东方中讯数字证书认证有限公司
电子认证业务规则（CPS）

（版本：v3.3）

修订表

版本	日期	备注
1.0	2003年10月28日	采用RFC3647标准
1.1	2005年4月30日	根据信息产业部电子认证服务管理办公室《电子认证业务规则规范（试行）完全版》修订
2.0	2005年11月1日	根据信息产业部电子认证服务管理办公室《电子认证业务规则规范（试行）完全版》修订
2.1	2008年12月18日	公司名称更换，修订
2.2	2011年3月21日	CRL发布周期、服务热线电话及审计日志保存周期修订
3.0	2014年2月20日	证书分类分级、鉴证手段等内容修订
3.1	2017年3月8日	公司电话、服务热线电话及地址变更
3.2	2018年4月8日	鉴证手段、信息库等修订
3.3	2018年11月12日	身份鉴证、证书发放方式、证书名称等修订

东方中讯数字证书认证有限公司安全管理委员会

发布日期：2018年11月12日

生效日期：2018年11月12日

版权声明

地址：重庆市南岸区复兴街9号6-1

电话：023-67030177、67030166

本CPS的最新版本请参见本公司网站http://www.ezca.org，除法律法规另有要求，不再针对特定对象另行通知。

东方中讯CA安全管理委员会负责本CPS的解释。

1 概括性描述

1.1 概述

1.1.1 电子认证业务规则

电子认证业务规则(CPS ,Certification Practice Statement，以下简称CPS)是电子认证服务机构(CA ,Certification Authority)对所提供的认证及数字证书生命周期（证书的管理、签发、注销以及更新）所涉及的相关业务规范的详细描述。电子认证业务规则包括责任范围、作业操作规范和信息安全保障措施等内容。

东方中讯CA 的CPS编制依据IETF组织关于证书业务规则的编写规则RFC3647和中华人民共和国工业和信息化部《电子认证业务规则规范（试行）》规范，并遵从《中华人民共和国电子签名法》，中华人民共和国工业和信息化部《电子认证服务管理办法》、《电子认证业务规则规范（试行）》，国家密码管理局《电子政务电子认证服务业务规则规范》以及《GB/T 28447-2012 信息安全技术电子认证服务机构运营管理规范》。

东方中讯CA电子认证业务规则详细描述了东方中讯CA从事电子认证服务所遵循的各项规范以及责任，适用于东方中讯CA所定制的数字证书策略（引用国标）。东方中讯CA电子认证业务规则适用于所有与东方中讯CA有关的终端实体，以及所有被东方中讯CA支持的服务提供者。

1.1.2 东方中讯CA

东方中讯数字证书认证有限公司成立于2001年4月12日，主要从事信息安全产品研发、电子认证服务、信息安全技术服务等业务，是经国家密码管理局、工业和信息化部批准的权威的、合法的、公正的第三方电子认证服务机构，是可以信赖的、专业的信息安全服务机构。公司获得了国家密码管理局颁发的《电子认证服务使用密码许可证》及《电子政务电子认证服务机构》许可、国家工信部颁发的《电子认证服务许可证》、公安部颁发的《计算机信息系统安全专用产品销售许可证》、“双软”企业和“双高”企业、国家

信息产业基地龙头企业等称号，并成立了重庆市电子认证工程技术研究中心和企业技术中心。

1.2 电子认证活动参与者

1.2.1 电子认证服务机构

负责创建、分发证书并在必要时提供验证以证实用户身份的机构，一般是受用户信任的权威机构，用户可以选择该机构为其创建密钥。通常将电子认证服务机构简称为CA，也成为CA中心、CA机构、认证机构、证书认证机构等。

1.2.2 安全管理委员会

东方中讯CA安全管理委员会负责安全策略、规范和决策制定，是东方中讯CA安全管理的决策机构。安全管理委员会的职责包括：收集与协调安全管理方面的问题和建议；制定并维护东方中讯CA的证书策略文件（CP）；对本CPS进行审核，以确保CPS与CP文件一致。 安全管理委员会应保证每年至少召开一次会议或进行一次文件会签，以对东方中讯CA相关制度规定进行检查修改和批准续期，并对中心运行状况进行通报。此外，在有其他重要变更时，安全管理委员会应根据实际情况及时通过会议或文件会签的方式对重要事项进行讨论和审批。安全管理委员会成员的组成来自于公司领导、各部门负责人以及法律顾问。

1.2.3 注册机构

具有下列一项或多项功能的实体，识别和鉴别证书申请者，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理用户撤销或挂起其证书的请求，同意或拒绝用户更新其证书或密钥的请求。通常将注册机构简称为RA或者RA机构。

1.2.4 订户

从电子认证服务机构接收证书的实体。在电子签名应用中，订户即为电

子签名人。

1.2.5 依赖方

依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

1.2.6 其他参与者

如证书制造机构、证书库服务提供者、以及其他提供电子认证相关服务的实体。

1.3 证书持有者分类

个人证书

东方中讯CA所指的个人证书对象为自然人，可用于需要区分、标识、鉴别个人身份的场合，还可用于数据加解密和信息签名，包括订单签名，以实现信息保密，提供信息原发性证明、完整性保障和抗抵赖。

机构证书

机构证书，包括机构单位证书和机构职位证书，可用于需要区分、标识、鉴别机构身份的场合，还可用于数据加解密和信息签名，包括订单、合同签名，以实现信息保密，提供信息原发性证明、完整性保障和抗抵赖。

设备证书

设备证书用于标识服务器、运营设备，还可用于数据加解密和信息签名，以实现信息保密，及提供信息原发性证明、完整性保障和抗抵赖。

1.4 证书应用

1.4.1 适合的证书应用

东方中讯CA的证书应用可分为身份证书、安全电子邮件证书、域名证书、VPN网关证书和代码签名证书等。

1.4.2 限制的证书应用

东方中讯CA所颁发的证书在功能上是受到限制的，如个人证书只能用于个人订户的应用，而不能作为服务器证书或机构证书使用。机构证书只能用于代表组织机构的场合。

证书的密钥用法扩展项中限制了与证书中公钥对应私钥的使用目的，如最终用户证书不能作为CA证书使用。这种限制是由基本限制扩展项缺省值确定的。然而，基于扩展项的限制的有效性取决于软件，如果有关软件不遵守有关约定，其对证书的使用将超出本CPS限定的应用范围，将是不受保护的。

同时，东方中讯CA所签发的数字证书严禁在一切违反中华人民共和国法律法规的情形下使用，否则其一切后果自行承担。

1.5 策略管理

1.5.1 策略管理者

东方中讯CA的CPS由安全管理委员会负责其起草、注册、维护以及发布。

1.5.2 联系人

联系人：东方中讯CA安全管理委员会

电话：023-67030177、67030166

地址：重庆市南岸区复兴街9号6-1

邮编：400061

1.5.3 CPS发布流程

东方中讯CA安全管理委员会编写CPS；

提交公司各部门进行审议，提出修改意见；

安全管理委员会整理修改意见，形成修改意见附件；

提交到公司领导层审议，并评注意见；

申请召开CPS评议会（公司高层领导参与）进行定稿评议；

评议通过并对外发布。

1.6 定义和缩写

1.6.1 公钥基础设施(PKI, Public Key Infrastructure)

公钥基础设施是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制，在这一体制中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性，又能保证信息具有不可抵赖性。目前，公钥体制广泛地用于CA认证、数字签名和密钥交换等领域。

1.6.2 证书策略(CP，Certificate Policy)

指一套规则，这些规则用于说明颁发给特定团体的证书的适用范围和/或遵从普通安全限制条件的应用的分类。

1.6.3 电子认证业务规则(CPS)

电子认证业务规则是电子认证服务机构对所提供的认证及相关业务的全面描述。电子认证业务规则包括责任范围、作业操作规范和信息安全保障措施等内容。

1.6.4 证书撤销列表(CRL，Certificate Revocation List)

证书撤销列表是一种包含注销的证书列表的签名数据结构。CRL是证书注销状态的公布形式，CRL就像信用卡的黑名单，它通知大家某些电子证书不再有效。

1.6.5 在线证书状态协议(OCSP，Online Certificate Status Protocol)

IETF颁布的用于检查数字证书在某一交易时间是否有效的标准。

1.6.6 电子签名认证证书(数字证书，Digital Certificate)

数字证书就是网络通讯中标志通讯各方身份信息的一系列数据，用于网络身份验证，其作用类似于日常生活中的身份证，所以数字证书又有“数字身份证”之称。它是由一个权威机构——CA(CertificateAuthority)中心发

行的，人们可以在网络通讯中用它来识别证书拥有者的身份。数字证书采用公钥密码体制，即利用一对互相匹配的密钥进行加密、解密。

数字证书的格式遵循ITUTX.509国际标准。标准的X.509数字证书应包含以下内容：

证书的版本信息；

证书的序列号，每个证书都有一个唯一的证书序列号；

证书所使用的签名算法，如RSA、SM2、SM3算法；

证书的发行机构（CA中心）的名称，命名规则一般采用X.500格式；

证书的有效期，现在通用的证书一般采用UTC时间格式，它的计时范围为1950年-2049年；

证书拥有者的名称，命名规则一般采用X.500格式；

证书拥有者的公开密钥；

证书发行机构（CA中心）对证书的数字签名。

1.6.7 电子签名人(证书持有者、订户)

被颁发给数字证书的个人、企业或者组织等证书主体，在电子签名行为中是作为主动使用数字证书对应私钥对信息内容进行加密。

1.6.8 电子签名依赖方(证书使用者、依赖方)

证书使用者是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

依赖方是指需要验证证书和签名的实体。依赖方可验证接收到的经过数字签名的数据电文的完整性和真实性。

1.6.9 私钥(电子签名制作数据，Private Key)

非对称加密算法中的一个密码串。它与公钥通过特定算法同时生成，其内容不同于公钥内容，与公钥互为加解密关系。其只保存于证书持有者处，在公钥基础设施PKI体系中，是证书持有者身份的真正标志。私钥通常用于解密公钥加密的密文（如：密钥交换）以及加密数据（如：电子签名），因此

又称为电子签名制作数据。

1.6.10 公钥(电子签名验证数据，Public Key)

非对称加密算法中的一个密码串。它与私钥通过特定算法同时生成，其内容不同于私钥内容，与私钥互为加解密关系。其被公开分发到证书依赖者处，在公钥基础设施PKI体系中，是验证证书持有者身份的重要数据。公钥通常用于加密数据（如：密钥交换）以及解密私钥加密的密文（如：电子签名），因此又称为电子签名验证数据。

2 信息发布与管理

2.1 信息库

东方中讯CA信息库是一个对外公开的信息库，它能够保存、取回证书及证书有关的信息，内容包括但不限于以下内容：最新的根和运营根、CRL、CPS和证书策略（CP）、公钥证书等相关资料。

东方中讯CA信息库不会改变任何从发证机构发出的证书和任何证书挂起或注销的通知，而是准确描述上述内容。

东方中讯CA信息库将及时发布包括证书、CPS修订、证书挂起和注销的通知和其它资料等内容，这些内容与CPS和有关法律法规保持一致。

除东方中讯CA授权者外，禁止访问信息库（或其它由CA RA维护的数据）中任何被CPS和/或东方中讯CA信息库宣布为机密信息的资料。

东方中讯信息库可通过下述地址访问

网站地址：www.ezca.org

CRL地址：

https://www.ezca.org/aspx/ch/userdownload.aspx?classid=136

OCSP地址：ocsp.ezca.org:20445/ocsp

2.2 信息发布

东方中讯CA的网站、认证系统的证书受理点、CRL及OCSP服务器构成东方中讯CA认证信息发布的信息库。

东方中讯CA的电子认证业务规则可从网站获取；用户证书可从证书受理点获取；已被撤销了的证书信息可从 CRL 站点、LDAP 查询，而证书的状态（有效性、撤销、挂起）可通过 OCSP获得。

