Kanton Zug

Finanzdirektion
Amt für Informatik und Organisation (AIO)

Zertifizierungsrichtlinien
Certification Practice Statement (CPS)

Kanton Zug Interne AIO PKI

Impressum

Walter Utzinger
CA Verantwortlicher

Rudolf Gisler
IT-SIBE

Aabachstrasse 1, 6300 Zug
T +41 41 728 51 00, F +41 41 728 51 09
www.zg.ch/finanzen

Inhalt

1. Einführung

1.1. Überblick

Das vorliegende Dokument beschreibt die Zertifikatstypen und die Zertifizierungsrichtlinien (CPS) der internen Zertifizierungsstelle (AIO PKI) des Kantons Zug. Die Zertifizierungsrichtlinien enthalten ein Regelwerk, das den Einsatzbereich von Zertifikaten für eine bestimmte Benutzergruppe und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen definiert. Die vorliegenden Zertifizierungsrichtlinien gelten für Zertifikate für Dienstleistungen wie sie im Kapitel 1.2 beschrieben werden und richten sich an die Teilnehmer dieser Dienste, also ausschliesslich an die Verwaltung des Kanton Zug und seinen Gemeinden.

1.2. Anwendungsbereich

Diese Zertifizierungsrichtlinien gelten ausschliesslich für Zertifikate, welche von der „AIO Internal Root CA Kanton Zug - G2“ für die sichere Client- und Server- Authentifizierung im Zusammenhang mit den Dienstleistungen des AIO ausgestellt werden.

- User Authentisierung
- Computer Authentisierung
- SSL Server Authentisierung
- Web Applikationen - Services
- Remote Gateways

Die „AIO Internal Root CA Kanton Zug - G2“ ist keine öffentliche CA. Die Teilnehmerzertifikate können nicht für verbindliche elektronische Signaturen (gemäss Signaturgesetz) verwendet werden.

1.3. Sprachregelung

In diesem Dokument werden die Ausdrücke "Teilnehmer" bzw. "Schlüsselinhaber" für Systeme und Mitarbeitende der kantonalen Verwaltung resp. des Kantons Zug mit seinen Einwohnergemeinden verwendet. Der Ausdruck "Aussteller" bezeichnet die juristische Person des CA Betreibers, also das Amt für Informatik und Organisation des Kantons Zug (AIO).

1.4. Abkürzungen

In diesem Dokument werden folgende Abkürzungen verwendet:

CA Certification Authority (Zertifizierungsstelle)
CPS Certificate Practice Statement (Zertifizierungsrichtlinien)
CRL Certificate Revocation List (Sperrliste)
DN Distinguished Name (Name des Zertifikatinhabers (Subject DN) bzw. des Zertifikatausgebers (Issuer DN))
ID Identifikation
PKI Public Key Infrastruktur
RDN Relative Distinguished Name (O=Organisation, OU=Organisational Unit, L=Locality, ST=State or Province, CN= Common Name, C=Country)

2. AIO Zertifikate

2.1. Zertifikatshierarchie

Die Zertifikatshierarchie besteht aus der self-signed AIO Internal Root CA Kanton Zug - G2, welche die AIO Issuing CA - G2 subordiniert hat.
Die AIO Issuing CA - G2 ist für das manuelle Ausrollen von Client- und Server Authentisierungszertifikaten und System Zertifikaten mit der Registration Authority und das automatische Ausrollen von User Zertifikaten, an Windows Domänen Clients resp. Servers zuständig.

2.2. Zertifikatstypen

Alle Details der Zertifikatstypen sind im Dokument „CA-& Zertifikatsspezifikation“ beschrieben.

2.2.1. Allgemeine Informationen

Alle von der AIO Internal Root CA Kanton Zug - G2 ausgestellten Zertifikate basieren auf dem X.509v3 Standard. Es werden ausschliesslich Zertifikate für 2048/4096 Bit RSA Schlüssel mit öffentlichem Exponent 65537 und SHA-256 als Hash-Algorithmus ausgestellt.

