芜湖华为云计算技术有限公司

电子政务电子认证业务规则

版本：V2.0

发布日期：2025年10月27日

生效日期：2025年10月27日

芜湖华为云计算技术有限公司

版本控制表

版本	状态	修订说明	审核/批准人	生效日期
V1.0	版本发布	新版本发布	公司安全策略管理委员会	2025年6月25日
V2.0	版本发布	1、修订证书更新的情形； 2、修订“吊销”为”撤销“； 3、修订6.2节程序控制部分； 4、修订6.3节人员控制部分	公司安全策略管理委员会	2025年10月27日

目 录

1 概括性描述

1.1 概述

《芜湖华为云计算技术有限公司电子政务电子认证业务规则》（以下简称CPS）由芜湖华为云计算技术有限公司按照国家密码管理局《商用密码管理条例》的要求，依据《电子政务电子认证业务规则规范》制定，并报国家密码管理局备案。

芜湖华为云计算技术有限公司Huawei Trust Services（简称华为CA）是权威、公正的电子认证服务机构。华为CA严格按照《中华人民共和国电子签名法》和《中华人民共和国密码法》、《商用密码管理条例》的要求，以及相关管理规定，提供数字证书签发、更新、撤销或管理等服务，并通过以PKI技术、数字证书应用技术为核心的应用安全解决方案，为电子商务、企业信息化及电子政务服务相关服务构建安全、可靠的信任环境。

本CPS详细阐述了华为CA在实际工作和运行中所遵循的各项规范。本CPS适用于华为CA及其员工、注册机构、证书申请人、订户和依赖方，各参与方必须完整地理解和执行本CPS所规定的条款，并承担相应的责任和义务。

1.2 文档名称与标识

本文档名称是《芜湖华为云计算技术有限公司电子政务电子认证业务规则》。

1.3 电子政务电子认证业务范围

电子政务电子认证业务范围包括面向政务部门、企事业单位、社会团体和社会公众的电子政务电子认证服务。

1.4 电子政务电子认证活动参与方及其职责

1.4.1 电子认证服务机构

华为电子认证服务机构是根据《中华人民共和国电子签名法》、《中华人民共和国密码法》、《商用密码管理条例》规定，依法设立的第三方电子认证服务机构（简称：华为CA）。

华为CA是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字

证书的实体。

1.4.2 注册机构

注册机构（简称：RA 机构）是受理数字证书的申请、更新和撤销等业务的实体。

华为CA可以授权下属机构作为注册机构，负责提供证书业务办理、身份鉴证与审核等服务。

华为CA除了承担CA的角色外，同时也承担RA的角色，华为CA无授权承担RA角色的第三方机构。

1.4.3 订户

订户是指向华为CA申请数字证书的实体。

1.4.4 依赖方

依赖方是指为某一应用而使用、信任本华为CA签发的证书，并验证证书和相应签名的实体。

1.4.5 其他参与者

其他参与者指为CA证书服务体系提供相关服务的其他实体。

1.5 电子政务电子认证业务规范

1.5.1 适合的证书应用

本华为CA签发的数字证书适合应用在企业信息化和电子商务等领域，用于证明订户在电子化环境中所进行的身份认证和电子签名，以及数据加密等服务。本华为CA的数字证书包含通用证书（个人、机构证书），具体如下：

a） 个人证书

个人证书，用于区分、标识、鉴别个人身份的场景，适用于个人身份认证和电子签名，以及数据加密等服务。

b） 机构证书

机构证书，用于需要区分、标识、鉴别机构身份的场景，适用于机构身份认证和电子签名，以及数据加密等服务。

1.5.2 限制的证书应用

本华为CA发放的数字证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，由此造成的法律后果由订户负责。

1.6 电子政务电子认证策略管理

1.6.1 策略文档管理机构

本CPS的管理机构是华为CA安全策略管理委员会。由华为CA安全策略管理委员会负责本CPS的制订、发布、更新等事宜。

本CPS由华为CA拥有完全版权。

1.6.2 联系人

本CPS在华为CA网站发布，对具体个人不另行通知。

网站地址：https://www.huaweicloud.com/product/ccm/hwca.html

电子邮箱地址：HuaweiCA@huawei.com

联系地址：安徽省芜湖市鸠江区楚江大道018号江北华为云数据中心AS1-3F

联系电话： 950808

1.6.3 决定 CPS 符合策略的机构

华为CA安全策略委员会是策略制定的主要机构，也是审核批准本CPS的最高权威机构。

1.6.4 CPS 批准程序

本CPS的最高管理机构是华为CA安全策略管理委员会，该委员会负责制定、批准、发布、实施、更新、废止CPS。

CPS 的具体编制、修订工作，由华为CA安全策略管理委会指定相关业务部门组成编写小组负责，并由编制人负责检查 CPS 与实际情况的符合性；该小组完成编制后，提交安全策略管理委员会审核和批准。

本CPS经华为CA安全策略管理委员会审批通过后，从对外公布之日起三十日内向住所地密码管理部门备案。

1.7 定义和缩写

下列定义适用于本CPS：

a) 公开密钥基础设施（PKI）Public Key Infrastructure

支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和不可否认性服务。

b) 电子认证业务规则(CPS) Certification Practice Statement

关于电子认证服务机构在证书签发、证书更新(或密钥更新)、证书撤销或证书管理过程中所采纳的业务实践的声明。

c) 电子认证服务机构（CA）Certification Authority

受用户信任，负责创建和分配公钥证书的权威机构。

d) 注册机构（RA）Registration Authority

具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销证书，处理订户撤销其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书（即RA 代表CA承担某些任务）。

e) 在线证书状态协议（OCSP）Online Certificate Status Protocal：

为依赖方提供实时查询证书状态信息的协议。

f) 数字证书(证书) Digital Certificate

也称公钥证书，由电子认证服务机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

g) 证书撤销列表 (CRL) Certificate Revocation List

一个经电子认证服务机构电子签名的列表，它指定了一系列证书颁发者认为无效的证书，也称黑名单服务。

h) CA撤销列表(ARL) Certificate Authority Revocation List

一个经电子认证服务机构电子签名的列表，标记已经被撤销的CA的公钥证书的列表，表示这些证书已经无效。

i) 私钥 Private Key

非对称密码算法中只能由拥有者使用的不公开密钥。

j) 公钥 Public Key

非对称密码算法中可以公开的密钥。

k) 安全授权认证 Secure Authorization

安全授权认证是指通过口令、短信验证码、生物识别信息、数字证书等认证凭证对其订户身份进行核验，同时作为订户对其私钥的控制的激活数据。

l) 身份标识（ID）Identity

应用中的身份标识号码，也称为序列号或账号，是某个应用中相对唯一的编码，在应用中相当于是一种“身份标识”，身份标识号一般是不变的，至于用什么来标识该“身份标识”，则由证书应用机构自己制定的规则来确定。

2 信息发布与信息管理

2.1 信息库

华为CA通过https://www.huaweicloud.com/product/ccm/hwca.html官网完整公布本CPS，以及相关的技术支持等信息。

2.2 认证信息的发布

华为CA通过目录服务（LDAP）发布CRL，订户可以通过访问华为CA的官方网站进行查询。

华为CA通过官网发布本CPS，订户可以通过官网进行查阅下载，华为CA同时提供证书状态查询服务，订户可以通过官网查询相关证书状态。

2.3 发布时间或频率

本华为CA的CPS按照1.6.4所述的批准流程，一经发布到华为CA的网站，即时生效。

2.4 信息库访问控制

对于公开发布的证书、CPS、CRL 等公开信息，本华为CA允许公众自行通过网站进行查询和访问。

本华为CA通过网络安全防护、安全管理制度确保这些信息只有授权人员才能修改。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

每个订户对应一个甄别名（Distinguished Name，简称 DN）。

数字证书中的主体的X.500 DN 是C=CN 命名空间下的X.500目录唯一名字。

3.1.2 对名称意义化的要求

订户的甄别名(DN)必须具有一定的代表意义，在数字证书的主体名称中，用于唯一标识证书主体的X.500名称。

个人证书的甄别名通常可包含个人的真实名称或者证件号码，作为标识订户的关键信息被认证。

机构证书的甄别名通常包含机构名称或机构的证件号码，作为标识订户的关键信息被认证。

3.1.3 订户的匿名或伪名

在CA证书服务体系中，原则上订户不得使用匿名或伪名。

3.1.4 理解不同名称形式的规则

甄别名（DN）的内容一般由 CN、OU、O、L、ST、C 等部分组成，具体的命名规则详见本 CPS§8.1.3 名称形式。

3.1.5 名称的唯一性

在CA的证书服务体系中，证书主体名称必须是唯一的。但对于同一订户，可以用其主体名为其签发多张证书，但证书的扩展项不同。

3.1.6 商标的承认、鉴别和角色

本华为CA签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

3.2 初始身份确认

3.2.1 证明持有私钥的方法

通过证书请求文件中所包含的数字签名来证明证书申请人持有与注册公钥对应的私钥。在CA证书服务体系中，私钥在用户端生成，证书请求文件中包含用私钥进行的数字签名，系统将使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断证书使用者拥有私钥。

华为CA要求证书申请人妥善保管自己的私钥，因此，证书申请人视作其私钥的唯一持有者。

3.2.2 组织身份的鉴别

申请组织机构证书或组织机构代表人证书时，华为CA或其注册机构对证书持有者所在的组织机构进行身份鉴证。包括：

1) 申请组织机构证书或组织机构代表人证书华为CA对组织机构的身份鉴证包括如下两个内容：

a) 确认组织机构是确实存在的、合法的实体。确认的方式可以是，政府签发的组织机构成立的有效文件，如营业执照、事业单位法人证书等，必要时，可以通过权威的第三方数据库确认。

b) 确认该组织机构知晓并授权证书申请，即代表组织机构提交证书申请的人是经过授权的。确认的方式可以是，检查组织或组织的法定代表人授权给经办人办理证书事宜的授权文件或授权条款等。

c）经办人的个人身份证明材料。鉴别方式可以采用面对面现场鉴别，由华为CA鉴证人员现场比对经办人身份。当华为CA认为有需要时，可以增加其他方式，包括但不限于鉴别组织的法定代表人身份或要求经办人提交法定代表人有效身份证件证明。

