深圳 CA 全球信任体系

电子认证业务规则

深圳市电子商务安全证书管理有限公司

生效日期：2024年6月7日

SZCA Global-Trust System

Certification Practice Statement

Shenzhen Digital Certificate Authority Co., Ltd.

Commencement Date:June 7th ,2024

深圳CA全球信任体系
电子认证业务规则

(深圳CA全球信任体系CPS)

版本V2.1

2024年

https://www.szca.com

Shenzhen CA Global-Trust System

Certification Practice Statement

(SZCA Global-Trust System CPS)

Version: V2.1

2024

https://www.szca.com

版本控制表

文档名称	深圳 CA 全球信任体系电子认证业务规则	保密级别	公开
版本历史变更信息			
版本	**生效时间**	**审批者**	**主要内容**	**备注**
V1.0	2020 年 9 月 14 日	SZCA 运营安全管理小组	首次制定	试行
V1.1	2021 年 9 月 13 日	SZCA 运营安全管理小组		版本更新
V2.0	2021 年 12 月 31 日	SZCA 运营安全管理小组	更新证书更新、撤销等流程的表述，修改审计与评估等内容。	修订
V2.1	2024 年 6 月 7 日	SZCA 运营安全管理小组	更新公司地址、联系方式，及机房访问的身份验证方式	修订

Version Control Table

Document name	SZCA Global-Trust System Certification Practice Statement	**Confidentiality level**	Public
History of revision			
Version	**Effective date**	**reviewed by**	**Main content**	**Notes**
V1.0	September 14, 2020	SZCA Operational Security Management Team	First formulation	Tentative
V1.1	September 13, 2021	SZCA Operational Security Management Team		Version update
V2.0	December 31,2021	SZCA Operational Security Management Team	Update the statement of procedures of certificate renewal and cancellation, and modify the content of audit and evaluation.	Amendent
V2.1	June 7,2024	SZCA Operational	Update the address、contact	Amendent

		Security Management Team	information and the authentication method for computer room access	

目录 Contents

1. 概括性描述 Introduction

1.1 概述 Overview

深圳CA，全称深圳市电子商务安全证书管理有限公司（Shenzhen Digital Certificate Authority Center Co., Ltd.，英文简称 “SZCA”），成立于2000年8月。深圳CA于2006年8月通过审查获得国家密码管理局颁发的《电子认证服务使用密码许可证》，并于2007年10月获得原信息产业部颁发的《电子认证服务许可证》；且于2010年11月通过国家密码管理局电子政务电子认证服务能力评估，2012年通过卫生部的审核，分别取得电子政务、卫生系统电子认证服务资质。且上述服务资质均处于有效期内。

本SZCA全球信任体系电子认证业务规则（SZCA Global Trust Certificate Certification Practice Statement，以下简称“本CPS”），全面阐述SZCA在提供电子认证服务过程中所遵循的规范及准则，及电子认证服务相关参与者所承担的责任，是对于SZCA证书服务活动业务、技术、权利义务方面的声明和描述。

本CPS遵循 CA/B（证书机构与浏览器）论坛公布的最新版本的《公众可信证书签发管理基线要求》、《代码签名证书签发和管理基线要求》、《EV证书签发和管理指导准则》、《EV代码签名证书签发和管理指导准则》、Adobe 系统公司发布的最新版本AATL（Adobe 认可的信任列表）的技术要求、及web trust审计规范相关要求进行签发和管理公众可信任的证书，并将持续根据其发布的版本修订CPS，如果本CPS与CA/B论坛发布的相关标准规范中的条款有不一致的地方，则以CA/浏览器论坛正式发布的规范的内容为准。

本CPS 不仅严格约束SZCA的业务经营活动，并同样适用于订户、依赖方、及其他电子认证活动参与方。所有电子认证活动的参与方，都必须完整地理解和执行本CPS规定的条款，据此行使权利和承担义务。

SZCA的证书结构体系：

SZCA目前有SZCA ROOT CA（RSA）和SZCA SM2 ROOT CA（SM2）2个根证书，SZCA不签发外部中级CA证书。

1.SZCA ROOT CA

SZCA ROOT CA 的算法为RSA，密钥长度为 4096 bits，下设8个中级 CA 证书，其中：

（1）SZCA EV SSL CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的EV SSL服务器类证书；

（2）SZCA OV SSL CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的OV SSL服务器类证书；

（3）SZCA DV SSL CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的DV SSL服务器类证书；

（4）SZCA EV CodeSigning CA ，密钥长度为 4096 bits，签发密钥长度为RSA 3072 bits、4096 bits的EV代码签名证书；

（5）SZCA CodeSigning CA ，密钥长度为 4096 bits，签发密钥长度为RSA 3072 bits、4096 bits的代码签名证书；

（6）SZCA Secure E-Mail CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的电子邮件类证书；

（7）SZCA Overseas CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits、4096 bits的跨境个人证书、机构证书、设备证书；

（8）SZCA Business CA ，密钥长度为 4096 bits，签发密钥长度为RSA 2048 bits、3072 bits 、4096 bits的业务个人证书、机构证书、设备证书。

2.SZCA SM2 ROOT CA

SZCA SM2 ROOT CA的算法为SM2,下设6个中级CA证书：

（1）SZCA SM2 EV SSL CA，签发SM2算法的EV SSL服务器类证书；

（2）SZCA SM2 OV SSL CA，签发SM2算法的OV SSL服务器类证书；

（3）SZCA SM2 DV SSL CA，签发SM2算法的DV SSL服务器类证书；

（4）SZCA SM2 Secure E-mail SSL CA，签发SM2算法的电子邮件类证书；

（5）SZCA SM2 Overseas CA，签发SM2算法的跨境个人证书、机构证书、设备证书；

（6）SZCA SM2 Business CA，签发SM2算法的业务个人证书、机构证书、设备证书。

Shenzhen Digital Certificate Authority Center Co., Ltd. (hereinafter referred to as “SZCA”) was founded in August 2000. SZCA has passed the examination in August 2006 and obtained the *Permit for Use of Cipher Codes for Electronic Certification Services* issued by the State Cryptography Administration (SCA), and obtained the *Permit for Electronic Certification Services* issued by the former Ministry of Information Industry in October 2007; and has passed the assessment of e-government electronic certification service capability of the State Cryptography Administration in November 2010 and passed the review of the Ministry of Health in 2012, and obtained the electronic certification service qualifications for e-government and health system respectively. The above service qualifications are still within the validity period.

The SZCA Global-Trust System Certification Practice Statement (hereinafter referred to as the “CPS") fully describes the specifications and guidelines to be followed by SZCA in the provision of electronic certification services as well as the responsibilities of the participants involved in the electronic certification services. It is the statements and descriptions on the activities, technologies and rights & obligations of the SZCA certification services.

The CPS complies with the latest version of the *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*, the *Baseline Requirements for the Issuance and Management of Code Signing Certificates*, the *Guidelines for the Issuance and Management of EV Certificates*, the *Guidelines for the Issuance and Management of EV Code Signing Certificates* published by CA/B (Certificate Authority and Browser) Forum, the technical requirements in the latest version of the Adobe Approved Trusted List (AATL) published by Adobe Systems Incorporated, as well as relevant requirements in web trust audit norm to issue and manage the publicly-trusted certificates, and will continue to revise the CPS in accordance with the issued versions. In case of any inconsistency between the terms of the CPS and relevant standards and specifications published by the CA/B Forum, the specifications officially published by the CA/Browser Forum shall prevail.

The CPS not only strictly restricts SZCA's business operations, but also applies to subscribers, relying parties and other participants in electronic certification activities. All participants in electronic certification activities must fully understand and implement provisions of the CPS, and thereby exercise their rights and obligations.

SZCA certificate structure system:

SZCA currently has two root certificates: SZCA ROOT CA (RSA) and SZCA SM2 ROOT CA (SM2), and SZCA does not issue any external subordinate CA certificate.

1. SZCA ROOT CA

SZCA ROOT CA adopts RSA algorithm with a key length of 4096 bits, and includes eight subordinate CA certificates, in which:

(1) SZCA EV SSL CA with a key length of 4096 bits is used to issue EV SSL server certificates with a key length of RSA 2048 bits, 3072 bits and 4096 bits;

(2) SZCA OV SSL CA with a key length of 4096 bits is used to issue OV SSL server certificates with a key length of RSA 2048 bits, 3072 bits and 4096 bits;

(3) SZCA DV SSL CA with a key length of 4096 bits is used to issue DV SSL server certificates with a key length of RSA 2048 bits, 3072 bits and 4096 bits;

(4) SZCA EV CodeSigning CA with a key length of 4096 bits is used to issue EV code signing certificates with a key length of RSA 3072 bits and 4096 bits;

(5) SZCA CodeSigning CA with a key length of 4096 bits is used to issue code signing certificates with a key length of RSA 3072 bits and 4096 bits;

(6) SZCA Secure E-Mail CA with a key length of 4096 bits is used to issue email certificates with a key length of RSA 2048 bits, 3072 bits and 4096 bits;

(7) SZCA Overseas CA with a key length of 4096 bits is used to issue cross-border personal certificates, organization certificates and equipment certificates with a key length of RSA 2048 bits, 3072 bits and 4096 bits;

(8) SZCA Business CA with a key length of 4096 bits is used to issue business personal certificates, organization certificates and equipment certificates with a key length of RSA 2048 bits, 3072 bits and 4096 bits.

2. SZCA SM2 ROOT CA

SZCA SM2 ROOT CA adopts SM2 algorithm, and includes six subordinate CA certificates:

(1) SZCA SM2 EV SSL CA is used to issue EV SSL server certificates of SM2 algorithm;

(2) SZCA SM2 OV SSL CA is used to issue OV SSL server certificates of SM2 algorithm;

(3) SZCA SM2 DV SSL CA is used to issue DV SSL server certificates of SM2 algorithm;

(4) SZCA SM2 Secure E-mail SSL CA is used to issue email certificates of SM2 algorithm;

(5) SZCA SM2 Overseas CA is used to issue cross-border personal certificates, organization certificates and equipment certificates of SM2 algorithm;

(6) SZCA SM2 Business CA is used to issue business personal certificates, organization certificates and equipment certificates of SM2 algorithm.

1.2 文档名称与标识 Document Name and Identification

本 CPS 名称为《深圳 CA 全球信任体系电子认证业务规则》，英文名称为 Shenzhen CA Global Trust Certification Practices Statement，简称 SZCA CPS、本 CPS。

The name of the CPS is the *Shenzhen CA Global-Trust System Certification Practice Statement* (SZCA CPS for short).

1.3 电子认证活动参与者 PKI Participants

1.3.1 电子认证服务机构 Certification Authorities

SZCA，作为合法第三方电子认证服务机构，负责证书签发、更新、吊销等证书管理，提供证书查询、证书黑名单（又称证书撤销列表或CRL）发布、证书策略制定等工作。

As a legal third-party electronic certification authority, SZCA is responsible for certificate management including certificate issuance, renewal and revocation , certificate status information services, release of certificate blacklist (also known as certificate revocation list or CRL), and certificate policy formulation, etc.

1.3.2 注册机构 Registration Authorities

SZCA的注册机构（Registration Authority,简称“RA”）负责订户证书的申请受理、审核（包括身份标识与鉴别）和管理，是经SZCA正式授权后的业务分支机构，包括证书注册审核中心（RA）、证书本地受理点（LRA）等。

Registration Authority of SZCA (hereinafter referred to as the “RA”) is responsible for the acceptance, review (including identification and authentication) and management of certificate applications for subscribers, and is a business branch duly authorized by SZCA, including the Certificate Registration Authority (RA), Certificate Local Registration Authority (LRA), etc.

1.3.3 订户 Subscribers

订户是指向 SZCA 申请证书的实体，通常为个人、机构。证书主体是与证书信息绑定的实体，包括基础设施的组成部件如路由器、防火墙、服务器或用于安全通信的其他设备。

A subscriber is an entity that applies certificates to SZCA and can be an individual or an organization. The subject of the certificate is the entity which the certificate is bound to, including infrastructure components such as routers, firewalls, servers or other equipment for secure communication.

1.3.4 依赖方 Relying Parties

依赖方是指信赖于证书、或其电子签名等所证明的相关事实（包括身份和信息数据）、行为的真实性，并依此进行业务活动的实体。依赖方可以是订户、也可以不是订户。

A relying party is the entity that acts on the authenticity of relevant facts (including identity and information data) and the behavior proven by the certificate or its electronic signature. The relying party may or may not be a subscriber.

1.3.5 其他参与者 Other Participants

其他参与者是指为 SZCA 的电子认证活动提供相关服务的其他实体。

Other participants refer to other entities that provide relevant services for SZCA's electronic certification activities.

1.4 证书应用 Certificate Usage

1.4.1 适合的证书应用 Appropriate Certificate Uses

SZCA 的订户证书可以广泛应用在电子政务、电子商务及其他社会化活动中，以实现身份认证、电子签名、关键数据加密等目的，同时也确保互联网上信息传递双方身份的合法性和真实性以及信息的完整性和保密性。

订户可以根据实际需要，自主判断和决定采用相应合适的证书类型，不同的证书具有不同的应用范围。

SZCA's subscriber certificate can be widely applied in e-government, e-commerce and other social activities to achieve the purposes of identity authentication, electronic signature, key data encryption, etc., as well as to ensure the validity and authenticity of the identities of both parties transferring information on the Internet and the integrity and confidentiality of the information.

Subscribers can independently judge and decide to adopt appropriate certificate types according to actual needs, and different certificates have different application scopes.

1.4.2 限制及禁止的证书应用 Restricted and Prohibited Certificate Uses

SZCA签发的证书禁止应用于任何违反国家法律、法规或破坏国家安全的情形，也不能用于SZCA与订户约定的证书禁止应用范围，否则由此造成的法律后果由订户自行承担。

各类证书都只能应用于证书所代表的主体身份适合的用途，订户证书的密钥用法在证书

的扩展项中进行了限制。然而基于扩展项限制的有效性取决于应用软件，如果参与方不遵守相关约定其对证书的应用超出本 CPS 限定的应用范围，将不受本CPS的保护。

证书不得应用于网络钓鱼攻击、网络诈骗或其他恶意犯罪行为，也不得应用于发布任何包含或疑似包含恶意代码的程序。

此外，证书不设计用于、不打算用于、也不授权用于危险环境中的控制设备，或用于要求防失败的场合，如核设备的操作、航天飞机的导航或通讯系统、空中交通控制系统或武器控制系统中，因为它的任何故障都可能导致死亡、人员伤害或严重的环境破坏。

The certificate issued by SZCA is forbidden to be used for any violation of national laws and regulations or damage to national security, nor shall it be applied to the prohibited application scope for certificates agreed between SZCA and the subscribers, otherwise the legal consequences incurred thereby shall be borne by the subscribers.

Various certificates can only be applied to the appropriate use of the subject identity represented by them, and the key use of the subscriber certificate is limited in the certificate extensions. However, based on that the validity of extension limit depends on the application software,if the participant does not comply with the relevant agreements, and its certificate application exceeds the application scope limited by the CPS, it will not be protected by the CPS.

The certificates are prohibited from being used for phishing attacks,fraudulent websites or other malicious criminal activities ,and releasing a program that contains or is suspected to contain malware.

In addition, the certificate is not designed, intended, or authorized to be used for control equipment in hazardous environments, or for occasions where failure prevention is required, such as operation of nuclear equipment, navigation or communication systems of spacecraft, air traffic control systems or weapon control systems, as any failure of them may result in death, personal injury or serious environmental damage.

1.5 策略管理 Policy Administration

1.5.1 策略文档管理机构 Organization Administering the Document

根据相关法律规定，SZCA指定“SZCA-CPS策略发展小组”负责CPS的起草、注册、维护和更新。“SZCA-CPS策略发展小组”由公司法务人员和技术人员组成，负责本CPS的日常管理及维护工作，包括一般性修订及负责有关本CPS及相关文件的疑问咨询工作。

According to relevant laws, SZCA designates the "SZCA-CPS Policy Development Team" to be responsible for the draft, registration, maintenance and update of CPS. The "SZCA-CPS Policy Development Team" consists of legal and technical personnel of the Company, who are responsible for the daily management and maintenance of the CPS, including general amendment, and consultation on the CPS and related documents.

1.5.2 联系人 Contact Person

任何有关 CPS 的问题、建议、疑问等，请与“SZCA-CPS 策略发展小组”联系：

部门：深圳市电子商务安全证书管理有限公司 SZCA-CPS 策略发展小组

电话：0755-26588388

电子邮件：kfzz@szca.com.com

邮寄地址：深圳市福田区梅林街道孖岭社区凯丰路 10 号翠林大厦 9 层 01、02、03、04-1、06、07、08 号房[518057]。

Please contact the SZCA-CPS Policy Development Team in case of any questions, suggestions or doubts related to the CPS:

Department: SZCA-CPS Policy Development Team of Shenzhen Digital Certificate Authority Center Co., Ltd.

Tel.: 0755-26588388

Email: kfzz@szca.com.com

Mailing address: Room 01, 02, 03, 04-1, 06, 07, 08, 9/F, Cuilin Building, No. 10 Kaifeng Road, Mailing Community, Meilin Street, Futian District, Shenzhen, China [518057].

1.5.3 决定 CPS 符合策略的机构 Organization Determining CPS Suitability for the Policy

“SZCA运营安全管理小组”是审批CPS（包含所有版本所有类型的CPS）、决定CPS是否符合对应证书策略的最高决策机构；由SZCA高级管理人员，核心技术人员和法律顾问组成。

The "SZCA Operational Safety Management Team" is the highest decision-making body to approve the CPS (including all versions of all types of CPS) and determine whether the CPS is in comformity with the corresponding certificate policy; and it consists of SZCA senior manager, core technical personnel and legal counsel.

1.5.4 CPS 批准程序 CPS Approval Procedures

“SZCA-CPS策略发展小组”负责起草和修订CPS形成讨论稿（或CPS修订内容），并征求各部门负责人意见，经讨论修改达成一致意见后形成送审稿，并确定文本格式和版本号形成定稿。

“SZCA-CPS策略发展小组”负责将定稿提交“SZCA运营安全管理小组”审阅。经该小组审议通过后，方可对外发布CPS。发布形式应符合行业标准，包括但不限于网上公布和向客户或合作对象书面提交。发布工作由“SZCA-CPS策略发展小组”协调相关部门完成，并将“SZCA运营安全管理小组”审批意见及CPS电子版存档。

本 CPS 每年至少修订、更新一次，并按上述程序报送审批、备案并发布实施。如无内容改动，则递增版本号、更新发布时间、生效时间及修订记录。

CPS公开发布在SZCA的官网https:www.szca.com,或通过其他方式向用户提供。自发布之

日起，各种形式提供的CPS必须与网站上CPS保持一致，“SZCA-CPS策略发展小组”负责依法在CPS公布之日起三十日内向工业和信息化部备案。

The SZCA-CPS Policy Development Team is responsible for drafting and revising the CPS to form a discussion draft (or CPS revision), soliciting the comments of the heads of various departments, forming a draft for review after discussion and amendment, and finalizing the text format and version number.

The SZCA-CPS Policy Development Team is responsible for submitting the final draft to the SZCA Operational Security Management Team for review. The CPS shall not be published until it is reviewed and approved by the SZCA Operational Security Management Team. The CPS shall be published in the form in accordance with industry standards, including but not limited to online publication and written submission to customers or partners. The SZCA-CPS Policy Development Team will complete CPS publication in coordination with relevant departments, and archive the approval opinoins of the SZCA Operational Security Management Team and the CPS electronic version.

The CPS is revised and updated at least once a year and then submitted for approval, filing and publication for implementation in accordance with the above procedures. If there is no change, SZCA will progressively increase the version number, and update the release time, effective time and revision history.

CPS is publicly published on SZCA's website https:www.szca.com or otherwise provided to users. The CPS provided in all forms must be consistent with the CPS on the website from the date of publication, and the "SZCA-CPS Policy Development Team" is responsible for filing with the Ministry of Industry and Information Technology within 30 days from the date of publication of the CPS as per laws.

1.6 定义和缩写 Definitions and Acronyms

表1.1-定义与缩写

缩写/名词	定义
电子认证服务机构	负责订户认证身份、签发公钥证书、管理证书密钥的第三方机构。
注册机构	RA面向订户，接受订户申请材料、审核订户材料，在订户的CA机构之间传递证书申请、审批及管理信息。
数字证书	经CA数字签名包含数字证书使用者身份公开信息和公开密钥的电子文件。
订户	申请证书的实体。
依赖方	基于对证书或者电子签名的信赖从事有关活动的人
电子认证业务规则/CPS	关于CA机构对证书、密钥等的全生命周期的管理活动的详细操作规范和业务操作实践的声明，包括认证技术、法律责任、认证业务等多方面的内容。
证书吊销（作废）列表/CRL	又称数字证书黑名单，指经CA签名的在证书有效期届满前被吊销而失效、不再受CA机构信任的证书的列表。
在线证书状态协议/OCSP	供实时查询、检查数字证书的状态信息。
LDAP	轻量级目录访问协议，用于查询、下载数字证书及数字证书吊销列表。
公钥	经由数学运算产生的密钥，可公开并可用于验证由其对应私钥产生的数字签名。公开密钥可依据其运算方法对文件、信息进行加密，并以对应的私钥进行解密。
私钥	经由数学运算产生的由持有者保管的密钥，可用于制作数字签名，亦可依据运算方式，对由其对应公钥加密的文件或信息进行解密。

SZCA	深圳市电子商务安全证书管理有限公司（Shenzhen Certificate Authority）
CPS策略发展小组	由SZCA任命的负责CPS的编制、修订、日常维护管理与咨询的组织。
SZCA运营安全管理小组	由SZCA任命的负责SZCA的CPS/CP核准及监督其执行的组织。
SZCA超级管理员	负责实施 CA的CP、设置或添加CA管理员、验证审计记录、管理CPS执行的角色、岗位。
SZCA系统管理员	负责安装、配置和维护CA系统的软硬件系统，及 CA服务器的启动和中止的角色、岗位。
SZCA录入员	负责录入证书申请者提交的信息。
SZCA审核员	负责审核证书申请信息。
SZCA证书制作员	负责为证书申请者制作证书。
SSL证书	是通过确认申请人对域名的所有权及控制权、认证该申请人的身份签发的证书。
代码签名证书	对代码开发、编写、发布人的身份进行认证后签发的证书，申请人用于对代码进行签名，保障代码的完整性、真实性。
甄别名	数字证书主体名称域中，用于唯一标识订户的名称，该名称需体现订户真实身份、具有实际意义的合法的名称。
PKI	公钥基础设施（Public Key Infrastructure）。
PKCS	公钥密码算法标准（Public Key Cryptography Standard）。

Table 1.1 - Definitions and Acronyms

Acronyms/Nouns	Definitions
Certification Authority/CA	A third-party organization responsible for subscriber identity authentication, issuance of public key certificates and management of

	certificate keys.
Registration Authority/RA	RA accepts subscriber application materials, reviews subscriber materials, and transmits certificate application, approval and management information between subscriber and CA.
Digital Certificate	Electronic documents with CA digital signature containing the public identity information and public key of the users of the digital certificates.
Subscriber	The entity applying for certificate.
Relying Party	Person engaged in relevant activities relying on trust in certificates or electronic signatures
Certification Practice Statement/CPS	Statement on detailed operating specifications and business operating practices of the CA for the whole life cycle management activities of certificates and keys, including certification technology, legal responsibility, certification business and other aspects.
Certificate Revocation List/ CRL	Also known as the blacklist of digital certificates, it refers to the list of certificates with signature of the CA that are revoked before the expiration of the validity period of the certificate and are no longer trusted by the CA.
Online Certificate Status Protocol/OCSP	Status information of digital certificates for real-time query and check.
LDAP	Lightweight Directory Access Protocol for query and download of digital certificates and digital certificate revocation lists.
Public Key	Keys generated by mathematical operations that can be published and used to verify the digital signatures generated by their corresponding private keys. The public key can encrypt files and information according to its operation method and its corresponding private key could be used to decrypt.

Private Key	Keys generated by mathematical operation and kept by the holder that can be used to produce digital signatures or to decrypt files or information encrypted by their corresponding public keys according to the operation method.
SZCA	Shenzhen Digital Certificate Authority Center Co., Ltd. (Shenzhen Certificate Authority)
CPS Policy Development Team	Organization appointed by SZCA for the compilation, revision, daily maintenance, management and consultation of CPS.
SZCA Operational Security Management Team	Organization appointed by SZCA for approval and implementation supervision of SZCA CPS/CP.
SZCA Super Administrator	Role responsible for implementing the CA CP, setting or adding the CA administrator, verifying the audit records, and managing the CPS implementation.
SZCA System Administrator	Role responsible for installing, configuring and maintaining the software and hardware systems of the CA system, as well as starting and stopping the CA server.
SZCA Entry Clerk	Role responsible for entering the information submitted by the certificate applicant.
SZCA Reviewer	Role responsible for reviewing certificate application information.
SZCA Certificate Maker	Role responsible for generation certificates for certificate applicants.
SSL Certificate	A certificate issued by confirming the applicant's ownership and control over the domain name and authenticating the applicant's identity.
Code Signing Certificate	A certificate issued after identity authentication of the code developer, writer and issuer, which is used by the applicant to sign the codes and

	ensure the integrity and authenticity of the codes.
Distinguished Name/DN	Legal name used to uniquely identify the subscriber name in the name domain of the digital certificate subject, which shall reflect the true identity of the subscriber and have practical significance.
PKI	Public Key Infrastructure.
PKCS	Public Key Cryptography Standard.

2. 信息发布与信息管理 Information Publication and Administration

2.1 信息库 Repositories

SZCA 信息库是对外公开的信息库，主要面向订户及证书应用依赖方提供信息服务。SZCA 信息库包括但不限于以下内容：证书、 CRL、 CPS、证书服务协议、技术支持手册、SZCA 网站信息以及 SZCA 不定期发布的信息。SZCA 信息库可通过 https://www.szca.com 或 SZCA 指定的其它方法访问、查询。

SZCA repositories are public repositories that provide information services for subscribers and relying parties of certificate application. SZCA repositories include, but are not limited to: certificate, CRL, CPS, certificate service protocols, technical support manuals, SZCA website information, and information published by SZCA from time to time. SZCA repositories can be accessed and queried by https://www.szca.com or other methods specified by SZCA.

2.2 认证信息的发布 Publication of Information

SZCA 在官方网站 https://www.szca.com 发布信息库，该网站是 SZCA 发布所有信息最首要、最及时、最权威的渠道。

SZCA 的 CPS 以及相关的技术支持信息等在 SZCA 网站上发布。用户可通过 SZCA 网站获取证书的信息和吊销证书列表；证书的实时状态信息也可通过 OCSP 服务查询。

同时，SZCA 也将会根据需要采取其他可能的形式进行信息发布。

SZCA publishes the repositories on the official website https://www.szca.com, which is the most primary, timely and authoritative channel of SZCA for publishing all information.

SZCA CPS and relevant technical support information are published on the SZCA website. The information of certificates and the certificate revocation lists can be obtained by user on the

SZCA website; And the real-time status information of the certificate can also be queried through the OCSP service.

At the same time, SZCA will publish information in other possible forms when necessary.

2.3 发布的时间或频率 Time or Frequency of Publication

订户证书签发或者吊销时，通过官方网站自动将证书和CRL发布。CRL可通过SZCA的官网下载，CRL更新周期为24小时，CRL的有效期为72小时；特殊情况时，也可人工发布最新CRL。

在紧急的情况下，SZCA可以自行决定证书和CRL的发布时间。SZCA每年发布一次电子认证服务机构的CA证书撤销列表（ARL）。

至于其他需要通过信息库向公众公布的信息，其公布内容和公布时间与频次等规则由SZCA自行决定，但SZCA的信息发布将遵循国家法律法规的规定，并保证发布信息行为是即时、高效的。

When the subscriber certificate is issued or revoked, the certificate and CRL are automatically published on the official website. CRL can be downloaded through SZCA's official website. The CRL update cycle is 24 hours and the validity period is 72 hours. In special cases, the latest CRL can also be manually published.

In case of emergency, SZCA may choose when to publish the certificate and CRL at its own discretion. SZCA releases CRL of CA (ARL) every year.

For other information to be published to the public through the repositories, its publishing content, publishing time and frequency are at the discretion of SZCA, on the premise that the information publication of SZCA will comply with the provisions of national laws and regulations and be immediate and efficient.

2.4 信息库访问控制 Access Controls on Repositories

SZCA信息库中的信息是对外公开发布的，任何人都能够查阅，对这些信息的只读访问不受任何限制。

SZCA通过信息访问控制机制和安全审计措施，保证只有经过授权的SZCA工作人员才能编写、修改和发布SZCA信息库中的信息。并且授权操作的操作日志、记录将留存并进行审计。

The information in SZCA repositories is publicly available. Anybody can read the relevant information, and there are no restrictions on the read-only access of such information.

With information access control mechanism and security audit measures, SZCA ensures that only authorized SZCA personnel can edit, modify and publish information in the repositories. In addition, operation logs and records of authorized operations will be kept for audit.