2.2.1 CPS

东方中讯CA的CPS内容经安全管理委员会审核通过后，发布网站：http://www.ezca.org上，供自由浏览。

2.2.2 公众信息

东方中讯CA的公众信息发布在网站：http://www.ezca.org上，供自由浏览。

2.2.3证书及CRL发布

东方中讯CA数字证书签发成功后，即可通过公司网站的OCSP查询数字证书状态以及获取CRL列表。

2.3 信息发布时间和频率

东方中讯CA将会根据CPS的修改情况以及公司对外信息的变化，实时地进行信息发布和信息更新。

东方中讯CA运营根签发的订户证书废止列表（CRL）每24小时更新一次。

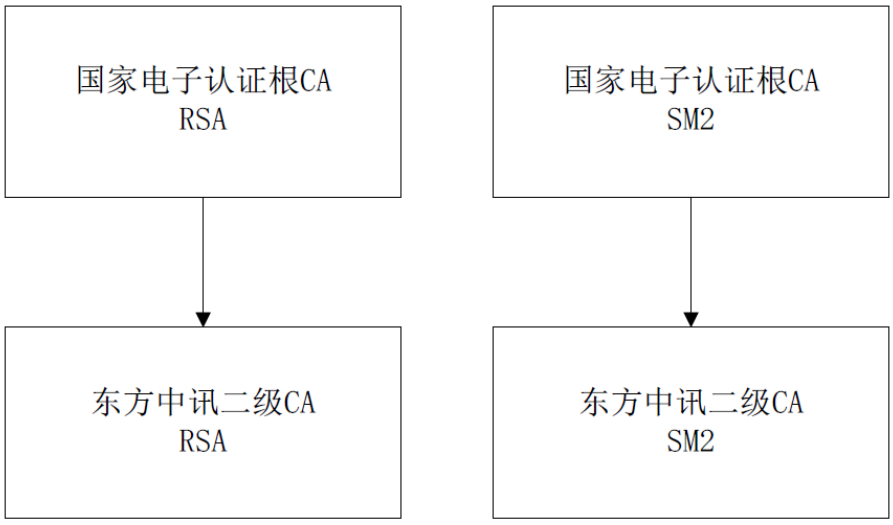
信息库中其他内容根据变更情况随时更改。

2.4 访问控制

东方中讯CA公布信息库允许所有互联网用户访问，但仅允许东方中讯CA可信管理员人进行更新。整个过程要做详细的报告，并做备份。

3 证书的身份识别与鉴别

3.1 根证书结构



其中顶级根证书为国家电子认证根CA。

3.2 命名

3.2.1 命名规范

根据证书对应实体的类型不同，东方中讯CA签发的证书实体命名符合X.500 甄别名规定。

东方中讯CA所发证书的签发者和主题域中包含X.500甄别名。

RSA根

国家电子认证根CA证书主题甄别名（CN=ROOTCA,O=OSCCA,C=CN）

东方中讯CA证书主题甄别名（CN = East-Zhongxun CA,O = East-Zhongxun Certificate Authority Center CO.LTD,C = CN）

SM2根

国家电子认证根CA证书主题甄别名（CN=ROOTCA,O=NRCAC,C=C）

东方中讯CA证书主题甄别名（CN = East-Zhongxun CA,O = East-Zhongxun Certificate Authority Center CO.LTD,ST = Chongqing,C = CN）

标准格式如下：

属性	备注
Country（C） =	国家
Organization（O） =	组织
Organizational Unit （OU） =	组织机构
State or Province （ST） =	省
Locality （L） =	市
Common Name （CN） =	通用名： 域名或IP（服务器证书）；个人名称（个人证书、代码签名证书）； 单位名称（单位证书、代码签名证书）。

3.2.2 命名意义

东方中讯CA订户在进行数字证书申请时不能使用匿名或伪名。

3.2.3 名称唯一性

东方中讯CA签发给某个实体的数字证书，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。

3.2.4 商标的承认、鉴别

东方中讯CA的数字证书不包含任何商标的信息。

3.3 初始身份确认

目前东方中讯 CA 的客户包括电子政务、医疗卫生、电子商务、互联网应用等客户。东方中讯CA必须根据证书申请订户所申请的证书类别的不同，

对于初始身份的鉴别， 将严格按照相关规范进行执行；不同证书类型，采用不同的鉴别方式；证书类别越高，安全等级越高，鉴别方式越严格，鉴别内容越全面。

对于所有类型的证书，包括个人类证书、机构证书、设备证书等，在申请时都必须对申请者进行真实身份的鉴别。

如通过查询权威第三方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。

个人类订户的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。

3.3.1个人证书的确认

第1类个人证书鉴别方法

需验证用户所提交的信息，证书中的通用名为订户的真实姓名。确认的方式可以是通过采用发送校验码或通过电话、手机短信等其他可靠的方式来验证申请者所提供的信息的真实性，必要时，还需通过查询权威第三方数据库等可靠的方式对申请者提供的身份信息进行核实验证，确保申请者所提供的信息与核查结果一致。

第2类个人证书鉴别方法

确认申请者身份的真实性和有效性。确认的方式必须是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），检查该证明文件是否有任何篡改或伪造的痕迹， 必要时可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。

确认申请者的地址。可通过银行卡账单或信用卡账单等核实申请者的地

址或直接依赖政府签发的身份证明文件上的地址。

核查证书请求的真实性。通过电话、邮件等方式，与申请者核实证书请求。

如果委托他人办理，需核查授权委托书及经办人身份证明。

对于以某个组织中的个人身份名义申请的，还需要提交其所在单位提供的证明材料。

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（如：企查查）、发送确认电子邮件等。

3.3.2 机构证书的确认

任何组织机构（政府机构、企事业单位等），在以组织机构名义申请机构类证书、设备类证书、SSL 服务器类证书等各类型证书时，应进行严格的身份鉴别，如通过查询权威可信第三方数据库（如：企查查）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。机构类订户的证书申请表上有申请者本身或被充分授权的证书申请者代表的签字（公章）表示接受证书申请的有关条款，并承担相应的责任。

东方中讯CA必须根据机构订户所申请的证书类别的不同，执行不同的身份鉴别方式，一般而言，证书类别越高，安全级别越高，鉴别方式越严格，鉴别内容越全面。确认机构是真实存在的、合法有效的实体。确认的方式可以是：政府机构签发的有效文件，包括但不限于工商营业执照、事业单位法人证书等，或通过签发有效文件的权威第三方数据库（如：企查查）确认。

可以通过语音通话、视频、拍照等方式，或查询权威第三方数据库（如：企查查）等方式对申请者及其申请材料进行验证，确保所提供的信息与核查结果一致。如有需要，可通过第三方（如：号码百事通114）得到的电话号码、邮政信函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个人身份真实情况。

东方中讯CA需检查数字证书申请表中机构授权的经办人信息与经办人有效身份证是否一致，确保经办人得到申请机构的授权。

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是否一致，确保经办人得到申请机构的授权。必要时，应对经办人身份实施面对面的审核方式，如有需要，东方中讯可通过第三方（如：号码百事通114)得到的电话号码与申请机构联系，以确认经办人身份真实性及授权。

在域名、设备名称被作为证书主题内容申请证书时，还需要验证该组织是否拥有该域名、设备的所有权，例如要求提交域名所有权文件、归属权证明文件或者申请者对所有权的书面承诺等。

如果认为有需要，东方中讯CA还可以通过从第三方获取（如：全国组织机构统一社会信用代码公示查询平台）的信息来验证该申请机构的身份， 如果东方中讯CA无法从第三方得到所有所需的信息，可要求申请者提供额外的信息和证明材料。

3.3.3 设备证书的确认

设备身份的鉴别会根据其设备拥有者的不同而不同，必须对订户进行身份鉴别，包括如下材料：数字证书申请表、设备拥有者身份证明的文件、所属行业特定证件、单位银行账户开户许可证、经办人身份证复印件（以上资料全部盖单位公章，申请表签名处经办人手写签名。数字证书申请表内包含经办人姓名、身份证号码、办理事宜等信息，机构在数字证书申请表盖公章即视为对经办人授权）。

鉴别方法：

个人订户：参照 3.3.1节第2类个人证书鉴别流程执行；

机构订户：参照 3.3.2节机构身份鉴别流程执行。

3.4 密钥更新请求中的标识与鉴别

密钥更新

在订户证书到期前，订户需要获得新的证书以保持证书使用的连续性。东方中讯CA一般要求订户产生一个新的密钥对代替过期的密钥对，称作“密钥更新”。

证书更新

东方中讯CA允许订户为一个现存的密钥对申请一个新证书，称作“证书更新”。

对于密钥更新而言，订户证书除公钥、有效期和序列号改变外，其他信息都没改变；对于证书更新而言，和密钥更新相比，订户的证书公钥不改变。密钥更新和证书更新与申请一个新证书在技术上是不同的。在申请一个新证书时，证书订户需到东方中讯或其注册机构的证书服务站点申请注册，填写必要的申请信息；而对于密钥更新和证书更新，订户虽然同样需要访问东方中讯CA相应服务网页，但用户需填写确认申请信息。

在东方中讯CA证书认证业务处理过程中，在证书有效期到期前只能通过密钥更新或证书更新签发具有相同签发者、主体名和证书用途的证书。除非先将证书撤销，否则在证书有效期到期前，不能通过申请新证书的方法获得具有相同签发者、主体名和证书用途的证书。

当用户申请信息发生变化时，东方中讯CA会将用户未到期证书进行证书撤销，在新申请证书的方式颁发一个证书。

3.4.1 常规密钥更新的标识与鉴别

对于一般正常情况下的密钥更新，订户访问东方中讯CA网站相应的服务网页进行密钥更新申请，系统自动获取订户原证书的相关信息，如订户甄别名、证书序列号等，形成证书密钥更新申请信息，申请信息包含新公钥并由

更新前的私钥签名（对于加密证书密钥更新而言，申请信息不包含新公钥）。

东方中讯CA的证书认证系统将对密钥更新申请进行验证，包括验证申请签名，然后进行与新证书申请一样的鉴证、审核操作。

3.4.2 撤销后密钥更新的标识与鉴别

东方中讯CA不进行撤销后的密钥更新操作，如用户需使用证书按照新申请方式处理。

3.5 撤销请求中的标识与鉴别

在东方中讯的证书业务中，证书撤销请求可以来自订户，也可以来自东方中讯或其注册机构。证书撤销的方式可以是订户自己撤销，也可以由订户要求东方中讯或其注册机构管理员撤销，东方中讯和其注册机构在认为必要的时候，有权发起撤销订户证书。

订户本人撤销时的身份标识与鉴别使用原始身份验证相同的流程，详见3.3.1个人身份的鉴别、3.3.2组织机构身份的鉴别和3.3.3其他身份的鉴别。

如果是因为订户没有履行本《电子认证业务规则》所规定的义务，由注册机构申请吊销订户的证书时，不需要对订户身份进行标识和鉴别。

3.6 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，对原证书进行吊销处理。

证书变更的标识与鉴别使用原始身份验证方式相同的流程，其要求与3.3相同。

3.7 证书更新的标识与鉴别

证书更新的标识与鉴别，订户访问东方中讯CA网站相应的服务网页进行证书更新申请，系统自动获取订户原证书的相关信息，如订户甄别名、证书

序列号等，形成证书更新申请信息，申请信息由私钥签名。

东方中讯CA的证书认证系统将对证书更新申请进行验证，包括验证申请签名，然后进行与新证书申请一样的鉴证、审核操作。

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

证书申请实体包括年满18岁以上具有独立法定民事及法律责任的中华人民共和国公民、具有独立法人资格的企事业单位、法律承认的各类社会团体、东方中讯CA授权的证书注册机构以及受理点。

4.1.2 证书注册过程及责任

东方中讯CA用户证书（除WEB服务器证书、VPN相关证书和仅用于加密的加密证书外）一律存储于安全电子令牌中进行发放，以保证用户证书发放环节的安全性。申请证书类型的不同，需要提供不同的身份证明材料。

