中国电子口岸数据中心
电子政务电子认证业务证书策略

中国电子口岸数据中心

目　　次

1 概括性描述

中国电子口岸数据中心于 2001 年 5 月 18 日经中央机构编制委员会办公室批准成立，系海关总署具有独立法人资格的直属事业单位。经国家密码管理局批准，中国电子口岸数据中心于 2010 年 12 月 13 日纳入电子政务电子认证服务机构目录（编号 B003）。

电子认证业务证书策略（CP，Certificate Policy）是电子认证服务机构对其提供的电子认证服务所涉及的主要内容及要求的详细描述。本《电子政务电子认证业务证书策略（CP）》按照《电子政务电子认证服务管理办法》和《电子政务电子认证服务业务规则规范》的有关要求起草和管理。

1.1 电子认证业务范围

电子政务电子认证业务范围包括向政务部门和企事业单位、社会团体、社会公众等用户提供的数字证书申请、数字证书签发、数字证书更新和数字证书撤销等数字证书全生命周期管理服务。

1.2 电子认证活动参与者

1.2.1 认证机构

中国电子口岸数据中心是电子政务电子认证服务机构，以下简称 CA 机构。

CA 机构是受用户信任，负责签发并管理身份认证数字证书的权威机构，是签发数字证书的实体。

1.2.2 注册机构

中国电子口岸数据中心在各地的分支机构是数字证书注册审批机构（以下简称 RA 机构）。

RA 机构作为受理数字证书申请、签发、更新和撤销等业务的实体，主要负责提供数字证书业务办理服务。

1.2.3 订户

从 CA 机构接收证书的实体称为订户。

1.2.4 依赖方

依赖于数字证书真实性的实体称为依赖方。依赖方可以是、也可以不是证书持有者。

1.2.5 其他参与者

其他参与电子认证相关服务的实体称为其他参与者。

1.3 电子认证策略管理

1.3.1 管理机构

本《电子政务电子认证业务证书策略（CP）》的管理机构为网络和信息安全部，由网络和信息安全部根据最新的政策法规、标准规范以及业务发展需要，组织制定、修订、评审、发布本 CP。

1.3.2 联系方式

本 CP 的策略机构联系方式如下：

网站地址：https://www.chinaport.gov.cn

联系地址：北京市顺义区李桥镇新桥 29 号地中国电子口岸数据中心

电话号码：010-95198

1.3.3 批准程序

本 CP 由网络和信息安全部组织制订，提交数据中心专业技术管理委员会审核并经分管网络安全工作的中心领导批准后发布。

1.4 定义和缩写

1.4.1 术语和定义

公钥基础设施 public key infrastructure（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。

公钥 public key：非对称密码算法中可以公开的密钥。

私钥 private key：非对称密码算法中只能由拥有者使用的不公开密钥。

数字证书 digital certificate：也称公钥数字证书，由数字证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人数字证书、机构数字证书和设备数字证书，按用途可分为签名数字证书和加密数字证书。

证书更新 Certificate update：指在不改变密钥的情况下，用一个新数字证书来代替旧数字证书的过程。

密钥更新 key update：用一个新密钥来代替旧密钥的过程，通常指数字证书与密钥同时更新。

1.4.2 符号和缩略语

CA	认证机构(Certification Authority)
CP	证书策略（Certificate Policy）
CPS	数字证书业务声明（Certification Practice Statement）
CRL	数字证书撤销列表(Certificate Revocation List)
LDAP	轻量级目录访问协议(Lightweight Directory Access Protocol)
OCSP	在线数字证书状态协议（Online Certificate Status Protocol ）
RA	注册机构(Registration Authority)
LRA	数字证书注册受理点（Local Registration Authority）