3. 身份标识与鉴别 Identification and Authentication

3.1 命名 Naming

3.1.1 名称类型 Type of Names

SZCA 颁发的数字证书，含有颁发机构和证书订户主体甄别名。证书持有者的标识命名，以甄别名（Distinguished Name）形式包含在证书主体内，是证书持有者的唯一识别名。SZCA 的证书符合 X.509 标准，分配给证书持有者实体的甄别名，采用 X.500 标准命名方式。

对于 SSL 服务器证书，所有的域名或 IP 地址都添加到主题别名中，而通用名必须是一个出现在主题别名中的域名或 IP 地址。对于 EV SSL 证书，主题别名中不能包含通配符域名和 IP 地址。

The digital certificate issued by SZCA contains the subject DN of issuing authority and the certificate subscriber. The identification name of the certificate holder is contained in the certificate subject in the form of distinguished name, and is the unique identifier of the certificate holder. The SZCA certificate complies with X.509 standard, and the distinguished name assigned to the certificate holder entity adopts X.500 standard naming method.

For SSL server certificates, all domain names or IP addresses are added to Subject Alternative Name, whereas the Common Name must be a domain name or IP address that exists in Subject Alternative Name. For EV SSL certificates, the Subject Alternative Name cannot contain wildcard domain names and IP addresses.

表3.1-SZCA证书颁发机构的主体甄别名命名规则

属性	值
国家（C）	CN
机构（O）	Shenzhen Digital Certificate Authority Center Co., Ltd.
通用名（CN）	CA 名称

Table 3.1 - Naming Rules of SZCA's Subject DN

Attribute	Value
Country (C)	CN
Organization (O)	Shenzhen Digital Certificate Authority Center Co., Ltd.
Common Name (CN)	Name of CA

表 3.2-SZCA 证书订户的主体甄别名命名规则

属性	值
国家（C）	CN
省（S）	订户所在省份（可选）
地区（L）	订户所在城市（可选）
机构（O）	对于有确定机构的订户，是订户所在机构名称；
机构部门（OU）	可以包含以下一个或多个内容： 订户所在机构的具体部门； 其他描述身份或证书类型的文字；
电子邮件（E）	订户的电子邮件地址 （可选）
通用名（CN）	域名/IP、订户名称或其他可识别的名称

Table 3.2 - Naming Rules of SZCA Certificate Subscriber's Subject DN

Attribute	Value
Country (C)	CN

State (S)	The state where the subscriber is located (optional)
Local (L)	The city where the subscriber is located (optional)
Organization (O)	The name of the organization where the subscriber is located for those subscribers with a defined organization;
Organization Unit (OU)	May contain one or more of the following: The specific department of the organization where the subscriber is located; Other text describing the identity or certificate type;
Email (E)	Email address of the subscriber (optional)
Common Name (CN)	Domain name/IP, or name of subscriber, or other identifiable names

3.1.2 对名称意义化的要求 Need for Names to be Meaningful

SZCA 使用DN项来标识证书主体及证书签发者实体，DN项中的名称具有一定的代表性意义，可以与使用证书的最终实体的身份或特有的属性相关。证书主体名称，描述了与订户主体公钥证书绑定相关的实体信息。

SZCA uses the distinguished name (DN) to identify the certificate subject and the certificate issuer entity. The distinguished name (DN) is representative and can be associated with the identity or unique attributes of the end entity using the certificate. The name of the certificate subject describes the information related to the entity bound with public key certificate of the subscriber subject.

3.1.3 订户的匿名或伪名 Anonymity or Pseudonymity of Subscribers

SZCA不接受或者允许订户申请中使用任何匿名或者伪名。

SZCA does not accept or allow the use of any anonymity or pseudonym in the subscriber application.

3.1.4 理解不同名称形式的规则 Rules for Interpreting Various Name Forms

SZCA 签发的数字证书符合 X.509 V3 标准，甄别名格式遵守 X.500 标准。甄别名的命名规则由 SZCA 定义。

The digital certificate issued by SZCA complies with X.509 V3 standard, and the DN's format complies with X.500 standard. The naming rules for DN are defined by SZCA.

3.1.5 名称的唯一性 Uniqueness of Names

在 SZCA 信任域内，不同订户的证书的主体甄别名不能相同，必须是唯一的。但对于同一订户，SZCA 可以用其唯一的主体甄别名为其签发多张证书。当证书申请中出现不同订户存在相同名称时，遵循先申请者优先使用，后申请者增加附加识别信息予以区别的原则。

Subject DN of certificate must be unique for different subscribers in SZCA trust domain, and the same DNs cannot be allowed as subscriber’s subject name. SZCA can issue more than one certificate using the unique DN for one subscriber. When DN is not unique to different subscribers, the first applicant has the priority to use the DN, and the latter could add more additional information to distinguish from others.

3.1.6 商标的识别、鉴别和角色 Recognition, Authentication, and Role of Trademarks

SZCA 签发的证书的主体甄别名中不包含商标名。

Subject DN of certificate issued by SZCA does not contain any trademarks.

3.2 初始身份确认 Initial Identity Validation

3.2.1 证明拥有私钥的方法 Method to Prove Possession of Private Key

证书申请者必须证明持有与所要注册公钥相对应的私钥，证明的方法包括在证书申请消息中包含数字签名（PKCS#10）、或其它与此相当的密钥标识方法、或 SZCA 要求的其它证明方式。

The certificate applicant shall prove the possession of the private key that corresponds to the registered public key. The proving methods include: digital signature (PKCS#10), other equivalent key identification methods, or other proving methods required by SZCA.

3.2.2 组织机构身份的鉴别 Authentication of Organization Identity

任何组织机构申请 SSL 证书、代码签名证书或其他机构类型证书时，应提交机构有效证件材料，包括但不限于：营业执照、法人登记证书、社会团体登记证书、民办非企业登记证书、外国（地区）企业常驻代表机构登记证、政府批文或其他机构所在国家（地区）政府颁发的官方登记证明文件。

CA 应进行严格的身份鉴别，如通过查询可信数据库验证其真实性以及其他可以获得申请者明确的身份信息的方式等。SZCA 接受申请后，检查证书申请材料，并审核订户身份的

真实性，处理证书申请后将依法留存与认证相关的订户材料、信息。

When any organization applies for a SSL certificate, code signing certificate or other organization type certificate, the organizations shall submit the valid identity documents ,including but not limited to:legal person code certificate,legal person registration certificate， private non-enterprise registration certificate， registration certificate of foreign(regional)enterprise , government approval and other registration certificate issued by the government where the organization has resided.The CA shall carry out strict authentication, such as verifying its authenticity by querying a reliable database and other means of obtaining identity information of the applicant.

3.2.2.1 机构身份鉴别 Authentication of Organization Identity

组织机构在以组织机构名义申请各种类型证书时，都应进行严格的身份鉴别，如通过查询可信数据库验证其真实性、鉴别身份材料以及其他可以获得申请者明确的身份信息的方式等。机构订户的证书申请表上有申请者本身或机构授权代表的签字表示接受证书申请的有关条款，并承担相应的责任。

机构证书申请的机构身份鉴别：

1. 确认机构是确实存在的、合法的实体。确认的方式是：通过权威第三方数据库对机构有效身份证明文件信息进行核查，确保申请机构信息与核查结果一致。
2. SZCA 通过可信第三方数据源得到的电话号码、电子邮件等方式与申请机构进行联络，以确认被申请者信息的真实性，如验证代理人的职位或验证申请表中的某个人是否是申请人。
3. 检查机构授权给经办人申请办理证书事宜的授权文件及经办人有效身份证件，确保经办人得到申请机构的授权。
4. SZCA 通过电话或电子邮件等方式与证书申请人核实证书请求信息，确认申请人的真实意愿。

5. 如果 SZCA 无法从第三方得到所有所需的信息，可委托第三方进行调查，或要求申请者提供额外的信息和证明材料。

此外，必要时，SZCA 还可以设定其它的鉴别方式和资料。申请者有义务保证申请材料的真实有效，并承担与此相关的法律责任。

对于 DV SSL 证书，SZCA 只验证网站域名所有权或控制权，不对申请机构身份进行验证。SZCA 建立并维护高风险证书申请者列表，在接受证书申请前，会对高风险证书申请人列表进行查询，如识别为“高风险”的证书请求申请者，SZCA 直接拒绝其申请。

EV 证书订户应满足以下条件：

1) 经当地机构注册管理机关合法注册设立，或经政府或上级组织许可、批准成立；

2) 授权负责人、专门机构负责申请证书；

3）未被登记机构等政府机构或司法机关等载入“停业”、“无效”、“过期”名单；

4) 有固定的经营场所和经营业务，并能够进行验证（对商业法人）；

5) 未被列入注册地政府任何黑名单或禁制名单中；

6) 经营所在地、注册地允许使用 SZCA 证书。

When applying for various types of certificates in the name of the organization, the organization shall be subject to strict authentication, such as verifying its authenticity by querying a reliable database, identifying the identity materials and other means of obtaining identity information of the applicant. And once the organization subscriber or the authorized representative of the organization signs on the certificate application form, it means they are willing to accept the relevant provisions of the certificate application and assume corresponding responsibilities.

Organization authentication for organization certificate application is as below:

1. Confirm the actual existence and legality of the organization. The confirmation method is: Check the valid organization identity document through an authoritative third-party database to ensure that the organization information is consistent with the verification results.

2. SZCA contacts the applicant organization through telephone, email and other ways obtained from trusted third-party data sources to confirm the authenticity of the applicant information, such as verifying the agent's position or verifying whether someone in the application form is the applicant itself.

3. The authorization documents issued by the organization to the agent for certificate application and the valid identity documents of the agent shall be checked to ensure that the agent is authorized by the applicant organization.

4. SZCA verifies the certificate request information with the certificate applicant through telephone or email, and confirms the intention of the applicant.

5. If SZCA is unable to obtain all the required information from a third party, it may entrust a third party to conduct an investigation or request the applicant to provide additional information and supporting materials.

In addition, SZCA may choose other authentication methods and materials when necessary. The applicant is obliged to ensure the authenticity and validity of the application materials and assume any relevant legal responsibilities.

For DV SSL certificates, SZCA only verifies the ownership or control of the website domain name and does not verify the identity of the applicant organization. SZCA establishes and maintains a high risk certificate applicant list and will check the list when accepting certificate applications. If the applicant is identified as a "high-risk" certificate applicant, SZCA will directly reject the application.

The EV certificate subscribers shall meet the following conditions:

1) Legally recognized or registered with the Incorporating or Registration Agency, or approved to be in existence and validly formed (e.g., incorporated) by the government or the superior institution in the Applicant’s Jurisdiction of Incorporation or Registration；

2) Authorizing reprensentative or agent to apply certificate;

3)Not designated on the records of the Incorporating or Registration Agency by labels such as “inactive”, “invalid”, “not current”, or the equivalent；

4) With a fixed place of business and operational business activity to be verified (only for business entity);

5) Not on any denial list or prohibited list by the governent, such as embargo;

6) The country where the applicant reside allows the CA to issue a certificate.

3.2.2.2 机构商业名称验证 Authentication of Tradename

若证书主题中包含 DBA 或商业名称，SZCA 通过以下方式中的至少一种以确认申请者有权使用该 DBA 或商业名称：

1. 政府机构提供的可证明申请者合法成立、存在或认可的文档，或与该政府机构沟通；
2. 可靠的数据来源；
3. 其他 SZCA 认为可靠的验证方式。

If the certificate subject contains a DBA or tradename, SZCA shall verify that the applicants have right to use the DBA/tradename using at least one of the following ways:

1. Valid documents provided by a government agency in the jurisdiction of the applicant’s legal creation, existence, or recognition, or communication with the government agency;
2. A reliable data source;
3. Other DBA/Tradename's authentication methods that the CA determines to be reliable.

3.2.2.3 国家的鉴别 Verification of Country

若证书主题项中包含国家选项，SZCA 通过以下方式中的至少一种进行国家的鉴别：

1. 通过权威第三方数据库查询网站 DNS 记录显示的 IP 地址或申请者的 IP 地址来确

认所在国，确保申请人的 IP 地址所在国与申请人实际所在国一致。

2. 通过本 CPS 第 3.2.2.1 节中申请者的机构信息进行所在国家的确认；

3. 申请域名的 ccTLD;

4. 域名注册机构提供的信息。

If the certificate subject contains an option of country, SZCA shall verify the country using one of the following ways:

1. Confirm the host country by checking the IP address displayed by the DNS record of the website or the IP address of the applicant through an authoritative third-party database, and ensure that the country where the applicant's IP address is located is consistent with the actual country where the applicant is located.

2. Confirm the country through the information provided by the applicant in Section 3.2.2.1 of this CPS;

3. The ccTLD of the requested domain name;

4. Information provided by the domain name registrar.

3.2.2.4 域名的确认和鉴别 Verification and Authentication of Domain Name

对于域名的验证，被验证的实体还可以是申请者的母公司、子公司或附属机构，SZCA 可采用以下鉴别方式中的一种：

1. 通过邮件方式发送随机值到由 ‘admin’， ‘administrator’，‘webmaster’，‘hostmaster’或 ‘postmaster’作为前缀，再加上符号@和授权域名作为尾缀的邮箱，然后收到使用该随机值的确认回复，确认申请人对域名的所有权。鉴别方式遵循 Baseline Requirments v1.8.0 第 3.2.2.4.4 节。

2. 通过验证域名在 DNS CNAME、TXT 或 CAA 记录中是否存在约定的随机值，确认

申请人对域名的所有权。鉴别方式遵循 Baseline Requirments v1.8.0 第 3.2.2.4.7 节。

3. 通过在验证域名的“/.well-known/pki-validation”目录下对约定的信息进行改动，确认申请人对域名的所有权。鉴别方式遵循Baseline Requirments v1.8.0 第3.2.2.4.18节。此方法不适用于通配符域名的验证。

SZCA 不为以.onion 为后缀的域名签发 SSL 证书。

必要时，SZCA 可以采取其它独立的审查措施，以确认域名的归属权，如果要求申请者提供相应的协助，申请者不得以任何理由拒绝。

For the verification of a domain name, the verified entity may be the applicant's parent company, subsidiary company or affiliate, SZCA may adopt one of the following authentication methods:

1. Confirm the ownership of the domain name by sending an email including a Random Value to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the prefix, followed by the at-sign ("@"), followed by an authorized domain name, and receiving a confirming response utilizing the Random Value. This way of validation conforms to Section 3.2.2.4.4 of the Baseline Requirements v1.8.0.

2. Confirm the applicant's ownership of the domain name by conforming the presence of a negotiated random value in a DNS CNAME, TXT or CAA record. This way of validation conforms to Section 3.2.2.4.7 of the Baseline Requirements v1.8.0.

3. Confirm the applicant's ownership of the domain name by making changes to the agreed information under the "/.well-known/pki-validation" directory. This way of validation conforms to Section 3.2.2.4.18 of the Baseline Requirements v1.8.0.This method doesn’t apply to the wildcard domain validation.

SZCA does not issue SSL certificates for domain names suffixed by .onion.

If necessary, SZCA may perform the independent investigation to confirm the ownership of

the domain name. The corresponding assistance is needed from Subscriber, the subscriber shall not refuse it for any reason.

3.2.2.5 IP 的确认和鉴别 Verification and Authentication of IP

SZCA 采用以下方式确认申请者拥有或控制该 IP 地址：

（1）通过在验证域名的“/.well-known/pki-validation”目录下对约定的信息进行改动，确认申请人对域名的所有权。鉴别方式遵循 Baseline Requirments v1.8.0 第 3.2.2.5.1 节。

SZCA 不为 IANA 标注的保留 IP 地址或内部 IP 地址签发证书，不为 IP 地址签发 EV SSL 证书。

SZCA shall confirm the applicant's ownership of the domain name by making changes to the agreed information under the "/.well-known/pki-validation" directory. This way of validation conforms to Section 3.2.2.5.1 of the Baseline Requirements v1.8.0.

SZCA does not issue a certificate for a Reserved IP Address marked by IANA or non-routable internal domain names, and does not issue EV SSL certificates for the IP address.

3.2.2.6 通配符域名的确认和鉴别 Verification and Authentication of Wildcard Domain Names

对于通配符域名，SZCA 根据本 CPS 第 3.2.2.4 节中规定的域名验证方式对通配符右侧的域名进行验证，确认申请者对于通配符右侧的域名的控制权或所有权，保证通配符右侧的域名是明确归属于某一个商业实体、社会组织或政府机构等机构，并经过注册获得的。

SZCA 拒绝通配符右侧的域名直接是顶级域名、公共后缀或由域名注册管理机构控制的域名的证书申请，除非申请者能够证明其完全控制该域名的所有命名空间。

For wildcard domain name, SZCA shall confirm the applicant's ownership of or control over the domain name to the right of the wildcard by using the validation methods in Section 3.2.2.4 of this CPS, to ensure that the domain name is clearly assigned to a commercial entity, social

organization or governmental agency, and obtained through legal registration.

SZCA refuses the certificate application if the domain name to the right of the wildcard is directly a top-level domain name, a public suffix, or the domain name is controlled by the domain name registration management authority, unless the applicant can prove its rightful control of the entire domain namespace.

3.2.2.7 数据来源的准确性 Data Source Accuracy

SZCA 将 EV 证书审核验证使用的数据源在官方网站（https://www.szca.com）上进行批露，并且在变更证书审核的数据源后，及时进行披露。

在将任何数据来源作为可依赖数据来源使用之前，SZCA 对该来源的可依赖性、准确性，及更改或伪造的可抗性进行评估，并考虑以下因素：

1. 所提供信息的年限；
2. 信息来源更新的频率；
3. 数据供应商，及数据搜集的目的；
4. 数据对公众的可用性及可访问性；
5. 伪造或更改数据的难度。
6. 对于签发的订户证书，若从评估为可依赖数据来源中获得的数据或文件的时间不超过证书签发前 398 天，则 SZCA 可使用该数据及文件。

SZCA discloses Authentication Data Source for EV Certificates on the official website (https://www.szca.com), and makes timely disclosure after changing the certificate authentication data source.

Prior to using any data source as a reliable data source, SZCA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification, and considers the following during its evaluation:

1. The age of the information provided;
2. The frequency of updates to the information source;
3. The data provider and purpose of the data collection;
4. The public availability and accessibility of the data;
5. The difficulty in falsifying or altering the data.
6. For the issued subscriber certificate, the data and documents may be used by SZCA if the time of obtaining data or documents from data source evaluated as reliable does not exceed 398 days before the issuance of the certificate.

3.2.2.8 认证机构授权 Certification Authority Authorization

对于 SZCA 颁发的满足 CA/ 浏览器论坛 EV Guidelines 、Baseline Requirements 要求的公共可信任的 SSL/TLS 证书， SZCA 对签发证书主题别名扩展项中的每一个 dNSName 做 CAA 记录检查 ，并遵循查询到的指示 。

SZCA 根据 RFC6844 （经勘误表 5065 修订） 的规定处理“ issue ”、 “issuewild ”及“iodef ”的属性标签， 若“ issue ”、“issuewild ”标签中不包含 “szca.com”，则 SZCA 不签发对应的证书 ；若 CAA 记录中出现“ iodef ”标签，则 SZCA 与申请者沟通后决定是否为其颁发证书 。

SZCA 以下列 CAA 记录查找失败情况作为可签发证书的条件：

1. 在非 SZCA 的基础设施中查询 CAA 记录失败；
2. 至少尝试过一次重新查找 CAA 记录；
3. 域名所在区域不存在指向 ICNNA 根区域的 DNSSEC 验证链。

For the publicly trusted SSL/TLS certificates issued by SZCA in comfromity with the EV Guidelines and Baseline Requirements of the CA/Browser Forum, SZCA shall check the CAA records and follow the processing instructions found for each dNSName in the Subject Alternative

Name extension of the certificate to be issued.

SZCA shall process "issue", "issuewild", and “iodef” property tags according to RFC6844 as amended by Errata 5065: SZCA will not issue corresponding certificates if the "issue", "issuewild" property tags do not contain "szca.com". In case the property tag “iodef” is present in the CAA records, SZCA will determine whether or not to issue certificates after communicating with the applicant.

SZCA treats a record lookup failure as permission to issue certificates if:

1. the failure is outside the SZCA's infrastructure;
2. the lookup has been retried at least once; and
3. the domain's zone does not have a DNSSEC validation chain to the ICANN root.

3.2.3 个人身份的鉴别 Authentication of Individual Identity

在证书申请时都必须对个人申请者或机构授权经办人进行真实身份的鉴别，如通过查询可信数据库验证其真实性、面对面鉴别身份材料以及其他可以获得申请者明确的身份信息的方式等。证书申请表上有申请者本身或被授权的证书申请者代表的签字表示接受证书申请的有关条款，并承担相应的责任。

SZCA 将确认个人申请者或机构授权经办人身份的真实性和有效性，具体鉴别流程如下：

1. 获得申请者至少一种由政府机构颁发的、有效的、带照片的身份证明文件（如居民身份证、护照、军官证或其他同等证照），SZCA 检查该证明文件是否有任何篡改或伪造的痕迹, 必要时，SZCA 可以通过签发有效身份证明文件的权威第三方数据库进行核查确认申请者身份，也可以通过语音通话、视频、拍照等方式对申请者提供的信息进行核实验证，确保所提供的信息与核查结果一致。
2. 核查证书请求的真实性。SZCA 通过电话、邮件等方式，与申请者核实证书请求。
3. 当申请信息包含机构信息时，需要确认该机构是否存在，以及申请人是否属于该机

构的成员。如要求提交任职证明文件、查询第三方数据库、发送确认电子邮件等。

4. 如果委托他人办理，需核查授权委托书及经办人身份证明。

SZCA 建立并维护高风险证书申请者列表，在接受证书申请前，会对高风险证书申请人列表进行查询，如识别为“高风险”的证书请求申请者，SZCA 直接拒绝其申请。

When applying for a certificate, the individual applicant or the authorized agent of the organization must be subject to strict authentication, such as verifying its authenticity by querying a reliable database, face-to-face identifying the identity materials, and other means of obtaining identity information of the applicant. And once the subscriber or the authorized representative of the subscriber signs on the certificate application form, it means he is willing to accept the relevant provisions of the certificate application and assume corresponding responsibilities.

SZCA will confirm the authenticity and validity of the identity of individual applicant or authorized agent of organization, and the specific authentication procedure is as follows:

1. Obtaining at least one valid government-issued photo identity document i (e.g. resident ID card, passport, military ID or other equivalent certificates). SZCA shall inspect whether the ID document has any indication of alteration or falsification. If necessary, SZCA may check the identity of the applicant through an authoritative third-party database issuing such valid identity document, or confirm the information provided by the applicant through voice call, video, photography, etc. to ensure that the provided information is consistent with the verification results.
2. Checking the authenticity of certificate request. SZCA checks the certificate request with the applicant through telephone, email, etc.
3. When the application information contains organizational information, it is necessary to confirm whether the organization exists and whether the applicant is a member of the organization. For example, by requesting to submit certificate of employment, inquiring third-party database, and sending confirmation email.
4. If another person is entrusted for application, the letter of authorization and the identity certificate of the agent shall be checked.

SZCA establishes and maintains high risk certificate applicants list and will check the list when accepting certificate applications. If the applicant is identified as a "high-risk" certificate applicant, SZCA will directly reject the application.

3.2.4 没有验证的订户信息 Non-Verified Subscriber Information

证书中的信息，未经 SZCA 验证不写入证书。

The information not verified by SZCA shall not be included in the certificate.

3.2.5 授权确认 Validation of Authority

当法人等机构通过授权第三人代理申请某一类型证书时，SZCA和其授权的证书服务机构还需要审核被授权人的身份和资格，包括被授权人的身份资料和授权证明，并且有权通过电话、信函或其它方式与授权人进行核实确认，以审核该授权行为的合法性。SZCA有权通过第三方或其它方式确认被授权人的信息，亦有权要求被授权人提供授权委托书等额外的信息证明材料，验证申请人代表申请证书的真实性，包括对申请人代表的授权文件，及申请证书的意愿确认。

When a legal person or other organization applies for a type of certificate through an authorized third party agent, SZCA and its authorized certificate certification authority also need to review the identity and qualification of the authorized person, including its identity information and authorization certificate, and have the right to check and confirm with the authorized person through telephone, letter or other means to review the legality of the authorization. SZCA has the right to confirm the information of the authorized person through a third party or other means, and also has the right to require the authorized person to provide additional information supporting materials such as the letter of authorization, to check the authenticity of the certificate application of the applicant's representative including the authorization documents for the applicant's representative, as well as the confirmation of the

intention of certificate application.

3.2.6 互操作准则 Criteria for Interoperation

不适用。

Not applicable.

3.3 密钥更新请求的标识与鉴别 Identification and Authentication for Rekey Requests

3.3.1 常规密钥更新的标识与鉴别 Identification and Authentication for Routine Rekey

对于一般正常情况下的更新密钥申请，订户须提交能够识别原证书的足够信息，如订户甄别名、证书序列号等，对申请的鉴别基于以下几个方面：

1. 申请对应的原证书存在并且由认证机构签发；
2. 用原证书上的订户公钥对申请的签名进行验证；
3. 基于原注册信息进行身份鉴别。

密钥更新会造成使用原密钥对加密的文件或数据无法解密，因此，订户在申请密钥更新前，必须确认使用原密钥对加密的文件或者数据已经解密，由此造成的损失，SZCA 将不承担责任。

For a general rekey request, the subscriber must submit sufficient information to identify the original certificate, such as the subscriber's DN, and certificate serial number. The identification of the application is based on the following aspects:

1. The original certificate exists, and it was issued by the CA;
2. Verifying the signature of the application with the subscriber's public key on the original

certificate;

3. Identity authentication based on the original registration information.

Rekey can cause files or data encrypted using the original key to be unable to be decrypted. The subscriber must confirm that the encrypted file or data using the original key has been decrypted before applying for the rekey, and SZCA will not be liable for the losses caused thereby.

3.3.2 吊销后密钥更新的标识与鉴别 Identification and Authentication for Rekey After Revocation

证书被吊销后申请密钥更新相当于订户申请新证书，即证书撤销后对密钥更新的标识与鉴别按照本 CPS 3.2 处理。

The rekey after the certificate is revoked is equivalent to the subscriber reapplying for the certificate. The identification and authentication of the rekey after revocation are the same as in CPS 3.2.

3.4 吊销请求的标识与鉴别 Identification and Authentication for Revocation Requests

对于订户及其代理人提出的证书撤销请求，具体识别与鉴别程序按照本 CPS 3.2 流程进行。

当由于 CPS4.9.1.1 所述理由需要撤销订户的证书时，SZCA 依据本 CPS 进行撤销证书，这种情况无须进行鉴别。

If the subscriber and its agent request for revocation of the certificate, the identification and authentication procedures for the revocation request are the same as in CPS 3.2.

When the subscriber certificate is to be revoked due to the reasons described in CPS 4.9.1.1, SZCA shall revoke the certificate according to this CPS without authentication.

4. 证书生命周期操作要求 Certificate Life-cycle Operational Requirements

4.1 证书申请 Certificate Application

4.1.1 证书申请实体 Who Can Submit a Certificate Application

证书申请实体包括个人和具有独立法人资格的组织机构(包括国家机关、事业单位、社会团体和人民团体等)。

The certificate application entities include individuals and organizations with independent legal personality (including Government Entity, Business Entity, Private Organization, People's Organizations, etc.).

4.1.2 注册过程与责任 Enrollment Process and Responsibilities

证书申请人通过线上或现场提交证书申请，并提交包括申请表、用户协议和相关身份证明材料，SZCA 或其注册机构受理证书申请，依据 CPS 身份鉴别流程，对申请人进行身份鉴别，最终决定是否签发证书。若申请人提交的申请信息不足，SZCA 有权从申请人处，或从可靠第三方处获得其他必要的信息，并经申请人确认。证书申请资料的录入和审核分别由信息录入员和审核员完成，并且信息录入员和审核员由不同的可信人员担当。

订户应该事先了解并接受用户协议和本 CPS 中所规定的相关责任与义务，并确保向 SZCA 或其注册机构提供真实、准确、完整的申请材料，并配合完成 CPS 3.2 中规定的鉴别

流程。证书签发后，订户有责任保护证书对应的私钥安全。

SZCA 或其注册机构承担对订户提供的证书申请信息与身份证明资料的一致性检查工作，同时承担相应审核责任。

The applicant shall submit the certificate application online or onsite, with the materials of the application form, user agreement and relevant identity documents. SZCA or its RA accepts the certificate application, identifies the identity of the certificate applicant according to the authentication procedure, and finally decides whether to issue the certificate. If the application information submitted by the applicant is insufficient, SZCA has the right to obtain other necessary information from the applicant or from any reliable third party after being confirmed by the applicant. The entry and review of certificate application materials are completed by the information entry clerk and the reviewer respectively, and the two positions are held by different trusted personnel.

The subscriber shall know in advance and accept the responsibilities and obligations stipulated in the user agreement and this CPS, guarantee that the application materials provided to SZCA or its RA are true, accurate and complete, and cooperate with the completion of the authentication procedure specified in CPS 3.2. After issuance of the certificate, the subscriber is responsible for protecting the security of the private key corresponding to the certificate.

SZCA or its RA shall ensure the consistency between certificate application information and identification which subscribers provided and bear corresponding responsibilities of review.

