THE WALT DISNEY COMPANY

PUBLIC KEY INFRASTRUCTURE
CERTIFICATE POLICY

November 2015
Version 4.0

Version Control

Version	Revision Date	Revision Description	Revised by
1.0			Ernst & Young LLP TWDC Corporate IT Security
1.01	March 8, 2006		Mark Randall
1.3	April 2008		Entrust Professional Services
1.4	April 2011	Revised for decommissioning of the Commerce CA (remove references) and to reflect changes to the baseline CP - the EMSPKI Commercial Private CP.	Entrust Professional Services
2.0	July 2011	Revised to reflect the implementation of a new PKI and new PKI hierarchy in support of moving the anchor of Public Trust to the Entrust Certificate Services 2048-bit Root CA	Entrust Professional Services
3.0	September 2014	Revised to reflect the new certificate issuance models.	Mark Randall and Entrust Professional Services
4.0	November 2015	Terminate public trust with ECS. Upgrade to SHA-256.	Mark Randall and Entrust Professional Services

Table of Contents

1 Introduction

1.1 Overview

This document is referred to as The Walt Disney Company (TWDC) Public Key Infrastructure (PKI) Certificate Policy (CP). This describes TWDC's policies involved in the issuance of digital certificates by the TWDC Root and Issuing Certification Authorities (collectively referred to as the "TWDC CAs").

The TWDC PKI CP is presented as a 'delta' document. As such it does not stand alone but must be read and applied in conjunction with the *X.509 Certificate Policy for the Entrust Managed Services Commercial Public Key Infrastructure (EMS CCP)* for the Entrust Managed Service, which is the operator of the TWDC CAs. Readers are instructed to refer to the *EMS CCP* document for baseline policy information applicable to the TWDC PKI certificates and refer to the TWDC PKI CP document for exceptions and differences only.

This document is organized in structure to be fully compliant with IETF RFC3647; however sections are only supplied with text where relevant exceptions or differences from the baseline exist. Those sections without text automatically default to that supplied in the *EMS CCP*.

This CP is applicable to all entities with relationships with TWDC PKI, including Subscribers, Relying Parties, and Registration Authorities (RA). This CP provides those entities with a clear statement of the policies and responsibilities of TWDC CAs, as well as the responsibilities of each entity in dealing with the CAs.

This Certification Policy (CP) consists of policy statements that outline the principles and requirements that govern TWDC PKI.

A CP specifies "what" the requirements are that will be implemented, while a corresponding Certification Practices Statement (CPS) describes "how" those requirements are met for a specific Certificate Authority. This Certificate Policy is therefore not designed to detail the processes and procedures that are involved in the management and governance of TWDC PKI; this information is entailed in the document, *TWDC Public Key Infrastructure Certification Practices Statement*.

1.2 Document Name and Identification

Document Name:	TWDC PKI Certificate Policy
Document Version:	4.0
Document Date:	November 2015
Document assigned object identifier:	2.16.840.1.114182.1.54.3 joint-ISO-CCITT(2) countries(16) USA(840) US Companies(1) TWDC(114182) PKI (1) CP(54) Major Version (3)

1.3 PKI Participants

1.3.1 Certification Authorities

The TWDC PKI is comprised of 2 Certification Authorities, as follows:

- The TWDC Root CA, which shall issue certificates only to subordinate CAs. Its purpose is to provide an anchor of trust within TWDC. The TWDC Root CA shall be subject to the stipulations of the *EMS CCP* for the Commercial Private Root CA, except where otherwise noted in this CP.
- TWDC Issuing CA, which shall issue certificates to TWDC external web sites and applications, internal users, devices, web servers and applications. It shall not issue certificates to subordinate Certification Authorities or perform cross-certifications with other Certification Authorities. The TWDC Issuing CA shall be subject to the stipulations of the *EMS CCP* for the Commercial Private SSP CA, except where otherwise noted in this CP.

The TWDC PKI CAs shall be operated as Entrust Managed Service Customer Dedicated CAs. They shall not be subordinate to any of the Entrust Managed Service Root CAs.

Where necessary, the TWDC PKI CP distinguishes the different users and roles accessing the CA functions. Where this distinction is not required, the term Certification Authority is used to refer to the total CA entity, including the hardware, software, personnel, processes, and its operations.

1.3.2 Registration Authorities

A Registration Authority (RA) shall be designated as an individual, organization or entity responsible for verifying the identity of a Subscriber. When required, the RA shall verify a Subscriber's authority to act on behalf of a client organization. Client organizations include TWDC business units/departments. Trusted RAs shall be formally nominated by the Management of the TWDC PKI.

1.3.3 Local Registration Authorities

Where applicable, the TWDC RA may delegate some of its responsibility to Local Registration Authorities (LRAs). These LRAs shall be restricted to performing RA functionality for a specific geographic region or for a specific group or organization or for specific certificate types. In other words, an LRA for *GroupX* shall be restricted to performing RA functions on *GroupX* Subscribers exclusively.

1.3.4 Trusted Agents

The RA may engage Trusted Agents (TA) to perform certain, limited registration activities. If used, the Trusted Agents shall be restricted to performing identity proofing as a proxy for the RA.

1.3.5 Subscribers

A Subscriber shall be the recipient of a digital certificate issued by the TWDC Issuing CA. Subscribers may include TWDC internal entities. With respect to the usage of TWDC PKI certificates, subscribing entities shall be limited to:

(1) Employees and contractors registered in the Enterprise Directory;

(2) Employees and contractors assigned a valid TWDC email address;

(3) TWDC external facing end entities;

(4) Services on digital processing entities, property of TWDC, or used for activities in which TWDC is involved; and

(5) End entities owned and/or operated by TWDC Business Partners that contain TWDC branded content.