华为CA按相关法规要求，在本CPS披露的期限内妥善保存组织机构的全部

申请材料，保存的组织机构申请材料可以是纸质或电子数据形式。

本CPS简要说明了如何进行组织身份鉴别。华为CA保留根据最新国家政策法规的要求更新组织身份鉴别方法与流程的权利。

3.2.3 个人身份的鉴别

华为CA对个人订户的实名身份信息进行核实鉴别，根据鉴别结果签发证书。实名鉴别的证明适用于各类数字证书应用场景，用于证明订户进行的身份认证和电子签名。

对于个人订户实名身份的鉴别，华为CA将核验个人有效身份证件的具体信息，核实个人订户身份的真实性，申请者需向华为CA提供申请实体确实存在的有效证明（居民身份证），鉴别方式采用面对面现场鉴别。必要时，可以通过权威第三方数据库信息比对、手机短信验证等其他可靠的方式鉴别。

对于个人订户身份的鉴别，华为CA按相关法规要求，在本CPS披露的期限内妥善保存组织机构的全部申请材料，保存订户申请材料可以是纸质或电子数据形式。

本CPS简要说明了个人身份鉴别方式。华为CA保留根据最新国家政策法规的要求更新个人身份鉴别方法与流程的权利。

3.2.4 政府部门内设机构及个人的身份鉴别

把证书签发给政府部门中的个人时，还将确认证书持有者和其所处的组织机构的关系，确认方式包括但不限于：

a) 申请者提交由所属政府部门盖章的证明文件，明确部门的名称并证明申请人和证书持有者属于该部门。

b) 通过申请者所在组织机构电话号码，然后联系组织机构的有关人员，确认申请者的身份及证书持有者确实被该组织机构雇佣，以及获得了所在组织机构的授权。

华为CA完成上述审核后，做出批准申请或拒绝申请的操作。如批准申请，将按照相关法律法规的要求妥善保管订户申请材料，订户申请材料可以是纸质或电子数据形式。

3.2.5 没有验证的订户信息

订户提交鉴证文件以外的信息为没有验证的订户信息。

3.2.6 授权确认

代表组织获取数字证书，需要出具组织授权其该组织为办理华为CA数字证书事宜的授权文件。组织在华为CA的数字证书申请表上加盖单位公章或采用其他安全有效方式体现申请机构真实意愿的方式，则证明本组织对办理人的授权确认。

华为CA不提供个人证书代办的服务。

3.2.7 互操作准则

不在此规定。

3.3 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

证书常规密钥更新中，证书订户使用当前有效私钥对包含新公钥的密钥更新请求进行签名，华为CA使用订户原有公钥验证确认签名来进行订户身份标识和鉴别。华为CA也可以使用初始身份验证相同的流程进行标识与鉴别。

3.3.2 撤销后密钥更新的标识与鉴别

证书撤销后的密钥更新等同于订户重新申请证书，其要求与本CPS§3.2相同。

3.3.3 证书变更的标识与鉴别

证书变更是指订户的证书信息发生变更，申请重新签发一张证书，对原证书进行撤销处理。

通用证书的证书变更的标识与鉴别使用初始身份验证相同的流程，其要求与本CPS§3.2 相同。

3.4 撤销请求的标识与鉴别

证书撤销请求的标识与鉴别使用初始身份验证相同的流程，其要求与本CPS §3.2 相同。

如果是因为订户没有履行本CPS所规定的义务，由华为CA和申请撤销订户的证书时，不需要对订户身份进行标识和鉴别。

4 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

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

4.1.2 申请过程与责任

证书申请人按照本CPS所规定的要求，通过现场面对面或在线方式提交证书申请，包括相关的身份证明材料。华为CA或注册机构应明确告知证书用户所需承担的相关责任和义务，证书申请人表达申请证书的意愿后，华为CA或注册机构依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否受理申请。

订户：订户需要提供本CPS § 3.2 所述的有效身份证明材料，并确保材料真实准确。配合华为CA完成对身份信息的采集、记录和审核。

华为CA：华为CA参照本CPS § 3.2 的要求对订户的身份信息进行采集、记录，审核。通过鉴证后，华为CA向订户签发证书。

证书申请人应当提供真实、完整和准确的信息，华为CA或其注册机构须按本CPS § 3.2的要求和流程对申请人身份材料信息进行审查。如证书申请人未向华为CA提供真实、完整和准确的信息，或者有其他过错，给华为CA或电子签名依赖方造成损失的，由证书申请人承担赔偿责任。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

华为CA按照本CPS所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见本CPS §3.2初始身份确认。

4.2.2 证书申请批准和拒绝

华为CA根据本CPS所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人通过本CPS所规定的身份鉴别流程且鉴证结果为合格，华为CA将批准证书申请，为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴证，华为CA将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因(法律禁止的除外)。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

华为CA将在合理时间内完成证书请求处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间不超过2个工作日。

华为CA能否在上述时间期限内处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了华为CA或注册机构的管理要求。

4.3 证书签发

4.3.1 证书签发过程中 CA 和 RA 的行为

在订户申请通过鉴别后，RA系统操作员录入订户申请信息，并提交RA系统审核员审核；RA系统审核员审核通过后，向CA系统提交申请；CA系统向RA系统返回证书，并以安全的形式将证书反馈给订户。

4.3.2 电子认证服务机构对订户的通告

华为CA通过注册机构对通用证书订户的通告有以下几种方式：

a) 通过面对面的方式，通知订户到注册机构领取数字证书；注册机构把密码和证书等直接提交给订户，来通知订户证书信息已经正确生成；

b) 电子邮件通知；

c) 电话通知；

d) 站内信通知；

e) 华为CA认为其他安全可行的方式通知订户。

4.3.3 证书签发后发布声明

对于证书申请者明确表示拒绝发布证书信息的，华为CA不发布该证书申请者证书信息。没有明确表示拒绝的，华为CA可将证书信息发布到目录系统。

4.4 证书接受

4.4.1 构成接受证书的行为

证书签发完成后，华为CA提供多种接受证书的方式，提供多种接受证书的方式，只要满足任何一个约定方式的条件，应当视为证持有者接受证书。包括但不仅限于：

- 通过面对面的提交，证书持有者接受载有证书和私钥的介质；
- 华为CA在订户允许下，代替订户下载证书，并把证书通过安全载体发送给订户；
- 证书获取通知发送给订户后，订户通过该通知下载证书。
- 订户接受了获得证书的方式，并且没有提出反对证书或者证书中的内容；
- 订户反对证书或者证书内容的操作失败。

完成以上行为表明证书持有者接受证书。

证书申请人从获得数字证书起1个工作日内无意见，就被视为同意接受证书。订户可联系华为CA客服人员协助解决证书下载问题。

在证书这接受到证书后，证书持有者应立即对证书进行检查和测试。

4.4.2 电子认证服务机构对证书的发布

华为CA在签发完数字证书后，采用数据库或目录服务方式，实现数字证书的存储与发布。对已发布的数字证书，华为CA提供证书目录信息查询服务。

查询方式包括但不限于用户在线自助或人工受理等。华为CA提供基于证书序列号查询证书状态的方式。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

对于其签发的证书，华为CA及注册机构不通知其他实体。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

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

通用证书订户接受到数字证书后，应妥善保存其证书对应的私钥。

订户的私钥和证书应用于规定的、批准的用途，且必须遵守本CPS的要求，妥善保存其私钥，避免他人未经本人授权而使用本人证书情形的发生，否则其应用是不受保障的。

订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书之后才能使用对应的私钥，并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

订户数字证书用于个人身份标识、身份认证，以及个人文档、邮件等信息的数字签名及加密等安全需求；

订户数字证书必须包含个人真实用户名及邮箱信息；

订户数字证书私钥产生及保存在安全芯片或安全容器中，如USB KEY等；

订户数字证书有效期不高于3年，证书到期前3个月启动更新。

如果证书中的某些字段明确了证书所标明的适用范围内的行为，那么该证书允许在这一范围内适用。任何超出适用范围内的行为，都将由行为人独立承担责任。华为CA对超出适用范围的任何使用行为，不承担任何由此产生的责任和义

务。

4.5.2 依赖方对公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份，并通过公钥验证对方电子签名的真实性。依赖方查看证书了解对方的身份时，应查看该证书的甄别名、内容、证书策略，对应本CPS3.2 定义的不同的鉴别方法，选择是否信任证书中标识的身份，承担不同鉴别方法可能存在的风险。

验证证书的有效性包括：

a) 用华为CA的证书验证证书中的签名，确认该证书是华为CA签发的，并且证书的内容没有被篡改。

b) 检验证书的有效期，确认该证书在有效期之内。

c) 检验通用证书有效性，需要检查该证书没有被撤销。

d）确认签名的有效性，确保签名对应的是依赖方信任的证书。在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

依赖方信赖华为CA签发的证书所证明的信任关系是需要：

a）获取并安装该证书的对应的证书链；

b）验证证书的有效性；

c）在信赖证书所证明的信任关系前确认该证书记载的内容与索要证明的内容一致。

4.6 证书更新

4.6.1 证书更新的情形

出于安全考虑,华为CA默认的方式是证书更新的同时，更新证书的密钥。证书订户也可以选择保留原有密钥，华为CA一般不建议进行这样的证书更新，但是如果订户提出，华为CA在考虑到安全和自身利益保障的前提下,可以为订户提供此种服务。

数字证书上都有明确的证书有效期，表明该证书的起始日期与截至日期。订户应当在证书有效期到期前，到华为CA申请更新证书。

4.6.2 请求证书更新的实体

证书订户、证书订户的授权代表（组织机构证书）或证书对应实体的拥有者。

4.6.3 证书更新请求的处理

证书更新申请者在数字证书到期前，应按要求向华为CA提出更新申请。华为CA对证书更新请求的处理流程与证书初始注册流程基本相同。华为CA或其注册机构对申请证书更新的订户进行查验与鉴别，鉴别要求同本CPS 4.2.1。

4.6.4 颁发新证书时对订户的通告

同 4.3.2。

4.6.5 构成接受更新证书的行为

同 4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同 4.4.2。

4.6.7 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新是指证书持有者生成新密钥并申请为新公钥签发新证书。