4.2 证书申请处理 Certificate Application Processing

4.2.1 执行识别与鉴别功能 Performing Identification and Authentication Functions

当 SZCA、注册机构接收到订户的证书申请后，依据 CPS 3.2 的规定对订户进行身份识

别与鉴别。在 SSL 证书签发前，SZCA 对主题别名中的每一个 dNSName 依照 CPS 3.2.2.8 进行 CAA 检查，确认 SZCA 是否可为该域名颁发证书。

若 SZCA 根据 CPS 3.2 指定来源获得的数据或证明文件不超过 398 天且该信息未发生变化，则 SZCA 可使用该数据或证明文件对订户身份进行识别和鉴别。

After receiving the certificate application of the subscriber, SZCA or the RA identifies and authenticates the identity of the subscriber according to CPS 3.2. SZCA shall check the CAA record on each dNSName in the Subject Alternative Name according to CPS 3.2.2.8 before issuing the SSL certificate , and confirms whether to issue a certificate for the domain name.

SZCA may use the documents and data obtained from a source specified under CPS 3.2 to identify and authenticate the subscriber's identity, provided that it obtained such data or document within no more than 398 days, and provided that no changes occurred to the documents and data within such time period.

4.2.2 证书申请批准和拒绝 Approval and Rejection of Certificate Applications

SZCA 或其注册机构依据 CPS 3.2 中的规定的鉴别流程对证书申请人进行身份识别和鉴别后，如证书申请人通过鉴别，将批准其证书申请，为证书申请人签发证书。

如果发生下列情形，注册机构（RA）拒绝证书申请：

1. 该申请不符合本 CPS 3.2 关于订户身份的标识和鉴别规定；
2. 申请者不能提供所需要的身份证明材料；
3. 申请者反对或者不能接受用户协议的有关内容和要求；
4. 申请者没有或者不能够按照规定支付相应的费用；
5. 申请的证书含有 ICANN 考虑中的新顶级域名；
6. SZCA 或其注册机构认为批准该申请将会对 SZCA 带来争议、法律纠纷或者损失。

如果法律法规明确禁止的申请人，或 SZCA 认为批准该申请具有高风险性，SZCA 可拒绝其证书申请。

SZCA 根据反钓鱼联盟、防病毒厂商或相关联盟、负责网络安全事务的政府机构等第三方发布的名单，或公共媒体公开报道中披露的信息，或 SZCA 之前由于怀疑网络钓鱼或其他诈骗用途或顾虑而拒绝的证书请求或吊销的证书，建立和维护证书高风险申请人列表，在接受证书申请时将会查询该列表信息。对于列表中出现的申请人，SZCA 将直接拒绝其申请。

对于拒绝的证书申请，SZCA 通知申请者证书申请失败的结果和原因。

After SZCA or its RA identifies and authenticates the identity of the certificate applicant according to the authentication procedure stipulated in CPS 3.2, if the certificate applicant passes the authentication, SZCA or its RA will approve the certificate application and issue a certificate for the certificate applicant.

The RA has the right to reject the certificate application if:

1. The application does not comply with the provisions of CPS 3.2 on the identification and authentication of subscribers;
2. The applicant cannot provide the required identity documents;
3. The applicant objects or cannot accept the relevant content and requirements of the user agreement;
4. The applicant fails to or cannot pay corresponding fees as required;
5. The certificate applied for contains a new top-level domain name under consideration by ICANN;
6. SZCA or its RA believes that the approval of the application will bring disputes, legal disputes or losses to SZCA.

If the applicant is prohibited clearly by laws and regulations, or SZCA considers that there is

a high risk to approve the application, SZCA may reject the certificate application.

SZCA establishes and maintains a list of high risk certificate applicants according to the list provided by anti-phishing alliance, antivirus vendor or related alliance, government agencies that are responsible for network security affairs and other third parties, or the disclosure of information through public media reports, or previously rejected certificate requests or revoked certificates by SZCA due to suspected phishing or other fraudulent usage or concerns. SZCA will query information from the list during accepting certificate application. If the applicants appear in this list, SZCA will reject their application directly.

For the rejected certificate applications, SZCA will inform the applicant of the failure of the certificate application and reasons.

4.2.3 处理证书申请的时间 Time to Process Certificate Applications

在申请者所提交的证书申请材料齐全完整并符合要求的情况下，SZCA 或授权的注册机构将在 3 个工作日内处理证书申请，如有特殊情况，可适当延长证书处理时间，但最长不得超过 7 个工作日。EV 证书的申请处理时间最长不超过 15 日。

If certificate application materials submitted by the applicant are complete and meet with the requirements, SZCA or its authorized RA will process the application within 3 working days. In case of special circumstances, the processing period of the certificate may be appropriately extended, but not more than 7 working days. The processing period for EV certificate application shall not exceed 15 days.

4.3 证书签发 Certificate Issuance

4.3.1 证书签发中注册机构和电子认证服务机构的行为 RA and CA Actions During Certificate Issuance

根 CA 的证书签发由 SZCA 授权的可信人员谨慎地发布直接指令，使根 CA 执行证书签名操作。

在证书的签发过程中 RA 的信息录入员录入证书申请信息，由审核员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发往 CA 的证书签发请求信息须有 RA 的身份鉴别与信息保密措施，并确保请求发到正确的 CA 证书签发系统。

CA 的证书签发系统在获得 RA 的证书签发请求后，对来自 RA 的信息进行有效性判断，对于有效的证书签发请求，证书签发系统签发订户证书。

SZCA 在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

Certificate issuance by the Root CA Certificate shall require a trusted person authorized by SZCA to deliberately issue a direct command in order for the Root CA Certificate to perform a certificate signing operation.

During the issuance process of the certificate, the information entry clerk of the RA is responsible for entering the certificate application information, and the reviewer is responsible for the approval of the certificate application, and transmission the request for certificate to the CA certificate issuance system by operating the RA system. The certificate issuance request issued by the RA to the CA requires the identity authentication and information security measures of the RA, and the request must be sent to the right CA certificate issuance system.

After obtaining the certificate issuance request from the RA, the CA certificate issuance system shall determine the validity of information from the RA, and issue the subscriber

certificate for valid certificate issuance request.

SZCA shall issue the certificate after approving the application. The issuance of the certificate means that the CA has approved the certificate application completely and formally.

4.3.2 电子认证服务机构和注册机构对订户的通告 Notifications to the Subscriber by the CA and RA

SZCA 通过注册机构告知订户申请的处理结果和证书下载方式，可通过电子或纸质回执、电子邮件、网络下载或其他 SZCA 认为安全可行的方式。

SZCA shall inform the subscriber of the application processing results and certificate download methods through the RA ， which includes electronic or paper receipt, email, downloading through network or other means that SZCA considers safe and feasible.

4.4 证书接受 Certificate Acceptance

4.4.1 构成接受证书的行为 Conduct Constituting Certificate Acceptance

证书签发后，订户通过 CA 机构或其注册机构所通告的方式获取证书，在以下情况下，CA 机构认为订户接受了证书：

1. 订户下载或安装了证书；
2. SZCA 在订户的允许下，代替订户下载证书，并把证书通过邮件等方式发送给订户；
3. SZCA 将证书获得方式发送给订户后，在约定时间内订户未表示拒绝或提出反对证书或者证书中的内容。

After the certificate is issued, the subscriber obtains the certificate through the method announced by the CA or its RA. In any of the following circumstances, the CA considers that the

subscriber has accepted the certificate:

1. The subscriber has downloaded or installed the certificate;
2. SZCA, with the permission of the subscriber, downloads the certificate for the subscriber and sends the certificate to the subscriber by email;
3. After SZCA sends the certificate acquisition methods to the subscriber, the subscriber does not refuse or object to the certificate or its content within the agreed time.

4.4.2 电子认证服务机构对证书的发布 Publication of the Certificate by the CA

SZCA 根据 Google 的 CT 策略（https://github.com/chromium/ct-policy），将 SSL 证书发布到至少三个 CT 服务器中。

SZCA submits the SSL certificate to no less than three CT servers based on Google's CT policy (https://github.com/chromium/ct-policy).

4.4.3 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance By the CA to Other Entities

SZCA 不对其他实体进行通告。其他实体可以通过从信息库上自行查询。

SZCA does not notify other entities, and other entities can make their own queries on the repository.

4.5 密钥对和证书的使用 Key Pair and Certificate Usage

4.5.1 订户私钥和证书的使用 Subscriber Private Key and Certificate Usage

订户在提交了证书申请并接受了SZCA所签发的证书后，均视为已经同意遵守与SZCA、依赖方有关的权利和义务的条款。

订户只能在适用的法律、本 CPS 以及用户协议规定的范围内使用私钥和证书。订户接受到证书，应采取合理措施妥善保存其证书对应的私钥避免未经授权的使用。证书到期或被撤销后，订户应停止使用该证书对应的私钥。

对于 SSL 证书，订户有责任和义务保证只在证书中列出的主题别名对应的服务器中部署证书。

The actions of submitting a certificate application and accepting the certificate issued by SZCA shall be deemed that the subscriber has agreed to abide by the terms of the rights and obligations related to SZCA and relying parties.

The subscriber shall only use the private key and certificate within the scope specified by applicable law, this CPS, and user agreement. The subscriber who receives the certificate shall properly take appropriate measures to keep the corresponding certificate private key from unauthorized use. The subscriber shall stop using the private key corresponding to the certificate after the certificate expires or is revoked.

For SSL certificates, the subscriber has the responsibility and obligation to ensure that the certificate is only deployed on the server corresponding to the Subject Alternative Name listed in the certificate.

4.5.2 信赖方公钥和证书的使用 Relying Party Public Key and Certificate

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

1. 获得数字签名对应的 CA 机构证书和信任链；
2. 查询 CRL 或 OCSP，确认数字签名对应的证书有效、状态正常；
3. 确认签名对应的证书是依赖方信任的证书；
4. 证书的用途适用于对应的签名；
5. 使用证书上的公钥验证签名。

以上任一条件不满足或步骤操作失败，依赖方应该拒绝接受签名信息。

When the relying party has received the message with digital signature, the party has the obligation to carry out the following operations to confirm:

1. Obtaining digital signature’s corresponding CA certificate and trust chain;
2. Confirm whether the signature's corresponding certificate is valid and in normal status by querying the CRL or OCSP;
3. Confirm that the signature's corresponding certificate is the one trusted by the relying party;
4. Certificate usage is suitable for the corresponding signature;
5. Use certificate’s public key to verify the signature;

If any of the above conditions are not met or the step operation fails, relying party shall refuse to accept the signature information.

4.6 证书更新 Certificate Renewal

4.6.1 证书更新的情形 Circumstances for Certificate Renewal

当订户证书即将到期，且密钥安全时，可为订户签发新证书。

When the certificate of the subscribers will expire and the keys of the certificate is secure , a new certificate will be issued.

4.6.2 请求证书更新的实体 Who May Request Renewal

请求证书更新的实体为证书订户。

Certificate subscribers may request renewal.

4.6.3 证书更新请求的处理 Processing Certificate Renewal Requests

对于证书更新，其处理过程包括申请验证、鉴别、签发证书。对申请的验证和鉴别须基于以下几个方面：

1. 订户的原证书存在且由 SZCA 所签发；
2. 验证证书更新请求在许可期限内；
3. 基于原注册信息进行身份鉴别。

若 SZCA 根据本 CPS 第 3.2 节获得的数据或证明文件的时间不超过 398 天且该信息未发生变化，则 SZCA 可复用该数据或证明文件用于订户身份识别和鉴别。

通过上述验证和鉴别后 SZCA 才可批准签发证书。在证书更新时，订户可以用原有的私钥对更新请求进行签名，SZCA 将会对用户的签名和公钥、更新请求内包含的用户信息进行正确性、合法性和唯一性的验证和鉴别。

订户也可以选择一般的初始证书申请流程进行证书更新，按照本 CPS 第 3.2 节的要求提

交相应的证书申请和身份证明资料。SZCA 在任何情况下可采取初始证书申请的鉴别方式作为证书更新时的鉴别处理手段。

The processing of certificate renewal includes application verification, authentication, and certificate issuance. The verification and authentication of the application must be based on the following aspects:

1. The original certificate of the subscriber exists, and it was issued by SZCA;
2. The certificate renewal request is within the permitted period;
3. Identity authentication based on the original registration information.

SZCA may reuse the documents and data obtained under Section 3.2 of this CPS to identify and authenticate the subscriber's identity, provided that it obtained such data or document within no more than 398 days, and provided that no changes occurred to the documents and data within such time period.

After going through the above verification and authentication, SZCA can approve the issuance of the certificate. When the certificate is renewed, the subscriber can sign the renewal request with the original private key, and SZCA will verify and authenticate the correctness, legality and uniqueness of the user's signature ，the public key and the user information contained in the renewal request.

The subscriber may also choose to perform the certificate renewal according to the general initial certificate application procedure, and he submits corresponding certificate applications with identity documents in accordance with the requirements of Section 3.2 of this CPS. SZCA may, in any case, adopt the authentication method of the initial certificate application when dealing with the certificate renew application.

4.6.4 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber

同本 CPS 4.3.2。

Same as this CPS 4.3.2.

4.6.5 构成接受更新证书的行为 Conduct Constituting Acceptance of A Renewal Certificate

同本 CPS 4.4.1。

Same as this CPS 4.4.1.

4.6.6 电子认证服务机构对更新证书的发布 Publication of the Renewal Certificate by the CA

同本 CPS 4.4.2。

Same as this CPS 4.4.2.

4.6.7 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance By the CA to Other Entities

同本 CPS 4.4.3。

Same as this CPS 4.4.3.

4.7 证书密钥更新 Certificate Rekey

4.7.1 证书密钥更新的情形 Circumstances for Certificate Rekey

证书密钥更新指订户生成一对新密钥并申请为新公钥签发一个新证书，SZCA 进行证书更新时，密钥也同时更新。

证书密钥更新时无需再提交证书注册信息，订户提交能够识别原证书的足够信息，如订户甄别名、证书序列号、原证书对应的私钥对证书密钥更新请求签名等，并提供新的公钥用

于签发新证书。

证书密钥更新包括但不限于以下情形：

1. 证书私钥泄露而吊销证书；
2. 证书到期；
3. 订户证实或怀疑证书密钥不安全；
4. 基于技术、政策安全原因，SZCA 要求证书密钥更新；
5. 其他可能导致密钥更新的情形。

The certificate rekey means that the subscriber generates a new key pair and requests to issue a new new public key certificate. When SZCA renews the certificate, the key shall be renewed at the same time.

The subscriber does not need to submit the information for certificate application again when applying for the certificate rekey. The subscriber shall only submit the sufficient information for identifying the original certificate, such as the subscriber's DN, the certificate serial number, signature of certificate rekey request using the private key corresponding to the original certificate, etc., and provide new public key for issuing a new certificate.

Certificate rekeys include, but are not limited to, the following circumstances:

1. When the certificate private key is compromised and the certificate is revoked;
2. When the certificate expires;
3. When the subscriber confirms or suspects that its certificate key is unsafe;
4. SZCA requires certificate rekey based on the reasons of technology and policy security;
5. Other circumstances that may result in a rekey.

4.7.2 请求证书公钥更新的实体 Who May Request Certification of a New Public Key

请求证书公钥更新的实体为证书订户。

Certificate subscriber may request certificate rekey.

4.7.3 证书密钥更新请求处理 Processing Certificate Rekeying Requests

同本 CPS3.3。

Same as this CPS 3.3.

4.7.4 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber

同本 CPS4.3.2。

Same as this CPS 4.3.2.

4.7.5 构成接受密钥更新的行为 Conduct Constituting Acceptance of A Rekeyed Certificate

同本 CPS4.4.1

Same as this CPS 4.4.1.

4.7.6 电子认证服务机构对密钥更新证书的发布 Publication of the Rekeyed Certificate by the CA

同本 CPS4.4.2。

Same as this CPS 4.4.2.

4.7.7 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance by the CA to Other Entities

同本 CPS4.4.3。

Same as this CPS 4.4.3.

4.8 证书变更 Certificate Modification

4.8.1 证书变更的情形 Circumstances for Certificate Modification

如果订户的注册信息发生改变，必须向 SZCA 提出证书变更申请。证书变更的申请和证书申请所需的流程、条件一致。

If the registration information of the subscriber changes, a certificate modification application must be submitted to SZCA. The procedures and conditions required for the certificate modification application are the same as the certificate application.

4.8.2 请求证书变更的实体 Who May Request Certificate Modification

请求证书变更的实体为证书订户。

Certificate subscriber may request certificate modification.

4.8.3 证书变更请求的处理 Processing Certificate Modification Requests

证书变更按照初次申请证书的过程进行处理。

The certificate modification is processed according to the procedures of the initial certificate application.

4.8.4 颁发新证书时对订户的通告 Notification of New Certificate Issuance to Subscriber

同本 CPS 4.3.2。

Same as this CPS 4.3.2.

4.8.5 构成接受变更证书的行为 Conduct Constituting Acceptance of A Modified Certificate

同本 CPS 4.4.1。

Same as this CPS 4.4.1.

4.8.6 电子认证服务机构对变更证书的发布 Publication of the Modified Certificate by the CA

同本 CPS 4.4.2。

Same as this CPS 4.4.2.

4.8.7 电子认证服务机构对其他实体的通告 Notification of Certificate Issuance by the CA to Other Entities

同本 CPS 4.4.3。

Same as this CPS 4.4.3.

4.9 证书撤销 Certificate Revocation

4.9.1 证书撤销的情形 Circumstances for Revocation

4.9.1.1 订户证书撤销的原因 Reasons for Revoking a Subscriber Certificate

若出现以下任一情况中，SZCA 必须在 24 小时之内撤销证书：

1. 订户以书面形式请求撤销证书；
2. 订户通知 SZCA 并有证据证明最初的证书请求未得到授权；
3. SZCA 获得了证据，证明与证书公钥对应订户私钥遭到了泄漏；
4. SZCA 获得了证据，证明对证书中 FQDN 或 IP 地址的域名授权或控制权的验证已不再可靠。

若出现以下情况中的一种或多种，SZCA 应在 24 小时之内撤销证书，且必须在 5 天之内撤销证书：

1. 证书不再符合 Baseline Requirements 第 6.1.5 节及第 6.1.6 节的相关要求；
2. SZCA 获得了证书遭到滥用的证据；
3. SZCA 获悉订户违反了用户协议、CPS 中的一项或多项重大义务和责任；
4. SZCA 获悉申请人不再被法律许可使用证书中的 FQDN 或 IP 地址（例如，法院已经撤销了域名注册人使用域名的权力，域名注册人与申请人的相关许可及服务协议被终止，或域名注册人未续订域名）；
5. SZCA 获悉某通配符证书被用于鉴别具有欺骗误导性的子域名；
6. SZCA 获悉证书中所含信息出现重大变化；
7. SZCA 获悉证书的签发未能符合 Baseline Requirements、EV Guideline 或 本 CPS 的相关要求
8. SZCA 确定或获悉订户证书中包含了不准确或错误的信息；
9. SZCA 依据 Baseline Requirements 签发证书的权力失效，或被撤销或被终止，除非其继

续维护 CRL/OCSP 信息库；

10. CPS 中职责的履行被延迟或受不可抗力的阻碍；自然灾害；计算机或通信失败；法律、规章或其它法律的改变；政府行为；或其它超过个人控制的原因并且对他人信息构成威胁的；
11. SZCA 已经履行催缴义务后，订户仍未缴纳服务费
12. SZCA 被告知出现了可使订户私钥泄露的经验证的方法，此类方法可根据公钥轻易地计算私钥值（例如 Debian 弱密钥，见： http://wiki.debian.org/SSLkeys ），或存在明确的证据，证明生成私钥的方法有缺陷。
13. 法律、行政法规、本 CPS 中规定的其他情形。

SZCA must revoke the certificate within 24 hours if any of the following occurs:

1. The subscriber requests in writing to revoke the certificate;
2. The subscriber notifies SZCA and has evidence that the original certificate request is not authorized;
3. SZCA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise;
4. SZCA obtains evidence that the validation of domain authorization or control for any FQDN or IP address in the certificate is no longer reliable;

SZCA shall revoke the certificate within 24 hours if one or more of the following occurs, and the certificate must be revoked within 5 days:

1. The certificate no longer complies with Sections 6.1.5 and 6.1.6 of the Baseline Requirements;
2. SZCA obtains evidence that the certificate was misused;
3. SZCA is made aware that the subscriber has violated one or more of its material obligations and responsibilities under the user agreement or CPS;
4. SZCA is made aware of any circumstance indicating that use of a FQDN or IP address in the certificate by the applicant is no longer legally permitted (e.g. a court has revoked a domain name registrant's right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain name

registrant has failed to renew the domain name);

5. SZCA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate domain name;
6. SZCA is made aware of a material change in the information contained in the certificate;
7. SZCA is made aware that the certificate issuance does not comply with the Baseline Requirements, EV Guideline or this CPS;
8. SZCA determines or is made aware that any of the information appearing in the subscriber's certificate is inaccurate or wrong;
9. SZCA's right to issue certificates under Baseline Requirements expires or is revoked or terminated, unless SZCA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. The fulfillment of the obligations in the CPS is delayed or encounters force majeure, such as natural disasters, computer or communications failures, changes of laws and regulations, government actions or other causes beyond the reasonable control, causing threats to the information of others;
11. Subscribers fail to pay the service fees after SZCA performed the obligations of notifying the subscribers to pay;
12. SZCA is made aware of a demonstrated or proven method that exposes the subscriber's private key to compromise and can easily calculate it based on the public key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the private key was flawed.
13. Other circumstances as stipulated by laws, administrative regulations and this CPS.

4.9.1.2 中级 CA 证书撤销的原因 Reasons for Revoking a Subordinate CA Certificate

若出现以下情况中的一种或多种，SZCA 应在 7 天之内吊销中级 CA 证书：

1. SZCA 获得了证据，证明与证书公钥对应的中级 CA 私钥遭到了损害，或不再符合

Baseline Requirements 第 6.1.5 节及第 6.1.6 节的相关要求；

2. SZCA 有证据证明证书遭到误用；
3. SZCA 获悉证书的签发未能符合 Baseline Requirements 要求，或中级 CA 未能符合 CP/CPS；
4. SZCA 确定证书中的信息不准确、不真实或具有误导性；
5. SZCA 由于任何原因停止运营，且未与另一家 CA 达成协议以提供证书撤销服务；
6. SZCA 依据 Baseline Requirements 签发证书的权力失效，或被撤销或被终止，除非其继续维护 CRL/OCSP 信息库；
7. SZCA 的 CP/CPS 要求吊销中级 CA 证书。

SZCA shall revoke a subordinate CA certificate within 7 days if one or more of the following occurs:

1. SZCA obtains evidence that the subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with Sections 6.1.5 and 6.1.6 of Baseline Requirements;
2. SZCA obtains evidence that the certificate was misused;
3. SZCA is made aware that the certificate was not issued in accordance with Baseline Requirements or that subordinate CA has not complied with the CP or CPS;
4. SZCA determines that any of the information appearing in the certificate is inaccurate, untrue or misleading;
5. SZCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
6. SZCA's right to issue certificates under Baseline Requirements expires or is revoked or terminated, unless SZCA has made arrangements to continue maintaining the CRL/OCSP Repository;
7. Revocation is required by SZCA's CP/CPS.

4.9.2 请求证书撤销的实体 Who May Request Revocation

请求证书撤销实体为订户、注册机构、SZCA、司法机关或其他有权机关。

此外，依赖方、应用软件提供商、防病毒机构或其他的第三方可以提交证书问题报告，告知 SZCA 有合理理由吊销证书。

The subscribers, RA, SZCA, judicial authority or other competent authority can initiate revocation.

In addition, relying parties, application software providers, anti-virus organizations and other third parties may submit certificate problem reports informing the SZCA of reasonable cause to revoke the certificate.

4.9.3 请求吊销的流程 Procedure for Revocation Request

4.9.3.1 订户主动提出吊销申请 A Subscriber Makes An Application for Revocation on One's Own Initiative

1. 订户向 SZCA 或其注册机构提出证书撤销申请，并填写证书撤销申请表，SZCA 或其注册机构根据本 CPS 3.4 节的要求对吊销申请进行鉴别。
2. 注册机构将证书撤销申请表提交给 SZCA，由 SZCA 完成吊销。
3. SZCA 提供 7*24 小时的证书撤销申请服务，订户可通过以下方式申请吊销：
   1) 联系人：巫敬芳
   2) 电话：4001123838
   3) 联系邮箱：report@szca.com
4. SZCA 收到申请后 24 小时内处理吊销申请。
5. SZCA 完成证书撤销后，通过电话、邮件等方式通知订户证书被撤销及撤销的理由，若未能联络订户时，在必要的情况下，SZCA 对吊销的证书将通过网站进行公告。

   证书撤销后，SZCA 将通过电话、电邮、短信等方式通知订户证书已吊销并告知理由。

1. The subscriber submits the certificate revocation application to SZCA or its RA and completes the Certificate Revocation Application Form. SZCA or its RA shall authenticate

the revocation application in accordance with Section 3.4 of this CPS.

2. The RA submits the Certificate Revocation Application Form to SZCA to complete the revocation.

3. SZCA provides 7*24h certificate revocation application service, and subscribers may apply for the revocation of a certificate through the following ways:

   1) Contact: Wu Jingfang

   2) Tel.: 4001123838

   3) Contact email: report@szca.com

4. SZCA shall process the revocation application within 24 hours of receiving the application.

5. After the certificate revocation, SZCA shall notify the subscriber of certificate revocation and reasons for the revocation via telephone or email. In case of failing to contact the subscriber, the SZCA will announce the revoked certificate through the website if necessary.

After the certificate revocation, SZCA shall notify the subscriber of certificate revocation and reasons for the revocation via telephone, email or text message.

4.9.3.2 订户被强制撤销证书 A Subscriber is Forced to Revoke A Certificate

1. 当 SZCA 或注册机构有充分的理由证明出现本 CPS 4.9.1.1 节中导致订户证书被强制撤销的情形时，SZCA 或注册机构将通过内部流程申请吊销证书。
2. 在证书撤销后，SZCA 或注册机构将通过适当的方式，包括邮件、电话等，通知最终订户证书已被吊销及被吊销的理由。若未能联络订户时，在必要的情况下，SZCA 对吊销的证书将通过网站进行公告。
3. SZCA 提供 7*24 小时的证书问题报告和处理流程。
4. 当依赖方、司法机构、应用软件提供商、防病毒机构等第三方发现证书可能存在问题，如私钥出现或怀疑出现泄漏、证书滥用、证书被用于可疑代码签名等，可及时通过以下

方式进行问题报告：

（1） 联系人：巫敬芳

（2） 电话：4001123838

（3） 联系邮箱：report@szca.com

SZCA 收到报告后，在 24 小时内对该证书问题报告内容进行调查，并基于以下标准来决定是否吊销证书：

（1） 所报告问题的性质；

（2） 相应问题的出现次数和频率；

（3） 问题报告或投诉的实体；

（4） 用户对 SZCA CP/CPS 和用户协议等相关规范的遵循情况；

（5） 现行法律法规的遵循。

1. When SZCA or RA has sufficient reason to believe that situations that will cause the enforced revocation of subscriber certificates in Section 4.9.1.1 of this CPS, SZCA or RA will apply for the revocation of the certificate through the internal procedure.
2. After the certificate revocation, SZCA or RA will notify the end subscriber of certificate revocation and the revocation reason through appropriate means, including email, telephone, etc. In case of failing to contact the subscriber, the SZCA will announce the revoked certificate through the website if necessary.
3. SZCA provides 7*24h certificate problem report and processing procedure.
4. When relying parties, judicial authority, application software providers, anti-virus organizations and other third parties find that the certificate may have problems, such as certificate misuse, the occurrence or suspected occurrence of private key compromise, certificate used for suspicious code signature, etc., a timely problem report can be done in the following ways:

   (1) Contact: Wu Jingfang

   (2) Tel.: 4001123838

(3) Contact email: report@szca.com

After receiving the report, SZCA shall investigate the content certificate problem of the report within 24 hours and decide whether to revoke the certificate based on the following criteria:

(1) The nature of the reported problem;

(2) The occurrence number and frequency of the problem;

(3) The entity of the problem report or complaint;

(4) The user's compliance with the relevant specifications of the CP/CPS and user agreement of the SZCA;

(5) The compliance with current laws and regulations.

4.9.3.3 电子认证服务机构本身证书的撤销 Revocation of the CA Certificate

对于 SZCA 的根证书和中级 CA 证书，SZCA 根据本 CPS 的规定决定是否撤销证书。

For SZCA's Root CA certificates and Subordinate CA certificates, revocation will be determined according to this CPS.

4.9.4 吊销请求宽限期 Revocation Request Grace Period

如果出现密钥泄露或有泄露嫌疑等事件，吊销要求必须在发现泄密或有泄密嫌疑 8 小时以内提出。其他吊销原因的吊销要求必须在变更前的 48 小时内提出。

In the event of a key compromise or suspected compromise, the revocation request must be filed within 8 hours of the discovery of a compromise or a suspected compromise. Revocation requests for other reasons must be filed within 48 hours.

4.9.5 电子认证服务机构处理吊销请求的时限 Time within Which CA Must Process the Revocation Request

SZCA 处理撤销请求的周期为 24 小时。

The period for processing the revocation request for SZCA is 24 hours.

