehl, wird der Antrag abgelehnt und in der CA-Datenbank archiviert.

4.2 Bearbeitung des Zertifikatsantrags

4.2.1 Root CA

Zertifikate für Issuing CAs werden signiert, sofern die notwendigen Rechtsgrundlagen existieren (z.B. STRB). Ansonsten bestehen keine speziellen Einschränkungen.

4.2.2 User CA

Es werden nur Zertifikate von städtischen Benutzern (E-Mail-Adressen städtischer Domänen) signiert. Ansonsten bestehen keine speziellen Einschränkungen

4.2.3 Machine CA

Es werden nur Zertifikate von städtischen Domänen signiert. Ansonsten bestehen keine speziellen Einschränkungen.

4.3 Zertifikatsausstellung

4.3.1 Root CA

CA Aktivitäten bei Zertifikatsausstellung	Alle Aktionen werden mittels Screendumps dokumentiert.
Benachrichtigung des Antragsstellers über die Zertifikatsausstellung	Der Antragsteller wird nach Zertifikatsausstellung benachrichtigt

4.3.2 User CA

CA Aktivitäten bei Zertifikatsausstellung	Die Ausstellung erfolgt automatisch. Einträge finden sich im Eventlog.
Benachrichtigung des Antragsstellers über die Zertifikatsausstellung	Es erfolgt keine Notifikation.

4.3.3 Machine CA

CA Aktivitäten bei Zertifikatsausstellung	Die Ausstellung erfolgt automatisch. Einträge finden sich im Eventlog.
Benachrichtigung des Antragsstellers über die Zertifikatsausstellung	Antragsteller werden über das Change Management Tool informiert, sofern die Zertifikatsausstellung manuell durch den [CA-ADMIN] erfolgt ist.

4.4 Annahme von Zertifikaten

4.4.1 Root CA

Als Annahme des Zertifikats geltende Handlungen	Das Zertifikat wird implizit durch den Import des Zertifikats durch den [CA-ADMIN] akzeptiert.
Publikation des Zertifikats durch die CA	Die Zertifikate werden durch den [CA-ADMIN] manuell im AD und auf der Website publiziert.
Benachrichtigung anderer Stellen über Zertifikatsausstellung	Betroffene Stellen werden informiert.

4.4.2 User CA

Als Annahme des Zertifikats geltende Handlungen	Das Zertifikat wird implizit durch Download akzeptiert.
Publikation des Zertifikats durch die CA	Die Zertifikate werden bei ausgewiesenem Bedarf im AD und auf der Website publiziert.
Benachrichtigung anderer Stellen über Zertifikatsausstellung	Es erfolgt eine E-Mail Notifikation.

4.4.3 Machine CA

Als Annahme des Zertifikats geltende Handlungen	Das Zertifikat wird implizit durch Download akzeptiert.
Publikation des Zertifikats durch die CA	Die Zertifikate werden bei ausgewiesenem Bedarf im AD und auf der Website publiziert.
Benachrichtigung anderer Stellen über Zertifikatsausstellung	Es erfolgt eine E-Mail Notifikation.

4.5 Nutzung von Schlüsselpaaren und Zertifikaten

4.5.1 Root CA

Nutzung von Private Key und Zertifikaten durch Zertifikatsinhaber	Die Zertifikate dürfen ausschliesslich für den deklarierten Zweck – das Signieren von Zertifikaten untergeordneter CAs und von CRLs – verwendet werden.
Nutzung von Public Key und Zertifikaten durch Zertifikatsprüfer	Der Umgang mit Zertifikat und Public Key soll sorgsam sein. Dies beinhaltet – Überprüfen der CRL – Prüfen der Gültigkeit des Zertifikates vor dem Einsatz – Prüfen der Gültigkeit des Public Keys anhand des Hash-Werts im Zertifikat

4.5.2 User CA

Nutzung von Private Key und Zertifikaten durch Zertifikatsinhaber	Die Benutzerzertifikate dürfen ausschliesslich durch die jeweiligen [USER] für den deklarierten Zweck verwendet werden. Konkret bedeutet dies: – S/MIME Signaturzertifikate für Signatur (E-Mails, Dokumente) – S/MIME Verschlüsselungszertifikate für Verschlüsselung (E-Mails, Dokumente). – User Authentisierungszertifikate für Authentisierung von Benutzern an Anwendungen (nicht Anmeldung an der Domäne). – Code Signing Zertifikate für das Signieren von Software (Zugriff beschränkt auf kleine [USER]-Gruppe).
Nutzung von Public Key und Zertifikaten durch Zertifikatsprüfer	Der Umgang mit Zertifikat und Public Key soll sorgsam sein. Dies beinhaltet – Überprüfen der CRL. – Prüfen der Gültigkeit des Zertifikates vor dem Einsatz – Prüfen der Gültigkeit des Public Keys anhand des Hash-Werts im Zertifikat

4.5.3 Machine CA

Nutzung von Private Key und Zertifikaten durch Zertifikatsinhaber	Die Maschinenzertifikate dürfen ausschliesslich für den deklarierten Zweck verwendet werden. Konkret bedeutet dies: – Authentisierung von Clients und Servern – Verschlüsselung der Kommunikation zwischen zwei Maschinen (Client/Server resp. Server/Server)
Nutzung von Public Key und Zertifikaten durch Zertifikatsprüfer	Der Umgang mit Zertifikat und Public Key soll sorgsam sein. Dies beinhaltet – Überprüfen der CRL. – Prüfen der Gültigkeit des Zertifikates vor dem Einsatz – Prüfen der Gültigkeit des Public Keys anhand des Hash-Werts im Zertifikat.

4.6 Zertifikatsverlängerung (Renewal)

Zertifikatsverlängerung bedeutet, dass die Gültigkeit des Zertifikates verlängert wird. Alle Angaben im Zertifikat, insbesondere die Keys, werden beibehalten.

Eine Zertifikatsverlängerung ist für die städtischen Klasse C Zertifikate grundsätzlich zulässig.

