附件：

国家电子政务外网电子认证业务规则

（第一版）

国家电子政务外网管理中心

二〇一二年四月

目 录

1 概括性描述

1.1 概述

国家电子政务外网电子认证业务规则(以下简称《电子认证业务规则》，CPS)，由国家电子政务外网管理中心电子认证办公室参照《中华人民共和国电子签名法》，按照国家密码管理局《电子政务电子认证服务管理办法》和《电子政务电子认证业务规则规范》，依据工业与信息化部颁布的《电子认证业务规则规范》制订，并报国家密码管理局备案。

2010年，国家发展改革委人事司批准成立“国家电子政务外网管理中心电子认证办公室”，主要职责是负责电子政务外网数字证书认证业务的相关管理、运行和服务工作，是国家电子政务外网电子认证工作统一对外管理和服务窗口。电子政务外网电子认证服务工作由国家电子政务外网数字证书中心（以下简称政务CA，缩写为ZWCA）承担，2011年政务外网数字证书中心获得国家密码管理局颁发的“电子政务电子认证服务机构”（编号B001）资质。政务CA是专业化电子政务证书认证机构，国家政务外网的信息安全基础设施，建有独立密钥管理中心，以密码技术为核心技术，其签发的数字证书是电子政务信息交换中确认身份、控制访问权限，保证信息源真实性、完整性和信息发送不可抵赖性的重要手段。对网络防泄密、抗侵入、拒黑客、识真伪、保信息安全有着不可替代的重要作用。

本规则阐明了政务CA的证书策略开展业务，包括：审批、鉴证、发放、作废、替换、冻结、解冻和更新证书业务的方式和过程、相应的服务、法律和技术上的措施和保障。

国家政务外网数字证书中心负责其注册中心（RA）和服务点（LRA）的建设和运行管理指导。国家政务外网数字证书中心的主要业务内容包括：

（一） 制作、签发、管理证书；

（二） 对签发的证书的真实性进行确认；

（三） 提供证书目录查询服务；

（四） 其他经主管部门核准办理的业务。

利用政务CA签发的证书以及相关PKI技术可以实现以下功能：

（一） 能够确认数据电文签署人的身份；

（二） 能够保证数据电文在传递、接收和储存过程中的完整性；

（三） 能够避免系统被侵入或者人为破坏以及数据电文被篡改；

（四） 能够保证网络信息的安全加密、解密。

国家政务外网电子认证业务规则是政务CA对所提供的全部证书服务生命周期中的业务实践（如发放、审批、作废、更新证书或密钥）所遵循的规范的详细描述和声明，包括责任范围、作业操作规范和信息安全保障措施等内容，是证书管理、证书服务、证书应用、证书分类、证书授权、证书责任等政策规则的集合，主要由以下几部分组成：

（一）概括性描述

（二）信息发布与信息管理

（三）身份标识与鉴别

（四）证书生命周期操作要求

（五）认证机构设施、管理和操作控制

（六）认证系统技术安全控制

（七）证书、证书撤销列表和在线证书状态协议

（八）认证机构审计和其他评估

（九）法律责任和其他业务条款

政务CA认证体系内的实体以及政务CA证书持有者，必须完整地理解和执行国家政务外网电子认证业务规则所规定的条款，承担相应的责任和义务。

1.2 文档名称与标识

本文档名称：《国家政务外网电子认证业务规则》。

本电子认证业务规则在政务CA的网站上予以发布。

1.3 电子认证活动参与者

1.3.1 政务 CA

政务CA是所有国家政务外网RA和实体的根。

政务CA制定政务CA管理文档，各种审计记录和各类表单所形成的日志，其中包括政务CA对外运营策略和规范的管理。并且同时提供5*8管理计划和维护计划。政务CA依法向证书申请者颁发证书、撤销证书、发布证书注销列表等对证书操作的一系列流程，并为政务CA制定出具体政策、管理制度、运作规范和相关的规则。政务CA根据国家相应的法律制定政务CA法律责任书，并有权让证书用户遵守政务CA的规定。政务CA制定财务责任书，并有权让证书用户遵守政务CA的规定。政务CA认证系统采用国际领先的PKI技术，采用双层结构，最高层也就是第一层CA叫做根CA，政务CA称为二级CA用于签发证书。政务CA由数字证书中心（CA）和注册中心（RA）两大部分组成。

1.3.2 注册机构（RA）

国家政务外网证书注册机构（Registration Authority），简称RA，是政务CA授权委托的下属机构，也称国家政务外网服务分中心，是政务CA数字认证体系的一个组成部分，在政务CA的统一领导和集中管理下开展业务活动。

政务CA-RA：指RA服务器设立在政务CA的RA系统，是政务CA直属RA，归政务CA所有，为不建立RA系统、没有RA操作人员的部委或地方提供服务。

各部委或地方RA：指RA服务器设立在部委或地方，归建设方所有，为部委或地方提供服务。

1.3.3 证书持有者

证书持有者，也称为证书用户，指持有政务CA颁发的各类证书且持有与列示于证书中的公钥相对应的私钥的人物对象或单位组织，包括个人、单位、团体、提供国家政务外网服务或享受国家政务外网服务的实体和应用服务器等。

1.3.4 依赖（证书）方

依赖证书中的数据来做决定的用户或代理。

即在政务CA证书服务体系之内作为依赖于证书真实性的实体，在电子签名应用中，为电子

签名依赖方。依赖方可以是也可以不是一个用户。在政务CA体系中，是信任政务CA证书，可以对使用政务CA证书机制进行的数字签名进行验证，使用其他政务CA证书用户的公钥加密信息的实体。

1.3.5 证书使用者

从政务CA接收证书的实体。在电子签名应用中，证书使用者即为电子签名人。指证书和证书相关服务的使用者，目前政务CA的证书在电子政务领域有广泛的应用。

1.3.6 其它参与者

其它参与指政务CA证书服务体系提供相关服务的其它实体或个人。

1.4 证书应用

1.4.1 证书类型及应用范围

政务CA拥有下表所属的证书类型。除政务CA认证业务说明或证书自身禁止，使用政务CA所提供的任何证书应由每个证书申请者自由选择。

政务CA证书种类及应用范围

证书种类	应用范围
个人证书	用于证明个人身份
机构证书	用于证明机构身份
设备证书	用于验证设备，主要用于网站服务器
代码签名证书	用于程序代码签名
认证机构证书	用于证明认证机构

1.4.2 证书禁止使用的情形

政务CA发放的数字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用户自己承担。

1.5 策略管理

1.5.1 策略文档管理机构

本CPS管理机构为国家政务外网数字证书中心，负责 《电子认证业务规则》的制订、发布和更新事宜。

本《电子认证业务规则》由国家政务外网数字证书中心拥用完全版权。

1.5.2 联系人

联系人：政务CA

地址：北京市西城区三里河路58号　　邮编：100045

电话：010 - 68557160

传真：010 - 68558058

电子邮址：cegnca@mx.cei.gov.cn

1.5.3 决定电子认证业务说明符合策略的机构

国家电子政务外网管理中心拥有对政务CA电子认证业务规则的决策权和审批权。

1.5.4 电子认证业务说明批准程序

CPS 批准主要分为计划、编写（修订）、审议和发布四个阶段：

1） 计划：政务CACPS编写组根据相关法律政策和运营策略提出CPS编写（修订）计划。

2） 编写（修订）：由CPS 编写组完成具体条款编写工作。

3） 审议：编写（修订）后的CPS 递交国家电子政务外网管理中心电子认证办公室 审议。

4） 发布：国家电子政务外网管理中心电子认证办公室审议通过后，通过政务CA网站或其他形式正式对外发布。政务CA对CPS的版本号将进行严格控制。若本CPS的变化会极大地影响用户使用政务CA发布的证书和证书撤销列表，则应在30天内通知用户，并增加CPS的版本号；若本CPS的变更不会或很小的影响用户使用政务CA发布的证书和证书撤销列表，则不用改变本CPS版本号也无须通知用户。

1.6 定义和缩写

1.6.1 定义

1) 公钥基础设施（PKI）：是利用公钥加密技术为电子政务的开展提供一套安全基础平台的技术和规范。它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，提供互联网环境的身份鉴别、信息加解密、数据完整性和不可否认性服务。

2) 在线证书状态协议（OCSP）：IETF 颁布的用于检查证书在某一交易时间是否有效的标准。

3) 证书使用者(Subscriber)：被颁发给一个证书的证书主体。

4) 依赖方(Relying party)：证书的接收者，他依赖于该证书和（或）该证书所验证的数字签名。在本标准中，术语“证书使用者”与“依赖方”可互换使用。

5) 唯一甄别名(DN ,Distinguished Name)：在证书的主体名称域中，用来唯一标识用户的X.500 名称。此域需要填写反映用户真实身份的、具有实际意义的、与法律不冲突的内容。

1.6.2 缩略语

DN Distinguished Name 唯一甄别名

LDAP Lightweight Directory Access Protocol 轻量目录访问协议

RA Registration Authority 注册权威

PIN Personal Identification Number 个人识别码

PKI Public Key Infrastructure 公钥基础设施

2 信息发布与信息管理

2.1 认证信息的发布

政务CA在对外的目录服务器中公布证书的相关信息，以定期和定时的方式公布失效证书信息（证书撤销列表CRL）。

在政务CA的网站上发布CPS等相关信息。

2.2 发布的时间或频率

政务CA签发的证书在最终用户收到证书之后立即发布。

政务CA的CRL可以实时发布和定期发布。

CPS在版本更新后立即在网站上更新发布。

2.3 信息库访问控制

在政务CA,只有经过严格授权的CA管理员可以访问CA数据库中的数据；

在政务CA,只有经过严格授权的RA管理员可以访问存储在RA服务器数据库中的数据；

用户可以访问政务CA目录服务器中的数据，没有权限访问CA和RA数据库中的数据。

3 身份识别与鉴别

3.1 命名

3.1.1 名称类型

证书从应用角度分为系统证书和用户证书，命名由用户应用决定。

政务CA证书体系中采用X.500定义的唯一甄别名（DN）标准来唯一标识一张证书使用者的身份信息。

根据证书对应实体的类型不同，政务CA签发的证书的实体名字可以是人员姓名、组织机构名称、部门名称、域名等，命名符合X.500唯一甄别名规定。

在通常情况下，政务CA证书主体的甄别名中的通用名（CN=）部分被鉴别和确认：

1)包含在组织机构身份证书主体甄别名中的通用名是一个机构的法定名称或法定机构中部门的名称。

2）包含在服务器证书主体甄别名中的的通用名一般是一个该组织机构拥有或授权使用的域名。

3）个人证书的通用名是这个人的通常被接受的名字。

3.1.2 对名称有意义的要求

政务CA签发的证书所包含的名称具有通常理解的语义，用它可以确定证书主体中的个人、组织机构或设备的身份。

3.1.3 证书持有者的匿名或伪名

证书持有者不能使用匿名或伪名申请证书。

3.1.4 理解不同名称形式的规则

依X.500甄别名命名规则解释。

3.1.5 名称的唯一性

政务CA签发给某个实体的证书，其主体甄别名，在该CA信任域内是唯一的，其中的例外是签发双证书时（一个签名证书、一个加密证书），属于同一实体的两个证书具有同样的主体甄别名，但证书的密钥用法扩展项不同。