4.9.6 依赖方检查证书撤销的要求 Revocation Checking Requirements for Relying Parties

SZCA 提供在线证书状态吊销查询服务，依赖方可通过 SZCA 网站查询。

SZCA provides online query service on revocation status. The relying party can query on the SZCA website.

4.9.7 CRL 发布频率 CRL Issuance Frequency

对于订户证书，SZCA 每 24 小时更新发布最新 CRL，且订户证书 CRL 有效期最长不超过 10 天。

对于中级 CA 证书，SZCA 每 12 个月更新发布最新 CRL。如果吊销中级 CA 证书，SZCA 在吊销后 24 小时之内更新 CRL，且中级 CA 的 CRL 有效期不超过 12 个月。

在特殊紧急情况下可以使 CRL 立即生效，CRL 的立即生效由 SZCA 制定的发布策略决定。

For the subscriber certificates, SZCA updates and reissues certificate revocation list (CRL) every 24 hours, and the CRL validity period of the subscriber certificate is not more than ten days(the value of the nextUpdate field must not be more than 10 days beyond the value of the thisUpdate field).

For the subordinate CA certificates, SZCA updates and reissues certificate revocation list

(CRL) every 12 months. In case the subordinate CA certificates are revoked, SZCA updates and reissues the certificate revocation list (CRL) within 24 hours after the revocation, and the CRL validity period of the subordinate CA is not more than 12 months(the value of the nextUpdate field must not be more than 12 days beyond the value of the thisUpdate field).

The CRL can immediately take effect in emergencies, which is determined by the issuance strategy developed by SZCA.

4.9.8 CRL 发布的最大滞后时间 Maximum Latency for CRLs

CRL 发布的最大滞后时间为 24 小时。

The maximum latency for CRL issuance is 24 hours.

4.9.9 在线状态查询的可用性 On-line Status Checking Availability

SZCA 向证书订户和依赖方提供在线证书状态查询服务。OCSP 响应须符合 RFC6960 的要求，并且被 OCSP 服务器签名。

OCSP 服务器的证书与正在查询状态的证书由同一个 CA 签发，OCSP 服务器的证书包含一个 RFC6960 定义的类型为 id-pkix-ocsp-nocheck 的扩展项。

SZCA provides the Online Certificate Status Protocol (OCSP) service to subscribers and relying parties. The OCSP responses must conform to RFC6960, and will be signed by an OCSP Responder.

The certificate of OCSP Responder is issued by the same CA as the certificate being queried, and contains an extension of type id-pkix-ocsp-nocheck defined by RFC 6960.

4.9.10 在线状态查询要求 On-line Status Checking Requirements

SZCA 提供 Get 和 Post 两种方式的 OCSP 查询服务。

对于订户证书， SZCA 至少每 4 天更新一次 OCSP 信息，OCSP 信息的有效期不超过 10 天。

对于中级 CA 证书，SZCA 至少每 12 个月更新 OCSP 信息。当吊销中级 CA 证书时，在 24 小时内更新 OCSP 信息。

对于未签发的证书的状态查询请求，SZCA 不返回“good”状态。

SZCA provides OCSP query services in both Get and Post methods.

For subscriber certificates, SZCA updates the OCSP information at least every four days. The validity period of OCSP information is no more than ten days.

For subordinate CA certificates, SZCA updates the OCSP information at least every twelve months, and within 24 hours after revoking a subordinate CA certificate.

SZCA does not respond with a "good" status for the request for status of a certificate that has not been issued.

4.9.11 吊销信息的其他发布形式 Other Forms of Revocation Advertisements Available

除 CRL、OCSP 服务外，SZCA 不提供其他发布形式的吊销信息。

SZCA does not provide any revocation information other than CRL or OCSP services.

4.9.12 密钥损害的特别要求 Special Requirements for Key Compromise

除本 CPS 第 4.9.1 节规定的情形外，当订户发现其密钥安全受到损害时，应主动及时向 SZCA 或其注册机构提出证书撤销请求。

Except as provided in Section 4.9.1 of this CPS, when a subscriber discovers that its key has been compromised, it shall voluntarily and timely submit a request for certificate revocation to SZCA or its RA.

4.9.13 证书挂起的情形 Circumstances for Suspension

不适用。

Not applicable.

4.9.14 请求证书挂起的实体 Who May Request Suspension

不适用。

Not applicable.

4.9.15 请求挂起的流程 Procedure for Suspension Request

不适用。

Not applicable.

4.9.16 证书挂起的时限 Limits on Suspension Period

不适用。

Not applicable.

4.10 证书状态服务 Certificate Status Services

4.10.1 操作特征 Operational Characteristics

证书的状态信息，SZCA 通过 OCSP、CRL 服务提供。对于被撤销的证书，SZCA 不删除其在 CRL 中的撤销记录。SZCA 不删除 OCSP 服务器中的撤销记录。

SZCA can provide certificate status information through OCSP and CRL services. For the revoked certificates, SZCA does not delete their revocation records from CRL. SZCA does not delete the revocation record in the OCSP Responder.

4.10.2 服务可用性 Service Availability

SZCA 提供 7X24 小时的证书状态查询服务。证书状态查询请求响应时间不超过 10 秒。在网络允许的情况下，订户能够实时访问证书状态查询服务获取证书状态信息。

SZCA provides a 7X24 hours certificate status query service with a query response time of no more than 10 seconds. The subscriber can obtain the certificate status information through the certificate status query service in real time when the network allows.

4.10.3 可选特征 Operational Features

不适用。

Not applicable.

4.11 订购结束 End of Subscription

订购结束的情形有以下情况：

1. 证书到期后，订户不续费且不申请更新证书，代表订户订购行为正式结束；
2. 证书在有效期内被撤销，代表订购结束。

The end of subscription includes the following situations:

1. When the certificate expires, the subscriber no longer extend the validity or renew the certificate, which means the subscriber' subscription is formally terminated;
2. After the certificate is revoked within the validity period, the subscription is terminated.

4.12 密钥托管与恢复 Key Escrow and Recovery

4.12.1 密钥托管和恢复的策略及行为 Key Escrow and Recovery Policy and Practices

订户密钥对由订户的密码设备生成，由订户自行保管，SZCA 不提供密钥托管和恢复业务。订户应妥善保管密钥，对其进行备份，在密钥丢失后进行恢复。

The subscriber key pair is generated by the subscriber's cryptographic equipment and kept by the subscriber. SZCA does not provide key escrow and recovery services. The subscriber shall keep the key properly, back it up and restore it after the key is lost.

4.12.2 会话密钥的封装和恢复的策略与行为 Session Key Encapsulation and Recovery Policy and Practices

不适用。

Not applicable.

5. 认证机构设施、管理和操作控制 Certification Authority Falities, Management and Operational Controls

5.1 物理控制 Physical Controls

SZCA 的认证服务系统处于安全稳固的建筑物内，具备独立的软硬件操作环境。且系统及设备等物理环境，配备有预防水患、火灾、电磁干扰与辐射及其他自然灾害、工业事故的各种装备、设施。

SZCA 实施功能分区及其访问控制制度，操作人员要进入、操作相应的管理区域及其他关键核心区域，必须进行身份认证，且被视频监控监测记录；且对该区域的设备与系统日常运行及人员操作过程进行监控。SZCA 的根密钥置于最高安全强度保护环境与状态，防止任何非法破坏或者未经授权的操作。SZCA 的核心 CA 系统及中级 CA 系统所使用的相关设备均有四道以上门禁系统做保护。

SZCA's certification service system is located in a safe and stable building with independent hardware and software operating environment. The physical environment of systems and devices is equipped with various equipment and facilities to prevent flood, fire, electromagnetic interference & radiation and other natural disasters and industrial accidents.

SZCA implements the functional area and access control system. The operators who enter and operate the corresponding management area and other key core areas must be authenticated and recorded by video surveillance; and the daily operation of equipment and systems in the area and personnel operation process are also under surveillance. SZCA's root key is placed in the protection environment and state with the highest security strength to prevent any illegal damage

or unauthorized operation. Relevant equipment used in SZCA's core CA system and subordinate CA system is protected by more than four access control systems.

5.1.1 场地位置与建筑 Site Location and Construction

SZCA 认证系统的主机房位于深圳市龙华区观澜街道库坑社区龙华大道泗黎段 402 号的 1 号楼 3 楼，机房按照功能划分为多个功能区。各功能区域对应的安全区域，实施不同的安全等级控制制度，SZCA 采用门禁控制、视频监控等多种有效的物理安全控制措施。机房具备抗震、防火、防水、恒湿温控、防电磁干扰与辐射、备用电力等功能，保障服务的连续性、可靠性。

The main computer room of the SZCA certification system is located at 3/F, Building 1, No. 402, Si Li Section, Longhua Avenue, Guanlan Street, Kukeng Community, Longhua District, Shenzhen. The computer room is divided into multiple functional areas according to their functions. The security areas corresponding to every functional area implement different security level control systems. SZCA takes various effective physical security control measures such as access control and video monitoring. The computer room is provided with the functions of seismic resistance, fire protection, waterproofing, constant humidity and temperature control, anti-electromagnetic interference, anti-radiation, and standby power to ensure the continuity and reliability of services.

5.1.2 物理访问 Physical Access

操作人员进入机房，必须通过 IC 卡门禁系统和密码系统的身份检验，并有 24 小时视频监控设备。操作人员进入具体工作区域进行操作，必须通过该区域密码验证和权限检验，并且所有的操作过程都进行记录。

操作人员进出每一道门都有时间记录和相关信息提示，服务区与核心区需要两个管理员同时使用身份识别卡和密码鉴别才可以进入，机房工作人员按照机房日常工作规范，每月对

门禁记录进行整理归档，保留一年的门禁记录。

物理访问控制包括如下几个方面：

1. 门禁系统：控制各层门的进出。操作人员需使用身份识别卡或结合口令或指纹鉴定才能进出，进出每一道门应有时间纪录和信息提示。
2. 报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。
3. 监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 7*24 小时不间断录像。所有录像资料至少保留 6 个月，以备查询。

Operators who enter the computer room must pass the authentication of the IC card access control system and cryptosystem, and there shall be 24-hour video monitoring equipment. Operators who enter the specific working areas for operation must pass password verification and authority check, and all operation processes are recorded.

Every access of each door by operators has time records and relevant information prompts. The service area and the core area require two administrators to use identification cards and password at the same time before entering. The computer room personnel shall sort out and file the access records monthly, and keep the access records for one year according to the daily work specifications of the computer room.

Physical access control includes the following aspects:

1. Access control system: controls the access to doors at all levels. Operators must use identification cards or in conjunction with passwords or fingerprint authentication for access, and access of each door shall have time records and information prompts.
2. Alarm system: The alarm system shall be triggered in case of any abnormal conditions such as illegal intrusion, door opening by abnormal means and door open for long

time.

3. Monitoring system: The video monitoring system is also used in conjunction with the access control and physical intrusion alarm system to provide 7 * 24 hours uninterrupted video recording of the security areas and the operation areas. All video records shall be kept for at least 6 months for inquiry.

5.1.3 电力与空调 Power and Air Conditioning

SZCA 系统采用双电源供电，在单路电源中断时，可以维持系统正常运转。同时，使用不间断电源（UPS），避免电源波动也保障紧急情况的供电。

系统机房使用中央空调,进行温度和湿度的调控。采用两部独立空调互为备份的方式运作，机房安置了新风系统，对机房进行换气，保证机房内的空气品质和解决新风供应以及机房对空气清洁度的要求等问题。

SZCA system is powered by dual power supplies, which can maintain the normal operation of the system when single power supply fails. At the same time, uninterruptible power supply (UPS) is used to avoid power fluctuation and ensure power supply in emergency.

Central air conditioner is used in the system computer room for temperature and humidity control. Two mutual backup independent air conditioners are used. The computer room is equipped with a fresh air system for ventilation, to ensure the air quality in the computer room and solve the problems of fresh air supply and the requirements of the air cleanliness.

5.1.4 水患防治 Water Exposures

SZCA 的机房及认证服务系统所处的环境为密闭式建筑，并且安装了水浸自动报警系统等预防水浸措施，一旦发生水患立即报警，通知有关人员采取应急措施，充分保障系统安全。

SZCA's computer room and the certification service system is located in a closed building,

equipped with water immersion prevention measures such as automatic water immersion alarm system. In case of water exposure, immediate alarm will be given to inform relevant personnel to take emergency measures and fully guarantee the system security.

5.1.5 火灾防护 Fire Prevention and Protection

SZCA 机房内安装了火灾自动报警系统及气体自动灭火系统，该系统具有自动、手动及机械应急操作三种启动方式。在自动状态下，当防护区发生火警时，火灾报警控制器接到防护区两个独立火灾报警信号后立即发出联动信号。经过 30 秒时间延时，火灾报警控制输出信号，启动灭火系统，同时，报警控制器接收压力讯号器反馈信号，防护区内门灯显亮，避免人员误入。当防护区经常有人工作时，可以通过防护区门外的手动/自动转换开关，使系统自动状态转换到手状态，当防护区发生火警时，报警控制器只发出报警信号，不输出动作信号。由值班人员确认火警，按下控制面板或击碎防护区外紧急启动按钮，即可立即启动系统，喷发气体灭火剂。当自动、手动紧急启动都失灵时，可进入储瓶间内实现机械应急操作启动。

Automatic fire alarm system and automatic gas fire extinguishing system are installed in the SZCA's computer room, which has three starting modes: automatic, manual and mechanical emergency operation. In the automatic mode, when protection area is on fire and detected by two independent alarms, fire alarm controller will immediately trigger a linkage signal. After 30 seconds' delay, the fire alarm control outputs the signal and starts the fire extinguishing system. At the same time, the alarm controller receives the feedback signal from the pressure signal device, and the door light in the protection area will be on to prevent personnel from entering by mistake. When personnel work in the protection area, the automatic mode of the system can be switched to the manual state through the manual/automatic changeover switch outside the protection area door. When the protection area is on fire, the alarm controller only sends an alarm signal and outputs no action signal. After the operator on duty confirms the fire, and presses the control panel or shatters emergency start button outside the protection area, the system immediately starts to spray gas

extinguishing agent. When automatic and manual modes both fail, operator can activate mechanical emergency operation in the extinguishing agent storage room.

5.1.6 介质存储 Media Storage

SZCA 对重要介质的存放和使用满足防火、防水、防震、防潮、防腐蚀、防虫害、防静电、防电磁辐射等的安全需求。采取了介质使用登记注册、介质防复制及信息加密等措施实现了对介质的安全保护。

SZCA meets the following storage and use requirements for important media: fire-proof, water-proof, shock-proof, moisture-proof, corrosion-proof, pest-proof, static-proof, electromagnetic radiation-proof, etc. and implement media usage registration, media copy protection, information confidentiality and other measures to achieve the security protection of the media.

5.1.7 废物处理 Waste Disposal

SZCA 的认证服务系统使用的硬件设备、存储设备、加密设备等，当废弃不用时，涉及敏感性和机密性的信息都被安全、彻底的消除。密码设备在作废处置前根据制造商的指南将其物理销毁或初始化。

文件和存储介质包含有敏感性和机密性信息时，在处理时都经过了特殊的销毁措施，保证其信息无法被恢复和读取。 所有处理行为将记录在案，以供审查的需要。

The sensitive and confidential information in hardware equipment, storage equipment, and encryption equipment used in SZCA's certification service system are eliminated in a safe and thorough way when the equipment is discarded. Cryptographic equipment shall be physically destroyed or initialized in accordance with the manufacturer's guidelines before being discarded.

Documents and storage media containing sensitive and confidential information shall be subject to special destruction measures to ensure that the information cannot be recovered and

read. All disposal actions will be recorded for review.

5.1.8 异地备份 Off-site Backup

SZCA 对重要数据、审计日志数据和其他敏感信息进行异地备份，遇到灾难情况发生时保证数据安全。

SZCA backs up important data, audit log data and other sensitive information at off-site location to ensure data security in case of disaster.

5.2 程序控制 Procedural Controls

5.2.1 可信角色 Trusted Roles

在 SZCA 提供电子认证服务过程中，能从本质上影响证书的颁发、使用、管理和吊销等涉及密钥操作的职位都被 SZCA 视为可信角色。这些角色包括但不限于：密钥和密码设备的管理人员、系统管理人员、安全审计人员、业务管理人员及业务操作人员等，具体岗位名称和要求以 SZCA 的岗位设置及其说明为准。

In the process of electronic authentication service provided by SZCA, persons who can essentially affect the processes of certificate issuance, usage, management and revocation, and other related positions related to key operation are considered as trusted roles. The trusted roles include but are not limited to: key and cryptographic equipment administrators, system administrators, security auditors, business administrators and business operators, etc. The specific position names and requirements shall be subject to SZCA's position description.

5.2.2 每项任务需要的人数 Number of Persons Required per Task

SZCA 在具体业务规范中对关键任务进行严格控制，敏感操作需要多个可信角色共同完

成，例如：

（1）密钥和密码设备的操作和存放：需要 3 个可信人员中的至少 2 个共同完成；

（2）证书签发系统的后台操作：需要 3 个系统管理人员中的至少 2 个可信人员共同完成；

（3）审核和签发证书：需要 2 个可信人员共同完成。

SZCA strictly controls key tasks in specific business specifications. Multiple trusted roles shall be required to jointly complete the sensitive operation. For example:

(1) For operation and storage of the key and cryptographic equipment, it requires at least two of three trusted persons;

(2) For background operation of the certificate issuance system, it requires at least two of three trusted persons;

(3) For review and issuance of the certificate, it requires two trusted persons.

表 5.1-可信角色最低人数配备

序号	可信角色	人数
1	运营安全管理小组	3-5
2	超级管理员	2
3	系统管理员	2
4	系统审计员	1
5	安全管理员	1
6	网络管理员	1
7	监控管理员	1
8	门禁管理员	1

9	密钥管理员	3
10	录入员	若干
11	审核员	1
12	制证员	1

Table 5.1 - Minimum Number of Trusted Roles

S/N	Trusted roles	Number
1	Operational Safety Management Team	3-5
2	Super administrator	2
3	System administrator	2
4	System auditor	1
5	Security administrator	1
6	Network administrator	1
7	Monitoring administrator	1
8	Access control administrator	1
9	Key administrator	3
10	Entry clerk	Several
11	Reviewer	1
12	Certificate maker	1

5.2.3 每个角色的识别与鉴定 Identification and Authentication for Each Role

所有 SZCA 的在职人员，根据所担任角色的不同进行身份鉴别。SZCA 根据各角色作业性质和职位权限，发放需要的系统操作卡、门禁卡、登录密码、操作证书等安全令牌。对于使用安全令牌的员工，SZCA 系统将独立完整地记录并监督其所有的操作行为。

All SZCA's in-service staff are identified according to their roles. SZCA grants the required system operation cards, access control cards, login passwords, operation certificates and other security tokens according to the operation nature and authority of each role. For employees using safety tokens, SZCA's system will independently and completely record and monitor all their operation behaviors.

5.2.4 需要职责分割的角色 Roles Requiring Separation of Duties

为保证系统安全，遵循可信角色分离的原则，即 SZCA 的可信角色由不同的人担任。SZCA 进行职责分离的角色，包括但不限于下列角色：

（1）证书业务受理

（2）证书或 CRL 签发

（3）系统工程与维护

（4）CA 密钥管理

（5）安全审计。

In order to ensure security of the systems, it should follow the trusted role segregation principle that the trusted roles must be assumed by different personnel in SZCA. Roles requiring segregation of duties include, but are not limited to:

(1) The acceptance of the certificate businesses

(2) The issuance of certificates or CRLs

(3) System engineering and maintenance

(4) CA key management

(5) Security audit.

5.3 人员控制 Personnel Controls

5.3.1 资质、经历和无过失要求 Qualifications, Experience, and Clearance Requirements

SZCA 对承担可信角色的工作人员的资格要求如下：

1. 具备良好的社会和工作背景；
2. 遵守国家法律、法规，服从 SZCA 的统一安排及管理；
3. 遵守 SZCA 有关安全管理的规范、规定和制度；
4. 具有良好的个人素质、修养以及认真负责的工作态度和良好的从业经历；
5. 具备良好的团队合作精神；
6. 无违法犯罪记录；
7. 关键和核心岗位的工作人员必须具备相关的工作经验，或通过 SZCA 相关的培训和考核后方能上岗。

The qualification requirements of personnel who undertake trusted roles in SZCA are as follows:

1. With good social and working background;

2. Complying with national laws and regulations, obeying SZCA's unified arrangement and management;
3. Complying with SZCA's related security management norms, rules and systems;
4. Having good personalities and working attitudes, with good working experience;
5. A good team player;
6. No illegal and criminal records;
7. Personnel in key and core positions must have relevant working experience or pass relevant SZCA training and examination first.

5.3.2 背景调查程序 Background Check Procedures

SZCA 员工的录用须经过严格的可信背景调查。SZCA 会与有关部门或调查机构合作，完成对 SZCA 可信员工的背景调查。

背景调查分为基本调查和高级调查。

1. 基本调查包括身份验证、工作经历、职业推荐、教育水平和身体状况方面的调查。
2. 高级调查除包含基本调查项目外，还包括对信用情况、犯罪记录、社会关系和社会安全方面的调查 。

调查程序包括：

1. 人事部门负责对应聘人员的个人资料予以确认。提供以下资料：个人履历、最高学历证明、资格证及身份证等相关有效证明。
2. 人事部门通过电话、网络、信函和走访等形式对应聘人员所提供材料的真实性进行鉴定。
3. 用人部门通过日常观察、现场考核和情景考验等方式对人员进行考察。

注册机构、注册分支机构和受理点操作人员的审查也必须参照 SZCA 可信人员调查制度对其进行考察。受理点可以在此基础上，增加调查、试用和培训条款，但不得违背 SZCA 证书受理的规程和 SZCA 电子认证业务规则。

The employment of SZCA's employees must be subject to strict and credible background check. The background check procedures for trusted employees of the SZCA shall be completed by the SZCA cooperating with relevant government departments and investigation organizations.

Background check is divided into basic check and advanced check.

1. The basic check includes check on identity, work experience, career recommendation, education, and physical condition.
2. In addition to the basic check items, the advanced check further includes the check on credit conditions, criminal records, social relations and social security.

The check procedure includes:

1. The HR department is responsible for confirming the personal data of the applicants. The following materials shall be provided: relevant valid proof such as resume, graduation certificate of highest education, qualification certificates, ID card, etc.
2. The HR department identifies the authenticity of the provided materials by telephone, network, letter, interview, etc.
3. The employing department examines the applicants through daily observation, on-site assessment, and scenario testing, etc.

The operators of the RA, RA branch and LRA must also be assessed with reference to SZCA’s Trusted Personnel Check System. LRA may add terms for check, probation and training on this basis, but shall not violate SZCA's procedures for certificate acceptance and the Certification Practice Statement.

5.3.3 培训要求 Training Requirements

SZCA 根据可信角色的职位需求，给予相应的岗前培训，综合培训内容如下：

1. SZCA 运营体系；
2. SZCA 技术体系；
3. SZCA 安全管理策略和机制；
4. 岗位职责统一要求；
5. PKI 基础知识；
6. 身份验证和审核策略和程序；
7. 灾难恢复和业务连续性管理；
8. CP、CPS 政策及相关标准和程序；
9. SZCA 管理政策、制度及办法等；
10. 国家关于电子认证服务的法律、法规及标准、程序；
11. 其他需要进行的培训等。

SZCA 将员工参加培训的情况形成记录并存档，对于签发 SSL 服务器证书和代码签名证书的操作员和审核员，上岗前必须通过培训并达到 Baseline Requirement 中要求的从事该项工作所必须的技能水平。

Based on the requirements of trusted role, SZCA provides the corresponding pre-job training. The comprehensive training are as follows:

1. SZCA operation system;
2. SZCA technology system;
3. SZCA security management policy and mechanism;

4. Job responsibilities requirements;
5. PKI basic knowledge;
6. Policies and procedures of authentication and review;
7. Disaster recovery and business continuity management;
8. CP & CPS policies and related standards & procedures;
9. SZCA management policies, systems, measures;
10. National laws, regulations, standards and procedures of electronic certification service;
11. Other training required.

SZCA records and archives the training attendance of employees. For operators and reviewers who issue SSL server certificates and code signing certificates, they must pass the training before taking up their posts and reach the skill level required by Baseline Requirement.

5.3.4 再培训周期和要求 Retraining Frequency and Requirements

对于充当可信角色或其他重要角色的人员，每年至少接受 SZCA 组织的培训一次。对于认证系统运营相关的人员，每年至少进行一次相关技能和知识培训。此外，SZCA 将根据机构系统升级、策略调整等要求，不定期的要求人员进行继续培训。

For personnel who act as trusted or other important roles, they shall be trained at least once a year by the SZCA. For personnel related to the operation of the certification system, they shall be trained on relevant skills and knowledge at least once a year. In addition, SZCA will require personnel to receive further training irregularly according to the requirements of its system upgrading, strategy adjustment, etc.

5.3.5 工作岗位轮换周期和顺序 Job Rotation Frequency and Sequence

SZCA 根据自身需要安排工作轮换，轮换周期视具体情况而定。

SZCA will arrange job rotation according to its own needs, and the rotation period shall be determined according to the specific condition.

5.3.6 未授权行为的处罚 Sanctions for Unauthorized Actions

当 SZCA 员工进行了未授权或越权操作，SZCA 立即作废或终止该人员的安全证书和 IC 卡。并视该人员未授权行为的情节严重性，实施对该名人员的通报批评、罚款、辞退以及提交司法机构处理等措施。

When SZCA's employee performs unauthorized operations or exceeds the authority, SZCA will immediately cancel or terminate the person's security certificate and IC card. SZCA takes the measures of circulating a notice of criticism, fine, dismissal and transferring to judiciary authorities for treatment depending on the seriousness of unauthorized behavior.

5.3.7 独立合约人的要求 Independent Contractor Requirements

SZCA 因为人力资源不足或者特殊需要，聘请专业的第三方服务人员参与系统维护、设备维护等，除了必须就工作内容签署保密协议以外，该服务人员必须在 SZCA 专人全程监督和陪同下从事相关工作。同时还需要对其进行必要的知识培训和安全规范培训，使其能够严格遵守 SZCA 的规范。

SZCA employs professional third-party service personnel to participate in system and equipment maintenance due to insufficient human resources or special needs. In addition to signing a confidentiality agreement on the work content, the service personnel must undertake the

relevant work under the whole-process supervision and accompany of SZCA's personnel. Necessary training on knowledge and safety specification is also required to strictly comply with SZCA specifications.

5.3.8 提供给员工的文档 Documentation Supplied to Personnel

在培训或再培训期间，SZCA 提供给员工的培训文档包括但不限于以下几类：

1. SZCA 员工手册；
2. SZCA 电子认证业务规则；
3. SZCA 技术体系文档；
4. SZCA 安全管理制度等。

The training documents provided by SZCA to employees during training or retraining include but are not limited to the following:

1. SZCA Employee Handbook;
2. SZCA Certification Practice Statement;
3. SZCA technology system documents;
4. SZCA security management regulations, etc.

5.4 审计日志程序 Audit Logging Procedures

5.4.1 记录事件的类型 Types of Events Recorded

所有发生在 SZCA 的重大安全事件都会自动地打上时间印章并记录在审计跟踪档案中，这些记录，不论是手动生成或者是系统自动生成，都应该包含以下信息：

1. 事件发生的日期和时间；
2. 记录的序列号；
3. 记录的类型；
4. 记录的来源；
5. 记录事件的实体。

这些事件包括但不限于：

（1） 密钥生命周期内的管理事件，包括密钥生成、备份、存储、恢复、使用、吊销、归档、销毁、私钥泄露等；

（2） 密码设备生命周期内的管理事件，包括设备接收、安装、卸载、激活、使用、维修等；

（3） 证书申请事件，包括订户接受用户协议，接受申请的单位、申请资料的验证、申请及验证资料的保存等；

（4） 证书生命周期内的管理事件，包括证书的申请、批准、更新、吊销等；系统安全事件，包括：成功或不成功访问 CA 系统的活动，对于 CA 系统网络的非授权访问及访问企图，对于系统文件的非授权的访问及访问企图，安全、敏感的文件或记录的读、写或删除，系统崩溃，硬件故障和其他异常；

（5） 防火墙和路由器记录的安全事件；

（6） 系统操作事件，包括系统启动和关闭，系统权限的创建、删除，设置或修改密码；

（7） CA 设施的访问，包括授权人员进出 CA 设施、非授权人员进出 CA 设施及陪同人和安全存储设施的访问；

（8） 可信人员管理记录，包括网络权限的帐号申请记录，系统权限的申请、变更、创建申请记录，人员情况变化。

All major security events occurred in SZCA will be automatically timestamped and logged in the audit trail records. Regardless of manual or automatic generation, these records should contain the following information:

1. The date and time of the event;
2. Sequence number for the record;
3. Type of record;
4. Record source;
5. Event recording entity.

