内蒙古网信

电子认证服务业务规则

NMGSCA

Certification Practice Statement

Version 4.0

生效日期：2023年11月21日

内蒙古网信电子认证有限责任公司

内蒙古网信电子认证有限责任公司版权声明

版本修订记录

修订日期	版本号	说明	状态	修订人	批准人/部门
2018.10.3	1.0	初次版本	编制	菅玲	高鲁兵
2021.4.6	2.0	根据RFC3647调整文件结构，文件名称修改为《内蒙古网信 电子认证服务业务规则》，CPS覆盖范围扩展至一般电子商务活动，结构及内容按照《电子认证服务管理办法》及国家标准修改。	修订	孙圣男	安委会
2021.5.30	3.0	1.文本错误修订 2.增加了关于业务连续性的描述 3.增加关于赔偿流程的描述	修订	孙圣男	安委会
2021.7.2	3.1	1.文本错误修订 2.增加关于RA机构范围的定义 3.修订岗位名称 4.修订初始订户私钥鉴别方法	修订	孙圣男	安委会
2023. 11.11	4.0	1. 优化证书吊销情形 2.个人信息私密性条款优化补充，新增订户同意隐私保护制度、各方负有保护隐私的责任等约定； 3.完善有效期限与终止条款，包括效力保留条款； 4.新增CPS更新通知途径、订户同意更新协议等约定 5.新增设备证书等证书类型名称意义和要求 6. 新增算法对象标识符、名称形式、证书扩展项内容	修订	付慧裕	安委会

目录

第一章 概括性描述

1.1. 概述

内蒙古网信电子认证有限责任公司(以下简称“内蒙古网信”，英文简称NMGSCA)成立于2011年3月， 注册资金5000万元，具备国家密码管理局颁发的电子认证服务使用密码许可证(证书 编号 :0041)和 工 业和信 息化 部颁 发 的电子认证服务许可证（许可证编号 ECP15010216041)。内蒙古网信致力于为电子政务、电子商务及社会信息化等应用及用户提供优质的电子认证服务。

内蒙古网信电子认证服务业务规则(简称NMGSCA CPS，本CPS)根据国家相关法律法规的要求,详细阐述了内蒙古网信CA提供的电子认证服务整个过程、电子认证业务所遵循的规范以及电子认证服务各方所承担的责任范围等。

本文档的编写遵从以下法律、法规、标准的当前有效版本。

- 全国人大常委会《中华人民共和国电子签名法》 、《中华人民共和国密码法》
- 国家密码管理局 《电子认证服务密码管理办法》
- 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)》
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework 公钥基础设施证书策略和认证服务框架
- GB/T 25056-2018 《信息安全技术 证书认证系统密码及其相关安全技术规范》

若本CPS与以上法律、法规、标准、规范的有效版本有任何冲突之处，则以上述法律、法规、标准、规范的有效版本优先。

1.2. 文档名称与标识

本文档称为《内蒙古网信电子认证服务业务规则》，是内蒙古网信对所提供的认证及相关业务的全面描述，对象标识符（OID）为1.3.6.1.4.1.57247.0.1。

1.3. 电子认证活动参与者

电子认证活动参与者包括：电子认证服务机构、注册机构、订户、依赖方以及其他参加者，下文将分别展开描述。

1.3.1.电子认证服务机构

电子认证服务机构CA （Certificate Authority） 承担证书签发、更新、吊销、密钥管理、证书查询、证书黑名单（又称证书吊销列表或CRL）发布、认证服务策略制定等工作，本文中仅指内蒙古网信。

1.3.2.注册机构

注册机构RA （Registration Authority） 负责订户证书的申请受理、审批和管理，直接面向证书订户，并负责在订户和CA之间传递证书管理信息。

注册机构可以由内蒙古网信自建或向第三方机构授权建立。当注册机构由第三方机构建立时，内蒙古网信必须与其签订协议，明确双方的权利和义务。

下文中，内蒙古网信RA机构包括内蒙古网信现场受理前台及合作的第三方机构。

1.3.3.订户

订户(Subscriber)是指向内蒙古网信申请证书的实体。

需要明确的是，证书订户与证书主体是两个不同的概念：

“证书订户”是指向内蒙古网信申请证书的实体，通常为个人或机构,即为“最终用户”；

“证书主体”是指与证书信息绑定的实体，服务器证书中的“证书主体”通常是指受信任的服务器或用于与某一机构安全通信的其他设施。

证书订户需要承担相应的责任与义务，而证书主体则是证书所要证明的可信赖方。

1.3.4.依赖方

依赖方是指依赖于证书所证明的基础信任关系并依此进行业务活动的实体。

1.3.5.其他参与者

除内蒙古网信、订户、依赖方以外的参与者称为其他参与者。

1.3.6.受益者及责任

内蒙古网信CA证书相关联的参与者均为受益者。

1. 受益方

内蒙古网信CA证书可以为下列主体提供信赖保证：

- 所有提交证书协议的订户
- 获取证书的申请者
- 获取证书的软件供应商

- 证书在生效期间的依赖方

2. 内蒙古网信CA证书可提供的保证：

- 证书拥有者的合法存在性
- 证书拥有者的身份经过有效识别
- 证书中关于证书拥有者信息的准确性
- 证书状态7*24小时可查询
- CA根据CPS规则，废止不符合生效条件的证书

1.4. 证书应用

1.4.1.适合的证书应用

内蒙古网信的证书分类主要包含以下几类：

个人证书：包括个人身份证书等，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、合同签名，以实现信息保密，提供信息源合法性证明、完整性保障和抗抵赖。

机构证书：包括机构单位证书、机构部门证书、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，提供信息源合法性证明、完整性保障和抗抵赖。

设备证书：设备证书用于标识终端、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，及提供信息源合法性证明、完整性保障。

1.4.2.受限的证书应用

各类证书的密钥用法在订户证书中的扩展项中进行了限制。然而基于证书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，将不受内蒙古网信的保护。

任何未经内蒙古网信认可的证书应用都将不受内蒙古网信的保护。

1.4.3.禁止的证书应用

证书禁止在任何违反国家法律、法规或破坏国家安全的情形下使用。否则，由此造成的法律后果由订户自己承担。

内蒙古网信签发的数字证书禁止的应用范围包括:

1)国家法律法规所规定的不允许使用的范围;

2) 任何未经过安全检测的环境及应用:

3)内蒙古网信与订户约定的证书禁止应用的范围。

1.5. 策略管理

1.5.1.策略文档管理机构

内蒙古网信成立信息安全管理委员会（以下简称安委会），作为本机构电子认证服务业务规则的管理机构，对电子认证服务业务规则进行维护与管理，包括:

1)确定《内蒙古网信电子认证服务业务规则》的维护职责，并建立合理、有效的修订和批准流程;

2)定期对存在的业务风险进行评估，并及时对《内蒙古网信电子认证服务业务规则》进行修订;

3)按照《电子认证服务管理办法》规定，将修订后的《电子认证服务业务规则》及时报工业和信息化部备案，并在服务范围内公开发布；

内蒙古网信安委会由来自于公司管理层及各部门拥有决策权的合适代表组成。

1.5.2.联系方式

内蒙古网信公布以下对外的相关联系方式，任何有关本 CPS 的问题、建议、 疑问等， 均可按照下述方式联内蒙古网信:

1) 联系部门：内蒙古网信电子认证有限责任公司综合管理中心

2) 网站地址： www.nmgsca.com

3) 电子邮箱：cps@imntea.com

4) 联系地址：内蒙古呼和浩特赛罕区恩和大厦1508室(010010)

5) 电话号码： 18098907927

6) 传真号码：0755-86013399

1.5.3.决定 CPS 符合策略的机构

CPS 起草小组拟定初稿或修订稿后，交由公司安委会审议，安委会将负责 CPS 是否符合相关要求，如果符合，将报总经理审批。总经理审批同意后，本 CPS 方可对外发布，并自发布之日起 20 天内向行业主管部门报备。

1.5.4.CPS 批准程序

内蒙古网信按照以下方式处理本 CPS 的起草制定、 审批、 发布、 变更、备案等流程:

(1) 起草小组成立和 CPS 指定

内蒙古网信安委会召集会议，指定相关部门和人员成立起草小组。

CPS 起草小组拟定初稿，在编写过程中应及时向内蒙古网信安委会报告制定进展，并就有关问题召集相关人员讨论。

(2) 审批

本 CPS 由起草小组编写制定后，提交内蒙古网信安委会审核。内蒙古网信安委会议一致通过后，即作为正式版本。

(3) 发布

根据服务范围和服务对象要求，内蒙古网信采取如下的方式发布本 CPS：

1)以电子的方式，在相应的网站发布。

2)以书面的方式，客户服务部门可以根据需求提供。

(4) 变更

根据国家的政策法规、技术要求、标准的变化及业务发展情况等需要对本 CPS 进行修订，由起草小组编写修改建议报告，提交内蒙古网信安委会审核。经过批准通过后，按照前述方式进行对外发布。

(5) 备案

根据主管部门的规定，内蒙古网信安全策略委员在批准本 CPS 的制定或修订后，内蒙古网信将自发布之日起 20 天内向行业主管部门报备。

1.6. 符号与缩略语

见附录一。

第二章 信息发布与信息管理

2.1. 信息库

内蒙古网信信息库面向订户及证书应用依赖方提供信息服务。内蒙古网信信息库包括但不限于以下内容：证书、 CRL、CPS、证书服务协议、网站信息及其他信息。

2.2. 认证信息发布

内蒙古网信的 CPS 及相关支持信息在官网上发布。订户证书可以通过现场办理获得，已被吊销了的证书的信息可从 CRL 站点获取，证书状态(有效、 吊销) 可通过 OCSP 服务获得。