2.2.2. AIO Internal Root CA Kanton Zug - G2 Zertifikat

Das AIO Internal Root CA Kanton Zug - G2 Zertifikat ist mit dem korrespondierenden privaten Schlüssel signiert (self-signed). Die Überprüfung des CA Zertifikats erfolgt durch Vergleich des Hash-Wertes (Fingerprint) des Zertifikats mit dem offiziell vom AIO publizierten Wert. Die Schlüssellänge des CA Zertifikats beträgt 4096 Bit.

Namensgebung

Das AIO Internal Root CA Kanton Zug - G2 Zertifikat hat folgenden Subject- und Issuer DN:

Aussteller	Beschreibung
CN	AIO Internal Root CA Kanton Zug - G2

Verwendungszweck

Der CA Schlüssel wird für das Ausstellen von Issuing CA Zertifikaten und das Ausstellen von Sperrlisten (CRL) verwendet.

Gültigkeitsperiode

Die Gültigkeitsperiode des AIO Internal Root CA Kanton Zug - G2-Zertifikats beträgt 24 Jahre. Das CA Zertifikat ist gültig vom Mittwoch, 11. November 2015 11:05:20 bis Freitag, 11. November 2039 11:15:16

Fingerabdruck

Hash-Algorithmus	Fingerprint
SHA-1	0d 35 5e 56 1e b3 ad 5a 11 55 2b a4 3c 4c bd 9c b8 42 4a 6c

Erweiterungen

Name	Wert
Basic Constraints	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=2
Key Usage	Digitale Signatur, Zertifikatsignatur, Offline Signieren der Zertifikatsperrliste, Signieren der Zertifikatsperrliste (86)
Subject Key Identifier	43 a3 f0 ea a5 47 38 cb 79 cf 9d 3f 37 a1 87 84 d4 e7 2b 74

2.2.3. AIO Issuing CA - G2 Zertifikat

Das AIO Issuing CA - G2 Zertifikat ist mit dem korrespondierenden privaten Schlüssel der AIO Internal Root CA Kanton Zug - G2 signiert (subordiniert). Die Überprüfung des AIO Issuing CA - G2 Zertifikats erfolgt durch die Überprüfung der Zertifikatssignatur mittels des Zertifikats der AIO Internal Root CA Kanton Zug - G2. Die Schlüssellänge des CA Zertifikats beträgt 4096 Bit.

Namensgebung

Das AIO Issuing CA - G2 Zertifikat hat folgenden Subject- und Issuer DN:

Aussteller	Beschreibung
CN	AIO Issuing CA - G3
DC	msworld
DC	zg
DC	ch

Verwendungszweck

Der CA Schlüssel wird für das Ausstellen von verschiedenen Client- und Server-Authentisierungszertifikaten, sowie für das Ausstellen von Sperrlisten (CRL) verwendet.

Gültigkeitsperiode

Die Gültigkeitsperiode des AIO Issuing CA - G2-Zertifikats beträgt 8 Jahre. Das CA Zertifikat ist gültig vom Mittwoch, 11. November 2015 11:08:25 bis Samstag, 11. November 2023 11:18:25.

Fingerabdruck

Hash-Algorithmus	Fingerprint
SHA-1	d6 db 4c b4 9c 27 a7 fa a4 09 c7 b1 df fe 90 98 a6 cf 04 99

Erweiterungen

Name	Wert
Basic Constraints	Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=1
Key Usage	Digitale Signatur, Zertifikatsignatur,

	Offline Signieren der Zertifikatsperrliste, Signieren der Zertifikatsperrliste (86)
Subject Key Identifier	d3 dc 77 f6 64 20 c3 46 77 da 9a 73 86 d4 b9 a9 e9 ea f6 6c

2.2.4. End-Entity Zertifikatsmatrix

Dieser Abschnitt zeigt, welche Zertifikatstypen der AIO Issuing CA - G2 für die verschiedenen Dienstleistungen zum Einsatz kommen.

Die nachfolgende Tabelle stellt eine Übersicht der End-Entity Zertifikate dar, welche von der AIO Issuing CA - G2 ausgestellt werden.

