Certificate policy

1. Introduction

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

This document, called the "CP", is the principal document governing TMCZ PKI. The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the TMCZ PKI and providing associated trust services.

1.1. Role of the TMCZ CP and Other Practices Documents

The CP describes at a general level the overall business, legal, and technical infrastructure of the TMCZ PKI. More specifically, it describes, among other things:

- Common security requirements
- Certificate usage, enrollment, and issuance requirements
- Intended purpose of certificate
- Policies and procedures under which the certificates are issued
- Authentication procedures
- Private key management requirements
- Minimal length for the public key and the private key pairs
- Requirements for revocation

Other important document relevant to TMCZ PKI is Certification Practice Statement ("CPS").

1.2. Certification Authority

Entity called "Certification Authority" or "CA" acts as trusted party to facilitate the confirmation of the binding between a public key and the identity or other attributes of the individual, entity, or device that is the "Subject" of the certificate. In case of individual or entity, the Subject is the "Subscriber". In case of device, the identity of "Subscriber" who administers the device is confirmed.

1.3. Registration Authority

CAs sometimes delegate certain roles (such as identity confirmation functions) to entity called "Registration Authority" or "RA". RAs establish enrollment procedures on behalf of a CA, obtain "Certificate Applications", confirm the identity of "Certificate Applicants", and either approve or deny Certificate Applications. RAs can also initiate Certificate revocation.

1.4. Subscribers

Subscribers are individuals or organizations that obtain Certificates for use in their applications. Certificates can be used for various purposes such as digitally signing email or creating secure channel between the Subscriber and the server (SSL/TLS web browsing, IPSEC VPN tunnel).

1.4.1. Certificate Applicant

Before a Subscriber obtains a Certificate, the Subscriber must first enroll for a Certificate as a Certificate Applicant. Certificate Applicants must complete the enrollment process established by a

CA or RA, in which a Certificate Application is submitted to the CA or RA. In response to a Certificate Application, the CA or RA confirms the identity and/or other attributes of the Certificate Applicant and either approves or denies the Certificate Application. If the Certificate Application is approved, a Certificate is issued to the Certificate Applicant. Following issuance, the CA makes the Certificate available to the Certificate Applicant. Retrieval and/or loading of a Certificate into software constitutes acceptance of the Certificate, at which time the Certificate Applicant becomes a Subscriber, unless the Subscriber previously manifested acceptance. The Subscriber must review the Certificate and notify the CA or RA of any mistakes in the Certificate content after receiving access to the Certificate. The new Subscriber agrees to be bound by Subscribers' obligations as defined through CP and CPS.

1.5.Contact Details

The organization administering this CP is the Data Reliance Shared Service Center ("DRSSC"). DRSSC serves as superior entity to all CAs and RAs within TMCZ PKI. The address and the contact person for the DRSSC is:

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

CAs shall perform the specific obligations appearing throughout this CP.

2.1.2. RA Obligations

RAs assist a CA by performing validation functions, approving or rejecting Certificate Applications, requesting revocation of Certificates, and approving renewal requests.

2.1.3. Subscriber Obligations

Certificate Applicants shall provide complete and accurate information on their Certificate Applications and perform Subscriber functions in accordance with the specific obligations appearing throughout this CP.

2.2.Liability

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

2.2.1. Certification Authority Warranties

CP shall warrant to Subscribers that:

- There are no material misrepresentations of fact in the Certificate originating from the entities approving the Certificate Application or issuing the Certificate.
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate.
- Their Certificates meet all material requirements of the applicable CPS.
- Revocation services and use of repository conform to the applicable CPS.

2.2.2. Registration Authority Warranties

CP shall warrant to Subscribers that:

- All information in or incorporated by reference in such Certificate is accurate.
- The entities approving the Certificate Application and issuing the Certificate have substantially complied with the applicable CPS when issuing the Certificate.

2.2.3. Subscriber Warranties

CP requires Subscribers that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and Certificate is operational (not expired or revoked) at the time the digital signature is created.
- No unauthorized person has ever had access to the Subscriber’s private key.
- All information supplied by the Subscriber and contained in the Certificate is true.
- The Certificate is being used exclusively for authorized and legal purposes, consistent with the applicable CPS.
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscribers have responsibility for private key protection. Any loss or damage resulting from failure to meet above stated requirements is the responsibility of Subscriber.

2.3.Dispute Resolution Procedures

Disputes among TMCZ and Customers shall be resolved pursuant to provisions in the applicable agreements among the parties.

2.4.Publication and Repository

TMCZ shall publish this CP, applicable CPS, CRL and CA certificate on the repository website.