2.3. 发布的时间或频率

CPS 在完成 1.5.4 的批准流程后的 10 个工作日内发布到内蒙古网信网站上，并可确保 7*24 小时可用。

2.4. 信息库访问控制

内蒙古网信的安全访问控制机制确保只有经过授权的人员才能编写和修改信息库中的信息，但不限制对这些信息的阅读权。

第三章 身份识别与鉴别

3.1. 命名

3.1.1.名称类型

内蒙古网信颁发的数字证书，根据证书对应实体的类型不同， 其实体名字可以是人员姓名、 组织机构名称、部门名、 域名等，证书包含订户和颁发机构主题甄别名， 命名符合X.500 定义的甄别名规范。

3.1.2.对名称意义化的要求

DN(Distinguished Name)：唯一甄别名，在数字证书的主题名称域中，用于唯一标识证书主体的X.500名称。此域需要填写反映证书主体真实身份的、具有实际意义的、与法律不冲突的内容。

个人证书的甄别名通常可包含个人的真实名称、证件号码或其他个人身份标识，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、机构的证件号码或其他能证明机构主体的标识信息，作为标识订户的关键信息被认证。

设备证书的甄别名通常包含订户所拥有的域名或者外网IP，结合该订户的其他信息一起被鉴别和认证。

事件型证书的甄别名通常包含业务场景的相关数据信息，包括但不限于业务场景中的实体名称信息、笔迹信息、电子数据信息以及其他场景信息。

云端协同证书的甄别名可参照个人和机构证书的相关要求。

标识证书的甄别名是按照预定义规则生成，作为标识证书与应用ID编码绑定的依据。

预签证书的甄别名按照预定义规则生成，作为预签证书与订户身份信息绑定的依据。

3.1.3.订户的匿名或伪名

使用匿名的订户提交的证书申请材料不符合内蒙古网信的审核要求， 将无法通过审核，也无法获得证书和服务。

使用伪名或伪造材料申请的证书无效，一经证实立即予以吊销。

3.1.4.理解不同名称的形式的规则

内蒙古网信签发的数字证书符合X.509V3标准，甄别名格式遵守X.500标准，甄别名（DN）的命名规则由内蒙古网信定义，一般由CN、OU、O、C等部分组成，具体命名规则详见本CPS 7.1.3 名称形式。

3.1.5.名称的唯一性

在内蒙古网信信任域内，不同订户证书的主题甄别名不能相同，必须是唯一的。

3.1.6.商标的识别、鉴别和角色

内蒙古网信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，内蒙古网信颁发证书时不验证申请人是否使用商标或处于商标纠纷中， 当发生有关纠纷时，内蒙古网信有权拒绝申请并吊销任何已发放证书。

3.2. 初始身份确认

3.2.1.证明持有私钥的方法

当订户通过内蒙古网信受理前台申请证书时，不对订户是否持有私钥进行验证；

当订户通过内蒙古网信的合作方以网络在线申请的方式申请证书时，证明订户 拥有私钥的方法是通过pcks#10所包含的数字签名来完成的。 此情况下， 内蒙古网 信在为订户签发证书前，系统将自动使用订户的公钥验证其私钥的有效性和申请数 据的完整性， 依此来判断订户拥有私钥。

3.2.2.订户身份的鉴别

订户在申请证书时按应指定并书面授权证书的申请代表，提供有效身份证明文件、证书申请文件， 并接受证书申请的有关条款，同意承担相应的责任。

内蒙古网信接受订户的证书申请后，应对订户的身份真实性进行审核，并按照相关法律法规的要求妥善保存订户申请材料。

内蒙古网信对订户身份的鉴别过程如下：

内蒙古网信证书RA机构收集订户的申请材料 ，生产中心注册专员对订户材料

及身份进行录入初审，生产中心鉴证专员对注册专员录入的信息进行审核鉴证，无误后，由注册专员协助订户下载证书。证书载体 (USBKey)由RA机构交付订户。

3.2.2.1.组织机构身份的鉴别

组织机构申请者填写证书申请表，经过单位授权代表的签署及单位盖章，表示 接受证书申请的有关条款，并承担相应的责任。内蒙古网信授权的RA机构必须对订 户进行以下资料的鉴别：

1)证书申请表原件；

2)申请机构含有统一社会信用代码的机构证件原件及复印件；

3)经办人身份证原件与复印件；

4)经办授权文件。

3.2.2.2.个人身份的鉴别

个人申请者填写证书申请表，需阅读数字证书服务协议，表示接受证书申请的 有关条款，并承担相应的责任。内蒙古网信授权的RA机构必须对订户进行以下资料 的鉴别：

1)证书申请表原件；

2)个人有效证件原件及复印件；

3)经办人身份证原件与复印件（如代办）；4)经办授权文件(如代办)。

内蒙古网信RA机构的审核人员合理、 审慎地核对申请资料的原件与复印件， 并通过电话、邮政信函、可靠数据源等方式确认该机构、个人资料信息的真实性，以及代表机构、个人进行证书申请的个人是否得到足够的授权。

3.2.2.3.允许的证件类型

个人证件类型	*机构证件类型*
居民身份证	统一社会信用代码证
护照	外国(地区) 企业常驻代表机构登记证
港澳居民往来内地通行证	政府批文
台湾居民来往大陆通行证	组织机构代码证*
户又簿	税务登记证*
临时居民身份证	企业营业执照*
外国人永久居留证	事业单位法人证书*
	社会团体登记证书*
	民办非企业登记证书*

*：根据公安部、工商总局、发展改革委等 13 部门联合下发的《关于推进全国统一“多证合一”改革的意见》及各地推进多证合一工作安排，内蒙古网信不再接受税务登记证、组织机构代码证、不含统一社会信用代码的企业营业执照、不含统一社会信用代码的事业单位法人证书、 不含统一社会信用代码的社会团体登记证书、 不含统一社会信用代码的民办非企业登记证书的申请提交

3.2.3.没有验证的订户信息

内蒙古网信签发的证书信息没有未经过验证的信息。

3.2.4.授权确认

内蒙古网信签发证书前， 将确认证书申请必须获得授权。 当申请者代表组织机构订户申请证书时，需要出示足够的证明信息以证明申请者是否已获得组织机构的授权。内蒙古网信有责任确认该授权信息，并将授权信息妥善保存。

3.2.5.互操作准则

对于内蒙古网信外的其他证书服务机构颁发的证书，可以与内蒙古网信进行互操作，但是必须符合内蒙古网信的证书策略的要求， 并且与内蒙古网信签署了相应的协议。

内蒙古网信将依据协议的内容， 接受非内蒙古网信的发证机构鉴别过的信息，并为之签发相应的证书。

如果国家法律法规对此有规定，内蒙古网信将严格予以执行。

3.3. 密钥更新请求的标识与鉴别

3.3.1.常规密钥更新的标识与鉴别

对于常规密钥更新，订户可以用原有的私钥对更新请求进行签名。内蒙古网信认证系统会对订户的签名和更新请求进行鉴别。

订户也可以选择一般的初始证书申请流程，按照初始身份验证步骤进行常规密钥更新，按照要求提交相应的证书申请和身份证明资料。

内蒙古网信RA机构的审核人员合理、 审慎地核对申请资料的原件与复印件，根据审核人员的管理规定对申请者的资料的真实性进行审查，并进行批准或拒绝的操作。

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数据已经解密 ，否则，由此造成的损失，内蒙古网信将不承担责任。

3.3.2.吊销后密钥更新的标识与鉴别

内蒙古网信不提供证书被吊销后的密钥更新。订户必须重新进行身份鉴别，按照初始身份验证步骤向内蒙古网信申请重新签发证书。

3.4. 吊销请求的标识与鉴别

证书吊销请求的标识与鉴别流程见本CPS的4.7。

第四章 证书生命周期操作

4.1. 证书申请

4.1.1.证书申请实体

任何实体需要使用内蒙古网信的证书时，均可向内蒙古网信的RA机构提出证书申请。

4.1.2.注册过程与责任

1.最终订户

最终订户即申请证书的实体，最终订户须明确表示其愿意接受本CPS中所规定的相关责任与义务(本CPS公布在内蒙古网信网站上），并需要按照3.2.2的要求提供真实、准确的申请信息； 根据《中华人民共和国电子签名法》的规定， 申请者未向内蒙古网信的注册机构提供真实、完整和准确的信息，或者有其他过错， 给电子签名依赖方、内蒙古网信或者内蒙古网信的注册机构造成损失的，订户应承担相应的法律及赔偿责任。订户有责任保护其拥有的证书私钥安全。

2. 认证及注册机构

内蒙古网信既是一个CA，同时也承担RA机构的职能，如订户可以直接向内蒙古网信申请证书，由内蒙古网信RA机构审核订户信息并处理订户的请求。内蒙古网信的注册机构对订户提供的身份信息参照3.2.2的要求进行鉴别，并记录订户申请 时的相关信息，通过RA系统向CA系统发送请求, 内蒙古网信的CA系统校验RA

请求 的格式及权限， 并对通过鉴别后的订户签发证书。 内蒙古网信及其注册机构，应妥 善保管订户证书申请信息。

4.2. 证书申请处理

4.2.1.执行识别与鉴别功能

内蒙古网信处理证书申请至少需要设置3个可信角色：信息收集、信息验证、签 发证书。

其中信息收集、信息验证可以由同一人完成； 但签发证书人员需要与信息收集、信息验证职责分离。

对于证书申请处理， 签发证书人员需对申请机构信息做最终审核：

1) 对所有用已验证申请机构证书申请的信息和文件进行复核，查找冲突的信息 或需要进一步验证的信息；

2) 如复核人提出的问题确实需要得到进一步的验证，内蒙古网信必须从申请机 构、 协议签署人、 申请审批人或其他合格的独立信息来源取得进一步验证的资料或 证据；

3)内蒙古网信必须保证已收集的与证书申请相关的信息和资料，足以确保签发 的证书不包含内蒙古网信已知或应发现的错误信息，否则内蒙古网信将会拒绝证书 的申请并通知申请机构或申请个人。

