CP/CPS – Stadt Zuerich PKI 2.0

Certificate Policy (CP) und Certification Practice Statement (CPS) der Certification Authorities (CA) der städtischen Public-Key-Infrastruktur (PKI) 2.0

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, S. Furrer

Version
1.0

Versions-Nr.	Datum	Name	Tätigkeit
1.0	14.02.17	oizlip	Ersterstellung

Inhalt

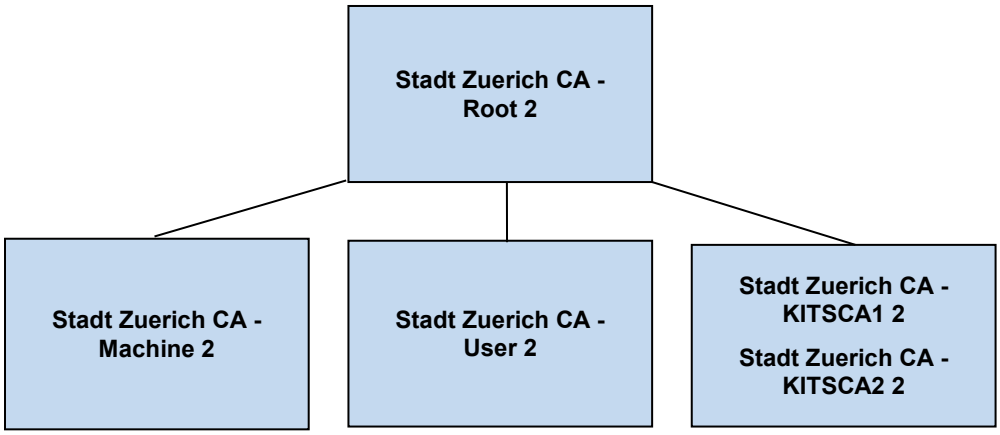
1 Einführung

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 2.0 weist folgende zweistufige Hierarchie auf:



Die städtische PKI 2.0 umfasst demnach aktuell fünf CA:

- Root CA:
  - «Stadt Zuerich CA - Root 2»
- Issuing CA:
  - «Stadt Zuerich CA - Machine 2»
  - «Stadt Zuerich CA - User 2»
  - «Stadt Zuerich CA - KITSCA1 2» und «Stadt Zuerich CA - KITSCA2 2»

Ein Ausbau mit weiteren Issuing CA ist möglich.

1.1.2 Zertifikatsklassen und Zertifikatstypen

Als rechtliche Grundlage gilt das «Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen (Bundesgesetz über die elektronische Signatur, ZertES)» (SR 943.03).

Für die Stadtverwaltung sind zudem die Standards des Vereins eCH massgebend, hier insbesondere der eCH-Standard «eCH-0048 PKI-Zertifikatsklassen». Dieser beschreibt vier Zertifikatsklassen mit unterschiedlichen Vertrauensniveaus. Die wichtigsten Anforderungen sind aus der nachfolgenden Tabelle ersichtlich.

Kriterium	Klasse 1	Klasse 2	Klasse 3	Qualifiziert
Vertrauensniveau	niedrig	hoch	sehr hoch	sehr hoch
Rechtsbezug	Elektronische Signatur gemäss ZertES	Fortgeschrittene elektronische Signatur gemäss ZertES	Fortgeschrittene elektronische Signatur gemäss ZertES	Qualifizierte elektronische Signatur gemäss ZertES
Identitätsnachweis	E-Mail-Account / Domain-Account / technischer Account	**Person**: Personalisierte Dokumente (z. B. Führerausweis) **Rolle, Gruppe und Maschine:** Auftrag des Verantwortlichen mit Berechtigungsnachweis	**Person**: Hoheitliches Dokument (Reisepass, ID) **Rolle, Gruppe und Maschine:** Auftrag des Verantwortlichen mit erweitertem Berechtigungsnachweis	**Person**: Hoheitliches Dokument (Reisepass, ID) **Rolle, Gruppe und Maschine:** Nicht anwendbar
Namen	Name kann frei gewählt werden (CN). Name des E-Mail- oder technischen Accounts wird im Zertifikat aufgenommen.	Natürliche Person gemäss Identitätsnachweis. Das Zertifikat kann auf ein Pseudonym ausgestellt werden. Spezielle Attribute (Berufsbezeichnungen, Titel etc.) erfordern gesonderten Berechtigungsnachweis zu deren Verwendung.		
Registrierung	Beliebiger Prozess mit faktischer Verifizierung der oben genannten Accountdaten	Sicherer Prozess, basierend auf eingereichten Identitäts-Unterlagen	Sicherer Prozess, basierend auf einer persönlichen Antragstellung ggf. auch bei Dritten	Persönliche Antragstellung bei anerkannten Registrierungsstellen.
Archivierung (Antragsdokumente/-daten)	Laufzeit plus 2 Jahre	Laufzeit plus 5 Jahre (Verjährungsfrist gemäss OR)	Laufzeit plus 11 Jahre	
Gültigkeit der Registrierung	wie Laufzeit Zertifikat	Maximal 6 Jahre		
Security Token	Software- oder Hardware-Token		Hardware-Token evaluiert gemäss FIPS 140-1/ 140-2 Level 2 oder BAKOM TAV	Hardware-Token gemäss BAKOM TAV SR 943.032.1
Key Management für Security Token	Key-Backup und –Recovery seitens CSP für: – Signaturschlüssel: DARF NICHT erfolgen – Verschlüsselungsschlüssel: KANN in sicheren und dokumentierten Infrastrukturen und Prozessen erfolgen			Hardware-Token gemäss BAKOM TAV SR 943.032.1
Anforderungen an CA (Betrieb, Personal, Prozesse)	Dokumentiertes Betriebs- und Sicherheitskonzept	Dokumentiertes Betriebs- und Sicherheitskonzept; Zugangskontrolle zu CA-Systemen und Backups etc.; jährliches Audit durch interne Verantwortliche	Dokumentiertes Betriebs- und Sicherheitskonzept; Zugangskontrolle zu CA-Systemen und Backups etc.; jährliches Audit durch ausgewiesen qualifizierte Revision (intern/ extern)	Gemäss: ETSI TS 101 456, Kap. 6.1, 7.1, 7.4, 7.5, 8.1; jährliche Audits. Details siehe BAKOM TAV SR 943.032.1, Kap. 3.2 Organisation und operative Grundsätze
Erlaubte Zertifikatsinhaber (Subject)	Keine Vorgaben	– natürliche Personen – juristische Personen, einfache Gesellschaften und Organisationen – Gruppen, Rollen – Maschinen (SSL, IPsec etc.)		natürliche Personen (Client-Zertifikate)
Einsatz	Alle Zwecke zugelassen			Signatur elektronischer Dokumente (Willenserklärung)
Widerrufsinformationen (per CRL und/oder OCSP)	MUSS publiziert werden	MUSS publiziert werden; mindestens tägliche Aktualisierung		MUSS per CRL angeboten werden; mindestens tägliche Aktualisierung.

Die städtische PKI stellt Zertifikate der Klassen 1 und 2 aus.

1.2 Name und Identifikation des Dokuments

Das vorliegende Dokument trägt die folgende Bezeichnung:

«Certificate Policy (CP) und Certification Practice Statement (CPS) der Certification Authorities (CA) der städtischen Public-Key-Infrastruktur (PKI) 2.0»
(kurz: «CP/CPS – Stadt Zuerich PKI 2.0» resp. «CP/CPS»).

OID der CP/CPS: 1.3.6.1.4.1.13569.10.20.10.1.

Das Dokument ist analog dem RFC 3647 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework» strukturiert.