By virtue of certificate subscription, the Subscriber agrees to adhere to this Certificate Policy and all other applicable laws and regulations that govern the use of digital certificates. The Subscriber shall also agree to provide true information to the best of one's knowledge at the time of certificate application. Should information provided by the Subscriber or contained in the Subscriber certificate appear to be false or misleading, the Subscriber shall notify the Contact Person listed in section 1.5.2 of this Certificate Policy.

1.3.6 Designated Certificate Holders

Under certain circumstances, automation may require an end-entity to hold a Certificate. In these situations, an individual user shall take ownership responsibility for these Certificate and the associated security.

An individual designated by TWDC to be the holder of a Certificate issued to a role, device or application for use on behalf of TWDC, may be a Designated Certificate Holder (DCH).

By virtue of Certificate subscription, the DCH agrees to adhere to this Certificate Policy and all other applicable laws and regulations that govern the use of digital certificates. The DCH shall also agree to provide true information to the best of one's knowledge at the time of certificate application. Should information provided by the DCH or contained in the certificate appear to be false or misleading, the DCH shall notify the Contact Person listed in section 1.5.2 of this Certificate Policy.

1.3.7 Relying Parties

With respect to certificates issued under this CP, a Relying Party is as follows:

- An individual, entity or organization that relies on a certificate issued by the TWDC Issuing CA. and
- All Subscribers of the TWDC PKI are themselves Relying Parties.

Relying Parties shall be responsible for checking certificate expiration and revocation status for verifying the validity of TWDC PKI issued certificates. Relying Parties shall agree to use these certificates in a manner consistent with the policies set forth in this CP.

1.3.8 Other Participants

Other participants of TWDC PKI shall include:

Participant	Role
Management of the TWDC PKI	The Management of the TWDC PKI shall consist of one or more TWDC organizational units responsible for ensuring that TWDC Certification Authorities operate as stated in the Certification Practice Statement.
PKI Policy Management Authority	The PKI Policy Management Authority (PPMA) shall be the custodian of PKI policy responsible for PKI policy administration including the approval of policy changes.
Support Services	Support Services shall include other TWDC departmental groups or third parties under contract to TWDC that support the PKI.
TWDC Internal Auditor	The TWDC Internal Auditor is responsible to inspect the audit logs generated by the on premise RA applications. The Internal Auditor also assists the External Auditor during the WebTrust audit activities.
External Auditor	The external auditor is responsible to audit the TWDC PKI for WebTrust compliance.
Directory Administrator	Directory Administrators are not associated with the PKI directly. They operate the Enterprise Directory, which is the repository for the PKI. All certificate policies, revocation lists and certificates issued by the PKI are published in Enterprise Directory. Directory Administrators have access to this data, but only to perform administration tasks of the directory itself. No modification of PKI content is permitted.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The TWDC Issuing CA shall issue user certificates to TWDC employees, contractors and business partners. User certificates shall be used for three purposes:

- access to systems or applications (authentication),
- digital signatures; and
- encryption.

The TWDC Issuing CA shall issue certificates to TWDC web servers (and clients employing mutual authentication) to enable secure communications. Server certificates shall support both authentication and encryption.

The TWDC Issuing CA shall issue SSL certificates for the purpose of supporting secure communications with TWDC external entities (i.e., the general public, extranet users, third party partners, etc.)

The TWDC Issuing CA shall issue certificates to TWDC computers and mobile devices for the purpose of supporting secure network authentication and communications.

The TWDC Issuing CA shall issue certificates to TWDC Subscribers for the purpose of data encryption.

The TWDC Issuing CA shall issue digital signature certificates to TWDC organizations for the purpose of code signing.

The TWDC PKI shall issue certificates for usages stipulated herein and not as stated in the *EMS CCP*.

1.4.2 Prohibited Certificate Uses

In general terms, applications for which TWDC PKI issued digital certificates are prohibited are those where:

- Business activities are conducted, other than for TWDC;
- Usage contravenes the TWDC PKI Policy and other governing TWDC policies or this CP; or
- Usage contravenes relevant law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The TWDC PKI Policy Management Authority (PPMA) shall be the custodian of this Certificate Policy. The PPMA is chaired by delegates selected by the Management of the TWDC PKI and may include representatives from the relevant business unit IT departments, Human Resources, Legal, Finance and Audit.

1.5.2 Contact Person

The primary contact for this CP is:

Mark Randall, Sr. Security Specialist
Enterprise Information Security
1120 Celebration Blvd.
Celebration, FL 34747
(407) 566-5172
mark.randall@disney.com

The secondary contact for this CP is:

Jeffrey Butler
Manager, Enterprise Security Infrastructure
500 S. Buena Vista St.
Burbank, CA 91521-9789
(818) 553-7945
jeffrey.butler@disney.com

1.5.3 Person Determining CPS Suitability for the Policy

The TWDC PKI Policy Management Authority (PPMA) shall approve the TWDC PKI Certification Practice Statement.

1.5.4 CP Approval Procedures

The TWDC PPMA may amend this Certificate Policy, or any part thereof, at any time at its discretion. Prior to any amendment of these Certificate Policies, the TWDC PPMA will provide notice of any proposed change in writing to the appropriate TWDC stakeholders.

Following proposed changes to this Certificate Policy, the TWDC PPMA shall circulate the proposed literature to the appropriate TWDC stakeholders for review and acceptance. Updates to this Certificate Policy as the result of any accepted changes must be approved by the TWDC PPMA and the Management of the TWDC PKI.