4.2.2.证书申请批准和拒绝

依据识别与鉴别的信息，内蒙古网信RA机构有权决定接受或拒绝订户的申请，拒绝时将及时通知申请者并告知拒绝原因。

4.2.3.处理证书申请的时间

内蒙古网信RA机构必须在1个工作日内对证书申请者提交的证书信息进行识别，并完成证书申请处理。

4.2.4.证书签发

在证书的签发过程中RA的管理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，并确保请求发至正确的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的信息进行鉴别与解密，对于有效的证书签发请求，证书签发系统签发订户证书。

内蒙古网信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。

通常内蒙古网信签发的证书在24小时内生效。

内蒙古网信会采取通过面对面的方式， 通知订户(如申请者到受理点领取等方式) 领取证书存放的安全介质。

4.2.5.电子认证服务机构对订户的通告

无论是拒绝还是批准订户的证书申请，内蒙古网信及其注册机构有义务告知订户申请结果。可通过电话、电子邮件或当面告知方式对订户进行通告。

4.3. 证书接受

4.3.1.构成接受证书的行为

在内蒙古网信数字证书签发完成后，内蒙古网信将把数字证书当面给订户，订户从获得证书起就被视为已同意接受证书。订户接受数字证书后，应妥善保存其证书对应的私钥。

4.3.2. 电子认证服务机构对证书的发布

订户接受证书后，内蒙古网信在24小时内将该订户证书发布到内蒙古网信的目录服务系统。

4.3.3. 电子认证服务机构对其他实体的通告

内蒙古网信不具有向其他实体进行单独通告的义务， 但使用证书的各类实体可以通过内蒙古网信查询服务获得所需证书信息。

4.4. 密钥对和证书的使用

4.4.1.订户私钥和证书的使用

订户的私钥和证书应用于规定的、批准的用途(在本CPS 1.4.1定义)，订户在使用证书时必须遵守本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。

证书持有者只能在指定的应用范围内使用私钥和证书，证书持有者只有接受了相关证书后才能使用对应的私钥，并且在证书到期或被吊销后，须停止使用该证书及对应的私钥。

4.4.2.依赖方对公钥和证书的使用

依赖方在依赖内蒙古网信签发的证书所证明的信任关系时，需

要 1) 获取并安装该证书对应的证书链；

2) 在依赖证书所证明的信任关系前确认该证书为有效证书， 包括：检查内蒙古 网信公布的最新CRL，确认该证书未被吊销； 检查该证书路径中所有出现过的证书 的可靠性；检查该证书的有效期； 以及检查其他能够影响证书有效性的信息；

3)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所要证明的内容一致。

4.5. 证书密钥更新

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书。

4.5.1.证书密钥更新的情形

1. 当订户证书即将到期或已经到期时；
2. 当订户证书密钥遭到破坏时；
3. 当订户证实或怀疑其证书密钥不安全时；
4. 其他可能导致密钥更新的情形。

4.5.2.请求证书更新的实体

已经申请过内蒙古网信证书的订户可申请证书密钥更新。

4.5.3.证书更新请求的处理

同3.3 。

4.5.4.颁发新证书时对订户的通告

同4.2.5 。

4.5.5.构成接受密钥更新证书的行为

同4.3.1 。

4.5.6.电子认证服务机构对密钥更新证书的发布

同4.3.2 。

4.5.7. 电子认证服务机构对其他实体的通告

同4.3.3 。

4.6. 证书变更

内蒙古网信不提供证书变更服务。

4.7. 证书吊销和挂起

4.7.1.证书吊销的情形

当发现以下的情况，证书将被吊销：

1) 私钥失窃、篡改、未经授权的泄露和其它安全威胁；

2) 证书主体(无论是CA还是订户) 违反了本CPS规定的重要职责、义务；

3) 本CPS中职责的履行被延迟或受不可抗力的阻碍且与订户协商一致的：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；

4) 存在超过订户个人控制的原因并且对他人信息构成威胁的；

5) 订户主动提出吊销请求；

6) 内蒙古网信发现订户在申请时提供的证明材料不真实；

7) 订户拖欠证书服务应付费用经通知仍未支付的；

8) 法律、行政法规规定的其他情形。

4.7.2.请求证书吊销的实体

请求证书吊销的实体包括：

1) 已申请内蒙古网信证书的订户；

2) 内蒙古网信可在4.7.1中所述情形下主动吊销订户的证书。

4.7.3.请求吊销的流程

吊销分为主动吊销和被动吊销。主动吊销是指由订户提出吊销申请，由内蒙古网信审核通过后吊销证书的情形； 被动吊销是指当内蒙古网信确认订户违反证书应 用规定、 约定或订户主体已经消亡等情况发生时 ， 采取吊销证书的手段以停止对该 证书的证明。

1. 主动吊销

订户申请吊销证书前应制定并书面授权证书吊销申请代表，提供有效身份证明文件及证书吊销申请文件， 并接收证书吊销申请的有关条款，同意承担相应的责任。

内蒙古网信收到订户的吊销申请材料后，将查询订户需吊销的证书是否为内蒙 古网信签发，证书是否在有效期内， 吊销理由是否属实，若均通过则对证书进行吊 销。

2. 被动吊销

当出现被动吊销的情形时，内蒙古网信将以适当形式通知订户， 告知拟吊销的 证书内容、 吊销原因、 吊销操作时限等事项，在确认订户收到吊销通知且无异议后 予以吊销。

4.7.4.吊销请求宽限期

在主动吊销的情形下，订户一旦发现需要吊销证书，应及时向内蒙古网信提出吊销请求。

在被动吊销的情形下，订户在收到吊销通知后的1个工作日内可向内蒙古网信提出申辩理由，内蒙古网信将会对申辩理由进行评估，若确认其理由正当则不予以吊销；若订户在1个工作日内未回复或回复无异议则内蒙古网信将予以吊销。

4.7.5.电子认证服务机构处理吊销请求的时限

内蒙古网信从收到证书吊销请求起24小时内完成请求的处理。

4.7.6.依赖方检查证书吊销的要求

依赖方在信任证书前，应检查证书的有效性，确认证书未被吊销。

4.7.7.CRL 发布频率

内蒙古网信CRL发布周期为24小时，特殊紧急情况下可以立即签发CRL。

4.7.8.CRL 发布的最大滞后时间

内蒙古网信吊销的证书从被吊销到被发布到CRL上的滞后时间最大为24小时。

4.7.9.在线证书状态查询的可用性

内蒙古网信向证书订户提供7×24小时在线证书状态查询服务(OCSP)。

4.7.10. 吊销信息的其他发布形式

证书吊销信息可以通过CRL或者OCSP服务获得。订户可通过证书扩展域中的 CRL地址获得CRL信息。

4.7.11. 对密钥遭受安全威胁的特别处理要求

内蒙古网信所有订户在发现证书密钥受到损害时，应立即通知内蒙古网信吊销

证书。

4.7.12. 证书挂起的情形

内蒙古网信目前不提供此业务。

4.8. 证书状态服务

4.8.1.操作特征

证书状态可以通过内蒙古网信提供的CRL及OCSP服务获得。

4.8.2.服务可用性

内蒙古网信至少24小时发布一次CRL。

内蒙古网信的OCSP (在线证书状态查询)服务，对依赖方提供7×24小时服务。

4.9. 订购结束

以下两种情形将被视为订购结束：

1. 证书到期后即视为订购结束。
2. 证书吊销视为订购结束。

4.10. 密钥生成、备份与恢复

证书订户的加密密钥由密钥管理中心（KMC）托管备份，当证书订户本人、国 家执法机关、司法机关或其他管理部门因管理需要提出恢复加密密钥时，由内蒙古 网信通过相应程序从KMC为其取得相应的加密密钥。加密密钥被加密存放在KMC管 理中心 。

为保证订户签名私钥的安全性，内蒙古网信不保管签名私钥 。 因此，要求订户 妥善保管签名私钥。由于签名私钥遗失所造成的损失由证书订户自己承担，内蒙古 网信不负责。

第五章 认证机构设施、管理和操作控制

5.1. 物理控制

1)内蒙古网信所在的物理环境严格按照《证书认证系统密码及其相关安全技术规范》的要求实施，具有电磁屏蔽、消防、物理访问控制、 入侵检测报警等相关措施，并取得了相关部门的检测证书。

2)内蒙古网信所有员工佩戴标识身份的工牌，工作人员需使用身份识别卡或结合又令或指纹鉴定才能进出机房。

3)所有门禁系统能够记录人员进出信息，记录信息能够保存六个月。

4) 针对不同的人员角色内蒙古网信设置不同的访问权限， 只有经过授权的人员才能进入相应的区域，非授权人员不能进入。

5)内蒙古网信采用UPS供电线路， 由3组共120块（一台主机）UPS线路供电和双链路网络线路，保证断电后至少保持8小时不间断运行。

6)对于报废的存储介质，经过检查无残留信息后，通过物理损坏的方式进行销毁。

7)内蒙古网信办公场所有巡检人员不间断巡视，监控室24小时有专人值班，每天有专人负责巡检机房设备。

5.2. 程序控制

5.2.1.可信角色

在内蒙古网信提供的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内蒙古网信视为可信角色。这些角色包

括但不限于： 密钥和密码设备的管理员、系统管理员、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内蒙古网信的岗位职责说明为准。

5.2.2.每项任务需要的角色

内蒙古网信确保单个角色不能接触、导出、恢复、 更新、废止内蒙古网信的CA 系存储的根证书对应的私钥。对于关键的操作进行物理与逻辑上的分割控制，使掌握设备物理权限的人不能再拥有逻辑权限。至少两个可信角色才能使用一项对参加操作人员保密的密钥分割和合成技术来进行任何钥匙恢复的操作。