1.3 PKI-Teilnehmer

1.3.1 Certification Authorities (CA)

Die städtische PKI 2.0 umfasst zum aktuellen Zeitpunkt die folgenden CA:

CA	Beschreibung	
Root CA	Bezeichnung	«Stadt Zuerich CA – Root 2»
	Zweck	Die städtische «Root 2 CA» stellt Zertifikate für alle untergeordneten Issuing CA aus.
	Namensraum	Die «Root CA» stellt Zertifikate für folgende Namensräume aus: – C = CH – O = Stadt Zuerich – E = pki@zuerich.ch
User CA	Bezeichnung	«Stadt Zuerich CA – User 2»
	Zweck	Die «User CA» stellt Zertifikate für Personen aus.
	Namensraum	Zertifikate werden für die folgenden Namensräume ausgestellt: – C = CH – O = Stadt Zuerich – OU = Departement/Dienstabteilung (gemäss städtischen Namenskonventionen) – E = pki@zuerich.ch
Machine CA	Bezeichnung	«Stadt Zuerich CA – Machine 2»
	Zweck	Die «Machine CA» stellt Zertifikate für Geräte aus (Clients, Server, Netzwerkgeräte etc.).
	Namensraum	Zertifikate werden für die folgenden Namensräume ausgestellt: – C = CH – O = Stadt Zuerich oder Marketingnamen – OU = Departement/Dienstabteilung (gemäss städtischen Namenskonventionen) – E = pki@zuerich.ch
KITS CA	Bezeichnung	«Stadt Zuerich CA – KITSCA1 2» «Stadt Zuerich CA – KITSCA2 2»
	Zweck	Die beiden «KITS CA» stellen Zertifikate für Geräte der Schulinformatik aus (Clients, Server, Netzwerkgeräte etc.).

1.3.2 Registration Authorities (RA)

Die Personalabteilungen der Departemente und Dienstabteilungen gelten als lokale Registrierungsstellen (LRA) und sind für die Identifizierung und Registrierung der Antragsteller für persönliche Zertifikate verantwortlich.

Die Rolle der RA wird implizit durch das Active Directory (AD) und dessen Betreiber resp. durch die CA-Administration und die Fachstelle Informationssicherheit wahrgenommen. Eine Identifizierung und Registrierung durch persönliches Vorsprechen bei der RA ist in der Regel nicht erforderlich.

1.3.3 Zertifikatsinhaber (Subscriber)

CA	Beschreibung
Root CA	Inhaber der durch die Root CA ausgestellten Zertifikate sind die Verantwortlichen von untergeordneten CA.
User CA	Inhaber der durch die User CA ausgestellten Zertifikate sind (interne und externe) Mitarbeitende der Stadtverwaltung, die im Active Directory (AD) erfasst sind.
Machine CA	Inhaber der durch die Machine CA ausgestellten Zertifikate sind Mitarbeitende der Stadtverwaltung als Antragsteller solcher Zertifikate resp. technische User (z. B. städtische Geräte wie Clients, Server oder Netzwerkgeräte, Programme oder Dienste).

1.3.4 Zertifikatsnutzer (Relying Parties)

Die Zertifikatsnutzung von durch die städtische PKI ausgestellten Zertifikaten erfolgt hauptsächlich innerhalb der Stadtverwaltung. Die Nutzung oder Verifikation städtischer Zertifikate durch externe Partner ist durch Aufbau der Vertrauenskette zu städtischen CA-Zertifikaten möglich.

CA	Beschreibung
Root CA	Nutzer der durch die Root CA ausgestellten Zertifikate sind die untergeordneten CA, sowie alle Personen und Maschinen, die die Vertrauenswürdigkeit dieser und untergeordneter Zertifikate überprüfen.
User CA	Als Nutzer der durch die User CA ausgestellten Zertifikate gelten Personen, die diese Zertifikate selbst nutzen oder verifizieren resp. ihnen vertrauen.
Machine CA	Als Nutzer der durch die Machine CA ausgestellten Zertifikate gelten persönliche oder unpersönliche/technische Benutzer, die diese Zertifikate selbst nutzen oder verifizieren resp. ihnen vertrauen.

1.3.5 Weitere Teilnehmer

Keine.

1.4 Zertifikatsverwendung

Städtische Zertifikate dürfen für die folgenden Einsatzzwecke verwendet werden.

CA-Zertifikate

- Signatur von Zertifikaten
- Signatur der Zertifikatsperrliste

Personenzertifikate

- Verschlüsselung und Signatur von E-Mails
- Signatur von Dokumenten und in Workflows
- Signatur von Softwarecode
- Benutzeranmeldung an Domäne und/oder Applikationen

Maschinenzertifikate

- TLS-Verschlüsselung (v. a. für interne Verbindungen)
- Client- und Server-Authentisierung (interne Geräte)
- Remote Access in mobilen Anwendungsfällen

Andere Verwendungszwecke von Zertifikaten

Andere Verwendungszwecke sind projektbezogen zu beantragen und durch die Fachstelle Informationssicherheit und die CA-Administration zu beurteilen und zu bewilligen.

1.5 Verwaltung der Policy

1.5.1 Organisation der Dokumentenverwaltung

Die CP/CPS basiert auf den folgenden Richtlinien und Standards:

- Handbuch Informationssicherheit der Stadt Zürich, STRB 634 vom 9. Juli 2014
- RFC 3647.

Für die Pflege der vorliegenden CP/CPS ist die Fachstelle Informationssicherheit verantwortlich.

1.5.2 Kontaktstellen / Rollen

Kontaktstelle für dieses Dokument:

Stadt Zürich
Organisation und Informatik (OIZ)
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.

Die für die PKI relevanten Rollen sind in Kapitel 1.6 entsprechend bezeichnet.

1.5.3 Genehmigungsverfahren

Anpassungen an diesem Dokument werden durch die Fachstelle Informationssicherheit 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.

Begriff	**Bedeutung**
AD	Active Directory
Administration	MitarbeiterIn von Server- oder Netzwerkadministration/-Betrieb *[Rolle]*
Auto-Enrollment	Automatisierter Bezug von Zertifikaten (siehe auch Self-Enrollment)
Benutzer	Im Active Directory erfasste Mitarbeitende *[Rolle]*
CA	Certification Authority (Zertifizierungsstelle)
CA-Administration	MitarbeiterIn von CA-Administration/-Betrieb *[Rolle]*
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
D/DA	Departement/Dienstabteilung der Stadtverwaltung Zürich
DN	Distinguished Name: Identifiziert den Eigner des Zertifikates
Enterprise-Administration	MitarbeiterIn mit vollen Administrationsberechtigungen im Active Directory *[Rolle]*
Fachstelle Informationssicherheit	MitarbeiterIn der Fachstelle Informationssicherheit der Organisation und Informatik *[Rolle]*
HSM	Hardware Security Modul (sicherer Hardware Schlüsselspeicher)
HSM-Administration	MitarbeiterIn von HSM-Administration/-Betrieb *[Rolle]*
LRA	Local Registration Authority (lokale Registrierungsstelle)
LRAO	Local Registration Authority Officer *[Rolle]*
OCSP	Online Certificate Status Protocol
OID	Object Identifier; weltweit eindeutiger Identifikator für die Bezeichnung von Dokumenten/Objekten
OIZ	Organisation und Informatik der Stadt Zürich
RA	Registration Authority (Registrierungsstelle) *[Rolle]*
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)
Service Desk	Zentraler Service Desk von OIZ *[Rolle]*
TPM	Trusted Platform Module; im Client integrierter Hardware-Chip, welcher die Umsetzung von Sicherheitsfunktionen erlaubt
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur

2 Publikation und Aufbewahrungsorte

2.1 Aufbewahrungsorte

Die durch die CA ausgestellten Benutzer- und Maschinenzertifikate werden in der Regel als Software-Token im Benutzerprofil und im Active Directory resp. auf dem Gerät (Client, Server etc.) gespeichert. Bei einigen Zertifikaten werden die privaten Schlüssel im TPM des Clients abgelegt.

