Certification practice statement

1. Introduction

T-Mobile Czech Republic a.s. (“TMCZ”) provides digital certificates (“Certificates”) through internally operated public key infrastructure (“PKI”).

This document, called the “CPS”, sets forth the operational policies within the TMCZ PKI and providing associated trust services.

All the listed provisions are related to T-Mobile Czech Republic a.s. (OID 1.3.6.1.4.1.16372), “T-Mobile CZ Root CA4” Certification Authority and all subordinate issuing Certification Authorities (“CA”) including relevant processes. The subordinate authorities serve as registration authorities at the same time.

1.1.Role of the TMCZ CPS and Other Documents

Certification practice is governed by Certificate Policy (“CP”), OID=1.3.6.1.4.1.16372.1.1.4.1, and applicable CPS, OID=1.3.6.1.4.1.16372.1.1.4.2. The CPS serves as a statement about the way that a CA issues certificates and it translates certificate policies into operational procedures on the CA level.

A CPS might include the following types of information:

- Positive identification of the CA, including the CA name, server name, and Domain Name System (DNS) address
- Certificate policies that are implemented by the CA and the certificate types that are issued
- Policies, procedures, and processes for issuing, renewing, and recovering certificates
- Cryptographic algorithms, cryptographic service providers (CSPs), and the key length that is used for the CA certificate
- Physical, network, and procedural security for the CA
- The certificate lifetime of each certificate that is issued by the CA
- Policies for revoking certificates, including conditions for certificate revocation, such as employee termination and misuse of security privileges
- Policies for certificate revocation lists (CRLs), including where to locate CRL distribution points and how often CRLs are published
- A policy for renewing the CA's certificate before it expires

1.2.Identification of the Certification Authority

Name of the root Certification Authority within TMCZ PKI: T-Mobile CZ Root CA4

Certificate attributes are listed below.

Subject and Issuer:

- CN = T-Mobile CZ Root CA4
- OU = Information Technology
- O = T-Mobile Czech Republic a.s.

- L = Prague
- C = CZ
- E = ca@t-mobile.cz

Valid from: February 11th, 2016 12:32:58

Valid to: February 11th, 2024 12:42:57

Serial number

- 11 a3 11 71 47 7e 6a b9 4e 4c 22 91 68 48 c2 2b

Subject Key Identifier

- 41 ae ae 99 90 5d 00 1a 10 ec d3 5b 88 a1 40 8b 9d 58 23 5e

Thumbprint (sha1)

- 83 50 aa 6f 41 d6 59 bd f5 59 d5 13 f8 0a dc e0 d4 48 48 61

Repository address is: http://cert.t-mobile.cz and http://cert.rdm.cz .

1.3.Contact Details

This CPS is maintained by the Data Reliance Shared Service Center ("DRSSC") of T-Mobile Czech Republic a.s. DRSSC serves as superior entity to all CAs and RAs within TMCZ PKI. Team email address is: it_security@t-mobile.cz

The address and the contact person for the DRSSC are:

Tomáš Kadlček
Senior IT Security Specialist – Key and Certificate Management
T-Mobile Czech Republic a.s.
Tomíčkova 2144/1, 148 00 Praha 4 - Chodov
Tel.: +420 603 607 099
Mobil: +420 603 272 570
E-Mail: tomas@kadlcek@t-mobile.cz

2. General Provisions

2.1.Obligations

2.1.1. CA Obligations

- CA shall notify all CA subscribers when the CA certificate is revoked.
- CA shall notify all CA subscribers whose certificates are being revoked or suspended.
- CA guarantees timely publication of certificates and revocation lists.
- CA revokes Subscriber's certificates in case of contract termination.

2.1.2. Subscriber Obligations

- Subscriber shall follow TMCZ IT Security policy when applying for a certificate and using it.

- Subscriber must protect his private key.
- Subscriber shall notify CA when the private key is compromised.