4.6.1 Root CA

Bedingung für Zertifikatsverlängerung	Die Zertifikate der «Stadt Zuerich CA – Class C – Root 1» werden nach 10 Jahren (=Renewal Time) erneuert. Die Zertifikate von untergeordneten CAs werden nicht gleichzeitig erneuert, ausser bei ausgewiesenem Bedarf. Eine Zertifikatsverlängerung ist unter folgenden Bedingungen zulässig: – Die Renewal Time ist abgelaufen – Die Schlüssellänge gilt für eine weitere Renewal Time als sicher
Wer kann ein Renewal beantragen	Das Zertifikats-Renewal wird durch den [CA-ADMIN] manuell beantragt.
Verfahren für Renewal Anträge	Das Renewal erfolgt analog dem Enrollment in Kapitel 4.1
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung des Renewal erfolgt analog dem Enrollment in Kapitel 4.3
Annahme eines Renewal Zertifikats	Die Annahme des Renewal erfolgt analog dem Vorgehen in Kapitel 4.4
Publikation des Renewal Zertifikats durch CA	Die Publikation des Renewal erfolgt analog dem Enrollment in Kapitel 4.3
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung des Renewal erfolgt analog dem Enrollment in Kapitel 4.3

4.6.2 User CA

Bedingung für Zertifikatsverlängerung	Die von der «Stadt Zuerich CA – Class C – User 1» ausgestellten Zertifikate können jederzeit verlängert werden, solange die Gültigkeitsdauer des User-CA-Zertifikats nicht überschritten wird. Eine Zertifikatsverlängerung ist unter folgenden Bedingungen zulässig: – Die Renewal Time ist abgelaufen – Die Schlüssellänge gilt für eine weitere Renewal Time als sicher
Wer kann ein Renewal beantragen	– Berechtigte [USER] per Auto-Enrollment, Self-Enrollment oder Web-Enrollment. – Zentral bereitgestellte Zertifikate: Enrollment durch [CA-Admin] und Bereitstellung auf zentralem Server.

Verfahren für Renewal Anträge	Das Renewal erfolgt analog dem Enrollment in Kapitel 4.1
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung eines Renewal erfolgt analog dem Enrollment in Kapitel 4.3
Annahme eines Renewal Zertifikats	Die Annahme eines Renewal erfolgt analog dem Vorgehen in Kapitel 4.4
Publikation des Renewal Zertifikats durch CA	Die Publikation eines Renewal erfolgt analog dem Enrollment in Kapitel 4.3
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung eines Renewal erfolgt analog dem Enrollment in Kapitel 4.3

4.6.3 Machine CA

Bedingung für Zertifikatsverlängerung	Die von der «Stadt Zuerich CA – Class C – Machine 1» ausgestellten Zertifikate können jederzeit verlängert werden, solange die Gültigkeitsdauer des Machine-CA-Zertifikats nicht überschritten wird. Eine Zertifikatsverlängerung ist unter folgenden Bedingungen zulässig: – Die Renewal Time ist abgelaufen – Die Schlüssellänge gilt für eine weitere Renewal Time als sicher
Wer kann ein Renewal beantragen	Berechtigte Clients und [USER] per Auto-Enrollment, SCEP, oder Self-Enrollment.
Verfahren für Renewal Anträge	Das Renewal erfolgt analog dem Enrollment in Kapitel 4.1
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung eines Renewal erfolgt analog dem Enrollment in Kapitel 4.3
Annahme eines Renewal Zertifikats	Die Annahme eines Renewal erfolgt analog dem Vorgehen in Kapitel 4.4
Publikation des Renewal Zertifikats durch CA	Die Publikation eines Renewal erfolgt analog dem Enrollment in Kapitel 4.3
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung eines Renewal erfolgt analog dem Enrollment in Kapitel 4.3

4.7 Zertifikatserneuerung (Re-Key)

Zertifikatserneuerung bedeutet, dass alle Angaben im Zertifikat beibehalten werden, ausser den Keys. Die Keys werden gewechselt.

Eine Zertifikatserneuerung ist für die städtischen Klasse C Zertifikate grundsätzlich zulässig.

4.7.1 Root CA

Bedingung für Zertifikatserneuerung	Die Zertifikate der «Stadt Zuerich CA – Class C – Root 1» werden nach 20 Jahren (=Re-Key Time, Lifetime) erneuert. Die Zertifikate von untergeordneten CAs werden nicht gleichzeitig erneuert, ausser bei ausgewiesenem Bedarf. Eine Zertifikatserneuerung ist in folgenden Fällen notwendig: – Die Lifetime ist abgelaufen – Das Zertifikat wurde revoziert (Key Compromise) – Die Schlüssellänge gilt als nicht mehr sicher
Wer kann ein Re-Key beantragen	Das Re-Key wird durch den [CA-ADMIN] manuell beantragt.
Verfahren für Re-Key Anträge	Das Re-Key erfolgt analog dem Enrollment in Kapitel 4.1
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.3
Annahme eines Re-Key Zertifikats	Die Annahme des Re-Key erfolgt analog dem Vorgehen in Kapitel 4.4
Publikation des Re-Key Zertifikats durch CA	Die Publikation des Re-Key erfolgt analog dem Enrollment in Kapitel 4.3
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung eines Re-Key erfolgt analog dem Enrollment in Kapitel 4.3

4.7.2 User CA

Bedingung für Zertifikatserneuerung	Die von der «Stadt Zuerich CA – Class C – User 1» ausgestellten Zertifikate können jederzeit erneuert werden, solange die Gültigkeitsdauer des User-CA-Zertifikats nicht überschritten wird. Eine Zertifikatserneuerung ist in folgenden Fällen notwendig: – Die Lifetime ist abgelaufen – Das Zertifikat wurde revoziert (Key Compromise) – Die Schlüssellänge gilt als nicht mehr sicher
Wer kann ein Re-Key beantragen	– Berechtigte [USER] per Auto-Enrollment, Self-Enrollment oder Web-Enrollment. – Zentral bereitgestellte Zertifikate: Enrollment durch [CA-Admin] und Bereitstellung auf zentralem Server.
Verfahren für Re-Key Anträge	Das Re-Key erfolgt analog dem Enrollment in Kapitel 4.1

Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.3
Annahme eines Re-Key Zertifikats	Die Annahme des Re-Key erfolgt analog dem Vorgehen in Kapitel 4.4
Publikation des Re-Key Zertifikats durch CA	Die Publikation des Re-Key erfolgt analog dem Enrollment in Kapitel 4.4
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.4

4.7.3 Machine CA

Bedingung für Zertifikatserneuerung	Die von der «Stadt Zuerich CA – Class C – Machine 1» ausgestellten Zertifikate können jederzeit erneuert werden, solange die Gültigkeitsdauer des Machine-CA-Zertifikats nicht überschritten wird. Eine Zertifikatserneuerung ist in folgenden Fällen notwendig: – Die Lifetime ist abgelaufen – Das Zertifikat wurde revoziert (Key Compromise) – Die Schlüssellänge gilt als nicht mehr sicher
Wer kann ein Re-Key beantragen	Berechtigte Clients und [USER] per Auto-Enrollment, SCEP, oder Self-Enrollment.
Verfahren für Re-Key Anträge	Das Re-Key erfolgt analog dem Enrollment in Kapitel 4.1
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.3
Annahme eines Re-Key Zertifikats	Die Annahme des Re-Key erfolgt analog dem Vorgehen in Kapitel 4.4
Publikation des Re-Key Zertifikats durch CA	Die Publikation des Re-Key erfolgt analog dem Enrollment in Kapitel 4.4
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.3

4.8 Zertifikatsänderung

Zertifikatsänderung bedeutet, dass einige Angaben im Zertifikat sowie die Keys geändert werden. Dies entspricht in seiner Art einer Neuausstellung.