These events include but are not limited to:

(1) Management events in key's life cycle, including generation, backup, storage, recovery, usage, revocation, archiving, destruction, private key compromise, etc.;

(2) Management events in life cycle of cryptographic equipment, including receiving, installation, unloading, activation, use, maintenance, etc.;

(3) Certificate application events, including subscribers' acceptance of user agreements, units accepting applications, verification of application material, preservation of application and verification material, etc.;

(4) Management events in certificate's life cycle, including application, approval, update, revocation, etc.; System security events, including successful or unsuccessful access to the CA system, unauthorized access and access attempts to the CA system network, unauthorized access and access attempts to the system files, reading, writing or deletion of security & sensitive files or records, system collapse, hardware failures and other abnormalities;

(5) Security events recorded by firewalls and routers;

(6) System operating events, including system startup and shutdown, creation or deletion of permission, configuration or modification of password;

(7) Access to CA facilities, including the access of authorized or unauthorized personnel and attendants, as well as security & storage facilities;

(8) Management record of trusted persons, including application record of accounts with network privileges, record of system access application, modification and creation and personnel change.

5.4.2 处理日志的周期 Frequency of Processing Logs

SZCA 每周进行一次日志跟踪处理，检查违反政策及其它重大事件，每月进行发证系统日志分析。所有的审计日志定期由专人进行检查和审阅，以便发现重要的安全和操作事件，及时采取相应的措施进行处理。

SZCA carries out log tracking process on a weekly basis, reviews the violations of policies and other major events, and analyses the certificate issuance system logs on a monthly basis. All the audit logs are checked and reviewed by specific personnel regularly in order to discover the significant security and operation events and take corresponding measures timely.

5.4.3 审计日志的保存期限 Retention Period for Audit Logs

SZCA 系统审计日志，保存期限为证书失效后七年。

The SZCA system audit log shall be kept for seven years after the certificate expires.

5.4.4 审计日志的保护 Protection of Audit Logs

SZCA 执行严格的物理和逻辑访问控制措施，确保只有 SZCA 授权的人员才能接近这些审查记录。这些记录处于严格的保护状态，严格禁止未经授权的任何访问、阅读并禁止任何

修改和删除等操作。

SZCA implements strict physical and logical access control measures to ensure that only personnel authorized by SZCA can access these audit logs. These records are under strict protection, and unauthorized access, reading, modification and deletion are strictly prohibited.

5.4.5 审计日志备份程序 Audit Log Backup Procedures

SZCA 的审计跟踪文档由业务管理员和审计人员每月进行审计日志和审计文档的归档备份。所有文档包括最新的审计跟踪文档应储存在磁盘中并存放在安全的文档库内。

SZCA's audit trail documents are archived and backed up by the business administrator and auditor for audit log and audit documents monthly. All documents including the latest audit trail documents should be stored in disks and placed in a secure document library.

5.4.6 审计收集系统 Audit Collection System

SZCA 设置自动审核系统以审核记录与资料，自动向有关人员或系统报告审核事件。

1. 审计日志收集系统；
2. 证书管理系统；
3. 证书签发系统；
4. 证书目录系统；
5. 远程通信系统；
6. 访问控制系统；
7. 网站、数据库安全管理系统；
8. 其他需要审计的系统。

SZCA uses the automatic review system to review records and materials, and automatically report review events to relevant personnel or systems.

1. Audit log collection system;
2. Certificate management system;
3. Certificate issuance system;
4. Certificate directory system;
5. Remote communication system;
6. Access control system;
7. Website & database security management system;
8. Other systems to be audited.

5.4.7 对导致事件实体的通告 Notification to the Event-Causing Subject

SZCA 发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

SZCA 有权决定是否对导致事件的实体进行通告。

When SZCA detects the attack phenomenon, it will record the attacker's actions, and trace the attacker within the scope permitted by law. SZCA reserves the right to take corresponding countermeasures. According to the actions of the attacker, measures such as cutting off the services that have been opened to the attacker and submitting them to the judicial department may be taken.

SZCA has the right to decide whether to notify the entity resulting in the event.

5.4.8 脆弱性评估 Vulnerability Assessments

在认证系统运行时，SZCA 从内部和外部对系统可能造成的威胁进行评估，并根据日志的日常审计和监督实施，随时调整和系统运行密切相关的安全控制措施，对于薄弱环节，SZCA 每季度对系统进行例行性质的技术漏洞评估，并针对评估结果进行相应处置，以降低系统运行的风险。认证系统本身以及支持认证系统安全运维的相关技术资源，若发生重大变更，亦针对变更项目进行例外性质的技术漏洞评估，确保变更未衍生相应重大技术漏洞。

When the certification system is in operation, SZCA carries out internal and external assessments of the possible threats to the system and adjusts the security controls closely related to the system operation at any time based on daily audits of logs and supervision of implementation. For weakness parts, SZCA conducts a routine technical vulnerability assessments on the system on a quarterly basis, and disposes of the results accordingly to reduce the risk of system operation. In the event of significant changes in the certification system and related technical resources supporting the security operation and maintenance of the certification system, an exceptional technical vulnerability assessment shall also be conducted to ensure that the changes will not give rise to a significant technical vulnerability.

5.5 记录归档 Records Archival

5.5.1 归档记录的类型 Types of Records Archived

SZCA 对以下几类事件进行归档记录，包括但不限于：

（1） 证书系统建设和升级文档；

（2） 证书和证书撤销列表；

（3） 证书申请支持文档，证书服务批准和拒绝的信息，与证书订户的协议；

（4） 审计记录；

（5） 证书策略、电子认证业务规则文档；

（6） 员工资料，包括但不限于背景调查、录用、培训等资料；

（7） 各类外部、内部评估文档。

SZCA archives the following events, including but not limited to:

(1) Documents for construction and upgrade of the certificate system;

(2) Certificate and certificate revocation lists;

(3) Documents supporting certificate applications, information on approval and rejection of certificate services, and agreements with certificate subscribers;

(4) Audit record;

(5) Certificate Policies and Certification Practice Statements;

(6) Employee information, including but not limited to the background investigation, hiring, training, etc.

(7) Various external, internal documents for assessment.

5.5.2 归档记录的保存期限 Retention Period for Archive

SZCA 对于不同的归档记录，其保留期限是不同的。

（1）对订户证书生命周期内的管理事件的归档，保留 7 年以上。

（2）对 CA 证书和密钥生命周期内的管理事件的归档，其保留期限不少于 CA 证书和密钥生命周期。

（3）订户证书的归档保留期限不少于证书失效后 7 年。

（4）CA 证书和密钥的归档在 CA 证书和密钥生命周期之外，额外保留 7 年。

（5）对于系统操作事件和系统安全事件记录，其归档应保留 7 年。

SZCA has different retention periods for different archived records.

(1) Archiving for management events in the subscriber certificate life cycle will be kept for more than 7 years.

(2) Archiving for management events in the CA Certificate and key life cycle will be kept for not less than the life cycle of the CA certificate and key.

(3) Archiving retention period of subscriber certificates will not be less than 7 years after the expiration of certificates.

(4) CA key and certificate archiving will be kept for 7 more years after the end of the life cycle.

(5) For system operation event records and system security event records, the archives will be retained for 7 years.

5.5.3 归档文件的保护 Protection of Archive

SZCA 对各种电子、磁带、纸质形式的归档文件，都有安全的物理和逻辑保护措施和严格的管理程序，确保归档的文件不会被损坏，防止非授权的访问、修改、删除或其它的篡改行为。

SZCA has secure physical and logical protection measures and strict management procedures for all types of archived documents in electronic, tape, and paper form to ensure that archived documents are protected from damage, unauthorized access, modification, deletion, or tampering.

5.5.4 归档文件的备份程序 Archive Backup Procedures

对于系统生成的电子归档记录，每周进行备份，备份文件进行异地存放。

对于书面的归档资料，不需要进行备份，但需要采取严格的措施保证其安全性。

所有归档的电子文件和数据库除了保存在 SZCA 的存储库，还在异地保存其备份。存

档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。SZCA 在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

Electronically archived records generated by the systems are backed up weekly and the backup files are stored off-site.

For the written archiving data, they do not need to be backed up, but some strict measures need to be taken to ensure their security.

All the documents and data archived usually are stored in the main storage site of SZCA. If necessary, the backups will also be saved in the offsite. Archived database is generally isolated physically or logically, with no interaction with the outside. Only authorized personnel or others under the supervision can conduct the operation for reading the files. SZCA provides mechanisms to protect archives and backups from being deleted or modified.

5.5.5 记录时间戳的要求 Requirements for Time-Stamping of Records

SZCA 的档案在创建的时候须加盖时间戳。

SZCA files shall be time-stamped when created.

5.5.6 归档收集系统 Archive Collection System

SZCA 的审计跟踪档案收集系统在本 CPS 第 5.4 节中作详细说明。

SZCA audit trail collection system is detailed in Section 5.4 of this CPS.

5.5.7 获得和检验归档信息的程序 Procedures for Obtaining and Verifying Archived Information

SZCA 定期验证存档信息的完整性。

SZCA regularly verifies the integrity of archived information.

5.6 电子认证服务机构密钥更替 Key Changeover

在证书到期以前，SZCA 将按照证书策略的规定对根密钥进行更换，生成新的证书。在进行密钥的生成时，严格按照 SZCA 关于密钥管理的规范。CA 密钥更替必须遵循以下原则：

1. 在 CA 证书生命周期结束前停止签发新的下级证书，确保在 CA 的证书到期时所有下级证书也全部到期。
2. 在停止签发新的下级证书后至证书到期时，继续使用 CA 私钥签发 CRL，直到最后一张下级证书过期。
3. 生成和管理 CA 密钥对时，严格遵守密钥规范。
4. 及时发布新的 CA 证书。
5. 确保整个过渡过程安全、顺利，不出现信任真空期。

Prior to the expiration of the certificate, SZCA will replace the root key in accordance with the provisions of CP, and generate a new certificate. When generating the new key, specifications of SZCA key management will be followed strictly. CA key replacement must comply with the following principles:

1. The new subordinate certificates can’t be issued before the end of the life cycle of CA certificates, which ensures that all subordinate certificates are expired as the CA certificates expire.

2. Before the expiration of the original private key, CA continues to sign CRLs with the original private key until every certificate issued by this CA expires.
3. CA key generation and management must strictly follow the key regulations.
4. Release the new CA certificate timely.
5. Ensure the entire transition process is safe and smooth with no vacuum of trust.

5.7 损害与灾难恢复 Compromise and Disaster Recovery

当 SZCA 遭到攻击，发生通信网络资源崩溃、毁坏、故障，及计算机设备系统不能正常提供服务，软件被破坏、数据库被篡改等情形或因不可抗力造成 SZCA 机房服务暂停或瘫痪时，SZCA 将依照《SZCA 灾难恢复计划》规定的事故处理、紧急应变、灾难恢复和业务持续运作的程序和应对措施实施恢复。并根据要求向 CA 机构的审计人员提供业务连续性和安全计划，并每年测试、审查和更新该程序。

In the event of an attack on SZCA, the collapse, destruction, or failure of communications network resources, the failure of computer equipment and systems to provide normal services, the destruction of software, the tampering of databases, or the suspension or breakdown of SZCA's server room services due to force majeure, SZCA will implement recovery in accordance with the procedures and responses for incident handling, emergency response, disaster recovery and business continuity as set forth in the *SZCA Disaster Recovery Plan*. Besides, SZCA will provide a plan of business continuity and security to the auditors of CA as required, and test, review and update the procedures annually.

5.7.1 事故或损害处理程序 Incident and Compromise Handling Procedures

为了及时响应和处理事故和损害发生的情况，SZCA 建立了一系列应急处理预案和事故

处理方案，例如：《SZCA 系统故障处理规范》、《SZCA 重大事故应急预案》、《SZCA 系统备份与恢复方案》。

相关岗位的工作人员将按照以上方案和相关制度的规定，积极实施抢修恢复计划和措施，每季度进行数据灾难恢复演练，每年进行一次重大事故应急演练。

To timely respond to and handle accidents and damages, SZCA has established a series of emergency response schemes and accident handling schemes, such as the *SZCA System Fault Handling Specification*, *SZCA Major Accident Emergency Scheme*, and *SZCA System Backup and Recovery Scheme.*

Related personnel will actively carry out the recovery plans in accordance with the regulations of the above schemes and related systems, and perform the data disaster recovery drill each quarter, and an emergency response drill on major accidents annually.

5.7.2 计算机资源、软件或数据的损坏 Damadge to Computer Resources, Software, and/or Data

SZCA 对业务系统及其他重要系统的资源、软件及数据进行了备份，并制定了相应的应急处理流程。当发生网络通信资源毁坏、计算机设备不能提供正常服务、软件被破坏、数据库被篡改等现象或因不可抗力造成灾难，SZCA 将按照灾难恢复计划实施恢复。

SZCA backs up resources, software and data of the business system and other important systems and formulates corresponding emergency treatment processes. When identified the destruction of network communication resources, failures of devices for daily services, malfunction of the software, or tampered database, etc., SZCA will launch the disaster recovery plan.

5.7.3 实体私钥损害处理程序 Entity Private Key Compromise Handling Procedures

在故意的、人为的或是自然灾难的情况下，SZCA 将采取下列步骤以恢复安全环境：

1. SZCA 认证系统的口令由业务管理员、业务操作员、系统管理员进行变更；
2. 根据灾难的性质，部分或全部证书需要吊销或之后重新认证；
3. 如果目录无法使用或者目录有不纯的嫌疑，目录数据和 CRL 需要进行恢复；
4. 及时访问安全现场尽可能合理地恢复操作；
5. 如果需要恢复业务管理员的配置文件，应由系统管理员执行恢复。

如果需要恢复 SZCA 业务操作员的配置文件，则由另外一名 SZCA 安全业务操作员或业务管理员对其进行恢复。

当 CA 根私钥被攻破、遗失、被篡改或泄露，SZCA 启动重大事件应急处理程序，制定行动计划。如果需要吊销 CA 证书，将会采取以下措施：

1. 立即向主管部门汇报，通过网站和其他公共媒体对订户进行通告，采取措施避免用户利益遭受更大损失；
2. 立即通知相关依赖方关闭与证书认证服务相关的系统；
3. 立即吊销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询。同时 SZCA 立即生成新的密钥对；
4. 新的根证书签发后，按照 SZCA CPS 关于证书签发的规定，重新签发下级证书和下级操作中级 CA 证书；SZCA 新的证书签发后，将立即通过 SZCA 信息库、目录服务器、HTTP 等方式发布。

当中级 CA 私钥出现遗失、被篡改、破解、泄露或被第三者窃用的疑虑时，操作 CA 立即向 SZCA 进行汇报并生成新的密钥对和证书请求，申请签发新的证书；

1. SZCA 立即向主管部门汇报，通过网站和其他公共媒体对订户进行通告，采取措施避免用户利益遭受更大损失；
2. 立即通知相关依赖方关闭与证书认证服务相关的系统；
3. 立即吊销所有已经被签发的证书，更新 CRL 和 OCSP 信息，供证书订户和依赖方查询；
4. 新的中级 CA 证书签发后，按照 SZCA CPS 关于证书签发的规定，重新签发订户证书；
5. SZCA 新的证书签发后，将立即通过 SZCA 信息库、目录服务器、HTTP 等方式进行发布。

证书订户的私钥可能出现损毁、遗失、破解、被篡改，或者被第三者窃用时，订户应按照 SZCA CPS 的规定，首先申请证书撤销，并按照规定重新申请新的证书。

In the intentional, man-made, or natural disaster situation, SZCA will take the following steps to restore the secure environment:

1. SZCA verification system’s password is changed by the business administrator, business operators and system administrator;
2. According to the type of disaster, some or all certificates will be revoked or re-verified later;
3. Directory data and CRL are needed for recovery if the directory is unavailable or directory with impure suspicion;
4. Timely access to security site as far as possible to restore operation reasonably;
5. If it is necessary to restore the business administrator's configuration file, it will be done by the system administrator.

If it is necessary to restore the SZCA business operator’s configuration file, it will be done by

another SZCA security business operator or administrator.

When the CA root private key has been damaged, lost, tampered, or leaked, SZCA starts a major emergency treatment process and develops a plan. If the CA certificate needs to be revoked, the following measures will be taken:

1. SZCA reports immediately to the supervising government departments, notifies subscribers through the website and other public media, and takes measures to protect users' interests without more losses;
2. SZCA notifies the relevant relying parties to disconnect the systems associated with the certificate authentication services immediately;
3. SZCA revokes immediately all the certificates issued and updates CRL and OCSP information for subscribers and the relying parties. Meanwhile, SZCA immediately generates a new key pair;
4. After the new root certificate has been issued, SZCA re-issues the certificates and the subordinate CA certificate in accordance with the SZCA CPS about provisions of certificates issuing; After the new root certificate has been issued by SZCA, it will be immediately published by the SZCA repository, LDAP, HTTP, etc.

If the private key of subordinate CA is missing, tampering, cracking, leaking, or used by unauthorized third parties suspiciously, subordinate CA should report immediately to the SZCA and generate a new key pair and certificate request to apply for a new certificate;

1. SZCA reports immediately to the supervising government departments, notifies subscribers through the website and other public media, and takes measures to protect users' interests without more losses;
2. SZCA notifies the relevant relying parties to disconnect the systems associated with the certificate authentication services immediately;

3. SZCA revokes immediately all the certificates issued and updates CRL and OCSP information for subscribers and the relying parties;

4. Subscriber certificate is re-issued in accordance with the provisions of SZCA CPS on the issuance of certificates after the new Subordinate CA certificate has been issued;

5. After the new certificate has been issued, it will be immediately published by the SZCA repository, LDAP, HTTP, etc. for distribution.

When the private key for a subscriber certificate is damaged, missing, cracked, tampered, or used by unauthorized third parties suspiciously, the subscriber should apply for certificate revocation immediately and re-apply for the new certificate following the provisions with the CPS of SZCA.

5.7.4 灾害后的业务连续性能力 Business Continuity Capabilities after a Disaster

SZCA 在遭遇本节 5.7.1、5.7.2 和 5.7.3 中描述的灾难后，通过其备份机制，将在 24 小时之内恢复各项业务的正常运行。

After encountering the disaster described in Sections 5.7.1, 5.7.2, and 5.7.3, SZCA can use the backup mechanisms to recover systems for operation and service delivery within 24 hours.

5.8 电子认证服务机构或注册机构的终止 CA or RA Termination

SZCA 终止事件的原因可以分为密钥受损原因和非密钥受损原因，密钥受损原因可能包括 SZCA 根密钥丢失，非密钥受损原因可能与商业因素有关。

在 SZCA 终止前，必须：

1. 委托业务承接单位；
2. 起草 SZCA 终止声明；
3. 通知与 SZCA 停止相关的实体；
4. 关闭从目录服务器；
5. 证书撤销；
6. 处理存档文件记录；
7. 停止认证中心的服务；
8. 存档主目录服务器；
9. 关闭主目录服务器；
10. 处理 SZCA 业务管理员和 SZCA 业务操作员；
11. 处理加密密钥；
12. 处理和存储敏感文档；
13. 清除 SZCA 主机硬件。

由于密钥受损和非密钥受损原因而终止 SZCA，几乎要完成相同的操作，唯一的不同在 SZCA 终止发送通知的时间限制上，由于密钥受损原因终止 SZCA，要求 SZCA 通知订户的过程尽快完成；由于非密钥受损原因终止 SZCA，在 SZCA 通知所有订户后，采取适当的步骤减轻 SZCA 终止对订户的影响。

The reason for the SZCA termination event may be key damage or non-key damage. Key damage may result from the loss of the SZCA root key, and the non-key damage reason may be related to commercial factors.

Before termination, SZCA must:

1. Arrange the business to undertake;

2. Draft SZCA termination statement;
3. Notify the entities that are related to SZCA termination;
4. Shut down subordinate LDAP;
5. Revoke the certificate;
6. Treat archive file record;
7. Terminate certificate authority service;
8. Archive main LDAP;
9. Shut down the main LDAP;
10. Handle SZCA business administrator and SZCA business operator;
11. Process encryption keys;
12. Process and store sensitive documents;
13. Remove SZCA mainframe hardware.

With the termination of SZCA due to key damage and non-key damage, the operations are mostly the same. The only difference is the time limitation that SZCA stops sending notifications. As for SZCA termination due to key damage, the process in which SZCA notifies the subscriber needs to be completed as soon as possible. As for SZCA termination due to non-key damage, it can take appropriate measures to mitigate the effects of SZCA termination on the subscriber after SZCA notifies all the subscribers.

6.认证系统技术安全控制 Technical Security Controls

6.1 密钥对的生成与安装 Key Pair Generation and Installation

6.1.1 密钥对的生成 Key Pair Generation

6.1.1.1 CA 密钥对生成 CA Key Pair Generation

CA 密钥对由国家密码主管部门批准和许可的设备生成的。密钥的生成、管理、存储、备份和恢复应遵循FIPS140-2标准的相关规定。由于FIPS140-2标准并非是国家密码主管部门认可和支持的标准，国家对于密码产品有严格的管理要求，因此FIPS140-2标准仅参照执行，是在国家密码管理政策许可前提下的选择性适用，具体参照设备厂商提供的资料。用于此类密钥生成的密码模块须通过国家密码主管部门鉴定、认证。

CA密钥对的生成过程需录像或由一名合格的审计师见证以确保其遵循CPS以及角色分离的要求。密钥对生成过程和操作均需记录并保存。

The key pairs of CAs are generated by the cryptographic devices approved and licensed by SCA. The generation, management, storage, backup, and recovery of the key pair shall comply with the relevant regulations of FIPS140-2. Since FIPS140-2 is not a standard approved and accepted by SCA and SCA implements strict management of state's cryptographic products, SZCA only applies part of the provisions of FIPS140-2 under the permission of SCA. Specifically, the product manual of the device is for your reference. Hardware Security Module used for key generation must be evaluated and certified by SCA.

The generation of the CA key pairs shall be video recorded or witnessed by a qualified auditor to ensure the generation process complies with the requirements of this CPS and follow the separation of roles principle. The procedures and operations related to key pair generation shall be recorded and archived.

6.1.1.2 订户密钥对生成 Generation for Subscriber Key Pair

对于SSL/TLS 证书和时间戳证书，订户的密钥对由订户自己生成并保管。

对于符合AATL技术要求的证书及代码签名证书，由订户采用符合标准要求的硬件设备生成密钥对，私钥不能复制和导出，同时必须使用口令激活私钥SZCA通过安全通道将激活口令传递给订户。

证书订户负有保护私钥安全的责任和义务，并承担由此带来的法律责任。如果订户使用弱密钥申请证书，SZCA直接拒绝该申请。

For SSL/TLS certificates and timestamp certificates, subscribers' key pairs are generated and kept by the subscribers themselves.

For certificates and code signing certificates that meet the technical requirements of AATL, subscribers shall use the hardware equipment that meets relevant requirements to generate key pairs, and private keys shall not be duplicated or exported, and the activation of which must require a password. SZCA will deliver the activation passwords to the subscribers through secure channels.

Subscribers have the responsibility and obligation to protect the security of private keys and bear the legal liabilities arising therefrom. If a subscriber uses a weak key to apply for a certificate, SZCA will reject the application directly.

6.1.2 私钥传送给订户 Private Key Delivery to Subscriber

对于 USBKey 内部生成的私钥，由 SZCA 将 USBKey 邮寄给订户；密钥对由订户自行生成的，不需要将私钥传送给订户。

For the private key generated internally by the USBKey, SZCA will mail the USBKey to the subscriber; if subscribers' private keys are generated by their own server or other devices, SZCA will not need to send the private keys to subscribers.

6.1.3 公钥传送给证书签发机构 Public Key Delivery to Certificate Issuer

订户通过 PKCS#10 格式的证书签名请求信息或其它数字签名的文件包格式，以电子文本的方式将公钥提交给 SZCA 签发证书。

The subscriber sends request information, which contains a public key, in digital form encoded as PKCS#10 or other packing formats with digital signature to SZCA for certificate issuance.

6.1.4 电子认证服务机构公钥传送给依赖方 CA Public Key Delivery to Relying Parties

SZCA 的公钥包含在 SZCA 自签发的根 CA 证书和中级 CA 证书中，通过 SZCA 官方网站进行发布。SZCA 支持从 SZCA 的网站下载的方式传递公钥，以供证书订户和依赖方查询使用。

Public keys of SZCA are included in the self-signed root CA certificate and subordinate CA certificate and published via SZCA's website. Subscribers and relying parties can transmit public keys by downloading them from this website.

6.1.5 密钥的长度 Key Sizes

SZCA 支持的 RSA 密钥长度为 2048 位或以上，支持的 SM2 密钥长度为 256 位，支持的 ECC 密钥长度为 256 或以上。如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，SZCA 将会完全遵从。

SZCA supports RSA keys of 2048 bits or more, SM2 keys of 256 bits, and ECC keys of 256 bits or more in length. If national laws and regulations, government authorities, etc. have clear specifications and requirements for key length, SZCA will fully comply with them.

6.1.6 公钥参数的生成与质量检查 Public Key Parameters Generation and Quality Checking

对于使用硬件密码模块的 SZCA 订户，公钥参数必须使用国家密码管理局批准许可的加密设备和硬件介质生成，例如加密机、加密卡、USB Key、IC 卡等生成和选取，并遵从这些设备的生成规范和标准。SZCA 认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

对于参数质量的检查，同样由通过国家密码管理局批准许可的加密设备和硬件介质进行，例如加密机、加密卡、USB Key、IC 卡等。SZCA 认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。

For SZCA subscribers using hardware cryptographic modules, public key parameters must be generated in encryption equipment and hardware medium approved and permitted by State Cryptography Administration, such as encryption machine, encryption card, USB Key, IC card, and follow generation norms and standards of these devices. Of course, SZCA considers that built-in protocols, algorithms for these devices and mediums have already met sufficient levels of security requirements.

The quality of public key parameters is also checked through the encryption equipment and

hardware medium approved and permitted by State Cryptography Administration, such as encryption machine, encryption card, USB Key, and IC cards. Of course, SZCA considers that built-in protocols, algorithms for these devices and mediums have already met sufficient levels of security requirements.

6.1.7 密钥使用目的 Key Usage Purposes

SZCA 的根 CA 密钥仅用于签署以下证书：

（1）代表根 CA 的自签证书；

（2）中级 CA 的证书及交叉证书；

（3）用于基础设施的证书（如 OCSP 响应验证证书）。

订户的密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等；加密密钥对可以用于信息加密和解密。

订户的密钥可用于身份认证、信息加解密、不可抵赖性和信息完整性等安全服务。

SZCA's root CA key is only used to sign the following certificates:

(1) Self-signed Root CA Certificates;

(2) Subordinate CA Certificates and Cross Certificates;

(3) Certificates for infrastructure (e.g. certificates for OCSP response verification).

The subscriber's key can be used to provide security services, such as identity authentication, non-repudiation, and information integrity; cryptographic key pairs can be used for information encryption and decryption.

The subscriber's key can be used to provide security services, such as identity authentication, information encryption and decryption, non-repudiation, and information integrity.

6.2 私钥保护与密码模块工程控制 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 密码模块标准与控制 Cryptographic Module Standards and Controls

SZCA 的密码设备都是经国家密码管理局认可的产品。密钥的生成、管理、存储、备份和恢复应遵循 FIPS140-2 标准的相关规定。SZCA 在选择加密设备时，将在国家密码管理政策许可前提下，选择性、或参照适用 FIPS140-2 标准的要求，具体参照设备厂商提供的资料，且用于密钥生成的密码模块须通过国家密码管理部门鉴定、认证。

Cryptographic devices used by SZCA are approved and licensed by SCA. The generation, management, storage, backup, and recovery of the key pair shall comply with the relevant regulations of FIPS140-2. SZCA selects encryption devices under the premise of the national cryptographic management policy permit, or refers to the applicable requirements of FIPS 140-2, with specific reference to the information provided by the manufacturer. The cryptographic module used for key generation shall be authenticated and certified by the national cryptographic management department.

6.2.2 私钥多人控制 Private Key Multi-Person Control

SZCA 私钥的生成、更新、吊销、备份和恢复等操作采用多人控制机制，即采取 3 选 2 方式，将私钥的管理权限分散到 3 位密钥管理员中，至少在其中 2 人在场并许可的情况下，插入管理员卡并输入 PIN 码，才能对私钥进行操作。

Generation, update, revocation, backup and recovery operations, etc. of SZCA private key adopt multi-person control mechanisms. Namely, the mechanism is two out of three, the key management authority is distributed to three key administrators, the operation of the private key is

performed in the presence and permission of no less than two employees via inserting cards of administrators and inputting their PIN code.

6.2.3 私钥托管 Private Key Escrow

SZCA 无 CA 密钥托管业务。

SZCA has no CA key escrow service.

6.2.4 私钥备份 Private Key Backup

CA 的私钥保存在防高温、防潮湿及防磁场影响的环境中，对私钥的备份操作必须 2 人或以上才可完成，系统初始化生成时进行的 CA 私钥备份。

SZCA 对 CA 的私钥进行备份。订户的签名私钥由订户产生，建议定期自行备份，并对备份的私钥采用口令或其他访问控制机制保护，防止非授权的修改和泄漏。

The CA private key is stored in an environment that is protected from high temperature, humidity, and magnetic fields. The backup operation of the CA private key must be done by 2 or more people during the initial generation of the system.

SZCA makes a backup of the CA private key. The subscriber's signature private key is generated by the subscriber and it is recommended that the private key be backed up periodically and that the backed-up private key be protected by a password or other access control mechanism to prevent unauthorized modification and leakage.

