keyon

Microsoft CERTIFIED Partner

MIGROS

# Zertifizierungsrichtlinien

## Certification Practice Statement (CPS)

# Migros Corporate PKI
# NG-PKI 2014
# Interne CA Hierarchie

keyon AG
Schlüsselstrasse 6
8645 Jona
Switzerland

Tel +41 55 220 64 00
Fax +41 55 220 64 01

www.keyon.ch
info@keyon.ch

keyon

Microsoft CERTIFIED Partner

# Änderungsnachweis

| Version | Autor | Datum | Kommentar |
|---|---|---|---|
| 1.0 | Keyon AG | 27.06.2014 | Initialversion nach Implementierung NG-PKI 2014 |

keyon

Microsoft CERTIFIED Partner

# Inhaltsverzeichnis

keyon

Microsoft CERTIFIED Partner

# 1 Einführung

## 1.1 Überblick

Das vorliegende Dokument beschreibt die Zertifikatstypen und die Zertifizierungsrichtlinien (CPS) der internen Zertifizierungsstelle (Migros Corporate PKI) der Migros.

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 Migros.

## 1.2 Anwendungsbereich

Diese Zertifizierungsrichtlinien gelten ausschliesslich für Zertifikate, welche von der „Migros Root CA 2“ für die sichere Client- und Server- Authentifizierung im Zusammenhang mit den Dienstleistungen der Migros ausgestellt werden.

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

**Die „Migros Root CA 2“ 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 Migros resp. die Migros selbst verwendet.

Der Ausdruck "Aussteller" bezeichnet die juristische Person des CA Betreibers, also des Migros-Genossenschafts-Bund (MGB).

## 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

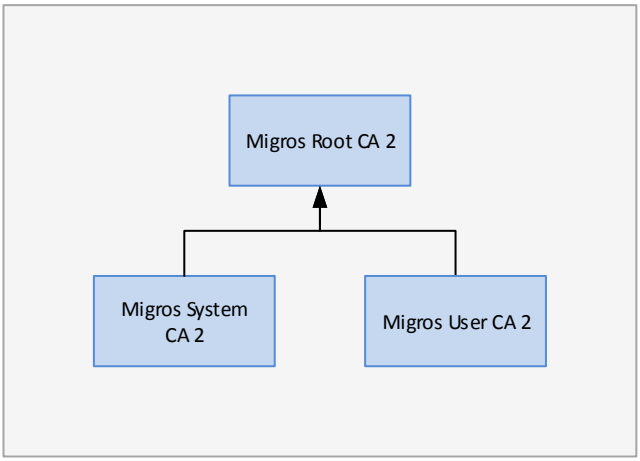
**RDN** Relative Distinguished Name (O=Organisation, OU=Organisational Unit, L=Locality, ST=State or Province, CN= Common Name, C=Country)

# 2 Migros Corporate PKI Zertifikate

## 2.1 Zertifikatshierarchie

Die Zertifikatshierarchie besteht aus der self-signed Migros Corporate PKI, welche die Migros System CA 2 und Migros User CA 2 subordiniert hat.

Die Migros System CA 2 und Migros User CA 2 sind 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 „MGB NG-PKI - Zertifikatsspezifikation“ der Migros beschrieben.

### 2.2.1 Allgemeine Informationen

Alle von der Migros Root CA 2 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 Migros Root CA 2 Zertifikat

Das Migros Root CA 2 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 von dem Migros publizierten Wert. Die Schlüssellänge des CA Zertifikats beträgt 4096 Bit.

#### Namensgebung

Das Migros Root CA 2 Zertifikat hat folgenden Subject- und Issuer DN:

| RDN | Beschreibung |
|---|---|
| CN | Migros Root CA 2 |
| O | Migros |
| C | CH |

#### Verwendungszweck

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

#### Gültigkeitsperiode

Die Gültigkeitsperiode des Migros Root CA 2-Zertifikats beträgt 20 Jahre. Das CA Zertifikat ist gültig vom Dienstag, 4. März 2014 10:10:52 bis Samstag, 4. März 2034 10:20:46.

#### Fingerprint

| Hash-Algorithmus | Fingerprint |
|---|---|
| SHA-1 | 8a 65 11 34 8a f1 c4 5b e6 30 fc 6e cf 0c c1 10 31 6a ef 68 |

#### Erweiterungen

| Name | Wert |
|---|---|
| Basic Constraints | – CA: true<br>– Path Length: none |
| Key Usage | – Certificate Signing<br>– CRL Signing<br>– Digital Signature |
| Subject Key Identifier | 9d ad 91 ba 91 ab 0e 7e 86 d2 e1 1a f9 99 67 00 4c 8b eb b8 |
| Policy ID | 1.3.6.1.4.1.4948.11.3.1 |

### 2.2.3 Migros System CA 2 Zertifikat

Das Migros System CA 2 und Migros User CA 2 Zertifikat ist mit dem korrespondierenden privaten Schlüssel der Migros Root CA 2 signiert (subordiniert). Die Überprüfung des Migros System CA 2 Zertifikats erfolgt durch die Überprüfung der Zertifikatssignatur mittels des Zertifikats der Migros Root CA 2. Die Schlüssellänge des CA Zertifikats beträgt 4096 Bit.