证书注册过程

证书申请者通过东方中讯CA网站或者微信公众号注册用户，注册完成后登录数字证书自助办理平台，选择需要办理证书的区域、行业、项目、类别并如实填写相关信息；

证书申请者上传申请表、单位证明材料、身份证明材料至证书自助办理平台进行审核(以上材料全部加盖单位公章、申请表签名位置手写签名)；

东方中讯CA注册机构工作人员认真负责地对用户身份进行鉴别；

东方中讯CA根据身份审核结果拒绝或签发数字证书。

证书注册中各方责任

东方中讯CA有责任按照统一的规范对申请用户的身份进行认真负责的审

核，并且负责安全地发放数字证书。证书申请用户需要准确如实地填写申请表，并提供真实的材料。

4.2 证书申请处理

东方中讯CA需要审查用户提交的申请材料是否齐全，填写的证书申请表是否符合规范，身份鉴别材料是否符合要求。

证书申请材料包括证书申请表和如下材料：

组织机构、企业申请者（详见3.2.1.2）

个人申请者（详见3.2.1.1）

东方中讯CA证书申请、签发周期为48小时，通常东方中讯CA将在申请材料完备的情况下即时进行申请处理流程，并且在审核通过的情况下马上签发数字证书。由于特殊原因未能当时领取证书的用户，东方中讯CA将会在尽可能短时间内通知用户领取证书或以快递等方式送达用户。

4.3 证书签发

4.3.1 证书签发中的行为

人员编制

鉴证人员和审核人员

工作分配

个人证书	机构证书	设备证书
录入、制证、交付由鉴证员完成；审核由审核员完成	录入、制证、交付由鉴证员完成；审核由审核员完成	录入、制证、交付由鉴证员完成；审核由审核员完成

4.3.2 证书签发通告机制

东方中讯CA的数字证书由东方中讯CA统一申请、发放，并且存储于安全电子令牌中或根据用户要求存储于其他存储介质，因此采取的是现场证书发

放方式，由用户填写或监督东方中讯CA工作人员填写申请信息，证书签发成功后将公钥证书安装到安全电子令牌中发放给用户。由于其他原因用户未能现场领取证书的，则直接通知用户领取证书或以快递等方式送达用户。

4.4 证书接受

4.4.1 申请者接受证书方式

对于由注册机构代替证书订户产生证书请求、证书密钥对、下载证书的情形，则订户通过面对面的方式从注册机构接受载有证书和私钥的介质的行为，即表明了用户接受了证书；

当订户通过其他方式，如邮件快递，接收载有证书和私钥的介质后，在约定的时间内未表示异议，即表明用户接受了证书；

订户根据指引，访问东方中讯的证书下载服务站点将证书下载到本地存放介质，证书即表明订户接受了证书。

用户同意接受证书，并履行其按规范使用证书以及保管自己证书、密钥的责任。

4.4.2 申请者接受证书行为

个人证书	机构证书	设备证书
由用户自行下载	当面交付或快递交付	当面交付或刻盘快递交付

4.4.3 证书发布方式

东方中讯CA在证书签发完成后，将用户数字证书通过LDAP证书库发布到从目录服务器上，用户可通过公司网站查询、下载数字证书。

除非与证书订户间有特别的约定，东方中讯CA将其签发的证书发布到目录系统上。

4.4.4 电子认证服务机构在颁发证书时对其他实体的通告

东方中讯CA不承担在颁发证书时主动通告其他用户的义务，用户可通过

东方中讯CA网站在目录服务器中查询并下载其他用户的数字证书。

4.5 密钥对和证书的使用

4.5.1 订户使用私钥和数字证书及其相关责任

订户接受证书后，对数字证书的使用具有如下责任：

合法使用证书，并按照东方中讯CA制定的证书使用规定、用户的法律责任和财务责任使用证书；

安全保管个人的密钥以及相关安全密码。

证书使用用途、范围以及限制见1.3、1.4节。

除东方中讯CACPS或证书自身禁止，使用东方中讯CA所规定的任何证书应由每个用户自由选择。如果任何证书的应用未列入使用范围，则不予批准使用。

4.5.2 依赖方使用订户私钥和数字证书及其相关责任

依赖方使用订户的公钥数字证书，可验证订户身份的真实性，订户数字签名信息的完整性以及不可抵赖性。并可与公钥证书对应订户实现信息加密共享。依赖方对证书的使用应，依据CPS规则检查其有效性。

4.6 证书更新

证书更新指不改变订户关于证书中的公开信息的情况下为订户重新签发一张证书。

4.6.1 证书更新情形

证书即将或已到期；

订户密钥泄露或受到攻击威胁；

订户特殊要求（如：证书数据损坏）；

其他。

4.6.2 请求更新的实体

处于使用状态的证书实体都可在上节描述情况下申请更新证书。

4.6.3 证书更新请求处理

东方中讯CA用户证书更新分为两种方式：

在线自助更新：用户通过原有数字证书（即将过期但尚未过期）访问东方中讯CA的自助更新网页进行更新操作；

现场更新：用户持原有数字证书到东方中讯CA授权RA注册机构，完成申请材料的审核，进行证书更新。

4.6.4 颁发新证书时对订户的通告

如果是在线自助更新，则不需要公告订户；如果是现场更新则直接通知订户领取新证书。

4.6.5 构成接受更新证书的行为

订户在线进行证书更新；

订户到东方中讯CA授权的RA注册机构进行证书更新，确认并接收更新证书。

4.6.6 电子认证服务机构对更新证书的发布

东方中讯CA将注销原证书，通过CRL发布。新证书可通过目录服务器查询下载。

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

通过东方中讯CA目录服务可查询证书是否有效。

4.7 证书密钥更新

证书密钥更新指订户或其他参与者生成一对新密钥，并申请为新的公钥签发一个新证书。

4.7.1 证书密钥更新情形

密钥对应的数字证书到期（一般用户私钥的有效期是与其对应的证书有效期一致的）；

忘记或泄露证书使用的安全密码；

证书数据损坏；

证书对应私钥安全性受到威胁；

技术发展（如：密钥位数以不能保证足够的安全性）。

4.7.2 证书密钥更新请求实体

所有证书状态为使用中的东方中讯CA证书用户。

4.7.3 签发更新密钥对的证书流程

同4.6.3节的证书更新流程。

4.7.4 颁发新证书给订户时的通告

同4.6.4节。

4.7.5 构成接受密钥更新证书的行为

同4.6.5节。

4.7.6 电子认证服务机构对密钥更新证书的发布

同4.6.6节。

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4.6.7节。

4.8 证书变更

4.8.1 证书变更情形

证书用户DN信息改变；

证书用户E-mail地址改变。

4.8.2 证书变更请求实体

所有证书状态为使用中的东方中讯CA证书用户。

4.8.3 证书变更请求处理流程

与原始证书签发流程相同，证书有效期为证书变更时间到原证书到期时间。

4.8.4 颁发新证书给订户时的通告

现场颁发新证书给用户，或者直接联系用户领取新证书。

4.8.5 构成接受变更证书的行为

东方中讯CA按修改后的用户信息生成X.509格式证书，并颁发证书给用户；

用户核对证书内容，并确认接受证书。

4.8.6 电子认证服务机构对变更证书的发布

同4.6.6节

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4.6.7节

4.9 证书撤销

4.9.1 证书必须撤销的情形

用户没有按规定及时缴纳数字证书服务费用；

用户没有按照CPS规范要求使用证书；

证书主体消亡；

用户提供的证书申请材料虚假；

用户要求撤销数字证书（如：证书对应私钥丢失、怀疑密钥受到攻击等）；

当东方中讯CA因某些原因停止业务，并且没有安排其他的CA提供证书撤销服务；

当东方中讯CA从事电子认证业务的资格被撤销后，东方中讯CA除继续维持CRL/OCSP信息库的情况外，将撤销或终结所有已签发的证书；

东方中讯CA用于签发证书的CA证书私钥可能被泄露时，将根据应急预案撤销所有已签发的证书；

证书的重要参数被国际国内主流标准认为有重大风险时；

其他情况（如：如果国家法律、法规要求）。

证书撤销分为主动撤销和被动撤销，主动撤销是指用户主动申请撤销其数字证书，RA机构审核申请后撤销其证书。被动撤销是指电子认证服务机构确认用户违反CPS规则内容申请使用证书，或者证书主体消亡，则撤销数字证书。

4.9.2 可请求撤销证书的实体

所有证书状态为使用中的东方中讯CA证书用户、东方中讯CA授权的证书注册机构以及具有足够证据可证明有必要撤销他人证书的实体。

同时，东方中讯CA也可在4.9.1所述的情况下主动撤销订户的证书。

4.9.3 证书撤销请求的流程

电子认证机构根据CPS规则以及CA策略授权RA机构管理人员执行撤销操作；

数字证书用户向RA机构申请撤销证书，经审核通过，根据CA策略由授权工作人员撤销其证书；

向RA机构申请撤销他人数字证书，须提交足够证据，RA机构经过证实，撤销数字证书。

4.9.4 订户证书撤销请求宽限期

证书有效期内订户都可以提交证书撤销请求。

4.9.5 电子认证服务机构必须处理撤销请求的时间

RA在接到撤销请求以及必要材料后，应在24小时内完成审核以及撤销操作。

4.9.6 依赖方检查其所依赖证书的状态

依赖方可通过访问东方中讯CA目录服务器获取证书状态信息。

4.9.7 CRL发布频率

CRL是由CA签发服务器产生的，其产生方式与证书的产生方式相同。CRL的产生可由CA系统的管理员通过系统的控制菜单手工产生或者通过系统的CRL产生策略自动生成。CRL产生后，通过目录服务器系统发布。

东方中讯CA的CRL通常为每日发布，并根据需要实时发布或延时发布。

4.9.8 CRL发布最大延迟

东方中讯CA的CRL发布最大延迟周期为24小时。

4.9.9 在线证书状态查询可用性

通过OCSP在线证书查询协议查询证书状态，该服务7X24小时可获得。

4.9.10 依赖方在线撤销状态查询

依赖方可通过东方中讯CA目录服务器或OCSP在线查询证书撤销状态。

4.9.11 撤销信息的其他可用发布形式

除了通过 LDAP目录服务发布 CRL，或通过OCSP在线状态服务查询外，东方中讯CA所发布的CRL也可通过网站相关服务获得。

4.9.12 因为私钥损害而造成的证书撤销

无论是订户还是东方中讯，发现证书密钥受到安全损害时应立即撤销证书。

4.9.13 证书挂起的情形

东方中讯CA不适用此业务。

4.10 证书状态服务

4.10.1 证书状态查询服务的操作特点

东方中讯CA证书和CRL发布于支持X.500协议标准的目录服务器中。证书和CRL的查询通过LDAP协议实现。证书由签发服务器发布到系统的主目录服务器上，并通过目录服务器的自动映射功能，将证书映射到从目录服务器中，供用户查询和下载。

东方中讯CA提供了方便的Web查询方式。

4.10.2 查询服务的可用性，以及服务不可用时的适用策略

东方中讯CA的查询服务是通过网站http://www.ezca.org提供，时间是7×24小时不间断。

由于不可预测原因造成通过目录服务无法进行查询，则东方中讯CA将在48小时之内，通过查询CA数据库中证书状态信息发布到网站上。

4.10.3 查询服务的其他可选特征

东方中讯CA证书订户可通过服务电话服务查询证书状态信息。

服务电话：（023）400 023 5888

电话服务时间：非节假日周一到周五每日9:00-18:00。

4.11 订购结束

订购结束是指当证书有效期满或者证书撤销后，该证书的服务时间结束。

订购结束包含以下两种情况：

证书有效期满，订户不再延长证书试用期或者不再重新申请证书时，东方中讯CA即视为订购结束；

证书在有效期内被撤销的，东方中讯CA也视为订购结束。

4.12 密钥托管和恢复

4.12.1 私钥生成、备份和恢复的策略和实践

使用安全证书存储介质（如：电子令牌、IC卡等）的用户，其签名密钥对将在硬件设备中产生，若通过浏览器申请的证书其对应签名密钥对则由本地计算机生成。用户的加密密钥对将在重庆市密钥管理中心（KMC）产生。用户签名私钥应由用户妥善保管，一般不做备份，也不能恢复。用户的加密密钥在KMC备份并可恢复。