1.6 Definitions and Acronyms

Activation data	Private data, other than keys, required to access Personal Security Environments that needs to be protected (e.g., password).
Authority Revocation List	A list of revoked CA certificates. An ARL is a Certificate Revocation List for CA cross-certificates or self-signed certificates.
Certificate	An electronic file in a format which is in accordance with ITU-T Recommendation X.509 and which contains a public key of a Subscriber or end entity, together with related information, digitally signed with the private key of the Certification Authority that issued it.
Certificate Revocation List	A list issued and maintained by the Certification Authority of the certificates that are revoked before their pre-set expiry time.
Certification Authority	An Entity trusted by one or more End Entities to issue and manage X.509 public key certificates and CRLs.
Certification Practice Statement	A statement of the practices that a Certification Authority employs in issuing certificates. The CPS must either contain, or point to other sources which contain sufficient information to demonstrate to the applicable PPMA how the requirements within the CP are being met.
Client Organization	An organization within TWDC that is a client, either Relying Party or Subscriber, of the TWDC PKI.
Cross-certificate	A certificate issued by a Certification Authority to establish a trust relationship between it and another Certification Authority.

Digital Signature	The result of a transformation of data by means of a cryptographic system using keys such that a person who receives the initial data can determine whether: 1. The transformation was created using the key that corresponds to the signer's key; and 2. The data has been altered since the transformation was made.
TWDC Business Partner	A TWDC PKI subscriber who is issued a certificate through a TWDC Business Liaison requesting a certificate on their behalf. A Business Partner will typically be performing operations functions (e.g., administration of a web site) on behalf of TWDC.
End entity	An Entity that uses the keys and certificates created within a public key infrastructure for purposes other than the management of keys and certificates. An End entity may be a Subscriber, a Relying Party, or a device, a role or an application.
Enrollment	A process by which an individual or an organization registers to receive a certificate and/or cryptographic keys for use within the TWDC PKI.
Entity	Any autonomous element within the PKI. This may be a CA, a trusted role within a CA, an RA or an End entity.
Non-repudiation	In a legal context, non-repudiation means sufficient evidence to persuade an adjudicator as to the origin and data integrity of digitally signed data, despite an attempted denial by the purported sender. In a technical context, non-repudiation refers to the assurance a Relying Party has that if a public verification key is used to validate a digital signature, that signature had to have been made by the corresponding private signing key.
Object Identifier	The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.
PKI Policy Management Authority	The Authority responsible for the maintenance of the CP and CPS.
Public Key Infrastructure	A set of policies, processes, server platforms, software and workstations used for the purpose of managing certificates and keys.
PKI Administrator	An individual who is responsible for the management of the Subscriber initialization process; the creation, renewal or revocation of certificates and the distribution of tokens (where applicable).
Registration Authority	A person, entity or organization that is responsible for the identification and authentication of Subscribers and other End Entities, but does not sign or issue the certificates. An RA may be asked to perform certain tasks by the CA.
Relying Party	With respect to certificates issued under this CPS, a Relying Party is an individual, entity or organization external to TWDC that relies on a certificate for establishing an SSL session with a TWDC end entity.

Repository	A system where CRLs, ARLs and public key certificates are stored for access by End Entities and Relying Parties. An LDAP directory is an example of a repository.
Subscriber	An individual or organization whose public key certificates are signed by the CA operating under these Certificate Policies.

1.6.1 List of Acronyms

ARL	Authority Revocation List
CA	Certificate Authority
CDP	CRL Distribution Point
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Subscriber Agreement
DCH	Designated Certificate Holder
DN	Distinguished Name
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HA	High Availability
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP over SSL
HSM	Hardware Security Module
IDS	Intrusion Detection System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
NIPS	Network Intrusion Prevention System
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PPMA	PKI Policy Management Authority
PKI	Public Key Infrastructure
PPMA	PKI Policy Management Authority
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request for Comment
RSA	Rivest-Shamir-Adleman

SAN	Storage Area Network
SPSE	Secure Personal Security Environment
SSL	Secure Sockets Layer
TA	Trusted Agent
TWDC	TWDC
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
US	United States

2 Publication and Repository Responsibilities

2.1 Repositories

The TWDC CAs shall publish issued certificates and its CRL to the LDAP based TWDC Enterprise Directory. Where used, the term "Repository" shall refer to this directory, including all required components for certificate and CRL publication.

Relying Parties shall access TWDC PKI CRLs published on the Certificate Distribution Point (CDP) hosted on *http://crl.disney.com/CRLs*, which shall be accessible on the public Internet and on the Global Disney Network. These CRLs shall be available 24/7 under normal conditions.

The TWDC Root CA certificate shall be published at
HTTP://crl.disney.com/AIA/CertsIssuedToDisneyRootCA.p7c

The TWDC Issuing CA certificate shall be published at
Http://crl.disney.com/AIA/CertsIssuedToDisneyIssuingCA.p7c.

2.2 Publication of Certification Information

The TWDC PKI CP and CPS shall be published internally within the TWDC corporate network. Publication of the CP and CPS shall be made available to all TWDC employees in a manner that requires the identification and authentication of the TWDC employee. The TWDC PKI CP shall also be publicly accessible at the following location:

http://crl.disney.com/CP/DisneyCP.pdf

By default, TWDC will not hand out its Certification Practice Statement to external entities. Exceptions will require approval from the PPMA.