证书密钥更新的具体情形如下：

a) 当订户密钥即将到期或已经到期时；

b) 当订户证书密钥遭到损坏时；

c) 当订户证实或存在其证书密钥不安全的可能性时；

d) 出于技术和政策安全的考虑，华为CA要求证书密钥更新；

e) 其它可能导致密钥更新的情形。

4.7.2 请求证书密钥更新的实体

证书持有者，包括个人、组织等所有持有由认证机构（CA）签发的证书的实体，均有权申请更新其证书的密钥。

4.7.3 证书密钥更新请求的处理

同 3.3。

4.7.4 颁发新证书对订户的通告

同 4.3.2。

4.7.5 构成接受密钥更新证书的行为

同 4.4.1。

4.7.6 电子认证服务机构对密钥更新证书的发布

同 4.4.2。

4.7.7 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

证书变更是指在证书有效期内订户的证书信息发生变更，申请重新签发一张证书，对原证书进行撤销处理。

证书变更的申请和证书申请所需的流程、条件是一致的。

4.8.2 请求证书变更的实体

订户可以请求证书变更。订户包括持有华为CA签发的个人、组织等各类证书的证书持有人。

4.8.3 证书变更请求的处理

同 4.6.3。

4.8.4 颁发新证书对订户的通告

同 4.3.2。

4.8.5 构成接受变更证书的行为

同 4.4.1。

4.8.6 电子认证服务机构对变更证书的发布

同 4.4.2。

4.8.7 电子认证服务机构在颁发证书时对其他实体的通告

同 4.4.3。

4.9 证书撤销和挂起

4.9.1 证书撤销的情形

a) 发生下列情形之一的，订户应当申请撤销数字证书：

1) 数字证书私钥泄露；

2) 数字证书中的信息发生重大变更；

3) 认为本人不能实际履行本电子认证业务规则以及订户协议；

4) 认为当前密钥管理方式的安全性得不到保证。

b) 发生下列情形之一的，华为CA可以强制撤销订户的数字证书：

1) 政务机构的证书持有者不从事原岗位工作；

2) 司法机构要求撤销证书持有者证书；

3) 证书持有者提供的信息不真实；

4) 证书持有者没有或无法履行有关规定和义务；

5) 认证机构或最终证书持有者有理由相信或强烈怀疑一个证书持有者的私钥安全已经受到损害；

6) 政务机构有理由相信或强烈怀疑其下属机构证书、人员证书或设备证书的私钥安全已经受到损害；

7) 与证书持有者达成的证书持有者协议已经终止；

8) 法律、行政法规规定的其他情形。

4.9.2 请求证书撤销的实体

根据不同的情况，订户、华为CA可以请求撤销最终用户证书。

4.9.3 撤销请求的流程

证书撤销请求的处理采用与初始证书签发相同的过程。

4.9.3.1 订户主动提出撤销申请

订户到华为CA书面或在线发起证书撤销申请，提供有效身份证明文件及证书撤销申请文件，并接受证书撤销申请的有关条款，完成身份鉴别，同意承担相应的责任；

华为CA对订户提交的撤销请求审核后撤销订户证书，并通过邮件、短信、电话等方式通知订户证书被撤销，订户证书的撤销信息在24小时内发布到CRL，向外界公布。

4.9.3.2 订户被强制撤销证书

华为CA在确认发生本 CPS § 4.9.1中 b）所述的强制撤销证书情形时，及时对订户证书进行强制撤销，撤销后将通过官网公告、注册机构或其他安全可行的

方式通告订户。订户证书的撤销信息将在24小时内发布到CRL，向外界公布。

4.9.4 撤销请求宽限期

如果出现订户私钥泄露等事件，撤销请求必须在发现泄露或有泄露嫌疑8小时内提出。其他撤销原因的撤销请求必须在48小时内提出。

4.9.5 电子认证服务机构处理撤销请求的时限

华为CA接到撤销请求并完成身份鉴别后立即处理，24小时生效。华为CA每日签发一次CRL，供请求者查询下载。

4.9.6 依赖方检查证书撤销的要求

对于安全保障要求比较高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在信赖一个证书前应当查询证书撤销列表确认该证书的状态。在具体应用中，依赖方可以使用以下两种功能之一进行所依赖证书的状态查询：

a) CRL查询：利用证书中标识的CRL地址，查询并下载CRL到本地，进行证书状态的检验。

b) 在线证书状态查询(OCSP)：利用证书中标识的OCSP地址，根据序列号查询证书状态。

注意：依赖方要验证CRL的可靠性和完整性，确保是经华为CA发布并且签名的。

4.9.7 CRL 的颁发频率

华为CA可采用实时或定期的方式发布CRL。颁发CRL的频率根据证书策略确定，一般为24小时定期发布。系统的CA证书的 CRL（ARL）定期进行更新。如果撤销 CA 证书，将在撤销后24小时之内更新ARL。

4.9.8 CRL 发布的最长滞后时间

CRL 发布的最长滞后时间为24小时。

4.9.9 撤销信息的其他发布形式

证书撤销信息通过CRL服务发布，订户可通过证书扩展域中的CRL地址获得CRL信息。

4.9.10 在线状态查询的可用性

华为CA提供的证书状态在线查询服务（OCSP）7*24 小时可用。

4.9.11 密钥损害的特别要求

无论是订户还是华为CA，发现证书密钥受到安全损害时应立即撤销证书。

4.9.12 证书挂起的情形

华为CA不提供证书挂起。

4.9.13 请求证书挂起的实体

不适用。

4.9.14 挂起请求的流程

不适用。

4.9.15 挂起的期限限制

不适用。

4.10 证书状态服务

证书的状态可以通过华为CA提供的OCSP服务和CRL服务获得。对于被撤销的证书，华为CA在该证书到期前，不删除其在CRL及OCSP中的撤销记录。

4.10.1 操作特点

请求者可以在证书状态查询服务（OCSP）上查询证书状态，或者通过下载CRL查询证书状态。

4.10.2 服务可用性

华为CA提供7*24小时的证书状态查询服务。

华为CA根据与依赖方约定，可向依赖方提供通用证书（包括个人证书、企业证书的状态查询服务。

4.10.3 可选特征

暂无

4.11 订购结束

订购结束是指当证书有效期满或证书撤销后，该证书的服务时间结束。订购结束包含以下两种情况：

a) 证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可以终止订购；

b) 在证书有效期内，证书被撤销后，即订购结束。

4.12 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略和行为

通用证书（个人或机构）的签名密钥对由订户的密码设备生成，加密密钥对由密钥管理中心生成。

通用证书（个人或机构）的密钥恢复是指加密密钥的恢复，密钥管理中心不负责签名密钥的恢复。密钥恢复分为两类：订户密钥恢复和司法取证密钥恢复。

a）订户密钥恢复：订户向华为CA申请，经审核后，通过华为CA向密钥管理中心请求；密钥恢复模块接受订户的恢复请求，恢复订户的密钥并下载于订户证书载体中。

b) 司法取证密钥恢复：司法取证人员在密钥管理中心申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定载体中。

构成接受密钥恢复的行为，同 4.4.1。

4.12.2 会话密钥的封装与恢复的策略和行为

非对称算法组织数字信封的方式来封装会话密钥。数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解开并恢复会话密钥。

5 支持服务

5.1 应用集成支持服务

5.1.1 服务策略和流程

华为CA提供的服务内容有：

1. 对业务系统进行充分调研，指导或参与业务系统证书应用部分的开发和实施；
2. 制定项目管理制度，规范系统和程序开发行为；
3. 制定安全控制流程，明确人员职责；
4. 实施证书软件发布版本管理，并进行证书应用环境控制；
5. 项目开发程序和文档等资料妥善归档保存。

5.1.2 应用接口

证书应用接口为上层提供简洁、易用的调用接口，其主要包括密码设备接口和通用密码服务接口。

5.1.3 密码设备调用接口

密码设备调用接口包括服务器端密码设备的底层应用接口和客户端证书介质的底层应用接口。服务器端密码设备的底层应用接口在符合国际标准 PKCS#11 技术规范的基础上，符合《公钥密码基础设施应用技术体系密码设备

应用接口规范》；客户端证书介质的底层应用接口符合《智能 IC 卡及智能密码钥匙密码应用接口规范》。

5.1.4 通用密码服务接口

通用密码服务接口是屏蔽了底层不同密码设备类型和底层接口的通用中间件，该接口符合《电子政务数字证书应用接口规范》，主要包括服务器端组件接口和客户端控件接口，提供证书环境设置、证书解析、随机数生成、签名验证、加解密、时间戳以及数据服务接口等功能。

服务器端组件和客户端控件支持不同认证机构所签发的符合《电子政务数字证书格式规范》的数字证书。

5.1.5 集成内容

华为CA为电子政务应用单位提供证书应用接口程序集成工作。包括以下服务：

1. 证书应用接口的开发包（包括客户端和服务器端）；
2. 接口说明文档；
3. 集成演示 Demo；
4. 集成手册；
5. 证书应用接口开发培训和集成技术支持；
6. 协助应用系统开发商完成联调测试工作。

5.2 使用支持服务

5.2.1 服务内容

使用支持服务是华为CA面向证书使用用户（即证书申请者、证书持用者）及证书应用单位提供的一系列售后服务及技术支持工作。

服务内容包括：数字证书管理、数字证书使用、证书存储介质硬件设备使用、电子认证软件系统使用、电子认证服务支撑平台使用以及各类数字证书应用（如证书登录、证书加密、数字签名）等贯穿证书使用和应用过程中的所有问题。

5.2.1.1 面向证书持有者的服务支持

1. 数字证书管理

包括数字证书的导入、导出，以及客户端证书管理工具的安装、使用、卸载等。

2. 数字证书应用

基于数字证书的身份认证、电子签名、加解密等应用过程中出现的各种异常问题，如：证书无法读取、签名失败、证书验证失败等。

3. 证书存储介质硬件设备使用

包括证书存储介质使用过程中出现的口令锁死、驱动安装、介质异常等。

4. 电子认证服务支撑平台使用

为用户提供在华为CA的数字证书在线服务平台中使用的各类问题，如：证书更新失败、下载异常、无法提交撤销申请等。

5.2.1.2 面向应用提供方的服务支持

1. 电子认证软件系统使用

提供受理点系统、注册中心系统、LDAP、OCSP、信息服务系统等系统的使用支持问题，如证书信息无法查询、数据同步失败、服务无响应等。

2. 电子签名服务中间件的应用

解决服务中间件在集成时出现的各种情况，如客户端平台适应性问题、服务端组件部署问题、服务器证书配置问题、签名验签应用问题等。

5.2.2 服务方式

华为CA提供多种服务方式，包括热线服务、在线服务、现场服务等，并公布相应的服务获取方式。华为CA建立了服务保障体系，包括建立专业的服务队伍、服务规范、满意度调查、投诉受理等。服务保障体系能根据服务业务的变化及时更新。

5.2.2.1热线服务

用户拨打华为CA的服务热线，通过语音系统咨询证书应用问题，热线根据用户的问题请求，查询相关信息，协助用户处理。

5.2.2.2 在线服务

在线服务通过提供Email在线帮助，满足用户多种服务帮助的需求。客户通过向华为CA发送咨询邮件，客服人员通过邮件解答相关问题。

5.2.2.3 现场服务

根据用户的实际需求，由技术支持工程师上门现场为用户处理数字证书应用中存在的问题。

5.2.2.4满意度调查

通过多种用户可接受的调查方式进行客户回访，包括电话、邮件系统、短信等。向用户提供调查表格以供用户填写，调查表格清晰载明此次回访的目的及内容。并将用户回访中产生的相关文档进行归档、保存。