End-Entity Zertifikate AIO Issuing CA - G2

#	Zertifikatsname	Key	Enrollment	Gültigkeit	Reenroll
1	AIO Web Server CS ext 2Y	2048 Bit	Manuell	2 Jahre	6 Wochen
2	AIO Code Signing	2048 Bit	Manuell	4 Jahre	6 Wochen
3	RDP Auth	2048 Bit	Automatisch via AD	2 Jahre	6 Wochen
4	AIO User - G2 (scep)	2048 Bit	Automatisch via AD	1 Jahre	6 Wochen
5	AIO host TPM_W10	2048 Bit	Automatisch via Policy	2 Jahre	8 Wochen

3. AIO PKI Infrastruktur

3.1. Betreiber

Der Betreiber der AIO PKI ist das Amt für Informatik und Organisation (AIO), Postfach, 6301 Zug.

3.1.1. Generierung

Die Erzeugung aller CA Schlüsselpaare der AIO PKI wurde in einer gesicherten Umgebung durchgeführt. Der Prozess der Schlüsselgenerierung garantiert, dass der private Schlüssel der CA nur auf dem dafür vorgesehenen System gespeichert ist.
Die CA Schlüsselpaare wurden zweifach zur Sicherheit (Backup) auf Hardware Token (verschlüsselte USB-Sticks) gespeichert. Die Hardware Token sind über Zugriffcodes geschützt und in Sicherheitstresoren abgelegt.

3.1.2. Verteilung des öffentlichen Schlüssels

Alle manuell ausgestellten Zertifikate werden dem Zertifikats-Antragssteller per E-Mail oder Help-Line Antrag zugesandt. Alle automatisiert ausgestellten Zertifikate werden dem Zertifikats-Antragssteller über den in Microsoft Windows enthaltenen, automatisierten Ausroll-Prozess übermittelt.

3.1.3. Einstellung der Tätigkeit

Das AIO informiert alle Teilnehmer, falls eine Einstellung der AIO PKI vorgesehen ist.

3.1.4. Aufbewahrungspflicht

Das AIO verpflichtet sich, die Teilnehmerdaten und Zertifikat mit den entsprechenden Statusinformationen der Teilnehmer für eine bestimmte Zeitdauer aufzubewahren:

3.2. Sicherheit

3.2.1. Systemsicherheit

Alle CA-Instanzen der AIO PKI werden auf einem dedizierten virtuellen System betrieben. Der Zugang zu den CA Systemen unterliegt physischen Zugangskontrollen.

3.2.2. Personelle Sicherheit

Der Zugriff auf die Systeme der AIO PKI ist auf einen festgelegten Personenkreis beschränkt. Alle kritischen Operationen werden ausschliesslich im Vieraugenprinzip durchgeführt.

3.3. Auditing

Die AIO PKI unterliegt einem periodischen Audit durch den IT-SIBE des AIO.

4. Zertifizierungsrichtlinien

4.1. Registrierung der Teilnehmer

Die Registrierung der Teilnehmer erfolgt gemäss geltendem Vertragsrecht der entsprechenden Dienstleistung gemäss Kapitel 1.2.

4.2. Generierung der Teilnehmerschlüssel

4.2.1. Authentisierungs- und Signatur Zertifikat

Die RSA Schlüsselpaare werden im AIO erzeugt. Der Prozess der Schlüsselgenerierung für die Authentisierungs- und Signaturzertifikate garantiert, dass der private Schlüssel nur auf Systemen der kantonalen Verwaltung gespeichert ist.

4.3. Zertifikatsantrag

Für jedes vom AIO verwalteten System, welches sich innerhalb der IT Infrastruktur des Kantons Zug befindet, kann ein Antrag auf ein Teilnehmerzertifikat gestellt werden. Die Prüfung des Antrags erfolgt durch das AIO. Es liegt in der Verantwortung des AIO, ein Teilnehmerzertifikat gemäss Antrag auszustellen oder den Antrag abzuweisen.

4.4. Verteilung der Schlüssel und Zertifikate

System-Zertifikate der AIO Issuing CA - G2 werden mittels der Registration-Authority Webapplikation oder Microsoft Autoenrollment ausgegeben.