2.3 Time or Frequency of Publication

The TWDC CAs shall publish to the Repository at least once every 24 hours. Publication shall include certificate and CRL information.

2.4 Access Controls on Repositories

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The TWDC CAs shall issue certificates with subject names that follow the X.501 Distinguished Name (DN) form. In the case of SSL certificates, the Common Name shall be the fully distinguished domain name of the subscribing end entity. Certificates of the same type shall have similar subject names that adhere to the naming conventions established by TWDC PKI.

In the case of code signing certificates, the Common Name shall be a unique identifier selected by the DCH. However the DCH email address shall be incorporated in the code signing certificate subject alternate name.

3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

When DNs are used, it is preferable that the common name represents the Subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter). Under typical legal frameworks devices, applications and roles cannot have legal names; therefore, the RA shall ensure that a record is retained of the person who owns the Certificate on behalf of the device, application or role.

For code signing certificates, the common name shall contain a unique identifier selected by the DCH. However, the DCH's email address shall be incorporated in the code signing certificate Subject Alternate Name.

CAs shall not issue certificates to the subscribers that contain domain names, IP addresses, DN, URL, and/or e-mail addresses that the subscribers do not legitimately own or control. Examples of fields and extensions where these names appear include subject DN and subject alternative names.

Application Note: Above general prohibition naturally also covers the case when the certificate can be used for Man in the Middle insertion or Traffic Interception and Management.

3.1.3 Anonymity or Pseudonymity of Subscribers

The TWDC PKI does not support the use of pseudonyms in subscriber common names at the exception of code signing certificates that may contain an identifier selected by the DCH. However, for this specific certificate type, the DCH's email address shall be incorporated in the code signing certificate subject alternate name.

3.1.4 Rules for Interpreting Various Name Forms

3.1.5 Uniqueness of Names

The TWDC CAs shall issue certificates with subject names that are unique to the certificate recipient.

3.1.6 Recognition, Authentication, and Role of Trademarks

The TWDC CAs shall not violate the trademark rights of third parties.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

3.2.2 Authentication of Organization Identity

The identity of the Applicant requesting a certificate representing an organization shall be verified by the RA, LRA or TA using credentials securely stored in TWDC repositories approved by the PPMA. These credentials can be transmitted by the Applicant to the RA, LRA or TA using online methods, in person or over the phone.

3.2.3 Authentication of Individual Identity

The identity of the Certificate Applicant shall be verified by the RA, LRA or TA using credentials securely stored in TWDC repositories approved by the PPMA. These credentials can be transmitted by the Certificate Applicant to the RA, LRA or TA using online methods, in person or over the phone.

The Certificate Applicants can also be authenticated by the RA, LRA or TA using their TWDC email addresses.

3.2.4 Non-verified Subscriber Information

The TWDC Issuing CA shall verify all Subscriber information that is relevant to the identification or authentication of the Subscriber.

3.2.5 Validation of Authority

The authority to request a TWDC PKI certificate shall be granted to:

- All persons who are provisioned in the TWDC Enterprise Directory.
- All persons who are provisioned with a valid TWDC email address.
- All computers member of the TWDC Active Directory forest and assigned a Group Policy Object allowing Certificate enrollment.

The RA or LRA shall be responsible for performing a verification of authority prior to accepting a certificate application.

3.2.6 Criteria for Interoperation

The TWDC Issuing CA shall interoperate only with the TWDC Root CA. Interoperation with other Certification Authorities shall be provided through the TWDC Root CA.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

The TWDC CAs shall require the same identification and authentication requirements for routine certificate re-key as the requirements for the initial enrollment for the certificate.

3.3.2 Identification and Authentication for Re-key after Revocation

The TWDC CAs shall require the same identification and authentication requirements for certificate re-key after revocation as the requirements for the initial enrollment for the certificate.

3.4 Identification and Authentication for Revocation Request

The TWDC CAs shall apply the same identification and authentication validation procedures for certificate application requests to certificate revocation requests.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The following TWDC applicants shall be allowed to apply for certificates:

- All persons who are provisioned in the TWDC Enterprise Directory.
- All persons who are provisioned with a valid TWDC email address.
- All computers member of the TWDC Active Directory forest and assigned a Group Policy Object allowing Certificate enrollment.

The TWDC applicants may apply for a certificate provided that the intended usage of the certificate complies with this Certificate Policy.

4.1.2 Enrollment Process and Responsibilities

The enrollment process and responsibilities, including certificate application processing, certificate issuance, and certificate acceptance, shall be described in the TWDC PKI Certification Practice Statement.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.2 Approval or Rejection of Certificate Applications

4.2.3 Time to Process Certificate Applications

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

4.4.2 Publication of the Certificate by the CA

The TWDC CAs shall publish certificates to the TWDC PKI Repository (see section 2.1).

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The TWDC CAs shall not notify entities, other than the above mentioned Repository, of certificate issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

4.5.2 Relying Party Public Key and Certificate Usage

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

4.6.2 Who May Request Renewal

4.6.3 Processing Certificate Renewal Requests

4.6.4 Notification of New Certificate Issuance to Subscriber

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

4.6.6 Publication of the Renewal Certificate by the CA

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

The TWDC Root CA shall permit certificate re-key under the following conditions:

- Current certificate is in the process of expiring.

The TWDC Issuing CA shall permit certificate re-key under the following conditions:

- Current certificate has expired or is in the process of expiring;
- Current certificate is allowed re-instantiation after revocation;
- Current certificate private keys has been compromised;
- Current certificate private key has been lost or is irrecoverable; or
- Current certificate requires an update or modification of information.