5.2.2.5 投诉受理

华为CA设立的专门的投诉电话和投诉邮件地址，向用户公布电子政务电子认证服务监管部门的投诉受理方式。可通过电话、电子邮件等方式及时接受客户投诉，投诉受理过程中记录投诉问题，并将结果及时反馈给客户。将投诉受理中产生的相关文档进行归档、保存。

5.2.2.6培训

华为CA提供全面的培训服务，包括：电子认证服务基础性技术知识、服务规范、证书应用集成规范及相关帮助文档、常见问题解答(FAQ)、操作手册等。培训方式可以由华为CA与客户双方约定的形式开展。

5.2.3 服务质量

热线服务、在线服务、现场服务时间充分满足各类用户的需要，为5*8小时工作时间。在有应急服务需求的特殊情况下，服务时间根据具体业务需求确定，提供7*24小时不间断服务。应对技术问题和技术故障按照一般事件、严重事件、重大事件进行分类，并制定相应处理流程和机制，以确保服务的及时性和连续性。技术支持响应时间以最大程度不影响客户使用为准则。

6 电子认证服务机构设施、管理和操作控制

6.1 物理控制

6.1.1 场地位置与建筑

a) CA机房的建筑物和机房建设按照下列标准实施：

1) GB/T 25056-2010《信息安全技术证书认证系统密码及其相关安全技术规范》

2) GB50174-2008《电子信息系统机房设计规范》

3) GB6650-86：《计算机机房活动地板的技术要求》

4) GB9361－2011《计算机站场地安全要求》

5) GB2887-2011《计算机场地通用规范》

6) GB50222-95《建筑内部装修设计防火规范》

7) GB50016—2014《建筑设计防火规范》

8) GB50116-2013《火灾自动报警系统设计规范》

9) GB50057－2010《建筑物防雷设计规范》

10) GB5054－2011《低压配电设计规范》

11) GBJ19－2003《采暖通风与空气调节设计规范》

12) YD/T754-95《通讯机房静电防护通则》

b) CA机房位于安徽省芜湖市鸠江区二坝镇杭州路018号，实行分层访问的安全管理：

CA机房的功能区域划分为，五个区域。

五个区域分别是：核心区、服务区、管理区、公共区、安全监控室

核心区：分为CA核心区和KM核心区。CA核心区存放离线根CA，签发服务器（包含主目录服务），数据库服务器和加密机等设备，提供证书签发服务；KM核心区存放密钥服务器，存储服务器和加密设备等，提供密钥对服务；

服务区：存放注册服务器，OCSP服务器，从目录服务器，数据库服务器和加密机等设备，提供证书注册等服务；

管理区：分为CA&RA管理区和KM管理区。CA&RA管理区搭载入侵检测管理终端，注册和签发服务/管理终端，运维人员进行日常的运维操作区域；KM管理区存放管理终端、安全管理终端、审计终端，运维人员进行日常的运维操作区域；

安全监控室：集中监控业务机房内基础设施和物理安防的区域；

公共区：CA机房入口以外的DC楼其他区域。

6.1.2 物理访问

为了保证本系统的安全，采取了一定的隔离、控制、监控手段。机房的所有门均具备足够的坚固性，能防止非法的进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

a) 门禁系统：控制各层门的进出。监控室、管理区和服务区门禁需要一名工作人员使用身份识别卡结合人脸鉴定才能进入，出门仅需使用身份识别卡。核心区的门禁要求两名工作人员使用身份识别卡结合人脸鉴定才能进入，出门需两名工作人员使用身份识别卡。进出每一道门均有时间记录和信息提示，并对门禁的异常事件做出记录和告警。

b) 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 24 小时不间断录像。所有录像资料需要保留不少于 12 个月，以备查询。

c） 物理入侵警报系统：与门禁系统和监控系统配合使用，非法入侵发生时即可在安全监控室产生报警提示。

三个系统均备有 UPS，并提供至少 8 小时的不间断供电。

6.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。采用双电源，在单路电源损坏时，可以自动切换，维持系统正常运转。

根据机房环境及设计规范要求，主机房和基本工作间，均设置了空气调节系统。空调系统使用双列行级空调作为备份。其组成包括精密空调、通风管路、新风系统。

6.1.4 水患防治

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

CA机房的系统有充分保障，能够防止水侵蚀。

目前机房内的上下水系统做了严格防水处理，由漏水检测系统提供（7*24）实时检测并在安全值班室的动环系统做集中监控。

6.1.5 火灾预防和保护

火灾预防：

a) CA机房建筑物的耐火等级必须符合 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级。

b) CA机房设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位设置双烟感探测器。

c) CA机房配置独立的气体灭火装置，使用七氟丙烷（HFC-227ea）等洁净气体灭火系统，备有相应的气体灭火器，管理区，公共区和安全监控室根据实际情况可配置水喷淋灭火装置。CA机房内除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。

d) 火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置。

e) 在公共区域内，设置有紧急出口，紧急出口必须设有消防门，消防门符合安全要求。紧急出口门外部不能有门开启的装置，且紧急出口门须与门禁报警设备联动外，需装配独立的报警设备。

灭火系统采用自动，手动，紧急启动三种方式：

a) 自动方式：公共区，管理区，安全监控室为双烟感或者单烟感加手动报警触发自动报警系统，感温元件感受到温升至68℃自动破裂触发湿式喷淋系统；服务区，核心区为双烟感或者单烟感加手动报警触发自动报警系统，感温元件感受到温升至68℃自动破裂触发七氟丙烷气体灭火系统。

b) 手动方式：人员对钢瓶或药剂瓶直接开启操作。

c) 紧急启动：防护区外设有紧急启动按钮供紧急时使用。

CA机房通过与华为云数据中心运维团队协调，实施消防灭火等应急响应措施。

6.1.6 介质存储

对储存产品软件和数据、归档、审计或备份信息的介质保存在安全设施中，这些设施受到适当的物理和逻辑访问控制的保护，只允许授权人员的访问，并防止这些介质受到意外损坏（如水、火灾和电磁）。

6.1.7 废物处理

当CA机房存档的敏感数据或密钥已不再需要或存档的期限已满时，应当将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

6.1.8 数据备份

华为CA对关键数据、审计日志数据等进行备份，备份方式采用双机热备，一台服务器存储备份数据到本地另一台服务器专门存储所有备份数据。

6.2 程序控制

6.2.1 可信角色

提供电子认证服务过程中，将能从本质上影响证书的颁发、使用、管理和撤销等涉及密钥操作的职位都视为可信角色。这些角色包括但不限于：

1） 密钥与密码设备管理人员，负责维护 CA 密钥和证书生命周期，负责管理密码设备；

2) 鉴证人员，负责订户信息录入、审核数字证书申请信息并完成鉴证和审批工作；

3) 系统维护人员，负责对 CA 系统的硬件和软件实施日常维护，并监控和排查故障；

4) 安全管理人员，负责场地安全、日常安全管理工作；

5) 安全审计人员，负责对业务操作行为进行审计；

6.2.2 每项任务需要的人数

华为CA对关键任务的职责承担严格控制，对于敏感操作，至少有两人以上的可信角色共同完成。具体地，屏蔽区场地访问设置为双人进出模式；CA密钥所在的密码设备的管理权限按照5选3方式进行分割，并由不同可信人员持有。

6.2.3 每个角色的识别与鉴别

所有华为CA的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和人脸识别；进入系统需要使用相应的数字证书进行身份鉴别。华为CA将独立完整地记录其所有的操作行为。

6.2.4 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，即华为CA的可信角色由不同的人担任。（NO 代表不可兼任）

角色 / 角色	密钥与密码设备管理人员	鉴证人员	系统运行维护人员	安全管理人员	审计管理人员

密钥与密码设备管理人员	—	NO	NO	NO	NO
鉴证人员	NO	—	NO	NO	NO
系统运行维护人员	NO	NO	—	NO	NO
安全管理人员	NO	NO	NO	—	NO
审计管理人员	NO	NO	NO	NO	—

数据库管理员与应用系统管理员和操作系统管理员不能兼任；CA系统操作员与审计员之间不能兼任；RA 业务操作员的录入员和审核员两个角色不能兼任；认证系统的管理员和维护人员不能兼任持有密码设备分割密钥的分管者。

6.3 人员控制

6.3.1 资格经历审查

在遵循相关法律法规和保护员工隐私的基础上，华为CA对工作人员的资格、经历以及经验等情况进行严格审查和核实，工作人员必须具备良好的社会和工作背景、无重大工作错误、无违法犯罪行为、无不良信用记录等。

6.3.2 保密协议签署

华为CA工作人员必须具有相应的安全意识，接受保密教育，签署员工保密协议。

6.3.3 人员培训要求

华为CA对所有入职员工提供培训计划，培训内容包括但不限于：

1） 华为公司核心价值观；

2） 系统硬件安装与维护、系统软件运行与维护、应用软件的运行和维护；

3） PKI基本知识；

4） 商业秘密&信息安全培训；

5） 可信人员管理办法；

6） 工作职责和岗位说明；

7） 其他与工作职责相关的专业知识培训。

6.3.4 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受一次华为CA组织的培训一次，以保证其保持完成所负责工作的技能水平。

华为CA根据工作人员对培训内容的掌握情况不定期安排再培训，如果相关业务流程调整或系统更新，应确保所有的相关工作人员受到适当的再培训。

6.3.5 工作轮换周期和顺序

对于可替换角色，华为CA将根据业务的安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。岗位轮换不违背职责分割策略。

6.3.6 未授权行为的处罚

员工一旦被发现进行了未授权的操作，将立即被终止所有权限，随后由华为CA对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

6.3.7 独立合约人的要求

不涉及。华为CA目前未聘用外部独立合约人从事认证相关的工作。

6.3.8 提供给员工的文档

为使得系统正常运行，华为CA向其员工提供完成其工作所必须的文档。

6.4 审计日志程序

6.4.1 记录事件的类型

华为CA记录与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生

时间段、事件的内容和事件相关的实体等。

1. 证书订户服务流程中产生的信息数据和资料，如申请表、协议、身份资 料等。同时证书的整个生命周期事件都应该在系统中被记录。

2. 电子认证服务系统日常操作产生的日志记录文件，包括但不限于：登录登出，签证发证，密钥的生成等。

3. 可信人员的操作事件，例如进出敏感区域的工作记录，密码的设置更替等。

4. 认证机构、注册机构工作规范和相关工作记录。

5. 不符合规程的事件，例如非法越权操作，非法修改安全配置等。

6.4.2 处理或归档日志的周期

对于系统的自动日志和操作人员的手工记录，华为CA每月进行一次检查和汇总。 对系统安全日志，每月进行一次跟踪处理，检查违反策略和规范的重大事件。

6.4.3 审计日志的保存期限

CA系统审计日志至少保存到证书失效后五年。

6.4.4 审计日志的保护

华为CA授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作。审计日志的制作和访问进行岗位分离。

6.4.5 审计日志备份程序

CA系统审计日志备份会在每月定时进行备份，由审计人员登录系统下载日志文件，保存至dbox上，后对于日志文件进行权限的锁定，非审计人员只有查看的权限。

6.4.6 审计日志收集

审计日志收集涉及：

- 证书注册系统；
- 证书签发系统；
- 证书受理系统；
- 网站和数据库系统；
- 网络安全等其他需要审计的系统。

华为CA使用审计工具满足对上述系统审计的各项要求。

6.4.7 对导致事件实体的通告

华为CA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，华为CA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。