#### Namensgebung

Das Migros System CA 2 Zertifikat hat folgenden Subject-DN:

| RDN | Beschreibung |
|---|---|
| CN | Migros System CA 2 |
| O | Migros |
| C | 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 Migros System CA 2 Zertifikats beträgt 20 Jahre. Das CA Zertifikat ist gültig vom Dienstag, 4. März 2014 11:11:35 bis Montag, 27. Februar 2034 11:11:35

#### Fingerprint

| Hash-Algorithmus | Fingerprint |
|---|---|
| SHA-1 | 26 82 3a 96 df 31 c6 a0 f1 a9 66 ad 0e 3a 67 1f 3d 41 bd 70 |

#### Erweiterungen

| Name | Wert |
|---|---|
| Basic Constraints | – CA: true<br>– Path Length: 0 |
| Key Usage | – Certificate Signing<br>– CRL Signing<br>– Digital Signature |
| Subject Key Identifier | 8b 3c ef 48 fd d4 1f 35 1e fc 3b ad ea f4 f5 bc 2c bf f2 f6 |
| Policy ID | 1.3.6.1.4.1.4948.11.3.1 |

### 2.2.4 Migros User CA 2 Zertifikat

Das Migros User CA 2 Zertifikat ist mit dem korrespondierenden privaten Schlüssel der Migros Root CA 2 signiert (subordiniert). Die Überprüfung des Migros User CA 2 Zertifikats erfolgt durch die Überprüfung der Zertifikatssignatur mittels des Zertifikats der Migros Root CA 2. Die Schlüssellänge des CA Zertifikats beträgt 4096 Bit.

#### Namensgebung

Das Migros User CA 2 Zertifikat hat folgenden Subject-DN:

| RDN | Beschreibung |
|---|---|
| CN | Migros User CA 2 |
| O | Migros |
| C | 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 Migros System CA 2 und Migros User CA 2 Zertifikats beträgt 20 Jahre. Das CA Zertifikat ist gültig vom Dienstag, 4. März 2014 11:13:14 bis Montag, 27. Februar 2034 11:13:14.

#### Fingerprint

| Hash-Algorithmus | Fingerprint |
|---|---|
| SHA-1 | 0b fd 4a 44 75 49 50 f7 72 c0 da a9 02 25 d4 a4 c7 18 b7 db |

#### Erweiterungen

| Name | Wert |
|---|---|
| Basic Constraints | – CA: true<br>– Path Length: 0 |
| Key Usage | – Certificate Signing<br>– CRL Signing<br>– Digital Signature |
| Subject Key Identifier | 7b 7d b4 37 cb b2 ea 49 c5 36 68 07 8a a9 66 e3 2d 49 0e 89 |
| Policy ID | 1.3.6.1.4.1.4948.11.3.1 |

### 2.2.5 End-Entity Zertifikatsmatrix

Dieser Abschnitt zeigt, welche Zertifikatstypen der Migros System CA 2 und Migros User CA 2 für die verschiedenen Dienstleistungen zum Einsatz kommen. Die End-Entity Zertifikate sind im Dokument „Migros NG-PKI - Zertifikatsspezifikation“ detailliert spezifiziert.

Die nachfolgende Tabelle stellt eine Übersicht der End-Entity Zertifikate dar, welche von der Migros System CA 2 und Migros User CA 2 ausgestellt werden.

#### 2.2.5.1 End-Entity Zertifikate Migros System CA 2

| # | Zertifikatsname | Key | Enrollment | Gültigkeit | Reenroll |
|---|---|---|---|---|---|
| 1 | Migros Webserver | 2048 Bit | Manuell via RA | 5 Jahre | 3 Monate |
| 2 | Migros Application Client Authentication | 2048 Bit | Manuell via RA | 5 Jahre | 3 Monate |

#### 2.2.5.2 End-Entity Zertifikate Migros User CA 2

| # | Zertifikatsname | Key | Enrollment | Gültigkeit | Reenroll |
|---|---|---|---|---|---|
| 1 | Migros User Authentication | 2048 Bit | Migros User RA | 3 Jahre | 3 Monate |
| 2 | Migros SSOSignAuth | 2048 Bit | Migros User RA | 3 Jahre | 3 Monate |
| 3 | Migros BasicSignAuth | 2048 Bit | Migros User RA | 3 Jahre | 3 Monate |

keyon

Microsoft CERTIFIED Partner

# 3 Migros Corporate PKI Infrastruktur

## 3.1 Betreiber

Der Betreiber der Migros Corporate PKI ist der Migros-Genossenschafts-Bund (MGB):