3.1.6 商标的识别、鉴别和角色

证书持有者不应在其证书申请中使用侵害他人知识产权的名称，但政务CA并不决定证书申请

者是否具有相关知识产权，也无需判断、裁决或解决任何关于域名、名称、商标、服务标的争端问题。当出现此类争端时，政务CA有权拒绝或挂起证书申请，直到争端得到有效解决。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

政务CA通过使用经数字签名的PKCS#10格式的证书请求，或其它相当的密码格式，或其他政务CA批准的方法，验证证书申请者拥有私钥。

如果政务CA代表证书持有者产生一个密钥对（如，将产生的密钥对放置到智能卡上），那么，这个要求不适用。

3.2.2 组织机构身份的鉴别

对于组织机构证书，包括组织机构身份证书、组织机构代表人证书、认证机构证书、服务器证书与代码签名证书，是签发给一个组织机构，或一个组织机构代表人，或一个组织机构拥有的服务器，或一个组织机构拥有的程序，对这类证书的签发，无论是政务CA审批，还是通过注册机构审批，政务CA及其注册机构必须按照《国家政务外网数字证书审批管理规范》的要求对证书持有者所在组织机构进行身份鉴别，包括如下两方面内容：

1）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，如事业单位法人证书、组织机构代码证等。

2）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。确认的方式可以是通过可靠的第三方途径，获得组织机构有关申请及授权事宜的确认。当证书中包含某个人（作为该组织的授权代表）的名字时，则此人的雇佣关系和他/她代表组织的权威性也应得到确认。

3.2.3 个人身份鉴别

对于所有类型的个人证书，政务CA或注册机构确认：

1）证书持有者确实存在；

2）证书持有者是证书申请中所说的那个人；

3）按照§3.2.1，确认证书持有者拥有与证书中所列公钥相对应的私钥；

4）除了未经验证的证书持有者信息，包含在证书中的信息是准确的；

具体鉴别过程按照《国家政务外网数字证书审批管理规范》执行。

3.2.4 没有验证的证书持有者信息

政务CA不对下列证书持有者信息进行验证：

1）组织机构的单元（OU）；

2）证书中指明不验证的其他信息。

3.2.5 授权确认

对于组织机构证书，政务CA在签发前，将确认证书持有者获得正当授权。确认的方式有多种，如通过可信第三方获得证书持有者所在组织机构电话号码，然后联系组织机构的有关人员，确认证书持有者获得了所在组织机构的授权。

3.3 密钥更新请求的标识与鉴别

在证书持有者证书到期后，证书持有者需要对原有证书进行更新。政务CA要求证书持有者产生一个新的密钥对代替过期的密钥对，称作“密钥更新”，在密钥更新时，证书持有者证书的DN没有改变。若证书持有者为一个现存的密钥对申请一个新证书，则称为“证书更新”。

政务CA产生一个新的密钥对代替过期的密钥对的过程，作为密钥更新请求的标识。在接到密钥更新请求时，政务CA下属RA注册机构应当对用户公钥和用户信息的真实性与合法性进行鉴别。

3.3.1 常规密钥更新的标识与鉴别

密钥更新前后，证书持有者的证书DN不改变，仍然作为新密钥的标识。

总体而言，政务CA的证书签发模式可分为“证书持有者自主生成模式”与“管理员生成模式”两种。“证书持有者自主生成模式”是指在政务CA或注册机构将用户证书签发后，证书持有者通过客户端自行将用户证书下载至证书存储介质（USB Key）中的操作方式；而“管理员生成模式”是指政务CA或注册机构的系统管理员在用户证书签发后直接将用户证书下载至对应的证书存储介质（USB Key）中并交付证书持有者的操作方式。对应这两种证书签发模式，政务CA在进行密钥更新时分别所需要的更新依据如下：

1）对于将通过“证书持有者自主生成模式”来获取更新证书的证书持有者，在进行证书密钥更新时，证书持有者可访问政务CA或其注册机构的证书服务站点相应的服务网页进行密钥更新申请。系统将自动获取证书持有者原证书相关信息，如证书持有者甄别名、证书序列号等，形成证书密钥更新申请信息，此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）。

政务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别。

2）对于将通过“管理员生成模式”来获取更新证书的证书持有者，在进行证书密钥更新时，证书持有者需向政务CA提供书面申请和原有的证书及存储介质（USB Key），政务CA将以此做为密钥更新的依据，然后再进行与新证书申请一样的鉴别。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后的密钥更新等同于证书持有者重新申请证书，申请流程见本CPS 4.2之规定。

3.4 吊销请求的标识与鉴别

在政务CA的证书业务中，证书吊销请求可以来自证书持有者，也可以来自政务CA或注册机构。证书吊销的方式可以是证书持有者自己吊销，也可以由证书持有者要求政务CA或注册机构管理员吊销，政务CA和注册机构在认为必须的时候，有权发起吊销证书持有者证书。

1） 在证书持有者自己吊销时，可接受的鉴别过程如下：

证书持有者在申请吊销证书时需提交挑战语，如果挑战语匹配，则证书吊销自动完成。

2） 证书持有者通过认证机构、注册机构吊销时，可接受的鉴别过程如下：

证书持有者通过一定的方式，如邮件、传真、电话等，向认证机构、注册机构提交请求，认

证机构、注册机构通过与证书保障级别相应的通讯方式与证书持有者联系，确认要吊销证书的人或组织确实是证书持有者本人。依据不同的环境，通讯方式可以采用下面的一种或几种：电话、传真、e-mail、邮寄或快递服务。

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

在国家电子政务外网范围内的任何单位机构的相关人员、设备、机构等需要在国家政务外网应用中进行基于证书的身份鉴别、需要采用数字签名及实现信息加密时，可向政务CA或下属RA注册机构提出证书申请。

个人证书由证书使用者本人或所在机构提出申请；机构证书由机构授权的人员申请；设备证书由域名拥有机构或个人、或被授权使用该域名的机构中的被授权人申请；代码签名证书由软件开发者本人或软件开发商授权的人员提出申请。具备完全行为能力的个人、单位用户及其认可的职能部门。认证机构证书由认证机构授权的人员申请。

4.1.2 注册过程与责任

证书持有者可到政务CA相应的证书注册服务站点和下属RA注册机构的证书注册服务站点注册申请证书。注册时证书持有者须填写证书申请表，并准备相关的身份证明材料。政务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。

申请过程中各方责任为：

证书持有者需明确表示其愿意接受证书申请协议中所规定的相关责任与义务，如需提供证书申请材料，并确保申请材料的真是准确等（具体要求见本CPS9.6.3所述）；

政务CA与注册机构负责接收证书申请人的请求材料，并通过现场审核或非现场审核的方式对证书持有者所提供的证书申请信息与身份证明资料的一致性进行查验。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

政务CA或注册机构按照本CPS的规定，对申请者提供的信息进行真伪鉴别，然后按CPS§3.2.2与3.2.3 所描述的过程对申请人的身份进行识别与鉴别。具体的鉴别流程详见§3.2.2 组织身份的鉴别和 3.2.3 个人身份的鉴别。

4.2.2 证书申请批准和拒绝

在政务CA或注册机构完成对证书申请的鉴别，有关鉴别获得通过并且证书申请者履行了其他应尽的责任后，政务CA或注册机构将会批准证书申请。

如果鉴别未获通过或证书申请者拒绝履行其他应尽的责任，政务CA或注册机构将会拒绝证书申请，并通知证书申请者鉴别失败，同时向证书申请者提供失败的原因(法律禁止的除外)。被拒绝的证书申请者可以在准备正确的申请材料或履行了其他应尽的责任后，再次提出申请。

4.2.3 处理证书申请的时间

政务CA及下属注册机构将在合理的时间内完成证书申请处理。在申请者提交的资料齐全且

符合要求的情况下，处理证书申请的时间不超过5个工作日。

4.3 证书签发

4.3.1 证书签发过程中政务 CA 和 RA 注册机构的行为

作为证书认证系统的运行者，国家政务外网是一个 CA，同时国家政务外网建设了 RA 系统提供证书零售服务。国家政务外网的注册机构在接受、处理证书请求时担当 RA的角色。

在证书签发前RA管理员负责证书申请的鉴别，在证书申请通过鉴别后，RA 管理员将批准证书请求。为了批准证书申请，RA管理员将使用证书登录到 RA 系统，查询系统记录的有关请求或上传证书申请请求与证书信息，并批准证书申请请求。批准的信息将会发送到国家政务外网的CA系统，CA系统签发证书并返回给RA系统供证书持有者或RA管理员下载。

4.3.2 政务 CA 和 RA 注册机构对证书持有者的通告

无论是拒绝还是批准证书持有者的证书申请，政务CA或下属注册机构都有义务告知证书持有者申请结果，告知的方式有以下几种：

1) 通过RA系统向证书持有者自动发送通知邮件。如果证书申请获得批准，邮件中将包含获取证书的信息。

2) 通过书面或通信方式，通知证书持有者前往政务CA或下属注册机构领取数字证书，或与证书持有者确认数字证书的邮寄地址；如果为“前往领取数字证书”，则政务CA或下属注册机构将会把密码信封和证书等直接提交给证书持有者，以此来通知证书持有者证书信息已经正确生成；