华为CA有权决定是否对导致事件的实体进行通告。

6.4.8 脆弱性评估

华为CA每年对系统进行渗透测试等脆弱性评估，且每天对系统进行漏洞扫描和入侵检测等脆弱性评估，以降低系统运行的风险。

6.5 记录归档

华为CA设置了专门的档案管理员，用于管理华为CA业务过程中产生的文件以及记录的归档，且对这些归档文件进行了相应的权限控制。

6.5.1 归档记录的类型

归档记录包括所有审计数据、证书申请信息、与证书申请相关的信息等，归档记录应详细包含了记录产生的时间和日期，详见CPS6.4.1。

6.5.2 归档记录的保存期限

除了法律法规和证书主管机构提出的保存期限以外，华为CA制订的有关第三方电子认证服务运营信息的归档保存期限至少应该如下：

面向企事业单位、社会团体、社会公众的电子政务电子认证服务，信息保存期至少为证书失效后5年。

面向政务部门的电子政务电子认证服务，信息保存期至少为证书失效后10年。

6.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。华为CA保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

6.5.4 归档文件的备份程序

对于系统生成的电子归档记录，每天进行备份；对于书面归档资料，不需要进行备份，但是采严格的措施保证其安全性，防止对档案及其备份进行删除、修改等操作。

6.5.5 记录时间戳要求

系统日志未采用时间戳技术。

6.5.6 归档收集系统

对于系统生成的电子记录，通过备份同步到存储服务器，每天进行备份。

对于手工生成的电子记录，归档到dbox文件夹当中或者由相关人员上传到存储服务器中。

对于纸质的归档资料，收集归档到保密柜内。

6.5.7 获得和检验归档信息的程序

华为CA采取了物理和逻辑的访问控制方法，以确保只有授权人员才能接近

这些归档信息，严禁未授权的访问、阅读、修改和删除等操作。

6.6 电子认证服务机构密钥更替

CA证书有效期不超过 20 年，CA密钥对的使用期限和CA证书有效期应保持一致。在CA证书到期前，华为CA将按照密钥安全管理制度对CA密钥进行更替，生成新的CA证书。华为CA密钥更替方式如下：

a) CA证书到期时间小于订户有效期之前，应停止签发新的订户证书（“停止签发日期”）；

b) 产生新的密钥对，签发新的CA证书；

c) 在“停止签发日期”之后，将采用新的CA密钥签发订户证书；

d) 华为CA将继续使用旧的私有密钥签发的 CRL，直到旧的私钥签发的最后证书到期为止。

6.7 损害和灾难恢复

6.7.1 事故和损害处理程序

发生故障时，华为CA将按照业务连续性计划实施恢复，并且应尽快完成恢复过程，如果无法在 8 小时内完成恢复过程，并且事故导致证书服务无法进行，则应启动备份恢复机制，在 24 小时内恢复证书服务。

业务连续性计划由“华为CA安全策略管理委员会”总负责，其职能包括指导和管理信息安全工作，批准、发布业务持续计划，根据实际情况决定启动灾难恢复等各项职能。

业务连续性计划中确立了关键服务流程及其业务恢复目标，以及CA系统可能出现的业务中断情形及应对方案，完全恢复时的操作程序以及操作内容。当发生紧急事件后，应急领导小组召集相关实施成员举行会议，对事件进行评估。按照确定的应急处理机制进行处理，并根据实际情况对受影响客户进行妥善处理。在紧急事件应急处置后，将评估已有风险防范措施的有效性并加以改进。

6.7.2 计算资源、软件和/或数据被破坏

华为CA遭到攻击，发生通信网络资源毁坏、计算机设备系统不能提供正常

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，华为CA将按照业务连续性计划实施恢复。

6.7.3 实体私钥损害处理程序

对于实体私钥的损害，华为CA有如下处理要求和程序：

1）当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立即前往华为CA或相应的注册机构撤销其证书，或者立即通过电话、电子邮件等方式通知华为CA或注册机构撤销其证书。

2）当华为CA或注册机构发现证书订户的实体私钥受到损害时，华为CA或注册机构将立即撤销证书，并通知证书订户，订户必须立即停止使用其私钥。

3）当华为CA的CA证书出现私钥损害时，华为CA将立即上报行业主管部门，撤销该CA证书所有签发的证书并及时通过各种途径通知依赖方，在更换新密钥生成CA证书前，不再签发新的证书。

6.7.4 灾难后的业务连续性能力

针对证书系统的核心业务系统，证书签发系统和证书接口系统采用集群方式；对核心数据库，证书管理系统数据库采用集群方式来确保证书系统的高可靠性和可用性。

华为CA建有本地离线备份服务器，固定获取所有所需备份文件存储到备份服务器硬盘下，发生自然或其它不可抗力性灾难后，华为CA可获取备份文件对运营进行恢复。该灾难备份系统，将认证提供运营所需要的软硬件设备、数据存储、密钥对、证书和用户信息、业务操作规范和灾难恢复文件，建立了备份系统和备份文件。备份系统软件及数据按照备份策略定期备份且妥善保存，此外系统管理员定期将其他电子备份数据导入到存储服务器中，由离线存储服务器管理员进行数据检查。

6.8 电子认证服务机构或注册机构的终止

因各种情况，华为CA需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

华为CA在终止服务九十日前，就业务承接及其他有关事项通知有关各方，

包括但不限于CA和订户等。

在终止服务六十日前向国家密码管理局报告，按照相关法律规定的步骤进行操作。

华为CA采用以下措施终止业务：

a) 起草CA终止业务声明；

b) 报告国家密码管理局；

c) 尝试与其他电子认证服务机构就业务承接进行协商，做出妥善安排；

d) 未能就业务承接事项与其他电子认证服务机构达成协议的，应当申请国家密码管理局安排其他电子认证服务机构承接其业务；

e) 停止认证中心所有业务；

f) 处理加密密钥；

g) 处理和存档敏感文件；

h) 清除主机硬件；

i) 管理CA系统管理员和安全官员；

j) 通知与CA终止运营相关的实体。

根据华为CA与注册机构签订的运营协议终止注册机构的业务。

7 认证系统技术安全控制

7.1 密钥对的生成和安装

7.1.1 密钥对的生成

CA系统和RA系统的密钥对是在密码机内部产生，密码机应具有商用密码产品认证证书。在生成CA密钥对时，华为CA按照密码机密钥管理制度，执行详细的操作流程控制计划，选定并授权5个密钥管理员，采取五选三方式，密钥管理员凭借USB-KEY对密钥进行控制。

订户的签名密钥的生成由订户负责，订户应确保其密钥产生的可靠性，并承担保护其私钥安全的责任和义务，并承担由此带来的法律责任，订户的加密密钥由华为CA的密码机生成存储在密钥管理系统中，并通过安全的方式传输给订户。

7.1.2 私钥传送给订户

订户的私钥由订户自己生成时不会进行传送。由华为CA的密钥管理中心产生时，将通过安全通道传到订户手中的密码设备中。

7.1.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到华为CA。

从RA到CA以及从密钥管理中心到CA的传递过程中，采用国家密码管理部门许可的通讯协议及密钥算法，保证了传输中数据的安全。

7.1.4 电子认证服务机构公钥传送给依赖方

依赖方可以从华为CA的网站下载根证书和CA证书，从而得到CA的公钥。

7.1.5 密钥的长度

华为CA遵从国家法律法规，政府主管机构等对密钥长度的明确规定和要求，目前华为CA电子认证系统支持签发SM2-256的密钥证书。

7.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理部门许可的密码设备或密码模块生成。对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均符合国家密码管理部门要求。

7.1.7 密钥使用目的

根CA私钥用于签发自身证书，下级CA证书，和CA的撤销列表。二级CA用于签发订户证书和CRL，证书的公钥用于验证私钥签名。订户的签名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。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

7.2 私钥保护和密码模块工程控制

7.2.1 密码模块标准和控制

华为CA系统所用的密码设备都是经国家相关部门鉴定并且批注使用的具有完全自主知识产权的产品，其安全性达到以下要求：

接口安全：不执行规定命令以外的任何命令和操作；

协议安全：所有命令的任意组合，不能得到私钥的明文；

密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

华为CA使用的加密机其公钥算法为：SM2-256，HASH算法为SM3，具有国家密码主管部门颁发的产品资质证书。

华为CA制定有专门的设备管理办法，从采购，验收，进入机房，初始化，激活使用，备份，维护，销毁等环节进行了规范化管理。

7.2.2 私钥的多人控制

CA证书的私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到5个管理员USB KEY中，只有其中超过半数以上管理员在场并许可的情况下，才能对私钥进行上述操作。CA证书的私钥的备份需要五个管理员同时在场且允许的情况下，才能对私钥进行上述操作。

7.2.3 私钥托管

订户加密证书对应的私钥由密钥管理中心托管，订户的签名证书对应的私钥由自己保管或控制，密钥管理中心不负责托管签名私钥。

密钥管理中心严格保证订户密钥对的安全，密钥以密文形式保存，密钥库具有最高安全级别，禁止外界非法访问。

7.2.4 私钥备份

华为CA和密钥管理中心不备份订户的签名密钥。加密私钥由密钥管理中心备份，备份数据以密文形式存在。华为CA的私钥由加密机产生，加密机拥有三机备份，并且保护在屏蔽机房内。华为CA私钥的备份由专门的人员负责，需要满足五位管理人员同时在场的访问控制来对需要备份的根私钥进行操作，备份恢复权限所需的USB KEY保存在保险柜中。

7.2.5 私钥归档

订户加密密钥对的归档是将已过生命周期或决定暂不使用的加密密钥以密文形式保存在数据库中，并通过数据库备份出来进行归档保存，归档后的密钥形成历史信息链，供查询或恢复，根私钥会被储存在CPS7.2.1所描述的密码设备中，以供查询和恢复。