Private Schlüssel von CA-Zertifikaten werden auf einem Hardware Security Modul gespeichert.

2.2 Publikation von Informationen

Allgemeine Informationen über die städtische PKI werden auf zwei unterschiedlichen Webseiten im Intranet der Stadt resp. im Internet publiziert:

Aufbewahrungsort	Inhalt

Intranet-Webseite:
http://fach-it.intranet.stzh.ch/
	Ausschliesslich innerhalb der Stadtverwaltung zugängliche Informationen:
	– Übersicht der PKI-Umgebung
	– Dokumente:
	  – Nutzungsrichtlinien
	  – Städtische Rechtsgrundlagen
	  – Beschreibungen, Anleitungen
	– Zertifikatsmanagement:
	  – Link auf die Zertifikat-Antragsseiten
	– Kontaktstellen

Internet-Webseite:
http://pki.stzh.ch
	Informationen, die auch ausserhalb der Stadtverwaltung zugänglich sein müssen:
	– Dokumente:
	  – Aktuelle Version der CP/CPS
	– Zertifikatsmanagement:
	  – CA-Zertifikate
	  – CRL (Zertifikatssperrlisten)
	– Kontaktstellen

Die Verantwortung für die Publikation all dieser Informationen liegt bei der OIZ.

2.3 Publikationsintervalle

Für die CA der städtischen PKI gelten die nachfolgenden Publikationsintervalle:

CA	Beschreibung	
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-Publikationspunkt: http://pki.stzh.ch/pki/crl/
	CA-Zertifikat	Publikation manuell

User CA	CRL	– Aktualisierung des CRL-Verzeichnisses: Täglich
		– Ausstellung der CRL: Alle 4 Tage
		– Überlappung der CRL: 3 Tage
		– Lebensdauer der CRL: 7 Tage
		– Delta CRL: Nein
		– CRL-Publikationspunkt:
		  – Primär: http://pki.stzh.ch/pki/crl/
		  – Sekundär: ldap:/// (Standard AD-Integration)

	CA-Zertifikat	Publikation manuell

Machine CA	CRL	– Aktualisierung des CRL-Verzeichnisses: Täglich
		– Ausstellung der CRL: Alle 4 Tage
		– Überlappung der CRL: 3 Tage
		– Lebensdauer der CRL: 7 Tage
		– Delta CRL: Nein
		– CRL-Publikationspunkt:
		  – Primär: http://pki.stzh.ch/pki/crl/
		  – Sekundär: ldap:/// (Standard AD-Integration)

	CA-Zertifikat	Publikation manuell

2.4 Zugriffsschutz

Die oben genannte Intranet-Webseite ist für städtische Mitarbeitende und im Auftragsverhältnis stehende externe Mitarbeitende im Züri-Netz lesend zugänglich.

Die Internet-Webseite ist allgemein – auch vom Internet her – für alle Zertifikatsnutzer zugänglich.

Auf Publikationsverzeichnisse haben nur CA-Administration und Enterprise-Administration Schreibrechte.

3 Identifikation und Authentisierung

Die städtische PKI verfügt über eigene ausgeprägte Prozesse. Diese gewährleisten, dass

- die Identität der Zertifikatsinhaber 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.

In den folgenden Abschnitten werden die Prozesse für die Identifikation und Authentisierung beschrieben.

3.1 Namensgebung

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

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

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

3.1.1 Root CA

Namensarten	Die Root CA «Stadt Zuerich CA – Root 2» stellt Zertifikate für untergeordnete (Issuing) CA 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 – Machine 2» und «Stadt Zuerich CA – User 2» – E = E-Mail-Adresse der zuständigen Organisation: pki@zuerich.ch
Aussagekräftige Namen	Die nach obigen Regeln erstellten Benennungen sind selbstredend.
Anonymisierung oder Pseudonymisierung	Nicht anwendbar.
Regeln für die Auslegung unterschiedlicher Namensarten	Nicht anwendbar.
Eindeutigkeit von Namen	Die Namen müssen eindeutig sein; dies wird bei der Ausgabe eines neuen Zertifikats sichergestellt.
Erkennung, Authentisierung und Rolle von Marken	Nicht anwendbar.

3.1.2 User CA

Namensarten	Die User CA «Stadt Zuerich CA – User 2» stellt Zertifikate für Personen – persönliche und unpersönliche Benutzer (z. B. Gruppen) – 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	Eine Anonymisierung bzw. Pseudonymisierung für ausgestellte Benutzerzertifikate ist nur zugelassen, wenn der tatsächliche Namen des Benutzers in den Registrierungsdaten hinterlegt ist (gemäss separaten Richtlinien).
Regeln für die Auslegung unterschiedlicher Namensarten	Nicht anwendbar.
Eindeutigkeit von Namen	Die Namen müssen eindeutig sein; dies wird bei der Ausgabe eines neuen Zertifikats gewährleistet (User Principle Name UPN).
Erkennung, Authentisierung und Rolle von Marken	Nicht anwendbar.

3.1.3 Machine CA

Namensarten	Die Machine CA «Stadt Zuerich CA – Machine 2» stellt Zertifikate für Geräte (Server, Clients, Router, Anwendungen 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: pki@zuerich.ch
Aussagekräftige Namen	Die nach obigen Regeln erstellten Benennungen sind selbstredend.
Anonymisierung oder Pseudonymisierung	Die für die erstellten Maschinenzertifikate verwendeten Namen sind technische Bezeichnungen gemäss städtischem Namenskonzept.
Regeln für die Auslegung unterschiedlicher Namensarten	Nicht anwendbar.
Eindeutigkeit von Namen	Die Namen müssen eindeutig sein, dies wird bei der Ausgabe eines neuen Zertifikats gewährleistet.
Erkennung, Authentisierung und Rolle von Marken	Nicht anwendbar.

3.2 Anträge für Zertifikatsausstellung

3.2.1 Root CA

Notwendige Credentials	Die Root CA stellt ausschliesslich Zertifikate für untergeordnete CA aus. Für die Implementation einer neuen Issuing CA muss ein bewilligter Projektauftrag vorliegen. Die Authentizität des Zertifikatsantrags (CSR) der untergeordneten CA wird durch die CA-Administration und die Fachstelle Informationssicherheit überprüft.
Authentizitätsprüfung der Credentials	Vier-Augen-Prinzip: Anwesenheit von CA-Administration und Fachstelle Informationssicherheit erforderlich.
Enrollment	Das Enrollment erfolgt manuell durch die CA-Administration an der Konsole. Der Antrag wird von der CA auf Hold gesetzt. Die Ausstellung des Zertifikates erfolgt manuell unter Berücksichtigung des Vier-Augen-Prinzips auf Basis eines Split-Passwortes.
Authentizitätsprüfung der Person	Der Antragsteller wird bei Eintritt in die D/DA gemäss einer separaten städtischen Richtlinie identifiziert und registriert.

3.2.2 User CA

Notwendige Credentials	User Account im AD und Mitgliedschaft in der entsprechenden AD-Gruppe oder bestehendes gültiges Zertifikat.
Authentizitätsprüfung der Credentials	– Die OIZ ist zuständig für die Struktur des AD. Sie eröffnet, mutiert und löscht OU. – Die Dienstabteilungen sind verantwortlich für die Vollständigkeit und Korrektheit ihrer eigenen Userdaten (User, E-Mail-Adressen, andere Attribute).
Enrollment	– Grundsätzlich Self-Enrollment. – Auto-Enrollment bei der ersten Benutzeranmeldung (falls der Benutzer bereits in der entsprechenden AD-Gruppe integriert ist).
Authentizitätsprüfung der Person	Der Benutzer wird bei Eintritt in die D/DA gemäss einer separaten städtischen Richtlinie identifiziert und registriert.