内蒙古网信对与运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制，保证至少一人操作，一人监督记录。

5.2.3.每个角色的识别与鉴别

所有内蒙古网信的在职人员，必须通过认证后，根据作业性质和职位权限的需要， 发放系统操作卡、门禁卡、登录密码、操作证书、 作业账号等安全令牌。对于使用安全令牌的员工，内蒙古网信系统将独立完整地记录其所有的操作行为。

所有内蒙古网信职位人员必须确保：

根据岗位安全等级的不同，进行不同程度层次的身份识别和鉴别措施；

基本的身份审查措施，确保符合岗位可信资格；

赋予可信员工相应的权限区分，为其发放安全令牌；

发放的安全令牌只直接属于个人或组织所有；

发放的安全令牌不允许共享。内蒙古网信的系统和程序通过识别不同的令牌，对操作者进行权限控制。

5.2.3.1. 需要职责分割的角色

内蒙古网信要求职责分割的角色包括（但不限于)以下几种：

安全员、系统管理员、网络管理员、操作员、订户信息收集人员（受理前台）、RA 注册管理员、RA 鉴证管理员。

5.3. 人员控制

5.3.1.资格、经历和无过失要求

内蒙古网信员工的录取经过严格的审查，根据岗位需要增加相应可信任的员工 。

内蒙古网信员工将接受入职考察，根据考察的结果安排相应的工作并进行培训上岗或者辞退。内蒙古网信根据需要对员工进行职责、岗位、 技能、政策、法律、安全等方面的培训。

内蒙古网信会对其关键的CA职员进行严格的背景调查 。背景调查主要通过（但不限于)以下方式：

1) 身份验证， 包括个人身份证件或户籍证件等；

2) 学历、学位等教育信息；

3) 个人履历，包括信用黑名单及社会公共安全记录等；

4)个人负面记录核查。

注册机构、 注册分支机构和受理点操作员的审查，可以参照内蒙古网信对可信任员工的考察方式。受理点责任机构可以在此基础上增加考察和培训条款 ，但不得违背内蒙古网信电子认证服务业务规则。

内蒙古网信确立流程管理规则，所有的员工与内蒙古网信签订保密协议，据此CA员工受到合同和章程的约束，不得泄露内蒙古网信证书服务体系的敏感信息。

5.3.2.背景审查程序

内蒙古网信制定了严格的员工背景审查程序，与有关的政府部门和调查机构，完成对内蒙古网信可信任员工的背景调查。身份背景调查过程中，存在(但不限于)下列情形之一，不得通过可信审查：

1) 伪造相关证件材料的

2) 伪造工作经历及工作证明人虚假的；

3) 虚假声称具有某种技能、能力的证件；

4)以往工作中存在重大不诚实行为的；

5)有犯罪记录的。

5.3.3.培训要求

内蒙古网信对内蒙古网信员工进行以下内容的综合性培训：

内蒙古网信运营体系；

内蒙古网信技术体系；

内蒙古网信安全管理策略和机制；

内蒙古网信岗位职责统一要求；

PKI基础知识；

身份验证和审核策略和程序；

内蒙古网信电子认证服务业务规则；

内蒙古网信灾难恢复和业务连续性管理；

内蒙古网信管理政策、制度及办法等；

国家关于电子认证服务的法律、法规及标准、程序；

其他需要进行的培训等。

5.3.4.再培训周期和要求

根据内蒙古网信策略调整、系统更新等情况，内蒙古网信将对员工进行每年至少一次继续培训机会，以保持其完成工作所需要的职业水平。

5.3.5.工作岗位轮换周期和顺序

根据岗位人员和业务上的实际情况内部自行安排。

5.3.6.未授权行为的处罚

当内蒙古网信员工进行了未授权或越权操作，将被立即终止工作并收到纪律处罚，其处理办法根据内蒙古网信相关管理规范执行。

5.3.7.独立合约人的要求

内蒙古网信的独立合约人及顾问执行与普通员工一致的可信资格确认， 此外独立合约人及顾问进入关键区域必须有专人的陪同与监督，必要时需签订保密协议。

5.3.8.提供给员工的文档

内蒙古网信向员工提供完成其工作所必须的文档 。

5.4. 审计日志程序

5.4.1.记录事件的类型

内蒙古网信的CA和RA运行系统， 记录所有与系统相关的事件，以备审查 。这些记录， 无论是纸质或电子文档形式， 都包含事件日期、 事件的内容、 事件的发生时间段、 事件相关的实体等。

内蒙古网信应记录的内容包括（但不限于）：

1)系统安全事件，包括 ： CA系统、RA系统和其他服务系统的活动，系统崩溃，硬件故障和其他异常。

2)电子认证服务系统操作事件，包括系统的启动和关闭。

3)认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员进入认 证机构设施及陪同人和安全存储设施的访问。

4)证书生命周期相关事件。

5.4.2.审计日志的保存期限

内蒙古网信会妥善保存认证服务的审计日志，本地保存期限至少三个月 ，离线存档为六年。

5.4.2.1. 审计日志的保护

内蒙古网信执行严格的保护和管理，确保只有内蒙古网信授权的人员才能访问 这些审查记录。并且实现异地备份，并禁止访问、阅读、修改和删除等操作。

5.4.2.2. 审计日志备份程序

内蒙古网信保证所有的审查记录和审查总结都按照内蒙古网信备份标准和程序进行。根据记录的性质和要求，采用离线备份工具，按照每月进行增量备份、每半年进行总量备份的方式执行。

5.4.2.3. 审计收集系统

内蒙古网信审查采集系统涉及：

证书签发系统；

证书注册系统;

证书目录系统;

证书审批受理系统;

访问控制系统(包括防火墙);

网站、数据库安全保障系统;

其他内蒙古网信认为有必要审查的系统。

5.4.2.4. 对导致事件实体的通告

对于审计收集系统中记录的事件，对导致该时间的个人、机构等主体，内蒙古网信不进行通告。

5.4.2.5.脆弱性评估

CA安全程序根据政策、技术和管理的变化及时进行薄弱环节分析，属于可以弥补的薄弱环节，及时弥补，属于不可弥补的薄弱环节，内蒙古网信每年对系统进行脆弱性评估，以降低系统运行的风险。

5.5. 记录归档

5.5.1.归档记录的类型

内蒙古网信对下列记录(包括但不限于)进行归档保存:

·系统建设和升级文档

·证书申请信息、证书服务批准和拒绝的信息 、与证书订户的协议、证书和CRL等

·系统运行和认证服务产生的日志数据、认证系统证书密钥升级和更新信息等

· 电子认证服务规则、 各类服务规范和运作协议、管理制度等

·系统数据库数据

·人员进出记录和第三方人员服务记录

·监控录像

·员工资料，包括背景调查、录用、培训等资料

·各类外部、内部审查评估文档

·证书订户的签名私钥和加密私钥由订户自己保存。有关私钥的保存责任应由订户本身承担。

5.5.2.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，内蒙古网信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、社会公众的电子认证服务，信息保存期为证书失效后五年。

·面向政务部门的电子认证服务，信息保存期为证书失效后十年。

5.5.3.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获取。内蒙古网信保护相关的档案免遭恶劣环境的威胁，例如温度、湿度和磁力等的破坏。

5.5.4.归档文件的备份程序

所有纸质归档记录按照备份策略和流程由专人定期执行， 备份介质在内蒙古网信公司本地备份管理。按照备份策略和流程，电子存档文件除了在内蒙古网信内本地备份外，还将在异地保存其备份。

5.5.5.记录时间戳要求

存档内容都按照归档策略和流程分别由专人收集、归档、 审核和保管。所有归档记录上均有参与归档操作的人员与时间记录。

5.5.6.归档收集系统

内蒙古网信的档案收集系统由人工操作和自动操作两部分组成。

5.5.7.获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。所有记录被访问后，在归还时需验证其完整性。 此外，内蒙古网信每年验证存档信息的完整性。

5.6. 认证服务机构密钥更替

认证机构进行密钥更替时应采用与初始化根密钥相同的方式进行。

确保新旧密钥更替期间，认证机构根密钥及信任链验证的有效性， 避免对现有应用造成影响 。新旧根证书过渡时 ，必须采用新私钥为旧公钥签名证书、 旧私钥为新公钥签名证书、 新私钥为新公钥签名的证书方式，保证用户和依赖方能够可靠地验证CA机构根证书以及确保证书信任链的有效性。

5.7. 损害与灾难恢复

5.7.1.事故和损害处理程序

内蒙网信安排7*24小时值班制度并建立不少于4人的值班巡检团队，可全天候对系统运行过程中出现的问题进行响应， 当遭到攻击 ，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，内蒙古网信将按照业务连续性计划实施恢复。

业务连续性计划由内蒙古网信安委会总负责， 其职能包括指导和管理信息安全 工作，批准、 发布业务连续性计划，根据实际情况决定启动灾难恢复等各项职能。

安全事件按其影响及范围分为以下三级：

特别重大安全事件应急预案(一级)

符合下列情形之一的，为特别重大安全事件(一级)：

公司主要业务系统瘫痪造成业务数据丢失或损坏；

公司主要业务系统不能正常运行造成系统中断服务8小时以上；

公司涉密的文件、 重要数据、 重大项目资料和重点客户档案等重要文档发生丢失、被盗，且丢失文件不能恢复。

重大安全事件应急预案(二级)

符合下列情形之一且未达到特别重大安全事件的，为重大安全事件(二级)：

公司主要业务系统瘫痪，但未造成业务数据丢失、损坏或业务系统数据通过技术手段可恢复的;

公司主要业务系统不能正常运行造成系统中断服务4—8小时;