4.7.2 Who May Request Certification of a New Public Key

4.7.3 Processing Certificate Re-keying Requests

The TWDC CAs shall process certificate re-keying requests in a manner similar to the processing of the initial certificate application.

4.7.4 Notification of New Certificate Issuance to Subscriber

The TWDC CAs shall notify the Subscriber of the issuance of a re-keyed certificate under the same process for notifying a first-time Subscriber of a newly issued certificate.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The actions constituting the acceptance of a re-keyed certificate shall be the same as the actions that constituted the acceptance of the initial certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

The TWDC CAs shall publish re-keyed certificates in the same repository entry of the original certificate. The original certificate shall be archived as it is replaced.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The TWDC CAs shall not notify entities, other than the above mentioned Repository, of certificate re-key.

4.8 Certificate Modification

The TWDC CAs shall not modify certificates without issuing a new certificate through certificate re-key.

4.8.1 Circumstance for Certificate Modification

No stipulation. The TWDC PKI does not support certificate modification.

4.8.2 Who May Request Certificate Modification

No stipulation. The TWDC PKI does not support certificate modification.

4.8.3 Processing Certificate Modification Requests

No stipulation. The TWDC PKI does not support certificate modification.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation. The TWDC PKI does not support certificate modification.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation. The TWDC PKI does not support certificate modification.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation. The TWDC PKI does not support certificate modification.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation. The TWDC PKI does not support certificate modification.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.2 Who Can Request Revocation

4.9.3 Procedure for Revocation Request

4.9.4 Revocation Request Grace Period

Subscribers shall place a revocation request within four (4) hours of the time of discovery of a key compromises or certificate usage abuse. For other reasons leading to the need for revocation, the certificate revocation request shall be placed within 24 hours.

4.9.5 Time within which CA Must Process the Revocation Request

The TWDC CAs shall process a certificate revocation request within 24 hours from the time of request.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties shall perform revocation checking through the access of TWDC published CRLs, which shall be made accessible as described in section 2.1.

4.9.7 CRL Issuance Frequency

4.9.8 Maximum Latency for CRLs

4.9.9 On-line Revocation/Status Checking Availability

The TWDC PKI does not support on-line revocation/status checking availability, such as through the online certificate status protocol (OCSP).

4.9.10 On-line Revocation Checking Requirements

No stipulation. The TWDC PKI does not support on-line revocation/status checking availability.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation. The TWDC PKI does not support other forms of revocation advertisements.

4.9.12 Special Requirements re: Re-key Compromise

In the event that certificates are re-keyed due to key compromise, the TWDC Issuing CA shall revoke the original certificate immediately and initiate an investigation to determine the cause of the key compromise.

4.9.13 Circumstances for Suspension

Suspension shall be permitted only for user certificates; end entity certificates shall be revoked.

The TWDC Issuing CA shall permit suspension of user certificates under the following conditions:

- The subscribing end entity requires a temporary halt to its service due to business reasons; or
- The certificate needs to be placed under suspension for the purpose of investigation.

4.9.14 Who Can Request Suspension

The TWDC Issuing CA shall permit the authorities entitled to request certificate revocation, outlined in section 4.9.2, to request for certificate suspension.

4.9.15 Procedure for Suspension Request

The TWDC Issuing CA shall endorse the same procedures for handling certificate revocation to handle the suspension of certificates.

4.9.16 Limits on Suspension Period

The TWDC Issuing CA shall allow certificates to be suspended for a maximum of 180 days, at which time the status of the suspended certificate shall be reviewed for either full revocation or continued suspension with proper business justification.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Refer to section 4.9.

4.10.2 Service Availability

Refer to section 2.1.

4.10.3 Optional Features

No stipulation. The TWDC PKI does not support optional features for certificate status services.

4.11 End of Subscription

The TWDC Issuing CA shall consider the revocation or expiration of a certificate without a following request for the re-key and issuance of a new certificate as the termination of the Subscriber's certificate subscription.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

5 Facility Management, and Operational Controls

The TWDC CAs shall be operated under the controls stipulated in the *EMS CCP*.

5.1 Physical Controls

5.1.1 Site Location and Construction

5.1.2 Physical Access

5.1.3 Power and Air Conditioning

5.1.4 Water Exposures

5.1.5 Fire Prevention and Protection

5.1.6 Media Storage

5.1.7 Waste Disposal

5.1.8 Off-site Backup

5.2 Procedural Controls

5.2.1 Trusted Roles

In addition to what is stipulate in the EMS CCP, TWDC defines the following Trusted Roles:

- TWDC Registration Authority
- TWDC Local Registration Authority

5.2.2 Number of Persons Required per Task

5.2.3 Identification and Authentication for Each Role

5.2.4 Roles Requiring Separation of Duties

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

5.3.2 Background Check Procedures

5.3.2.1 Entrust EMS Trusted Roles

As per section 5.3.2 of the EMS CCP.

5.3.2.2 TWDC Trusted Roles

Background checks shall be conducted on the TWDC trusted Roles (RA and LRAs) upon hire and as requested by the Disney PPMA.

A background investigation shall cover the following areas:

- Employment;
- Criminal background check.

If the trustworthiness of an individual filling a Trusted Role is questioned, the individual shall be removed from the sensitive position while the problem is being investigated. Based on the outcome of the investigation, the PPMA may re-instate the individual in the Trusted Role or permanently remove them from their Trusted Role.

5.3.3 Training Requirements

In addition to what is stipulated in the EMS CCP, all TWDC personnel and contractors performing duties with respect to the operation of the CA or RA or LRA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA and RA security principles and mechanisms;
- All PKI software versions in use on the RA system;
- All PKI duties they are expected to perform; and
- Stipulations of this policy.