2 身份标识与鉴别

2.1 数字证书命名与格式

2.1.1 证书类别

CA 机构可提供以下类型的数字证书：

1. 机构数字证书

用以代表政务机关和参与电子政务业务的企事业单位、社会团体或其他组织的身份，如：代表单位和部门等机构身份数字证书。

2. 个人数字证书

为各级政务部门的工作人员和参与电子政务业务的社会公众颁发的数字证书，用以代表个体的身份，如：某企业法定代表人/负责人、某企业业务操作员、某局职员的数字证书等。

3. 设备数字证书

为电子政务系统中的服务器或设备颁发的数字证书，用以代表服务器或设备的身份，如：服务器身份证书、IPSec VPN 设备证书等。

2.1.2 证书命名

CA机构通过甄别名（DN，Distinguished Name）来唯一标识数字证书使用者的身份信息。不允许使用匿名或假名。

2.1.3 证书版本

X.509 V3。

2.2 证书申请人的身份确认

2.2.1 证明持有私钥的方法

CA 机构通过如下方式对申请者拥有私钥的方法进行验证：

1. 签名私钥是否通过国家密码管理局核准的密码设备中产生，由数字证书申请者专有；

2. 数字证书申请者是否使用其私钥对数字证书请求信息进行数字签名；

3.CA 使用数字证书申请者公钥验证数字申请者对数字证书请求信息进行的签名。

2.2.2 组织机构身份的鉴别

组织机构在申请数字证书时，应向 CA 机构提交用于身份鉴别的必要材料，包括但不限于：

1. 办理数字证书业务相关的业务申请表单（需机构主要负责人签字，并加盖本机构公章）；

2. 组织机构有效主体资格证明材料（如：工商营业执照、事业单位法人证书等）；

3. 组织机构法定代表人/主要负责人身份证明材料（包括：中华人民共和国居民身份证，无居民身份证的，可以使用护照、台湾居民来往大陆通行证或港澳居民来往内地通行证）；

4. 组织机构授权的经办人身份证明材料（包括：中华人民共和国居民身份证，无居民身份证的，可以使用护照、台湾居民来往大陆通行证或港澳居民来往内地通行证）。

由 RA 机构对组织机构提交的身份鉴别材料进行审核，根据审核情况批准或拒绝数字证书申请请求。

2.2.3 个人身份的鉴别

组织机构内的个人在申请数字证书时，应向 CA 机构提交用于身份鉴别的必要材料，包括但不限于：

1. 办理数字证书业务相关的业务申请表单（需机构主要负责人签字，并加盖本机构公章）；

2. 证书申请者身份证明材料（包括：中华人民共和国居民身份证，无居民身份证的，可以使用护照、台湾居民来往大陆通行证或港澳居民来往内地通行证）；

3. 组织机构授权的经办人身份证明材料（包括：中华人民共和国居民身份证，无居民身份证的，可以使用护照、台湾居民来往大陆通行证或港澳居民来往内地通行证）。

4. 在把数字证书签发给政府部门中的个人时，还应向 CA 机构提交数字证书持有者的在职证明。

由 RA 机构对个人身份鉴别材料进行审核，根据审核情况批准或拒绝数字证书申请请求。

2.3 密钥更新请求的识别与鉴别

2.3.1 常规的密钥更新请求的识别与鉴别

对于一般正常情况下的密钥更新申请，数字证书持有者应提交能够识别原数字证书的足够信息，并使用更新前的私钥对包含新公钥的申请信息签名。

1. 订户数字证书有效期内更新密钥：需提供相关身份证明，联系 RA 机构更新。CA 机构使用原数字证书上的证书持有者公钥对密钥更新申请进行验证，以实现对订户身份的实体鉴别。