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 den Benutzer: Username/Passwort. – Die Dienstabteilungen sind verantwortlich für die Vollständigkeit und Korrektheit ihrer eigenen Accountdaten (User, E-Mail-Adressen, andere Attribute). – Bei maschinellem Enrollment: Vorweisen eines gültigen Zertifikates.
Enrollment	– Self-Enrollment (über offizielle Website, MMC oder SCEP). – Auto-Enrollment bei Domain-Login durch Computeraccount (falls in Zertifikatsvorlage definiert).
Authentizitätsprüfung der Person	– Bei Enrollment durch den Benutzer: Der Antragsteller wird bei Eintritt in die D/DA gemäss einer separaten städtischen Richtlinie identifiziert und registriert. – Bei maschinellem Enrollment: nicht anwendbar.

3.3 Anträge für Zertifikatserneuerung

3.3.1 Root CA

Notwendige Credentials	Bestehendes gültiges Zertifikat. Die Authentizität wird im Vier-Augen-Prinzip durch die CA-Administration und die Fachstelle Informationssicherheit überprüft.
Enrollment	Das Enrollment erfolgt manuell durch die CA-Administration an der Konsole. Der Antrag wird von der CA auf Hold gesetzt. Die Ausstellung des Zertifikates erfolgt manuell unter Berücksichtigung des Vier-Augen-Prinzips.

3.3.2 User CA

Notwendige Credentials	User Account im AD und bestehendes gültiges Zertifikat.
Enrollment	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 Benutzer (lokaler Admin). – Auto-Enrollment im Computer-Account Kontext. – Bei Web-Enrollment (z. B. TLS): Prozess analog Erstausstellung.

3.4 Anträge für Zertifikatsrevokation

3.4.1 Root CA

Notwendige Credentials	Verifikation Antrag/Antragsteller. Anwesenheit von CA-Administration und Fachstelle Informationssicherheit.
Authentizitätsprüfung der Credentials	Vier-Augen-Prinzip auf Basis Split-Passwort.
Revokation	Revokation unter Berücksichtigung des Vier-Augen-Prinzips mit Hilfe der beiden Split-Passwörter.

3.4.2 User CA

Authentizitätsprüfung der Person (inkl. Ablauf)	– Der Benutzer kontaktiert den Service Desk im Falle eines Schlüsselverlusts (inkl. Schlüsselbeschädigung). – Der Service Desk erstellt einen Incident und weist diesen der CA-Administration zu. – Die CA-Administration revoziert das Zertifikat nach Rücksprache mit dem Benutzer 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. Verlust des Schlüssels, Auflösung des Arbeitsverhältnisses.

3.4.3 Machine CA

Authentizitätsprüfung der Person (inkl. Ablauf)	– Bei Diebstahl/Verlust eines Clients: Der Benutzer kontaktiert den Service Desk. – Bei Kompromittierung eines Serverzertifikats: Die verantwortliche Administration kontaktiert den Service Desk. – Der Service Desk erstellt einen Incident und weist diesen der CA-Administration zu. – Die CA-Administration revoziert das Zertifikat nach Rücksprache mit dem Benutzer oder der verantwortlichen Administration.
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)	– Der Benutzer kontaktiert den Service Desk im Falle eines Schlüsselverlusts oder einer Schlüsselbeschädigung. – Der Service Desk erstellt einen Incident mit Angaben über das betroffene Verschlüsselungszertifikat (Serienummer). – Die CA-Administration exportiert den betroffenen – mit Key Recovery Agent verschlüsselten – Schlüssel aus der Datenbank (Key Recovery 1. Teil). – Die Fachstelle Informationssicherheit entschlüsselt den verschlüsselten Schlüssel (mit Key Recovery Agent Client und zugehörigem Passwort), stellt ihn als passwortgeschützte PKCS#12-Datei dem Benutzer zu und löscht die Datei anschliessend (Key Recovery 2. Teil). – Die Fachstelle Informationssicherheit stellt dem Service Desk das Passwort für den Key-Import (ab Datei) beim Benutzer zu. – Der Service Desk kontaktiert den Benutzer, um den wiederhergestellten Schlüssel im Postfach des Benutzers mit Hilfe des Passworts zu entschlüsseln und ins Profil zu importieren; der Benutzer kann alle Aktionen mitverfolgen.

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 Zertifikatsarchiv 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 CA dürfen ausschliesslich durch die CA-Administration und die Fachstelle Informationssicherheit im Team (im 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 durch die CA-Administration und die Fachstelle Informationssicherheit mit Soft-Keys erstellt. – Root CA: Einloggen durch Split-Passwort durch CA-Administration und Fachstelle Informationssicherheit. – Root CA: CA-Administration und Fachstelle Informationssicherheit reichen den Antrag mittels mmc ein und erzeugen das Zertifikat. – Untergeordnete CA: Import des Zertifikates. – Speichern des Zertifikates und der Schlüssel als PKCS#12 File auf 2 CDs (Sicherstellung/ Verschlüsselung mit Split-Passwort). Es werden neue Passwörter definiert. – Import von Zertifikate und Schlüssel ins HSM, anschliessend sicheres Löschen der Soft-Keys. – Sicherstellung jeweils einer CD in den beiden Safes von CA-Administration und Fachstelle Informationssicherheit.

4.1.2 User CA

Wer kann einen Zertifikatsantrag einreichen?	Alle Benutzer mit einem AD-Account dürfen Anträge stellen.
Enrollment Prozess und Verantwortungen	– Anträge erfolgen über Self-Enrollment oder Auto-Enrollment. – Der 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 für mindestens 1 Jahr archiviert. Der Event wird zudem an den Loghost weitergeleitet.

4.1.3 Machine CA

Wer kann einen Zertifikatsantrag einreichen?	Anträge dürfen durch – die CA-Administration aufgrund eines vorliegenden AD-Accounts – Benutzer und Computer mit einem AD-Account gestellt werden.
Enrollment Prozess und Verantwortungen	– Anträge erfolgen über die PKI-Website, Self-Enrollment oder Auto-Enrollment. – Der 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 für mindestens 1 Jahr archiviert. Der Event wird zudem an den Loghost weitergeleitet.

4.2 Bearbeitung des Zertifikatsantrags

4.2.1 Root CA

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

4.2.2 User CA

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

4.2.3 Machine CA

Es werden nur Zertifikatsanträge 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 und in der CA-Datenbank.
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 und in der CA-Datenbank.
Benachrichtigung des Antragsstellers über die Zertifikatsausstellung	Antragsteller werden über das Change Management Tool informiert, sofern die Zertifikatsausstellung manuell durch die CA-Administration 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 die CA-Administration akzeptiert.
Publikation des Zertifikats durch die CA	Die Zertifikate werden durch die CA-Administration 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 an die CA-Administration.

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 an die CA-Administration.

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 CA und von CRL – 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 Zertifikate dürfen ausschliesslich durch die jeweiligen Benutzer 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 Benutzer-Gruppe). Die Zertifikate müssen – soweit möglich – über die Attribute «Schlüsselverwendung» und «Erweiterte Schlüsselverwendung» eine anderweitige Nutzung verhindern.
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). Die Zertifikate müssen – soweit möglich – über die Attribute «Schlüsselverwendung» und «Erweiterte Schlüsselverwendung» eine anderweitige Nutzung verhindern.
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)

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

Eine Zertifikatsverlängerung ist für die städtischen Zertifikate grundsätzlich zulässig.

4.6.1 Root CA

Bedingung für Zertifikatsverlängerung	Die Zertifikate der «Stadt Zuerich CA – Root 2» werden nach 10 Jahren (=Renewal Time) erneuert. Die Zertifikate von untergeordneten CA 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	Ein Zertifikats-Renewal wird durch die CA-Administration manuell beantragt.
Verfahren für Renewal Anträge	Ein Renewal erfolgt analog dem Enrollment in Kapitel 4.1.1.
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung des Renewals erfolgt analog dem Enrollment in Kapitel 4.3.1.
Annahme eines Renewal Zertifikats	Die Annahme des Renewals erfolgt analog dem Vorgehen in Kapitel 4.4.1.
Publikation des Renewal Zertifikats durch CA	Die Publikation des Renewals erfolgt analog dem Enrollment in Kapitel 4.4.1.
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung des Renewals erfolgt analog dem Enrollment in Kapitel 4.4.1.