5.3.4 Retraining Frequency and Requirements

In addition to what is stipulated in the EMS CCP, TWDC individuals and contractors responsible for CA, RA and LRA roles shall be aware of changes in the CA and RA operation. Any significant change to the operations shall include the appropriate training**.** Examples of such changes are RA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

5.3.6 Sanctions for Unauthorized Actions

In addition to what is already stipulated in the EMS CCP, the PPMA shall take appropriate administrative and disciplinary actions against TWDC personnel and contractors who have performed actions involving the CA or its repository not authorized in this CP, the CPS, or other procedures approved and published by the PPMA. The CPS shall describe the sanctions or sanctions process such that personnel and contractors are clearly aware of consequences for unauthorized actions while meeting their obligations.

5.3.7 Independent Contractor Requirements

In addition to what is stipulated in the EMS CCP.

TWDC Contractor personnel employed to perform functions pertaining to the CA shall meet applicable requirements as set forth in this policy. Contracts providing personnel that serve in the Trusted Roles defined in this CP shall explicitly cite compliance with this CP, the applicable CPS, the TWDC Operations Manual and other references necessary to ensure that personnel are contractually bound to serve in their roles responsibly.

5.3.8 Documentation Supplied to Personnel

In addition to what is stipulated in the EMS CCP.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

In addition to what is stipulated in the EMS CCP, the TWDC shall record the information collected by its RA during the following certificate management operations:

- Certificate requests;
- Verification of certificate requests;
- Certificate renewal and rekey requests; and
- Certificate suspension and revocation requests.

5.4.2 Frequency of Processing Log

In addition to what is stipulated in the EMS CCP, the TWDC PKI Services Group shall review the audit logs generated by the on premise RA applications as requested by the Disney PPMA.

At a minimum, a statistically significant set of security audit data generated by the RA applications, since the last review, shall be examined, as well as a reasonable search for any evidence of malicious activity. The TWDC PKI Services Group shall explain all significant events in an audit log summary.

At a minimum, review shall involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any logged alerts or irregularities that might have an impact on the overall security and/or trustworthiness of the PKI. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Log

5.4.4 Protection of Audit Log

5.4.5 Audit Log Backup Procedures

5.4.6 Audit Collection System

5.4.7 Notification to Event-Causing Subject

5.4.8 Vulnerability Assessments

5.5 Records Archival

5.5.1 Types of Records Archived

In addition to what is stipulated in the EMS CCP, the TWDC shall archive audit log data generated during the following certificate lifecycle activities:

- Certificate requests;
- Verification of certificate requests;
- Certificate renewal and rekey requests; and
- Certificate suspension and revocation requests.

5.5.2 Retention Period for Archive

5.5.3 Protection of Archive

5.5.4 Archive Backup Procedures

5.5.5 Requirements for Time-stamping of Records

5.5.6 Archive Collection System (Internal or External)

5.5.7 Procedures to Obtain and Verify Archive Information

5.6 Key Changeover

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

In addition to what is stipulated in the EMS CCP:

The PPMA shall be notified if any CAs and RAs operating under this policy experience the following:

- Suspected or detected compromise of the CA and RA systems;

- Suspected or detected compromise of the Repository;
- Physical or electronic penetration of CA and RA systems;
- Successful denial of service attacks on CA and RA components; or
- Any incident preventing the CA from issuing a CRL prior to the time specified in the next update field of its currently valid ARL/CRL.

The PPMA take appropriate steps to protect the integrity of TWDC PKI. The CA's PPMA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

5.7.3 Entity Private Key Compromise Procedures

5.7.4 Business Continuity Capabilities after a Disaster

5.8 CA or RA Termination

The PPMA shall designate a TWDC entity as the custodian of all TWDC PKI archived data in the event of termination.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.2 Private Key Delivery to Subscriber

6.1.3 Public Key Delivery to Certificate Issuer

6.1.4 CA Public Key Delivery to Relying Parties

If a Relying Party requires the TWDC CA Certificates for the facilitation of building trusted certificate chains, the Certificates may be downloaded from the following public Internet locations.

http://crl.disney.com/AIA/CertsIssuedToDisneyRootCA.p7c

http://crl.disney.com/AIA/CertsIssuedToDisneyIssuingCA.p7c

6.1.5 Key Sizes

TWDC CA and RA certificate key-pairs shall use 2048-bit RSA.

Subscriber certificate key-pairs shall use 2048-bit RSA.

6.1.6 Public Key Parameters Generation and Quality Checking

6.1.7 Key Usage Purposes

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

6.2.2 Private Key Multi-Person Control

6.2.3 Private Key Escrow

6.2.4 Private Key Backup

6.2.5 Private Key Archival

6.2.6 Private Key Transfer into or from a Cryptographic Module

6.2.7 Private Key Storage on Cryptographic Module

6.2.8 Method of Activating Private Key

6.2.9 Method of Deactivating Private Key

6.2.10 Method of Destroying Private Key

6.2.11 Cryptographic Module Rating

Refer to Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The key-pair for a certificate issued by the TWDC PKI shall only be valid during the operational lifetime of the certificate.

Certificates shall be issued with the following maximum lifetimes:

- TWDC CA signing certificates shall have a maximum lifetime of twenty (20) years after the date of issuance.
- RA and Subscriber signing certificates issued with 2048-bit RSA keys shall have a maximum lifetime of three (3) years after the date of issuance.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.2 Activation Data Protection

6.4.3 Other Aspects of Activation Data

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

6.5.2 Computer Security Rating

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

6.6.2 Security Management Controls

6.6.3 Life Cycle Security Control

6.7 Network Security Controls

In addition to what is stipulated in the EMS CCP.