2.5.Compliance Audit

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 at the sole expense of the audited entity. TMCZ is entitled to perform Compliance Audit by the means of self-audit.

2.5.1. Communications of Results

Following any Compliance Audit, the audited entity shall receive the annual report and attestations based on its audit or self-audit within fourteen (14) days after the completion of the audit.

2.5.2. Actions Taken as a Result of Deficiency

After receiving a report based on the Compliance Audit the audited entity shall discuss any exceptions or deficiencies shown by the Compliance Audit. The audited entity shall, in good faith, use commercially reasonable efforts to agree on a corrective action plan for correcting the problems causing the exceptions or deficiencies and to implement the plan. If necessary, TMCZ shall be entitled to determine whether revocation is necessary.

2.6.Confidentiality and Privacy

TMCZ shall implement a privacy policy in accordance with local privacy laws. TMCZ shall not disclose or sell the names of Certificate Applicants or other identifying information about them. When terminating CA, TMCZ is entitled to transfer such information to a successor CA.

2.6.1. Types of Information to be Kept Confidential and Private

The following records of Subscribers shall be kept confidential and private (“Confidential/Private Information”):

- CA application records, whether approved or disapproved,
- Certificate Application records
- Private keys held by PKI (which includes keys managed by PKI administrator for third parties)
- Transactional records (both full records and the audit trail of transactions)
- Audit trail records created or retained by TMCZ or Customers
- Contingency planning and disaster recovery plans
- Security measures controlling the operations of PKI and the administration of Certificate services and designated enrollment services

2.6.2. Types of Information Not Considered Confidential or Private

PKI participants acknowledge that Certificates, Certificate revocation and other status information, repositories, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

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 a 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. Need for Names to be Meaningful

Subscriber Certificates shall include meaningful names in the following sense: end-user Subscriber Certificates shall contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate. For such Certificates, pseudonyms (names other than a Subscriber's true personal or organizational name) shall not be permitted.

3.1.3. Uniqueness of Names

The names of Subscribers within the PKI shall be unique within subdomains for a specific class of Certificates. It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name. TMCZ shall not arbitrate in case of name claim dispute. TMCZ shall be entitled to reject or suspend any Certificate Application because of such dispute.

3.1.4. Method to Prove Possession of Private Key

The method to prove possession of a private key shall be PKCS #10. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber.

3.1.5. Authentication

Confirmation of the identity of a Certificate Applicant for a personal, organizational, or server Certificate shall include:

- A determination that the entity exists by using at least one internal database, or alternatively, organizational documentation issued by TMCZ.
- In the case of server Certificates, a determination that the Certificate Applicant is authorized to use the domain or IP address.
- In the case of third party, the additional checks necessary to verify contractual status to TMCZ through TMCZ employee responsible for third party.

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

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 has 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.

4.2. Certificate Issuance

4.2.1. Issuance of End-User Subscriber Certificates

After a Certificate Applicant submits a Certificate Application, the entity receiving the Certificate Application shall confirm or disconfirm the information in the Certificate Application pursuant to CP. Upon successful performance of all required authentication procedures pursuant to CP, the entity receiving the Certificate Application shall approve the Certificate Application. If authentication is unsuccessful, the entity receiving the Certificate Application shall deny the Certificate Application.

A Certificate shall be created and issued following the approval of a Certificate Application or following receipt of an RA's request to issue 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.

4.2.2. Issuance of CA and RA Certificates

The identity of entities wishing to become CA/RA shall be authenticated in accordance with CP and, if approved, the Certificates needed to perform their CA or RA functions shall be issued.

4.3. Certificate Acceptance

CA issuing Certificates to end-user Subscribers shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the

Certificates by notifying them that their Certificates are available and notifying them of the means for obtaining them.

Upon issuance, Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate. Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance 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,
- 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 (DR SSC) and shall proceed with revocation pursuant this 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

Applicable CPS must state the CRL issuance frequency. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

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.

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, 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.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Key pair generation shall be performed in accordance with this CP, using processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.1.2. Private Key Delivery to Entity

End-user Subscribers’ private keys are generally generated by the end-user Subscribers themselves, and therefore private key delivery to a Subscriber is unnecessary. Private keys shall be delivered to end-user Subscribers only when generating keys that are managed by PKI administrator for third parties. PKI administrator shall deliver private keys to third parties and shall secure such delivery in order to prevent the loss, disclosure, modification, or unauthorized use of such private keys.

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 pair 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.

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 so as to be able to recover from disasters and equipment malfunction. 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 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.

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.

7. Certificate and CRL Profile

7.1. 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

7.2.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

7.3.CRL

CA shall issue CRLs that conform to RFC 3280.

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.