Eine Zertifikatsänderung ist im Rahmen einer Zertifikatserneuerung möglich.

4.9 Zertifikatssperrung

Zertifikatssperrung (Revokation) bedeutet, dass das Zertifikat ungültig ist und definitiv zurückgezogen wird. Revokation kommt im ordentlichen Betrieb vor.

4.9.1 Root CA

Bedingungen für Revokation	Verschiedene Ursachen können zu einer Revokation führen. CA Signatur Zertifikate: – Key Compromise der Root CA oder einer Issuing CA: Bei erhärtetem Verdacht oder falls bestätigt – Key Lost: Eine der CDs mit den Keys geht verloren – Auflösung der CA aufgrund eines STRB – Modifikationsanforderung: Ein oder mehrere Felder des Zertifikates müssen angepasst werden.
Wer kann eine Revokation beantragen	Die Zertifikatssperrung wird durch den [CA-ADMIN] manuell beantragt.
Verfahren für Revokation	– Root CA: Erreichbarkeit herstellen ([CA-ADMIN] und [IT-SEC] – Untergeordnete CAs: Der Setup-Prozess der untergeordneten CA erstellt eine Anfrage oder der [CA-ADMIN] stellt Request manuell – Root CA: Einloggen mit Hilfe der Split Keys. Der gesamte Ablauf wird mittels Screendumps dokumentiert – Root CA: revoziert das Zertifikat mittels mmc der CA – Root CA: Publikation der CRL
Frist für Ausstellung von Anträgen	Die Certificate Revocation soll umgehend erfolgen.
Frist für Bearbeitung von Anträgen	Die Certificate Revocation soll umgehend erfolgen.
Prüfpflichten	Die Revokation wird in der CRL visuell geprüft.
Häufigkeit der CRL-Ausstellung	– Ausstellung alle 5 Monate – Overlapping 1 Monat – Keine Delta CRL.
Maximale Verzögerung für CRLs	Die CRLs werden innerhalb eine Tages auf der Website publiziert.
Option zur Online-Überprüfung	Die CRLs sind online im AD und auf der Website publiziert.
Anforderungen für die Online-Überprüfung	Die CRLs sind online im AD und auf der Website publiziert und können nach Namen, Typ und Hash durchsucht werden.

Weitere Optionen zur Bekanntgabe von Revokationen	Weitere Zugriffsmöglichkeiten sind vorerst nicht vorgesehen (z.B. SCEP)
Besondere Anforderungen bei kompromittierten Schlüsseln	Erweiterte Anforderungen bestehen nicht.

4.9.2 User CA

Bedingungen für Revokation	Verschiedene Ursachen können zu einer Revokation führen. Allgemeine Bedingungen: – Key Compromise der übergeordneten CA – erhärteter Verdacht oder bestätigt. – Key Lost: Eine der CDs mit den CA Keys geht verloren – Auflösung der CA: aufgrund eines STRB – Modifikationsanforderung: Ein oder mehrere Felder des Zertifikates müssen angepasst werden. – Re-Key des CA Zertifikats – Austritt des Mitarbeitenden
Wer kann eine Revokation beantragen	– Persönliche Zertifikate: [USER], Personalabteilung – Applikations-Zertifikate: [CA-ADMIN], [USER]
Verfahren für Revokation	– [CA-ADMIN] revoziert das Zertifikat mittels mmc der CA. – Dokumentation erfolgt in Form von Einträgen im Eventlog. – Publikation der CRL
Frist für Ausstellung von Anträgen	Die Certificate Revocation soll umgehend erfolgen.
Frist für Bearbeitung von Anträgen	Die Certificate Revocation soll umgehend erfolgen.
Prüfpflichten	Die Revokation wird in der CRL visuell geprüft.
Häufigkeit der CRL-Ausstellung	– Ausstellung alle 14 Tage – Overlapping 14 Tage – Keine Delta CRL.
Maximale Verzögerung für CRLs	Die CRLs werden umgehend im AD und innerhalb von 30 Minuten auf der Website publiziert.
Option zur Online-Überprüfung	Die CRLs sind online im AD und auf der Website publiziert.
Anforderungen für die Online-Überprüfung	Die CRLs sind online im AD und auf der Website publiziert und können nach Namen, Typ und Hash durchsucht werden.
Weitere Optionen zur Bekanntgabe von Revokationen	Weitere Zugriffsmöglichkeiten sind vorerst nicht vorgesehen (z.B. SCEP)
Besondere Anforderungen bei kompromittierten Schlüsseln	Erweiterte Anforderungen bestehen nicht.

4.9.3 Machine CA

Bedingungen für Revokation	Verschiedene Ursachen können zu einer Revokation führen. Allgemeine Bedingungen: – Key Compromise der übergeordneten CA – erhärteter Verdacht oder bestätigt. – Key Lost: Eine der CDs mit den CA Keys geht verloren – Auflösung der CA: aufgrund eines STRB – Modifikationsanforderung: Ein oder mehrere Felder des Zertifikates müssen angepasst werden. – Re-Key des CA Zertifikat Zusätzliche Bedingungen: – Server Zertifikate: Ablösung des Servers – Wireless Zertifikate: Ablösung des Wireless Devices – Netzwerk Zertifikate: Ablösung des Gerätes
Wer kann eine Revokation beantragen	– Ausstellender [USER] oder [SYSTEMADMIN] der betroffenen Machine
Verfahren für Revokation	– [CA-ADMIN] revoziert das Zertifikat mittels mmc der CA. – Dokumentation erfolgt in Form von Einträgen im Eventlog. – Publikation der CRL
Frist für Ausstellung von Anträgen	Die Certificate Revocation soll umgehend erfolgen.
Frist für Bearbeitung von Anträgen	Die Certificate Revocation soll umgehend erfolgen.
Prüfpflichten	Die Revokation wird in der CRL automatisch geprüft.
Häufigkeit der CRL-Ausstellung	– Ausstellung alle 14 Tage – Overlapping 14 Tage – Keine Delta CRL.
Maximale Verzögerung für CRLs	Die CRLs werden umgehend im AD und innerhalb von 30 Minuten auf der Website publiziert.
Option zur Online-Überprüfung	Die CRLs sind online im AD und auf der Website publiziert.
Anforderungen für die Online-Überprüfung	Die CRLs sind online im AD und auf der Website publiziert und können nach Namen, Typ und Hash durchsucht werden.
Weitere Optionen zur Bekanntgabe von Revokationen	Weitere Zugriffsmöglichkeiten sind vorerst nicht vorgesehen (z.B. SCEP)
Besondere Anforderungen bei kompromittierten Schlüsseln	Erweiterte Anforderungen bestehen nicht.