4.6.2 User CA

Bedingung für Zertifikatsverlängerung	Die von der «Stadt Zuerich CA – User 2» 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 Benutzer per Auto-Enrollment, Self-Enrollment oder Web-Enrollment. – Zentral bereitgestellte Zertifikate: Enrollment durch die CA-Administration und Bereitstellung auf zentralem Server.
Verfahren für Renewal Anträge	Ein Renewal erfolgt analog dem Enrollment in Kapitel 4.1.2.
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung eines Renewals erfolgt analog dem Enrollment in Kapitel 4.3.2.
Annahme eines Renewal Zertifikats	Die Annahme eines Renewals erfolgt analog dem Vorgehen in Kapitel 4.4.2.
Publikation des Renewal Zertifikats durch CA	Die Publikation eines Renewals erfolgt analog dem Enrollment in Kapitel 4.4.2.
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung eines Renewals erfolgt analog dem Enrollment in Kapitel 4.4.2.

4.6.3 Machine CA

Bedingung für Zertifikatsverlängerung	Die von der «Stadt Zuerich CA – Machine 2» 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 Benutzer per Auto-Enrollment, SCEP, oder Self-Enrollment.
Verfahren für Renewal Anträge	Ein Renewal erfolgt analog dem Enrollment in Kapitel 4.1.3.
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung eines Renewals erfolgt analog dem Enrollment in Kapitel 4.3.3.
Annahme eines Renewal Zertifikats	Die Annahme eines Renewals erfolgt analog dem Vorgehen in Kapitel 4.4.3.
Publikation des Renewal Zertifikats durch CA	Die Publikation eines Renewals erfolgt analog dem Enrollment in Kapitel 4.4.3.
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung eines Renewals erfolgt analog dem Enrollment in Kapitel 4.4.3.

4.7 Zertifikatserneuerung (Re-Key)

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

Eine Zertifikatserneuerung ist für die städtischen Zertifikate grundsätzlich zulässig.

4.7.1 Root CA

Bedingung für Zertifikatserneuerung	Die Zertifikate der «Stadt Zuerich CA – Root 2» werden nach 20 Jahren (=Re-Key Time, Lifetime) mit neuen Schlüsseln erneuert. Die Zertifikate von untergeordneten CA 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 die CA-Administration manuell beantragt.
Verfahren für Re-Key Anträge	Das Re-Key erfolgt analog dem Enrollment in Kapitel 4.1.1.
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.3.1.
Annahme eines Re-Key Zertifikats	Die Annahme des Re-Key erfolgt analog dem Vorgehen in Kapitel 4.4.1.
Publikation des Re-Key Zertifikats durch CA	Die Publikation des Re-Key erfolgt analog dem Enrollment in Kapitel 4.4.1.
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung eines Re-Key erfolgt analog dem Enrollment in Kapitel 4.4.1.

4.7.2 User CA

Bedingung für Zertifikatserneuerung	Die von der «Stadt Zuerich CA – User 2» 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 Benutzer per Auto-Enrollment, Self-Enrollment oder Web-Enrollment. – Zentral bereitgestellte Zertifikate: Enrollment durch die CA-Administration und Bereitstellung auf zentralem Server.
Verfahren für Re-Key Anträge	Das Re-Key erfolgt analog dem Enrollment in Kapitel 4.1.2.
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.3.2.
Annahme eines Re-Key Zertifikats	Die Annahme des Re-Key erfolgt analog dem Vorgehen in Kapitel 4.4.2.
Publikation des Re-Key Zertifikats durch CA	Die Publikation des Re-Key erfolgt analog dem Enrollment in Kapitel 4.4.2.
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.4.2.

4.7.3 Machine CA

Bedingung für Zertifikatserneuerung	Die von der «Stadt Zuerich CA – Machine 2» 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 Benutzer per Auto-Enrollment, SCEP, oder Self-Enrollment.
Verfahren für Re-Key Anträge	Das Re-Key erfolgt analog dem Enrollment in Kapitel 4.1.3.
Benachrichtigung an Nutzer über Ausstellung eines neuen Zertifikats	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.3.3.
Annahme eines Re-Key Zertifikats	Die Annahme des Re-Key erfolgt analog dem Vorgehen in Kapitel 4.4.3.
Publikation des Re-Key Zertifikats durch CA	Die Publikation des Re-Key erfolgt analog dem Enrollment in Kapitel 4.4.3.
Benachrichtigung anderer Stellen durch CA	Die Benachrichtigung des Re-Key erfolgt analog dem Enrollment in Kapitel 4.4.3.

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: – 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 die CA-Administration oder die Fachstelle Informationssicherheit beantragt.
Verfahren für Revokation	– Erreichbarkeit herstellen (CA-Administration und Fachstelle Informationssicherheit). – Der Setup-Prozess der untergeordneten CA erstellt eine Anfrage oder die CA-Administration stellt Request manuell. – Einloggen mit Hilfe des Split-Passwortes durch CA-Administration und Fachstelle Informationssicherheit. Der gesamte Ablauf wird mittels Screendumps dokumentiert. – Revozieren des Zertifikats mittels mmc der CA. – Publikation der CRL.

Frist für Ausstellung von Anträgen	Die Revokation soll umgehend erfolgen.
Frist für Bearbeitung von Anträgen	Die Revokation 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 CRL	Die CRL wird innerhalb eine Tages auf der Website publiziert.
Option zur Online-Überprüfung	Die CRL ist online im AD und auf der Website publiziert.
Anforderungen für die Online-Überprüfung	Die CRL ist online im AD und auf der Website publiziert und kann nach Namen, Typ und Hash durchsucht werden.
Weitere Optionen zur Bekanntgabe von Revokationen	Weitere Zugriffsmöglichkeiten sind vorerst nicht vorgesehen (z. B. OCSP).
Besondere Anforderungen bei kompromittierten Schlüsseln	Erweiterte Anforderungen bestehen nicht.

4.9.2 User CA

Bedingungen für Revokation	Verschiedene Ursachen können zu einer Revokation führen: – Key Compromise der übergeordneten CA. – 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: Benutzer, Personalabteilung. – Applikations-Zertifikate: CA-Administration, Benutzer.
Verfahren für Revokation	– Die CA-Administration revoziert das Zertifikat mittels mmc der CA. – Dokumentation erfolgt in Form von Einträgen im Eventlog. – Publikation der CRL.
Frist für Ausstellung von Anträgen	Die Revokation soll umgehend erfolgen.
Frist für Bearbeitung von Anträgen	Die Revokation soll umgehend erfolgen.
Prüfpflichten	Die Revokation wird in der CRL visuell geprüft.
Häufigkeit der CRL-Ausstellung	– Ausstellung alle 4 Tage. – Overlapping 3 Tage. – Keine Delta CRL.
Maximale Verzögerung für CRL	Die CRL wird umgehend im AD und innerhalb von 30 Minuten auf der Website publiziert.
Option zur Online-Überprüfung	Die CRL ist online im AD und auf der Website publiziert.
Anforderungen für die Online-Überprüfung	Die CRL ist online im AD und auf der Website publiziert und kann nach Namen, Typ und Hash durchsucht werden.
Weitere Optionen zur Bekanntgabe von Revokationen	Weitere Zugriffsmöglichkeiten sind vorerst nicht vorgesehen (z. B. OCSP).
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. – 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 Benutzer oder Administration der betroffenen Machine.
Verfahren für Revokation	– Die CA-Administration revoziert das Zertifikat mittels mmc der CA. – Dokumentation erfolgt in Form von Einträgen im Eventlog. – Publikation der CRL.
Frist für Ausstellung von Anträgen	Die Revokation soll umgehend erfolgen.
Frist für Bearbeitung von Anträgen	Die Revokation soll umgehend erfolgen.
Prüfpflichten	Die Revokation wird in der CRL automatisch geprüft.
Häufigkeit der CRL-Ausstellung	– Ausstellung alle 4 Tage. – Overlapping 3 Tage. – Keine Delta CRL.
Maximale Verzögerung für CRL	Die CRL wird umgehend im AD und innerhalb von 30 Minuten auf der Website publiziert.
Option zur Online-Überprüfung	Die CRL ist online im AD und auf der Website publiziert.
Anforderungen für die Online-Überprüfung	Die CRL ist online im AD und auf der Website publiziert und kann nach Namen, Typ und Hash durchsucht werden.
Weitere Optionen zur Bekanntgabe von Revokationen	Weitere Zugriffsmöglichkeiten sind vorerst nicht vorgesehen (z. B. OCSP).
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 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.
- Abbau und 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-Administration und Fachstelle Informationssicherheit) geschützt auf CD gesichert und bei einem externen Key Escrow Service hinterlegt.

