国家电子政务外网
电子签名认证证书策略

版本 V1.0

国家信息中心
State Information Center

版本控制表

版本	状态	修订说明	修订人	审批人	生效日期
1.0	新增	按照《电子政务电子认证服务管理办法》要求编制	电子认证制度编制组	国家电子政务外网管理中心电子认证办公室	2026-01-06

目录

1　概括性描述

1.1　概述

国家电子政务外网电子签名认证证书策略(以下简称《策略》，CP)，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》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”（以下简称“认证办”），主要职责是负责国家电子政务外网电子认证服务业务的相关管理和服务工作。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）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。2011年政务CA 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是专业化电子政务电子认证服务机构，是国家电子政务外网的信息安全基础设施，设有独立密钥管理中心。政务CA 以密码技术为核心技术，通过签发数字证书对电子政务信息交换中的身份进行确认、控制访问权限，保证信息的真实性、完整性和不可抵赖性，对政务网络防泄密、抗侵入、拒黑客、识真伪，保障网络和信息安全有着不可替代的重要作用。

国家电子政务外网电子认证服务（以下简称“外网认证服务”）按照《策略》所规定的服务内容及要求开展。

认证办负责各省注册服务中心和注册服务分中心/注册服务点的建设和运行管理指导。

政务CA的主要业务内容包括：

1）制作、签发、管理证书；

2）对签发的证书的真实性进行确认；

3）提供证书目录查询服务；

4）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：

1）能够对相关实体的身份进行认证；

2）能够保证数据电文在传递、接收和存储过程中的完整性；

3）能够确认数据电文签署人的身份以及确认数据电文相关操作的不可抵赖性；

4）能够实现网络信息的安全加密、解密。

本策略是政务CA对所提供的全部证书服务生命周期中的业务实践（如申请、受理、签发、接受、使用、更新证书或密钥、撤销、冻结与解冻、备份与恢复、归档）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：

1）概括性描述；

2）信息发布与信息管理；

3）身份标识与鉴别；

4）证书生命周期操作要求；

5）认证机构设施、管理和操作控制；

6）认证系统技术安全控制；

7）证书、证书撤销列表和在线证书状态协议；

8）认证机构审计和其他评估；

9）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本策略所规定的条款，承担相应的责任和义务。

1.2 文档名称与标识

本文档名称：《国家电子政务外网电子签名认证证书策略》。

本策略在政务CA的网站上予以发布。

本证书策略的对象标识符为：1.2.156.112829。

1.3 电子认证活动参与者

1.3.1 政务CA

政务CA由认证办进行管理。

政务CA制定相关管理文档，记录各种审计内容和各类表单所形成的日志，同时提供5*8管理计划和维护计划。政务CA向证书申请者提供颁发证书、撤销证书、发布证书撤销列表等一系列证书服务，并制定业务策略、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定期对其管理的服务机构进行服务质量评估，及时对服务业务规则进行修订，并在服务范围内发布。

1.3.2 注册机构

注册服务机构，指经政务 CA 批准认可的，在授权服务范围内开展电子认证注册服务的机构，以下简称“注册机构”。

注册机构与政务 CA 签署委托协议，获得开展电子签名认证证书注册业务的授权。政务 CA 在 30 日内向注册机构所在省、自治区、直辖市密码管理部门备案。备案内容发生变更的，政务 CA 应当自变更之日起 30 日内向注册机构所在省、自治区、直辖市密码管理部门备案。政务 CA 应当对受委托机构开展证书注册业务的行为进行监督，并对该行为的后果承担责任。

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实体对象，包括个人、单位、和设备等。

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。在政务CA体系中，依赖方是信任政务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，使用政务CA证书的公钥加密信息的实体。

1.3.5 其他参与者

其他参与者指为政务CA证书服务体系提供相关服务的其他实体或个人。

1.4 证书应用

1.4.1 证书类型及应用范围

政务CA拥有下表所示的证书类型。除本策略或证书自身禁止等要求外，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