3) 通过其他政务CA认为安全可行的方式通知证书持有者。

4.4 证书接受

4.4.1 构成接受证书的行为

政务CA证书持有者接受证书的方式可以有如下三种：

1) 证书持有者根据电子邮件中获取证书的的指示，访问专门的证书下载服务站点将证书下载到本地存放介质，如本地计算机硬盘、USB Key、智能卡。认证系统会记录证书持有者已下载证书。

2) 通过面对面的提交，即证书持有者前往政务CA或下属注册机构领取载有证书和私钥的介质。在这种情况下由政务CA或注册机构代替证书持有者产生证书请求、证书密钥对、下载证书。

3) 通过邮寄的提交，即政务CA或注册机构将载有证书和私钥的介质通过邮寄方式向证书持有者进行发放。在这种情况下同样由政务CA或注册机构代替证书持有者产生证书请求、证书密钥对、下载证书。

对于第一种方式，系统记录证书持有者下载了证书即表明证书持有者接受了证书。而对于第二和第三种方式，当证书持有者接受了载有证书的介质即表明证书持有者接受了证书。

4.4.2 政务 CA 对证书的发布

政务CA将在其信息库、目录服务中和由政务CA决定的其它一个或多个信息库里发布证书的副本。证书持有者也可以在其它场所公布他们的证书。

4.4.3 政务 CA 对其他实体的通告

证书持有者、依赖方可以通过政务CA目录服务、政务CA网站等查询自己或他人的证书。

4.5 密钥对和证书的使用

4.5.1 证书使用者私钥和证书的使用

证书持有者使用证书时，必须妥善保管和存储与证书相关的私钥，避免遗失、泄露、被篡改或者被盗用。任何人使用证书时都必须检验证书的有效性。

在使用与政务CA所签发的证书有关的签名及经过签名的信息时，参与方（政务CA、证书持有者和依赖方等）按本CPS 的规定享有相应的权利和应尽的义务。参与方均视为已被通知并同意遵守本CPS 以及政务CA与各方签署的协议、规范中的条款。任何超出本CPS 的规定的证书及私钥的使用，政务CA将不承担任何由此产生的责任和义务。

政务CA签发的各类证书，仅用于表明证书持有者在申请证书时所要标识的身份，以及验证证书持有者用于该证书包含的公钥相对应的私钥做出的签名。这样，通过签名和签名的验证，保证证书持有者的身份真实性、信息的完整性、信息的不可抵赖性等。如果证书持有人将该证书用于其它用途，政务CA将不承担任何由此产生的责任和义务。如果证书中的某些字段明确了证书的使用范围和用途，那么该证书将在也只被允许在这一范围内使用。任何超出证书所标明的适用范围内的行为，都将由行为人独立承担责任。政务CA对超出适用范围内的任何使用行为，不承担任何由此产生的责任和义务。

4.5.2 依赖方公钥和证书的使用

在信任证书和签名前，依赖方要独立地作出应有的努力和合理的判断。除非本CPS 另有规定，证书并不是来自发证机构的对任何权利或特权的承诺。依赖方在本CPS 规定的范围内信赖证书和证书中包含的公钥，并对此做出决定。

如果证书中的某些字段明确了证书的使用范围和用途，那么该证书也只被允许在这一范围内进行使用。依赖方必须对此做出合理的判断，任何对超出证书所标明的适用范围的行为的信赖，都将由依赖人独立承担责任，政务CA对此不承担任何责任和义务。

4.6 证书更新

证书更新指政务 CA 在不改变证书中证书持有者公钥的情况下，为政务 CA 电子签名认证证书持有者签发一张新证书。为确保证书及其密钥对的安全有效性，政务 CA 会为所签发的证书设置有效期，以保证证书持有者的权利。如果证书持有者需要更新证书，必须在证书有效终止日期前一个月内到政务 CA 办理。更新证书时发证机构将根据证书持有者的要求决定新证书是否使用原证书密钥。

4.6.1 证书更新的情形

在证书有效期到期前，如果证书持有者原来的注册信息继续有效，证书持有者可访问政务CA或下属的注册机构的证书更新站点申请证书更新，或可到政务CA与下属的注册机构申请证书更新。证书更新的具体情形如下：

1) 证书的有效期将要到期；

2) 密钥对的使用期将要到期；

3) 因加密密钥的丢失、损坏或泄漏导致原证书被吊销且还有证书使用需求；

4）其他。

4.6.2 请求证书更新的实体

政务CA信任体系内的证书持有者均可向政务CA申请更新持有的证书。包括：由政务CA签发的原有证书有效期限未到的个人、单位、设备、机构等提供网上服务和享受网上服务的各种实体，以及其他凡是政务CA各类证书（包括测试证书）的有效期限未到的证书持有者。

4.6.3 证书更新请求的处理

对于不更换密钥的证书更新请求，国家政务外网认证系统会自动完成如下验证操作：

1）申请对应的原证书存在并且由认证机构签发；

2）证书更新请求在允许的期限；

3）用原证书上的证书持有者公钥对更新申请的签名进行验证。

在此基础上，政务CA或下属RA注册机构按与初次证书申请一样的鉴别过程完成证书更新请求的鉴别，然后批准、签发证书。

对于更换密钥的证书更新，参见 4.7.3。

4.6.4 签发新证书时对证书持用者的通告

签发新证书时对证书持用者的告知同本CPS4.3.2之规定。

4.6.5 构成接受更新证书的行为

构成接受更新证书的行为同本CPS4.4.1之规定。

4.6.6 政务 CA 对更新证书的发布

更新证书的发布同本CPS4.4. 2之规定。

4.6.7 政务 CA 对其他实体的通告

政务CA对其他实体的告知同本CPS4.4.3之规定。

4.7 证书密钥更新

证书密钥更新是指证书持有者需要生成新密钥并申请为新公钥签发新证书。

4.7.1 证书密钥更新的情形

证书密钥更新有两种情况：补发和换发。补发是指在证书有效期内，证书持有者更新证书（密钥）的操作，补发操作成功时，旧证书将被吊销，新证书有效期从补发成功之日起到旧证书失效日止。换发是指在证书将要过期的三个月内或证书过期后，证书持有者申请更换证书（密钥）的操作，换发操作成功时，旧证书将被吊销，新证书有效期将从证书换发之日起加一个证书有效周期（已经过期的证书换证，其有效期仅为证书有效期）。补发和换发时，证书DN均不改变。

以下情况证书持有者需要申请证书补发：

1）证书持有者忘记或泄漏了证书使用口令；

2）证书持有者证书（文件）丢失或损坏，例如存放证书的介质损坏；

3）证书持有者认为原有证书和密钥不安全（例如证书持有者怀疑证书被盗用或密钥受到了攻击）。

以下情况证书持有者需要申请证书换发：证书持有者证书到期或已经过期。

当证书持有者忘记电子钥匙口令时，使用者提供有效身份或单位证明后，可申请口令解锁。

4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体与本CPS4.6.2中的证书申请实体相同。

4.7.3 证书密钥更新请求的处理

对于证书密钥的更新，证书持有者须提交能够识别原证书的足够信息，如证书持有者甄别名、证书序列号等，使用更新前的私钥对包含新公钥的申请信息签名，在此基础上，政务CA或下属RA注册机构将执行下述操作：

1) 申请对应的原证书存在并且由认证机构签发；

2) 用原证书上的证书持有者公钥对申请的签名进行验证；

3) 基于原注册信息进行身份鉴别。

4.7.4 签发新证书时对证书使用者的通告

签发新证书时对证书使用者的告知同本CPS第4.3.2之规定。

4.7.5 构成接受密钥更新证书的行为

构成接受密钥更新证书的行为同本CPS第4.4.1的规定。

4.7.6 政务 CA 对密钥更新证书的发布

政务CA在签发证书的同时会将密钥更新证书发布到对外目录服务器上进行公开；同时将旧证书序列号发布到CRL列表中。

政务CA系统在签发密钥更新证书的同时会将证书发布到对外目录服务器上进行公开；同时将旧证书序列号发布到CRL列表中。CA中心发布在CRL和在线证书状态查询服务器中。

4.7.7 政务 CA 对其他实体的告知

政务CA对其他实体的告知同本CPS4.4.3之规定。

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未到期之前，更改除公钥及有效期之外的其他信息。政务CA的认证业务不直接支持证书变更。证书持有者要变更证书中的内容时，视为申请一张新证书，需要先将原有证书吊销，才能申请新证书，且证书的申请及处理流程与申请新证书一致。

4.8.2 请求证书变更的实体

无规定。

4.8.3 证书变更请求的处理

无规定。

4.8.4 签发新证书时对证书持有者的通告

无规定。

4.8.5 构成接受变更证书的行为

无规定。

4.8.6 政务 CA 对变更证书的发布

无规定。

4.8.7 政务 CA 对其他实体的通告

无规定。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

出现下列情况之一，政务CA将强制吊销所签发的证书：

1）当政务CA或下属注册机构发现证书持有者申请证书时提供的资料不真实；

2）证书持有者未履行证书服务责任约定的义务；

3）当政务CA或下属RA注册机构发现证书持有者主体消亡；

4)根据法律法规或司法部门的要求,政务CA或下属RA注册机构对证书持有者证书进行吊销；

5）证书持有者声明不再使用证书并要求政务CA或下属RA注册机构予以吊销；

6）证书持有者相信或怀疑密钥泄漏或遭受攻击，要求吊销证书；

7）数字证书中的信息发生重大变更；

8）证书持有者认为本人不能实际履行数字证书认证业务规则。

吊销分为主动吊销和被动吊销。主动吊销是指由证书持有者提出吊销申请，由RA 审核通过后吊销证书的情形；被动吊销是指当政务CA或下属RA注册机构确认证书持有者违反证书应用规定、约定或证书持有者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。当出现上述提到的第1-4种情况时，适用于被动吊销，5-8种情况适用于主动吊销。