4.12.2 会话密钥封装和恢复的策略和实践

会话密钥通常采用非对称密钥对进行加密封装和解密恢复。

5 认证机构设施、管理和操作控制

东方中讯CA严格遵循电子认证行业相关国家标准。其认证服务信息系统

在符合安全和管理策略情况下接受第三方审计和审查。东方中讯CA对参与管理的工作人员都进行了严格的背景审查和专业培训，保证了密钥生成、实体鉴别、证书签发、证书撤销、审计和归档等相关操作的安全和规范。

5.1 物理控制

5.1.1 场地位置和建筑

东方中讯CA中心的机房严格按照国家相关标准建设，并通过了国家密码管理局安全性审查和验收，具备抗震、防火防水、恒温恒湿、双路供电、备用发电、门禁视频监控等功能，确保了认证服务的连续性和可靠性。

5.1.2 物理访问

东方中讯CA的机房区域分为管理区、服务区和核心区，每个区域进出采用指纹加门禁卡进行身份认证，且每个区域均有独立的视频监控进行动态录像。

外来人员访问机房，需经过公司相关领导批示，并持临时访问证在内部工作人员陪同下进行。

内部操作人员访问机房，管理区采用单人指纹加门禁卡，服务区和核心区采用双人指纹加门禁卡。所有的内部工作人员进入机房后均受到严格的访问控制，并有24小时视频监控。

5.1.3 电力和空调

主备机房供电均采用市电+UPS双路供电，保证外部供电中断后仍有两小时后备电源；主机房超过两小时以上（含两小时）的停电由大楼发电机组实施供电，备份机房则没有发电机配备。

主备机房空调均采用高效能的机房专用精密恒温恒湿空调系统，保证了认证系统正常运行。东方中讯CA参照相关标准对电力和空调系统进行定期维护和保养。

5.1.4 水患防治

主备机房建设时严格按照高安全机房建设规范采取相应措施，防止水患

的发生，并在易发生水患处部署了漏水检测系统最大限度的减小对认证系统的影响。

5.1.5 火灾预防和保护

东方中讯CA主备机房均采用防火阻燃材料建设，所有区域配有全自动防火监控系统和七氟丙烷气体消防系统，避免火灾的发生，并通过了消防部门验收。

5.1.6 介质存储

认证系统中包含软件、数据、审计、归档和备份信息的所有介质均放于机房安全存储区域中。所有的介质均受到严格的访问控制和安全保护，保证其不会被意外破坏。

5.1.7 废物处理

根据废物的不同存在特性（如：物理垃圾、信息数据等）采用不同的销毁办法。敏感的文件资料（包括纸质、光盘）抛弃前要进行粉碎处理；对于存储或传输信息的介质，在抛弃前要做不可读处理；加密设备在报废前要根据生产厂商的指南做格式化或者物理销毁。

5.1.8 异地备份

东方中讯CA主机房采用硬盘拷贝方式对数据进行备份，并定期对保存的数据进行恢复测试，确保数据的可用性。当主系统不能正常运行时，能及时切换到备份系统，继续提供认证服务，保证了服务了连续性。

5.2 操作过程控制

5.2.1 可信角色

东方中讯CA提供具有高可靠性和高安全性的服务。必须确保具有以下操作权限的员工、第三方服务人员、顾问等是东方中讯CA认定的可信人员：

接受、拒绝或者进行其他对证书的申请、撤销、更新等操作；

处理用户的注册信息或注册请求；

操作和控制有关东方中讯CA信息系统；

根据以上定义，东方中讯CA的可信角色包括但不限于：

●网络安全管理员

●数据库管理员

●密钥管理员

●系统管理员

●CA管理员

●CA审计员

●RA管理员

●RA审计员

●目录服务管理员

●RA审核人员

●RA录入员

●制证人员

●发布系统管理员

通过建立上述角色，能够明确责任分担，建立符合需要的安全管理机制，从而有效的控制内部风险和危机的发生，保证了内部的操作规范，有效减少了内部风险的发生。担当可信角色的人员必须是可信人员。

东方中讯CA根据本CPS和授权协议的许可范围，制定了证书服务机构的运营管理规范，确保其受信任的人员在受到相关约束的同时够根据其职责范围对系统进行管理。

5.2.2 角色身份鉴别

东方中讯CA对其可信角色有严格的识别和鉴定过程。在成为东方中讯CA可信人员之前，必须进行身份背景调查与认证：

根据实际需要确定不同的角色，对其划分权限和职责要求，设定不同角色的身份背景要求；

按照设定的背景要求，对符合相应角色要求的人员进行身份背景调查；

通过背景调查的人员，对其检查其他条件是否满足东方中讯CA相关要求；

在通过身份鉴别之后，根据作业性质和权限的需要，发放系统操作门禁卡、登录密码、登录安全电子令牌等，并且系统将独立完整地记录其所有的操作行为。

5.2.3 角色任务划分

东方中讯CA对每个操作人员的责任和权限进行了明确的划分，禁止进行超越安全权限的操作和行为。不同角色由不同的人员担任。进行角色任务划分人员，包括但不限于：

●验证证书申请信息的工作人员；

●负责证书的申请、撤销、更新和进行信息注册等服务请求的批准、拒绝或其他操作的人员；

●负责进行证书的签发、撤销等工作或者能够访问敏感信息的人员；

●负责处理注册用户信息的人员；

●生成、签发和销毁CA系统证书的人员；

●能更改、重置和删除重要口令的人员；

●密钥及密码设备的管理、操作人员。

必须确保有至少一名密钥管理员及两名密钥分管员同时在场，才能对密码机进行相关操作。所有涉及到对东方中讯CA信息系统直接或间接操作时，都应至少有两名以上工作人员同时在场，一人进行操作，另外一人进行监督和记录。

非东方中讯CA人员或第三方服务人员需要进入机房操作时，必须经审查同意后，在至少一名可信人员全程陪同和监督下，完成相关操作。

东方中讯CA按照知识分割、双重控制以及最小权限的原则，会限制某些

岗位角色之间由同一组人员兼任的安全要求，这就是角色的职责分割。涉及职责分割的角色主要包括系统维护、技术研发、密钥管理、证书管理、安全管理以及运营审计几大类。

5.2.3.1 系统维护类

负责生产系统的管理和维护，包括

- ●运维管理人员；
- ●网络安全管理员；
- ●系统维护管理员；
- ●数据库管理员；
- ●CA系统管理员

5.2.3.2 技术研发类

负责系统开发和实施，包括

- ●产品研发人员
- ●项目实施人员

5.2.3.3 密钥管理类

负责密钥管理系统的操作，包括

- ●密钥管理员
- ●密钥分管员

5.2.3.4 证书管理类

负责证书批准、撤销等操作，包括

- ●鉴别验证服务人员

5.2.3.5 安全管理类

负责运营安全管理，包括

●安全管理员

●物理环境安全管理员

5.2.3.6 运营审计类

负责运营审计，包括

●运营审计员

5.3 人员控制

5.3.1 工作人员资质

东方中讯CA对工作人员的资质、经历以及经验等情况都进行了严格的审查和核实，要求无重大工作失误、无违法犯罪记录、无不良信用记录等。

东方中讯CA要求所有的系统管理和操作人员必须具备符合该岗位需要的相关技能资质，在经过内部培训和保密教育后，方能录用。

5.3.2 背景审查

东方中讯CA与有关政府部门和调查机构合作，通过合法手段对可信人员进行背景审查和评估。背景审查流程如下：

●行政人事部对应聘人员的资料进行确认；

●行政人事部通过与有关单位和部门进行联系审查资料真实性；

●用人部门对试用员工进行考核观察；

●三个月的试用期考核；

●签署保密协议；

●正式上岗工作。

根据不同的岗位特点，背景审查应包括但不限于：

●身份证明，如个人身份证、户口本、护照等；

●学历、学位及其他资格证书；

●个人简历，包括受教育、培训经历，工作经历以及相关证明人；

●无犯罪记录证明材料；

●诚信记录或信用记录材料。

东方中讯CA确立此流程管理规则，确保可信人员受到合同的约束，不许泄露东方中讯CA证书服务体系的敏感信息。

5.3.3 人员培训

东方中讯CA提供其工作人员在职时所必须的技能培训，使他们能够令人满意的履行自己的工作职责。

根据人员岗位以及角色的不同，东方中讯CA提供的培训包括(但不限于)：

●PKI的基本概念和知识；

●岗位工作职责；

●东方中讯CA运营管理规范；

●系统硬件与软件的安装、维护和管理；

●东方中讯CA业务操作规范；

●灾难恢复和保持业务连续性处理程序。

东方中讯CA要求员工认真参与培训，并定期对培训内容进行考核。

5.3.4 再培训周期和过程

根据东方中讯CA策略调整、系统更新以及岗位职责变动等情况，要求员工定期进行继续培训以适应新的变化。

5.3.5 工作岗位轮换

为了配合认证系统的运营需要和岗位适应性的需要，东方中讯CA会根据各方面综合考量，选择合适的人员，在不同的岗位进行轮换。东方中讯CA严格控制进行岗位轮换的人员，使得进行运维人员和负责系统设计、开发的的

人员承担不同的职责，双方的岗位分离，为了确保安全，双方角色不能互换。

5.3.6 未授权行为及权利使用和处罚

根据东方中讯CA运营管理规范和安全规范的要求，可信人员的操作将被严格限制在其本身的职责范围内。未授权行为包括（但不限于）：

未经授权、滥用权利使用东方中讯CA系统；

超出权限使用东方中讯CA系统等进行的越权操作；

越过安全系统或者使用伪装、欺骗等手段使用东方中讯CA系统。

当员工被怀疑，或者已进行了未授权的操作，东方中讯CA在得到信息后立即撤销该员工物理和逻辑上的系统访问权限，同时，将会由安全管理委员会指定专人对事件进行详细调查。如果事实成立，将根据情节严重程度，采取包括批评教育、移交司法机关等相应处理措施。

5.3.7 对独立签约者而非实体内部人员的控制

东方中讯CA将严格依照本CPS和相关规定的要求聘请专业的第三方服务人员参与系统维护、设备维护等。任何第三方服务人员进入系统前必须事先按照要求进行背景调查和资质审查，第三方服务人员需在内部可信人员的陪同下才能访问和控制东方中讯CA认证系统。独立签约者将不会被允许访问核心区以及包含敏感信息的区域和系统。

经过相关背景调查的人员按照内部人员执行，未经过相关背景调查的人员需在内部可信人员的全程陪同下进行服务。

5.3.8 培训文档

为了使得业务保持可用性和连续性，东方中讯CA提供给员工必要的文档以让他们能顺利的完成工作，培训文档至少包括：

系统软、硬件的操作说明文档、密码设备的操作说明文档；

CA系统操作说明文档；

东方中讯CA运营管理规范；

系统安全管理规范；

岗位职责；

其他文档材料。

5.4 审计日志程序

东方中讯CA根据本CPS和其他相关管理规范的要求，建立完善的日志和审计系统。实现该系统的目的在于维护一个安全的环境。

5.4.1 记录事件类型

东方中讯CA记录的事件与CA、RA运行系统相关。其主要记录形式可以是手写、打印稿或者电子文档等形式，但其必须包含事件日期、事件的内容、事件的发生时间段、时间相关的实体等。包括（但不限于）：