4.10 Zertifikatssuspendierung

Zertifikatssuspendierung bedeutet, dass ein Zertifikat temporär ungültig ist und die Absicht besteht, es in einem späteren Zeitpunkt wieder zu aktivieren.

Auf der städtischen PKI wird keine Zertifikatssuspendierung, sondern nur Revokation betrieben.

4.11 Dienste zum Zertifikatsstatus

Die Information in Zertifikaten kann mit Hilfe des eigenen Arbeitsplatzes geprüft werden (z.B. Internet Explorer, Zertifikatsmanager certmgr.msc, mmc).

Auf allen AD-integrierten Systemen sind die städtischen CA-Zertifikate zur Verifizierung der Vertrauenskette vorinstalliert.

Die Sperrlisten (CRL) stehen auf der Webseite (siehe oben) und im AD zur Verfügung

4.12 Ende der Zertifikatsnutzung

Ein Abbau der städtischen CA muss vom Stadtrat mittels STRB bestimmt werden. Dafür notwendige Schritte:

- Information der Betroffenen
- Stoppen des Services
- Revokation des CA-Zertifikats
- Entsorgung gemäss geltenden Richtlinien (Handbuch Informationssicherheit)

4.13 Key Escrow und Key Recovery

4.13.1 Root CA

Der Private Key wird mit Split Passwort ([CA-ADMIN] und [IT-SEC]) geschützt auf CD gesichert und bei einem externen Key Escrow-Service hinterlegt.

Bei Bedarf kann der Private Key im Vier-Augen-Prinzip (durch [CA-ADMIN] und [IT-SEC]) wieder entschlüsselt werden (Key Recovery).

4.13.2 User CA

Die Wiederherstellung von Verschlüsselungsschlüsseln der Zertifikatsinhaber ist möglich. Das Key Recovery erfolgt immer im Vier-Augen-Prinzip.

4.13.3 Machine CA

Eine Schlüsselhinterlegung (Key Escrow) und Wiederherstellung (Key Recovery) nach Definition existiert für die Machine CA nicht.

5 Einrichtung, Verwaltung und Betriebskontrollen

5.1 Physische Sicherheit

Lage und Beschaffenheit der Standorte	Die Server der PKI befinden sich im OIZ RZ und werden einem hohen Schutz-Niveau angemessen geschützt.
Physischer Zugang	Der Zugang zu den Servern ist durch ein restriktives Rollenmodell auf Administratoren eingeschränkt. Die CA Keys sind passwortgeschützt und verschlüsselt in OIZ Tresore ausgelagert.
Stromversorgung und Klimatisierung	Die Stromversorgung ist mit einer unterbruchsfreien, batteriegestützten Stromversorgung ergänzt. Das RZ ist klimatisiert, um eine optimale Umgebung nach allgemein anerkannten Verfahrensweisen zu schaffen.
Wasserschaden	Es besteht kein direktes Wasserrisiko.
Brandschutz	Das RZ ist mit einem angemessenen Brandschutzsystem ausgerüstet.
Ablage von Datenträgern	Für die Auslagerung der Daten steht das zweite Rechenzentrum zur Verfügung.
Abfallentsorgung	Vertrauliche Dokumente werden geschreddert. Disks und andere Datenträger werden physisch zerstört.
Backup	Alle Daten werden gesichert (Betrieb in zwei unterschiedlichen Rechenzentren)

5.2 Verfahrenskontrollen

Vertrauenswürdige Rollen	– Der [CA-ADMIN] hat nach dem Einloggen (die volle Kontrolle über den CA-Server und dessen Applikationen. Er ist auch für die Nutzung des Private Keys im HSM berechtigt, kann damit mit Zertifikaten arbeiten (ausstellen, revozieren, etc.). Export des Private Keys ist nicht möglich. – [HSM-ADMIN]: Kann HSM-Partitionen aktivieren/deaktivieren und somit die Verwendung von Private Keys der CAs ermöglichen oder unterbinden. – [IT-SEC]: Hat als Auditorin Zugriff zu Logfiles der PKI mit dem Ziel zu verifizieren, dass die vorliegende CP/CPS eingehalten wird. Sie kann beim [CA-ADMIN] Einsicht auf die CA-Infrastruktur verlangen. [IT-SEC] darf nicht gleichzeitig [CA-ADMIN] sein. – Der Registration Authority Operator [RA-OP] kann Zertifikatsanträge stellen. Der [RA-OP] kann von [CA-ADMIN] getrennt sein, muss aber nicht.
Anzahl erforderlicher Personen pro Task	Durch den Einsatz von Split-Keys oder mehreren Tokens sind für kritische Prozesse (gemäss Beschreibung in den jeweiligen Kapiteln) zwei Mitarbeitende erforderlich.
Identifikation und Authentisierung	Die Mitarbeitenden müssen einander persönlich bekannt sein. Es erfolgt eine Face-to-Face Identifikation.
Rollen mit getrennten Pflichten (Separation of Duties)	Um eine strikte Trennung der Pflichten zu gewährleisten, sind die oben aufgeführten vertrauenswürdigen Rollen wie dokumentiert zu vergeben.