2.2.Liability

The warranties, disclaimers of warranty, and limitations of liability among TMCZ and respective business partners are set forth and governed by the agreements among them.

2.3.Publication and Repository

TMCZ shall publish the CP, public version of applicable CPS, CRL and CA certificates on the repository website. CPS shall be reviewed on a yearly basis.

CRL of root CA shall be published on a quarterly basis. CRL of subordinate CAs shall be published weekly.

Individual certificates are not published by means of certification authorities. Only the E-mail encryption certificates for TMCZ Active Directory System ("ADS") users are published within the ADS.

2.4.Compliance Audit

TMCZ is a subject of audit activities driven by TMCZ internal audit, DTAG audits and ISMS audits based on their focus scope. TMCZ shall undergo a periodic "Compliance Audit" to ensure compliance with industry standards and requirements defined in CP and applicable CPS after it begins the operations. TMCZ is entitled to perform other reviews and investigations to ensure trustworthiness of PKI. Compliance Audits shall be conducted at least annually. TMCZ is entitled to perform Compliance Audit by the means of self-audit.

2.5.Confidentiality and Privacy

All private keys are considered strictly confidential; all data stored in a subject field of a certificate are public. This CPS, CA certificates and CRLs are public information.

3. Identification and Authentication

3.1.Initial Registration

3.1.1. Types of Names

End-user Subscriber Certificates shall contain an X.501 distinguished name in the Subject name field. The Subject distinguished name of end-user Subscriber Certificates shall include a common name (CN) component. The authenticated common name value included in the Subject distinguished names of organizational Certificates shall be a domain name (in the case of server) or the legal name of the organization or unit within the organization. The authenticated common name value included in the Subject distinguished name of an organizational Certificate, however, shall be the generally accepted personal name of the organizational representative authorized to use the organization's private key, and the organization (O) component shall be the legal name of the organization. The common name value included in the Subject distinguished name of individual Certificates shall represent the individual's generally accepted personal name. Common names shall be authenticated.

3.1.2. Authentication

The Identity of a Subscriber is validated against a TMCZ ADS domain account or by an account of a person with the right to request a certificate on behalf of a temporary ADS account provided to a partner by TMCZ contact person.

3.2.Routine Rekey (Renewal)

The entity approving a Certificate Application for the Subscriber of an end-user Subscriber Certificate shall be responsible for authenticating a request for renewal. Renewal procedures shall ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber of the Certificate. Confirmation of the identity can be performed by using internal database.

3.3.Rekey After Revocation

The reason for revocation shall be reviewed from the security perspective. Renewal following revocation of the Certificate is permissible as long as renewal procedures ensure that the organization or CA seeking renewal is in fact the Subscriber of the Certificate. Procedure is governed by the same requirements as routine rekey.

3.4.Revocation Request

Revocation procedures shall ensure prior to any revocation of any Certificate that the revocation has in fact been requested by the Certificate's Subscriber or the entity that approved the Certificate Application. CA/RA Administrators are entitled to request the revocation of end-user Subscriber Certificates within the CA's/RA's subdomain.

4. Operational Requirements

4.1.Certificate Application, Processing and Issuance

Certificate Application may be submitted by individual (who is the subject of the Certificate) or authorized representative of Organization, CA or RA.

4.1.1. Certificate Applications for End-User Subscriber Certificates

All end-user Certificate Applicants shall undergo an enrollment process consisting of:

- completing a Certificate Application and providing the requested information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key to the issuing CA/RA,
- demonstrating to the issuing CA/RA that the Certificate Applicant is in possession of the private key corresponding to the public key delivered to the CA/RA, and
- manifesting assent to the relevant CP and CPS.

4.1.2. Certificate Applications for CA or RA Certificates

Subscribers of CA or RA Certificates are not required to complete formal Certificate Applications. Instead, they enter into contract with CA administrator to demonstrate their identity and provide contact information during the contracting process.