公司涉密的文件、 重要数据、 重大项目资料和重点客户档案等重要文档发生丢失、被盗，但丢失文件可恢复。

较大安全事件应急预案(三级)

符合下列情况之一且未达到重大安全事件(二级)的，为较大安全事件(三级):

公司主要业务系统局部瘫痪未造成业务数据丢失或损坏，但通过技术手段可以恢复的。

公司主要业务系统不能正常运行造成CA系统中断服务4小时以下。

CA机房其他配套设施等系统出现瘫痪故障，未对公司业务造成损失。

公司非关键文件、 数据、 项目资料和客户档案等文档发生丢失、被盗。 对于三级安全事件，内蒙古网信将在7小时内解决;

对于二级安全事件，内蒙古网信将在24小时内解决;

对于一级安全事件，内蒙古网信将在48小时内利用备份数据恢复电子认证服务。

5.7.2.计算资源、软件或数据的损坏

内蒙古网信对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并 制定了相应的应急处理流程。 当出现计算机资源、软件或数据的损坏时，能在最短 的时间内恢复被损害的资源、软件和/或数据。

5.7.3.实体私钥损害处理程序

对于实体私钥的损害，内蒙古网信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 即通知内蒙古网信或注册机构吊销其证书。内蒙古网信按CPS发布证书吊销信息。

2）当内蒙古网信或注册机构发现证书订户的实体私钥受到损害时，内蒙古网信 或注册机构将立即吊销证书， 并通知证书订户，订户必须立即停止使用其私钥。内 蒙古网信按CPS发布证书吊销信息。

3）当内蒙古网信的证书出现私钥损害时，内蒙古网信将立即吊销CA证书并及 时通过途径通知依赖方， 并及时汇报主管机构， 然后生成新的CA密钥对、 签发新的 CA证书。

5.7.3.1.灾难后的业务连续性能力

除非物理场地出现了毁灭性的、 无法恢复的灾难，内蒙古网信能够在出现灾难 后最短时间内，根据业务连续性计划恢复其业务能力 。

5.7.3.2.认证服务机构或注册机构的终止

与认证机构或注册机构终止和终止通告相关的过程，应按照 《电子认证服务管理办法》、 《电子政务电子认证服务管理办法》的要求， 处理好相关承接事项，包括认证机构或注册机构档案记录管理者的身份问题。

第六章 认证系统技术安全控制

6.1. 密钥对的生成和安装

6.1.1.密钥对的生成

1.CA密钥对的产生

内蒙古网信密钥对由专门的密钥管理员及若干名接受过相关培训的可信雇员在内蒙古网信安全设施中按照规定的密钥生成规程进行产生。内蒙古网信密钥生成、保存的密码模块符合国家密码主管部门的要求， 并通过国家密码主管部门的鉴定。

2.RA密钥的生成

RA的签名私钥在安全控制下产生，RA证书由内蒙古网信签发。

3.最终证书持有者密钥对的产生

证书持有者签名证书可以使用硬件密码模块（如USBKey，智能卡）产生密钥对，加密证书的密钥由KMC产生，通过安全通道传递给证书持有者。

6.1.2.私钥传送给订户

订户的私钥由订户自己生成时将不会进行传送。由内蒙古网信生成时将离线或者在线安全方式传送，订户委托内蒙古网信或其他人产生私钥时，内蒙古网信或者受托方需确保私钥在交给客户前未被使用， 并且不能保留签名私钥的备份。

6.1.3.公钥传送给证书签发机构

订户可通过安全方式将公钥证书发送给内蒙古网信，或者通过电子邮件的形式发送给内蒙古网信。

6.1.4.电子认证服务机构公钥传送给依赖方

用于验证内蒙古网信签名的验证公钥（证书链)以及证书状态等信息可从内蒙古网信的信息库获得。

6.1.5.密钥的长度

内蒙古网信的电子认证系统支持签发SM2/SM3算法组合的证书。

6.1.6.公钥参数的生成和质量检查

公钥参数由国家密码主管部门许可的加密设备生成，内蒙古网信采购这些设备时要求其必须具有国家密码主管部门的相应资质，并遵从国家密码主管部门发布的《证书认证系统密码及相关安全技术规范》以及其他相关规范和标准要求， 如对生成的公钥参数的质量检查标准， 这些设备内置的协议、算法等均已达到足够的安全等级要求等。

6.1.7.密钥使用的目的

根CA私钥用于签发自身证书、下级CA证书和CA的吊销列表，中级CA证书用于签发订户证书和CRL，证书的公钥用于验证私钥签名。订户证书依据应用场景配置密钥用法(KU)及增强密钥用法(EKU)， 即，用于数字签名(包括身份验证)的证书将设置数字签名及/或不可否认的密钥用法，用于密钥或数据加密的证书将设

置密钥加密及/或数据加密的密钥用法，用于密钥协商的证书将设置密钥协商的密钥用法。 每种订户证书中至少包含两种密钥用法或增强密钥用法。

内蒙古网信根据国家标准要求为订户颁发双证书，增强密钥用法根据场景进行 配置。

6.2. 私钥保护和密码模块工程控制

6.2.1.密码模块的标准和控制

内蒙古网信CA系统生成密钥的密码模块 (加密机)安置在内蒙古网信机房核心 区域，使用通过国家密码主管部门批准使用的主机设备 ， 支持SM2 、SM3等国产密 码算法。

内蒙古网信使用的加密机， 其公钥算法为SM2 ， HASH算法为SM3 ， 具有国家 密码主管部门颁发的产品资质证书。

内蒙古网信制定有专门的加密机管理办法，对采购、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审批管理。加密机仅与对应系统直连， 并存放在屏蔽机房内。

6.2.2.私钥多人控制

内蒙古网信CA密钥存放在加密机中，加密机的管理密钥被分割保存在5把 USBKEY中， USBKEY由5位经过授权的可信人员掌握，并保存在屏蔽机房中的安全 区内的保险箱中。 当激活CA私钥时 ， 必须由5个可信人员的中的3个同时在场才能完 成，从技术及制度上保证了敏感操作的安全性。

6.2.3.私钥托管

对于CA私钥，内蒙古网信无托管业务。

6.2.4.私钥备份

CA的私钥由加密机产生，加密机有双机备份，并保存在防高温、防潮湿及防磁 场影响的环境中，对加密机的备份操作须3人以上(包括3人）才可完成。

订户私钥由订户产生，建议订户自行备份，并对备份的私钥采用又令或其他访 问控制保护机制， 防止非授权的修改或泄露。

6.2.5.私钥归档

当内蒙古网信的CA密钥对到期后，这些密钥对将被归档保存至少10年。归档的CA密钥对保存在本CPS 6.2.1所述的硬件密码模块中， 并且内蒙古网信的密钥管理策略和流程都确保了归档后的CA密钥对不会再被用于生产系统中。 当归档的CA密钥对达到归档保存期限后，内蒙古网信将按照本CPS6.2.10所述的方法进行安全的销毁。

内蒙古网信基于PKI理论为订户产生的加密私钥的归档参照CA的密钥归档方法 进行归档。

6.2.6.私钥导入、导出密码模块

内蒙古网信通过硬件模块产生CA密钥对，部署了备份加密设备，CA密钥对在 备份传递时以离线加密方式进行。

通过硬件产生的订户私钥不能导出密码模块。其他方法产生的订户私钥在导出 时应采取加密的方式进行。

6.2.7.私钥在密码模块的存储

私钥以密文的方式分段加密存放在硬件加密模块中。

6.2.8.激活私钥的方法

1. 激活订户私钥

当订户使用硬件密码模块产生、保存私钥时，订户使用硬件密码模块又令（或 pin码)保护私钥，硬件加密模块被加载，密码模块验证又令完成后，私钥被激活。

2. 激活CA私钥

内蒙古网信采用硬件设备（加密机）产生、保存CA私钥，其激活数据按照本CPS 6.2.2要求进行分割。一旦CA私钥被激活， 激活状态将保持到CA离线。

6.2.9.接触私钥激活状态的方法

对于订户私钥，当服务程序被停止、系统注销或系统断电后私钥进入非激活状态。

对于CA私钥，当硬件密码模块断电或重新初始化时，私钥进入非激活状态。

6.2.10. 销毁私钥的方法

当CA的生命周期结束后，内蒙古网信将根据本CPS6.2.5将CA私钥自行归档，其他的CA私钥备份将被安全销毁。归档的私钥在其归档期结束后，需要在3名以上可信人员参与下进行安全地销毁。

订户私钥的销毁须经授权后安全地销毁。密钥生命周期最后，销毁所有订户密钥的副本和碎片。

6.2.11. 密码模块的评估

内蒙古网信使用国家密码主管部门鉴定并批准使用的主机加密设备，接受其颁布的各类标准、规范、 评估结果等各类要求。

6.3. 密钥对管理的其他方面

6.3.1.公钥归档

对于生命周期外的CA和订户证书，内蒙古网信将进行归档 。归档的证书存放在 归档数据库中。 归档要求参照本CPS 5.5的相关规定。

6.3.2.证书操作期和密钥对使用期限

证书操作期终止于证书过期或者被吊销。内蒙古网信为订户颁发的证书操作周 期通常与密钥对的使用周期是相同的。

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。为了保证能够验证在证书有效期内的签名的信 息，公钥的使用期限可以在证书的有效期限外。

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。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。

6.4. 激活数据

6.4.1.激活数据的产生和安装

内蒙古网信的CA私钥产生遵循本CPS 6.2.2中的要求。

如果订户证书私钥的激活数据是又令，这些又令必须:

由订户产生;

至少6位字符或数字;

不能包含很多相同的字符;

不能和操作员的名字相同;

不能使用生日、电话等数字;