4.9.2 请求证书吊销的实体

在符合本CPS4.9.1所述的情形下，请求证书吊销的实体与本CPS4.1.1证书申请实体相同。

另外，政务CA及下属RA注册机构也可以在本CPS4.9.1所述的相关情形下主动提出吊销证书的请求。

4.9.3 吊销请求的流程

当最终证书持者有吊销证书的需求时，证书持有者可按照以下流程申请吊销证书：

1) 证书持有者通过书面或通信方式向政务CA或下属RA注册机构提出吊销证书请求；

2) 证书持有者根据政务CA或下属RA注册机构的要求，填写并提交书面申请表；

3) 政务CA或下属RA注册机构在验证了申请者身份的真实性、吊销理由的正当性及书面申请表的有效性后将吊销证书持有者的证书；

4) 证书持有者证书被吊销后，政务CA或下属RA注册机构将通过适当的方式，包括邮件、传真等，通知证书持有者证书已被吊销，并会及时将证书吊销信息发布到政务CA或下属RA注册机构信息库和目录服务。

当政务CA或下属RA注册机构有充分的理由相信需要吊销证书持有者的证书时，政务CA或下

属RA注册机构的有关人员可以通过内部确定的流程提请吊销证书。在证书吊销后，政务CA或下属RA注册机构将会通过适当的方式通知该证书持有者。

4.9.4 吊销请求宽限期

证书持有者一旦发现需要吊销证书，应向发放该证书的注册机构及时提出吊销请求。如果出现私钥泄露等事件，吊销请求必须在发现泄露或有泄露嫌疑8 小时内提出。其他吊销原因的吊销请求必须在24小时内提出。

4.9.5 政务 CA 处理吊销请求的时限

政务CA或下属RA注册机构从收到吊销请求到审核完成，做出吊销决定并将吊销证书发布到目录服务，全部工作应当在24小时内完成。从证书持有者正式提出证书吊销申请到证书正式吊销前24小时内因使用该证书造成的损失，政务CA或下属RA注册机构不予承担。

说明：证书持有者在正式提出证书吊销申请后不得在工作中继续使用此证书，否则由此产生的后果，由证书持有者自行承担。证书持有者在正式提出证书吊销申请后必须立即将此情况通知与此证书相关的依赖方，以便在工作中停止使用该证书，否则由此产生的后果，由证书持有者自行承担。

4.9.6 依赖方检查证书吊销的要求

依赖方应当检查他们所信任的证书是否被吊销。检查方式是通过查询政务CA发布的CRL完成。

4.9.7 CRL 发布频率

CRL发布频率为24小时一次，在发布的同时对原有内容进行更新。

4.9.8 CRL 发布的最大滞后时间

CRL发布的最长滞后时间为24小时。

4.9.9 在线状态查询的可用性

政务CA向证书持有者及依赖方提供的7*24小时的CRL服务。

4.9.10 在线状态查询要求

依赖方在信赖一张证书前必须对此证书进行证书状态查询，查询方式为检查CRL，政务CA没有设置任何读取权限。

4.9.11 吊销信息的其他发布形式

除了CRL外，政务CA所发布的吊销信息也可通过政务CA的OCSP来查询和获得。

4.9.12 密钥损害的特别处理要求

无论是证书持有者还是政务CA、注册机构，发现证书密钥受到安全损害时应立即吊销证书。

4.9.13证书挂起的情形

无规定。

4.9.14请求证书挂起的实体

无规定。

4.9.15挂起请求的流程

无规定。

4.9.16挂起的期限限制

无规定。

4.10 证书冻结

4.10.1 证书冻结的情形

证书仍处于有效期，为了保留证书持有者的证书使用权利，而不申请吊销该证书，当出现下列情况时，可以进行证书冻结：

1. 证书持有者要求暂停使用该证书一段时间；

2. 证书持有者未能履行与政务CA签订的协议中应尽的义务，但向政务CA提出申请并获得批准后；

3. 除证书持有者（或者其授权的委托代理人）外的其它实体，如政务CA或下属RA注册机构、法院、政府主管部门及其他公共权利部门，向政务CA提出冻结证书请求并获得批准。

4.10.2 请求证书冻结的实体

在符合本CPS4.10.1所述的情形下，请求证书冻结的实体与本CPS4.1.1证书申请实体相同。

另外，政务CA、下属RA注册机构、法院、政府主管部门及其他有关部门等也可以在本CPS4.10.1所述的相关情形下主动提出证书冻结的请求。

4.10.3 证书冻结与解冻流程

当最终证书持者有冻结或解冻证书的需求时，证书持有者可按照以下流程申请冻结或解冻证书：

1) 证书持有者通过书面或通信方式向政务CA或下属RA注册机构提出冻结或解冻证书的请求；

2) 证书持有者根据政务CA或下属RA注册机构的要求，填写并提交书面申请表；

3) 政务CA或下属RA注册机构在验证了申请者身份的真实性、冻结或解冻理由的正当性及书面申请表的有效性后将冻结或解冻证书持有者的证书；

4) 证书持有者证书被冻结或解冻后，政务CA或下属RA注册机构将通过适当的方式，包括邮件、传真等，通知证书持有者证书已被冻结或解冻，并会及时将证书冻结或解冻信息发布到政务CA或下属RA注册机构信息库和目录服务。

当政务CA或下属RA注册机构有充分的理由相信需要冻结证书持有者的证书时，政务CA或下属RA注册机构的有关人员可以通过内部确定的流程提请冻结证书。此外，当法院、政府主管部门及其他有关部门等如有充分的理由证明需要冻结证书持有者的证书时，则法院、政府主管部门及其他有关部门等也需按规定填写书面申请表并提交证明材料。在证书被冻结后，政务CA或下属RA注册机构将会通过适当的方式通知该证书持有者。

4.10.4 冻结的期限限制

证书冻结后，如证书持有者没有在规定时间内申请解冻、吊销或恢复等其他证书相关业务，

政务CA将对该证书做吊销处理。

证书冻结的最长时间是6个月，如果没有接到证书持有者的解冻或其他申请，该证书将被废除。如证书冻结时间内到达有效期，政务CA也将废除该证书。

4.11 证书状态服务

政务 CA 中证书状态可以通过 LDAP 目录查询和 OCSP 查询服务获得。

4.11.1 操作特征

政务CA提供的证书状态查询以网络服务的形式。证书目录LDAP 符合LDAP V3（RFC3377，2251-2256，2829-2830）。OCSP 符合 RFC2560，反映证书的当前状态。

4.11.2 服务可用性

政务CA提供7*24小时不间断证书状态查询服务。

4.11.3 可选特征

无。

4.12 证书持有终止

以下三种情形将被视为证书持有终止：

1)证书持有者在证书到期后两周内没有提出对证书密钥进行更新,将被视为证书持有终止。

2）在证书有效期内，证书持有者主动提出对证书进行吊销视为证书持有终止，政务CA将按照“证书吊销流程”处理证书持有者申请。

3）被动吊销视为证书持有终止。

4.13 口令解锁

当证书持有者忘记电子钥匙口令时，使用者提供有效身份或单位证明后，申请口令解锁。

4.14 密钥生成、备份与恢复

4.14.1 密钥生成、备份与恢复的策略和行为

证书持有者的签名密钥对由证书持有者的密码设备（如智能 USB KEY）生成与保存，加/解密密钥对由国家设立的专门密钥管理机构（KMC，密钥管理中心）生成。目前KMC托管在国家信息中心，系统每天对数据进行备份。

密钥恢复是指加密密钥的恢复，是一种严格受控的过程，只有在如下情况下才允许进行密钥恢复：

1）证书持有者提出申请；

2）注册机构提出申请，并有充分的理由；

3）国家执法、司法机构因执法、司法的需要；

4）国家其他管理部门管理需要。

密钥恢复只有在必须的情况下才进行，并且申请要提出充分的理由和提供有关文件、材料。

4.14.2 会话密钥的封装与恢复的策略与行为

会话密钥是指用户在使用证书建立加密通道时临时生成的加密密钥，该密钥由应用环境来决定使用，国家政务外网不对其进行保存和恢复。

5 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

政务CA位于国家信息中心主楼内，进入机房须经过三道审核，机房电磁屏蔽指标达到BMB二级敏感区域和通信的安全标准。机房具备抗震、防火、防水、恒湿温控、独立供电、备用发电、门禁控制、视频监控等功能，可保证认证服务的连续性和可靠性。

5.1.2 物理访问

外来人员进入机房，需经过政务外网管理中心电子认证办公室和国家信息中心保卫保密处审核同意。支持政务CA系统的服务设施，如配电盘、通讯与电话间、通风以及空调系统都采取严格的保护措施，限制人员的随意进入。整个楼宇和机房设备区设有录像监控系统，实行24小时实时监控。

操作人员进入CA机房，须经过指纹认证、密码、门禁授权卡等身份认证，并有24小时视频监控设备进行监控。

5.1.3 电力与空调

政务CA采用两路供电措施，并使用UPS提供电力保护，同时还考虑了应急环境设施。

政务CA机房采用中央空调和新风设备，保证机房内温度和湿度达到国家标准（GBJ19-87《采暖通风与空气调节设计规范》、GB50174-93 《电子计算机机房设计规范》）。

5.1.4 水患防治

政务CA要有专门的技术措施防止、检测漏水的出现，并能够在出现漏水时最大程度地减小漏水对认证系统的影响。

5.1.5 火灾防护

政务CA的电器系统要符合电子数据处理设备的防火标准、组织政策、职业安全与保健法等。机房内要配备自动火情警报及处理装置。

5.1.6 介质存储

政务CA的存储介质包括硬盘、磁带等，介质存储地点和政务CA系统分开，并且保证物理安全，注意防磁、防静电干扰、防火、防水，由专人管理。

5.1.7 废物处理

废弃纸介质实行专人负责，不可还原处理，其他介质以不可恢复原则进行相应的销毁处理。对于硬件设备必须销毁存储介质后方可搬出CA机房。

5.1.8 异地备份

为了提高灾难恢复的时间和质量及安全信息的保密性，审计日志等关键数据，及其它敏感数据应进行备份，并异地保存。

5.1.9 注册机构物理控制

政务CA下属的注册机构的物理场地也需要有足够的安全措施，保证只有授权的人员才能进

入，只有授权的人员才能接触系统进行证书管理。

5.2 程序控制

5.2.1 可信角色

政务CA可信角色包括：

- 安全管理员
- 密钥管理员
- 系统管理员
- 网络管理员
- 数据库管理员
- 系统维护组长
- 业务管理员
- 业务操作员
- 客服人员

5.2.2 每项任务需要的人数

政务CA制定了规范和策略，严格控制任务和职责的分割，对于最敏感的操作，例如访问和管理CA的加密设备及其密钥，需要3个可信角色。

其它操作，例如发放证书，需要至少2个可信角色。

政务CA对于人员有明确的分工，贯彻多人控制、互相监督的安全机制。

5.2.3 每个角色的识别与鉴别

所有政务CA的在职人员，按照所担任的角色的不同进行身份鉴别。对于物理访问控制，政务CA通过门禁磁卡、指纹识别、密码鉴别不同人员，并确定相应的权限。

政务CA对可信角色进行识别与鉴别，是通过其使用的基于USB Key存储的数字证书实现的，系统将独立完整地记录所有操作行为。

5.2.4 要求职责分割的角色

为保证系统安全，遵循关键岗位职责分割的原则，即由不同的可信角色去担任重要操作。任何密钥恢复的操作，都需要至少两人以上的人员来完成，而密钥分割和合成技术对操作人员来说是保密的。要求职责分割的角色包括（但不限于）以下几种：安全管理员、系统管理员、网络管理员、操作员。