●CA密钥生命周期管理的事件，CA和订户的密钥生命周期事件，其他安全相关事件：

●CA密钥的生成、存储、恢复、归档和销毁等；

●认证系统各类服务系统密钥对的生成、内置、变更等操作的日志记录；

●CRL的操作记录；

●进入机房各区域内的记录表格、安全令牌进出记录、机房值班日志、系统维护日志、监控录像等；

●系统软硬件设备的上线、更换、下线等记录；

●认证机构、注册机构的受理点之间的协议、规范和相关工作记录；

●东方中讯CA还要记录与系统不直接相关联的时间，例如：物理通道参观记录、人事变动；

●可信人员管理记录，包括网络权限的账号申请记录，系统权限的申请、变更、创建申请记录，人员情况变化；

●系统安全事件，包括：访问CA系统的活动记录，试图通过非法途径（物理和逻辑上）访问CA系统、敏感信息或文件、安全设备或其他信息系统的日志记录，安全、敏感文件或记录的读、写或删除，系统；

●防火墙和入侵检测系统等其他网络设备记录的安全事件。

5.4.2 处理和归档日志的周期

对于CA密钥和注册用户密钥生命周期内的事件日志，每半年进行一次内部检查、审计。对于系统安全事件和系统操作事件日志，每周进行一次检查。对于物理设施的访问日志，每月进行一次检查、处理。

5.4.3 审计日志的保存期

根据东方中讯CA运营管理规范和相关标准，审计日志系统保存期为一年，归档保存期至少为七年。

5.4.4 审计日志保护

东方中讯CA严格执行物理和逻辑访问控制，确保只有东方中讯CA的可信人员在相关授权下才能接近这些审查记录。这些记录处于严格的保护状态，并按序号进行保存。

5.4.5 审计日志备份程序

东方中讯CA采用先进专业的安全厂商的备份系统，可靠稳定的存储介质按照东方中讯CA备份标准和程序进行备份。根据记录的性质和要求，有实时、每天、每周、每月和每年多种备份周期，在线和离线多种备份形式。

5.4.6 审计收集系统

东方中讯CA采用自动和手工相结合的方式进行备份。自动审计数据生成和记录了应用程序、网络和操作系统数据。手动生成的审核数据记录由授权的东方中讯CA可信人员执行。

5.4.7 对导致事件实体的通告

当有关认证系统的运行出现影响安全控制措施的时候，必须通知安全管理人员，采取有关应对措施。当安全管理人员不在场时，应当立即执行“应急预案”中的相关措施，并通知安全管理员。在东方中讯CA进行审查中发现的攻击行为，将有安全管理员在法律许可范围内追溯攻击者，对于造成重大损失的攻击行为，东方中讯CA将保留采取相应措施的权利，包括上报国家安

全部门，递交司法部门等。

5.4.8 脆弱性评估

东方中讯CA每年都会进行至少一次脆弱性评估，以掌握审计系统的详细信息，定期对审计系统可能存在的漏洞以及审计系统运行可能对CA整体系统的影响做出分析评估。

5.5 记录归档

5.5.1 归档记录类型

东方中讯CA对由信息系统产生的记录进行归档，包括（但不限于）：

审计日志;

证书归档（主要是对已经过期的证书进行归档）；

门禁视频监控记录归档;

东方中讯CA数据库数据归档;

CA运营相关材料归档（如：证书生命周期中的各种申请、审核材料）。

5.5.2 归档记录保存期

所有东方中讯CA的归档记录一旦被归档将被保存不少于7年，对于特殊归档记录文件，东方中讯CA将有权自行决定信息的定期保存期限。

5.5.3 归档的保护

归档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的可信人员按照特定的安全方式才能处理各种归档文件。要求归档环境要防水、防火、防潮、防盗。

5.5.4 档案的备份

所有存档的文件和数据，通常保存在东方中讯CA的主要存储场所。确有必要的，还将在异地保存其备份。存档的数据库一般采用物理或逻辑隔离的方式，与外界不发生信息交互。只有授权的可信人员才能在监督的情况下，

对存档进行读取操作。东方中讯CA在安全机制上保证禁止对档案及其备份进行删除、修改和操作。

对于需要持续保存、归档的文件和数据，将根据东方中讯CA的备份策略进行归档和整理。

当认证系统因为异常情况导致无法正常运行时，按照东方中讯CA的恢复策略，利用这些归档保存的数据进行系统的恢复。

5.5.5 记录的时间标识

所有东方中讯CA认证系统的全部存档内容，都有时间标识。

5.5.6 档案收集系统

东方中讯CA的归档收集分为人工和自动方式。只有被授权的可信人员才可以进行归档收集。

5.5.7 获得和检验归档信息的程序

只有东方中讯CA的授权的可信人员能够访问归档记录，东方中讯CA将会定期组织人员验证归档信息的完整性。

5.6 CA密钥更替

东方中讯CA采用系统CA密钥更新功能进行CA的密钥更新。当完成一个CA密钥更新操作时，需要签发下面三个证书：

用新的私钥对旧的公钥签名的证书：这是一个自签发的CA证书，它是使用新CA签名私钥对旧的CA验证（verification）公钥签名的证书。这使得用CA新签名密钥签发的证书用户能够验证由旧CA签名密钥签发的证书。该证书的合法期限从旧的公/私钥对产生时起至旧的共钥密钥对作废为止。

用旧的私钥对新的公钥签名的证书：这是一个自签发的CA证书，它是使用旧CA签名私钥对新的CA验证（verification）公钥签名的证书。这使得用旧CA签名私钥签发的证书用户能够验证由新CA签名密钥签发的证书。该证书的合法期限从新的公/私钥对产生时起至所有的CA用户都安全获得了新的CA

公钥为止（至少到旧的公钥作废为止）。

用新的私钥对新的公钥签名的证书：这是一个自签发的CA证书，它是使用新CA签名私钥对新的CA验证（verification）公钥签名的证书。这使得用新CA签名私钥创建的用户能够相互验证对方的证书而无需验证内部交叉认证链，该交叉认证链由一个旧的自签发CA证书作为链的起始。该证书的合法期限从新的公/私钥对产生时起至CA再次更新公/私钥对证书制定的作废期为止。

5.7 损害和灾难恢复

东方中讯CA制订了可靠完善的灾难恢复计划与应急预案，使系统能够在最短时间内重新恢复认证系统的运行，东方中讯CA要求在突发情况下至少采取下列步骤恢复安全环境：

所有东方中讯CA口令由首席安全官员、安全官员、主用户进行变更；

根据灾难的性质，部分或全部证书需要撤销或之后重新认证；

如果目录无法使用或者目录有不纯的嫌疑，目录数据，加密证书和CRL需要进行恢复及从备份中恢复。一旦目录管理员从备份中恢复了目录，东方中讯CA运营安全管理委员会可从东方中讯CA权威控制系统的目录恢复东方中讯CA数据；以CA数据库数据为标准恢复目录服务；

及时访问安全现场尽可能合理地恢复操作；

如果需要恢复首席安全官员的配置文件，应由主用户执行恢复；

如果需要恢复PKI管理员的配置文件，则由另外一名PKI管理员或首席安全官员对其进行恢复。

5.7.1 资料或数据损坏

东方中讯CA的私钥由证书服务器密码机生成，CA中心的私钥生成后，能够通过特定的密钥存储卡安全地备份到另一台证书服务器密码机中，如果其中一台证书服务器密码机中的密钥被破坏，可以从另外一台证书服务器密码机进行恢复。证书和用户资料可通过系统所制定的备份策略和备份方式，定

期地将这些信息备份到外部介质上（CD或磁带等），这些保存了备份信息的外部介质存放在中心机房之外的安全地点，当发生灾难性故障时，能够很快地安全恢复证书以及用户资料，使系统尽快恢复运行。

5.7.2 实体私钥泄露的处理

东方中讯CA制订了严格的安全策略，以此来确保密钥的安全。当东方中讯CA私钥出现泄露或疑似泄露时，在场的工作人员应:

立即向东方中讯CA进行汇报，并通知安全官员，生成新的密钥对和证书请求，向东方中讯CA申请签发新的证书；

通过网站和其他公共媒体紧急通知所有东方中讯CA证书用户更新证书；立即撤销所有由该子CA签发的证书，更新CRL和OCSP信息，供注册用户和依赖方查询；

新的子CA证书签发之后，按照本CPS关于证书签发的规定，重新签发注册用户证书；

新证书签发以后，将会立即通过东方中讯信息库、LDAP服务器、HTTP等方式进行对外发布；

安全官员或安全管理员对事件进行详细调查，并公布调查结果，按照相关规定处理善后。

5.7.3 灾难后的业务连续性能力

东方中讯CA由专业的内部工作人员制订了详细的应急响应策略，避免由于突发灾难事故造成认证业务停顿。东方中讯CA建立了设施完善的备份机房，确保了在短时间内无法恢复业务时，能第一时间启用备份系统，继续提供证书服务。

异地灾难备份中心将根据需要每年至少进行一次灾难恢复计划的训练和测试，并根据实际情况及时更新应急响应策略。从而保证在出现异常灾难时，东方中讯CA系统能在短时间内恢复系统运行和服务提供，将损失降到最小。

5.8 CA机构或RA机构终止

如果东方中讯CA因计划而终止运营时，将会按照相关法律规定，向主管部门报告，并按照法定程序终止提供证书签发服务。

5.8.1 终止过程

CA和RA 终止事件可能由于密钥受损或非密钥受损原因。密钥受损原因可能包括CA根密钥丢失。非密钥受损原因可能与商业问题有关。

在CA 终止期间，必须：

准备 CA 终止状态；

通知 CA 停止实体(E-mail和WEB)；

证书注销；

处理存档文件记录；

停止认证中心；

存档主目录服务器；

关闭主目录服务器；

关闭从目录服务器；

处理加密密钥；

处理/存储敏感信息；

清除CA 硬驱动。

由于密钥受损和非密钥受损原因而终止 CA，几乎要完成相同的操作，唯一的不同在CA终止发送E-mail通知的时间限制上。由于密钥受损原因终止CA要求：终止过程在E-mail通知过程中。因为在这种情况下终止动作应当尽快完成。否则，CA 终止过程在E-mail通知所有用户过程后完成，并采取适当的步骤减轻CA终止影响。

5.8.2 终止通知

当东方中讯CA授权的证书服务机构因故终止服务时，东方中讯将会经过

主管部门和法律审批准备后发布CA终止生命。

东方中讯CA运营安全管理委员会是唯一有权发布CA 终止声明的人。

东方中讯CA将会在终止声明发布后，按照本CPS和有关法律法规处理其他事项。

6 认证系统技术安全控制

本章阐述东方中讯CA为保护其密钥和激活数据（如PIN码、口令字或手持密钥共享）而采取的安全措施。说明对东方中讯CA证书库、订户和其他参与者进行的限制，以保护他们的私钥、私钥激活数据和关键安全参数。描述东方中讯CA使用的其他技术安全控制手段，用以安全地实现密钥生成，用户鉴别，证书注册，证书撤销，审计和归档等功能。技术控制包含生命周期安全控制（包括软件开发环境安全，可信的软件开发方法论）和操作安全控制。

6.1 密钥对的产生和安装

6.1.1 密钥对的生成

根CA密钥：

CA系统根密钥的生成由通过国家密码管理局商用密码管理委员会鉴定的证书服务器密码机完成。当多数管理员在场并通过身份认证后，启动证书服务器密码机的管理程序进行证书服务器密码机的密钥对的初始化生成。

用户加密密钥：

加密密钥对是由中华人民共和国国家密码管理委员会办公室（以下简称国密办）许可的、证书服务加密机生成的，由重庆市国家密码管理委员会办公室所属的KMC控制管理；。

用户签名密钥：

在客户端生成（如：WEB应用服务器、密码硬件设备或应用软件等）。

东方中讯CA设置密钥管理员及若干名接受过相关培训的可信雇员，在密

钥生成室按照东方中讯CA的密钥管理策略中规定的密钥生成规程进行产生。东方中讯密钥生成规程规定了 CA 密钥产生的流程控制及参加人员。东方中讯CA的密钥对使用符合国家密码主管部门的要求的密码硬件产生。