7.2.6 私钥导入或导出密码模块

CA私钥在硬件密码模块中产生。在需要备份或迁移CA私钥时，从密码模块中导出的私钥必须由多人控制。华为CA不提供订户私钥从密码设备或密码模块中导出的方法。根私钥在需要导出密码模块时，必须满足五选三的访问控制，导出的根私钥以密文形式存储，根私钥在再次导入密码模块时，同样需满足五选三的访问控制，导入导出权限所需的USB KEY需保存在保险柜中（或银行保管柜等安全等级不低于本地的场所）。

7.2.7 私钥在密码模块中的存储

CA系统采用国家密码管理部门认可的密码设备，这些设备内置的协议、算法等均符合国家密码行业的标准要求。

订户私钥在密码设备或密码模块中加密保存。

7.2.8 激活私钥的方法

CA私钥存放在硬件密码设备中，具有激活私钥权限的管理员使用含有自己

的身份的USB KEY登录，启动密钥管理程序，进行激活私钥的操作，需要超过半数以上的管理员同时在场。

7.2.9 解除私钥激活状态的方法

对于CA私钥，具有解除私钥激活状态权限的管理员使用含有自己的身份的USB KEY登录，启动密钥管理程序，进行解除私钥的操作，需要超过半数以上的管理员同时在场。

7.2.10 销毁密钥的方法

对于CA私钥，具有销毁密钥权限的管理员使用含有自己的身份的USB KEY登录，启动密钥管理程序，进行销毁密钥的操作，需要超过半数以上的管理员同时在场。

7.2.11 密码模块的评估

华为CA使用通过检测认证的服务器密码机，符合国家有关标准。密码机采用以分组密码体制为核心的高强度密码算法和非对称密码体制，密钥采取分层结构，逐层提供保护。主要技术指标如下：

a) 通信接口：符合国际 ITU Ethernet RJ45标准；

b) 带宽控制：10M/100M/1000M 自适应，充分满足突发业务需要；

c) 并发容量：可支持同时并发100个的独立安全处理容量；

d) 密钥管理：密钥不以明文形式出现在服务器密码机以外；通信密钥通过身份鉴别后协商得到；

e) 身份鉴别：采用 USB-KEY对用户进行身份鉴别管理，以控制对加密系统的使用；

f) 处理速度：数据加解密处理能力大于 100Mbps。

7.3 密钥对管理的其他方面

7.3.1 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥。它们由 华

为CA和密钥管理中心定期归档。

7.3.2 证书操作期和密钥对使用期限

CA证书有效期不超过25年，订户证书有效期最长不超过三年。

CA密钥对使用期限和CA证书的有效期保持一致。订户证书的密钥对使用期限和订户证书的有效期保持一致。特殊情况下，对于签名类证书，为了验证在证书有效期内签名的信息，与之对应的公钥可以在证书的有效期限以外使用，直到私钥收到损坏或密钥对存在被破解的风险，如加密算法被破解。

7.4 激活数据

7.4.1 激活数据的产生和安装

激活数据指的是用以操作私钥或包含私钥的密码模块所需的数据值，而不是整个私钥数据，对激活数据的保护是为了防止对私钥的非授权使用

对于CA主体而言，私钥的激活数据存储于华为CA的密码保管箱中。

对于用户而言，私钥的激活数据是口令，那么这些口令必须满足以下要求：

至少 12 位字符或数字；

- 至少包含一个字符和一个数字；
- 不能和操作员的名字相同；
- 不能包含用户名信息中的较长的子字符串。

7.4.2 激活数据的保护

对于 CA 私钥的激活数据，华为CA按照可靠的方式由可信人员掌管，存储在华为CA密码保管箱中。在取用时需要完成双因子认证（工号权限认证+手机验证码验证）。

对于订户私钥的激活数据，必须在安全可靠的环境下产生，必须进行妥善保管，或者记住以后进行销毁，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。

7.4.3 激活数据的其他方面

只有在拥有证书介质并知道证书介质的PIN值时才能激活证书存储介质，进而使用私钥。

对于CA私钥的激活数据，存有华为CA数字认证中心的 CA 私钥，私钥的激活数据通常保存在华为CA的密码保管箱里面。不在其他任何地方存储，如因某种特殊情况确实需要带出时，其传送过程需在华为CA两名可信人员的监督下进行。并且用完一定要销毁，其他人员不得私自保存。

对于订户私钥的激活数据，通常情况下由订户保管， 若私钥激活数据因特别的原因需要进行传送时，订户应保护它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。 对于申请证书的订户激活数据的生命周期，建议订户根据业务应用的需要随时予以变更，使用期限超过 3 个月后应要进行修改。

7.5 计算机安全控制

7.5.1 特别的计算机安全技术要求

7.5.1.1设备保管与维护制度

对于设备有一套完整的保管和维护制度：

1） 设备登记与标签：对所有计算机设备进行详细登记，包括设备型号、序列号、购买日期、配置信息及责任人等。为每台设备贴上唯一识别标签，便于追踪和管理。

2） 存放环境要求：确保设备存放在干燥、通风、无尘、温度适宜的环境中，避免阳光直射和极端温度变化。禁止在设备周围存放易燃、易爆、腐蚀性物品。

3） 访问控制：设立专门的设备存放区域，实施门禁系统或钥匙管理制度，限制非授权人员进入。对重要设备（如服务器、核心交换机）实施物理锁定，防止未授权移动或操作。

4） 库存盘点：定期进行设备库存盘点，确保账实相符，及时发现并处理遗失或损坏的设备。

5） 定期清洁维护：定期对计算机设备进行检查、内外清洁、保养维护，防

止灰尘积累影响散热和性能。

6） 软件更新与补丁管理：定期检查和安装操作系统、应用软件及安全软件的更新和补丁，确保系统安全。

7） 设备维修：制定设备维修计划，建立满足正常运转最低要求的易损坏备件库。对设备进行维修时，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修有关的情况等。设备维修时，必须有派专人在场监督。

7.5.1.2系统稳定运行策略

1） 设备选型与验收：为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收。

2） 冗余和备份设计：采用增加冗余资源的方法，使系统在有故障时仍能正常工作。制定完善的数据备份策略，定期备份系统数据和业务数据，并建立快速恢复机制，确保在数据丢失或系统故障时能够迅速恢复业务运行。

3）操作规范制定：制定标准化的操作流程，明确不同操作人员的权限范围，制定数据安全、网络安全、物理安全等方面的规范，定期对操作人员进行培训，确保系统安全稳定运行。

7.5.2 计算机安全评估

华为CA及其运行环境通过了国家密码管理局和工信部的审查，并取得了相应资质。

华为CA使用的网络设备、主机、系统软件等均取得了国家有关认证检测机构出具安全标准的凭证。

华为CA及其整体运行环境具有高度安全性和合规性。华为CA不仅在设计、实施、运行等方面都符合国家的安全标准和法律法规要求，而且在管理、运维等方面也具备了相应的能力和保障措施，能够为用户提供安全可靠的数字证书服务。

7.6 生命周期技术控制

7.6.1 系统开发控制

系统开发采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员

的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

7.6.2 安全管理控制

1） 持续监控：对系统或应用进行持续的安全监控，包括日志分析、入侵检测等。通过日志检查来检查系统和数据完整性和硬件的正常操作。

2） 漏洞修复与更新：定期更新系统或应用的补丁和安全配置，以应对新的安全威胁和漏洞。同时，对已知漏洞进行及时修复，防止被恶意利用。

3） 应急响应：制定应急响应计划，明确在发生安全事件时的应对措施和流程。

4） 安全退役：当系统或应用达到退役期限或需要替换时，进行安全的数据擦除和设备销毁。

5） 合规性管理：确保整个生命周期内的安全管理活动符合相关法律法规和行业标准的要求。

7.6.3 生命周期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了管理部门鉴定，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施。针对密钥这一核心安全要素，我们还实施了严格的密钥管理策略，包括密钥的生成、存储、分发、使用、更新及销毁等各个环节，均有严格的安全措施加以保障，确保密钥的安全性与可用性，整个系统安全可靠。

7.7 系统网络的安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库运行的安全。华为CA采取防火墙、病毒防治、入侵检测、漏洞扫描、数据备份、灾难恢复等安全防护措施。

7.8 时间戳

系统签发的数字证书、CRL 包含有日期信息，且这些日期信息是经过数字签名的。

系统日志、操作日志都有相应的时间标识。这些时间标识不需要采用基于密码的数字时间戳技术。

系统所取的时间源是国家可信标准时间。

8 证书、证书撤销列表和在线证书状态协议

8.1 证书

CA签发的证书符合 X.509 V3格式。遵循RFC5280标准。

8.1.1 版本号

X.509 V3。

8.1.2 算法对象标识符

符合国家密码管理部门批准的算法对象标识符。

8.1.3 名称形式

CA数字证书中的主体(Subject)字段采用X.500可分辨名称(DN)格式，其命名空间遵循C=CN（国家=中国）的层级结构。该DN作为证书持有者在X.500目录体系中的唯一标识符，其所有属性值均采用UTF8String编码格式进行编码。其主体 Subject 其格式如下：

DN	全称	含义
CN	Common Name	主体的通用名称
OU	Organizational Unit	组织单位，表示公司内部的部门或分支机构（可选）。
O	Organization	组织名称，表示证书颁发者或持有者的公司/机构。
L	Locality	城市或地区名称（可选）。
ST	State or Province	州或省名称（可选）。

C	Country	国家/地区代码

8.1.4 证书扩展项

CA证书扩展项除使用 IETF RFC 5280中定义的证书扩展项，还支持私有扩展项。

CA采用的 IETF RFC 5280 中定义的证书扩展项：

- 颁发机构密钥标识符 Authority Key Identifier
- 主体密钥标识符 Subject Key Identifier
- 密钥用法 Key Usage
- 扩展密钥用途 Extended Key Usage
- 私有密钥使用期 Private Key Usage Period
- 主体可选替换名称 Subject Alternative Name
- 基本限制 Basic Constraints
- 证书撤销列表分发点 CRL Distribution Points

私有扩展项可支持以下类型：

- 个人身份证号码 Identify Card Number
- 企业营业执照（统一社会信用代码）IC Registration Number

8.2 证书撤销列表

CA签发的证书撤销列表符合 X.509 V2格式。遵循RFC5280标准。

8.2.1 版本号

X.509 V2。

8.2.2 CRL 和 CRL 条目扩展项

CRL扩展项：颁发机构密钥标识符Authority Key Identifier。

CRL条目扩展项：不使用CRL条目扩展项。

8.2.3 证书撤销列表结构

CRL 的结构如下：

a) 版本号(version)

b) 颁发者名称(issuer)

c) 生效日期(this update)

d) 下次更新(next update)

e) 签名算法(signature algorithm)

f) 授权密钥标识符(authority key identifier)

g) CRL数字(crl number)

h) 指纹(fingerprint)

i) 用户证书序列号/撤销日期(user certificate/revocation date)