5.3 人员控制

5.3.1 资格、经历和无过失要求

成为政务CA可信角色的人员必须提供相关的背景、资历证明，并具有足以胜任其工作的相关经验，且没有相关的不良记录。

5.3.2 背景审查程序

政务CA在雇佣人员担任可信任角色前，会依据以下流程对其进行审查：

1）应聘者提交的个人资料

最高学历毕业证书、学位证书、资格证及有效身份证件原件等相关的有效证明和履历。

2）应聘者个人身份的确认

政务CA人力资源部门通过电话、信函、网络、走访、调阅档案等形式对其提供材料的真实性进行鉴定。

3）三个月的试用期考核

通过现场考试、日常观察、情景考验等方式对其考察。

以上三方面的审查结果必须符合第5.3.1节中规定的要求。

5.3.3 培训要求

政务CA对录用人员按照其岗位和角色安排培训。培训内容有：PKI的相关知识、岗位职责、内部规章制度、认证系统软件、相关应用软件、操作系统与网络、CPS等。并且保证对所有员工进行不定期的安全意识教育和培训，增强安全意识和工作责任感。

5.3.4 工作岗位轮换周期和顺序

政务CA根据具体工作情况安排并制定员工工作岗位的轮换周期与顺序。

5.3.5 未授权行为的处罚

员工一旦被发现执行了未经授权的操作时，将被立即中止工作并受到纪律惩罚，其处理办法根据政务CA相关的管理规范执行。

5.3.6 提供给员工的文档

为保证系统的正常运行，政务CA根据员工的不同角色提供其工作所必须的培训和相关的文档。

5.4 审计日志程序

政务CA中心的审计日志由运维部门统一保存，定期备份，备份介质分别存放在政务CA中心及异地存储中心。一旦出现审计纠纷，需要对审计日志提出复查，应由用户向证书发放部门申请，经负责人同意后，由运维人员查询。

5.4.1 记录事件的类型

1、CA密钥生命周期内的管理事件，包括密钥生成、备份、恢复、归档和销毁。

2、RA系统记录的证书持有者身份信息，包括机构名称、个人姓名、证件号码、地址、邮箱、联系人等信息。

3、证书生命周期中的各项操作，包括证书申请、证书批准、证书密钥更新、证书撤销等事件；

4、系统、网络安全记录，包括入侵检测系统的记录、系统日常运行产生的日志文件、系统故障处理工单、系统变更工单等；

5、人员访问控制记录；

6、系统巡检记录；

7、政务CA中心物理环境巡检记录；

8、事故处理记录。

上述日志信息包括记录时间、序列号、记录的实体身份、日志种类等。

5.4.2 处理日志的周期

对于CA密钥和证书持有者证书生命周期内的管理事件日志，政务CA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，政务CA每周进行一次检查、处理。

对于物理设施的访问日志，政务CA每月进行一次检查、处理。

对事件处理记录每半年进行一次内部检查、审计。

5.4.3 审计日志的保存期限

审计日志每月形成新的归档文件，交由相关部门保存归档，审计跟踪文档至少保存二年，密钥和证书信息档案至少保存到证书失效后五年。

5.4.4 审计日志的保护

建立完善的管理制度，并采取物理和逻辑的控制方法确保只有经政务CA授权的人员才能对审计日志进行操作。审计日志处于严格的保护状态，并且有异地备份，严禁未经授权的任何操作。

5.4.5 审计日志备份程序

审计文档由管理员每周进行一次归档。所有文档包括最新的审计跟踪文档需储存在磁盘中并存放在安全的文档库内并进行备份。

5.4.6 审计收集系统

应用程序、网络和操作系统等都会自动生成审计数据和记录信息。

5.4.7 对导致事件实体的告知

对于审计收集系统中记录的事件，对导致该事件的个人、机构等主体，政务CA不进行告知。

5.4.8 脆弱性评估

根据审计记录，政务CA和RA要定期进行系统、物理设施、运营管理、人事管理等方面的信息安全脆弱性评估，并根据评估报告采取措施。

5.5 记录归档

日志记录由系统定期归档，由运维人员每天复查，每周由运维人员进行有效性验证，以检查归档记录是否可用。

5.5.1 归档记录的类型

政务CA对审计数据、证书用户公开身份信息、CA系统数据和目录服务数据、密钥历史等记录归档保存。

5.5.2 归档记录的保存期限

自证书期满或撤销之日起，记录会保存至少5年以上。如果法律需要，政务CA将延长记录保存期限。

5.5.3 归档文件的保护

根据本CPS的存档要求保护存档记录，确保只有被授权的可信任人员才允许访问存档数据，并通过适当的物理和逻辑访问控制防止对电子归档记录进行未授权的访问、修改、删除或其它操作。政务CA将使用可靠的归档数据存储介质和归档数据处理应用软件，确保归档数据在其归档期限内只有被授权的可信任人员才能成功访问。

5.5.4 归档文件的备份程序

系统每天对证书信息进行备份，该备份数据采用物理隔离方式，与外界不发生信息交互。

5.5.5 记录的时间戳要求

归档的记录都需要标注时间；按照操作的实际时间进行记录。

5.5.6 获得和检验归档信息

只有被授权的可信人员才能获得归档信息。当归档信息被恢复后会对其完整性进行检验。

5.6 事故与灾难恢复

5.6.1 事故和损害处理流程

当政务CA遭到攻击、发生通讯网络故障、计算机设备不能正常提供服务、软件遭破坏、数据库被篡改等情况下或因不可抗力造成政务CA主中心机房无法正常提供服务时，政务CA将依据灾难恢复方案实施修复。

政务CA承诺，保证在发生灾难48小时之内恢复CA的目录查询服务，一月之内恢复证书签发和证书管理服务。在数据恢复中，最多允许丢失灾难发生前48小时内的数据。

5.6.2 计算资源、软件、数据的损坏

政务CA对业务系统及其它重要系统的资源、软件、数据进行了备份，并制定了相应的应急处理规范，当出现计算机资源、软件、数据损坏时在最短的时间内恢复被损害的资源、软件、数据。

5.6.3 实体私钥损害处理程序

对于实体私钥的损害，政务CA有如下处理要求和程序:

1、当证书持有者发现实体证书私钥损害时，证书持有者必须立即停止使用其私钥，并立即前往或通过电话、传真、电子邮件等方式通知政务CA或注册机构撤销其证书。

2、当政务CA或下属RA注册机构发现证书持有者的实体私钥收到损害时，政务CA或下属RA注册机构将立即撤销其证书，并通知证书持有者，证书持有者必须立即停止使用其私钥。

3、当政务CA的CA证书出现私钥损害时，政务CA将立即撤销CA证书并及时通知依赖方，然后生成新的CA密钥对、签发新的CA证书。

5.6.4 灾难后的业务连续性能力

政务CA拥有一套较为完善的系统恢复办法，建设有适当的测试系统以恢复所备份的数据和配置文件，除非物理场地出现了毁灭性的、无法恢复的灾难，政务CA能够在出现灾难后最短的时间内恢复其业务能力。

5.7 政务 CA 或注册机构的终止

当政务CA及下属RA注册机构需要停止其业务时，将会严格按照国家的相关法律及规定执行。

6 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

加密密钥对：由国家密码管理局许可的、政务CA证书签发系统支持的加密机设备生成。

签名密钥对：证书申请者可使用国家密码管理局认可的、政务CA证书签发系统支持的介质生成签名密钥对。签名私钥存储在介质中不可导出，保证无法复制。

设备证书的密钥对：由证书持有者自己产生，证书持有者应妥善保管。

政务CA在技术、流程和管理上保证密钥对产生的安全性。

6.1.2 私钥传送给证书使用者

证书持有者的加密私钥是在密钥管理中心（KMC）产生，该私钥只保存在KMC 和证书持有者介质中。在加密私钥从KMC 到证书持有者的传递过程中采用国家密码管理局许可的对称密钥算法加密。政务CA无法获得，保证了证书持有者的密钥安全。

6.1.3 公钥传送给证书签发机构

政务CA从KMC 取得证书持有者公钥后为其签发证书，在此过程中也采用国家密码管理局许可的对称密钥算法加密，保证传输中数据的安全。

6.1.4 政务 CA 公钥传送给依赖方

政务CA的根公钥包含在政务CA自签的根证书中。证书持有者可以从政务CA网站上下载政务CA根证书。

6.1.5 密钥的长度

政务CA完全遵从国家法律法规、政府主管机构等对密钥长度的明确规定和要求，目前：

- 政务CA用于签名的RSA密钥长度为1024位；
- RA注册机构用于签名和加密的RSA密钥长度为1024位；
- 证书持有者产生的签名密钥长度为1024位；
- 证书持有者产生的加密密钥长度为1024位。

6.1.6 公钥参数的生成和质量保证

公钥参数由国家密码管理局鉴证许可、政务CA政务CA证书签发系统支持的硬件产生，符合国家密码管理部门的要求。

6.1.7 密钥的使用

在政务CA电子认证服务体系中的密钥用途和证书类型紧密相关。CA证书的签名密钥用于签发RA证书和证书撤销列表（CRL）；签名密钥用于提供网络安全服务，如信息在传输过程中不被篡改、接收方能够通过证书来确认发送方的身份、发送方对于自己发送的信息不能抵赖等；加密密钥用于对需在网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。