对于个人证书和机构证书，订户使用国家密码管理部门许可的密码模块（如USB Key，智能卡）生成密钥对。

对于服务器证书，订户使用服务器程序使用的密码模块提供的密钥生成功能生成密钥对。

对于东方中讯运行系统将使用专门的程序软件在国家密码管理部门许可的密码模块（如加密卡或加密机）中生成密钥对。

对于管理员证书，私钥使用国家密码管理部门许可的客户端密码模块（如USB Key）产生。

东方中讯各类 CA 证书密钥对由东方中讯CA在其安全运营场地内部由东方中讯自身持有和保存，东方中讯CA在备份机房系统密钥的传输过程中将通过安全的途径将保存有证书私钥的密码硬件传送到备份机房，并确保在传送过程中私钥不会被非授权的使用、被泄露或被损坏。

6.1.2 私钥传送给订户

签名私钥在客户端生成，由订户保管。加密私钥在KMC中心由加密机生成，只保存于KMC中心内，通过国密办规定的传输加密算法安全发送给订户（东方中讯CA加密证书必须使用支持SSF33算法的证书存储介质，在东方中讯CA的RA机构完成签发）。

对于东方中讯签发的其他最终用户证书，通常的情况下密钥对在订户本地的密码模块（如 USB Key）中产生，私钥由最终用户保存在本地密码模块中，不存在私钥的传送问题。但在一些特别的安排下，东方中讯CA可能会代最终用户在约定的密码硬件中（如 USB Key）产生证书密钥对，且私钥保存在密码硬件中。在这种情形下，东方中讯CA将通过安全的途径将保存有证书私钥的密码硬件传送到最终用户手中，并确保在传送过程中私钥不会被非授

权的使用、被泄露或被损坏。

6.1.3 公钥传送给证书签发机构

订户通过 PKCS#10 格式的证书签名请求信息文件，以电子的方式将公钥提 东方中讯CA，这些请求通过网络传送时使用安全套接层协议（SSL）和其他安全协议。

6.1.4 电子认证服务机构公钥提供给潜在的依赖方

东方中讯CA将根证书发布于公司网站http://www.ezca.org上，供用户或潜在依赖方下载。

6.1.5 密钥长度

东方中讯CA使用的非对称密钥体系的密钥长度为RSA 1024位、RSA2048位以及SM2 256位。

6.1.6 公钥参数的生成和质量检查

公钥参数由符合国家密码管理局要求的硬件产生。

6.1.7 密钥使用目的

在数字证书“密钥用途”域中定义，与证书用途有联系。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

东方中讯CA的CA系统模块采用通过国家密码管理局商用密码管理委员会鉴定的证书服务器密码机，证书服务器密码机采用黑盒设计方案，外界（包括Authority）无法取得其私钥，加密/解密只能通过证书服务器密码机接口进行。此外密码机具有较高的抗电磁干扰、抗电源冲击能力，这样确保了系统私钥的安全性。

客户密码模块主要是密钥生成和存储环境。

东方中讯CA使用国家密码管理局认可、批准的硬件密码模块生成CA密钥对，并存储CA私钥。

东方中讯CA制定有专门密码管理策略，在从运输 、初始化、离线存放、在线使用到销毁的整个密码设备生命周期内，对密码模块进行管理和控制。CA 密码存储模块离线存放

在CA密钥离线存放核心区保险柜中，CA密码模块在线放置在屏蔽机房内机柜中。

东方中讯CA运行使用的密码模块的标准及控制同 CA密钥密码模块。

最终用户证书使用国家密码管理部门认可的密码模块，并妥善保护、保管其密码模块，防止其失窃、丢失、损坏及被非授权的使用。

6.2.2 私钥多人控制

东方中讯CA只允许多人同时在场的情况下才可以访问存储在加密机中的密钥，且至少有一名公司高层领导在场，采用M选N控制方式，M为5、N为3。

6.2.3 私钥托管

加密密钥可根据客户需求由KMC进行托管，签名密钥为了保证其不可否认性，由客户自行保管。

东方中讯CA所有CA系统（包括根CA和运营CA）的私钥均未在其他地方托管。

东方中讯CA订户加密密钥根据国家密码管理局的要求由KMC对订户加密证书的私钥进行托管。

6.2.4 私钥备份

东方中讯CA的CA系统根密钥生成后由证书服务器密码机保存。根密钥对初始化生成后东方中讯CA的密钥管理员会对证书服务器密码机中各种密钥进行备份，一旦加密机中的密钥对遭到破坏可以及时得到恢复。

对于最终订户证书，东方中讯CA提供的存储介质一般不具有私钥备份功能，建议订户妥善保管存储介质和介质保护口令。

6.2.5 私钥归档

当东方中讯CA的CA密钥对超过使用期后，这些密钥对将归档保存至少5

年。归档密钥对保存在 CPS 6.2.1所述的硬件密码模块中，并且由东方中讯CA的密钥管理策略和流程阻止归档密钥对返回到生产系统中。对归档私钥到了归档保存期后，东方中讯CA将按原厂要求进行销毁。

东方中讯CA不对最终订户证书的私钥进行归档。

6.2.6 私钥导入、导出密码模块

证书服务器密码机可将非对称密钥对导入、导出，用于密钥对的备份、恢复。在密钥导入、导出时，私钥是加密的。

用户密钥导入、导出根据密钥存储方式的不同，有不同的特点。

东方中讯CA的 CA 密钥对（根CA、运营CA）在硬件密码模块上生成，保存和使用。此外，为了常规恢复和灾难恢复，东方中讯CA对 CA的密钥对进行复制。当CA 密钥对从一个硬件密码模块复制到另一个硬件密码模块上时，被复制的密钥对以加密的形式在模块之间传送，并且在传递前要进行模块间的相互身份鉴别。另外东方中讯CA还有严格的密钥管理流程对 CA 密钥对复制进行控制。以上这些手段有效防止了 CA 私钥的丢失、失窃、修改、非授权的泄露、非授权的使用等。

东方中讯CA生产系统的私钥需要导出、导入，则必须由东方中讯CA的可信人员进行相关的操作。在进行导出、导入时，将确保导出的证书私钥不以明文形式存在（如具有足够强度的口令保护），并在完成导出、导入后立即、彻底地销毁导出的私钥。

东方中讯CA不支持用户密钥的导入、导出。

6.2.7 私钥在密码模块中的存储

东方中讯CA 的CA私钥（根CA、运营CA）以加密形式存放在符合国家密码管理局要求的硬件密码模块中，且私钥的使用也在硬件密码模块中进行。

对于个人证书和机构证书，最终用户须将私钥保存在其可控制、国家密码管理局认可的密码模块中（如 USB Key），私钥在密码模块中须以加密形式存储，且私钥的使用受口令或指纹等安全措施保护。最终用户须采取必要

的措施防止其他人员对私钥的非授权访问、获取和使用。

对于服务器证书，最终用户需将私钥保存在国家密码管理局认可的密码模块中，且存放私钥的密码模块必须在其可控制的范围内，并要采取相应的安全手段防止对私钥的非授权访问、获取和使用。

6.2.8 私钥激活

最终用户的证书私钥保存在密码模块中，需输入口令（或PIN码）或提取指纹等密钥保护信息（激活数据）后才被激活，才能够被使用。

东方中讯CA的根CA、运营CA私钥存放在硬件密码模块中，并且其激活数据按M选N的方式（M=5、N=3）进行分割。当需要使用私钥时（在线或离线），需要东方中讯CA 5个密钥分管员中的至少3人和密钥管理员同时到场，由3个密钥分管员输入各自分管的密钥口令（激活数据）后才能激活。

6.2.9 解除私钥激活状态

解除私钥激活可通过关闭密码模块设备、停止私钥服务应用、移开私钥环境等方式实现。

6.2.10 销毁私钥

根据私钥的不同存储环境采用不同销毁方法。

对于东方中讯CA的最终用户证书私钥，若不再使用，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。若私钥撤销、到期作废后，还需要用于信息解密的，最终用户应该妥善保存，以便于解开加密信息。若私钥无需再保存，则将通过私钥的删除、系统或密码模块的初始化来销毁。

东方中讯CA的CA 私钥（根CA和运营CA）生命周期结束后，将继续保存在一个备份硬件密码模块中，并进行归档，其他的 CA 私钥备份被安全销毁。归档的 CA 私钥在其归档期限结束后，需在多名可信人员参与的情况下安全销毁。CA 私钥的销毁将确保 CA 私钥从硬件密码模块中彻底删除，不留有任何残余信息。

由国家密码管理部门负责。

6.3 密钥对管理的其他方面

6.3.1公钥归档

主要对到期证书进行归档。

6.3.2证书操作期和密钥对的使用期限

东方中讯CA颁发给用户的数字证书有效期与密钥有效期一致，根据用户要求设定有效期，其有效期不能超过根证书有效期。

公钥和私钥的使用期限与证书的有效期相关但却有所不同。

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，直到私钥受到损害或密钥对存在被破解的风险，如加密算法被破解。当私钥受到损害或密钥对存在被破解的风险后，签名证书的公钥在技术上仍然可以用于验证数字签名，但这种验证在法律上不一定是有效的。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公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加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

另外无论是订户证书还是 CA证书，有效期到了后，在保证安全的情况下，允许证书进行更新而密钥对不变。但是密钥对不能无限期使用。对于不同的证书，密钥对通过证书更新允许的最长使用期限如下：

对于RSA2048位CA密钥对的最长允许使用年限是10年；

对于SM2 256位CA密钥对的最长允许使用年限是20年；

对于RSA2048位用户密钥对的最长允许使用年限是3年；

对于SM2 256位用户密钥对的最长允许使用年限是3年。

6.4 激活数据

激活数据指使用私钥的保护密码数据，由用户设定并妥善保管。其根据不同的私钥存储介质有不同的设定要求。

东方中讯 CA 私钥的激活数据由硬件加密模块内部产生，并分割保存在5 个 IC 卡中，需通过专门的读卡设备和软件读取。东方中讯CA 私钥激活数据的产生过程，按东方中讯CA密钥生成规程参考指南中的规定进行。所有密钥分割的创建和分发有相应的记录，包括产生时间、持有人等信息。

6.5 计算机安全控制

6.5.1计算机安全控制要求

在安全方面：首先在安装的时候把驱动器格式化为NTFS格式，为了防范病毒与黑客对操作系统进行破坏，在所有的机器上都装上杀毒软件，关闭网上邻居共享与所有除与数据库和CA系统应用软件无关的端口与服务功能，时时注意操作系统服务商提供的补丁程序，及时修正操作系统的漏洞。另外定期升级防火墙与杀毒软件，以便杀死新的或是变种的病毒程序，防范病毒与黑客攻击是当前最重要的任务，以便达到安全防范的目的。

在备份与修复方面：为了防止系统出现致命性的损坏，系统管理员定期备份操作系统，以便在必要的时候恢复操作系统，首先在所有软件与设置都做好准备之后，备份系统注册表；其次利用系统自带的BACKUP或外部软件对每个驱动器进行数据备份。当操作系统出现损坏性错误时进行覆盖式修复达到最快的时间内使系统正常运行。

在日常维护方面：定期对系统日志进行分析处理，对不正常的日志显示作特别的事件处理。

6.6.2计算机安全评估

东方中讯CA系统安全等级采用TCSEC（受信计算机系统评测标准）安全标准。

6.6 生命周期技术控制

东方中讯CA应用软件的开发严格按照软件开发和管理的相关规范和标准进行开发和生命周期管理。

6.7 网络安全控制

网络安全控制的目标是保证网络安全可靠的运行，从网络拓扑结构、网络安全区域的划分、防火墙系统的设置等各个方面的设计中防范来自INTERNET的攻击并加强对内部的安全管理。

整个网络划分为四个区：公共区、DMZ、操作区和安全区。各安全层次之间采用不同类型的国内的优秀的防火墙产品。每个安全层次在一个子网上，安全策略不尽相同，使得网络系统具备很强的防范能力。