5.3 Personelle Sicherheit

Qualifikation, Erfahrung und Sicherheitsprüfung	Die Mitarbeitenden im Umfeld der PKI müssen über angemessene Erfahrung und Qualifikation verfügen. Neben den ordentlichen Prüfungen des OIZ Anstellungsprozesses sind keine weiteren Abklärungen notwendig.
Schulung und Weiterbildung	Die Mitarbeitenden müssen für den Betrieb einer PKI ausgebildet sein. Fehlt die Ausbildung, ist sie nachzuholen. Nachschulungen und Weiterbildung werden bedarfsbezogen durchgeführt. Die OIZ klärt den Bedarf ab. Job Rotation ist für die Aufgaben im PKI Umfeld nicht vorgesehen.
Strafen für nicht autorisiertes Vorgehen	Unerlaubte Aktionen im PKI Bereich werden im Rahmen des Personalrechts verfolgt.
Anforderungen für Vertragspartner	Es sind keine Vertragspartner vorgesehen.
Dokumentation für Personal	Keine spezifischen Anforderungen.

5.4 Audit

Aktionen werden soweit möglich geloggt.

Folgende Events werden aufgezeichnet	– Neue Certificate Requests – Abgewiesene Certificate Requests – Misslungene Anmeldeversuche – Erfolgreiche Anmeldungen – Zertifikat Signatur – Zertifikatsrevokation – CRL Signatur – Zertifikats Ablauf (Diese Aufzählung ist nicht abschliessend)
Häufigkeit der Log-Verarbeitung	Logs müssen einmal monatlich durch [CA-ADMIN] ausgewertet werden.
Archivierungsdauer von Logs	Die Logdateien werden mindestens 6 Monate aufbewahrt.
Schutz der Logs	Die Logs sind nur [CA-ADMIN] und [IT-SEC] lesend zugänglich.
Backup von Logs	Die Logs werden mit dem täglichen Backup ausgelagert.
Log-Erfassung	Die CAs und HSMs loggen auf den zentralen Loghost.
Benachrichtigung von Log-Verursachern	Der Auslöser eines Log-Eintrags wird nicht benachrichtigt.
Bewertung von Sicherheitslücken	Die Umgebung wird regelmässigen Audits unterzogen. Die Auditdaten werden bei [IT-SEC] gehalten.

5.5 Archivierung

Es gibt keine explizite Archivierung. Zertifikate werden nicht gelöscht und werden gebackupt.

5.6 Auswechseln von Schlüsseln

Die Parameter sind im Kapitel 6.4 „Nutzungsdauer von Zertifikaten und Schlüsselpaaren“ festgelegt.

5.7 Schlüsselkompromittierung

5.7.1 Root CA

Im Falle einer Kompromittierung der Root CA Schlüssel wird die PKI neu aufgebaut.

5.7.2 User CA

Falls ein einzelner durch die User CA ausgestellter Schlüssel eines Teilnehmers kompromittiert wird, wird das entsprechende Zertifikat revoziert. Bei Encryption Keys ist dafür zu sorgen (entschlüsseln, zwischenspeichern), dass die Daten gelesen werden können.

Im Falle einer Kompromittierung der User CA Schlüssel wird die User CA neu aufgebaut, die Benutzer erhalten neue Zertifikate und anschliessend werden alle alten Teilnehmerzertifikate revoziert.

5.7.3 Machine CA

Falls ein einzelner durch die Machine CA ausgestellter Subscriber-Key kompromittiert wird, wird das entsprechende Zertifikat revoziert.

Im Falle einer Kompromittierung der Machine CA Schlüssel wird die Machine CA neu aufgebaut, die Systeme erhalten neue Zertifikate und anschliessend werden alle alten Subscriber-Zertifikate revoziert.

5.8 Disaster Recovery

Bei einem Disaster Recovery wird die betroffene CA neu installiert und anhand des Backups aufgebaut.

5.9 Ausserbetriebnahme der CA

Die CAs der städtischen PKI können nur per STRB aufgehoben werden.

6 Technische Sicherheit

6.1 Schlüsselerzeugung

6.1.1 Root CA

Erzeugung von Schlüsselpaaren	Die Keys werden auf der CA erstellt, ins HSM und auf CD (Split Passwort) exportiert und danach auf der CA gelöscht. Zusätzlich werden sie verschlüsselt Off-Site hinterlegt (siehe oben).
Bereitstellung des Private Key an Zertifikatsinhaber	Dieser Fall kommt nicht vor: Keys werden immer durch untergeordnete CA erzeugt.
Bereitstellung des Public Key an CA	Der CSR wird dem [CA-ADMIN] persönlich durch den [RA-ADMIN] übergeben.
Bereitstellung des Public Key an Zertifikatsprüfer	Kann über den städtischen Webserver heruntergeladen werden.
Schlüssellängen	Länge der RSA Schlüssel für alle CAs: 4096 Bits
Qualitätsprüfung von Public-Key Parametern	Die Schlüssel werden mit dem Microsoft Standard Security Provider erstellt. Aussagen zur Qualität können hier keine gemacht werden.
Verwendungszweck der Schlüssel (gemäss X.509 v3 Key Usage Field)	Digitale Signatur, Zertifikatsignatur, Offline Signieren der Zertifikatsperrliste, Signieren der Zertifikatsperrliste (86)

Zertifikatsparameter für Issuing CAs:

Name	«Stadt Zuerich - CA – Class C – XXX»
Lebensdauer	10 Jahre
Renewal Period	5 Jahre
CRL Veröffentlichungspunkte	http://pki.stzh.ch/pki/crl
Zertifikat im AD speichern	Ja (sofern stadtweit verwendet)
Key Archivierung	Ja
Symmetrische Algorithmen im Zertifikat	Nein
Minimale Schlüssellänge	4096 Bits
Privater Schlüssel exportierbar	Ja
Auto-Enrollment	Nein
Speicherort des privaten Schlüssels	Im HSM und PKCS#12 File auf CD
Subject Name	Common Name, E-Mail-Name
Issuance Requirements	Keine

Application Policy	http://pki.stzh.ch/pki (OID 1.3.6.1.5.5.7.3.4)
Issuance Policy	http://pki.stzh.ch/pki (OID 1.3.6.1.5.5.7.3.4)
Key Usage	Digitale Signatur, Zertifikatsignatur, Offline Signieren der Zertifikatsperrliste, Signieren der Zertifikatsperrliste (86)
Critical Attributes	Nur Basic Constraints
Issuer Statement	«Stadt Zuerich CA – Class C – Root 1»