8.3 在线证书状态协议

8.3.1 版本号

使用OCSP版本1（OCSP v1）。

8.3.2 OCSP 扩展项

不使用OCSP扩展项。

9 电子认证服务机构审计和其他评估

9.1 评估的频率或情形

审计和评估是为了检查、确认华为CA是否按照CPS及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。审计分内部审计和外部审计。

内部审计是由华为CA自己组织内部人员进行的审计，审计的结果可供华为CA改进、完善业务，内部审计结果不需要公开。

每年进行一次运营风险评估工作，识别内部与外部的威胁，评估威胁事件发生的 可能性及造成的损害，并根据风险评估结果，制定并实施处置计划。

除了内部审计和评估外，华为CA每年还委托第三方审计机构实施质量管理

体系和信息安全管理体系审计。

9.2 评估者的资质

内部审计和评估，由华为CA内部审计评估人员执行。

外部审计，由华为CA委托具备资质的第三方机构。。

9.3 评估者与被评估者之间的关系

内部审计人员与本机构的系统管理员、业务管理员、业务操作员的工作岗位不能重叠。

外部审计机构和华为CA之间是相互独立的关系，双方无任何足以影响评估客观性的利害关系。

9.4 评估内容

审计所涵盖的主题包括：

a. 人事审查；

b. 物理环境建设及安全运营管理规范审查；

c. 系统结构及其运行审查；

d. 密钥管理审查；

e. 客户服务及证书处理流程审查。

9.5 对问题与不足采取的措施

对审计中发现的问题，华为CA将根据审计报告的内容准备一份解决方案，明确对此采取的行动。华为CA将根据国际惯例和相关法律、法规迅速解决问题。

9.6 评估结果的传达与发布

除非法律明确要求，华为CA一般不公开评估结果。

对CA关联方，华为CA将依据签署的协议来公布评估结果。

10 法律责任和其他业务条款

10.1 费用

10.1.1 证书签发和更新费用

数字证书的收费标准按照国家和芜湖华为云计算技术有限公司相关主管部门批准的收费标准执行。根据证书实际应用的需要，华为CA在不高于收费标准的前提下可以对证书价格进行适当调整。

10.1.2 证书查询费用

在证书有效期内，对该证书信息进行查询，华为CA不对证书查询收取专门的费用。

10.1.3 证书撤销或状态信息的查询费用

证书撤销和撤销列表（CRL）的获取不应收取任何费用。

对于在线证书状态查询(OCSP)，由华为CA与依赖方或订户在协议中约定。

10.1.4 其他服务的费用

华为CA可根据请求者的要求，订制各类通知服务，具体服务费用，在与订制者签订的协议中约定。

10.1.5 退款策略

在实施证书操作和签发证书的过程中，华为CA遵守并保持严格的操作程序和策略。一旦订户接受数字证书，华为CA将不办理退证、退款手续。

如果订户在证书服务期内退出数字证书服务体系，华为CA将不退还剩余时间的服务费用。如果由于华为CA的原因，造成订户合同无法履行、订户证书无法使用，华为CA会将有关费用返还给订户。

10.2 财务责任

华为CA保证其具有维持其运作和履行其责任的财务能力。它应该有能力承担对订户、依赖方等造成的责任风险，并依据 CPS 规定，进行赔偿担保。

10.3 业务信息保密

10.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

1） 华为CA订户的签名私钥及解密密钥。

2） 审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被华为CA视为保密信息，只有安全审计员和业务管理员可以查看；除法律要求，不可在公司外部发布。

3） 其他由华为CA保存的个人和公司信息应视为保密，除法律要求，不可公布。

10.3.2 不属于保密的信息

不属于保密的信息包括但不限于以下方面：

a) 信息主体同意公开的信息不属于保密信息。

b) 依据法律、行政法规规定可以公开的信息，华为CA可以选择公开。

c) 订户数字证书的相关信息可以通过华为CA目录服务等方式向外公布，但华为CA认为涉及订户保密信息的除外。

d) 其他可以通过公共、公开渠道获取的信息。

10.3.3 保护保密信息的责任

a) 各方有保护自己和其他人员或单位的机密信息的并保证不泄露给第三方的责任。不将机密数据和信息(也不会促使或允许他人将机密数据和信息)用于协议项下活动目的之外的其他用途，包括但不限于将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储存机密数据和信息。

b) 当华为CA在任何法律、法规或规章的要求下，或在法院的要求下必须提供本电子政务电子认证业务规则中具有保密性质的信息时，华为CA应按照要求，向执法部门公布相关的保密信息，此情形下华为CA无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

10.4 用户隐私保护

10.4.1 隐私保密方案

华为CA尊重证书订户的资料的隐私权。保证完全遵照国家对隐私保护相关的法律法规要求，采取有效手段，保护个人隐私信息。

同时，华为CA将确保全体职员严格遵从内部工作相关制度和规定。

10.4.2 作为隐私处理的信息

证书申请人提供的不构成数字证书内容的资料被视为隐私信息。

10.4.3 不被视为隐私的信息

证书申请人提供的用来构成数字证书内容的资料，通常不认为是隐私信息，法律或行政法规另有规定的除外。

10.4.4 保护隐私的责任

除非执法、司法方面的强制需要，华为CA及其注册机构在没有获得客户授权的情况下，不会将客户隐私信息透露给第三方。

10.4.5 用户个人信息的收集

根据《电子签名法》第二十条规定，电子签名人向电子认证服务提供者申请电子签名认证证书，应当提供真实、完整和准确的信息。电子认证服务提供者收到电子签名认证证书申请后，应当对申请人的身份进行查验，并对有关材料进行审查。

华为CA作为合法的第三方电子认证企业，在受理用户申请数字证书时有权

对用户的身份进行核实。华为CA要求用户即证书申请人申请证书时通过纸质申请表、电子申请表等方式提供其能够证明其真实身份的证明材料。华为CA在《证书申请表》等其他相关协议中中已明确告知用户华为CA对用户包含但不限于用户个人的姓名、性别、年龄、身份证号码、联系方式等信息进行收集。

10.4.6 使用隐私信息的告知与同意

华为CA将采取适当的步骤保护证书订户的个人隐私，并将采取可靠的安全手段保护已存储的个人隐私信息。

华为CA如需超出约定范围及用途使用证书订户的隐私信息，应事先告知证书订户并获得同意及授权；如未获得同意及授权，华为CA不会将订户隐私信息透露给任意第三方。

10.4.7 个人信息的存储

华为CA使用高保密性的保密柜存储用户的纸质个人信息，采用双因子解锁方式。并且建立独立的机房设备存储已收集到的用户电子个人信息，采取严格的技术手段对存储的数据信息进行加密处理，确保用户个人信息不被窃取、泄露，但该等措施并不排除在华为CA的数据信息存储系统受到恶意黑客入侵等特殊情况及地震、洪水等不可抗力的自然因素而可能发生数据信息泄露的风险。

10.4.8 用户个人信息的使用

华为CA不会在与用户自身使用证书服务及应用无关的系统或场合使用证书用户个人信息。发生下列情形之一的，华为CA将依法提供用户个人相关信息：

1、基于国家法律、行政法规、规章的规定而提供的；

2、经过用户本人书面授权或同意提供的。

除上述情形外，华为CA不会向任何第三方提供用户的个人信息，不会将用户个人信息用于其他用途。

10.4.9 CA 对于用户个人信息的管理

华为CA通过以下措施规范用户个人信息的内部管理：

1、遵循法律法规的要求及行业规范要求采取对个人信息安全保护措施；

2、内部建立严格的用户个人信息收集、查阅、使用、处理等管理制度；

3、通过加强内部员工关于个人信息保护的培训，要求员工参加学习培训后签署用户个人信息保护的相关承诺书；

4、要求注册机构建立不能低于华为CA对用户个人信息的保护级别的用户个人信息保护制度，并提交华为CA备案。

10.4.10个人信息的查阅

用户如需查阅及浏览自身的个人信息，请用户按华为CA官方网站公布的联系方式联系华为CA查询。

10.4.11个人信息的删除和更改

1、个人信息的删除

按照法律法规要求或与用户证书服务协议以及华为CA个人信息保护政策的约定，用户在不涉及电子认证服务相关资料留存规定的特定情况下可以要求华为CA对用户的信息进行删除。

2、个人信息的更改

用户在使用CA证书服务过程中，个人信息发生变更的，应当自个人信息变更之日起5日内通过华为CA官方网站公布的联系方式提出；由于用户自身原因未及时将变更信息通知华为CA的，由此发生的风险由用户自身承担。

10.5 知识产权

除非额外声明，华为CA享有并保留对证书以及华为CA提供的全部软件的一切知识产权，包括但不限于所有权、名称权、著作权、专利权和利益分享权等。华为CA有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

按本CPS的规定，所有由华为CA签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于华为CA所有，这些知识产权包括所有相关的文件和使用手册。注册机构应征得华为CA的同意使用相关的文件和手册，并有责任和义务提出修改意见。