在采用多层防火墙技术增加系统的安全性的同时，我们采用了国内著名厂家的入侵监测系统。通过入侵监测可以从多方面对网络系统进行监测和分析，能够及时发现入侵者并及时报警，同时还能够采取一定的补救措施。

6.8 时间戳

数字时间戳（DTS：Digital Time Stamp）是对时间信息的电子签名，主要用于实现确定在某一时间某个文件确实存在和确定多个文件在时间上的逻辑关系功能。

东方中讯CA提供数字时间戳服务，时间源来源于国家授时中心提供的标准时间，精确度为秒，能够通过HTTP协议申请严格遵循国际标准（RFC3161）和PKCS#7两种时间戳协议的时间戳。时间戳密钥采用通过国家鉴定的密码设备产生和保存，密钥长度不小于1024具有很高的安全性能。

7 证书、证书撤销列表和在线证书状态协议

该章说明证书、证书撤销列表和在线证书状态协议的格式，包括描述、版本号和扩展项的使用。

7.1 证书

7.1.1 版本号

东方中讯CA数字证书格式符合X.509 v3标准。

7.1.2 证书扩展项

CA 的公钥标识（Authority Key Identifier）

公钥标识（SET 未使用）（Key Identifier）

含义：签发证书者证书的签发者的甄别名

证书的序列号Certificate Serial N

含义：CA 签名证书所用的密钥对的唯一标识

用户的公钥标识（SubjectKeyIdentifier）。

含义：用来标识与证书中公钥相关的特定密钥进行解密。

证书中的公钥用途（Key Usage）

含义：用来指定公钥用途。

用户的私钥有效期（Private Key Usage Period）

起始日期（Note Before）

终止日期（Note After）

含义：用来指定用户签名私钥的起始日期和终止日期。

CA 承认的证书政策列表（Certificate Policies）

含义：用来指定用户证书所适用的政策，证书政策可由对象标识符表示。

用户的代用名（Substitutional Name）

含义：用来指定用户的代用名。

CA 的代用名（Issuer AltName）

含义：用来指定 CA 的代用名。

基本制约（Basic Constraints）

含义：用来表明证书用户是最终用户还是 CA。

CRL 数据定义版本（Version）

含义：显示 CRL 的版本号。

CRL 的签发者（Issuer）

含义：指明签发 CRL 的 CA 的甄别名。

CRL 发布时间（this Update）

预计下一个 CRL 更新时间（Next Update）

撤销证书信息目录（Revoked Certificates）

CRL 扩展（CRL Extension）

CA 的公钥标识（Authority Key Identifier）

CRL 号（CRL Number）

7.1.3 密码算法对象标识符

常用密码算法标识

摘要算法：SHA1、SHA256、SM3

对称算法：DES、3DES、CAST、RC2、RC4、RC5、IDEA、SDBI

非对称算法：RSA、SM2

7.1.4 名称形式

通常采用X.500 甄别名格式。

7.1.5 名称限制

根据X.500 甄别名格式规范进行限制。

7.1.6 证书策略对象标识符

证书策略对象标识符标识了电子认证机构制定的证书策略。经国际标准化组织的审定获得其OID标识。

7.1.7 策略约束扩展项的使用

东方中讯CA未使用此扩展项。

7.1.8 关键证书策略扩展项的处理规则

东方中讯CA未使用此扩展项。

7.2 证书撤销列表CRL

7.2.1 版本号

东方中讯CA签发的CRL符合X.500标准，采用X.509 V2格式。

7.2.2 CRL和CRL扩展项

CRL基本项：版本（Version）

含义：显示CRL版本号。

签名（Signature）

含义：CA对签发的CRL的签名。

算法标识（Algorithm Identifier）

含义：定义签名CRL所使用的算法。

CRL签发者（Issuer）

含义：签发CRL的CA的甄别名。

CRL发布时间（this Update）

下次更新时间（next update）

撤销证书信息目录（revoked certificates）

CRL扩展：

CA公钥标识符

CRL号

7.3 在线证书状态协议OCSP

7.3.1 版本号

OCSP版本1 （参见RFC 2560）

7.3.2 OCSP扩展

暂无

8 一致性审计和其他评估

8.1 评估的频率和情形

东方中讯CA审计评估分为内部审计评估和第三方审计评估。

根据国家相关主管部门要求进行相关评估，评估频率分为运营前评估、系统改造或升级后评估、年度评估等。

8.2 评估者的资质

东方中讯CA第三方评估者所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：

必须是经许可的、有营业执照的、具有计算机安全专门技术知识的审计人员或审计评估机构，且在业界享有良好的声誉；了解计算机信息安全体系、通信网络安全要求、PKI技术、标准和操作；具备检查系统运行性能的专业技术和工具。

8.3 评估者与被评估者关系

东方中讯CA第三方审计评估者必须是一个独立于东方中讯CA的实体，与东方中讯CA无任何业务、经济以及其他利益联系。

东方中讯CA的管理员和与之相对应的审计员不能由同一人来承担。

8.4 评估内容

第三方审计：

东方中讯CA支持的证书认证操作规程是否完全与本电子认证业务规则表达一致，包括东方中讯CA的技术、手续和员工的相关管理政策和业务声明；

东方中讯CA是否实施了相关技术、管理、相关政策和业务声明；

审计者或东方中讯CA认为有必要审计的其他方面。

内部审计：

东方中讯CA每个季度对东方中讯CA各个管理模块进行审计，并配有专门的审计员进行审计工作。

8.5 对问题与不足采取的措施

根据问题的情况，东方中讯CA工作人员将与东方中讯CA运营安全管理委员会联系，并尽快提出解决方案。经公司领导审批后及时进行修正，并提请审计人员或审计机构检查评估。

8.6 评估结果的传达与发布

第三方评估则由评估者直接通知被评估者结果信息。

内部评估则由审计人员通知相应管理部门。

9 法律责任和其他业务条款

本章涵盖了一般性的业务和法律问题。在业务条款中说明不同服务的费用问题，和各参与方为了保证资源维持运营，针对参与方的诉讼和审判提供支付所需承担的财务责任。法律责任条款则与通用的技术协定标题相近，涉及保密、隐私、知识产权、担保及免责等内容。

9.1 费用

9.1.1 证书签发或更新费用

用户使用东方中讯CA电子认证服务，需要向东方中讯CA缴纳证书服务费用，东方中讯CA证书服务费用经过重庆市物价局审批，标准费用如下表所示，具体费用参见东方中讯CA证书服务收费项目和基准收费标准表。

费用 证书类别	介质费	年服务费
个人证书	无	无
机构证书	280	200
设备证书	无	1000

9.1.2 证书查询费用

目前暂不收取。但今后如对证书查询收取任何费用，公司将在网站予以公布。

9.1.3 证书撤销和状态的查询费用

目前暂不收取。但今后如对证书撤销和状态的查询收取任何费用，公司将在网站予以公布。

9.1.4 其他服务费用

东方中讯CA保留收取其他服务费用的权利。

9.1.5 退款策略

除非东方中讯CA违背了本CPS所规定的责任，订户可以要求退款。否则，东方中讯CA对订户所收取的费用均不退还。

订户应该提供符合东方中讯CA要求的完整、真实、准确的个人（机构）信息，否则东方中讯CA对此造成的损失和后果不承担任何责任。

9.2 财务责任

9.2.1 保险范围

暂无。

9.2.2 其他资产

暂无。

9.2.3 对最终实体的保险和担保范围

暂无相应险种。

9.3 业务信息保密

9.3.1 保密信息范围

东方中讯CA用户的数字签名及解密密钥，并且CA和RA均无权访问这些密钥；

审计记录包括：本地日志、服务器日志、归档日志的信息，这些信息被东方中讯CA视为保密信息，只有审计员和安全官员可以查看。除法律要求，

不可在公司外部发布；

除了公钥证书、ARL、CRL、和本中心对外发布的CPS的信息，其他由CA和RA保存的个人和公司信息应视为保密，除法律要求，不可公布。

除非法律或本规则特别规定，东方中讯CA没有义务公布或透露证书持有者证书以外的信息。

9.3.2 不属于保密的信息

以下信息可视为不保密信息：

由东方中讯CA发行的证书和CRL中的信息；

经东方中讯CA许可，只有东方中讯CA用户方使用，在东方中讯CA网站公开发布的信息；

其他东方中讯CA信息的保密性取决于特殊的数据项和申请；

在目录服务器中公布证书的相关信息，供网上查询；

法律法规规定的应予公布的其它信息。

9.3.3 保护机密信息的责任

电子认证参与各方均有义务承担保密义务，但任何一方有对方授权公布或透露的保密信息除外。电子认证参与各方不得将电子认证服务相关保密信息用于除电子认证以外的其他用途。不得对双方提供的被认为是保密信息的内容进行非法获取，如：程序跟踪、反汇编、加密信息破解等。

当法律法规要求，司法机构、仲裁机构或行政机构执法人员需要东方中讯CA提供下列的证书使用者的相关信息时，东方中讯CA不被视为违反了其保密义务，且不承担任何保密责任，并不承担任何由此导致的损失：

证书使用者的基本信息；

证书使用者用个人加密密钥加密的信息；

东方中讯CA将按照法律要求向执法人员提供相关信息。

当保密信息的所有权人要求东方中讯CA提供保密信息，所有权人应该向

东方中讯CA 提供授权公开保密信息的委托书。

9.4 个人隐私保密性

9.4.1 隐私保密方案

东方中讯CA将依法保护订户的个人隐私。任何人同意接受东方中讯CA中心的任何服务，则其自动认可本CPS规则关于隐私保密方案。

9.4.2 作为隐私处理的信息

与证书持有者证书公钥配对的私钥是保密的，证书持有者应妥善保管，不能泄露给他人。如果证书持有者擅自泄露私钥，则由此引起的后果由证书持有者自负。

9.4.3 不被视作隐私的信息

证书中公开的个人信息以及CRL中的证书撤销信息。

9.4.4 保护隐私的责任

电子认证参与各方都有保护隐私的责任。

9.4.5 使用隐私信息的通知与同意

除法律法规要求使用隐私信息，否则必须经授权后方可使用。但东方中讯CA将隐私信息用于订户身份识别、管理和服务的除外。

9.4.6 依法律和行政程序的信息披露

当法律法规、司法机构、仲裁机构或行政机构执法人员要求东方中讯CA对隐私信息进行披露时，东方中讯CA可以披露，且不承担任何法律责任。

9.4.7 其他信息披露情形

在不违反相关法律法规的情形下披露可公开信息。

9.5 知识产权

东方中讯CA享有并保留对证书以及东方中讯CA提供的全部软件的独一无二的一切知识产权，包括但不限于：

著作权、所有权、名称权、利益分享权、商标权技术秘密、专利等）；

东方中讯CA对数字证书系统软件具有所有权、名称权、利益分享权；

东方中讯CA有权决定采用何种软件系统；

东方中讯CA网站上公布的一切信息均为东方中讯CA财产，未经东方中讯CA书面允许，他人不能转载用于商业行为；

东方中讯CA发行的证书和CRL均为东方中讯CA的财产，东方中讯CA享有其完整知识产权及财产权；

对外运营策略和规范为东方中讯CA所有；

用来表示目录中东方中讯CA域中的实体的甄别名（DN）以及该域中颁发给终端实体的证书，均为东方中讯CA的财产。

9.6 陈述与担保

东方中讯CA订户以及东方中讯CA均承诺接受本电子认证业务规则的约束。在东方中讯CA与包括订户在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本电子认证业务规则的规定执行；对协议中与本电子认证业务规则相冲突部分，按双方协议中约定的内容执行。