6.2.5 私钥归档 Private Key Archival

CA 私钥到期后，SZCA 对私钥进行归档并保存至少 7 年。私钥通过加密后保存在外部存储介质中，并存放于安全区域。

SZCA 不归档订户的私钥。

After the CA private key expires, SZCA archives and keeps the private key for at least 7 years. The private key is saved in an external storage medium by encryption and stored in a secure area.

SZCA does not archive subscribers' private keys.

6.2.6 私钥导入、导出密码模块 Private Key Transfer into or from a Cryptographic Module

SZCA 不提供订户私钥从硬件密码模块中导出的方法，也不允许如此操作。对于存放在软件密码模块中的私钥，如果订户愿意并且自行承担相关风险，订户可自主选择导入导出的方式，操作时需要采用口令保护等授权访问控制措施。

SZCA does not provide the export of subscriber’s private key from hardware cryptographic module or allow this operation. As for the private key stored in the software cryptographic module, and if the subscriber is willing to bear the relevant risks, he/she can choose the way of import and export with access control such as password, etc.

6.2.7 私钥存储于密码模块 Private Key Storage on Cryptographic Module

CA 系统的密码设备采用国家密码管理局批准和许可的服务器密码机，硬件密码模块至少符合 FIPS 140-2 三级标准或同等级安全水平，私钥的数据存储在服务器密码机硬件中，在整个生命周期都不会明文出现在硬件密码机之外。

订户的私钥存储在符合国家密码管理规定的 USB Key 介质或文件证书中，所有在 USB Key 中存储的私钥，都以密文的形式保存。对于使用软件密码模块生成的私钥，最好在硬件密码模块中存储和使用，订户也可以自主选择使用有安全保护措施的特定软件密码模块。

用于安全存储代码签名证书订户私钥的硬件密码模块至少符合 FIPS 140-2 二级标准或

同等级安全水平。

The CA system's cryptographic device uses a cryptographic server approved and permitted by SCA, with hardware cryptographic modules that reach at least Level 3 of FIPS 140-2 or equivalent levels of security, and the data for the private key is stored in the hardware of the cryptographic server and does not appear in plaintext outside the hardware of the cryptographic server throughout its life cycle.

The subscriber's private key is stored in a USB Key media or file certificate that complies with national cryptographic management regulations. All private keys stored in the USB Key are stored in the form of ciphertext. For private keys generated using the software cryptographic module, they are preferably stored and used in the hardware cryptographic module, or the subscriber may choose to use a specific software cryptographic module with security measures.

The hardware cryptographic module used to securely store the subscriber private key for the code signing certificate at least meets the FIPS 140-2 level 2 standards or equivalent level of security.

6.2.8 激活私钥的方法 Method of Activating Private Key

密钥管理员使用自己的管理员卡登录服务器密码机，进行激活私钥的操作，需要 2 名管理员同时在场。

对于存放在诸如 USB Key、加密卡、加密机或者其他形式的硬件密码模块中的订户私钥，订户可以通过口令、IC 卡等方式进一步保护。当订户计算机上安装了相应的驱动后，将 USB Key、IC 卡等插入相应设备中，输入保护口令，则私钥被激活。对于存放在订户计算机软件密码模块中的私钥，订户应该采用合理的措施从物理上保护计算机，以防止在没有得到用户授权的情况下，其他人员使用订户的计算机和相关私钥。如果存放在软件密码模块中的私钥没有口令保护，那么软件密码模块的加载意味着私钥的激活。如果使用口令保护私钥，软件密码模块加载后，还需要输入口令才能激活私钥。

Key administrators use their own administrative cards to log in to the cryptographic server. Two administrators need to be present for the private key activating operation.

For subscriber private keys stored in, for example, USB Keys, encryption cards, encryption machines, or other forms of hardware cryptographic modules, subscribers can protect them by passwords, IC cards, etc. When the corresponding driver is installed on the subscriber's computer, the private key is activated by inserting the USB Key, IC card, etc. into the corresponding device and entering the protection password. For private keys stored in the subscriber's computer software password module, the subscriber should take reasonable measures to physically protect the computer to prevent other persons from using the computer and the associated private key without the subscriber's authorization. If the private key stored in the software cryptographic module is not password protected, the loading of the software cryptographic module implies the activation of the private key. If a password is used to protect the private key, it is necessary to enter the password to activate the private key after the software cryptographic module is loaded.

6.2.9 解除私钥激活状态的方法 Method of Deactivating Private Key

密钥管理员使用含有自己的管理员卡登录服务器密码机，进行解除私钥的操作，需要 2 名管理员同时在场。

一旦私钥被激活，除非这种状态被解除，私钥总是处于活动状态。在某些私钥的使用当中，私钥每次被激活，只能进行一次操作，如果需要进行第二次操作，需要再次进行激活。

SZCA 解除私钥激活状态的方式包括退出登陆状态、切断电源、将硬件密码模块移开、注销用户或系统等。未经授权的任何人员，绝不可以进行相关操作。

订户解除私钥激活状态由其自行决定，当每次操作后注销计算机，或者把硬件密码模块从读卡器中取出，切断电源时，私钥就被解除。

Key administrators use their own administrative cards to log in to the cryptographic server.

Two administrators need to be present for the private key deactivating operation.

Once a private key is activated, it keeps active unless it is deactivated. For some private keys, they can only be operated once each time they are activated, and if a second operation is required, they need to be activated again.

SZCA can deactivate the private key by logging out, cutting off the power supply, removing the hardware cryptographic module, logging off the user or system, etc. No unauthorized person may ever perform the operation in question.

The subscriber can deactivate the private key at his or her discretion. The private key is deactivated when the computer is logged off after each operation, or when the hardware cryptographic module is removed from the card reader and the power is cut off.

6.2.10 销毁私钥的方法 Method of Destroying Private Key

如果私钥不再被使用，或者与私钥相对应的公钥到期或者被吊销后，如果其处于软件加密模块内，那么该软件加密模块必须被覆盖方式清除；如果位于硬件加密模块内，那么加密设备或者 IC 卡等必须被清空为零。同时，所有用于激活私钥的 PIN 码、IC 卡等也必须被销毁或者收回。

订户的私钥不再被使用，或者与私钥相对应的公钥到期或者被吊销后，由订户决定其销毁方法，订户必须保证有效销毁其私钥，并承担有关的责任。涉及到密钥到期后保存和归档的，订户必须按照本 CPS 的规定执行。

If the private key is no longer in use, or after the corresponding public key is expired or revoked, for the circumstance that the key is in the software encryption module, it must be cleared by methods of mulching. For the circumstance that the key is in the hardware encryption module, it should be cleared in the encryption device or IC card. Meanwhile, all the PIN codes, IC cards for activating the private key also must be destroyed or recovered.

If the subscriber's private key is no longer in use, or the public key corresponding to the

private key expires or is revoked, the method of its destruction shall be determined by the subscriber, and the subscriber must ensure the effective destruction of its private key and assume responsibility therefor. The subscriber must comply with this CPS if the key is saved and archived after expiration.

6.2.11 密码模块的评估 Cryptographic Module Rating

SZCA 使用国家密码管理局批准和许可的密码产品。

SZCA uses the cryptographic products approved and permitted by SCA.

6.3 密钥对管理的其他方面 Other Aspects of Key Pair Management

6.3.1 公钥归档 Public Key Archival

对系统产生的公钥数据进行定时的归档保存，对保存的公钥信息进行对称加密，确保能获取安全完整的公钥信息。公钥到期后，SZCA 定期完成归档操作。

SZCA should carry out archiving and preservation timely for public key data generated by the system and use symmetric encryption for public key information. Ensure to obtain safe and complete public key information. Once the key reaches the expiration date, SZCA will complete the archiving operation regularly.

6.3.2 证书与密钥对使用的有效期 Certificate Operational Periods and Key Pair Usage Periods

密钥对的使用期限与证书的有效期相关一致，对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在

证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外。

对于不同的证书，其密钥对允许通过证书更新的最长使用期限如下：

1.对于根 CA 证书，有效期最长不超过 25 年；

2.对于中级 CA 证书，有效期最长不超过 20 年；

3.对于代码签名证书，有效期最长不超过 39 个月；

4.对于 SSL 服务器证书，有效期最长不超过 398 天，；

5．对于时间戳证书，有效期最长不超过 10 年。

6.对于 PDF 签名证书和邮件证书，有效期最长不超过 3 年。

The use period of the key pair is consistent with the validity period related to the certificate. For a signature certificate, its private key can be used for digital signature only within the validity period of the certificate. The service life of the private key does not exceed the validity period of the certificate. However, in order to ensure that the signed message is verified during the validity period of the certificate, the public key can be used for a period beyond the validity period of the certificate.

For different certificates, the maximum period of use allowed by the certificate renewal for the key pair is as follows:

1. For root CA certificates, valid for a maximum of 25 years;

2. For subordinate CA certificates, valid for a maximum of 20 years;

3. For code signing certificates, valid for a maximum of 39 months;

4. For SSL server certificates, valid for a maximum of 398 days;

5. For timestamp certificates, valid for a maximum of 10 years.

6. For PDF signature certificates and email certificates, valid for a maximum of 3 years.

6.4 激活数据 Activation Data

6.4.1 激活数据的产生与安装 Activation Data Generation and Installation

为了保护私钥的安全，证书订户生产和安装激活数据必须保证安全可靠，从而避免私钥被泄漏、被偷窃、被非法使用、被篡改、或者被非法授权的披露。

CA 私钥的激活数据，必须按照有关密钥激活数据分割和密钥管理办法的要求，严格进行生成、分发和使用。订户私钥的激活数据，包括用于下载证书的口令（以密码信封等形式提供）、USB Key、IC 卡的登陆口令等，都必须在安全可靠的环境下随机产生。

订户私钥的激活数据，包括用于下载证书的口令（（以密码信封等形式提供）、USB Key、IC 卡的登陆口令等，都是在安全可靠的环境下随机产生。这些激活数据，都是通过安全可靠的方式，例如离线当面递交、邮政专递等方式交给订户。对于非一次性使用的激活数据，SZCA 建议用户自行进行修改。

所有的保护口令都应该是不容易被猜到的，应该遵循以下几个原则：

1. 至少 8 位字符；
2. 至少包含一个字符和一个字数；
3. 不能包含很多相同的字符；
4. 不能和操作员的名字相同；
5. 不能使用生日、电话等数字；
6. 用户名信息中的较长的子字符串。

Subscribers must use secure and reliable generation and installation of activation data to protect the private key from exposure, theft, unauthorized usage, modification, or unauthorized disclosure.

Activation data of CA private key must be generated, distributed, and used strictly according to the requirements which are related to the segmentation of key activation data and key management. Activation data of subscriber private key, including password (provided in the form of password envelope, etc.) used to download the certificate, USB Key, login password of IC card, must be generated randomly in secure and reliable environments.

Activation data of subscriber private key, including password (provided in the form of password envelope, etc.) used to download the certificate, USB Key, login password of IC card, are generated randomly in secure and reliable environments. The activation data are delivered to subscribers safely and reliably, such as through offline face-to-face submission, post courier, delivery, etc. For activation data of non-single usage, SZCA suggests users modify the data by themselves.

All the protection passwords should not be guessed easily and should follow the principles as below:

1. Contain at least 8 characters;
2. Contain one character and one letter at least;
3. Not contain many same characters;
4. Not be the same as the operator’s name;
5. Not use birthdays, telephone numbers;
6. Longer substring in user name.

6.4.2 激活数据的保护 Activation Data Protection

对于 CA 私钥的激活数据，必须将激活数据按照可靠的方式分割后由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求。

订户的激活数据必须在安全可靠的环境下产生，必须进行妥善保管，不可被他人所获悉。

如果证书订户使用口令或 PIN 码保护私钥匙，订户应妥善保管好其口令或 PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法窃取。同时为了配合业务系统的安全需要，应该经常对激活数据进行修改。

Activation data of CA private key must be separated in a reliable way and kept by different trusted personnel. The administrator must meet the requirements of responsibility division.

Subscriber’s activation data must be generated in a safe and reliable environment and properly safeguarded, and cannot be leaked to others. If the certificate subscriber uses a password or PIN to protect the private key, the subscriber should take good care of the password or PIN to prevent leakage or theft. If the certificate subscriber uses biological characteristics to protect the private key, the subscriber should also pay attention to preventing his/her biological characteristics from being illegally obtained. Meanwhile, in order to meet the security requirements of business systems, activation data should be modified regularly.

6.4.3 激活数据的其它方面 Other Aspects of Activation Data

当订户私钥的激活数据进行传送时，应保护他们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

当订户私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或者全部，比如记录有口令的在纸页必须粉碎。

Activation data of subscriber's private keys shall be protected from loss, theft, modification, unauthorized disclosure, or unauthorized usage during the transmission.

The activation data of subscriber's private keys which are no longer used shall be destroyed and protected from theft, disclosure, or unauthorized use during the destruction. The result of destruction is that some or all of activation data can’t be recovered directly or indirectly from the residual information and medium, papers recorded with passwords must be shredded.

6.5 计算机安全控制 Computer Security Controls

6.5.1 特别的计算机安全技术要求 Specific Computer Security Technical Requirements

SZCA 对系统的信息安全管理符合国家相关标准和规定的要求，制定全面、完善的安全管理策略和制度，在运营中予以实施、审查和记录。主要的安全技术和控制措施包括：身份识别和验证、逻辑访问控制、物理访问控制、人员职责分权管理、网络访问控制等。

实行严格的双因素验证机制，为每位拥有系统（包括 CA 系统、RA 系统）访问权限的人员分配唯一的账户，账户的访问权限限制为执行工作职责要求的最小权限。访问时同时采用用户名、口令以及数字证书双因素登录方式。

通过严格的安全控制手段，确保 CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。

核心系统必须与其他系统物理分离，生产系统与其他系统逻辑隔离。这种分离可以阻止除指定的应用程序外对网络的访问。使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。

SZCA's information security management of the system meets the requirements of relevant national standards and regulations. SZCA draws up comprehensive and perfect security management strategies and standards, which have been implemented, reviewed, and recorded within the operation. The main security technologies and control measures include identification and authentication, logic access control, physical access control, management of personnel's responsibilities decentralization, network access control, etc.

A dual-factor authentication mechanism shall be utilized in the login process to validate the digital certificate and username/password of users. SZCA assigns each user of the CA/RA system a unique account with minimum permissions according to the requirements of users.

Strict security controls ensure that the system of CA software and data files is secure and reliable and will not be accessed without authorization.

The core system must be separated physically from other systems and the production system must be separated from other systems logically. This separation can prohibit network access except for specific applications. The usage of a firewall is to prevent intrusion from the internal and external network production system and restrict activities of the access production system.

6.5.2 计算机安全评估 Computer Security Rating

SZCA 根据法律法规和主管部门的规定，按照国家计算机安全等级的要求，实现安全等级制度。SZCA 的 CA 系统、网络设备、硬件和系统软件等都经过测试验证后正式验收的合格产品。

SZCA implements a security rating system in accordance with laws, regulations, the provisions of competent authorities, and the national rating requirements for computer security. SZCA's CA system, network equipment, hardware, and system software have been tested, verified, and officially accepted as qualified products.

6.6 生命周期技术控制 Life Cycle Technical Controls

6.6.1 系统开发控制 System Development Controls

SZCA 的软件设计和开发过程遵循以下原则：

1. 制定公司内部的升级变更申请制度，并要求工作人员严格按照流程执行；
2. 制定公司内部的采购流程及管理制度；
3. 开发程序必须在开发环境进行严格测试成功后，再申请部署于生产环境；

4. 变更部署前进行有效的在线备份；

5. 第三方验证和审查；

6. 安全风险分析和可靠性设计。

同时，SZCA 的软件开发操作规范，也同时参考 CMMI 的标准，执行相关的规划和开发控制。

The software design and development process of SZCA follows the principles as below:

1. Establish an internal application system for upgrade and change. The employees should follow this system strictly;

2. Establish an internal purchasing process and management system;

3. After the programs have passed strict tests in the development environment, they can be deployed to the production environment;

4. An effective online backup must be done before deployment changes;

5. Verification and review by third parties;

6. Security risk analysis and reliability design.

The operation specifications for software development, with reference to CMMI standards to perform related planning and development control.

6.6.2 安全管理控制 Security Management Controls

CA 系统使用严格的控制措施，所有的系统都经过严格的测试验证后才进行安全和使用，任何修改和升级会记录在案并进行版本控制、功能测试和记录。SZCA 还对认证系统进行定期和不定期的检查和测试。

SZCA 采用一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

The CA system has strict control measures, and all the systems can be used only after being rigorously tested and verified. Any modifications and upgrades will be recorded for reference and made for version control, functional test, and record. SZCA also carries out regular and irregular inspections and tests on the certification system.

SZCA uses a flexible management system to control, monitor system configuration, and prevent unauthorized modification.

6.6.3 生命期的安全控制 Life Cycle Security Controls

SZCA 认证系统的软硬件设备具备可持续性的升级计划，其中包括了对软、硬件生命周期的安排。

Software and hardware of the SZCA certification system have sustainable upgrade plans such as the arrangement of software and hardware lifetimes.

6.7 网络安全控制 Network Security Controls

SZCA 采用多级防火墙以及其它的访问控制机制保护，其配置只允许已授权的机器访问。只有经过授权的 SZCA 员工才能够进入 SZCA 签发系统、SZCA 注册系统、SZCA 目录服务器、SZCA 证书发布系统等设备或系统。所有授权用户必须有合法的安全证书，并且通过密码验证。

为了确保网络安全，SZCA 认证业务系统安装部署了入侵检测、安全审计、防毒防范和网管系统，并且及时更新防火墙、入侵监测、安全审计、防病毒和网管系统的版本，以尽可能的降低来自于网络的风险。

SZCA is protected by a multi-level firewall and other access control mechanisms that are configured to only allow authorized machines to access. Only authorized SZCA employees can access the SZCA issuing system, SZCA registration system, SZCA LDAP, SZCA certificate issuing system, and other equipment or systems. All authorized users must have legal security

certificates and be authenticated by password.

In order to ensure network security, the SZCA authentication business system has been equipped with intrusion detection, security auditing, virus protection, and network management systems, and updated to the version of the above systems, as much as possible to reduce the risks from the network.

6.8 时间戳 Time-Stamping

SZCA 提供符合 RFC 3161 要求的时间戳服务，时间源采用国家授时中心提供的标准时间。

SZCA provides a time-stamping service that complies with RFC 3161 with a time source that uses standard time provided by the National Timing Center.

7. 证书、证书撤销列表和在线证书状态协议 Certificate, CRL, and OCSP Profiles

7.1 证书 Certificate Profile

SZCA 使用的详细证书格式符合国家相关标准要求，是 ITU-T 推荐的一个国际标准 ITU-T X.509v3（1997）：信息技术-开放系统互连-目录：认证框架（1997 年 6 月）标准和 RFC 5280：Internet X.509 公钥基础设施证书和 CRL 结构（2008 年 5 月）。

The detailed certificate format used by SZCA meets the requirements of relevant national standards and is recommended by ITU-T as an international standard ITU-T X.509v3 (1997): information technology - open systems interconnection - the directory: authentication framework (June 1997) standard and RFC 5280: Internet X.509 public key infrastructure certificate and CRL structure (May 2008).

7.1.1 版本号 Version

SZCA 签发的证书符合 X.509 V3 版证书格式。

The certificate issued by SZCA conforms to the format of X.509 V3 certificates.

7.1.2 证书扩展项 Certificate Extensions

SZCA 除了使用 X.509 V3 版证书标准项和标准扩展项以外，还使用了自定义扩展项。

- 证书标准项

1.证书版本号(Version)

指明 X.509 证书的格式版本，值为 V3。

2.证书序列号（Serial Number）

即由 SZCA 通过 CSPRNG 生成大于 0 且长度为 64 位的非序列性的证书序列号，是证书唯一的数字型标识符。

3.签名算法标识符（Signature）

指定由 SZCA 签发证书时所使用的签名算法。

4.签发机构名（Issuer）

用来标识签发证书的 CA 的 X.500 DN 名字。即 SZCA 各个属性，包括国家、省、市、机构、单位部门、和通用名。例如：

CN = SZCA EV SSL CA

OU = IT Dept

O = SZCA

L = Shenzhen

S = Guangdong

C = CN

5.证书有效期（Validity）

用来指定证书的有效期，包括证书开始生效的日期和时间以及失效的日期和时间。每次使用证书时，需要检查证书是否在有效期内。

6.证书主体（Subject）

指定证书持有者的 X.500 的甄别名。包括国家、省、市、机构、单位部门和通用名，还可包含 email 地址等个人信息等。

SSL 证书，通用名应包含与服务器关联的用户所拥有或控制，且为主体别名扩展项之一的的域名或 IP 地址；EV SSL 证书的通用名只能为域名，不能为 IP 地址，不能为通配符。

7.证书持有者公开密钥信息（subject Public Key Info）

证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值；公开密钥使用的算法标识符。此标识符包含公开密钥算法和 hash 算法。

- 证书扩展项

1.颁发机构密钥标识符（authorityKeyIdentifier）

颁发机构密钥标识符扩展提供了一种方式，以识别与证书签名私钥对应的公钥。当颁发者由于有多个密钥共存或由于发生变化而具有多个签名密钥时使用该扩展。

2.主体密钥标识符（subjectKeyIdentifier）

本项提供一种识别包含有一个特定公钥的证书的方法。此扩展标识了被认证的公开密钥。它能够区分同一主体使用的不同密钥（例如，当密钥更新发生时）。

3.密钥用法 (key usage)

指定各种密钥的用法：电子签名，不可抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证 CRL 签名，只加密，只解密，只签名。

4.CRL 发布点

由 SZCA 指定的 CRL 发布点。

5.主题替换名/主题别名

非关键项，包括证书用户所拥有、控制的与其服务器关联的所有域名或 IP 地址。EV 证书该项不能包含通配符或 IP 地址。

6.机构信息访问

包含证书颁发机构 SZCA 的 OCSP 响应的 HTTP URL（accessMethod = 1.3.6.1.5.5.7.48.1），

及颁发证书的 OCSP 的响应的 HTTP URL（accessMethod = 1.3.6.1.5.5.7.48.2）。通过访问该地址，能够获取 SZCA 的 CA 证书及其颁发的用户证书的状态信息。

In addition to the X.509 V3 certificate standard items and standard extension items, SZCA also uses customized extensions.

- Certificate standard items

1. Version

This field describes the version of X.509 certificates, with the value of V3.

2. Serial Number

As a unique integer assigned to each certificate by SZCA through CSPRNG, the serial number is a non-sequential certificate sequence number greater than 0 with 64 bits in length.

3. Signature Algorithm Identifier

The algorithm identifier is used to identify a signing algorithm used by SZCA to issue the certificate.

4. Issuer

The issuer field identifies X.500 DN of CA that has signed and issued the certificate, namely each attribute of SZCA, including country, province, city, organization, department, and common name. For example:

CN = SZCA EV SSL CA

OU = IT Dept

O = SZCA

L = Shenzhen

S = Guangdong

C = CN

5. Validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate, including two dates: the date on which the certificate validity period begins and the date on which the certificate validity period ends. The validity must be checked each time the certificates are used.

6. Subject

The subject field identifies X.500 DN of subscribers, including country, province, city, organization, department, and common name. It may also contain email addresses and other personal information.

The common name of SSL certificates shall contain the domain name or IP address owned or controlled by the user associated with the server and is one of the subject alternative name extensions; the common name of EV SSL certificates can only be the domain name, instead of the IP address or wildcard.

7. Subject Public Key Info

This field is used to carry the public key and identify the algorithm with which the key is used. This identifier identifies the public key algorithm and hash algorithm.

- Certificate Extensions

1. Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover).

2. Subject Key Identifier

The subject key identifier extension provides a means of identifying certificates that contain a particular public key. The extension identifies the authorized public key. It provides a means to identify different keys used by the same subject (e.g. when rekeying).

3. Key Usage

The key usage extension defines the purpose (e.g., electronic signature, non-repudiation, key encryption, data encryption, key protocol, certificate signature verification, CRL signature validation, only encryption, only decryption, and only signature) of the key contained in the certificate.

4. CRL Distribution Points

It refers to CRL Distribution Points specified by SZCA.

5. Subject Replacement Name/ Subject Alternative Name

Non-critical items, including all domains or IP addresses that are owned and controlled by certificate users, and associated with their servers. The EV certificate item cannot contain wildcards or IP addresses.

6. Authority Information Access

It contains the HTTP URL of the OCSP response from the certificate authority SZCA (accessMethod = 1.3.6.1.5.5.7.48.1), and the HTTP URL of the response from the OCSP that issues the certificate (accessMethod = 1.3.6.1.5.5.7.48.2). The information about the status of SZCA's CA certificates, and the user certificates SZCA issues can be obtained by accessing the address.

7.1.3 算法对象标识符 Algorithm Object Identifiers

SZCA 签发的证书中，密码算法的标识符为 sha256RSA、 sha384RSA、SM3withSM2。

The signing algorithm identifiers of certificates issued by SZCA include sha256RSA,

sha384RSA, and SM3withSM2.

7.1.4 名称形式 Name Forms

SZCA 签发的证书名称形式的格式和内容符合 X.501 Distinguished Name(DN)的甄别名格式。

SSL/TLS 证书主题项不能仅含有诸如“.”,“-”,“ ”空格字符，或其他任何表示该项为空、不完整、或不适用的内容。

The name of certificates issued by SZCA is formatted in accordance with X.501 Distinguished Name (DN).

SSL/TLS certificate subject items cannot only contain metadata such as ".", "-" and " " (empty) characters and/or any other indication that the value/field is absent, incomplete, or not applicable.

7.1.5 名称限制 Name Constraints

不适用。

Not applicable.

7.1.6 证书策略对象标识符 Certificate Policy Object Identifier

EV SSL 证书策略对象标识符：1.2.156.115215.1.4.1 及 2.23.140.1.1 (Baseline Requirements 要求)

OV SSL 证书策略对象标识符：1.2.156.115215.1.4.2.2 及 2.23.140.1.2.2 (Baseline Requirements 要求)

DV SSL 证书策略对象标识符：1.2.156.115215.1.4.2.1 及 2.23.140.1.2.1 (Baseline

Requirements 要求)

EV 代码签名证书策略对象标识符：1.2.156.115215.1.5.1 及 2.23.140.1.3

普通代码签名证书策略对象标识符：1.2.156.115215.1.5.2 及 2.23.140.1.4.1

邮件证书策略对象标识符：1.2.156.115215.1.3.1

个人证书策略对象标识符：1.2.156.115215.1.1.1

机构证书策略对象标识符：1.2.156.115215.1.2.1

EV SSL policy object identifier: 1.2.156.115215.1.4.1 and 2.23.140.1.1 (Baseline Requirements)

OV SSL policy object identifier: 1.2.156.115215.1.4.2.2 and 2.23.140.1.2.2 (Baseline Requirements)

DV SSL policy object identifier: 1.2.156.115215.1.4.2.1 and 2.23.140.1.2.1 (Baseline Requirements)

EV code signing certificates policy object identifier: 1.2.156.115215.1.5.1 and 2.23.140.1.3

Common code signing certificates policy object identifier: 1.2.156.115215.1.5.2 and 2.23.140.1.4.1

Email certificates policy object identifier: 1.2.156.115215.1.3.1

Personal certificates policy object identifier: 1.2.156.115215.1.1.1

Authority certificates policy object identifier: 1.2.156.115215.1.2.1

7.1.7 策略限制扩展项的用法 Usage of Policy Constraints Extension

不适用。

Not applicable.

7.1.8 策略限定符的语法和语义 Policy Qualifiers Syntax and Semantics

不适用。

Not applicable.

7.1.9 关键证书策略扩展项的处理规则 Processing Rules for the Critical Certificate Policies Extension

不适用。

Not applicable.

7.2 证书撤销列表 CRL Profile

SZCA 定期签发 CRL（证书撤销列表），供用户查询使用。 SZCA 签发的 CRL 遵循 RFC5280 标准。

SZCA issues CRL regularly for the subscribers to query. CRLs issued by SZCA follow the RFC 5280 standard.

7.2.1 版本 Version

SZCA 的证书撤销列表采用 X.509 v2 版的证书格式。

The CRLs issued by SZCA are formatted in accordance with X.509 v2.

7.2.2 CRL 项与 CRL 条目扩展项 CRL and CRL Entry Extensions

SZCA 的证书撤销列表（CRL）是一个带有时间戳并且经过数字签名的已吊销证书的列表。CRL 的签发者是 CA，SZCA 通过发布 CRL 提供它所签发的数字证书的状态信息。

（1）CRL 的版本号：用来指定 CRL 的版本信息，SZCA 采用的是同 X.509 V3 证书对应的 CRL V2 版本。

（2）签名算法：SZCA 采用 sha256RSA、sha384RSA、SM2withSM3 签名算法。

（3）颁发者：指定签发机构的 DN 名，由国家、省、市、机构、单位部门和通用名等组成。

（4）生效时间：指定一个日期/时间值，用以表明本 CRL 发布的时间。

（5）更新时间：指定一个日期/时间值，用以表明下一次 CRL 将要发布的时间（本标准强制使用该域）。

（6）吊销证书列表：指定已经吊销的证书列表。本列表中含有证书的序列号和证书被吊销的日期和时间。

（7）颁发机构密钥标识符（Issuer Unique Identifier）：本项标识用来验证在 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥。

The CRL of SZCA is a revoked certificate list with a timestamp and digital signature. The issuer of CRL is CA. SZCA provides certificate status information through releasing CRL.