6.1.2 User CA

Erzeugung von Schlüsselpaaren	Die Keys werden auf der CA erstellt, ins HSM und auf CD (Split Passwort) exportiert und danach auf der CA gelöscht. Zusätzlich werden sie verschlüsselt Off-Site hinterlegt (siehe oben).
Bereitstellung des Private Key an Zertifikatsinhaber	Dieser Fall kommt nicht vor.
Bereitstellung des Public Key an CA	Der Public Key wird als Bestandteil des CSR an die übertragen.
Bereitstellung des Public Key an Zertifikatsprüfer	Dieser Fall kommt nicht vor.
Schlüssellängen	4096 Bits
Qualitätsprüfung von Public-Key Parametern	Die Schlüssel werden mit dem Microsoft Standard Security Provider erstellt. Aussagen zur Qualität können hier keine gemacht werden.
Verwendungszweck der Schlüssel (gemäss X.509 v3 Key Usage Field)	Digitale Signatur, Zertifikatsignatur, Offline Signieren der Zertifikatsperrliste, Signieren der Zertifikatsperrliste (86)
Issuer Statement	«Stadt Zuerich CA – Class C – User 1» – Klasse C Zertifikate – Nur für stadtinterne Verwendung

Parameter für mit User CA verwendete Zertifikatsvorlagen:

Name	Stadt Zuerich [Name]
Lebensdauer	1, 2 oder 4 Jahre
Renewal Period	8 Wochen
CRL Veröffentlichungspunkte	http://pki.stzh.ch/pki/crl LDAP:/// (Standard LDAP Pfad)
Zertifikat im AD speichern	Ja
Key Archivierung	Nur Verschlüsselungsschlüssel
Symmetrische Algorithmen im Zertifikat	Nein
Minimale Schlüssellänge	2048 Bits

Privater Schlüssel exportierbar	Nein (nur im Ausnahmefall erlaubt für zentrale Services)
Auto-Enrollment	Ja
Speicherort des privaten Schlüssels	Normalerweise im Key Store des Benutzerprofils (Ausnahmefall: Zentrale Services)
Subject Name	Common Name, E-Mail-Name, UPN (Daten stammen bei Auto- und Self-Enrollment aus dem Active Directory)
Issuance Requirements	keine
Application Policy	Je nach Vorlage/Verwendungszweck: – Sichere E-Mail – Codesignatur – Clientauthentifizierung
Issuance Policy	Stadt Zuerich - Class C
Key Usage	Je nach Vorlage/Verwendungszweck: – Digital Signature – Encryption – Code Signing
Critical Attributes	Nur Basic Constraints

6.1.3 Machine CA

Erzeugung von Schlüsselpaaren	Die Keys werden auf der CA erstellt, ins HSM und auf CD (Split Passwort) exportiert und danach auf der CA gelöscht. Zusätzlich werden sie verschlüsselt Off-Site hinterlegt (siehe oben).
Bereitstellung des Private Key an Zertifikatsinhaber	Dieser Fall kommt nicht vor.
Bereitstellung des Public Key an CA	Der Public Key wird als Bestandteil des CSR an die CA übertragen.
Bereitstellung des Public Key an Zertifikatsprüfer	Dieser Fall kommt nicht vor.
Schlüssellängen	4096 Bits
Qualitätsprüfung von Public-Key Parametern	Die Schlüssel werden mit dem Microsoft Standard Security Provider erstellt. Aussagen zur Qualität können hier keine gemacht werden.
Verwendungszweck der Schlüssel (gemäss X.509 v3 Key Usage Field)	Digitale Signatur, Zertifikatsignatur, Offline Signieren der Zertifikatsperrliste, Signieren der Zertifikatsperrliste (86)
Issuer Statement	«Stadt Zuerich CA – Class C – Machine 1» – Klasse C Zertifikate – Nur für stadtinterne Verwendung

Parameter für mit Machine CA verwendete Zertifikatsvorlagen:

Name	Stadt Zuerich [Name]
Lebensdauer	1, 2, 4 oder 5 Jahre (je nach Verwendungszweck)
Renewal Period	8 Wochen
CRL Veröffentlichungs-punkte	http://pki.stzh.ch/pki/crl LDAP:/// (Standard LDAP Pfad)
Zertifikat im AD speichern	Nein
Key Archivierung	Nein
Symmetrische Algorithmen im Zertifikat	Nein
Minimale Schlüssellänge	2048 Bits
Privater Schlüssel expor-tierbar	Nein (nur im Ausnahmefall für zentrale Services denkbar, Be-willigung durch [IT-SEC] erforderlich)
Auto-Enrollment	Nein (im Ausnahmefall Ja)
Speicherort des privaten Schlüssels	Keystore abhängig vom Client, Server, sonstigen Device
Subject Name	Common Name, E-Mail-Name, UPN (Daten stammen bei Au-to- und Self-Enrollment aus dem Active Directory)
Issuance Requirements	keine
Application Policy	Je nach Vorlage/Verwendungszweck: – Clientauthentifizierung – Serverauthentifizierung
Issuance Policy	Stadt Zuerich - Class C
Key Usage	Je nach Vorlage/Verwendungszweck: – Digital Signature – Encryption
Critical Attributes	Nur Basic Constraints

6.2 Schutz der Private Keys / Hardware Security Module

6.2.1 Root CA

Verschlüsselungsmodule	Es kommt ein Hardware-Verschlüsselungsmodul HSM zum Einsatz auf welchem der Private Key und das zugehörige Zertifikat gespeichert sind.
Multi-Personen Kontrolle	Multi-Personen Token werden nicht eingesetzt.
Hinterlegung des Private Key	Die Private Keys werden bei einem externen Key Escrow Unternehmen hinterlegt.
Backup des Private Key	Die Keys werden als PKCS#12 Dateien auf zwei CDs sichergestellt. Die CDs werden von [PKI-ADMIN] und [IT-SEC] verwaltet. [PKI-ADMIN] und [IT-SEC] dienen mittels Split-Key Verfahren als Backup-Agent.
Archivierung des Private Key	Der Private Key wird durch die Speicherung auf CDs archiviert (siehe Backup des Private Key).
Übertragung von Private Keys auf Verschlüsselungsmodul	Das Schlüsselpaar wird aus einem PKCS#12-File im Vier-Augen-Prinzip ins HSM importiert.
Speicherung von Private Keys auf Verschlüsselungsmodul	Das Schlüsselpaar der Root-CA ist in einer eigenen HSM-Partition abgelegt.
Verfahren zur Aktivierung des Private Key	Vor jeder Verwendung des Root-CA- Private Keys muss die HSM-Partition per Token des [CA-ADMIN] aktiviert werden.
Verfahren zur Deaktivierung des Private Key	Die Deaktivierung des Private Keys erfolgt durch Deaktivieren der zugehörigen HSM-Partition.
Verfahren zur Zerstörung des Private Key	Private Keys werden nicht zerstört
Unterstützte Standards und Zertifizierungen des HSM	Das verwendete HSM unterstützt die Standards FIPS 140-2 Level 3 und Common Criteria EAL4+.