不能包含订户名信息中的较长的子字符串。

6.4.2.激活数据的保护

保存有内蒙古网信根私钥的激活数据的5个智能卡，由内蒙古网信5个不同的超级管理员掌管， 而且超级管理人员必须符合内蒙古网信职责分割的要求， 签署协议确认他们知悉密钥分割掌管者责任。

如果证书订户使用又令或PIN码保护私钥，订户应妥善保管好其又令或PIN码，防止泄露或窃取。

6.4.3.激活数据的其他方面

6.4.3.1.激活数据的传输

存有内蒙古网信根CA私钥的激活数据的智能卡，通常保存在内蒙古网信的安全设施中，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在内蒙古网信安全管理人员和密钥管理人员的共同监督下进行。

当订户证书私钥的激活数据需要进行传送时，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。

6.4.3.2.激活数据的销毁

存有内蒙古网信根私钥的激活数据的智能卡，其销毁所采取的方法包括将智能卡初始化，或者彻底销毁智能卡，保证不会残留有任何秘密信息。

当订户证书私钥的激活数据不需要时应该由订户自行销毁，订户应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部。

6.5. 数据安全控制

6.5.1.制定安全方案确保数据安全目标

1. 内蒙古网信将采取授权访问的策略和加密签名的手段，确保对CA的控制和 证书申请等相关数据以及证书的相关流程的机密性、完整性和可用性，确保其不受 到未经授权或非法的访问、使用、 披露、修改或销毁，保护其不受到意外的丢失、 销毁或损坏； 以及不受到可预见的威胁和破坏；

2.确保验证“证书数据”、 签发证书、 维护信息库和吊销证书的密钥、软件和流 程的机密性、完整性和可用性；

3. 内蒙古网信将确保其维护的数据符合相应法律规定的其他安全要求。

6.5.2.安全方案定期风险评估

1.内蒙古网信定期评估风险，识别可预见的使“证书数据”和“证书流程”受到未 经授权的访问、错误使用、 披露、修改或销毁的内外部威胁。

2.风险评估将根据“证书数据”和“证书流程”的敏感程度评估所识别威胁因素发 生的可能性和发生后预计造成的破坏程度。

3.每年将定期评估CA用于控制这些风险的制度、流程、信息系统、 技术或其 他因素是否足够。

6.5.3.安全计划

内蒙网信将根据风险评估结果制定安全计划，内容包括制定、 实施并维护安全流程、 措施以及为数据安全设计的产品。根据“证书数据”和“证书流程”的敏感程度以及操作流程的复杂程度和范围， 合理的管理和控制所识别的风险。安全计划包括与CA业务、“证书数据”和“证书流程”的规模、复杂程度、性质和范围相适应的行政、组织架构、 技术和物理环境的安全控制措施。制定安全控制措施时，考虑今后可用 的技术和相应的成本；安全控制措施程度必须与缺失该控制可能造成的破坏以及该 控制所保护数据的性质相符合。

6.6. 计算机安全控制

6.6.1.特别的计算机安全技术要求

内蒙古网信的数字证书签发系统的数据文件和设备由内蒙古网信系统管理员维护，未经内蒙古网信管理员授权， 其它人员不能操作和控制内蒙古网信系统；其它普通订户无系统账号和密码。内蒙古网信系统部署在多级防火墙之内，确保系统网络安全。

6.6.2.计算机安全评估

内蒙古网信的CA系统已通过国家密码管理局等有关部门的安全性审查。

6.7. 生命周期技术控制

6.7.1.CA 系统运行管理

内蒙古网信每天由专人负责巡检机房设备的工作情况，定期由技术人员检查软件系统的运行情况。部署了漏洞扫描系统、入侵检测系统和防火墙等，以确保网络环境的安全稳定。

6.7.2.CA 系统的访问管理

设置关键岗位和职责分工，对于CA系统的访问权限进行严格限制，未授权人员不得访问CA系统。

6.7.3.CA 系统的开发和维护

原则上不对CA系统进行技术开发和直接调用其数据， 仅将CRL 、OCSP对外提供查询和访问服务。

6.8. 网络的安全控制

内蒙古网信网络中有防火墙、入侵检测、漏洞扫描和网络防病毒等安全机制保护， 其配置只允许已授权的机器访问 。只有经过授权的内蒙古网信员工才能够进入内蒙古网信签发系统、内蒙古网信注册系统、内蒙古网信目录服务器、内蒙古网信证书发布系统等设备或系统。所有授权订户必须有合法的安全令牌 ， 并且通过密码验证。

CA系统只开放与申请证书、 查询证书等相关操作功能 ， 其他端又和服务全部关闭 。CA系统的边界控制设备拒绝一切非电子认证业务的服务。

6.9. 时间戳

内蒙古网信认证系统的各种系统日志、操作日志有对应的记录时间 。时间源自国家标准时间源。

第七章 证书、证书吊销列表(CRL)和在线证书状态协议(OCSP)

7.1. 证书

内蒙古网信前发的证书格式符合 GM/T 0015-2012 数字证书格式规范， 包含如下证书域:

7.1.1.版本号

内蒙古网信签发的证书格式符合X.509V3标准，这一版本信息包含在证书版本属性内。

7.1.2. 算法对象标识符

符合国家密码管理部门批准的算法标识符。

7.1.3.名称形式

CA数字证书中的主体Subject的X.500 DN是 C=CN命名空间下的X.500目录唯一名字，各属性的编码一律使用UTF8String。

主体Subject的 X.500 DN 支持多级 O 和OU，其格式如下:

C=CN

O=xx

O=xx

OU=xx

OU=xx

CN=xx

其中：

- C（Country）应为CN，表示中国；
- O（Organizatioon）中的内容分为3种：

A）证书主题或者证书主体所属单位具有明确的上一级单位，则应为其上一级单位的名称全称；

B）不存在A）中所属的上一级单位，则应为证书主体或者证书主体所属单位的所在省、自治区、直辖市名称全称；

C）CA机构自定义的信息标识，例如：注册机构的信息标识、应用单位的信息标识等；

- OU（Organization Unit）中的内容分为3种：

A） 证书主体或者证书主体所属单位的名称全称；

B） 证书主题的类型，其中个人为Individual，组织机构为Organization；

C） 采用的特殊身份鉴别方式或备注信息，需要依赖纺织系并选择是否信赖，详见第3.2章。

- CN（Common Name）中的内容分为6种:

A）个人证书应为证书主体的姓名，还可以包含其他标识信息；

B）单位机构证书中应为证书主体单位的标准名称或简称，还可以包含其他标识信息；

C） 服务器证书应为证书主体设备的域名或者IP地址或者设备编码；

D）代码签名证书应为负责人的姓名，或者是所属单位的标准简称；

E） 标识证书、预签证书中应为一个按照预定义规则生成的用户标识；

F） 事件型证书中代表签名行为业务场景的相关信息，分两种：

- 当订户是电子签名人时，CN中的内容是订户的名称；
- 当订户是申请对签名行为业务场景相关信息进行固化的实体时，CN中的内容可以是实体名称，也可以是需要固化的签名行为相关信息；
- Email仅在邮件证书的DN中存在，应为证书主题的有效电子邮件地址。

7.1.4.证书扩展项

证书扩展项是一个或多个证书扩展的序列，针对某种证书类型或者特定用户，内蒙古网信签发的证书将包含私有扩展项，私有扩展项将被设置为非关键性扩展。对于CA证书的证书扩展项，除4个扩展项：基本限制(BasicConstraints)，密钥用法(KeyUsage)，证书策略(CertificatePolicies)，增强密钥用法(ExtendedKeyUsage)，其他扩展项遵循RFC5280标准。

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:

- 颁发机构秘钥标识符 Authority Key Identifier
- 主体密钥标识符 Subject Key Identifier
- 秘钥用法 Key Usage
- 扩展密钥使用期 Private Key Usage Period
- 主体可选替换名称 Subject Alternative Name
- 基本限制 Basic Constraints

证书吊销列表分发点 CRL Distribution Points

私有扩展项可支持以下类型:

- 个人身份证号码 Identtify Card Number
- 企业营业执照（统一社会信用代码）IC Registration Number
- 签名证据项：Siggnature Evidences，应包含签名相关证据内容，如声音、图像等。

7.1.4.1.颁发机构密钥标识符

内蒙古网信订户证书及 CA 证书中包含颁发机构密钥标识符扩展项，此扩展项用于识别与证书签名私钥项对应的公钥，可辨别同一 CA 使用不同的密钥 。该扩展项为非关键项。

7.1.4.2. 主题密钥标识符

订户证书中包含主题密钥标识符扩展项，它标识了被认证的公钥，可用于区分同一主体使用的不同密钥（如证书密钥更新时)。 该扩展项为非关键项。

7.1.4.3.密钥用法

密钥用法指明已认证的公开密钥用于何种用途。

对于 CA 证书的密钥用法， 该项为关键扩展。 密钥用法包括证书签名、 CRL 签发，其他密钥用法不能出现。对于订户证书， 该项为关键扩展。

7.1.4.4.基本限制

基本限制项用来标识证书的主体是否是一个 CA，通过该 CA 可能存在的认证路径有多长，该项定义遵照 RFC5280 的规定，订户证书中该项为关键扩展。

7.1.4.5.增强密钥用法

本项指明已验证的公钥可用于一种或多种用途，可作为对密钥用法扩展项中的基本用途的补充或替代 。该扩展项为非关键项。

7.1.4.6.CRL 分布点

系统签发的证书包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供的地址和协议下载 CRL 。该扩展项为非关键项。

7.1.4.7.主题备用名称

主题备用名称包含一个或多个可选替换名(可使用多种名称形式中的任一个)供实体使用， CA 把该实体与认证的公开密钥绑定在一起 。该扩展项的使用符合 RFC5280 的规定。