(1) CRL version: It refers to version information of CRL. SZCA adopts CRL V2 corresponding to X.509 V3 certificate.

(2) Signature algorithm: SZCA adopts sha256RSA, sha384RSA, and SM2withSM3 signature algorithms.

(3) Issuer: It refers to DN of issuing authority, including country, province, city, organization,

department, common name, etc.

(4) Effective time: It refers to the date/time which indicates CRL issuing time.

(5) Update time: It refers to the date/time which indicates the next issuing time of CRL. (It's an enforced field in this CPS).

(6) Certificate Revocation List: It refers to a list of revoked certificates. The list contains the certificate serial number and revocation date and time.

(7) Issuer Unique Identifier: It is used to authenticate the public key which is used to verify the signature of CRL. It can distinguish different keys used by the same CA.

7.3 在线证书状态协议 OCSP Profile

SZCA 采用 IETF PKIX 工作组开发的一个在线证书状态协议 (Online Certificate Status Protocol，OCSP，RFC6960)，该协议定义了一种标准的请求和响应信息格式以确认证书是否被吊销了。

SZCA 签发的 OCSP 响应至少包含以下所述的 OCSP 机构基本域和内容：

1. Version：客户端使用的 OCSP 协议的版本号；SZCA 的在线证书状态协议为 v1 版；
2. signatureAlgorithm：签发 OCSP 的算法；
3. responderID：签发 OCSP 的实体。签发者公钥的 SHA1 数据摘要值和证书甄别名；
4. producedAt：OCSP 响应生成的日期和时间；
5. Signature：OCSP 响应消息的数字签名；
6. Nonce(一次性随机数)：在状态请求消息中的每一个 requestExtensions 变量和响应消息中的 responseExtension 变量中包含一次性随机数，防止重放攻击；
7. 证书状态：证书的最新状态，包括有效、吊销和未知。

SZCA adopts an Online Certificate Status Protocol (OCSP, RFC6960) developed by the IETF

PKIX working group. This protocol defines standard request and response information formats to query whether a certificate is revoked.

The OCSP response message issued by SZCA contains at least OCSP organization basic domains and contents described below:

1. Version: OCSP protocol version number used by the client. The version of SZCA OCSP is v1;
2. SignatureAlgorithm: Algorithm used for signing and issuing OCSP;
3. ResponderID: ID of the entity that issues OCSP. It consists of SHA1 of the issuer's public key and DN of the certificate;
4. ProducedAt: Date and time when OCSP response message is generated;
5. Signature: Digital signature of OCSP response message;
6. Nonce: The nonce, which is used to prevent replay attacks, is included in requestExtensions variable of the state request message and responseExtension of response message;
7. Certificate status: The latest status of the certificate, including effective, revocation, and unknown.

7.3.1 OCSP 请求和响应处理 Processing of OCSP Request and Response

一个 OCSP 请求包含以下数据：协议版本、服务要求、目标证书标识和可选的扩展项等。

在接受一个请求之后，OCSP 服务端响应时进行如下检测：

SZCA 的 OCSP 响应符合 RFC6960 标准。客户通过 http 协议访问 SZCA 的 OCSP 服务， SZCA 会对查询请求进行检查， OCSP 签名证书包括 RFC6960 定义的 id-pkix-ocsp-nocheck 的扩展项。

- 信息正确格式化
- 响应服务器被配置提供请求服务
- 请求包含了响应服务器需要的信息，如果任何一个先决条件没有满足，那么 OCSP 服务端将产生一个错误信息；否则的话，返回一个确定的回复

所有确定的回复都由证书签发者密钥进行数字签名，主要回复状态包括：证书有效、已吊销、未知。回复信息由以下部分组成：

- 回复语法的版本
- 响应服务器名称
- 对请求端证书的回复
- 可选扩展
- 签名算法对象标识符号
- 对回复信息散列后的签名

如果出错，OCSP 服务器会返回一个出错信息，这些错误信息没有 SZCA 证书签发者密钥的签名。出错信息主要包括：

- 未正确格式化的请求（malformedRequest）
- 内部错误（internalError）
- 请稍后再试（trylater）
- 需要签名（sigRequired）
- 未授权（unauthorized)

An OCSP request contains the following data: protocol version, service request, target certificate identifier, and optional extensions.

After receiving a request, the OCSP server carries out the following tests during response:

SZCA's OCSP response complies with RFC6960. The client accesses SZCA's OCSP service via the http protocol, and SZCA will check the query request. The OCSP signing certificate includes the extension of id-pkix-ocsp-nocheck as defined in RFC 6960.

- Information is formatted correctly
- The response server is configured to provide the request services
- The request contains all the information needed by the response server. If any pre-condition is not met, the OCSP server will return an error message. Otherwise, it returns a determinate response.

All determinate responses are signed by the certificate issuer key. The main response statuses are valid, revoked, and unknown. The response message consists of the following components:

- Reply syntax version
- Response server name
- Response to the request client certificate
- Optional extensions
- Signature algorithm object identifier
- The signature after the response information is hashed

If an error occurs, the OCSP server will return an error message, which doesn't contain the key signature signed by the SZCA certificate issuer. The error message includes:

- malformedRequest
- internalError
- trylater
- sigRequired
- unauthorized

8. 认证机构审计与其它评估 Compliance Audit and Other Assessments

8.1 评估的频率或情形 Frequency and Circumstances of Assessment

SZCA 将开展以下评估：

（1）外部评估

根据我国《电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等法律法规，接受主管部门的年度评估和检查。

根据国际和国内标准，接受第三方审计机构的定期 Webtrust 审计。

（2）内部评估

SZCA 运营安全管理小组，按照监管法律法规、CPS/CP 及其他 SZCA 内部的管理制度规章，定期进行内部审查，频率通常为每年一次，特殊情况除外。

SZCA will conduct the following assessments:

(1) External assessment

It is subject to annual assessment and inspection by the competent authorities in accordance with the laws and regulations of China, such as the *Electronic Signature Law*, the *Measures for the Administration of Electronic Certification Services,* and the *Measures for the Administration of Passwords for Electronic Authentication Services*.

It will receive regular Webtrust audits by third-party auditors in accordance with international

and national standards.

(2) Internal assessment

The SZCA Operational Safety Management Team, in accordance with regulatory laws and regulations, CPS/CP, and other internal SZCA management system regulations, conducts regular internal reviews, usually at a frequency of once a year, except in exceptional circumstances.

8.2 评估者的资质 Qualifications of Assessor

外部审计机构，应熟悉 IT 运营管理、具备多年审计经验，审计师的要求如下：

（1） 熟练掌握公钥基础设施技术，具备信息安全工具和技术，信息技术和安全审计有关的第三方认证服务资质；

（2） 能够按照审计标准独立进行审计;

（3） 具备 WebTrust 认证服务资质;

（4） 受法律、政府法规或职业道德规范的约束。

内部审计人员为运营安全管理小组或其指定人员。

External auditors shall be familiar with IT operations management and have many years of audit experience. The auditor requirements are as below:

(1) Proficiency in the technology of public key infrastructure, with information security tools and the qualification for third-party certification services related to the audit of information technology and security;

(2) Able to conduct audits independently in accordance with auditing standards;

(3) Qualified for WebTrust certification services;

(4) Bound by law, government regulations, or professional codes of ethics.

The internal auditors shall be the Operational Safety Management Team or its designated personnel.

8.3 评估者与被评估者的关系 Assessor's Relationship to Assessed Entity

第三方评估者与 SZCA 之间没有任何的业务、财务往来，或者其它任何足以影响评估客观性的利害关系。

SZCA 的内部评估者与 CA 的系统管理员、业务管理员、业务操作员工作岗位可信人员不重叠。

There are no businesses or financial dealings between the third-party assessor and SZCA, or any other interest sufficient to affect the objectivity of the assessment.

SZCA's internal assessor does not overlap with trusted personnel such as CA's System Administrator, Business Administrator, and Business Operator.

8.4 评估内容 Topics Covered by Assessment

评估内容包括但不限于以下：

（1）CA 物理环境和控制；

（2）密钥管理操作；

（3）基础 CA 控制；

（4）证书生命周期管理；

（5）CA 业务规则的执行；

（6）是否存在其他可能的安全风险。

第三方审计师事务机构按照 WebTrust 最新的有效审计标准中的要求，对 SZCA 进行独

立审计。

The assessment includes, but is not limited to, the following:

(1) CA physical environment and controls;

(2) Key management operations;

(3) Basic CA controls;

(4) Certificate lifecycle management;

(5) Implementation of CA business rules;

(6) Determination of whether there are other possible security risks.

The third-party auditing agency performs independent audits of SZCA as required in WebTrust's most recent standards for effective audit.

8.5 对问题与不足采取的措施 Actions Taken to Address Problems and Deficiencies

第三方审计机构的评估，SZCA 将根据评估结果检查缺失和不足，提交纠正改进和预防措施以及整改计划书，并接受其对整改计划的审查，以及对整改情况的再次评估。

SZCA 完成内部评估后，评估人员需要列出所有问题项目的详细清单，交由相关职能部门评估和改进，解决问题，并将结果书面通知 SZCA 运营安全管理小组。

For the assessment by a third-party auditor, SZCA will check for deficiencies and shortcomings based on the results of the assessment, submit corrective improvement and preventive measures and a corrective action plan, and accept its review of the corrective action plan and re-assessment of the corrective action.

Once SZCA has completed the internal assessment, the assessor is required to make a detailed list of all problem items, refer them to the relevant functions for assessment and improvement, resolve the issues and notify the SZCA Operational Safety Management Team in writing of the results.

8.6 评估结果的传达与发布 Communications of Results

对于内部审计结果由 SZCA 运营安全管理小组在公司内部进行传达和公布，对于第三方外部审计机构评估的结果，SZCA 将在公司官网(www.szca.com)进行公布。如果审计的结果可能对订户造成安全隐患，SZCA 应及时向订户通报。

任何第三方向被评估实体通知评估结果或者类似的信息，都必须事先明确向 SZCA 表明通知的目的和方式，并征得 SZCA 的同意，法律另有规定的除外；SZCA 保留在这方面的法律权力。

For internal audits, the results are communicated and published internally by SZCA Operational Safety Management Team, and for the results assessed by third-party external auditors, SZCA will publish them on the company's official website (www.szca.com). SZCA will notify the subscribers of any potential security risks timely.

Third-party should communicate its purposes and methods to SZCA in advance and obtain the consent of SZCA before notifying the evaluation entity of the assessment results or similar information, except otherwise defined by law; SZCA reserves the legal rights in this part.

8.7 自我评估 Self-assessment

同本 CPS 8.1。

Same as this CPS 8.1.

9. 法律责任和其它业务条款Other Business and Legal Matters

9.1 费用 Fees

9.1.1 证书签发与更新费用 Certificate Issuance or Renewal Fees

根据市场、物价部门及行业主管部门的规定，SZCA 将收取合理的证书及相关服务费用。在订户向 SZCA 提出各种证书申请要求时，SZCA 提前告知订户 SZCA 证书签发等各种证书管理行为的收费项目、标准与方式。

SZCA will charge reasonable fees for certificates and related services in accordance with the regulations of the market, price departments, and industry authorities. When a subscriber requests various certificates from SZCA, SZCA will inform the subscriber in advance of the items, standards, and methods of fees for various certificate management acts such as certificate issuance by SZCA.

9.1.2 证书查询费用 Certificate Access Fees

SZCA 暂不收取此项收费，但保留对此项服务收费的权利。

SZCA does not charge this fee temporarily but reserves the right to charge for this service.

9.1.3 证书状态信息查询费用 Status Information Access Fees

SZCA 暂不收取此项收费，但保留对此项服务收费的权利。

SZCA does not charge this fee temporarily but reserves the right to charge for this service.

9.1.4 其它服务费用 Fees for Other Services

SZCA 保留收取其他服务费的权利。

SZCA reserves the right to charge other service fees.

9.1.5 退款策略 Refund Policy

如 SZCA 违背本 CPS 所规定的责任或义务，订户可以要求撤销证书并退款。否则，SZCA 对订户收取的费用均不退还。完成退款后，订户如果继续使用该证书，SZCA 将追究其法律责任。

If SZCA violates its defined responsibilities or obligations under this CPS, subscribers can request SZCA to revoke certificates and refund. Otherwise, any fees charged by SZCA to the subscriber are non-refundable. After refund completion, if a subscriber continues to use the certificate, SZCA shall investigate his/her legal liabilities.

9.2 财务责任 Financial Responsibility

9.2.1 保险范围 Insurance Coverage

不适用。

Not applicable.

9.2.2 其他资产 Other Assets

SZCA 确保具有足够的财务实力来维持其正常经营并保证相应义务的履行，并合理地承担对订户及对依赖方的责任。

SZCA ensures that it has sufficient financial strength to maintain its normal operations and to ensure that the corresponding obligations are met and that it is reasonably liable to its subscribers and relying parties.

9.2.3 对最终实体的保险与担保 Insurance or Warranty Coverage for End-entities

目前，SZCA 仅根据《电子签名法》的规定，对于由于 SZCA 的原因给订户造成的直接损失予以限额赔偿。根据订户所使用的证书的类型，赔付的额度有所不同，具体的赔付标准同本 CPS 9.8。在适当的情况下，SZCA 将安排采购适当的保险或作出符合监管部门要求其他方式的赔偿安排（例如赔偿保证存款金）。

Currently, SZCA only provides limited compensation for direct losses caused to subscribers due to SZCA in accordance with the provisions of the *Electronic Signature Law*. Payments vary depending on the type of certificate used by the subscriber and are subject to the same payout criteria as this CPS 9.8. Where appropriate, SZCA will arrange to procure appropriate insurance or make arrangements for indemnification (such as indemnification of guaranteed deposits) that meet regulatory requirements in other ways.

9.3 业务信息保密 Confidentiality of Business Information

9.3.1 保密信息范围 Scope of Confidential Information

保密信息包括但不限于以下内容：

1. SZCA 与 SZCA 授权的注册机构之间、SZCA 及其授权的注册机构与订户之间、SZCA 与其它证书服务相关方、SZCA 关联方之间的协议、往来函和商务协定等；
2. 与订户证书公钥配对的私钥；
3. SZCA 的审计日志及其他审计文件等；
4. 有关 SZCA 认证体系的运营信息；
5. 灾备计划、应急方案、安全措施等内部流程管制文件；
6. 订户证书信息以外的非公开信息等。

以上信息除非法律明文规定或政府、执法部门等的要求，或 SZCA 认为有必要，SZCA 没有义务也不会对外公布或披露。

Confidential information includes, but is not limited to, the following:

1. Agreements, correspondence, and business agreements between SZCA and SZCA-authorized registrars, between SZCA and its authorized registrars and subscribers, between SZCA and other certificate service-related parties, and SZCA affiliates;
2. A private key paired with the subscriber's certificate public key;
3. SZCA's audit log and other audit documents;
4. Information on the operation of the SZCA certification system;
5. Internal process control documents such as disaster preparedness plans, contingency plans, security measures, etc.;
6. Non-public information other than subscriber certificate information, etc.

The above information is not obligated and will not be released or disclosed by SZCA to the public unless expressly required by law or requested by government or law enforcement

authorities, etc., or unless SZCA deems it necessary.

9.3.2 非保密信息 Non-confidential Information

非保密信息包括以下内容：

1. SZCA 公布或提供的与证书申请及使用有关的指导说明性文件、及 CPS 等；
2. 订户证书中包括的相关公开信息，如订户公钥等；
3. 证书状态及吊销列表信息；
4. 其他可以通过公共、公开渠道获得的信息。

虽然上述属非保密信息，并不意味着其能够被第三方任意不被授权的商业性使用，对于利用非保密信息的第三方主体，SZCA 和信息的所有人保留追究其法律责任的权利。

其它：SZCA 信息的保密性取决于特殊的数据项和申请。

Non-confidential information includes the following:

1. Instructional documents published or provided by the SZCA relating to the application and use of certificates, and the CPS;
2. Relevant public information in the subscriber certificate, such as the subscriber's public key;
3. Certificate status and revocation list information;
4. Other information available through public, open channels.

Although the above information is non-confidential, it does not mean that it can be used by third parties for arbitrary and non-authorized commercial purposes, and SZCA and the owner of the information reserve the right to pursue legal liability against third party subjects who make use of non-confidential information.

The confidentiality of SZCA information depends on special data items and applications.

9.3.3 保护保密信息的责任 Responsibility to Protect Confidential Information

SZCA、任何订户、依赖方以及与认证业务相关的参与方等，均有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

SZCA 制定员工信息保密管理规范，并与员工签订保密协议，且会对所有员工进行信息保密的相关培训，规范员工访问、获取及使用上述保密信息的行为，保障 SZCA 的证书管理工作严格符合信息保密的相关法律规定要求。

当机密信息的所有者要求 SZCA 公开或披露其保密信息，SZCA 按在法律法规规定和订户的要求进行公开；同时，机密信息持有者应向 SZCA 提供书面授权文件，说明授权公开信息意愿，公开的方式、内容和范围。如发生与该获授权的保密信息披露行为相关或由此引发的任何第三方的损失赔偿，SZCA 不承担责任，由订户负责赔偿所有损失，包括 SZCA 的损失在内。

当 SZCA 按照法律法规、司法机关裁判文书的要求，必须披露具有保密性质的信息时，SZCA 可以向执法部门披露相关的保密信息。这种披露不视为违反保密的要求和义务。

SZCA, any subscriber, relying parties, and participants in connection with the certification business, etc., are obligated to assume the appropriate responsibilities to protect confidential information in accordance with the provisions of this CPS.

SZCA develops norms for the confidential management of employee information, and signs confidentiality agreements with employees. Besides, it will conduct training on information confidentiality for all employees to regulate employee access, obatining, and use of the above confidential information, and ensure that SZCA's certificate management strictly conforms to the requirements of the relevant legal provisions on information confidentiality.

When the owner of confidential information requests SZCA to disclose or reveal its confidential information, SZCA shall disclose it in accordance with the provisions of laws and regulations and the subscriber's request; and at the same time, the holder of confidential information shall provide SZCA with a written authorization document stating its intention to authorize the disclosure of information, the manner, content, and scope of the disclosure. SZCA shall not be liable for any damages to any third party in connection with or arising out of such authorized disclosure of confidential information, and the subscriber shall be responsible for all damages, including those of SZCA.

When SZCA is required to disclose information of a confidential nature in accordance with laws and regulations and judicial authority adjudication documents, SZCA may disclose the relevant confidential information to law enforcement authorities. Such disclosure is not considered a violation of the requirements and obligations of confidentiality.

9.4 个人信息保密 Confidentiality of Personal Information

9.4.1 隐私保护方案 Privacy Plan

SZCA 尊重所有订户的隐私。SZCA 的隐私保护策略，按照法律法规的要求和国际公认的个人数据隐私保护原则执行。一旦出台新的与保护隐私相关的法律，本 CPS 将自动予以引用并将之作为隐私保护的基本依据来执行。

任何人选择使用 SZCA 的任何服务，就意味着表示已经同意接受 SZCA 有关隐私保护的制度。

SZCA respects the privacy of all subscribers. SZCA's privacy protection policy is implemented in accordance with the requirements of laws and regulations and internationally recognized privacy protection principles for personal data. When new laws relating to the protection of privacy are introduced, this CPS will automatically refer to them and enforce them as the basic basis for privacy protection.

By choosing to use any of SZCA's services, any person agrees to be bound by SZCA's system of privacy protection.

9.4.2 作为隐私处理的信息 Information Treated as Privacy

SZCA 在管理和使用订户申请、注册证书时提供的相关信息时，除了证书已经包括的信息及证书状态信息外，该订户的基本信息和身份认证资料，非经订户同意，或法律法规作出规定，及相关司法机关裁判要求，绝对不会任意对外公开。

When managing and using the relevant information provided by subscribers for certificate application and registration, SZCA will not arbitrarily disclose the subscriber's basic information and identification information to the public without the consent of the subscribers, or as stipulated by laws and regulations, and as required by the judgment of the relevant judicial authority, except for the information already included in the certificate and certificate status information.

9.4.3 非隐私的信息 Non-private Information

订户的公钥证书内包括的信息，以及该证书的状态信息等，是可以公开的，将不被视为隐私信息。

The information contained in the subscriber's public key certificate, as well as the status information of the certificate, is publicly available and will not be considered private information.

9.4.4 保护隐私的责任 Responsibility to Protect Private Information

SZCA、任何订户、依赖方以及与认证业务相关的参与方等，都有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

当 SZCA 在任何法律法规、或者司法机关在合法程序的要求下，或者信息所有者书面

授权的情况下，SZCA 可以向特定对象披露相关的隐私信息。这种披露不被视为违反隐私保护义务。与披露行为相关的或由此引发的损失，SZCA 无须为此承担任何责任。

SZCA, any subscriber, relying parties, and participants in connection with the certification business, etc., are obligated to assume the appropriate responsibilities to protect confidential information in accordance with the provisions of this CPS.

SZCA may disclose private information to specific recipients when required to do so by any law or regulation, or by a judicial authority in a lawful proceeding, or when authorized in writing by the owner of the information. Such disclosure is not considered a violation of privacy protection obligations. SZCA shall not be liable for any loss in connection with or arising out of the act of disclosure.

9.4.5 使用隐私信息的告知与同意 Notice and Consent to Use Private Information

SZCA 采取适当的步骤保护证书订户的个人隐私信息，并将采取可靠的安全手段保护已存储的个人隐私信息。

SZCA 在有关法律法规规定或者司法机关、行政执法机关等有权机关通过合法程序的要求下，或者信息所有者书面授权的情况下向特定对象披露隐私信息时，无需告知订户的义务。

SZCA 与其授权注册机构在 CPS 规定的隐私政策及业务范围内使用获取的任何订户信息。如果需要将订户隐私信息用于双方约定的用途以外的目的，在法律允许的情况下，事前需告知订户并征得其书面同意，获得订户的授权证明。

SZCA takes appropriate steps to protect the certificate subscriber's personal privacy and takes reliable security measures to protect stored personal privacy information.

SZCA is not required to inform subscribers of its obligation to disclose private information to specific recipients when required to do so by relevant laws and regulations or by a competent

authority such as a judicial or administrative law enforcement agency through a lawful procedure, or when authorized in writing by the owner of the information.

SZCA and its authorized registrars use any subscriber information obtained in accordance with the privacy policy and within the scope of business as set forth by CPS. If it is necessary to use the subscriber's private information for purposes other than those agreed upon by the parties, the subscriber must be informed in advance with his or her written consent to obtain the subscriber's certificate of authorization if permitted by law.

9.4.6 依司法或行政程序进行信息披露 Disclosure Pursuant to Judicial or Administrative Process

除非符合下列条件之一，否则 SZCA 会将订户的个人隐私信息提供给任何第三方主体：

1. 订户书面授权同意 SZCA 披露的；
2. 执法部门、政府或其他法律上授权的部门依据法律法规向 SZCA 提出要求的；
3. CPS 中规定的可以披露的情形。

证书订户因自身的原因，向 SZCA 提出隐私信息披露申请的，SZCA 将根据书面授权文件或相关协议对相关信息进行披露。经授权同意进行的披露行为，如发生任何与披露相关的或由于披露该隐私信息所造成的任何损失、及不利影响，SZCA 一律不承担任何责任。

SZCA will provide subscriber's private information to any third-party subject unless one of the following conditions is met:

1. The subscriber authorizes SZCA to make disclosure in writing;
2. The law enforcement department, government, or other legally authorized department makes requirements to SZCA in accordance with laws and regulations;
3. Disclosure as specified in the CPS.

If the subscriber of the certificate submits an application for privacy information disclosure to SZCA for its own reasons, SZCA will disclose the relevant information according to the written authorization document or relevant agreement. SZCA will not be liable for any loss or adverse effect arising out of or in connection with the disclosure of such private information in connection with the disclosure of which consent has been given.

9.4.7 其他信息披露情形 Other Information Disclosure Circumstances

其他为用户提供服务所必需对相关服务商、供应商提供的信息。

Other information provided to relevant service providers and suppliers that is necessary for the provision of services to users.

9.5 知识产权 Intellectual Property Rights

SZCA 享有并保留对证书以及 SZCA 提供的全部软件、文档、数据的全部知识产权，包括保证证书和软件的完整权、冠名权、著作权和利益分享权等。

所有与 SZCA 发行的证书和 SZCA 提供的软件相关的一切版权、商标和其它知识产权均属于 SZCA 所有，上述知识产权包括但不限于相关的 SZCA 的规范性文件、CP/CPS、技术支持文件和使用手册等各种数据、信息、资料。SZCA 的其他电子认证服务机构在征得 SZCA 的授权同意后，可以使用相关的文件和手册。

在没有 SZCA 事先书面同意的情况下，任何使用者在任何证书到期、作废或效力终止后，不能商业性地使用任何 SZCA 使用的名称、商标、或可能与之相混淆的名称、商标或商务称号。

SZCA enjoys and reserves all intellectual property rights to the certificate and all software, documents, and data provided by SZCA, including the right to guarantee the integrity of the certificates and software, the naming right, copyright, and benefit-sharing right.

All copyrights, trademarks, and other intellectual property rights related to the certificates issued by SZCA and the software provided by SZCA belong to SZCA, and the said intellectual property rights include, but are not limited to, SZCA's relevant normative documents, CP/CPS, technical support documents and user manuals and other various data, information and materials. Other electronic certification service providers of SZCA may use the relevant documents and manuals with the authorized consent of SZCA.

No user may commercially use any name or trademark used by SZCA, or name, trademark, or trade designation which may be confused with the foresaid one, after the expiration, revocation, or termination of the validity of any certificate, without the prior written consent of SZCA.

9.6 陈述与担保 Representations and Warranties

9.6.1 电子认证服务机构的陈述与担保 CA Representations and Warranties

1. SZCA 遵守电子签名法及相关法律法规要求，依据 CPS 流程签发订户证书，对签发证书承担相应的法律责任；
2. 根据 CPS 3.2 的要求验证申请人的身份；
3. 将向证书订户通报任何已知的，将在本质上影响订户的证书的有效性和可靠性事件。
4. 验证申请者对列在证书主题字段及主题别名扩展中的域名及 IP 地址拥有使用权或控制权；
5. 验证申请者证书（申请）的意愿，及证书申请代理人/代表人代表订户申请证书的授权；
6. 验证证书中所包含的全部信息的准确性（主体的机构部门名称属性项除外），降低证书主题所包含的除机构部门名称属性项外的信息存在误导的可能性；
7. 将根据 CPS 的要求及时吊销证书。
8. 若 SZCA 与订户无关联，则 SZCA 与订户是合法有效且可执行的用户协议双方，

该用户协议符合 CA/浏览器论坛发布的 Baseline Requirements 等要求；若 SZCA 与订户为同一实体或有关联，则申请人代表已认可使用条款；

9. 针对所有未过期的证书的当前状态信息（有效或已吊销）建立及维护全天候的（24x7）公开的信息库。

1. SZCA complies with the requirements of the *Electronic Signature Law* and related laws and regulations, issues subscriber certificates in accordance with the CPS procedure, and assumes the corresponding legal responsibility for issuing certificates;
2. SZCA verifies the identity of the applicant in accordance with the requirements of CPS 3.2;
3. SZCA informs subscribers of any known events, which will fundamentally affect the validity and reliability of the certificate.
4. SZCA verifies that the applicant has the right to use or control the domain name and IP address listed in the certificate subject field and Subject Alternative Name extension;
5. SZCA verifies the applicant's intention to apply for a certificate (application) and the authorization of the agent/representative of the certificate applicant to apply for the certificate on behalf of the subscriber;
6. SZCA verifies the accuracy of all information contained in the certificate (except for the subject's agency name attribute item) and reduces the likelihood that the information contained in the certificate subject other than the agency name attribute item is misleading;
7. SZCA will revoke certificates in a timely manner as required by the CPS.
8. If SZCA is not affiliated with the subscriber, then SZCA and the subscriber shall be parties to a legally valid and enforceable user agreement that meets the Baseline Requirements published by the CA/Browser Forum; if SZCA and the subscriber are the same entity or are affiliated, then the applicant representative shall have accepted the terms of use;
9. SZCA creates and maintains a 24x7 public repository for the current status information (valid or revoked) of all valid certificates.