认证办负责本策略的制订、发布和更新事宜，并对本策略拥有完全版权和最终解释权。

1.5.2 联系方式

发布网址：www.sic.gov.cn

联系地址：北京市西城区三里河路58号

邮　　编：100045

电　　话：400-044-40080

传　　真：010 - 68558058

1.5.3 决定电子认证业务说明符合策略的机构

认证办拥有对本策略的解释权。

1.5.4 《策略》批准程序

CP批准主要分为计划与编写（修订）、审议、发布和备案四个阶段：

1）计划与编写（修订）：CP编写组由认证办成员及其组织的相关专家组成。CP编写组根据相关法律政策和运营策略提出CP编写（修订）计划并完成具体条款编写(修订)工作。

2）审议：将编写（修订）后的CP递交认证办审议。

3）发布：认证办审议通过后，通过政务CA网站或其他形式正式对外发布。政务CA对CP的版本号将进行严格控制。若本CP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CP的版本号；若本CP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CP版本号也无须通知用户。

4）备案：经审议通过的CP向国家密码管理局备案。

1.6 定义和缩写

1.6.1 定义

1）公钥基础设施（PKI）：基于公钥密码技术实施的具有普适性的基础设施，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务。

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）证书持有者(Subscriber)：被颁发给一个证书的证书主体。

4）证书依赖方（Certificate Dependent）：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证书持有者。

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

CP Certification Policy 证书策略

CPS Certification Practice Statement 电子认证业务规则

DN Distinguished Name 唯一甄别名

LDAP Lightweight Directory Access Protocol 轻量级目录访问协议

CRL Certification Revocation List 证书撤销列表

CA Certification Authority 认证机构

RA Registration Authority 注册机构

LRA Local Registration Authority 注册机构受理点

PIN Personal Identification Number 个人识别码

PKI Public Key Infrastructure 公钥基础设施

OCSP Online Certificate Status Protocol 在线证书状态协议

USB KEY Universal Serial Bus Key 采用USB接口的证书存储介质

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CP等相关信息。

2.2　发布的时间或频率

政务CA签发证书后立即发布到目录服务。

政务CA的CRL定期发布到目录服务。

CP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，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　身份标识与鉴别

3.1　命名

3.1.1 名称类型

电子政务数字证书命名符合《GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范》要求。

根据证书对应实体的类型不同，政务CA签发的证书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。

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，或者冻结证书，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通过使用经证书持有者私钥进行数字签名的PKCS#10格式（或其他相当的密码格式）的证书请求，或政务CA批准的其他方法，验证证书持有者拥有私钥。

3.2.2 订户身份的鉴别

订户在申请政务CA签发的证书前，应仔细阅读申请数字证书相关事项，亲自或指定授权代表，提供有效身份证明文件、证书申请文件或以政务CA认可的安全方式提交真实有效信息，接受证书申请的有关条款，同意承担相应的责任。

政务CA或者政务CA授权的RA机构接受订户的证书申请后，应对订户及其授权代表的身份真实性、完整性、准确性进行鉴别（核验），对申请者提交的证书信息进行审核，妥善保存订户申请材料及鉴别记录。

3.2.3 没有验证的证书持有者信息

政务CA签发的证书信息没有未经过验证的信息。

3.2.4 授权确认

对于组织机构证书，政务CA在签发前，将确认代表组织机构提交证书申请的人出示足够的证明信息以证明申请者已获得组织机构的授权。政务CA将对授权信息妥善保存。

3.3 密钥更新请求的标识与鉴别

证书密钥更新有两种情况:补发和换发。

1、证书补发

补发是指在证书有效期内，证书持有者更新证书的操作。以下情况证书持有者需要申请证书补发。

(1)证书持有者证书丢失或损坏，例如存放证书的介质损坏；

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

(3)其它经政务CA认可的原因　　。

当证书持有者需要补发证书时，应主动向政务CA的注册机构提出证书补发申请。在证书的有效期内需进行补发的，证书持有者无需提交身份验证材料，仅需提交证书申请表，注明原证书的DN。政务CA仅通过证书持有者初次申请时的信息进行身份验证即可。超过有效期后，则需对证书持有者身份进行重新验证。验证流程及要求与初次申请相同。