2. 订户数字证书超出有效期更新密钥：订户需采用与新申请数字证书相同的流程办理，经过与初始身份确认相同的实体鉴别流程。

2.3.2 撤销之后的密钥更新请求的识别与鉴别

数字证书撤销后不能进行密钥更新。

如订户重新办理数字证书，需采用与新申请数字证书相同的流程办理，经过与初始身份确认相同的实体鉴别流程。

2.4 证书变更请求的识别与鉴别

订户证书信息发生变更时，应申请重新签发数字证书，CA 机构在受理该申请时，将对原证书进行撤销处理。

证书变更需经过与初始身份确认相同的实体鉴别流程。

2.5 证书撤销请求的身份标识与鉴别

数字证书撤销请求可以来自数字证书持有者，也可以来自 CA 机构、RA 机构。

数字证书持有者通过 RA 机构申请撤销数字证书时，其身份标识和鉴别使用原始身份验证相同的流程。

由 CA 机构、RA 机构申请撤销证书持有者的证书时，不需要对证书持有者身份进行标识和鉴别。

3 数字证书服务操作规范

3.1 数字证书申请

3.1.1 申请的提交

机构证书由组织机构授权的人员申请；个人证书由证书持有者本人经所在组织机构授权后申请，或者由所在组织机构授权的人员申请；设备证书由设备所属组织机构授权的人员申请。

申请人可以通过在线方式或到 RA 机构现场提交数字证书申请，证书申请材料见 2.2。

3.1.2 注册过程及责任

申请人应遵循诚实守信原则，在向RA机构申请数字证书时，应当提供真实、完整、准确的信息和资料，如因申请人故意或过失提供的资料不真实，一经发现并核实，RA机构有权退回其数字证书申请或撤销已签发的数字证书。

RA机构收到申请者的申请后，对申请者及申请信息按照本CP2.2的方式进行审核。审核通过后注册申请者的信息；审核不通过的，应告知订户审核不通过的原因。

RA 机构应告知用户数字证书办理须知和使用注意事项。

3.2 数字证书申请处理

3.2.1 执行识别与鉴别功能

RA 机构接收到申请者的数字证书申请后，应按照初始身份鉴别的要求，对数字证书申请者的身份进行鉴别：

1. 核查证书申请材料是否充分、完整；
2. 确认申请者获得了合法有效的授权；
3. 验证证书申请信息与身份证明资料的一致性；
4. 确认申请者已知晓数字证书办理须知，并提交了有效的承诺声明；
5. 对申请资料妥善保管。

3.2.2 数字证书申请批准和拒绝

RA 机构在对申请者经过初始身份鉴别的基础上，决定批准或拒绝申请：

如果拒绝申请，将通过在线方式或面对面方式告知数字证书申请者；

如果批准申请，将为数字证书申请者办理数字证书签发服务。

3.2.3 处理数字证书申请的时间

RA 机构应在 2 个工作日内响应数字证书请求。

3.3 数字证书签发

3.3.1 数字证书签发中 RA 和 CA 的行为

RA 机构将申请者信息录入 RA 系统，通过安全的方式将 DN 信息以及公钥发送至 CA 系统。

CA 系统对 RA 系统提交的 DN 信息以及公钥按照 X.509 证书格式标准组织并生成数字证书，然后发送至 RA 系统完成数字证书签发。RA 机构将签发成功的数字证书交付给证书申请者。

3.3.2 CA 和 RA 通知数字证书申请者数字证书的签发

RA 机构将通过以下几种方式向申请者通告数字证书签发成功：

1. 通过面对面方式或电话通知申请者领取数字证书；
2. 通过系统在线方式向申请者推送数字证书签发成功。

3.4 数字证书接受

3.4.1 构成接受数字证书的行为

证书申请机构主要负责人或机构授权的经办人接收存储数字证书的安全产品介质（智能密码钥匙等），视为确认接受数字证书。

3.4.2 CA 对数字证书的发布

数字证书签发后，CA 通过 LDAP 证书库将数字证书发布至从目录服务器上，用户可查询、下载数字证书。

CA机构不承担在签发数字证书时主动通告其他用户的义务，依赖方可通过目录服务器查询并下载用户的数字证书。

3.5 密钥对和证书的使用

证书持有者的密钥对和证书应当用于规定的、批准的用途。

3.5.1 数字证书持有者私钥和数字证书使用

签名密钥对用于签名与签名验证，加密密钥对用于加密解密。如果密钥对允许用于身份鉴别，则可以用于身份鉴别。密钥对和证书不应用于其规定的、批准的用途之外的目的，否则其应用不受保障。