9.6.2 注册机构的陈述与担保 RA Representations and Warranties

经 SZCA 合法程序获得授权的注册机构 RA 保证：

1. 遵循本 CPS、CP 和 SZCA 的授权协议、业务管理规范及其它 SZCA 的认证业务标准和流程，依法受理并处理证书申请；
   1) 根据证书申请材料，采取法律法规及本 CPS 规定的合理措施，对订户的身份进行鉴别与验证。如注册机构对订户的证书申请材料审查没有通过，注册机构有向订户进行告知的义务；
   2) 注册机构应在规定的时间内完成证书申请处理；
   3) 注册机构有义务通知订户阅读 SZCA 发布的 CP、CPS 以及其它相关规定，在订户完全知晓并同意 CP、CPS 和证书服务协议内容的前提下，为订户办理数字证书；
   4) 在 SZCA 生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请者的信息不一致；
   5) 注册机构须对订户的信息及与认证相关的信息妥善保存，并于适当的时间转交 SZCA 归档。
2. 遵循 SZCA 制订的业务处理规范、业务运营规范、系统运作规范及其他运营服务管理规范等；
3. 依据 SZCA 的授权设置各类下级证书服务受理机构，包括 RA、LRA 等，并按照行业法律及 SZCA 的各种运营服务管理规范，对其进行监督和管理等；
4. 按照 SZCA 的要求，通过安全通道将证书信息传给 CA 机构。
5. 接受 SZCA 根据本 CPS 和授权协议对 RA 进行管理，包括接受服务资质审核和规

范执行检查，根据相关协议内容配合 SZCA 需要的电子认证业务合规性审计。

RA (registration authority) authorized by the legal procedure of SZCA, guarantees to:

1. Follow the authorization agreements, business management specifications of this CPS, CP, and SZCA, and other certification business standards and processes of SZCA to receive and handle certificate applications in accordance with the law;

    1) Take reasonable measures stipulated by laws and regulations and this CPS to identify and verify the identity of the subscriber based on the certificate application materials. The registration authority is obliged to inform the subscriber if the application materials for a certificate fail to pass the review;

    2) The registration authority shall complete the processing of the application for a certificate within the prescribed time period;

    3) The registration authority is obliged to inform the subscriber to read the CP, CPS, and other relevant regulations issued by SZCA, and to handle a digital certificate for the subscriber on the premise that the subscriber is fully aware of and agrees to the contents of the CP, CPS and certificate service agreement;

    4) When generating certificates, SZCA does not allow the inconsistencies between certificate information and certificate applicant information due to mistakes of registration authority;

    5) The registration authority shall keep the subscriber's information and the information related to the certification in a safe place and forward it to SZCA for archiving in due course.

2. Follow the business processing norms, business operation norms, system operation norms, and other operational service management norms established by SZCA;

3. Set up various subordinate certificate service acceptance authorities, including RAs,

LRAs, etc., according to the authorization of SZCA, and supervise and manage them in accordance with industry laws and various operation and service management specifications of SZCA;

4. Transmit certificate information to the CA through a secure channel as required by SZCA.

5. Accept SZCA's management of the RA in accordance with this CPS and the authorization agreement, including the audit of service qualification and check of specification execution, and cooperate in the audit of compliance of the electronic certification business required by SZCA in accordance with the relevant agreement.

9.6.3 订户的陈述与担保 Subscriber Representations and Warranties

订户一旦接受 SZCA 签发的证书，就被视为向 SZCA、注册机构及信赖证书的有关当事人作出以下承诺：

1. 已了解并接受 SZCA 的用户协议和本 CPS 中的所有条款和条件。
2. 在证书的有效期内使用证书，证书一旦被撤销，不再使用证书。
3. 订户在申请证书时向 SZCA 或其注册机构提供的信息都是真实、完整和准确的，愿意承担任何提供虚假、伪造等信息的法律责任。
4. 与订户证书所含公钥相对应的私钥所进行的每一次签名，都是订户自己的签名，并且在进行签名时，证书是有效证书（证书没有过期、吊销），证书的私钥为订户本身访问和使用。
5. 一经接受证书，订户就应当承当如下责任：始终保持对其私钥的控制，使用可信的系统，采取合理、安全的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用；
6. 不得拒绝任何来自 SZCA 公示过的声明、改变、更新、升级等，包括但不限于策略、规范的修改和证书服务的增加和删减等。

7. 证书在本 CPS 中规定使用范围内合法使用，只将证书用于经过授权的或其他合法的使用目的。
8. 对于 SSL 证书，订户有责任和义务保证只在证书中列出的主题别名对应的服务器中部署证书。
9. 若发现以下情况，订户应立即向 SZCA 申请吊销证书：1）证书中的信息为或将成为错误或不准确的信息；2）证书中与公钥有关的私钥被误用或被损坏；3）有证据表明，该代码签名证书被用于签署可疑代码。

Once subscribers accept a certificate issued by SZCA, the subscriber is considered to make the following commitments to SZCA, registration authority, and related parties who trust the certificate:

1. Have acknowledged and accepted all the terms and conditions of the SZCA user agreement and this CPS.
2. Use the certificate for the duration of its validity; once the certificate is revoked, it shall no longer be used.
3. All information that the subscriber provides to SZCA or its registration authority during the certificate application process must be true, complete, and accurate. The subscriber is willing to take legal responsibility for any false or forged information.
4. Each signature made by the private key corresponding to the public key contained in the subscriber certificate is the subscriber's own signature, and the certificate used at the time of signing is a valid certificate (the certificate has not expired or is revoked), and the private key of the certificate is used by the subscriber for access and use.
5. Once the certificate is accepted, the subscriber should assume the following responsibilities: always maintain control of their private keys; use trustworthy systems; and take reasonable and safe precautions to prevent the loss, disclosure, alteration, or unauthorized usage of the private keys;
6. Prohibited for rejecting any statements, changes, updates, and upgrades published by SZCA, including but not limited to modification of strategies and standards as well as additions and deletions of certificate services.

7. The subscriber uses the certificate only for authorized or other lawful purposes within the range specified by this CPS.
8. For SSL certificates, the subscriber has the responsibility and obligation to ensure that the certificate is only deployed on the server corresponding to the Subject Alternative Name listed in the certificate.
9. Subscribers shall promptly request the revocation of their certificates by SZCA in case of the following situations: 1) any information in the certificate is or becomes incorrect or inaccurate; 2) there is any misuse or compromise of the subscriber's private key associated with the public key included in the certificate; 3) there is evidence that such code signing certificates are used to sign suspicious codes.

9.6.4 依赖方的陈述与担保 Relying Party Representations and Warranties

依赖方在信赖任何 SZCA 签发的证书时保证：

1. 熟悉所信赖所使用的类型的证书所对应的 CPS 及证书策略，了解证书的使用目的和可获得的保证，只在符合本 CPS 规定的证书应用范围内信任该证书；
2. 依赖方在信任证书前，须同意依赖方协议中的条款，并根据使用的环境和条件判断该证书是否可信任；
3. 在信赖 SZCA 签发的证书前，已经对证书进行过合理的检查和审核，包括：检查 SZCA 公布的最新的 CRL 或 OCSP 获得该证书的状态，确认该证书没有被吊销；检查该证书信任路径中所有出现过的证书的可靠性；检查该证书的有效期以及适用范围；检查其它能够影响证书有效性的信息；

一旦由于疏忽或者其它原因未履行合理检查的义务，依赖方愿意承担因此造成的自身或他人的损失，并且就此对 SZCA 带来的损失进行补偿。

4. 对证书的信赖行为，表明依赖方已经接受本 CPS 有关依赖方权利义务责任的所有规

定，尤其是其中有关免责、限制责任及担保和义务的条款；

5. 信任证书前确认证书记载内容与信任所需的证明是一致的；

6. 依赖方须承担因未履行以上责任所产生的法律责任。

When relying on any certificate issued by SZCA, the relying parties ensure to:

1. Be familiar with the CPS and certificate policy corresponding to the type of certificate being relied upon, understand the purpose for which the certificate is to be used and the assurances that can be obtained, and trust the certificate only to the extent that it conforms to the application in this CPS;

2. Before trusting a certificate, relying parties must agree to the terms in the relying party agreement and judge whether the certificate can be trusted in light of the circumstances and conditions of use;

3. Before trusting a certificate issued by the SZCA, the relying parties have reasonably checked and reviewed the certificate, including checking the status of the latest CRL or OCSP published by SZCA to obtain the certificate and confirming that the certificate has not been revoked; checking the reliability of all certificates that have appeared in the certificate's trust path; checking the validity of the certificate and its scope of application; checking other information that can affect the validity of the certificate;

In the event of failure to perform a reasonable inspection due to negligence or other reasons, the relying parties shall be liable for any loss caused to themselves or others and shall indemnify SZCA for such loss.

4. Trusting the certificate indicates that the relying parties have accepted all provisions of this CPS relating to the rights and obligations and liabilities of the relying parties, in particular, the provisions therein relating to the exclusion, limitation of liability, and warranties and obligations;

5. Confirm that the content in the certificate is consistent with the certificate required for trust before trusting the certificate;
6. The relying parties shall be liable for any legal liability arising from their failure to perform the above liabilities.

9.6.5 其它参与方的陈述与担保 Representations and Warranties of Other Participants

所有其他 SZCA 电子认证活动的参与方，均需遵守本 CPS 的规定。

All other participants in SZCA's electronic certification activities shall comply with this CPS.

9.7 担保免责 Disclaimers of Warranties

除本 CPS 9.6.1 中明确承诺的外，SZCA 不随担其他任何形式的保证和义务：

1. 不保证证书订户、信赖方、其他参与者的陈述内容。
2. 不对电子认证活动中使用的任何软件做出保证。
3. 不对证书在超出规定目的以外的应用承担任何责任。
4. 对由于不可抗力，如战争、自然灾害等造成的服务中断并由此造成的客户损失承担责任。
5. 订户违反本 CPS 9.6.3 之承诺时，SZCA 不承担责任；
6. 证书依赖方违反本 CPS 9.6.4 之承诺时，得以免除 SZCA 的责任；

Except for the commitments declared in CPS 9.6.1, SZCA does not assume any other forms of guarantee and obligation:

1. Do not guarantee the statements of certificate subscribers, relying parties, and other participants.
2. Do not guarantee any software used in electronic certification activities.

3. Do not assume any liability when the certificate is used beyond the prescribed purposes.
4. Do not assume any responsibility for the service interruption and customer losses caused by force majeure, such as war, and natural disasters.
5. When subscribers violate the commitments defined in CPS 9.6.3, SZCA shall not be liable for it;
6. When relying parties violate the commitments defined in CPS 9.6.4, SZCA can be exempt from liability;

9.8 有限责任 Limitations of Liability

SZCA 仅为 CPS 规定的认证服务提供赔偿，且当事人提出赔偿请求，需提供相应的合法证明材料，如法院或仲裁机构的裁决文书等。但 SZCA 能证明是按照《电子签名法》、《电子认证服务管理办法》等认证服务行业法律法规，及在工信部备案的 CPS 提供服务的，则 SZCA 不具过错，无需向订户或依赖方进行赔偿或补偿。

SZCA 对订户、依赖方的损失赔偿责任，是一种限额责任。且 SZCA 只对因使用、信赖证书而产生的直接损害负责，而不承担对间接损害、利润利息损失、精神损害等的赔偿责任，及惩罚性赔偿等责任。

除非有关特定证书的生效的法院裁决或仲裁机关的裁定对赔偿金额另有规定，SZCA 及其授权的注册机构，就每份证书对于该证书关系所有参与人（包括但不限于订户、依赖方）合计的赔偿金额，限制在下述数额的范围内（单位：人民币元）：

SZCA only provides indemnities for the certification services stipulated by the CPS, and the party requesting indemnities needs to provide the appropriate legal supporting documents, such as the court or arbitration body's award document. However, if SZCA can prove that the services are provided in accordance with the *Electronic Signature Law*, the *Measures for the Administration of Electronic Certification Services,* other laws and regulations of the certification service industry, and the CPS filed with the Ministry of Industry and Information Technology, then SZCA is not at

fault and is not required to indemnify or compensate the subscribers or the relying parties.

SZCA's liability for losses to subscribers and relying parties is limited. Furthermore, SZCA is only liable for direct damages arising from the use and reliance on the certificate, but not for indirect damages, loss of interest on profits, moral damages, and punitive damages.

Unless otherwise specified in a court decision or arbitration award in force in respect of a particular certificate, the amount of indemnity payable by SZCA and its authorized registration authorities to all participants (including, but not limited to, subscribers and the relying parties) of that certificate in aggregate is limited to the following amounts (in RMB):

证书类型	赔偿金额上限
DV SSL 证书	50,000 元（RMB）
OV SSL 证书	400,000 元（RMB）
EV SSL 证书	800,000 元（RMB）
EV 代码签名证书	300,000 元（RMB）

Type of Certificate	Maximum Amount of Indemnity
DV SSL Certificate	RMB 50,000
OV SSL Certificate	RMB 400,000
EV SSL Certificate	RMB 800,000
EV Code Signing Certificate	RMB 300,000

每份证书的赔偿责任均有限额，无论数字签名费用、交易损失的多少，也不考虑提出索赔请求主体人数或索赔额度。

该限额内的赔偿款项的支付，依据的是生效的支持索赔请求的法院判决书或仲裁机构的

仲裁裁决。赔偿款项的赔付，按照索赔人向 SZCA 提交有效的裁判文书或裁决书的顺序进行，不论该限额赔偿在多个索赔者直接如何分配。对于限额赔偿完毕后的其他主体的赔付请求，SZCA 对于超出赔偿限额部分的赔偿请求不予赔偿。

The liability for indemnity for each certificate is limited regardless of the cost of the digital signature, the amount of the transaction loss, or the number of claim requesting parties, or the amount of the claim.

The payment of indemnities within this limit is based on a court judgment in force supporting the claim or an arbitral award by an arbitral body. Payments are made in the order in which the claimant files a valid adjudicative instrument or award with the SZCA, regardless of how the limited indemnity is distributed directly among multiple claimants. SZCA does not indemnify other requesting parties against the claims that exceed the indemnity limits after the limited indemnity has been paid.

9.9 赔偿 Indemnities

1.CA 机构的赔偿 Indemnification by CAs

订户或依赖方进行的民事活动因 SZCA 提供的认证服务而遭受的损失,如 SZCA 签发内容有误的证书或证书失误签发交付给订户外主体、或 SZCA 造成密钥失密泄露、SZCA 在订户申请资料提交不全或虚假且明知的情况下签发内容不实的证书等，SZCA 将依据本条款进行相应的赔偿。对于委托第三方的，SZCA 和受托第三方间的责任按照合同进行分配，但首先应由 SZCA 按照本款要求对损失各方履行全部赔偿责任。

除了 CA 是政府实体的情况之外，CA 应对每个应用软件供应商进行辩护，赔偿并保护其免受此类应用软件供应商因发出的证书而遭受的任何和所有索赔、损害和损失。但是，这不适用于此类应用软件供应商因 CA 颁发的证书而遭受的任何索赔、损害或损失，此类索赔、损坏或损失直接由此类应用软件供应商的软件显示为不值得信任的证书仍然有效或显示为可信：（1）已过期的证书，或（2）已被吊销的证书（但仅限于当前可从 CA 在线获取吊销

状态的情况，以及应用程序软件未能检查此状态或忽略吊销状态的指示）。

SZCA shall indemnify the subscribers or the relying parties in accordance with these Terms and Conditions for any loss or damage suffered by the subscribers or the relying parties as a result of the certification services provided by SZCA, such as the issuance of a certificate with incorrect content by SZCA or the delivery of a certificate to a subject other than the subscribers by mistake, or the disclosure of the key caused by SZCA, or the issuance of a certificate with inaccurate content by SZCA in the event that the subscribers submit incomplete or false application information and are aware of such inaccuracy. Where a third party is entrusted, the liability between SZCA and the entrusted third party shall be allocated in accordance with the contract, but first, SZCA shall perform all the liability for indemnifying the parties that suffer losses as required by this paragraph.

Except where CA is a governmental entity, CA shall defend, indemnify and hold harmless each application software provider from any and all claims, damages and losses suffered by such application provider as a result of the certificate issued. However, this shall not apply to any claim, damage, or loss suffered by such application software provider as a result of a CA-issued certificate, where such claim, damage, or loss is directly attributable to such application software provider's software indicating that an untrustworthy certificate is still valid or shown to be trustworthy: (1) an expired certificate, or (2) a revoked certificate (but only to the extent that the revocation status is currently available online from CA and the application software fails to check this status or ignores the indication of the revocation status).

2.订户的赔偿责任 Indemnification by Subscribers

有下列情形之一的，订户应承担相应的损失赔偿责任：

(1) 订户申请注册证书时，故意、过失提供不真实、不完整、不准确的申请材料，造成SZCA、注册机构或者第三者遭受损害的；

(2) 证书信息发生变更时未停止证书使用并及时通知 SZCA 及其授权的证书服务机构；

(3) 订户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有通知依赖方、SZCA 及其授权的证书服务机构；

(4) 没有对证书私钥采取有效的安全保护措施或在不安全的系统使用证书，造成私钥丢失、被盗或者泄露等；

(5) 将私钥及证书不当交付他人使用，造成 SZCA、依赖方遭受损害的；

(6) 将证书用于非本 CPS 规定的其它用途或业务范围的，或者将证书用于法律法规禁止的违法犯罪活动；

(7) 证书被吊销（包含但不限于证书到期）期间仍然使用证书；

(8) 其他订户使用证书违反本 CPS 及相关操作规范的情形。

在订户提出证书撤销请求后，到 SZCA 实际完成吊销该证书的期间，如果该证书被用以进行非法交易，或者发生其他相关证书使用纠纷的，如果 SZCA 按照本 CPS 的规范进行有关操作，相关证书纠纷产生的法律责任由订户自行承担。

SZCA 与订户签署的协议另有赔偿规定的，从其规定。

The subscriber shall be liable for damages in any of the following cases:

(1) Subscribers who, when applying for certificate registration, intentionally or negligently provide untrue, incomplete, or inaccurate application materials, causing damage to SZCA, registration authorities, or third parties;

(2) Failure to stop using the certificate or notify SZCA and its authorized certificate service provider in time when the certificate information is changed;

(3) Subscribers intentionally or negligently cause the leakage or loss of its private key and fail to notify the relying parties, SZCA, and its authorized certificate service provider, knowing that the private key has been leaked or lost;

(4) Failure to take effective security protection measures for the private key of the

certificate or use the certificate in an insecure system, resulting in the loss, theft, or leakage of the private key;

(5) Improper delivery of the private key and certificate to another person for use, resulting in damage to SZCA and the relying party;

(6) Use of the certificate for other purposes or business scope than those specified in this CPS, or for illegal and criminal activities prohibited by laws and regulations;

(7) Use of a certificate while it is revoked (including but not limited to its expiration);

(8) Other circumstances in which subscribers' use of the certificates violates this CPS and related codes of practice.

During the period between the subscriber's request for certificate revocation and the actual completion of the revocation of such certificate by SZCA, if such certificate is used for illegal transactions or other related disputes occur, the subscriber shall bear the legal liability arising from the related certificate disputes if SZCA performs the relevant operations in accordance with the specifications of this CPS.

If the agreement between SZCA and the subscriber provides otherwise for indemnification, the provisions shall prevail.

3. 依赖方的赔偿责任 Indemnification by Relying Parties

用户使用或信赖证书时，未能依照本 CPS 4.5.2 和 9.6.4 中有关依赖方责任和义务等规范履行合理审核、注意义务，导致 SZCA 或第三方遭受损害的，依赖方将对上述主体的损失进行赔偿。

If the user fails to perform the duty of reasonable review and care in accordance with the norms of sections of 4.5.2 and 9.6.4 in this CPS regarding the duties and obligations of the relying party when using or relying on the certificate, which results in damage to SZCA or a third party, the relying party will indemnify the said party for the losses.

9.10 有效期与终止 Term and Termination

9.10.1 有效期限 Term

本 CPS 自发布之日起正式生效，文档中将详细注明版本号及发布日期，最新版本的 CPS 请访问 SZCA 网站下载获取，对具体个人不做另行通知，新发布的 CPS 自动取代废止旧 CPS。

This CPS is effective from the date of release, and the version number and release date will be detailed in the document. Please visit the SZCA website to download the latest version of the CPS, without notice to specific individuals. The new CPS automatically replaces and repeals the old CPS.

9.10.2 终止 Termination

本 CPS 及其更新版本在 SZCA 终止电子认证服务时失效。在终止服务六十日前向工信部等主管部门报告，并做出妥善安排。

This CPS and its updates expire when SZCA terminates the electronic certification service. SZCA shall report to the Ministry of Industry and Information Technology and other competent authorities sixty days prior to termination of service and make proper arrangements.

9.10.3 效力的终止与保留 Effect of Termination and Survival

在本 CPS 中涉及审计、保密信息、隐私保护、归档、知识产权的条款，以及涉及 SZCA 赔偿责任及有限责任的条款，在本 CPS 终止后仍然继续有效存在。

The provisions of this CPS relating to audits, confidential information, privacy protection, archiving, intellectual property rights, and those relating to SZCA's liability and limited liability, shall remain valid after the termination of this CPS.

9.11 对参与者的个别通告与沟通 Individual Notices and Communications with Participants

SZCA 及其授权注册机构在必要的情况下，如在提前终止 CPS 时，会通过适当方式，如电话、电子邮件、信函、传真等，个别通知订户、依赖方。订户或依赖方如有需要，也可以通过 SZCA 的联系方式向 SZCA 咨询了解 SZCA 终止的相关业务处理情况。

SZCA and its authorized registration authorities will notify subscribers and the relying parties individually by appropriate means, such as telephone, e-mail, letter, and fax, if necessary, in the case of early termination of the CPS. Subscribers or relying parties may also contact SZCA based on SZCA's contact information to konw the handling of the business terminated by SZCA if necessary.

9.12 修订 Amendments

9.12.1 修订程序 Procedure for Amendment

SZCA 将根据法律法规要求及业务实际需要，对 CPS 内容进行适当的必要的修改、调整。CPS 编写小组每年至少审查一次本 CPS，确保其符合国家法律法规和主管部门的要求及相关国际标准，符合 CP 的要求，符合认证业务开展的实际需要。

具体修订程序详同本 CPS 1.5.4“CPS 批准程序”。修订版本的 CPS 将报工信部备案，且在 SZCA 的网站上公布，自公布之日起生效。

SZCA will make appropriate and necessary changes and adjustments to the CPS in accordance with the requirements of laws and regulations and the actual requirements of the business. The CPS compilation team reviews this CPS at least once a year to ensure that the CPS meets the requirements of national laws and regulations and administration department as well as relevant international standards, the requirements of CP and actual needs of certification business operations.

The amendment procedures are detailed in this CPS 1.5.4, "CPS Approval Procedures". The revised version of the CPS will be filed with the Ministry of Industry and Information Technology, published on the SZCA's website, and effective from the date of publication.

9.12.2 通知机制与期限 Notification Mechanism and Period

SZCA 有权修订本 CPS 中任何术语和条款，而且无须预先通知任何一方。

SZCA 在网站 https://www.szca.com 信息库中公布修订内容，及修订后的 CPS 完整版本，自修订后的 CPS 公布之日起该 CPS 生效。有关 CPS 修改内容的处理，以修改后的 CPS 条款为准进行。

SZCA 在认为有必要时，或应订户或依赖方请求，可以采取邮寄、电子邮件等的方式向上述主体在申请证书过程中提交的地址、邮箱，发送书面（包含电子 CPS）的 CPS。

若订户在修订后的 CPS 发布后 15 日内未提出证书撤销请求的，视为同意受该 CPS 约束。

SZCA shall have the right to amend any term and clause in this CPS without prior notice to any party.

SZCA publishes the revisions, and the full version of the revised CPS in the repository on the website (https://www.szca.com), and the CPS is effective as of the date of publication of the revised CPS. The processing of CPS modifications shall be subject to the clauses of the modified CPS.

SZCA may send a written (including electronic CPS) CPS by mail, email, etc. to the address and email address submitted by the above parties in the certificate application process, if deemed necessary or at the request of the subscriber or relying party.

Subscribers are deemed to be bound by the revised CPS if they do not submit a request for revocation of the certificate within 15 days of the issuance of the revised CPS.

9.12.3 业务规则必需修改的情形 Circumstances under Which CPS Must be Changed

如果出现下列情况，必须对 CPS 进行修订：

1. CPS 披露流程、业务范围、技术等不满足电子认证业务的需求；
2. 认证系统和有关管理规范发生重大升级或改变；
3. 法律法规和主管部门的要求；
4. 现有 CPS 出现重要缺陷；
5. CPS 内容与管辖的法律法规要求、CA/B 论坛最新发布的相关规范、WebTrust 审计要求不一致时。

The CPS must be revised in case of:

1. CPS disclosure processes, the scope of operations, technology, etc. do not meet the requirements of the electronic certification business;
2. Significant upgrades or changes to the certification system and related management specifications;
3. The requirements of laws and regulations and the competent authorities;
4. Significant deficiencies in the existing CPS;
5. Inconsistencies between the CPS content and governing laws and regulations, the latest relevant specifications published by the CA/B Forum, and the WebTrust audit requirements.

9.13 争议处理 Dispute Resolution Provisions

SZCA、证书订户、依赖方等实体在电子认证活动中产生争议可按以下步骤解决：

（1）根据本 CPS 中的规定，明确责任方；

（2） 由 SZCA 相关部门负责与申请人协调；

（3）若协调失败，再由有关法律部门进行裁决；

（4）任何与 SZCA 或注册机构就本 CPS 所涉及的任何争议提起诉讼的，受 SZCA 注册所在地人民法院管辖。

If SZCA, certificate subscribers, relying parties and other entities have disputes in the electronic certification activities, the following steps can be taken for resolution:

(1) Confirm the party to be held responsible according to this CPS;

(2) SZCA's related departments are responsible for coordinating with the applicants;

(3) If coordination fails, these parties should reach out to the legal authorities;

(4) Prosecutions against SZCA or its RA over any disputes arising from this CPS should be governed by the people's court in the place where SZCA is registered.

9.14 管辖法律 Governing Laws

有关证书、证书策略及具体类型证书对应的 CPS 的任何争议，包括适用、解释、有效性等各种争议，无论订户或依赖方居住于何地或者其在何处使用证书，都应适用证书签发地，即 SZCA 及其注册机构所在地（住所地）的法律。

Any dispute regarding the certificate, the certificate policy, and the CPS corresponding to a specific type of certificate, including various disputes regarding its application, interpretation, validity, etc., shall be governed by the laws of the place where the certificate is issued, i.e. the place (domicile) where SZCA and its registration authorities are located, regardless of where the subscriber or the relying party resides or where it uses the certificate.

9.15 与适用法律的符合性 Compliance with Applicable Law

SZCA 的各项策略，均遵守并符合中华人民共和国的法律和国家工信部等主管部门的要求。

SZCA's strategies comply with and conform to the laws of the People's Republic of China

and the requirements of other competent authorities such as the Ministry of Industry and Information Technology.

9.16 一般条款 Miscellaneous Provisions

9.16.1 完整协议 Entire Agreement

本 CPS 将替代先前的与该主题相关的书面或口头说明、解释，并与订户协议、依赖方协议及其他补充协议构成 SZCA 与各方参与者之间的完整协议。

This CPS shall supersede the previously written or oral statements, explanations, and interpretations relating to the subject matter and, together with the Subscriber Agreement, the Relying Party Agreement, and other supplemental agreements, shall constitute the entire agreement between SZCA and all participants.

9.16.2 转让 Assignment

本 CPS 中规定的认证实体各方的权利和义务，如需进行转让，各方当事人应按照法律的相关规定进行。

If the rights and obligations of each party of the certification entity specified in this CPS need to be transferred, each party shall do so in accordance with the relevant provisions of the law.

9.16.3 分割性 Severability

如果本 CPS 的任何条款或其应用由于与 SZCA 所在管辖区的法律产生冲突而被判定为无效或不具执行力时，SZCA 可以在最低必要的限度下修订该条款，使其继续有效，其余部分不受影响。

在根据根据修订后的 CPS 要求签发证书之前，SZCA 将发送邮件至 question@cabforum.org，通知 CA/B 论坛 CPS 中已修订的信息，并确认其已被发至公共邮件列表和存在于公共档案列表(https://cabforum.org/pipermail/public/)。

若 CPS 制定依据的法律失效，或 CA/B 论坛的 Baseline Requirements 等规范被修改，则本 CPS 中与此相关的任何对 SZCA 业务操作的调整将不再继续适用。SZCA 因此对业务操作进行的相关调整，对 CPS 的修订，及向 CA/B 论坛的通知将在 90 天内完成。

In case any clause or provision of this CPS is held to be unenforceable or invalid due to any conflicts with the laws of any jurisdiction in which SZCA operates, SZCA may modify any conflicting clause or provision to the minimum extent necessary to make them continue to be valid, and other clauses and provisions will remain valid without being affected.

SZCA will (and prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of any modified content in the CPS by sending emails to question@cabforum.org, and confirm that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/.

If the laws under which the CPS was formulated are invalid, or the specifications such as the CA/B Forum's Baseline Requirements are modified, any related adjustments to SZCA's business operations in this CPS will no longer apply. SZCA's related adjustments to business operations, revisions to the CPS, and notification to the CA/B Forum will be completed within 90 days.

9.16.4 强制执行 Enforcement

SZCA 声明，若证书订户、依赖方等实体未执行本 CPS 中某项规定，不被认为该实体将来不执行该项或其他规定。

SZCA declares that if the subscribers or relying parties did not execute any item within this CPS, it should not be considered that they need not be executed in the future.

9.16.5 不可抗力 Force Majeure

SZCA 不对因战争、瘟疫、火灾、地震、传染性疾病、互联网黑客、病毒和其他不可抗力的事件所造成本 CPS 规定担保责任的违反、延误或无法履行负责。

SZCA is not liable for any breach, delay, or inability to perform its warranty obligations under this CPS caused by war, plague, fire, earthquake, infectious disease, Internet hacking,

viruses, and other force majeure events.

9.17 其它条款 Other Provisions

SZCA 对本 CPS 拥有最终解释权。

SZCA has final interpretation rights to this CPS.