证书补发时新证书有效期从补发操作起到原证书失效日止。

2、证书换发

换发是指在证书将要过期的三个月内或证书过期后，证书持有者申请更新原证书DN有效期的操作。

证书换发时需要对证书持有者身份进行重新验证。重新验证证书持有者身份的验证流程及要求与初次申请相同。

证书换发新证书有效期将从证书换发之日起至原证书到期为止再另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周期)。

为保障用户在执行证书更新期间服务不受到影响，在SSL服务器证书更新30天后吊销原有证书。而其他证书会在证书更新时立即吊销原有证书，并发布CRL信息。

3.3.1 常规密钥更新的标识与鉴别

同 3.3。

3.3.2 撤销后密钥更新的标识与鉴别

证书撤销后的密钥更新等同于订户重新申请证书，其要求与3.2相同。

3.4 撤销请求的标识与鉴别

在政务CA的证书业务中，证书撤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。证书撤销的方式可以是证书持有者自己撤销，也可以由证书持有者要求政务CA或注册机构管理员撤销，政务CA和注册机构在认为必须的时候，有权发起撤销证书持有者证书。

1）在证书持有者自己撤销时，可接受的鉴别过程如下：

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

2）证书持有者通过认证机构、注册机构撤销时，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，向政务CA或注册机构提交请求，政务CA或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，确认要撤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、设备等需要在国家政务外网应用中进行基于证书的身份鉴别、数字签名及信息加密时，可向政务CA或注册机构提出证书申请。

个人证书由证书持有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。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

注册时证书持有者须提供真实有效的申请信息，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，如需提供证书申请信息，并确保申请信息的真实准确等（具体要求见本CP9.6.3 所述）；

政务CA或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CP的规定，对申请者提供的信息进行真伪鉴别，然后按CP3.2.2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CP3.2.2 组织机构身份鉴别和CP3.2.3 个人身份鉴别。

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持有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持有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，并通知证书持有者鉴别失败，同时向证书持有者提供失败的原因(如：无法完成鉴别和验证身份信息；用户未提交所规定的文件；用户未在规定时间内回复通知；未收到证书费用等。)。被拒绝的证书持有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。政务CA或注册机构应妥善保管证书持有者的证书申请信息。

4.2.3 处理证书申请的时间

政务CA或注册机构处理证书请求的最长响应时间应不超过24小时。

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，政务CA建设RA系统提供证书服务。政务CA的注册机构在接受、处理证书请求时担当RA的角色。

在证书签发过程中，RA和政务CA将采用身份认证和数据安全传输等措施，将证书申请信息由RA系统发送给政务CA。政务CA在获得RA的证书请求后，对来自RA的信息进行鉴别和解密，对于有效的证书签发请求，政务CA将签发证书并返回给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，邮件中将包含如何获取证书的信息；

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或注册机构将会把证书及其密码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）对于移动证书等扩展业务，将采取业务App或短信方式，通知证书持有者证书信息已经正确生成；

4）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、短信和业务APP中获取证书的指示，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、移动终端。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证书即表明证书持有者接受证书。而对于第二和第三种方式，当证书持有者接受载有证书的介质即表明证书持有者接受证书。

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确定的其他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他场所公布他们的证书。

4.4.3 政务CA对其他实体的通告

CA不需要通知其他实体证书的签发。

4.5 证书使用处理

4.5.1 执行识别与鉴别功能

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。

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）按照本CP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CP以及政务CA与各方签署的协议、规范中的条款。任何超出本CP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。如果证书持有者将该证书用于其他用途，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，依赖方要独立地做出应有的努力和合理的判断。除非本CP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CP规定的范围内信赖证书和证书中包含的公钥。