6.3 Archivierung des Public Key

Alle CA-Zertifikate werden auf der Website online angeboten. Die Website und die CA werden gebackupt. Eine explizite Archivierung ist nicht vorgesehen.

6.4 Nutzungsdauer von Zertifikaten und Schlüsselpaaren

Microsoft empfiehlt, bei einer Zertifikatserneuerung auch die Schlüssel zu erneuern. Dies wird entsprechend bei den städtischen CAs so gehandhabt.

Root CA	– Lebensdauer des Zertifikats:	20 Jahre
	– Zertifikaterneuerung nach:	10 Jahren
	– Schlüsselerneuerung nach:	10 Jahren
User CA	– Lebensdauer des Zertifikats:	10 Jahre
	– Zertifikaterneuerung nach:	5 Jahren
	– Schlüsselerneuerung nach:	5 Jahren
Machine CA	– Lebensdauer des Zertifikats:	10 Jahre
	– Zertifikaterneuerung nach:	5 Jahren
	– Schlüsselerneuerung nach:	5 Jahren

6.5 Aktivierungsdaten

Für den Betrieb des HSM sind mehrere HW-Tokens erforderlich. Diese sind auf die Rollen [HSM-ADMIN], [CA-ADMIN] und [IT-SEC] aufgeteilt. Jede HSM-Partition ist zusätzlich mit einem sicheren Passwort geschützt.

6.6 Sicherheitsmassnahmen für die CA

6.6.1 Root CA

- Windows 2008 R2 Enterprise Server mit den aktuellen Service Packs und Security Updates
- **Keine** Active Directory Integration.
- Die Root CA wird Offline betrieben.
- Während des Online-Betriebs ist die CA durch die integrierte Windows-Firewall geschützt.
- Bitlocker-Verschlüsselung
- Aktueller Virenscanner

6.6.2 User CA

- Windows 2008 R2 Enterprise Server mit den aktuellen Service Packs und Security Updates
- Active Directory integriert.
- Sie schützt sich gegen andere Geräte durch eine Firewall.
- Bitlocker-Verschlüsselung
- Aktueller Virenscanner

6.6.3 Machine CA

- Windows 2008 R2 Enterprise Server mit den aktuellen Service Packs und Security Updates
- Active Directory integriert.
- Sie schützt sich gegen andere Geräte durch eine Firewall.
- Bitlocker-Verschlüsselung
- Aktueller Virenscanner

6.7 Technische Kontrollen zum Lebenszyklus

Für die verwendeten Standardprodukte für CA und HSM bestehen ordentliche Lizenz- und Supportverträge.

6.8 Sicherheitskontrollen des Netzwerks

Die Netzwerksicherheit wird durch den Einsatz von Firewalls gewährleistet.

6.9 Zeitsynchronisation und Time-Stamping

Die CAs synchronisieren sich am städtischen Zeitdienst. Damit ist gewährleistet, dass alle Zertifikate, CRL und Logeinträge synchronisiert sind.

In der Stadt steht kein Zeitstempeldienst zur Verfügung, es werden bei Bedarf externe Zeitstempeldienste eingesetzt.

7 Profile von Zertifikaten, CRL und OCSP

In diesem Abschnitt werden die grundlegenden Eigenschaften der PKI beschrieben.

7.1 Zertifikatsprofil

Die ausgestellten Zertifikate der städtischen CAs halten sich an die Vorgaben gemäss RFC 3280 (Internet X.509 Public Key Infrastructure).

Version Number	X.509 Zertifikat, Version 3
Certificate Extension:	Gemäss RFC 3280, Section 4
– Certificate Extensions	Es werden keine Extensions eingesetzt
– Standard Extensions	OID
– Authority Key Identifier	Besteht aus dem Hash (SHA-1) des Public Keys der jeweils ausstellenden CA.
– Subject Key Identifier	Besteht aus dem Hash (SHA-1) des Public Keys der antragstellenden CA.
– Key Usage	Gemäss RFC 3280, Section 4 (Festlegung Verwendungszweck)
– Private Key Usage Period	Wird nicht eingesetzt
– Certificate Policies	http://pki.stzh.ch/pki
– Policy Mappings	Wird nicht eingesetzt.
– Subject Alternative Name	Wird je nach Bedarf auf den Issuing CAs eingesetzt. Alle standardmässig unterstützten Attribute sind möglich: DNS, E-Mail, UPN, URL, DN, IP-Address, GUID, OtherName
– Issuer Alternative Name	Wird nicht eingesetzt
– Subject Directory Attributes	Wird nicht eingesetzt
– Basic Constraints	Subject Type = CA
– Name Constraints	nicht definiert.
– Policy Constraints	nicht definiert
– Path Length	keine
– Extended Key Usage	In von den Issuing CAs ausgestellten Zertifikaten ist hier der Einsatzbereich der jeweiligen Zertifikate definiert und eingegrenzt
– CRL Distribution Points	Die Distribution Points zeigen auf die PKI-Website. http://pki.stzh.ch/pki/crl/
– Inhibit Any-Policy Extension	Wird nicht verwendet
– Freshest CRL	Delta CRL werden nicht eingesetzt

Algorithm Object Identifiers	OID – Root: 1.3.6.1.5.5.7.3.4
Name Forms	Die CA unterstützen voll qualifizierte X.500 Distinguished Namen (Aussteller und Zertifikatseinsatz).
Applicable Certificate Policy Object Identifier (CP OID)	OID – Root: 1.3.6.1.5.5.7.3.4
Usage of Policy Constraints Extensions	Nicht implementiert.
Policy Qualifiers Syntax and Semantics	Nicht implementiert.
Processing Semantics for the Critical Certificate Policy Extensions	Die PKI Clients müssen die als kritisch gekennzeichneten Extensions verarbeiten (können).

7.2 CRL Profil

Version Number	Es kommt CRL Version 2 zum Einsatz (fix vorgegeben).
Authority Key Identifier	Generiert durch die CA. Key ID (SHA1) der ausstellenden CA
Reason Code	Generiert durch die CA. Erfasst durch den [CA-ADMIN]. Folgende Gründe werden unterstützt: – Unspecified – Key Compromise – Austritt – Ausserbetriebnahme

7.3 OCSP Profil

OCSP wird zurzeit nicht unterstützt.

8 Compliance Audit und andere Beurteilungen

8.1 Häufigkeit oder Voraussetzungen

Die Root CA sowie die untergeordneten CAs werden technisch und organisatorisch gemäss den Vorgaben aus Kap. 8.4 geprüft (Audit).