Bei Bedarf kann der Private Key im Vier-Augen-Prinzip durch CA-Administration und Fachstelle Informationssicherheit 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 durch CA-Administration und Fachstelle Informationssicherheit.

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 in einem OIZ RZ und werden dem erhöhten Schutzbedarf entsprechend angemessen geschützt.
Physischer Zugang	Der Zugang zu den Servern ist durch ein restriktives Rollenmodell auf wenige, zertifizierte Personen des RZ-Betriebsteams eingeschränkt. Die CA-Keys sind in HSM abgelegt sowie passwortgeschützt 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	– Die CA-Administration hat nach dem Einloggen die volle Kontrolle über den CA-Server und dessen Applikationen. Die CA-Administration 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. – Die HSM-Administration kann HSM-Partitionen aktivieren und deaktivieren und somit die Verwendung von Private Keys der CA ermöglichen oder unterbinden. – Die Fachstelle Informationssicherheit hat als Auditorin Zugriff zu Logfiles der PKI mit dem Ziel, zu verifizieren, dass die vorliegende CP/CPS eingehalten wird. Sie kann bei der CA-Administration Einsicht auf die CA-Infrastruktur verlangen. Die Fachstelle Informationssicherheit darf nicht gleichzeitig CA-Administration sein.
Anzahl erforderlicher Personen pro Task	Durch den Einsatz von Split-Passwörtern 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 – Zertifikatssignatur – Zertifikatsrevokation – CRL-Signatur – Zertifikatsablauf – Aktionen und Konfigurationsanpassungen auf HSM. (Diese Aufzählung ist nicht abschliessend.)
Häufigkeit der Log-Verarbeitung	Logs werden einmal monatlich durch die CA-Administration ausgewertet.
Archivierungsdauer von Logs	Die Logdateien werden mindestens 6 Monate aufbewahrt.
Schutz der Logs	Logs sind nur der CA-Administration und der Fachstelle Informationssicherheit lesend zugänglich.
Backup von Logs	Logs werden mit dem täglichen Backup ausgelagert.
Log-Erfassung	Die CA und HSM loggen auf den zentralen Loghost.
Benachrichtigung von Log-Verursachern	Der Auslöser eines Log-Eintrags wird nicht benachrichtigt.
Bewertung von Sicherheitslücken	Die Umgebung wird regelmässigen Sicherheitsüberprüfungen unterzogen. Die Auditdaten werden bei der Fachstelle Informationssicherheit gehalten.

5.5 Archivierung

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

5.6 Auswechseln von Schlüsseln

Die entsprechenden Parameter sind im Kapitel 6.3 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 CA 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 sicher 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 der CA-Administration persönlich durch den [RA-ADMIN] übergeben.
Bereitstellung des Public Key an Zertifikatsprüfer	Kann über den städtischen Webserver heruntergeladen werden.
Schlüssellänge	4096 Bits
Hash-Algorithmus	SHA-256
Qualitätsprüfung von Public-Key Parametern	Die Schlüssel werden mit dem «Microsoft Software Key Storage Provider» (FIPS 140-2) erstellt und über den HSM-Key Storage Provider (FIPS 140-2 Level 3) verwendet.
Verwendungszweck der Schlüssel (gemäss X.509 v3 Key Usage Field)	Digitale Signatur, Zertifikatsignatur, Offline Signieren der Zertifikatsperrliste, Signieren der Zertifikatsperrliste (86).

Zertifikatsparameter für Issuing CA:

Name	«Stadt Zuerich - CA – 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
Minimaler Hash-Algorithmus	SHA-256
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 – Root 2»

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.
Schlüssellänge	4096 Bits
Hash-Algorithmus	SHA-256
Qualitätsprüfung von Public-Key Parametern	Die Schlüssel werden mit dem «Microsoft Software Key Storage Provider» (FIPS 140-2) erstellt und über den HSM-Key Storage Provider (FIPS 140-2 Level 3) verwendet.
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 – User 2» – Klasse 1 und 2 Zertifikate

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, wo benötigt
Key Archivierung	Nur Verschlüsselungsschlüssel
Symmetrische Algorithmen im Zertifikat	Nein
Minimale Schlüssellänge	2048 Bits
Hash-Algorithmus	SHA-2
Key Provider	Muss FIPS 140-2 Standard erfüllen
Privater Schlüssel exportierbar	Nein bei Zertifikaten, die direkt durch Benutzer bezogen werden können. Nur im Ausnahmefall möglich bei Zertifikaten, die nur durch die CA-Administration ausgestellt werden können und anschliessend dem Antragssteller zugestellt werden.
Auto-Enrollment	Ja, wo benötigt.

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 - PKI2 - Policy
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.
Schlüssellänge	4096 Bits
Hash-Algorithmus	SHA-256
Qualitätsprüfung von Public-Key Parametern	Die Schlüssel werden mit dem «Microsoft Software Key Storage Provider» (FIPS 140-2) erstellt und über den HSM-Key Storage Provider (FIPS 140-2 Level 3) verwendet.
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 – Machine 2» – Klasse 1 Zertifikate

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 Veröffentlichungspunkte	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
Hash-Algorithmus	SHA-2
Key Provider	Muss FIPS 140-2 Standard erfüllen
Privater Schlüssel exportierbar	Nein bei Zertifikaten, die direkt durch Clients oder Server bezogen werden können. Ja bei Zertifikaten, die nur durch die CA-Administration ausgestellt werden können und anschliessend dem Antragssteller zugestellt werden.
Auto-Enrollment	Ja, wo benötigt.
Speicherort des privaten Schlüssels	Keystore abhängig vom Client, Server, sonstigen Device.
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: – Clientauthentifizierung – Serverauthentifizierung
Issuance Policy	Stadt Zuerich - PKI2 - Policy
Key Usage	Je nach Vorlage/Verwendungszweck: – Digital Signature – Encryption
Critical Attributes	Nur Basic Constraints

6.2 Schutz der Private Keys / Hardware Security Module

Verschlüsselungsmodule	Es kommt ein Hardware-Verschlüsselungsmodul HSM zum Einsatz, auf welchem der Private Key und das zugehörige Zertifikat der CA gespeichert sind.
Multi-Personen Kontrolle	Zugriffe auf das HSM erfolgen mittels unterschiedlicher Hardware-Token von Fachstelle Informationssicherheit und CA-Administration, abhängig von der jeweils benötigten Berechtigung.
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 CA-Administration und Fachstelle Informationssicherheit verwaltet. CA-Administration und Fachstelle Informationssicherheit dienen mittels Split-Passwort-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 CA ist in einer eigenen HSM-Partition abgelegt.
Verfahren zur Aktivierung des Private Key	Vor jeder Verwendung des CA-Private Keys muss die HSM-Partition per Token der CA-Administration 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 Andere Aspekte der Schlüsselpaarverwaltung

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.	
Nutzungsdauer von Zertifikaten und Schlüsselpaaren	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

6.4 Aktivierungsdaten

Für den Betrieb des HSM sind mehrere Hardware-Tokens erforderlich. Diese sind auf die Rollen HSM-Administration, CA-Administration und Fachstelle Informationssicherheit aufgeteilt. Jede HSM-Partition ist zusätzlich mit einem sicheren Passwort geschützt.