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 证书与密钥更新

证书与密钥更新是指订户证书到期或者损坏等，生成新密钥并申请为新公钥签发新证书。

4.7 证书补办

补办是指在证书有效期内，证书持有者出现证书载体丢失和证书载体损坏时进行证书补发的操作。

4.8 证书变更

证书变更是指在证书未到期之前，证书持有者申请对已签发的数字证书进行证书信息变更。

4.9 证书撤销

4.9.1 证书撤销的情形

出现下列情况之一，政务CA将强制撤销所签发的证书：

1）当政务CA或注册机构发现证书申请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或注册机构发现证书持有者主体消亡；

4）根据法律法规或政府主管机构/部门的要求，政务CA或注册机构对证书持有者证书进行撤销；

5）证书载体变更；

6）证书持有者声明不再使用证书并要求政务CA或注册机构予以撤销；

7）证书持有者相信或怀疑密钥泄漏或遭受攻击，要求撤销证书；

8）数字证书中的相关信息发生重大变更；

9）证书持有者认为其不能实际履行数字证书认证业务规则；

10）政务机构的证书持有者不从事原岗位工作；

11）证书遗失。

撤销分为主动撤销和被动撤销。主动撤销是指由证书持有者提出撤销申请，由政务CA或注册机构审核通过后撤销证书的情形；被动撤销是指当政务CA或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，采取撤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1-5种情况时，适用于被动撤销，第6-11种情况适用于主动撤销。

4.9.2 请求证书撤销的实体

在符合本CP4.9.1 所述的情形下，请求证书撤销的实体与本CP4.1.1 证书申请实体相同。

另外，政务CA或注册机构也可以在本CP4.9.1 所述的相关情形下主动提出撤销证书的请求。

4.9.3 撤销请求的流程

当最终证书持者有撤销证书的需求时，证书持有者可按照以下流程申请撤销证书：

1）证书持有者可通过书面、通信、APP等方式向政务CA或注册机构提出撤销证书请求；

2)当证书持有者通过书面、通信方式申请证书撤销时，根据政务CA或注册机构的要求，填写并提交书面申请表；当证书持有者通过证书APP自助申请证书撤销时，需使用原证书对撤销申请进行数字签名；

3）政务CA或注册机构在验证了申请者身份的真实性、撤销理由的正当性及书面申请表的有效性（或含有效数字签名的撤销申请）后将撤销证书持有者的证书；

4）证书持有者证书被撤销后，政务CA或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撤销，并及时将证书撤销信息发布到政务CA或注册机构信息库和目录服务。

当政务CA或注册机构有充分的理由相信需要撤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撤销证书。在证书撤销后，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 撤销请求宽限期

证书持有者一旦发现需要撤销证书，应向发放该证书的政务CA或注册机构及时提出撤销请求。如果出现私钥泄露等事件，撤销请求必须在发现泄露或有泄露嫌疑8小时内提出。其他撤销原因的撤销请求必须在24小时内提出。

4.9.5 政务CA处理撤销请求的时限

政务CA或注册机构从收到撤销请求到审核完成，做出撤销决定并将撤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撤销申请到证书正式撤销前24小时内因使用该证书造成的损失，政务CA或注册机构不予承担。

说明：证书持有者在正式提出证书撤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撤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。

当证书持有者通过证书在线服务系统或证书APP自助申请证书撤销，政务CA或注册机构将立即完成证书撤销，并在24小时内将撤销证书发布到目录服务。

4.9.6 依赖方检查证书撤销的要求

依赖方应当检查他们所信任的证书是否被撤销。检查方式是通过查询政务CA发布的CRL进行，或通过查询政务CA的OCSP服务进行。

4.9.7 CRL 发布频率

CRL发布频率不超过24小时一次，在发布的同时对原有内容进行更新。

4.9.8 CRL 发布的最长滞后时间

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 撤销信息的其他发布形式

除了CRL外，政务CA所发布的撤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撤销证书。（待讨论）

4.10 证书冻结和解冻

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，而不申请撤销该证书，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；