10.6 陈述与担保

10.6.1 电子认证服务机构的陈述与担保

华为CA在提供电子认证服务活动过程中的承诺如下：

a) 华为CA遵守《中华人民共和国电子签名法》、《中国人民共和国密码法》等相关法律的规定，接受国家密码管理局的领导，对签发的数字证书承担相应的法律责任。

b) 华为CA保证使用的系统及密码符合国家政策与标准，保证华为CA本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。

c) 华为CA签发给订户的证书符合华为CA的CPS的所有实质性要求。

d) 华为CA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，通报的有效形式包括但不限于邮件通知、官网公告。

e) 华为CA将及时撤销证书，并发布到CRL上供订户查询。

f) 华为CA拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

g) 证书公开发布后，华为CA向证书依赖方证明，除未经鉴证的订户信息外，证书中的其他订户信息均是准确的。

10.6.2 注册机构的陈述与担保

华为CA的注册机构在参与电子认证服务过程中的承诺如下：

a) 提供给证书订户的注册过程完全符合华为CA的CPS的所有实质性要求。

b) 在华为CA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人的信息不一致。

c) 注册机构将按CPS的规定，及时向华为CA提交证书申请、撤销、更新等服务请求。

10.6.3 订户的陈述与担保

订户一旦接受华为CA签发的证书，就被视为向华为CA、注册机构及信赖证书的有关当事人作出以下承诺：

a) 订户需熟悉本CPS的条款和与其证书相关的证书政策，还需遵守证书持有人证书使用方面的有关限制。

b) 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，可供华为CA或注册机构检查和核实。

c) 订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生。

d) 私钥为订户本身访问和使用，订户对使用私钥的行为负责。

e) 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应立刻通知华为CA和注册机构，申请采取撤销等业务处理。

f) 订户已知其证书被冒用、破解或被他人非法使用时，应按华为CA的CPS相关条款及时申请办理撤销其证书业务及时通知华为CA撤销其证书。

10.6.4 依赖方的陈述与担保

依赖方必须熟悉本CPS的条款以及和订户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方应了解证书中包含的各种重要信息及相关事项，以确保其合法性和有效性，包括但不限于：

a）证书持有者信息：确认证书中记录的签名者身份是否与实际签名者一致

b）证书的有效期：确保证书在有效期内使用，避免在证书过期后使用。

c）证书的用途：了解证书被授权的具体用途，确保其在合法范围内使用。

d）证书序列号：每个证书都有唯一的序列号，用于区分和追踪。

e）证书撤销信息：在证书撤销时，依赖方可采用适当的检查机制检查证书是否被撤销，可以通过证书撤销列表（CRL）或在线证书状态协议（OCSP）进行验证。

依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及电子签名的有效性。

证书依赖方对证书的信赖行为就表明他们已阅读并理解本CPS的所有条款，并同意承担证书依赖方有关证书使用的相关责任和义务。

10.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同 10.6.4。

10.7 担保免责

华为CA不对其签发的证书适用于其规定的目的以外的任何应用承担任何担保，对证书在其规定的目的以外的应用不承担任何责任。对由不可抗力，如战争、地震、洪灾、爆炸、恐怖活动等，造成的服务中断并由此造成的客户损失，华为CA不承担责任。

华为CA在签发数字证书之前，证书申请者已同意遵守责任书中的各项规定。如果证书申请者故意或无意地提供不完整、不可靠或已过期的信息，而又根据正常的流程提供了必须的审核文件，由此得到了华为CA签发的数字证书，由此引起的法律和经济责任由证书申请者全部承担，华为CA不承担与证书内容相关的法律和经济责任，但可以根据受害者的请求提供协查帮助。华为CA也不承担任何其他未经授权的人或组织以华为CA名义编撰、发表或散布不可信赖的信息所引起的法律责任。

10.8 赔偿责任限制

10.8.1 赔偿责任范围

如出现下述情形，华为CA承担相应有限赔偿责任：

a） 在订户提交信息或资料真实、完整、准确的情况下，华为CA签发的证书含有错误信息，导致订户或依赖方由此遭受损失；

b） 由于华为CA原因致使证书私钥被破译、窃取、泄露，导致订户或依赖方遭受损失；

c） 对于订户申请撤销的证书，华为CA未能及时撤销证书由此导致依赖方遭受损失。

华为CA只在证书有效期限内承担损失赔偿责任。在证书有效期内产生的损失，订户或依赖方应在知道或应当知道损失发生之日起三年内向华为CA书面提出索赔。

10.8.2 赔偿责任限额

华为CA对所有当事实体（包括但不限于订户、申请人或信赖方）的合计责任不超过该特定证书适用的赔偿责任上限。对于一份证书产生的所有数字签名和交易处理，华为CA对于任何实体有关该特定证书赔偿的合计责任应该限制在一个不超出下述赔偿责任上限的范围内。对直接损失所付法律责任的上限为：每张证书的赔偿额，不得超过证书的实付价格的3倍，这种赔偿上限可以由华为CA根据情况重新制定 ，华为CA会将重新制定的CPS公布于华为CA的网站以通知相关当事人。如在本CPS公布修订的1个月后继续使用华为CA提供的数字证书服务，即表明同意接受此等修订的约束。如果不予接受本CPS中的约束，订户可以停止使用证书或在上述期限内以书面形式向华为CA申请撤销证书。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有上限而不考虑电子签名和交易处理等有关的其他索赔的数量。当超过责任上限时，可用的责任上限将首先分配给最早得到索赔解决的一方。华为CA没有责任为每份证书支付高出责任上限的赔偿，而不管责任上限的总量在索赔提出者之间如何分配的。

10.8.3 责任免除

有下列情况之一的，应当免除华为CA之责任。

a) 订户在申请和使用华为CA数字证书时，有违反如下义务之一的：

a. 订户有义务提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息。如已提供的关键材料或信息有变更，可能影响证书使用的，订户应当及时通知华为CA。如因材料或信息变更未及时通知华为CA，给订户本人或第三方造成的损失，华为CA不承担责任；

b. 订户应当妥善保管 华为CA所签发的数字证书载体、私钥、保护密码、PIN的安全，不得泄漏或随意交付他人；

c. 订户在应用自己的密钥或使用数字证书时，应当使用可依赖、安全的系统；

d. 订户知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知 华为CA及相关各方，并终止使用该电子签名制作数据；

e. 订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度。不得

将数字证书用于华为CA规定使用范围外的其他任何用途使用；

f. 订户必须在证书有效期内使用该证书；不得使用已失密或可能失密、已过有效期、被冻结、被撤销的数字证书；

g. 订户有义务根据规定按时向华为CA交纳服务费用。

h. 由于下列依赖方的原因造成的损失，华为CA不承担任何赔偿责任，由依赖方自行承担。

b) 依赖方未经检验证书的状态即决定信赖证书的；

c) 依赖方明知或者应当知道证书存在超范围使用、超期限使用、被人窃取或者信息错误等情况，仍然信赖该证书并从事有关活动的。

外部注册机构或其他合作方依据协议约定或实际上承担履行证书受理与审核、订户身份鉴别、证书交付等工作的，因其违反协议约定或存在过错（包括但不限于未尽审核与鉴别义务、未妥善交付证书、未经授权处理订户私钥等行为），导致订户、依赖方或自身遭受损失的，订户或依赖方可以追究注册机构或合作方的责任，华为CA给予配合，但华为CA不承担赔偿或补偿责任。

由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。关于不可抗力的描述参见CPS 10.16.4。

因华为CA的设备或网络故障等技术故障而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的；本项所规定之技术故障引起原因包括但不限于：（1）不可抗力；（2）关联单位如电力、电信、通讯部门而致；（3）黑客攻击；（4）设备或网络故障。

如果华为CA能够证明其提供的服务是符合法律、行政法规相关规定实施的，华为CA将不对订户或依赖方承担任何赔偿或补偿责任。

10.8.4 有限责任

a) 华为CA所有的赔偿义务不得高于本CPS § 10.8.2 规定的赔偿责任上限。

b) 华为CA根据判决或裁定应当承担赔偿或补偿责任的，华为CA将按照法院的判决、仲裁机构的裁定承担相应的赔偿或补偿责任。

c) 对于由于华为CA自身原因，如没有严格按业务流程进行证书审批导致证

书的错误签发、假冒，或管理上的疏忽导致CA私钥泄漏、盗用等，造成了证书订户、依赖方的损失，华为CA将承担相应的赔偿责任，但这种责任是有限的。华为CA只对由于自身原因造成的用户直接损失承担责任，对间接的损失不承担责任。

10.9 赔偿

华为CA按照本CPS § 10.7 条款承担赔偿责任。

证书订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致华为CA和注册机构产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任。

a) 未向华为CA提供真实、完整和准确的信息，而导致华为CA或有关各方损失。

b) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。

c) 在知悉证书密钥已经失密或者可能失密时，未及时告知华为CA，并未终止使用该证书，而导致华为CA或有关各方损失。

d) 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个电子签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。

e) 证书的非法使用，即违反华为CA对证书使用的规定，造成了华为CA或有关各方的利益受到损失。

f）如订户在证书的申请、使用过程中存在的其他违反本CPS、服务协议、相关法律、法规的规定的行为，给华为CA造成损失的。

10.10 有效期限与终止

10.10.1有效期限

本CPS自发布之日起正式生效。

本CPS中将详细注明版本号及发布日期。

10.10.2终止

当新版本的CPS正式发布生效时，旧版本的CPS自动终止。

10.10.3效力的终止与保留

华为CA的CPS的中止（而非更新），意味着华为CA认证业务的终止。华为CA中止认证业务的过程将按国家有关主管部门的规定进行，并根据规定对受影响的客户进行安排，保证客户的利益不受影响或将受影响的程度减少到最小。

当由于某种原因，如内容修改、与适用法律相冲突，CPS和其他相关协议中的某些条款失效后，不影响文件中其他条款的法律效力。CPS的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

10.11　对参与者的个别通告与沟通

华为CA及其注册机构在必要的情况下，如在主动撤销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。认证活动的某一参与方与另一参与方进行通信时必须使用安全通道，以使其通信过程在法律上有效。

10.12　修订

10.12.1修订程序

本认证业务规则将尽量避免不必要的修改。但不定期地华为CA将对本CPS进行检查、评估，当华为CA认为应该对本CPS做出修改时，华为CA安全策略委员会成员将对本CPS及其他相关文档、协议提出修改建议，获得华为CA安全策略管理委员会批准后，由安全策略委员会组织CPS编写小组进行有关文档、文件的修改。修改后的CPS及其他相关文档、协议经华为CA法律顾问认可后，报安全策略委员会批准后正式发布。

10.12.2通告机制和期限

本CPS在华为CA的网站上发布。版本更新时，最新版本的CPS在华为CA的网站发布，对具体个人和单位订户不做另行通知。

10.12.3必须修改业务规则的情形

当管辖法律、适用标准及操作规范等有重大改变时，必须修改本CPS。

10.13 争议处理

华为CA、证书订户、依赖方等实体在电子认证活动中产生争端可按照以下步骤协商解决：

a) 当事人首先通知华为CA或其注册机构，根据本CPS中的规定，明确责任方；

b) 由华为CA相关部门负责与当事人协调；

c) 如果无法协商解决的，可以请求国家电子政务电子认证服务监管部门、仲裁部门或司法机构予以解决处理。

10.14 管辖法律

中华人民共和国法律、规则、规章、法令和政令将管辖华为CA的电子政务业务活动。

华为CA的任何业务活动受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能同有关法律、法规相冲突。

10.15 与适用法律的符合性

华为CA的所有业务、活动、合同、协议符合中华人民共和国法律、法规，包括但不限于，公司法、合同法、隐私法、消费者权益保证法等。

10.16 一般条款

10.16.1完整规定

本CPS将替代先前的、与主题相关的书面或口头解释。

10.16.2分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

10.16.3强制执行

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

10.16.4不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

在数字证书认证活动中，华为CA由于不可抗力因素而暂停或终止全部或部分证书服务的，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

10.17　其他条款

包括未在上述说明的其他相关内容条款，华为CA对本CPS拥有最终解释权。