6.5 Sicherheitsmassnahmen für die CA

Root CA	– Windows Server mit den aktuellen Rollups 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
User CA	– Windows Server mit den aktuellen Rollups und Security Updates – Active Directory integriert – Sie schützt sich gegen andere Geräte durch eine Firewall – Bitlocker-Verschlüsselung – Aktueller Virenscanner
Machine CA	– Windows Server mit den aktuellen Rollups und Security Updates – Active Directory integriert – Sie schützt sich gegen andere Geräte durch eine Firewall – Bitlocker-Verschlüsselung – Aktueller Virenscanner

6.6 Technische Kontrollen zum Lebenszyklus

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

6.7 Sicherheitskontrollen des Netzwerks

Die Netzwerksicherheit wird durch den Einsatz von Firewalls gewährleistet.

6.8 Zeitsynchronisation und Zeitstempel

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

In der Stadt steht kein Zeitstempeldienst zur Verfügung; bei Bedarf werden externe Zeitstempeldienste eingesetzt, um qualifizierte Zeitstempel zu generieren.

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 CA 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-2) des Public Keys der jeweils ausstellenden CA.
– Subject Key Identifier	Besteht aus dem Hash (SHA-2) 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 CA 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 CA 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 (SHA-2) der ausstellenden CA.
Reason Code	Generiert durch die CA. Erfasst durch die CA-Administration. 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 CA werden technisch und organisatorisch gemäss den Vorgaben aus Kap. 8.4 geprüft.

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

Die Fachstelle Informationssicherheit 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.
- Die CA-Administration 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 Durch die Beurteilung abgedeckte Themen

Die Fachstelle Informationssicherheit macht einen Vorschlag für die zu überprüfenden Themen. Bei ausgewiesenem Bedarf werden die Themen durch die OIZ-Geschäftsleitung verabschiedet.

8.5 Massnahmen nach festgestellten Mängeln

Auditresultate werden wie folgt behandelt:

- Die aufgezeigten Mängel werden durch die Fachstelle Informationssicherheit 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 die Fachstelle Informationssicherheit koordiniert.

8.6 Mitteilung der Resultate

Die Resultate des Audits werden der OIZ-Geschäftsleitung mitgeteilt.

9 Weitere geschäftliche/rechtliche Bestimmungen

9.1 Gebühren

Alle für die städtische PKI anfallenden Kosten werden durch die OIZ als Teil der Stadtverwaltung Zürich getragen. Sie sind für die partizipierenden Dienstabteilungen und Angestellten der Stadt Zürich in den jeweiligen Service Produkten der OIZ enthalten.

Für Dritte richten sich die Kosten nach separat zu vereinbarenden Verträgen.

9.2 Finanzielle Verantwortung

9.2.1 Versicherungen

Es gelten die Versicherungen der Stadt Zürich.

Das Inventar der OIZ ist angemeldet und versichert.

9.2.2 Versicherungen oder Garantien für Nutzer

Für allfällige Schäden, die infolge elektronisch unterschriebener Dokumente entstehen, sind die Benutzenden alleine verantwortlich.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Umfang vertraulicher Informationen

Folgende Geschäftsinformationen sind vertraulich klassifiziert und sind entsprechend zu behandeln:

- Alle Daten der Benutzenden von Zertifikaten, die den Bestimmungen dieser CP/CPS-Richtlinie unterliegen und die nicht aus den Zertifikaten selbst ersichtlich sind.
- Logs, die durch die Stadt Zürich im Rahmen der Nutzung der Zertifikate resp. der PKI-Infrastruktur generiert und gespeichert werden.
- Audit-Berichte und andere Resultate von Sicherheitsüberprüfungen.

9.3.2 Nicht vertrauliche Informationen

Folgende Informationen gelten ausdrücklich als nicht vertraulich:

- Daten von Benutzenden, die in den Zertifikaten selbst ersichtlich sind.
- Alle Dokumente und sonstigen Informationen, die im Zusammenhang mit der PKI publiziert werden und sich an interessierte Personen richten (z. B. vorliegende Richtlinie CP/CPS, CA-Zertifikate, Zertifikatssperrlisten).

9.3.3 Verantwortlichkeiten für den Schutz vertraulicher Informationen

Die Stadt Zürich sowie ihre Mitarbeitenden sind verantwortlich für die Einhaltung dieser Geheimhaltungspflichten (vgl. dazu auch die relevanten Bestimmungen des Personalrechts der Stadt Zürich sowie das Handbuch Informationssicherheit der Stadt Zürich).

9.4 Vertraulichkeit von Personendaten

Die Stadt Zürich hält die bestehenden Datenschutz- und Informationssicherheitsvorgaben ein, insbesondere

- das Gesetz über die Information und den Datenschutz (IDG) des Kantons Zürich
- die Verordnung über die Information und den Datenschutz (IDV) des Kantons Zürich
- die Datenschutzverordnung (DSV) der Stadt Zürich und
- das Handbuch Informationssicherheit der Stadt Zürich.

Die Stadt Zürich verpflichtet sich insbesondere, personenbezogene Daten nur soweit zu bearbeiten, als dies für die Zertifikatsausstellung notwendig ist. Personenbezogene Daten werden auf keine Falle für Werbe- und/oder Marketingzwecke verwendet.

9.5 Immaterialgüterrechte

Alle Immaterialgüterrechte an den folgenden Dokumenten und Informationen stehen ausschliesslich der Stadt Zürich zu:

- Vorliegende CP/CPS-Richtlinie in der jeweils gültigen Version
- Richtlinien zur Registrierung von Zertifikatantragstellern bei der Stadt Zürich in der jeweils geltenden Version
- Verträge und andere Vereinbarungen zwischen der Stadt Zürich und ihren Kundinnen (intern oder extern)
- Von der Stadt Zürich herausgegebene digitale Zertifikate.

Vervielfältigung und Präsentation (inklusive insbesondere Publikation, Verteilung und Verwertung) dieser Unterlagen ohne schriftliche Zustimmung der Stadt Zürich, Organisation und Informatik, ist untersagt.

An den von der Stadt Zürich herausgegebenen Zertifikaten erwerben die Nutzenden keinerlei Eigentumsrechte, sondern vielmehr nur ein Recht auf Nutzung der Zertifikate.

9.6 Zusicherungen und Gewährleistungen

9.6.1 Zusicherungen und Gewährleistungen der CA

Die Stadt Zürich sichert zu, die Verwaltung von digitalen Zertifikaten unter Einhaltung der gesetzlichen Vorgaben und in Übereinstimmung mit der vorliegenden Richtlinie zu tätigen.

Die städtischen CA werden ferner durch die OIZ im Auftrag der Stadt Zürich nach dem aktuellen Standard mit dem Ziel einer angemessenen Sicherheit implementiert. Angemessen bedeutet, dass ausgestellte Zertifikate in der Regel durch das Windows-Passwort geschützt sind. Hardware Security Module für die Speicherung von privaten Schlüsseln werden nur in wenigen ausgewiesenen Fällen verwendet.

Die ausgestellten Zertifikate sind nur dann geeignet für starke Authentisierung, wenn die Aufbewahrung des privaten Schlüssels sicher ist und dieser nicht exportiert werden kann. In jedem Fall muss ein solcher Einsatz durch die Fachstelle Informationssicherheit bewilligt werden.