9.6.1 东方中讯CA（含授权注册机构）的陈述与保证

承诺建立健全CPS、服务规则、以及其它制度或规则；

严格遵守本规则，按照本规则约定的内容及程序办理认证事务；

严格按照法律规定从事CA认证工作，并依法承担相应的法律责任；

承诺并保证经验证后的信息均系真实准确的，但订户提供的虚假信息造成验证后的信息虚假除外。

9.6.2 订户陈述与保证

在申请并经核准后颁发证书至证书有效期间，订户承诺并保证：

在证书申请上所列明的信息及声明均是完整、精确、真实的，不存在任

何虚假陈述或表示，对提供的资料的真实性负责，并愿意接受EZCA的检查与核实，愿意无条件承担任何因虚假信息及或资料给东方中讯CA或第三人造成的任何经济损失或名誉损失或任何其它法律责任；

保证遵守本规则所约定的条款，并愿意遵守申请、使用规则；

保证合法地使用证书或证书包含的信息，不得用于非法目的；

一经接受证书，表示已经熟知本规则及有关协议的内容；

一经接受证书，表示愿意按照本规则承担可能因违反本规则应承担的法律责任；

一经接受证书，表示愿意遵守东方中讯CA制定或修改的规则、规范或声明、更新、升级等。

9.6.3 依赖方陈述与保证

信赖证书前已经熟知并充分理解本规则的所有条款；

在使用证书前已经对证书进行了合理必要的审核与验证，包括但不限于对证书的有效性等；

对证书的接受表明愿意遵守并接受本规则的所有规定，并愿意遵守东方中讯CA制定的规则、规定或声明或升级、更新等。

9.6.4 其它各方的陈述与保证

同9.6.3的规定。

9.7 担保免责

东方中讯CA及其授权注册机构不承担上述有关东方中讯CA及其授权注册机构赔偿责任条款以外的其他任何形式的责任，包括但不限于：

不可抗力；

非东方中讯CA的原因而造成的设备故障、线路中断导致签发数字证书错误、延误或中断或无法签发；

订户提供虚假信息；

数字证书订户将信息用于其它用途等。

9.8 有限责任

东方中讯CA系依据我国《公司法》等法律法规成立的有限责任公司，其以其注册资本为限，承担有限责任。

9.9 赔偿

9.9.1 赔偿责任范围

9.9.1.1东方中讯CA赔偿责任

在证书签发时，如果未按照本CPS的规定进行处理，或者违反法律法规的要求而造成证书订户损失的，东方中讯CA应当承担赔偿责任；

因为操作人员恶意、故意或者疏忽，未按照本CPS的规定办理证书的签发、撤销等请求，而造成证书订户损失的，东方中讯CA应赔偿订户的损失；

因东方中讯CA的根密钥出现问题，造成订户证书出现问题的，东方中讯CA应赔偿相关的损失；

证书订户或者其它有权提出撤销证书的人提出撤销请求后，到东方中讯CA将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者交易时产生纠纷的，如果东方中讯CA按照本CPS的规范进行了有关操作，东方中讯CA不承担任何损失赔偿责任；

证书订户赔偿的追溯有效期限，按照有关法律法规的要求进行操作；

若数字证书订户未向东方中讯CA缴纳费用，我司不承担任何损失的赔偿责任。

9.9.1.2注册机构（包括分理中心和受理点）责任

注册机构及其操作人员没有妥善保管订户的注册和身份验证的相关隐私信息，而造成订户信息泄露、被冒用、篡改或者任意使用导致产生损失的，

注册机构应负担损失赔偿责任；

如果因为操作人员恶意、故意或者疏忽，未按照本CPS的规定办理证书的服务注册，或者违反法律法规而造成证书订户损失的，注册机构应该赔偿用户的直接损失，以及其他随之产生的附带损失和相关补偿；

因为注册机构的原因造成系统或软件错误，未能在本CPS规定的时间内，将订户的证书申请、撤销、更新等请求发给东方中讯CA，而导致订户或者依赖方损失的，注册机构应负担所有的损害赔偿责任；

该类赔偿的追溯有效期限，按照有关法律法规的要求进行操作。

9.9.1.3订户责任

订户申请注册证书时，因故意、过失或者恶意提供不真实资料，导致造成东方中讯CA及其授权的证书服务机构或者第三方遭受损害的；

订户因故意或者过失造成其私钥泄露、遗失，明知私钥已泄露、遗失而没有告知东方中讯CA及其授权的证书服务机构，以及不当交付他人使用造成东方中讯CA及其授权的证书服务机构、第三方遭受损害的；

订户使用证书或者依赖方信任证书的行为，有违反本CPS及相关操作规范，或者将证书用于非本CPS规定的业务范围的；

用户使用或信赖证书时，未能依照本CPS等规范进行合理审查，导致东方中讯CA及其授权的证书服务机构或第三方遭受损害的；

证书订户或者其他有权提出撤销证书的实体提出撤销请求后，到东方中讯CA将该证书撤销信息予以发布的期间，如果该证书被用以进行非法交易，或者如果东方中讯CA按照本CPS的规范进行了有关操作，进行交易时产生纠纷的；

东方中讯CA与之签署的协议另有赔偿规定的，参照其规定。

9.9.1.4其他

对使用伪造、作废的证书，冒用他人的证书进行非法活动者，或与他人

共谋欺诈或有其他非法行为，东方中讯CA有权依法追究其相关法律责任。

9.9.2赔偿程序

9.9.2.1东方中讯CA及其授权注册机构赔偿流程

东方中讯CA数字证书订户由于东方中讯CA及其授权注册机构过错而造成损失要求赔偿的，由该数字证书订户向东方中讯CA及其授权注册机构提出赔偿要求，东方中讯CA及其授权注册机构将根据此赔偿机制对用户进行赔偿，如果发生赔偿争议，该数字证书订户可向东方中讯CA住所地法院提起诉讼。

9.9.2.2东方中讯CA数字证书订户赔偿流程

东方中讯CA及其授权注册机构或第三人由于东方中讯CA数字证书订户过错而造成损失的，则东方中讯CA及其授权注册机构或第三人将根据相关法律及本CPS条款要求该数字证书订户进行赔偿，如发生赔偿争议，东方中讯CA及其授权注册机构或第三人可向东方中讯CA住所地法院提起诉讼。

9.9.3赔偿限额

东方中讯CA及其授权的发证机构，对所有当事人（包括但不限于订户、申请者、接受者或依赖方）的合计赔偿责任，不可能超过如下所述对这些证书的封顶赔偿金额。

对于有关一张特定证书的所有签名和交易处理的总计，东方中讯CA及其授权的证书服务机构对于任何人（或者其他实体）有关该特定证书的合计赔偿责任应该限制在一个不超出下述数额的范围内（单位：人民币元）：

个人类证书，不超过 1000 元

单位类证书，不超过 30000 元

设备类证书，不超过 50000 元

本条款限制适用于一定形式的损害，包括但不局限于任何人或实体（包括但不限于订户、申请者、接受者或依赖方）由于信任或使用东方中讯CA签

发、管理、使用或撤销的证书或已过期证书而导致的直接的、补偿性的、间接的、特别的、结果的、惩戒性的或以外的损害。

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。每份证书的赔偿均有限额而不考虑签名、交易处理或其他有关的索赔数量。当超过赔偿限额时，除非得到依法判决或仲裁，可用的赔偿限额将首先分配给最早得到索赔解决的一方。东方中讯CA没有责任为每张证书支付高出赔偿限额总和的赔偿，而不管高出赔偿限额总和在索赔提出者之间是如何分配的。若数字证书订户未向东方中讯CA缴纳费用，则东方中讯CA不向订户、申请者、接受者或依赖方承担赔偿责任。

9.10 有效期限与终止

9.10.1 有效期限

东方中讯CA电子认证业务规则从发布之日起生效，其有效期到新版本替换时。文档及协议的有效期将会明确注明。

9.10.2 终止

东方中讯CA电子认证业务规则在新版本替换时终止。文档和协议有效期到期时终止。

9.10.3 效力的终止与保留

协议的某些条款在协议终止后继续有效，如知识产权承认和保密条款。另外，终止可能涉及到各参与方返还保密信息到其拥有者的责任。

9.11 对参与者的个别通告与沟通

电子认证活动中某一参与方与另一参与方进行通信时必须依照《中华人民共和国电子签名法》以使其通信过程在法律上有效。

9.12 修订

9.12.1修订程序

收集修订意见，包括用户意见；

提交到公司各部门进行审议，提出意见；

安全管理委员会整理修改意见，形成修订意见书；

提交到公司领导层审议，并评注意见；

申请召开CPS评议会（公司高层领导参与）进行定稿评议。

9.12.2通知机制和期限

修订后的业务规则在信息产业部备案后将发布到公司网站上，替换旧规则。并在网站上作出相应通知，通知期限不少于3个月。

9.12.3必须修改业务规则的情形

公司业务规则或CA系统有重大改变时，必须依据相应改变修改CPS。

9.13 争议处理

东方中讯CA与用户之间出现争议，包括但不限于合同纠纷、侵权纠纷等，如无法协商处理，各方同意将争议提交东方中讯CA住所地法院管辖。

如用户之间因使用东方中讯CA数字证书出现争议，则用户首先向东方中讯CA提交处理申请以及相关信息，由东方中讯CA派出专业人员进行事件判断，然后提出处理意见供双方参考。如还不能解决争端则将争议提交东方中讯CA住所地法院管辖。

9.14 法律适用

本CPS受中华人民共和国法律法规管辖及解释，电子认证各参与方的行为均受我国法律的管辖。

9.15 与适用法律的符合性

东方中讯CA电子认证服务严格遵从《中华人民共和国电子签名法》，符合国家相关管理部门的规范、规定。

9.16 一般条款

9.16.1完整协议

当前条款完全替换所有先前或同时期的、与相同主题相关的书面或口头解释的条款。

9.16.2转让协议

将一方的权利转让给另一方或授权其某种义务。

9.16.3分割性条款

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。

9.16.4强制执行

可以声明在合同纠纷中有利的一方有权将代理费作为偿还要求的一部分，或者声明免除一方对合同某一项的违反应该承担的责任，但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。

9.16.5不可抗力条款

通常用于出现超出受影响方控制的事件的发生时，免除一方或多方对合同的执行责任。通常，免除执行的时间与事件所造成的延迟时间相当。此条款也可包括协议终止的环境和条件。构成不可抗力的事件包括战争、恐怖袭击、罢工、自然灾害、供应商或卖方执行失败、因特网或其他基础设施的瘫痪。不可抗力条款的起草应与框架的其他部分相一致，并达到适用的服务级别协议。例如，业务连续性和灾难恢复的责任和能力可以将某些事件置于组织的可控范围之内，如在停电时启用备份电源的义务。

9.17 东方中讯CA拥有本CPS的最终解释权

9.18 其他规定

9.18.1 各种规范的冲突

若本CPS声明的规定与其他规定、指导方针或协议相互抵触，订户必须接受本认证业务声明的约束，除非本认证业务声明的规定在为法律所禁的范围内，且除非该项冲突的协议。

其签署日期在本认证业务声明首次公开发行之前；

该协议明确地优于本认证业务声明，因此必须由该协议规范所有当事人。

9.18.2 安全资料的财产权益

下列与安全相关的资料视为下列指定的当事人所拥有：

证书为东方中讯CA的产权所有。本规范旨在保护订户的隐私，避免未经授权者公布其证书；

本CPS声明的产权为东方中讯CA所有；

辨认名称为该名实体（或其雇主或委托人）所有；

不论密钥是以何种实体媒介存放或保护，私人密钥为合法使用或有权使用该密钥订户（或其雇主或委托人）所有；

无论密钥以何种实体媒介存放或保护，公开密钥为订户（或其雇主或委托人）所有；

东方中讯CA作为自身的根节点的公开密钥，是东方中讯CA的财产。这个公钥由东方中讯CA授权分配，放在值得信任的硬件或软件中。

9.18.3 损害性资料

证书申请人与订户不能把包含以下言论的任何资料提交给东方中讯CA或其业务受理点：

诽谤、中伤、不雅、色情、侮辱、迷信、憎恶或种族歧视的言论；

鼓吹非法活动或讨论非法活动，并试图从事此类活动的言论；

其他违法言论。

（全文结束）