7.1.5.算法对象标识符

内蒙古网信签发的证书采用 SM2/SM3 密码算法签名， SM2 算法 OID 为 1.2.840.10045.2.1 ，附加参数为 1.2.156.10197.1.301。

7.1.6.主题名称

本项用于描述与主题公钥项中的公钥对应的实体的情况。内蒙古网信签发的证书的甄别名符合 X.500 关于甄别名的规定，内蒙古网信保证签发的证书对应的每个主题实体的甄别名称是唯一的。

7.1.7.名称限制

内蒙古网信签发的证书， 其实体名称不允许为无意义的匿名或者伪名， 必须是有明确含义的识别名称，使用英文名称时应能正确表达实体名称。

7.1.8.证书策略及对象标识符

CA 证书的证书策略扩展项中，本项设置为 anyPolicy。

7.1.9.策略限制扩展项的用法

未使用本扩展域。

7.1.10.策略限定符的语法和语义

未使用本扩展域。

7.1.11.关键证书策略扩展项的处理规则

未使用本扩展域。

7.2. CRL

7.2.1.版本号

内蒙古网信目前使用的是 X.509 V2 版本的 CRL。

7.2.2.CRL 和 CRL 条目扩展项

CRL 数据定义如下:

1.版本(Version)显示 CRL 的版本号。

2.CRL 的签发者（Issuer）指明签发 CRL 的 CA 的甄别名。

3.CRL 的发布时间（thisUpdate)。

4.预计下一个 CRL 更新时间（nextUpdate)

5.签名算法

6.列出吊销的证书， 包括吊销证书的序列号和吊销日期。

7.3. 在线证书状态协议

内蒙古网信提供在线证书状态查询服务， 正常的网络状态下，内蒙古网信可确保有足够的资源使 CRL 和 OCSP 服务在合理的时间内向用户反馈查询结果。

第八章 认证机构审计和其他评估

8.1. 评估的频率或情形

内蒙古网信在如下情形中进行评估：

1.根据《中华人民共和国电子签名法》、 《中华人民共和国密码法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》规定， 接受主管部门的评估和检查。

2.根据业务情况发展，对注册机构进行评估。

评估的频率为：

1.年度评估：接受主管部门对内蒙古网信进行的年度检查 。

2.运营前评估：在新系统向公众提供服务之前由行业主管部门对新系统进行评估，评估合格后方可正式运营。

8.2. 评估者的资质

除主管部门指定外，当需要外部机构对内蒙古网信进行评估，内蒙古网信将选 择熟悉 IT 运营管理、 具有多年审计经验的审计机构对内蒙古网信的运营管理进行 一致性审计。在审计进行前，审计机构必须熟悉 PKI 技术及相关法律法规、标准规 范要求。

8.3. 评估者与被评估者的关系

评估者与内蒙古网信应无任何业务、 财务往来或其他足以影响评估客观性的利 害关系。

8.4. 评估内容

评估的内容包括但不限于：

CA 物理环境和控制

密钥管理操作

基础 CA 控制

证书生命周期管理

CA 业务规则

8.5. 对问题与不足采取的措施

内蒙古网信管理层将对评估报告进行评估，对评估中发生的重大问题采取行动，从完成评估到采取行动纠正问题的时间不超过 20 个自然日。

8.6. 评估结果的传达与发布

当内蒙古网信接受行业主管部门的检查或评估后，行业主管部门会向公众发布 检查或评估结果。当内蒙古网信进行内部审计后，审计结果将只在公司内部进行传达。

8.7. 其他评估

内蒙古网信定期进行内部审计，并将根据项目需要指定审计计划。

第九章 法律责任相关要求

9.1. 费用相关

9.1.1.证书签发和更新费用

根据市场管理部门的规定，内蒙古网信将收取合理的费用。费用情况将根据不 同项目需要单独确定并由项目合作方提前通知订户。 内蒙古网信也可以通过其他方 法通知证书持有者或其他各方费用变化。

9.1.2.证书查询费用

内蒙古网信目前不对此项收取专门的费用，但保留对此服务收费的权利。

9.1.3.证书吊销或状态信息的查询费用

内蒙古网信目前不对此项收取专门的费用，但保留对此服务收费的权利。

9.1.4.其他服务费用

内蒙古网信保留收取其他服务费用的权利。

9.1.5.退款策略

如果由于内蒙古网信违背了本 CPS 所规定的责任与义务，订户可以要求退款。

订户应当提供符合内蒙古网信要求的完整、真实、准确的证书申请信息，否则 内蒙古网信对此造成的损失和后果不承担责任。

9.2. 财务责任

内蒙古网信保证具有维持、运作和履行其责任的经济基础，有能力承担对订户、依赖方因合法使用数字证书时而造成的责任风险，并依据本电子认证服务业务规则规定的方式和范围进行有过错时的赔偿。

9.2.1.保险范围

内蒙古网信将根据业务发展情况和保险公司业务开展情况决定是否投保及投保 策略。

9.2.2.其他资产

内蒙古网信目前有能力维护运营和应对可能出现的赔付。

9.2.3.对最终实体的保险或担保

如果根据司法判定，内蒙古网信需承担赔偿和/或补偿责任的，内蒙古网信将按 照相关仲裁机构的裁定或法院的判决承担相应的赔偿责任。

当证书订户发起赔偿申请时，由技术服务中心确认是否属于上述赔偿范围内，且应由国家权威部门或司法鉴定机构出具责任认定书后，财务部根据订户订购协议 进行赔偿操作。

赔偿流程由内蒙古网信综合管理中心监督执行。

9.3. 业务信息保密

内蒙古网信有专门的信息保密制度，保护自身和订户的敏感信息、商业秘密。

9.3.1.保密信息范围

内蒙古网信保密的信息包括（但不限于）：

1. 系统方面

-认证系统结构、 配置， 包括系统、网络、 数据库等；

-认证系统安全策略和方案；

-系统操作、维护记录；

-各类系统操作又令。

2.运营管理方面

-物理安全策略与实施方案，包括场地、 访问控制、入侵检测等实施方案；

-密钥管理策略与操作记录；

-CA或RA批准或拒绝的申请纪录；

-可信人员名单；

- 内部安全管理策略与制度；

-审计记录。

3.订户信息

-订户的注册信息;

-订户系统、应用访问CRL、OCSP的记录(时间、频度) ;

-订户与认证机构、 注册机构签订的协议。

9.3.2.不属于保密的信息

内蒙古网信电子认证服务业务规则、证书申请流程、 手续、 申请操作指南、证书吊销列表等。

9.3.3.保护保密信息的责任

内蒙古网信有各种严格的管理制度、流程和技术手段保护自身的商业秘密，每个员工都必须接受信息保密方面的培训。任何参与方有责任保证不泄露保密信息。

9.4. 个人信息私密性

9.4.1.隐私保密方案

内蒙古网信制定有隐私保护制度，保证证书订户的个人信息不被滥用、未授权使用或出售，同时采取必要措施防止客户资料被遗失、盗用与篡改。订户通过勾选、点击确认或其他方式表示接受隐私保护制度，或以任何方式使用证书服务的，则表明已经同意接受内蒙古网信的隐私保护制度。

9.4.2.作为隐私处理的信息

作为隐私处理的信息包括：最终订户注册申请证书中提交的信息 ，包括联系电话、地址等；订户与内蒙古网信、 注册机构签订的协议。

9.4.3.不被视为隐私的信息

不被认为是隐私信息包括：用来构成证书内容的信息，证书及证书状态。

9.4.4.保护隐私的责任

内蒙古网信、注册机构、订户、依赖方等机构或个人均负有义务按照本CPS的规定，承担相应的隐私保护责任。在法律法规或执法、司法、行政等公共权利部门通过合法程序要求下，内蒙古网信及其注册机构可以向特定对象披露隐私信息。

9.4.5.使用隐私信息的告知与同意

订户同意，内蒙古网信按照所发布的隐私保护制度的相关约定使用所获得的任何订户信息。

内蒙古网信或其注册机构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，则需要事先告知订户并获得订户同意和授权，订户同意和授权信息以下列方式之一传送给内蒙古网信或其注册机构：

1) 将手写签名的同意和授权文件邮寄、 快递到内蒙古网信或其注册机构；

2）将手写签名的同意和授权文件传真到内蒙古网信或其注册机构；

3）以签名电子邮件的形式同意并授权。

4）根据法律法规的相关规定征得订户授权及同意。

9.4.6.依法律或行政程序的信息披露

当内蒙古网信在任何法律、法规或规章条款的要求下，或在司法机关的要求下必须披露本电子认证服务业务规则中具有保密性质的信息时，内蒙古网信可以

按照 法律、法规或规章条款以及司法机关的要求， 向执法部门公布相关的保密信息 。这 种披露不被视为违反了保密的要求和义务，内蒙古网信无需承担由此产生的任何责任。

9.4.7.其他信息披露情形

对其他信息的披露受制于法律、行政法规的相关规定，以及订户与内蒙古网信的相关协议。

9.5. 知识产权

内蒙古网信保留对本CPS的所有知识产权。内蒙古网信保留其签发的证书和证 书吊销信息的所有知识产权。任何人可以免费地复制、分发证书和证书吊销列表， 只要他们进行完整复制并且证书和证书吊销列表的使用符合相应的依赖方协议。证 书申请者保留证书申请中包含的申请者拥有的商标、服务标志或商业名称以及签发 给该证书申请者的证书中的可辨识名的所有权利。证书所有者拥有其证书相关的密 钥对的知识产权。

9.6. 陈述与担保

9.6.1.电子认证服务机构的陈述与担保

除非内蒙古网信做出特别约定， 若本电子认证服务业务规则的规定与其他内蒙古网信制定的相关规定、 指导方针相互抵触，订户必须接受本电子认证服务业务规则的约束。在内蒙古网信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服务业务规则的规定执行；