2）除证书持有者（或者其授权的委托代理人）外的其他实体，司法机构向政务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CP4.10.1 所述的情形下，请求证书冻结的实体与本CP4.1.1 证书申请实体相同。

另外，政务CA、注册机构、法院、政府主管部门及其他有关部门等只有在本CP4.10.1 所述的相关情形下才有权提出证书冻结的请求。

4.10.3 证书冻结与解冻流程

当最终证书持有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或注册机构提出冻结或解冻证书的请求；

2） 也可通过APP证书管理页面，提交冻结或解冻申请

2）证书持有者根据政务CA或注册机构的要求，填写并提交书面申请表；

3）政务CA或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或注册机构信息库和目录服务。

当政务CA或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，或当法院、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、撤销或恢复等其他证书相关业务，政务CA将对该证书做撤销处理。

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。

4.12 证书失效

以下两种情形将被视为证书失效：

1）证书到期。

2）证书撤销。

4.13 口令解锁

当证书持有者的电子钥匙被锁死后，在成功验证证书持有者身份后，可以提供口令解锁服务。

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、移动端软件密码模块）生成与保存，加/解密密钥对由政务CA密钥管理中心（KMC）生成，系统每天对数据进行备份。

密钥恢复是指加密密钥的恢复，即按照证书申请的身份鉴别流程执行，将加密证书的归档或备份密钥，恢复到可用状态。密钥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。

司法密钥恢复按照国家密码管理局的规定执行。

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

本章规定参见CPS相关内容。

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 私钥传送给证书持有者

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加密算法。第三方无法获得，保证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，在此过程中采用国家密码管理局许可的加密算法，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用于签名和加密的SM2密钥长度是256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使用国家密码管理局许可的产品，密码模块的安全级别和标准符合国家密码管理局的规定和要求。

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。KMC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。

KMC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密钥对在达到国家密码管理局许可的一定安全级别的密码模块上生成、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的私钥存储在达到国家密码管理局许可的一定安全级别的密码模块中，

证书持有者必须将所有的私钥保存在达到国家密码管理局许可的一定安全级别的密码模块中。

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设备登录，启动密钥管理程序，进行激活私钥的操作，需要至少2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密码设备登录，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名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

政务CA使用的加密模块是经国家密码管理局批准使用的具有自主知识产权的达到一定安全级别的产品。

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KMC定期归档。

6.3.2 证书和密钥对使用期限

所有证书持有者的证书有效期和其对应的密钥对的有效期是一致的。

签名私钥在签名证书到期后不得继续使用，加密证书的公钥在加密证书到期后不能继续使用。

6.4 系统升级与相关安全性控制

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。私钥激活数据的产生安全可靠，并具有日志记录。激活数据具有足够的复杂度。政务 CA 私钥进行分割保护。激活数据在传输中确保机密性，并在不需要时，妥善销毁。

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。

6.6.2 安全管理控制

政务CA对系统进行维护，保证操作系统、网络设置和系统配置的安全。通过日志检查系统与数据的完整性以及硬件的正常操作。

6.6.3 生命周期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保障的。依据国家有关标准对系统安全进行严格设计，使用的算法和密码设备均通过主管部门鉴定，使用基于标准的强化安全通信协议确保通信数据的安全，在系统安全运行方面，充分考虑人员权限、系统备份、密钥恢复等安全运行措施，确保整个系统安全可靠。

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、时间戳应答以及时间戳编码格式，时间源采用北斗卫星授时中心提供的标准时间。

6.9 应用集成支持服务

政务CA在CPS中制定证书集成支持服务。

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，符合《GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范》要求，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** 为证书的起止时间；
- **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