Migros-Genossenschafts-Bund
Migros IT-Services
Heinrichstrasse 216
Postfach
CH-8031 Zürich

## 3.2 Migros Corporate PKI Schlüssel

### 3.2.1 Generierung

Die Erzeugung aller CA Schlüsselpaare der Migros Corporate PKI wurde in einer gesicherten Umgebung durchgeführt. Die Schlüsselpaare wurden mehrfach redundant auf verschiedenen Hardware Token gespeichert. Die Hardware Token sind über Zugriffcodes geschützt und in Sicherheitstresoren abgelegt.

Der Prozess der Schlüsselgenerierung garantiert, dass der private Schlüssel der CA nur auf den dafür vorgesehenen Hardware Token gespeichert ist. Der private Schlüssel kann den Hardware Token nicht verlassen.

### 3.2.2 Verteilung des öffentlichen Schlüssels

Alle manuell ausgestellten Zertifikate werden dem Zertifikats-Antragssteller per Email zugesandt.

Alle automatisiert ausgestellten Zertifikate werden dem Zertifikats-Antragssteller über den in Microsoft Windows enthaltenen, automatisierten Ausroll-Prozess übermittelt.

### 3.2.3 Einstellung der Tätigkeit

Die Migros informiert alle Teilnehmer, falls eine Einstellung der Tätigkeiten der Migros Corporate PKI Hierarchie vorgesehen ist.

### 3.2.4 Aufbewahrungspflicht

Die Migros verpflichtet sich, die Daten der Teilnehmer für eine bestimmte Zeitdauer aufzubewahren:

- Teilnehmerdaten
- Zertifikat mit den entsprechenden Statusinformationen

## 3.3 Sicherheit

### 3.3.1 Systemsicherheit

Alle CA-Instanzen der Migros Corporate PKI werden auf einem dedizierten System betrieben. Der Zugang zu den CA Systemen (HSMs) unterliegt physischen Zugangskontrollen.

### 3.3.2 Personelle Sicherheit

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

## 3.4 Auditing

Die Migros Corporate PKI unterliegt einem periodischen Audit durch Revisoren der Migros.

# 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 bei der Migros erzeugt. Der Prozess der Schlüsselgenerierung für die Authentisierungs- und Signaturzertifikate garantiert, dass der private Schlüssel nur auf Systemen der Migros gespeichert ist. Die Migros hat keine Kopie des privaten Schlüssels der Authentisierungs- und Signaturzertifikate.

## 4.3 Zertifikatsantrag

Für jedes von der Migros verwaltete System, welches sich innerhalb der IT Infrastruktur der Migros befindet, kann ein Antrag auf ein Teilnehmerzertifikat gestellt werden. Die Prüfung des Antrags erfolgt durch die Migros. Es liegt in der Verantwortung der Migros, ein Teilnehmerzertifikat gemäss Antrag auszustellen oder den Antrag abzuweisen.

## 4.4 Verteilung der Schlüssel und Zertifikate

System-Zertifikate der Migros System CA 2 und Migros User CA 2 werden mittels der Registration-Authority Webapplikation oder Microsoft Autoenrollment ausgegeben.

### 4.4.1 Registration Authority Webapplikation

Alle Zertifikatsanträge werden im Ticketing System des Migros 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 Email dem Zertifikatsantragssteller übermittelt. Bei manuell ausgestellten PKCS#12 Dateien werden die Datei und das dazugehörige Passwort auf separatem Weg per Email dem Zertifikatsantragssteller übermittelt.

### 4.4.2 Microsoft Autoenrollment

Zertifikate für Systeme welche sich im Active Directory des Migros in der Domäne corp.ads.migros.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 Migros Root CA 2 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 Migros Corporate 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 der Migros 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 Migros 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 Migros und/oder Dienstleistungen gemäss Kapitel 1.2 durch den Teilnehmer
- Einstellung des PKI Betriebs

### 4.6.3 Sperrlisten (CRL)

Die von den CAs der Migros Corporate 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 Migros Corporate PKI ausgestellten Sperrlisten werden intern verfügbar gemacht. Die Sperrlisten werden von den Systemen der Migros zur Überprüfung der Gültigkeit von Zertifikaten eingesetzt.

## 4.7 Haftung

Für die Verwendung der Teilnehmerzertifikate gemäss Kapitel 1.2 gelten die Haftungsklauseln der entsprechenden Verträge.

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