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

证书持有者应妥善保管数字证书、其对应私钥和安全密码。

3.5.2 依赖方对公钥和数字证书使用

依赖方应按约定的方式对签名信息进行验证：

A. 获得对应的证书及信任链；

B. 签名时验证证书的有效性；

C. 确认该签名对应的证书是依赖方信任的证书；

D. 证书的用途适用于相应的签名；

E. 使用证书上的公钥验证签名。

以上任何一个环节失败，依赖方应该拒绝接受签名信息。未按规定用途使用造成损失的，由依赖方自行承担责任。

依赖方需要发送加密信息给接收方时，可以通过适当途径获得接收方的加密证书，使用接收方的公钥进行信息加密。

3.6 数字证书与密钥更新

3.6.1 数字证书与密钥更新的情形

1. 数字证书与密钥通常同时更新。适用的场景包括：

A. 数字证书即将到期；

B. 数字证书数据损坏；

C. 数字证书对应私钥安全性受到威胁；

D. 技术发展（如：密钥位数已不能保证足够的安全性）。

2. 证书更新业务规则参照密钥更新执行。

3. 被撤销或已过期的数字证书不能进行密钥更新和数字证书更新。

3.6.2 数字证书与密钥更新申请的提交

数字证书持有者、数字证书持有者的授权代表（如：机构数字证书等）或数字证书对应实体的拥有者（如设备数字证书等）在证书满足更新条件时，可以向 RA 机构提交带有数字证书持有者电子签名的更新申请。

3.6.3 处理数字证书与密钥更新请求

同 3.2。

3.6.4 通知数字证书持有者新数字证书的签发

同 3.3。

3.6.5 构成接受更新证书的行为

同 3.4.1。

3.6.6 CA 对更新证书的发布

同 3.4.2。

3.7 数字证书补办

补办是指在数字证书有效期内，数字证书持有者出现数字证书载体丢失或数字证书载体损坏时进行数字证书补发的操作。补发操作成功时，旧数字证书将被撤销。数字证书补办业务的操作流程，按照数字证书申请的身份鉴别和受理流程执行。

3.8 数字证书变更

证书持有者如在数字证书有效期内发生数字证书信息变更，可向 RA 机构提出申请对已签发的数字证书进行信息变更。CA 机构在受理该申请时，将重新签发数字证书，并对原证书进行撤销处理。

数字证书变更业务的操作流程，按照数字证书申请的身份鉴别和受理流程执行。

3.9 数字证书撤销

3.9.1 数字证书撤销的条件

CA机构、RA机构及数字证书持有者在发生下列情形之一时，应申请撤销数字证书：

A. 数字证书持有者不从事原岗位工作；

B. 司法机构要求撤销数字证书持有者数字证书；

C. 数字证书持有者提供的信息不真实；

D. 数字证书持有者没有或无法履行有关规定和义务；

E. CA 机构、RA 机构或最终数字证书持有者有理由相信或强烈怀疑一个数字证书持有者的私钥安全已经受到损害；

F. 政务机构有理由相信或强烈怀疑其下属机构数字证书、个人数字证书或设备数字证书的私钥安全已经受到损害；

G. 与数字证书持有者达成的数字证书持有者协议已经终止；

H. 数字证书持有者请求撤销其数字证书；

I. 法律、行政法规规定的其他情形。

3.9.2 数字证书撤销的发起

以下实体可以请求撤销一个证书持有者证书：

A. CA 机构、RA 机构、电子政务机构或其他部门可依法主动撤销 CA 签发给证书持有者的证书。

B. 对于个人证书，证书持有者经其所在组织机构授权许可后，可以请求撤销他们自己的个人证书。

C. 对于机构证书，只有机构授权的代表有资格请求撤销已经签发给该机构的证书。

D. 对于设备证书，只有拥有该设备的机构授权的代表有资格请求撤销已经签发给该设备的证书。

3.9.3 数字证书撤销的处理

认证机构、注册机构在接到数字证书持有者的撤销请求后，将通过核实身份证明材料、验证预留信息等方式，对其身份进行鉴别并确认其为数字证书持有者本人或得到了数字证书持有者的授权，以保证请求确实来自证书持有者。