A review of the TWDC PKI networking environment shall be performed as requested by the PPMA.

6.8 Time-stamping

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The TWDC CAs shall issue all certificates in the X.509 Version 3 certificate format. Certificate fields supported by TWDC CAs shall abide by the following requirements:

Certificate Field	**Requirements**
Version	X.509 Version 3
Serial Number	Each certificate shall receive a unique serial number.
Signature	The signature algorithm shall use RSA with SHA-1 or SHA-256.
Issuer	TWDC Root CA Distinguished Name: {*CN=The Walt Disney Company Root CA, ou=TWDC-PKI, dc=disney, dc=com*} TWDC Issuing CA Distinguished Name: {*CN=The Walt Disney Company Issuing CA, ou=TWDC-PKI, dc=disney, dc=com*}
Validity	The certificate validity time periods are specified in section 6.3.2
Subject	The subject Distinguished Name shall conform to the certificate subject naming conventions of the TWDC PKI CP.
Subject Public Key	The subject public key shall contain the secure hash algorithm identifier and the certificate public key.
Extensions	Refer to section 7.1.2 below.

7.1.1 Version Number

The TWDC CAs shall issue X.509 Version 3 certificates.

7.1.2 Certificate Extensions

The TWDC CAs shall support the following extensions when issuing certificates:

Certificate Extension	**Criticality**
Basic Constraints	Critical
CRL Distribution Points	Non Critical
Key Usage	Non Critical
Authority Information Access	Non Critical
Authority Key Identifier	Non Critical
Subject Key Identifier	Non Critical
Subject Directory Attributes	Non Critical
Subject Alternative Name	Non Critical

Certificate Extension	Criticality
Private Key Usage	Non Critical
Certificate Policies	Non Critical
Entrust Version Info	Non Critical

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use at least one the following OIDs for signatures:

Signature Algorithm Identifier	OID
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1 }
RSA with PSS padding	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-SHA224	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) ecdsa-with-SHA2(3) 1}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) ecdsa-with-SHA2(3) 2}

7.1.4 Name Forms

The TWDC CAs shall issue certificates using the Distinguished Name of the certificate subject.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Certificates issued by the TWDC CAs shall contain the policy OID assigned to the CP as described in Section 1.2. The publicly accessible location of this document, as described in Section 2.2, shall be included with the policy OID.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

The TWDC CAs shall issue all Certificate Revocation Lists in the X.509 Version 2 certificate format. CRL fields supported by TWDC CAs shall abide by the following requirements:

CRL Field	**Requirements**
Version	Version 2
Signature	The signature algorithm shall use RSA with SHA-1 or SHA-256.
Issuer	TWDC Root CA Distinguished Name: {*CN=The Walt Disney Company Root CA, ou=TWDC-PKI, dc=disney, dc=com*} TWDC Issuing CA Distinguished Name: {*CN=The Walt Disney Company Issuing CA, ou=TWDC-PKI, dc=disney, dc=com*}
This Update	The effective date shall indicate the CRL's time of issuance.
Next Update	The next update date shall indicate the next expected CRL update which shall be approximately 24 hours after the time of the last CRL issuance.
Extensions	Refer to section 7.2.2 below.

7.2.1 Version Number

The TWDC CAs shall only issue CRLs in the X.509 Version 2 format.

7.2.2 CRL and CRL Entry Extensions

The TWDC CAs shall use the following X.509 CRL extensions and entry extensions:

CRL Extension	**Criticality**
CRL Number	Non Critical
Authority Key Identifier	Non Critical
CRL Entry Extension	**Criticality**
Reason Code	Non Critical
Invalidity Date	Non Critical

7.3 OCSP Profile

7.3.1 Version Number

The TWDC PKI does not use OCSP.

7.3.2 OCSP Extensions

The TWDC PKI does not use OCSP.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

In addition to what is stipulated in the EMS CCP:

The TWDC Internal Audit Group shall perform an annual self-assessment of the RA function.

8.2 Identity/Qualifications of Assessor

In addition to what is stipulated in the EMS CCP:

The TWDC PPMA shall be responsible for identifying and engaging a qualified auditor for the self-assessment of its RA function.

8.3 Assessor's Relationship to Assessed Entity

In addition to what is stipulated in the EMS CCP:

The TWDC PPMA shall be responsible for identifying and engaging a qualified auditor for the self-assessment of its RA function.

8.4 Topics Covered by Assessment

In addition to what is stipulated in the EMS CCP:

The purpose of an RA self-assessment shall be to verify that the TWDC RA function comply with all of the requirements of the current version of this policy and the CA's CPS. All aspects of the RA operation shall be subject to the RA self-assessment.

If no significant changes to policies, procedures or operations have occurred during the previous year, a delta self-assessment of the RA function is acceptable in lieu of a full compliance self-assessment. A delta self-assessment covers all changes to policies, procedures, or operations that have occurred during the previous year. Examples of significant changes include, but are not limited to:

- Modifications to RA operating procedures;
- Modifications to the certificate policy.

The following topics must be addressed in a delta self-assessment even if no changes have occurred since the last full compliance audit:

- Personnel controls;
- Audit review frequency and scope;
- Types of events recorded in electronic audit logs;
- Protection of physical and electronic audit data; and
- Backup and Archive generation and storage.