4.4.1. Registration Authority Webapplikation

Alle Zertifikatsanträge werden im HelpLine Ticketing System des AIO erfasst und werden dann von einem RA-Agent geprüft. Der RA-Agent analysiert den Antrag und kann diesen dann durchführen oder abweisen. Manuell ausgestellte Zertifikate werden per E-Mail dem Zertifikatsantragssteller übermittelt. Bei manuell ausgestellten PKCS#12 Dateien werden die Datei und das dazugehörige Passwort auf separatem Weg per E-Mail bzw. SMS dem Zertifikatsantragssteller übermittelt.

4.4.2. Microsoft Autoenrollment

Zertifikate für Systeme welche sich im Active Directory des AIO in der Domäne Msworld.zg.ch befinden werden mit dem Autoenrollment Mechanismus von Microsoft ausgestellt.

4.5. Verpflichtungen der Teilnehmer

4.5.1. Verwendungszweck der Teilnehmerzertifikate

Die Teilnehmerzertifikate sind ausschliesslich für die Dienstleistungen gemäss Kapitel 1.2 und den vertraglich vereinbarten Bedingungen einzusetzen. Der alleinige Verwendungszweck ist die Client- und Server- Authentisierung für die Dienstleistungen gemäss Kapitel 1.2.
Die AIO Internal Root CA Kanton Zug - G2 ist keine öffentliche CA. Die Teilnehmerzertifikate können nicht für verbindliche elektronische Signaturen (gemäss Signaturgesetz) verwendet werden.

4.5.2. Verpflichtungen der Schlüsselinhaber

Der Schlüsselinhaber ist für die Sicherheit der privaten Schlüsselkomponenten in seinem Besitz verantwortlich. Um die Sicherheit zu gewährleisten, hat der Schlüsselinhaber insbesondere folgendes zu beachten:

- Den privaten Schlüssel ausschliesslich für den vorgegebenen Verwendungszweck gemäss Kapitel 1.2 einzusetzen
- Bei Kompromittierung des Schlüssels oder Verlust des Zertifikats unverzüglich sperren zu lassen

4.6. Sperren von Zertifikaten

Die AIO PKI bietet die Möglichkeit, Zertifikate unwiderruflich zu sperren (revozieren). Die Sperrung ist eine irreversible, vorzeitige Beendigung der Gültigkeit eines Zertifikats. Gesperrte Zertifikate können nicht mehr für die Dienstleistungen gemäss Kapitel 1.2 verwendet werden. Sowohl die Teilnehmer wie auch der Aussteller kann eine Sperrung der Zertifikate veranlassen.

4.6.1. Teilnehmerseitige Gründe für eine Sperrung

Jeder Teilnehmer muss eine Sperrung seines Teilnehmerzertifikates beantragen bei

- begründetem Verdacht, dass der Teilnehmerschlüssel kompromittiert wurde
- Diebstahl oder Verlust des Zertifikats / PKCS12 Datei
- Vertragsauflösung

4.6.2. Austellerseitige Gründe für eine Sperrung

Das AIO hat das Recht, Teilnehmerzertifikate ohne spezifischen Antrag des Teilnehmers unter folgenden Voraussetzungen zu sperren:

- begründeter Verdacht, dass der Teilnehmerschlüssel kompromittiert wurde:
- Missbrauch der Systeme des AIO und/oder Dienstleistungen gemäss Kapitel 1.2 durch den Teilnehmer
- Einstellung des PKI Betriebs

4.6.3. Sperrlisten (CRL)

Die von den CAs der AIO PKI ausgestellten Sperrlisten basieren auf dem X.509 v2 Standard. Es werden keine "per-certificate" Extensions (z. B. Reason Codes) unterstützt. Als "per-CRL" Extension erscheint eine fortlaufend aufsteigende Seriennummer in der Sperrliste.
Die von den CAs der AIO PKI ausgestellten Sperrlisten werden intern verfügbar gemacht. Die Sperrlisten werden von den Systemen der AIO zur Überprüfung der Gültigkeit von Zertifikaten eingesetzt.

4.7. Haftung

Es wird jede Haftung abgelehnt, falls die Teilnehmerzertifikate für andere als die im Kapitel 1.2 definierten Zwecke verwendet werden.

4.8. Änderungen der Richtlinien

Die AIOs behält sich das Recht vor, diese Zertifizierungsrichtlinien ohne Vorankündigung zu ändern.