符合《GM/T 0015-2012 基于SM2密码算法的数字证书格式规范》。

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、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。

主题项格式按照《国家电子政务外网数字证书主题项格式规范》命名规范命名。

7.1.6 证书策略对象标识符

证书策略由政务CA制定并对外广泛发布，同时向国内标准化组织申请标准的对象标识符（OID），从而保证与其他应用相兼容，对象标识符在通信服务中进行传递，作为政务CA证书策略的标识，代表政务CA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，才可以从政务CA去申请和获得证书。

7.1.7 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。

7.1.8 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。

7.1.9 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

政务CA定期签发CRL，其所签发的CRL遵循RFC 5280 标准。

7.2.1 版本号

X.509 V2。

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）

9）CA的公钥标识 (Authority Key Identifier)

10）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，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的OCSP服务遵循 RFC 6960 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 认证机构审计和其他评估

8.1 评估的频率或情形

由政务CA指定审计者。政务CA对国家政务外网的关联单位（包含注册机构等证书体系成员）所有的流程和操作进行审计，检验其是否符合本CP和相应的证书策略的规定，其频率可由政务CA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将选择有运营管理资质、具有信息安全审计经验的审计机构，审计人员必须熟悉公钥基础设施技术，具备上述条件的审计机构对政务CA的运营管理进行一致性审计。

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

按照相关法律法规，参照CPS中的相关章节。

9.4 个人信息私密性

按照相关法律法规，参照CPS中的相关章节。

9.5 知识产权

本CP下的知识产权归政务CA所有。

9.6 权利和责任

9.6.1 政务CA的权利和责任

政务CA的职责是：

1）依据本CP制定CPS。

2）公布CPS，确保提供的服务符合CPS。

3）制定和发布运营政策、操作管理规范、规定登记程序和安全保障措施。

4）与注册机构签订注册服务委托协议，并执行监督，确保证书业务合法合规开展。

9.6.2 注册机构的权利和责任

注册机构的职责是：

1）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。

2）依据本CP和CPS执行证书注册相关操作。

3）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；

4）应承担因在CP规定的用途外使用注册机构管理员证书所造成的损失的责任；

5）对于政务CA提供的属于政务CA专有的技术、软件开发包等只有使用权，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：

a）获得有效合格证书的权利。

b）提出中止或撤销证书的权利。

2）证书持有者负有以下责任：

a）提交申请时，必须提供详细且正确的申请资料。

b）妥善保护证书私钥，及时修改密码。

c）了解并同意接受本政策及电子政务电子认证服务机构CPS及使用要求。

d）密钥被盗或怀疑不安全时，及时向注册机构提出撤销。

9.6.4 证书依赖方的权利和责任

证书依赖方须熟悉本CP以及和证书持有者证书相关的证书策略，了解和遵守证书的使用目的，确保证书确被用于预定的目的。

证书依赖方在信赖证书持有者的证书前，必须查证持有者的数字证书的有效性。

证书依赖方在信赖证书所证明的信任关系前，必须确认该证书记载的内容与所要证明的内容一致。

同意 CP 中关于政务CA责任限制的规定。

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

政务CA在CPS中制定有限责任与免责条款。

9.8 赔偿

政务CA在CPS中制定赔偿相关内容。

9.9 CP的有效期与终止

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

9.10 CP的修订

当出现以下情形时政务CA将对CP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）因其他原因而引起政务CA业务规则发生改变。

CP的修正流程为：

1）在CP修订小组进行修改并提交政务CA决策层批准；

2）再次进行审议和生效，并通过政务CA网站或其他方式发布。

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

本CP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，其他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、互联网或其他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《策略》与其他规定、指导方针相互抵触，用户必须接受本《策略》的约束，除非本《策略》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《策略》。

在政务CA与包括用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，均视为双方均同意按本《策略》的规定执行；对协议中不同于本《策略》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。