In der Regel findet eine Prüfung pro Kalenderjahr statt. Weitere Prüfungen können auf Wunsch der Betreiberin OIZ oder als Folge eines vorhergehenden Audits erfolgen.

[IT-SEC] ist für die Organisation der Audits zuständig.

8.2 Identität und Qualifikation des Auditors

Für Auditoren gelten folgende Anforderungen:

- Ein ausgewiesenes Know-how in technischen und organisatorischen PKI Aspekten muss vorhanden sein.
- [CA-ADMIN] darf nicht auch Auditor sein (Unabhängigkeit).

8.3 Beziehung des Auditors zur geprüften Stelle

Um Unabhängigkeit zu garantieren werden Audits durch eine externe Stelle durchgeführt.

8.4 Von der Beurteilung abgedeckte Themen

[IT-SEC] macht einen Vorschlag für die Prüfthemen. Die Themen werden durch die OIZ-Geschäftsleitung ratifiziert und – falls erforderlich – der ITLK vorgestellt.

8.5 Massnahmen nach festgestellten Mängeln

Auditresultate werden wie folgt behandelt:

- Die aufgezeigten Mängel werden durch [IT-SEC] gewichtet und priorisiert. Aus diesen Punkten wird eine Massnahmenliste erstellt.
- Die Massnahmenliste wird gegebenenfalls der OIZ-Geschäftsleitung zur Vernehmlassung gegeben.
- Die Abarbeitung der Massnahmenliste wird durch OIZ vorgenommen und durch [IT-SEC] koordiniert.

8.6 Mitteilung der Resultate

Die Resultate des Audits werden der OIZ-Geschäftsleitung mitgeteilt.

9 Weitere geschäftliche/rechtliche Bestimmungen

9.1 Gebühren

Die Dienstleistungen der städtischen PKI sind nicht kostenpflichtig, da es sich um einen Basisdienst der OIZ zu Gunsten der Stadtverwaltung handelt.

Demzufolge sind Neuausstellung von Zertifikaten, Ersatz von abgelaufenen Zertifikaten, Revokation etc. ohne Kostenfolge.

9.2 Finanzielle Verantwortung

Die OIZ schliesst soweit gesetzlich möglich jede Haftung aus. Die OIZ übernimmt insbesondere keine Haftung für direkte oder indirekte Folgeschäden, für Schäden, die aus einem Nutzungsausfall entstanden sind, und /oder für entgangenen Gewinn.

Die OIZ lehnt ferner jede Haftung ab, die durch oder im Zusammenhang mit dem Gebrauch der Zertifikatsinfrastruktur entstehen oder sich infolge eines Missbrauchs der Zertifikate durch die Zertifikatsnutzenden mit oder ohne ihr Wissen entstehen könnte. Ebenfalls ausgeschlossen sind Haftungsansprüche für Schäden, die durch die Löschung, Zerstörung, das Scheitern oder Misslingen beim Speichern von Nachrichten oder dergleichen infolge der Zertifikatsverwendung entstehen könnten.

Die Zertifikatsnutzenden haften in Gegenzug für alle Schäden, die der OIZ oder Dritten infolge eines Missbrauchs der Zertifikate entstehen.

Das Inventar der OIZ ist angemeldet und versichert.

9.3 Vertraulichkeit von Geschäftsinformationen

Die OIZ trifft kryptographische Massnahmen bedarfsbezogen. Richtlinien für die Bedarfsabklärung leiten sich aus dem Handbuch Informationssicherheit ab, sofern Massnahmen nicht von übergeordnetem Recht verlangt werden.

9.4 Vertraulichkeit von Personendaten

Es gelten die Vorgaben von IDG, IDV und DSV.

9.5 Rechte des geistigen Eigentums

Siehe Kapitel 9.2.

9.6 Zusicherungen und Gewährleistungen

Siehe Kapitel 9.2.

9.7 Gewährleistungsausschluss

Die städtischen CAs wurden durch die OIZ im Auftrag der Stadt Zürich nach dem aktuellen Standard mit dem Ziel einer angemessenen Sicherheit implementiert. Angemessen bedeutet, dass das erreichte Sicherheitsniveau demjenigen des Windows Passwortes entspricht.

Die ausgestellten Zertifikate sind nur dann geeignet für starke Authentisierung, wenn die Aufbewahrung des Private Keys sicher ist und dieser nicht exportiert werden kann.
In jedem Fall muss ein solcher Einsatz durch [IT-SEC] bewilligt werden.

Jegliche Haftungsansprüche, die durch dieses Dokument zu entstehen scheinen, sind nichtig und werden wegbedungen.

9.8 Haftung

Siehe Kapitel 9.2.

9.9 Schadenersatz

Siehe Kapitel 9.2.

9.10 Inkrafttreten und Beendigung

Dieses Dokument tritt durch die Publikation in Kraft und behält seine Gültigkeit bis

- es durch eine neue Version ersetzt wird
- es durch [IT-SEC] explizit als ungültig erklärt wird.

Die CP/CPS bleibt gemäss Urheberrecht auch nach ihrem Rückzug geistiges Eigentum der Stadt.

9.11 Einzelbenachrichtigungen und Mitteilungen an Teilnehmer

Nicht anwendbar – Die OIZ betreibt die städtische PKI für die Stadt.

9.12 Änderungen

Anpassungen an der vorliegenden CP/CPS werden durch [IT-SEC] durchgeführt und erfolgen ohne vorherige Ankündigung. Mit der Publikation auf der Website gemäss Kapitel 2 tritt die neue Regelung in Kraft.

Anpassungen werden im städtischen Intranet signalisiert. Die Details der Anpassungen werden dabei nicht mitgeteilt. Mit der Publikation auf der Website gemäss Kapitel 2 tritt die neue Regelung in Kraft.

Anpassungen am Ablageort werden vorfallsbezogen durch [IT-SEC] bestimmt. Der neue Ort wird im Intranet bei den News publiziert.

9.13 Beilegung von Streitigkeiten

Alleiniger Gerichtsstand ist Zürich.

9.14 Gerichtsstand

Alleiniger Gerichtsstand ist Zürich.

9.15 Einhaltung geltenden Rechts

Diese CP/CPS untersteht der Schweizer Rechtsprechung.

9.16 Sonstige Bestimmungen

Eine Kompromittierung der Dienste durch höhere Gewalt wird umgehend durch [IT-SEC] verfolgt.

Ansonsten gelten keine weiteren Bestimmungen.