4.1.3. Certificate Application Processing

CA/RA shall perform identification and authentication of all required Subscriber information. Upon successful identification and authentication of all required Subscriber information, the Certificate Application shall be approved. CA/RA shall reject a Certificate Application if identification and authentication cannot be completed. CA/RA shall process the Certificate Application within a reasonable time of receipt. There is no time stipulation to complete the processing of an application. A Certificate Application remains active until rejected.

4.1.4. Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by CA or following receipt of an RA's request to issue the Certificate. CA shall, either directly or through an RA, notify Subscribers that their certificates are available. Certificates shall be made available to end-user Subscribers either by ADS services (certificate autoenrollment) or via a message sent to the Subscriber containing the Certificate. The procedures of this section shall also be used for the issuance of Certificates in connection with the submission of a request to renew the Certificate.

4.2.Key Pair and Certificate Usage

Use of the private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has accepted the certificate. The certificate shall be used lawfully in accordance with the terms of the CP and this CPS. Certificate use must be consistent with the KeyUsage field extensions included in the certificate. Subscribers shall protect private keys from unauthorized use.

4.3.Certificate Renewal and Re-Key

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate. Certificate rekey is the application for the issuance of a new certificate that certifies the new public key. Certificate rekey is supposed for all certificate classes.

Prior to expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew or rekey a new certificate to maintain continuity of the Certificate usage. A Certificate may also be renewed or rekeyed after expiration. Only the Subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal or rekey. Renewal and rekey procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

4.4.Certificate Revocation

4.4.1. Circumstances for Revocation

An end-user Subscriber Certificate shall be revoked if:

- The entity approving the Subscriber’s Certificate Application discovers or has reason to believe that there has been a Compromise of the Subscriber’s private key.
- The affiliation between TMCZ and Subscriber is terminated or has otherwise ended.
- The entity approving the Subscriber’s Certificate Application discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to a person other than

the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate.

- The entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.
- In the case of organizational Certificates, the Subscriber's organization name changes.
- The information within the Certificate is incorrect or has changed.
- The Subscriber requests revocation of the Certificate in accordance with CP.
- The continued use of that certificate is harmful to TMCZ or PKI participants.

A CA/RA Certificate shall be revoked if:

- The CA's or RA's superior entity discovers or has reason to believe that there has been a Compromise of the CA or RA private key.
- The CA's or RA's Superior Entity discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to an entity other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the entity named as the Subject of such Certificate.
- The CA requests revocation of the Certificate.
- The continued use of that certificate is harmful to TMCZ or PKI participants.

4.4.2. Who Can Request Revocation

In case of end-user Subscriber certificate, revocation can be requested by:

- Individual Subscriber who wants to revoke their own individual Certificates
- In case of organizational Certificate, a duly authorized representative of the organization
- Entity that approved Subscriber's Certificate Application

In case of CA/RA certificate, revocation can be requested only by respective CA/RA administrator.

4.4.3. Procedure for Revocation Request

An end-user Subscriber requesting revocation shall communicate the request to the entity that approved the Subscriber's Certificate Application (a CA or RA), and such entity shall revoke the Certificate itself. Communication of such request shall be in accordance with CP. A CA or RA revoking an end-user Subscriber Certificate upon its own initiative shall revoke the Certificate itself.

A CA or RA requesting revocation shall communicate the request to its superior entity (DRSSC) and proceed with revocation pursuant the CP.

4.4.4. Revocation Request Grace Period

Revocation request shall be submitted within commercially reasonable time and as promptly as possible.

4.4.5. CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once a week. CRLs for CA Certificates shall be issued at least quarterly, but also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration. CRLs are

posted to the repository within a commercially reasonable time after generation. This is done automatically within minutes of generation.

4.4.6. CRL Checking Requirements

Relying Parties shall check the status of Certificates on which they wish to rely by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Certificate status information shall be available via a web-based repository.

4.5.Compromise and Disaster Recovery

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Backups of CA private keys shall be generated and maintained.