对协议中有不同于本电子认证服务业务规则内容的约定，按双方协议中约定的内容执行。

内蒙古网信承担的责任和义务是:

保证电子认证服务机构本身使用和发放的公钥算法在现有通常技术条件下不会被攻破； 保证内蒙古网信的签名私钥在内蒙古网信内部得到安全的存放和保护 ；内蒙古网信建立和执行的安全机制符合国家政策的规定。内蒙古网信不对由于客观意 外或其他不可抗力事件造成的操作失败或延迟承担任何损失、损坏或赔偿责任。 这些事件包括政府行为、劳动纠纷、交易一方故意或无意的行为、 罢工 、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他大灾难等。针对上述内容补充解释如下:

第一： 除上述所规定的职责条款，内蒙古网信的服务机构、内蒙古网信授权的 发证机构、内蒙古网信的雇员不承担其它任何义务。 必须指出，本电子认证服务业 务规则的内容， 没有任何信息可以暗示或解释成内蒙古网信必须承担其它的义务或 内蒙古网信必须对其行为做出其它的承诺。

第二：在上述内容中所罗列不可抗力的任何情况下，内蒙古网信由于受到影响，可免除本节所述的责任和相应的证书策略规定的责任和义务。

第三：由于技术的进步与发展，为保证证书的安全性，内蒙古网信会要求证书 持有者及时更换证书以保证内蒙古网信能更好地履行本节所述之责任。

9.6.2.注册机构的陈述与担保

注册机构必须遵守所有的登记程序和安全保障措施 。这些程序和保障由内蒙古 网信决定， 并在本电子认证服务业务规则或相应的注册机构协议中规定，以

后内蒙古网信可以根据情况修改有关内容， 并及时公布。 注册机构必须遵守和符合本电子认证服务业务规则的条款。

9.6.3.订户的陈述与担保

所有的订户必须严格遵守关于证书申请以及私钥的所有权和安全保存相关的程序:

订户在证书申请表上填列的所有声明和信息必须是完整、精确、真实和正确的，可供内蒙古网信或受理点检查和核实;

订户必须严格遵守和服从电子认证服务业务规则规定的或者由内蒙古网信推荐使用的安全措施； 订户需熟悉本电子认证服务业务规则的条例和与证书相关的证书政策，遵守订户证书使用方面的有关限制;

一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘或泄密以及其他情况，订户应立刻通知内蒙古网信或内蒙古网信授权的发证机构， 申请采取挂失、 废除等处理措施。

9.6.4.依赖方的陈述与担保

依赖方确认，在任何信赖行为发生之前， 阅读了依赖方协议，并评估了在特定应用中信赖证书的适当性，不在证书适用目的以外的应用中信任证书。

9.6.5.其他参与者的陈述与担保

未列明的其他参与者应遵守本CPS的所有规定。

9.7. 担保免责

有下列情形之一的，应当免除内蒙古网信之责任：

1)订户在申请和使用内蒙古网信数字证书时，有违反如下义务之一的：

- 订户应当提供真实、完整、准确的材料和信息，不得提供虚假、无效的 材料和信息；
- 订户应当妥善保管内蒙古网信所签发的数字证书载体和保护PIN码，不 得泄漏PIN码或将数字证书载体随意交付他人；
- 订户在应用自己的密钥或使用数字证书时，应当使用可依赖的、安全的 系统；
- 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 知内蒙古网信及相关各方， 并终止使用该电子签名制作数据；
- 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 得将数字证书在内蒙古网信规定使用范围之外的其他任何用途使用；
- 订户必须在证书有效安全期内使用该证书，不得使用已失密或可能失密、已过有效期、被吊销的数字证书。

2)由于不可抗力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；本项所规定之“不可抗力”， 是指不能预见、不 能避免并不能克服的客观情况，包括（但不限于）：

- 自然灾害，包括地震、火山爆发、滑坡、泥石流、 雪崩、洪水 、 台风等；
- 社会异常或者政府行为， 包括政府颁发新的政策或调整、变更、法律和行政法规，或

战争、罢工 、骚乱等社会异常事件。

3)内蒙古网信已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.8. 有限责任

在与订户和依赖方签订的协议中，对于因订户或依赖方的原因造成的损害不 具有赔偿义务：

(1)对于由如下原因造成的订户或依赖方损失，内蒙古网信对订户或依赖方进行赔偿：

1)内蒙古网信在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发；

2)由于内蒙古网信的原因，使得证书中出现了错误信息 。

(2)在如下情况，订户对自身原因造成的内蒙古网信、 依赖方损失承担责任：

1)订户在证书申请中对事实的虚假或错误描述；

2)在证书申请中订户没有披露重要的事实，如果这种错误表述或遗漏是因为粗心或故意欺骗任何一方；

3)订户没有使用可信系统保护私钥，或者没有采取必要的注意防止订户私钥的安全损害、丢失、泄漏、修改或非授权的使用；

4)订户使用的名字（包括但不限于通用名、 域名和e-mail地址）破坏了第三方的知识产权法。

(3)在如下情况，依赖方对自身原因造成内蒙古网信损失承担责任：

1) 依赖方没有执行依赖方职责义务；

2) 依赖方在不合理的环境下信赖一个证书；

3) 而依赖方没有检查证书状态确定证书是否过期或吊销。

(4)内蒙古网信承担赔偿责任(法定或约定免责除外)的赔偿限制如下:

1)内蒙古网信对任何证书订户、 依赖方等实体有关证书赔偿的合计责任限制偿上限可以由内蒙古网信根据情况重新制定，内蒙古网信会将重新制定后的情况立刻通知相关当事人。

2)对于由订户或依赖方的原因造成的损失，内蒙古网信不承担责任。

3)内蒙古网信只有在其证书有效期限内承担损失损害赔偿。

9.9. 有效期限与终止

9.9.1.有效期限

本CPS自在官网公布之日起生效，除非内蒙古网信特别声明CPS提前终止 。

9.9.2.终止

当新版本的CPS生效时或内蒙古网信终止业务时， 旧版本CPS自动终止；当内蒙古网信终止业务时，内蒙古网信CPS自动终止， 但内蒙古网信将在合同期限内提前通知。

9.9.3.效力的终止与保留

本CPS终止后， 已签发符合本证书策略的证书， 效力作用直到证书到期或撤消;但涉及的审计、保密信息、隐私保护、知识产权、以及涉及赔偿的有限责任条款，在本CPS终止后继续有效。

当由于某种原因，如内容修改、 与适用法律相冲突，证书策略、电子认证服务业务 规则、订户协议、依赖方协议和其他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 。

9.10. 对参与者的个别通告与沟通

内蒙古网信及其注册机构在必要的情况下，如在主动吊销订户证书、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。

9.11. 修订

内蒙古网信有权在合适的时间修订本电子认证服务业务规则中任何术语、条件和条款，而且无须预先通知任何一方。

内蒙古网信有权在内蒙古网信的自主数据库中设置和公布修改结果，或以其他方式(如修改CPS版本的形式或在网站上)公布。所有的修订在公布后立刻生效。

9.11.1. 修订程序

修订程序见1.5.4。

9.11.2. 通知机制和期限

修改后的CPS经批准后将立即在内蒙古网信信息库更新通告栏等官方或授权渠道发布。对于需要 通过电子邮件、信件、媒体等方式通知的修改，内蒙古网信将在合理的时间内通知 有关各方，合理的时间保证有关方面受到的影响最小 。

内蒙古网信保留随时对CPS进行修订的权利，订户应及时留意并查阅更新后CPS。订户在本CPS更新或调整后继续使用证书服务的，表示订户已经充分阅读、理解并接受修改后的内容，也将遵循修改后的内容。

9.11.3. 必须修改业务规则的情形

内蒙古网信员工根据公司业务情况提出，内蒙古网信安委会审批。

9.12. 争议处理

如果各参与方之间无法协商解决出现的问题和争端，可通过法律途径解决。

9.13. 管辖法律

本规则在各方面服从《中华人民共和国电子签名法》、《电子认证服务管理办法》等中华人民共和国法律、规则、规章、法令和政令的约束和解释。内蒙古网信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。

9.14. 与适用法律的符合性

本CPS的使用也必须遵从使用地的相关法律和法规。

9.15. 一般条款

9.15.1.完整协议

CP 、CPS、订户协议及依赖方协议及其补充协议将构成内蒙古网信信任域参与者间的完整协议。

9.15.2.转让

内蒙古网信、 注册机构、订户及依赖方之间的责任、义务不能通过任何形式转让给其他方。

9.15.3.分割性

法律允许的范围内，在内蒙古网信订户协议、依赖方协议和其他订户协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不应该影响协议中其他条款效力 。

9.15.4.强制执行力

无。

9.15.5.不可抗力

当由于不可抗力 ，如地震、洪灾、雷电等自然灾害和战争、政府行为等， 造成内蒙古网信、 注册机构无法提供正常的服务时，内蒙古网信、 注册机构不承担由此给客户造成的 损失。

9.15.6.其他条款

内蒙古网信对本CPS具有最终解释权。

附录一

项目	缩写定义(英文)	缩写定义(中文)
CA	Certification Authority	电子认证服务机构
KMC	Key Management Center	密钥管理中心
RA	Registration Authority	注册审核服务机构
LRA	Local Registration Authority	本地注册受理点
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
CRL	Certification Revocation List	证书吊销列表
OCSP	Online Certificate Status Protocol	在线证书状态协议
PIN	Personal Identification Number	个人身份识别码
CSR	Certificate Signature Request	证书签名请求
PKCS	Public KEY Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公共密钥基础设施
RFC	Request For Comments	请求评注标准(一种互联网建议标准)
X.509		国际电信同盟认证体系的证书标准
IETF	The Internet Engineering Task Force	互联网工程任务组