8.5 Actions Taken as a Result of Deficiency

In addition to what is stipulated in the EMS CCP:

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the RA function, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the parties identified in this Policy of the discrepancy; and
- The party responsible for correcting the discrepancy shall propose a remedy, including expected time for completion, to the MSO PA and TWDC PPMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the MSO PA and TWDC PPMA may decide to halt temporarily operation of the affected CA, to revoke a certificate issued by the CA, or take other actions it deems appropriate. The MSO PA and TWDC PPMA shall develop procedures for making and implementing such determinations.

8.6 Communication of Results

In addition to what is stipulated in the EMS CCP:

A Self-Assessment Compliance Report, including identification of corrective measures taken or being taken by affected parties, shall be provided to the MSO PA and TWDC PPMA as set forth in this Policy or the applicable CPS. The MSO PA and TWDC PPMA may, at its discretion, require a special compliance audit to confirm the implementation and effectiveness of the remedy.

9 Other Business and Legal Matters

9.1 Fees

TWDC shall not charge fees for the issuance of certificates.

9.1.1 Certificate Issuance or Renewal Fees

9.1.2 Certificate Access Fees

9.1.3 Revocation or Status Information Access Fees

9.1.4 Fees for Other Services

9.1.5 Refund Policy

9.2 Financial Responsibility

TWDC denies any financial responsibilities for damages or impairments resulting from its operation.

9.2.1 Insurance Coverage

9.2.2 Other Assets

9.2.3 Insurance or Warranty Coverage for End-Entities

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Any information about subscribers that is not made public by the certificates issued by the TWDC PKI, CRLs, or the LDAP directory entry for the subscriber is considered confidential and will be not disclosed, nor is it required to disclose confidential information without an authenticated and justified request specifying:

1. The subscriber is requesting information about him/herself; or
2. A court order.

9.3.2 Information not within the Scope of Confidential Information

All information made public within a certificate issued by a TWDC CA or contained within the CRL shall not be considered confidential.

9.3.3 Responsibility to Protect Confidential Information

PKI participants that receive confidential information as part of the operational processes of the PKI shall secure all such information from compromise, and refrain from using it or disclosing it to third parties.

Any suspected compromise of confidential information must be reported immediately to the Corporate IT Security Policy Officer.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

9.4.2 Information Treated as Private

9.4.3 Information not Deemed Private

9.4.4 Responsibility to Protect Private Information

9.4.5 Notice and Consent to Use Private Information

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

9.4.7 Other Information Disclosure Circumstances

9.5 Intellectual Property Rights

TWDC owns and reserves all intellectual property rights associated with its databases, web sites, digital certificates, and any other publication originating at TWDC including this CP.

9.6 Representations and Warranties

There are no warranties, expressed or implied, to any subscriber of the TWDC PKI.

9.6.1 CA Representations and Warranties

9.6.2 RA Representations and Warranties

9.6.3 Subscriber Representations and Warranties

9.6.4 Relying Party Representations and Warranties

9.6.5 Representations and Warranties of Other Participants

9.7 Disclaimers of Warranties

There are no warranties, expressed or implied, to any subscriber of the TWDC PKI.

9.8 Limitations of Liability

Subscribers will have no claims against TWDC arising from the use of TWDC PKI certificates. In no event will TWDC be held liable for any losses, including direct and indirect, incidental, consequential, special, or punitive damages arising out of or relating to any certificate issued by the TWDC CAs.

9.9 Indemnities

Under no circumstance will TWDC be held liable for the misuse of a digital certificate by a subscriber. A subscriber is wholly responsible for the usage of their certificate as stipulated in the TWDC Certificate Subscriber Agreement.

9.10 Term and Termination

This CP is to remain active until superceded by newer revisions, or until the termination of the TWDC PKI. No provision in this CP may be terminated without review of the TWDC PKI Policy Management Authority (PPMA).

9.10.1 Term

9.10.2 Termination

9.10.3 Effect of Termination and Survival

9.11 Individual Notices and Communications with Participants

A subscriber is obligated to inform their RA (registrar), the PKI Services Group, or Corporate IT Security of any changes to their employment status, or any change in status that would affect the usage of their digital certificate.

An RA (registrar), PKI Administrator, or other sponsor of the PKI is required to notify Corporate IT Security and the PKI Services Group in the event of a change in their status, or any change in the status of their approved subscribers.

9.12 Amendments

The TWDC PPMA may amend these Certificate Policies/Procedures, or any part thereof, at any time at its discretion.

The TWDC PPMA is not obligated to notify any or all subscribers of the TWDC PKI of any amendments to this CP.

9.12.1 Procedure for Amendment

Prior to any amendment of these Certificate Policies, the TWDC PPMA will provide notice of any proposed change in writing to Corporate IT Security.

9.12.2 Notification Mechanism and Period

TWDC does not implement any specific notification mechanism to its subscribers.

9.12.3 Circumstances under Which OID Must be Changed

Change of the OID of this CP shall be decided upon on a case by case basis by the PPMA.

9.13 Dispute Resolution Provisions

The laws of the state of California, United States shall govern all aspects of the TWDC PKI.

9.14 Governing Law

The laws of the state of California, United States shall govern all aspects of the TWDC PKI.

9.15 Compliance with Applicable Law

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

9.16.2 Assignment

9.16.3 Severability

In the event that a court determines that a clause within this CP is, for some reason invalid or unenforceable, the remainder of this document remains in force.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

9.16.5 Force Majeure

Events compromising TWDC PKI services that are outside the control of TWDC shall be dealt with by the board of directors of TWDC.

9.17 Other Provisions