4.5.1. Entity Key is compromised

Upon Compromise of the private key of an entity, the Certificate of that entity shall be revoked in accordance with CP.

4.6.CA Termination

A terminating CA and PKI administrator shall, in good faith, use commercially reasonable effort to agree on a termination plan that minimizes service disruption to Subscribers and relying parties. The termination plan may cover issues such as:

- Provisions needed for the transition of the CA's services to a successor CA.
- Providing notice to parties affected by the termination, such as Subscribers, relying parties.
- The continuation of Subscriber and customer support services.

5. Physical, Procedural, and Personnel Security Controls

5.1.Physical Controls

5.1.1. Site Location and Construction

All CA and RA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

5.1.2. Physical Access

Physically protected environment can be accessed only by authorized personnel. Online CAs are protected through the use of locked cabinets. Offline CAs are protected through the use of locked safes, cabinets and containers.

5.2.Procedural Controls

5.2.1. Trusted Roles

Employees, contractors, and consultants that are designated to manage infrastructural trustworthiness shall be considered to be "Trusted Persons." Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- or the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to, customer service personnel, system administration personnel, designated engineering personnel, and executives that are designated to manage infrastructural trustworthiness.

5.2.2. Identification and Authentication for Each Role

TMCZ shall confirm the identity and authorization of all personnel seeking to become Trusted Persons. Authentication of identity shall include the personal (physical) presence of such personnel before Trusted Persons performing HR or security functions within an entity and a check of well-recognized forms of identification.

5.3.Personnel Controls

5.3.1. Background, Qualifications, Experience, and Clearance Requirements

TMCZ requires that personnel seeking to become Trusted Persons shall be qualified and experienced to perform their prospective job responsibilities competently and satisfactorily.

5.3.2. Training Requirements

TMCZ shall provide its personnel with the requisite training when being hired, and shall provide the requisite on-the-job training, needed for their personnel to perform their job responsibilities relating to CA or RA operations competently and satisfactorily. TMCZ shall also periodically review the training programs, and the training shall address the elements relevant to functions performed by their personnel.

5.3.3. Contracting Personnel Requirements

TMCZ shall permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly-defined outsourcing relationships and only under the following conditions:

(1) the entity using the independent contractors or consultants as Trusted Persons does not have suitable employees available to fill the roles of Trusted Persons, and

(2) the contractors or consultants are trusted by the entity to the same extent as if they were employees.

5.4.Audit Logging Procedures

5.4.1. Types of Events Recorded

TMCZ manually or automatically logs the following significant events:

- CA key life cycle management events, including:
    - Key generation, backup, storage, recovery, archival, and destruction
    - Cryptographic device life cycle management events.

- CA and Subscriber certificate life cycle management events, including:
    - Certificate Applications, renewal, rekey, and revocation
    - Successful or unsuccessful processing of requests
    - Generation and issuance of Certificates and CRLs.
- Security-related events including:
    - Successful and unsuccessful PKI system access attempts
    - PKI and security system actions performed by TMCZ personnel
    - Security sensitive files or records read, written or deleted
    - Security profile changes
    - System crashes, hardware failures and other anomalies
    - Firewall and router activity
    - CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Kind of entry.

5.4.2. Frequency of Log Processing

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, TMCZ reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within TMCZ PKI CA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, and inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

5.4.3. Retention, Protection and Backup Procedures

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived. Audit logs shall be protected from unauthorized viewing, modification, deletion, or other tampering. Incremental backups of audit logs are created daily and full backups are performed weekly.

5.5.Records Archival

TMCZ archives:

- All audit data
- Certificate Application information
- Documents supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

TMCZ protects the archive so that only authorized trusted persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system.

5.6.Key Changeover

CA key pairs are retired from the service at the end of their respective maximum lifetimes as defined in this CPS. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pair and to support new services.