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

政务CA政务CA使用国家密码管理局许可的产品，密码模块的标准符合国家规定和要求。

政务CA的密码模块使用加密机密码模块，加密机安置在安全区。并在有至少两名管理员在场的情况下才可以访问存储在加密机中的密钥。加密机的数据包括两方面的内容：管理员口令卡、CA私钥的备份。备份与恢复加密机必须分别同时拥有三张管理员口令卡片、备份卡，才能对加密机进行备份与恢复的操作。

政务CA私钥的备份数据存放在保险柜中，如有特殊情况需要使用，必须经过运维负责人与安全员共同申请，由CA中心负责人签字。负责保险柜的管理员将对应的政务CA私钥备份文件交给使用人，使用时必须由运维负责人和使用人同时在场，严禁复制，使用完毕后由运维负责人亲自将数据销毁。

6.2.2 私钥多人控制（m 选 n）

政务CA采用多人控制策略激活、使用、停止根证书和CA证书。

6.2.3 私钥托管

KMC 可以根据客户和法律的需要，对用户证书的加密密钥进行托管。签名私钥不进行托管，以保证其不可否认性。

6.2.4 私钥备份

政务CA私钥通过一定的安全程序进行备份，备份数据存放在保险柜中。备份数据的使用需要主管签字，在双人控制下使用。

作为灾难恢复的一项措施，证书的持有者需要备份他们的加密私钥，以确保这些私钥的安全。密钥管理中心负责备份托管加密私钥，确保加密私钥的安全。

6.2.5 私钥归档

政务CA密钥对超过使用期限后，要进行归档保存至少5年。

密钥管理中心提供过期的托管加密私钥的存档服务，归档期限也是5年。

6.2.6 私钥导入、导出密码模块

政务CA密钥对在硬件密码模块上生成，保存和使用。此外，为了常规备份和灾难恢复，对政务CA 密钥进行了导出备份，此过程有严格的管理流程控制。

在政务CA认证服务体系中，使用政务CA的软件可以把证书持有者加密证书的私钥导入密码模块中。

私钥无法从硬件及软件密码模块中导出。必须通过口令验证之后，才可能使用存储在密码模块中的私钥进行加解密操作。

6.2.7 私钥在密码模块的存储

政务CA的私钥存储在硬件密码模块中，

证书持有者必须将所有的私钥保存在硬件密码模块中。

6.2.8 激活私钥的方法

具有激活私钥权限的运维部门管理员使用含有自己的身份的加密IC卡登录，启动密钥管理程序，进行激活私钥的操作，需要至少3名管理员同时在场。

6.2.9 冻结私钥的方法

具有冻结私钥权限的运维部门管理员使用含有自己的身份的加密IC卡登录，启动密钥管理程序，进行冻结私钥的操作，需要至少3名管理员同时在场。

6.2.10销毁私钥的方法

在进行用户密钥的销毁时，需要3个管理员通过身份认证后方可进行。密钥销毁操作完成后，同时对数据库中该密钥的备份进行销毁。

6.2.11密码模块应达到的标准

使用的加密机是国家密码管理局批准使用的江南计算技术研究所生产的具有自主知识产权的高速主机加密设备。

6.3 政务 CA 密钥的保管

6.3.1 公钥归档

证书持有者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。它们由政务CA和密钥管理中心定期归档。

6.3.2 证书和密钥对使用期限

所有证书使用者的证书有效期和其对应的密钥对的有效期是一致的。

其中：

- 个人证书有效期为一年或两年；
- 机构证书有效期为一年或两年；
- 设备证书的有效期为五年；
- 代码签名证书有效期为一年或两年。

个人证书、机构证书和代码签名证书的具体使用期限，由各地注册服务机构根据业务需要自行选择。

6.4 系统升级与相关安全性控制

描述系统开发控制、安全管理控制和生命周期安全等级，系统开发控制包括开发环境安全、开发人员安全、产品维护期的配置管理安全、软件工程实施、软件开发方法论、模块化、层次化、使用容错设计和实现技术（如防御性编程）、以及开发工具安全。安全管理控制包括执行工具和程序，保证操作系统和网络符合设置的安全标准。

6.4.1 系统升级控制

政务 CA 的软件设计和开发过程遵循以下原则：

- 第三方的验证和审核
- 安全风险和可靠性设计

6.4.2 安全管理控制

政务 CA 的配置以及任何修改和升级都会记录在案并进行控制，并且政务 CA 采取一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

6.5 安全控制

政务 CA 有防火墙以及其他访问控制机制保护，其配置只允许已授权的机器访问。只有经过授权的政务 CA 员工才能够进入政务 CA 签发系统、政务 CA 注册系统、政务 CA 目录服务器、政务 CA 证书发布系统等设备或系统。所有授权证书持有者必须有合法的安全令牌，并且通过密码验证。

6.6 生命周期技术控制

6.6.1 系统开发控制

在系统开发过程中，政务CA在安全的开发环境下，严格按照软件工程的要求进行开发控制。系统是PKI的核心组成部分，主要有：

- 验证并标识证书申请者身份。
- 确保CA用于签名证书的非对称密钥的质量。
- 确保整个签证过程的安全性，确保签名私钥的安全性。
- 证书资料信息（包括公钥证书序列号、CA标识等）的管理。
- 确定并检查证书的有效期限。
- 确保证书主体标识的唯一性，防止重名。
- 发布并维护作废证书列表。
- 对整个证书签发过程作日志记录。

6.6.2 安全管理控制

政务CA对系统的维护保证操作系统、网络设置和系统配置安全。通过日志检查系统与数据完整性和硬件的正常操作。

6.6.3 生命期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。安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主管部门鉴定，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，整个系统安全可靠。

6.7 网络的安全控制

政务CA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。政务CA采用防火墙、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。

6.8 时间戳

政务CA中心提供时间戳服务，系统严格遵循国际标准时间戳协议（RFC3161），采用标准的时间戳请求、时间戳应答经及时间戳编码格式，时间源采用北斗卫星授时中心提供的标准时间。

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

7.1.1 证书格式标准

政务CA签发的证书均符合国家标准证书格式，遵循GB/T 16264.8标准，并可以提供支持证书扩展的能力。

7.1.2 证书标准项

- **证书序列号** 即证书参考号码，唯一标识该证书。
- **证书有效期** 证书的起止时间。
- **主题** 为证书持有者申请证书时所填写的申请信息。
- **发行者** 为政务CA

7.1.3 证书扩展项

证书扩展项即证书扩展部分。包括证书签发者的甄别名，签发证书序列号，用户主体的公钥标识，CRL发布，证书公钥用途，用户私钥有效期，政务CA承认的证书策略列表，用户主体目录属性，CA签名算法标识等。

7.1.4 算法对象标识符

政务CA签发的证书符合X509 V3标准，采用SHA-1 RSA算法签名。

7.1.5 名称形式

政务CA证书通过DN来命名。具体内容依次由CN、E、OU、OU、O、C 七部分组成。其中:

CN为用户姓名，表示证书持有者的姓名；

E为电子邮件，表示证书持有者的邮件地址；

OU为三级组织部门，表示科级组织名称；

OU为二级组织部门，表示县/处级组织名称；

OU为一级组织部门，表示地市/厅局级组织名称；

O为组织名称，表示各个部委或是省份的名称；

C为国家，表示中国。

7.1.6 名称限制

个人和机构CA证书的DN 中，除电子邮件，其它项目只能使用中文字符。

7.1.7 证书策略对象标识符

证书策略由发证机构制定并对外广泛发布，同时向国际标准化组织申请标准的对象标识符（OID），从而保证与其它应用相兼容，对象标识符在通信服务中进行传递，作为该证书机构证书策略的标识，代表该认证机构提供证书服务的相关策略。另一方面，只有用户同意该证书策略，才可以从认证中心去申请和获得证书。

7.1.8 策略限制扩展项的用法

规定在CA体系中的各层CA使用相同的CP以及是否和其他CA体系互相信任。政务CA未使用本扩展域。

7.1.9 策略限定符的语法和语义

Certificate Policies CA　　证书策略

Policy Mappings　　策略映射

Basic Constraints　　基本制约

政务CA未使用本扩展域。

7.1.10关键证书策略扩展项的处理规则

政务CA未使用证书策略扩展项。

7.2　证书撤销列表

7.2.1 版本号

政务CA定期签发CRL（证书废除列表），其所签发的CRL遵循RFC 3280 标准。采用X.509中的CRL V2 格式。

7.2.2 CRL 和 CRL 条目扩展项

CRL 数据定义：

（1）版本（Version）

含义：显示CRL 的版本号。

（2）签名（Signature）

含义: 签发CRL 的CA的签名。

（3）算法标识（Algorithm Identifier）

含义:定义签发CRL 所使用的算法。

（4）CRL 的签发者（Issuer）

含义:指明签发CRL 的CA的甄别名。

（5）CRL 发布时间（This Update）

（6）预计下一个CRL 更新时间(Next Update)

（7）撤销证书信息目录(Revoked Certificates)

（8）CRL 扩展（CRL Extension）

CA的公钥标识(Authority Key Identifier)

CRL 号（CRL Number）

7.3　在线证书状态协议

7.3.1 版本号

政务CA为证书持有者提供OCSP（在线证书状态查询服务），OCSP 为CRL 的有效补充，方便证书持有者及时查询证书状态信息。政务CA OCSP 服务遵循RFC 2560标准。

7.3.2 OCSP 扩展项

采用标准扩展，基于X.509版本3 证书所使用的扩展模型，主要有：

(1) 随机数鉴别符(Nonce)

(2) 证书撤销列表参考(CRL References)

(3) 可接受的回复类型(Acceptable Response Types)

(4) 证书撤销列表项目扩展(CRL Entry Extensions)

(5) 服务定位器（Service Locator）

8 认证机构审计和其它评估

8.1 评估的频率或情形

由国家政务外网数字证书中心指审计者。国家政务外网数字证书中心需要对国家政务外网的关联单位（包含国家政务外网服务分中心、服务点等证书体系成员）所有的流程和操作进行审计，检验其是否符合本CPS和相应的证书策略的规定，其频率可由国家政务外网数字证书 中心决定或由法律制定的监管机构决定。