9.6.2 Zusicherungen und Gewährleistungen der RA

Die Registrierungsstelle verpflichtet sich zum sorgfältigen Umgang beim Identifizieren und Registrieren von Personen, die neue Zertifikate beantragen.

9.6.3 Zusicherungen und Gewährleistungen der Zertifikatsinhaber

Die Zertifikatsinhaber verpflichten sich, die für sie ausgestellten Zertifikate samt zugehörigen privaten Schlüsseln gemäss den geltenden Richtlinien und gemäss dem jeweiligen Verwendungszweck zu beschaffen, zu nutzen und zu unterhalten.

9.6.4 Zusicherungen und Gewährleistungen der Zertifikatsnutzer

Die Zertifikatsnutzer verpflichten sich, Zertifikate nur gemäss dem vorgesehenen Verwendungszweck zu nutzen oder zu verifizieren.

9.6.5 Zusicherungen und Gewährleistungen anderer Beteiligter

Keine Bestimmungen.

9.7 Gewährleistungsausschluss

Abgesehen von den im vorstehenden Kapitel 9.6 festgehaltenen Zusicherungen und Gewährleistungen wird jegliche weitere Gewährleistung der in Kapitel 9.6 aufgeführten Parteien wegbedungen.

9.8 Haftung

9.8.1 Haftungsbegrenzung

Die OIZ haftet im Rahmen der gesetzlichen Bestimmungen gegenüber Dritten. Soweit gesetzlich möglich, schliesst die OIZ jede Haftung aus, insbesondere übernimmt die OIZ keine Haftung für:

- Schäden, die aus einer Benutzung der Zertifikate und/oder der Schlüsselpaare, die sich im Widerspruch zur vorliegenden CP/CPS, weitergehender Vorgaben der Stadt Zürich im PKI-Umfeld und/oder der Vorgaben in den Zertifikaten befinden, resultieren
- Schäden aufgrund von höherer Gewalt
- Schäden, die durch Malware auf der Infrastruktur der Benutzungen entstehen (Viren, Trojaner, etc.)

Für alle anderen Schäden, die durch die Benutzung der Zertifikate entstehen, ist die Haftung soweit gesetzlich möglich beschränkt auf:

- Im Falle der leichten Fahrlässigkeit: auf die Höhe der Gebühren, die ein Benutzer pro Jahr für die Zertifikatsservices der Stadt Zürich entrichtet, maximal jedoch CHF 50'000 pro Fall und pro Jahr.

9.8.2 Haftung LRA

Die Personalabteilungen der Departemente und Dienstabteilungen als lokale Registrierungsstellen haften für die korrekte Identifizierung und Registrierung der Antragsteller für persönliche Zertifikate.

9.8.3 Haftung der Benutzenden

Die Haftung der Benutzenden (insbesondere Mitarbeitende der Stadt Zürich oder Dritte) richten sich nach den anwendbaren gesetzlichen Bestimmungen. Insbe-

sondere sind die Benutzenden haftbar für Schäden, die aufgrund der Missachtung der gebührenden Sorgfalt durch den Benutzenden entstehen (z. B. durch Herausgabe des Passworts zur Nutzung des Zertifikats durch Dritte, Nichtmeldung von kompromittierten Zertifikaten, u.dgl.)

9.9 Weitergehende Entschädigungen

Die Entschädigungen sind abschliessend in Kapitel 9.6 bis 9.8 festgehalten. Weitergehende Entschädigungen sind, soweit gesetzlich möglich, wegbedungen.

9.10 Inkrafttreten und Beendigung

Die CP/CPS tritt am 14. Februar 2017 in Kraft.

Die CP/CPS ist solange gültig, bis sie durch eine neue Version ersetzt wird oder die Stadt Zürich ihre Tätigkeit als Herausgeberin von Zertifikaten beendet.

Die Bestimmungen bezüglich Datenschutz, Geheimhaltung und Archivierung bleiben auch nach Beendigung weiterhin gültig.

9.11 Einzelbenachrichtigungen und Mitteilungen an Teilnehmer

Die OIZ kommuniziert mit den städtischen Bezügerinnen und Bezügern der städtischen PKI (vgl. Kap. 9.16) grundsätzlich via E-Mail oder via Intranet.

Allfällige Mitteilungen an Dritte (vgl. dazu ebenfalls Kap. 9.16) erfolgen ebenfalls via E-Mail, falls notwendig auch via Briefpost.

Vereinbarung und Verträge sowie jede Änderung solcher Dokumente unterliegen der Schriftform.

9.12 Änderungen

Anpassungen an der vorliegenden CP/CPS werden durch die zuständigen Stellen der Stadt Zürich (OIZ – Fachstelle Informationssicherheit) durchgeführt und erfolgen ohne vorherige Ankündigung. Mit der Publikation auf der Website gemäss Kapitel 2 tritt die neue Regelung in Kraft. Die Details der Anpassungen werden dabei nicht mitgeteilt.

Wesentliche Änderungen werden unter einer Anzeigefrist von 30 Tagen vor Inkrafttreten der Änderung auf dem Intranet publiziert. Anpassungen am Ablageort werden fallbezogen durch die zuständigen Stellen der Stadt Zürich (OIZ – Fachstelle Informationssicherheit) bestimmt. Der neue Ort wird im Intranet bei den News publiziert.

Sind Dritte an der CP/CPS beteiligt, richtet sich das Vorgehen hinsichtlich Änderungen nach den Bestimmungen in den Verträgen mit den Dritten.

9.13 Beilegung von Streitigkeiten

Entstehen zwischen den an dieser CP/CPS beteiligten städtischen Stellen (vgl. dazu Kap. 9.16) Unstimmigkeiten bezüglich der Leistungserbringung und/oder der Einhaltung der Verpflichtungen, wird versucht, diese in einem Gespräch allenfalls unter Einbezug einer dritten, sachverständigen Partei gütlich beizulegen. In Fällen, in denen keine Einigung der städtischen Stellen erzielt werden kann, suchen die entsprechenden Departementsvorstehenden der Stadt Zürich eine Lösung und entscheiden abschliessend.

Wenn Dritte (vgl. Kap. 9.16) an dieser CP/CPS beteiligt sind, sind die Parteien bestrebt, Streitigkeiten möglichst einvernehmlich zu lösen und sehen dafür ein einfaches und rasches Eskalationsverfahren vor. Ansonsten gilt Kap. 9.14.

9.14 Anwendbares Recht und Gerichtsstand

Anwendbar ist schweizerisches Recht. Gerichtsstand ist Zürich.

9.15 Einhaltung geltenden Rechts

Die Stadt Zürich hält die relevante schweizerische Gesetzgebung im Bereich elektronischer Signaturen ein, insbesondere das Bundesgesetz und die Verordnung über die elektronische Signatur (ZertES, VZertES) – soweit diese anwendbar sind – , sowie die relevanten datenschutzrechtlichen Bestimmungen, insbesondere das Gesetz über die Information und den Datenschutz (IDG) mit der dazugehörenden Verordnung (IDV) des Kantons Zürich. Ferner verpflichtet sich die Stadt Zürich, die gesetzlichen Export- und Importvorschriften einzuhalten.

9.16 Sonstige Bestimmungen

Die OIZ erbringt ihre Leistungen gegenüber der Stadt Zürich (Departemente und Dienstabteilungen, angeschlossene Stellen und Unternehmungen, die zu mindestens 50% im Besitz der Stadt Zürich sind resp. das von diesen Einheiten angestellte Personal).

Beteiligen sich Dritte an dieser CP/CPS, werden allfällig notwendige weitere Bestimmungen in den Verträgen mit den Dritten festgelegt.

9.17 Weitere Bestimmungen

Rechtsverbindlich ist die deutsche Version dieser CP/CPS. Allfällige Versionen in anderen Sprachen dienen rein informativen Zwecken.