Prior to the expiration of the CA Certificate for the superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the superior CA's hierarchy for the old superior CA key pair to the new CA key pair. CA key changeover process requires that:

- A superior CA ceases to issue new subordinate CA Certificates no later than 60 days before the remaining lifetime of the superior CA key pair equals the approved Certificate Validity period for the specific type of certificates issued by subordinate CAs in the superior CA's hierarchy.
- Upon successful validation of subordinate CA or end-user Subscriber Certificate requests, Certificates will be signed with a new CA key pair.

The superior CA continues to issue CRLs signed with the original superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

5.7.Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued.

5.7.2. Computing Resources, Software, and/or Data are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to TMCZ PKI administrator and incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, TMCZ PKI key compromise and disaster recovery procedures will be enacted.

5.7.3. Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a TMCZ PKI or CA, key compromise response procedures are enacted by TMCZ PKI administrator.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to relying parties through the repository
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected TMCZ PKI participants
- The CA will generate a new key pair in accordance with CPS § 5.8.

5.7.4. Business Continuity Capabilities after a Disaster

The procedures are defined by relevant TMCZ documents and contracts with outsourcing partners.

5.8.CA or RA termination

In the event that it is necessary for a CA to cease operation, TMCZ makes a commercially reasonable effort to notify Subscribers, relying parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, TMCZ will develop a termination plan to minimize disruption to customers, Subscribers, and relying parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, relying parties, and customers, informing them of the status of the CA
- Handling cost of such a notice
- The revocation of the Certificate issued to the CA by TMCZ
- The preservation of the CA's archives and records for the time periods required in this CPS
- The continuation of Subscriber and customer support services
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary
- Disposition of the CA's private key and the hardware tokens containing such private key
- Provisions needed for the transition of the CA's services to a successor CA

6. Technical Security Controls

6.1.Key Pair Generation and Installation

6.1.1. Key Pair Generation

CA key pair generation is performed by CA administrator using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys. Generation of end-user Subscriber key pairs is generally performed by the Subscriber. The Subscriber typically uses their browser software for key generation. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software.

6.1.2. Private Key Delivery to Subscriber

When end-user Subscriber key pairs are generated by the end-user Subscriber, private key delivery to a Subscriber is not applicable. Where end-user Subscriber key pairs are pre-generated by TMCZ, such key pairs are distributed to end-user Subscribers by TMCZ via a password protected PKCS #12 file. The password is communicated to the end-user Subscriber using an out-of-band process.

6.1.3. Public Key Delivery to Certificate Issuer

When a public key is transferred to the CA/RA to be certified, it shall be delivered through a mechanism ensuring that the public key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred public key. The acceptable mechanism within the TMCZ PKI for public key delivery is a PKCS #10 Certificate Signing Request (CSR).

6.1.4. CA Public Key Delivery to Users

TMCZ shall make the public keys of its CAs publicly available to Relying Parties via CA Certificates in a secure fashion.

6.1.5. Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The current TMCZ PKI standard for minimum key sizes is the use of key pairs equivalent in strength to 1024 bit.

6.1.6. Public Key Parameters Generation

TMCZ PKI participants using the Digital Signature Standard shall generate the required Key Parameters in accordance with FIPS 186-2 standard.

6.1.7. Key Usage Purposes (As per X.509 v3 Key Usage Field)

For X.509 Version 3 Certificates, CAs/RAs generally populate the KeyUsage extension of Certificates they issue in accordance with RFC 3280.

6.2.Private Key Protection

Private keys shall be protected and private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such private keys. TMCZ has implemented a combination of physical, logical, and procedural controls to ensure the security of CA private keys.

6.2.1. Private Key Escrow

Private keys of CAs or end-user Subscribers shall not be escrowed.

6.2.2. Private Key Backup

CAs/RAs shall back up their own private keys for routine recovery or disaster recovery purposes. Private keys that are backed up are to be protected from unauthorized modification or disclosure through physical or cryptographic means. Backups shall be protected with a level of physical and cryptographic protection equal to or exceeding that on CA.