政务CA的评估根据情况而定，有年度评估、运营前评估、安全事件发生后的评估和随时进行评估。

8.2 评估者的资质

政务CA将选择熟悉IT运营管理、具有多年审计经验的审计机构对政务CA的运营管理进行一致性审计。在进行审计前，审计机构必须熟悉公钥基础设施技术。

8.3 评估者与被评估者的关系

为了保障评估的公正性，评估者与被评估者应无任何业务、财务往来或其它利害关系足以影响评估的客观性。

8.4 评估内容

评估的内容包括但不限于以下方面：

1、CA物理环境和控制

2、密钥管理操作

3、基础CA控制

4、证书生命周期管理

5、CA业务规则

8.5 对问题与不足采取的措施

政务CA管理层将对审计报告进行评估，对在审计中发现的重大意外或不作为采取行动。从完成审计到采取行动纠正问题的时间不超过20天。

8.6 评估结果的传达与发布

评估结果根据需要在内部进行传达，并根据要求上报给行业主管部门。

9 法律责任和其他业务条款

9.1 费用

暂无。

9.2 财务责任

暂无。

9.3 业务信息保密

政务CA根据国家相应的法律法规制定并落实严格的信息保密规章制度，所有相关人员（包括政务CA及其业务代理机构的工作人员、证书持有者）必须遵守该规章制度。由政务CA制定及实施的信息保密规章制度符合国家保密机构的相关规定。政务CA有权根据情况修改相关内容。

除非有法律明确规定和要求，有关递交证书申请的用户信息将由政务CA保密并且在没有得到申请人授权的情况下不得泄露。这不适用于证书中由政务CA来自公众的不涉及许可授权的用户信息。其他各参与方的相关机密等按照保密协议进行保密。

除非有法律明文规定，政务CA没有义务公布或透露用户所持有证书以外的信息。

9.3.1 保密信息范围

以下信息应视为保密信息但不限于以下方面：

保密信息包括但不限于以下内容

1） 政务CA与其授权的注册机构、证书持有者、依赖方之间的协议、资料中未公开的内容等属于保密信息。

2） 证书持有者私钥属于机密信息，证书持有者应该根据本CPS的规定妥善保管，如因证书持有者自己泄漏私钥造成的损失，证书持有者应自行承担。

3） 所有对于政务CA或其相关机构的审计报告、审计结果等信息视为机密信息。

4） 有关CA认证系统的运行信息、技术手册等资料属于保密信息。

5） 除非法律明文规定或政府、执法机关等的要求，政务CA承诺不对外公布或透露证书持有者证书信息以外的任何个人隐私信息；同时，政务CA在同所有注册机构签署授权协议时，都将此条作为协议条款。

9.3.2 不属于保密的信息

以下信息可视为不保密信息

1）CA系统签发的证书和CRL中的信息。

2）在提供方披露数据和信息之前，已被接受方所持有的数据和信息。

3）在提供方披露数据和信息时或在披露数据和信息之后，非由于接受方的原因而被披露的信息。

4）经公开或通过其他途径成为公众领域的一部分数据和信息。

5）有权披露的第三方披露给接受方的数据和信息。

6）其他可以通过公共、公开渠道获得的信息。

9.3.3 保护机密信息的责任

政务CA有各种严格的管理制度、流程和技术手段来保护机密信息，包括但不限于商业机密、客户信息等。政务CA的每个员工都要接受信息保密方面的培训。各方有保护自己和其他人员或单位的机密信息并保证不泄露的责任。

9.4 个人信息私密性

9.4.1 隐私保密方案

个人私密信息保密方案遵守现行法律和政策。

9.4.2 作为隐私处理的信息

政务CA在管理和使用证书持有者提供的相关信息时，除了证书中已经包括的信息以及证书状态信息外，该证书持有者的基本信息将被视为隐私处理，只有经证书持有者同意或有关法律法规、公共权力部门根据合法的程序要求，才可以公开。

9.4.3 不视为隐私的信息

证书持有者的证书相关信息是可以公开的，通过政务CA目录服务、Web服务、OCSP方式向外公布。

9.4.4 保护隐私的责任

政务CA、证书持有者、注册机构、依赖方等机构或个人都有义务按照本CPS的规定，承担相应的保护隐私责任。在法律法规或公共权力部门通过合法程序要求下，政务CA可以向特定的对象公布隐私信息，政务CA无需承担由此造成的任何责任。

9.4.5 使用隐私的告知与同意

1） 证书持有者同意，政务CA在业务范围内使用所获得的任何证书持有者信息，无论是否涉及到隐私，政务CA均可以不用告知证书持有者。

2） 证书持有者同意，在任何法律法规或公共权力部门要求下，政务CA向特定对象披露隐私信息时，政务CA均可以不用告知证书持有者。

9.4.6 依法律或行政程序的信息披露

除非符合下列条件，政务CA不会将证书持有者的保密信息提供给其他个人或第三方机构：

1） 司法、行政部门或其他法律法规授权的部门依据政府法律法规、规章、决定、命令等的规定通过合法授权提出的申请。

2） 证书持有者采用书面形式的信息披露授权。

3） 本CPS规定的其他可以披露的情形。

9.4.7 其它信息披露情形

政务CA、证书持有者、注册机构、依赖方等机构或个人都有义务按照本CPS的规定，承担相应的保护隐私责任。在法律法规或公共权力部门通过合法程序或证书持有者书面申请授权要求下，政务CA可以向特定的对象公布隐私信息，政务CA无需承担由此造成的任何责任。

9.5 知识产权

政务CA享有并保留对证书以及政务CA提供的全部软件、资料、数据等的著作权、专利申请权等知识产权；政务CA制订并发布的CPS以及相关政策、发布的证书和CRL均为政务CA的财产，政务CA对其拥有知识产权；在政务CA域内目录中使用的代表单位的甄别名称(DN)和在同一域内发给最终实体的证书中的甄别名称都会含有一个相关的代表政务CA的名称，政务CA对此拥有知识产权。

9.6 权利和责任

9.6.1 政务 CA 的权利和责任

政务CA享有的权利主要有以下方面：

1) 要求证书申请者提供真实资料的权利，有权按申请不同类型的证书，要求申请者提供不同的真实资料：对个人证书申请者、机构证书申请者、设备证书申请者要求提供的有关资料参见政务CA证书申请表的相关内容（申请表可以从政务CA网站、受理点等处获得）。政务CA在遵循合法程序的前提下有权对上述内容进行调查、审核。

2) 有权提供不同类型的证书，满足不同的证书用户的不同需要。

3) 政务CA有权向证书申请者颁发证书、撤销证书、发布证书撤销列表等对证书操作的一系列流程，并为政务CA制定出相关的规则。

4) 政务CA有权根据国家相应的法律法规制定政务CA法律责任书和服务责任书，并有权让证书用户遵守政务CA的规定。

5) 政务CA在法律许可范围内有权对所有证书遭受破坏或盗用的情况协助调查，其调查包括但不限于面谈、记录与相关程序、相关设施的检查等。

6) 政务CA对于下列情况之一，将有权主动废止所签发给证书持有者的证书：

- 证书申请初始注册时，提供不真实材料；
- 违反国家法律或者其它规章制度，不应签发证书的；
- 有盗用、冒用、伪造或者篡改他人证书；
- 不履行政务CA的服务规范，如本电子认证业务说明中的规定；
- 与证书中的公钥相对应的私钥被泄密；
- 证书中的相关信息有所变更；
- 由于证书不再需要用于原来的用途而要求终止；
- 用户未履行证书更新手续（该手续包括提出证书更新的书面申请，以及按规定缴纳相关费用）；
- 其他情况。

7) 政务CA有权确认：证书申请人确为证书申请书所说明的实体（依据证书类型描述的内容）；证书申请人合法地持有证书中所列的公开密钥所对应的私人密钥；除未经证实的证书用户资料外，证书中所记载的资料均准确无误，任何申请列有证书申请人公开密钥的证书的代理人是经过合法授权提出申请的。

8) 当使用或信赖证书的证书依赖方或政务CA的业务代理机构和雇员的违约行为或其他行为导致政务CA发生任何损失、损坏或债务责任和法律费用以及成本损耗，政务CA有权要求赔偿。

政务CA对所担负的法律规范的有限责任做出如下承诺：

1) 政务CA的运作遵守《中华人民共和国电子签名法》，接受国家密码管理局及相关主管部门的领导。

2) 为进行网上业务的各方提供信息安全基础设施，并且经过国家有关管理机关鉴定和审批，合法许可经营。

3) 建立并执行符合国家政策规定的安全机制，管理所拥有的信息安全基础设施，使其处于良好运行状态，并使政务CA的签名私钥在政务CA内部得到安全的存放和保护。

4) 对申请证书登记人的身份进行严格的审查和认证，保证发放的证书具有可靠的权威性和信任度，保证证书的真实有效性，即所发放证书中的公共密钥同某个确定身份的人是一一对应的。

5) 政务CA有告知的责任，应向社会公开披露以下内容并保证该内容的准确完整：

一是根证书；二是证书上所列明的数字信息；三是用户的公钥；四是认证业务操作规范（CPS）；五是证书撤销列表（CRL）。

6) 负责证书签发和管理，包括控制实际的证书产生过程，证书的发布，证书的撤销和证书的更新；及负责确保根据本电子认证业务说明的要求说明和做好与证书有关的服务、操作等各方面的工作。

7) 遵守政务CA电子认证业务说明的规定，做好电子认证业务说明的版本管理与控制，对修订后的电子认证业务说明及时予以发布。

8) 使用政务CA提供的证书与安全软件的用户的网上交易信息对无关者是保密的，而且在网上传输中是不可篡改的。

9) 在现有技术条件下，除非政务CA私钥丢失，政务CA签发的证书不会被成功地伪造、篡改；如果由于政务CA的私钥管理问题造成证书被伪造、篡改，政务CA将承担相应责任。