6.3.Other Aspects of Key Pair Management

6.3.1. Public Key Archival

CAs shall back up and archive their own public keys, as well as the public keys of all of the Subscribers within their subdomains.

6.3.2. Usage Periods for the Public and Private Keys

The operational period for Certificates shall be set to the time limits set forth in table below.

CA self-signed	up to 8 years
CA to subordinate CA	up to 4 years
CA to end-user Subscriber	up to 2 years

6.4.Computer Security Controls

CA and RA functions shall take place on trustworthy systems secure from unauthorized access. TMCZ limits access to production servers to those individuals with a valid business reason for such access. General application users do not have account on production servers. TMCZ uses firewalls to protect

the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

6.5.Network Security Controls

TMCZ shall perform CA and RA functions using networks secured to prevent unauthorized access, tampering, and denial-of-service attacks.

6.6.Time Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7. Certificate and CRL Profile

7.1.Intended Purpose

The certificates issued by PKI are suitable for the following applications:

- Secure remote access to TMCZ network
- Authentication of partners to access TMCZ applications
- Server authentication in internal production and testing environment for TMCZ internal users and for TMCZ business partners
- E-mail encryption and signing certificates for TMCZ users
- Signatures for TMCZ internal approval workflow

The use of such certificates is restricted and has to be approved and treated in a specific way:

- Code signing – only for specific internal purpose

The use of PKI for the following applications is prohibited:

- Server authentication for customer facing applications
- Signing of a code delivered by a third party and intended for TMCZ customers

7.2.Certificate Profile

Certificates shall conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 (“RFC 3280”).

At a minimum, X.509 Certificates shall contain the basic fields and indicated prescribed values or value constraints listed below:

- Serial Number
- Signature Algorithm
- Issuer DN
- Valid From
- Valid To
- Subject DN
- Subject Public Key

- Signature

7.3.Certificate Extensions

TMCZ shall populate X.509 Certificates with the extensions listed below:

- Key Usage
- Certificate Policies Extension - Certificates shall be populated with the object identifier of applicable CPS
- Subject Alternative Names - optional
- Basic Constraints - CA Certificates shall be populated with a Basic Constraints extension with the CA field set to TRUE
- Extended Key Usage - Certificates shall be populated with an Extended Key Usage extension configured to include the key purpose object identifiers (OID)
- CRL Distribution Points - Certificates shall be populated with a CRL Distribution Points extension containing the URL of the location where a Relying Party can obtain a CRL to check the Certificate's status
- Authority Key Identifier - Certificates shall be populated with an Authority Key Identifier extension, which contains the location of public key of the issuing CA
- Subject Key Identifier - Certificates shall be populated with an Subject Key Identifier extension, which contains the public key of the Subject of the Certificate

7.4.CRL

CA shall issue CRLs that conform to RFC 3280.

CRLs contain the basic fields and contents specified below:

- Version
- Signature Algorithm - algorithm used to sign the CRL in accordance with RFC 3279
- Issuer - entity who has signed and issued the CRL
- Effective Date - issue date of the CRL. CRLs are effective upon issuance
- Next Update - date by the which the next CRL will be issued
- Revoked Certificates - listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date

8. Acronyms and Definitions

Acronyms

ADS	Active Directory System
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
PKI	Public Key Infrastructure
RA	Registration Authority
TMCZ	T-Mobile Czech Republic a.s.

Definitions

Certificate	A message that, at least, states a name or identifies the CA, identifies a Subscriber, contains the Subscriber's public key, identifies the Certificate's operational period, contains Certificate serial number and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Revocation List	A periodically (or exigently) issued list, digitally signed by CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times for revocation.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private.
Relying Party	An individual or organization that acts in reliance on a Certificate and/or a digital signature.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Superior Entity	An entity above a certain entity within a TMCZ PKI hierarchy.
Trusted Persons	An employee, contactor, or consultant of an entity within the TMCZ PKI responsible for

	managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.