10) 在现有技术条件下所采用的密码机制无法攻破。如果发生证书密码机制问题，而政务CA没有及时采取应对措施，政务CA将承担责任。

除上述的责任条款，政务CA及其工作人员不做任何其他保证和履行任何进一步的义务。

需要明确的是，本电子认证业务说明的内容，没有任何信息可以暗示或解释为政务CA必须承担其它的义务或政务CA必须对其行为做出其它的承诺。

9.6.2 政务 CA 下属 RA 的权利和责任

RA 注册机构的职责是：

1) RA 应遵守由政务CA制定的所有运营政策、操作管理规范、规定登记程序和安全保障措施，政务CA有权根据情况修改有关内容；

2) RA 有责任验证申请人提供信息的准确性和可靠性，验证过程由RA 审核执行，通过政务CA制定的审核步骤，确定颁发的证书的有效性和真实性；

3) 承担发布CRL并保证CRL准确性与及时性的责任；

4) RA应使用政务CA确定的信息传输协议和标准，与政务CA交换信息；

5) RA应承担因在CPS规定的用途外使用RA管理员证书所造成的损失的责任；

6) 对于政务CA提供的属于政务CA专有的技术、软件开发包只有使用权，并对其承担保密义务；无权将未经政务CA授权的属于政务CA独有的技术/产品以任何方式让第三方知道和使用，并应对泄密承担相应责任。

9.6.3 证书持有者的权利和责任

证书持有者（或证书用户）是政务CA的客户，是接受电子认证服务的一方。

1、证书持有者应享有以下权利：

1） 获得有效合格证书的权利：证书持有者在提供了符合要求的信息资料并交纳证书服务费用后，有权利取得有效的、具有所需功能的证书。

2） 提出中止或撤销证书的权利：在前述的有关政务CA应该中止或撤销证书的条件下，证书持有者或其代理人有权提出中止或撤销证书的申请。

2、证书持有者负有以下责任：

1） 证书持有者对其私钥应保持控制，采取合理的预防措施避免遭受破坏或盗用，并不得向未经授权的人泄露，确保私人密钥的安全，以防止任何遗失、泄漏、修改或密钥的未经授权使用。因私钥的不安全控制而造成的损失，由证书持有者承担。

2） 如果证书持有者的私密钥出现问题，例如遗失、盗用、破坏或者泄密等，证书持有者应当在察觉后的第一时间内通知所有所能预见到的受证书影响的单位及个人，包括政务CA；同时向政务CA申请撤销该证书。

3） 证书持有者在申请证书时应真实陈述政务CA颁发证书时要求其提供的事项，提供真实准确的信息作为证书申请材料。证书持有者应为其在证书中的错误陈述承担责任，并应承担因其所提供的申请信息侵犯他人权利而造成后果的责任。

4） 证书持有者应向政务CA按时交纳服务费用以享受相关服务。

9.6.4 证书依赖方的权利和责任

1） 证书依赖方须熟悉本电子认证业务说明以及和证书持有者证书相关的证书策略，还须了解和遵守证书的使用目的。证书依赖方必须确保证书确被用于预定的目的。

2） 证书依赖方在信赖证书持有者的证书前，必须根据最新的证书撤销列表（即CRL）检查证书的状态，查明证书是否还在有效期内。

3） 当证书依赖方在网上进行电子活动时，有权审查自己或对方的证书是否在有效期内，是否已被列为“黑名单”，证书依赖方应该在做出决定是否相信某个证书之前，应该先查看“查询证书”以确定该证书是否有效、未经撤销或更新，然后再用该证书来确认该电子签名是否有效，是否由证书中所列的公开密钥相对应的私人密钥所产生，加入电子签名的信息未被改动。必要时有权向政务CA联系和查询。

9.6.5 其他参与者的权利和责任

具有与依赖方同样的权利和责任。

9.7 有限责任与免责条款

9.7.1 特定责任的排除

政务CA在与用户和依赖方签定的协议中，对于因用户或依赖方的原因造成的损害不具有赔偿义务。

对于由于证书、数字签名或根据政务CA电子认证业务说明而提供或设计的任何其他服务的使用、签发、授权、执行或拒绝执行而导致的或与之有关的任何间接性的、特别性的、附带性的、或结果性的损失，或任何利益损失、数据丢失，或其他间接性的、结果性的或惩罚性的损

失，无论是否可以合理预见，政务CA将不会对此承担任何责任。

9.7.2 免责条款

1) 政务CA不对由于客观意外或其它不可抗拒力事件造成的操作失败或延误承担任何损失、损坏和赔偿责任。

2) 政务CA在签发证书之前，事先就与证书申请者签定电子认证服务协议，都有事先告知证书持有者的免责条款规定：政务CA发放的各类型证书只能用于在网络上标识身份、加密数据、签名认证、保证网络安全通讯等相应证书规定的用途，不能作为其他任何用途，不承担任何形式的责任和义务。若证书持有者将其证书用于其他用途，政务CA不承担任何责任。

3) 如果证书申请者有意或无意地提供不完整、不可靠或已过期的信息，而他又根据正常的流程提供了必须的审核文件，由此得到了政务CA签发的证书，由此引起的经济纠纷由证书申请者全部承担，政务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。

4) 与证书持有者公钥配对的私钥是保密的，证书持有者应当妥善保管，不得泄漏或交付他人。如因故意、过失导致他人知道或遭盗用、冒用、伪造或者篡改，证书持有者应当自行负责承担一切责任。

5) 政务CA在进行身份认证或证书持有者下载证书时，将充分遵守政务CA的安全操作流程。如果由于非政务CA自身的原因而造成的政务CA设备故障、线路中断，导致签发证书错误、延迟、中断或者无法签发，政务CA不负任何赔偿责任。

6) 政务CA仅仅提供电子活动中签名“不可抵赖”的依据，但并不对此承担法律责任等方面的约定。

7) 当政务CA在任何法律、法规或规章条款的要求下，或在法院的要求下必须披露本电子认证业务说明中具有保密性质的信息时，政务CA可以依从法律、法规或规章条款以及法院判定的要求，向执法部门公布相关的保密信息。此种信息披露不视为违反了保密的要求和义务。

8) 当保密信息的所有者出于某种原因，要求政务CA公开或披露其所拥有的保密信息，政务CA应当满足其要求。如果这种保密信息的披露行为涉及或有可能引起对其他方的赔偿义务，政务CA有权拒绝其要求，且不应该承担任何由此相关的或由于公开保密信息引起的损失和损坏的赔偿责任。保密信息的所有者应负责政务CA与此相关的或由于保密信息公开引起的损失和损坏的赔偿责任。

9) 政务CA不承担任何其他未经授权的人或组织以政务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) 政务CA用户证书的有限期为一年、两年或五年，自用户申请之日起计算。用户必须在证书失效前20天向CA中心或受理点提出证书更新请求，否则证书到期后将自动失效，政务CA不对因用户使用被撤销或过期证书而造成的损害承担任何责任。

11) 如证书用户出于某种原因不希望继续使用证书时，应当立即申请撤销证书。政务CA在接到撤销申请后，在24小时之内正式撤销用户的证书。政务CA不对证书正式撤销前造成的损害承担任何责任。

9.8 赔偿

9.8.1 理赔

在政务CA违反了前文9.6.1 款条例规定的职责，政务CA承担赔偿责任（法定的或约定免责除外）。赔偿责任的限制如下：

政务CA所有的赔偿义务均依据中华人民共和国的有关法律法规执行。

政务CA只有在用户证书有效期限内承担这种损失或损害赔偿。

9.8.2 索赔

由以下情况造成用户或依赖方的损失并同时损害政务CA利益的，政务CA拥有向用户和依赖方索取赔偿的权利。这些情况是：

1） 用户没有提供正确的身份信息而申请到信息不正确的证书的；

2） 用户在证书应用时不检查证书撤销信息CRL的；

3） 用户未按规定使用证书，有意或无意泄漏证书相关私密信息的；

4） 将证书应用于政务CA不允许的领域或应用的；

5） 其它不符合政务CA要求和规定的行为。

9.9 CPS 的有效期与终止

政务CA的CPS自发布之日起正式生效。CPS中将详细注明版本号及发布日期。最新版本的CPS请访问政务CA网站以获得，对具体个人不做另行通知。当新版本的CPS正式发布生效，旧版本的CPS将自动终止。

9.10 CPS 的修订

当出现以下情形时政务CA将对CPS 进行修订：

1） 因相关法律法规要求而引起政务CA业务规则发生改变；

2） 因相关技术条件变化而引起政务CA业务规则发生改变；

3） 因其它原因而引起政务CA业务规则发生改变。

CPS的修正的流程为：

1） CPS修订小组提出修订意见，征询各方的建议，包括用户和依赖方；

2） 搜集各方意见并进行研究讨论；

3） 在CPS修订小组进行修改并提交政务CA决策层批准；

4） 再次进行审议和生效，并通过政务CA网站或其它方式发布。

9.11 争议解决

当政务CA与用户或依赖方出现争议，如通过协商仍未能达成一致意见时，当事人有权将争议提交当地仲裁机构，根据仲裁条例在时效内裁决。

9.12 管辖法律

政务CA的电子认证业务说明（CPS）及协议中条款的制定均依从《中华人民共和国合同法》、《中华人民共和国电子签名法》以及中华人民共和国相关法律。

9.13 与适用法律的符合性

政务CA的各项策略的执行、解释、翻译、和有效性均适用中华人民共和国法律法规和国家信息安全主管部门要求。法律的选择是确保对所有用户有统一的程序和解释，而不论他们在何地居住以及在何处使用证书。

9.14 一般条款

9.14.1完整协议

现行条款替代所有以前的和同时期的条款。

9.14.2分割性

对于法庭或其他仲裁机构判定某条款非法和不可执行而导致协议无法执行的情况，保留采用法律解决的权利。

9.14.3强制执行

合同一方或几方不履行合同条款的，其它方可以要求强制执行。

9.14.4不可抗力

由于不可预见的原因和不可控的原因，视为不可抗力，会导致合同或协议的终止。例如战争、恐怖行动、罢工、自然灾害、供货商或代理商倒闭、互联网或其它基础设施无法使用等。但各方都有义务建立灾难恢复和业务连续性机制。

9.15 各种规范的冲突

若本电子认证业务说明与其它规定、指导方针相互抵触，用户必须接受本电子认证业务说明的约束，除非本电子认证业务说明的规定在法律禁止的范围之内，或有关规定、指导方针明确地言明优于本电子认证业务说明。

在政务CA与包括用户在内的其它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，均视为双方均同意按本电子认证业务说明的规定执行；对协议中不同于本电子认证业务说明内容的约定，按双方协议中约定的内容执行。

9.16 补充说明

暂无。