验证通过的请求，CA 机构、RA 机构应在 24 小时内，在系统中执行撤销证书操作，并将撤销证书发布到证书撤销列表中。

3.9.4 依赖方检查数字证书撤销的要求

对于安全保障要求比较高并且完全依赖证书进行身份鉴别与授权的应用，依赖方在信赖一个证书前，应当采用以下方法查询数字证书撤销列表确认该数字证书的状态：

1. 应根据证书标明的发布地址获取证书撤销列表。

2. 应验证撤销列表的签名，确认其来自于该证书对应的签发机构。

3. 应验证证书撤销信息，确认证书是否被注销。

3.9.5 CRL 发布方式及频率

CRL 由 CA 系统管理员通过系统的控制菜单手工产生或通过系统的 CRL 产生策略自动生成。CRL

产生后，将通过目录服务器系统发布。

CA 系统 CRL 发布周期为 24 小时，根据实际需要也可实时发布或延时发布。

3.9.6 CRL 发布的最大滞后时间

数字证书从撤销到发布到 CRL 上的滞后时间最长为 24 小时。

3.9.7 在线状态查询的可用性

通过在线查询服务（OCSP）查询证书状态。依赖方可以通过证书状态发布服务器在线查询数字证书撤销状态。

3.10 密钥生成、备份与恢复

证书持有者的签名密钥对由证书持有者的安全产品介质（如智能密码钥匙或智能 IC 卡）中生成，加密密钥对由密钥管理中心 KMC 生成。

签名密钥由证书持有者保管，不做备份，不能恢复。加密密钥由密钥管理中心托管，每天进行数据备份，并可按要求进行密钥恢复。

4 认证机构设施、管理和操作控制

中国电子口岸数据中心按照GM/T0034-2014《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》的要求建设、维护、管理电子认证基础设施。

4.1 物理控制

4.1.1 场所区域与建筑物

CA 机房根据业务功能由外向内划分公共区、RA 区、CA 区、KM 区等区域，安全等级和要求逐级提高。安全等级要求越高，安全防护措施和配套设施要求越严格。其中，CA 区和 KM 区机房使用屏蔽室，以防止电磁干扰，增加系统的安全性，机房屏蔽效果达到 C 级标准。

4.1.2 物理访问

1. CA 区和 KM 区使用厚钢防盗门，安装指纹门禁系统、机械组合锁等装置。在有人操作期间里层门由出入卡系统进行控制；在无人操作期间，外层门加锁保护，能够防止非法进入。

2. 对各个区工作人员权限进行严格划分，工作人员离岗或换岗时将删除或转移其物理访问权限。

3. CA 机房及办公场地所有人员都佩戴标识身份的证明，工作人员需提交申请并经过审批后，方可进入 CA 机房。

4. 留存 CA 机房人员进出记录，并妥善、安全保存。

4.1.3 电力和空调

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

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

机房空调采用高效能、高灵敏度的机房专用精密恒湿空调系统，保证了系统正常运行。

4.1.4 水患防治

机房内无上下水系统，机房内无渗水、漏水现象，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。系统有充分保障，能够防止水侵蚀。

4.1.5 火灾预防和保护

根据 GB50174-93《电子计算机机房设计规范》要求，部署消防自动报警系统和管网型 FM200 气体灭火系统，并为每个独立空间安装感烟和感温探头，能够对火灾发生区域发出报警信号，并能以手动或自动的方式启动灭火设备。

4.1.6 介质存储

存储介质通过温度调节、湿度调节、防火、防水、防静电干扰以及防磁损害等安全措施保证了其物理安全性，同时通过严格的管理制度防止了存储介质的人为损害。

4.1.7 废物处理

存档的敏感数据（包括纸质、光盘、磁盘等介质）已不再需要或存档的期限已满时，将进行销毁处理。加密设备在退出系统前将进行恢复出厂设置。

4.1.8 异地备份

采用磁带数据备份方式，并且保存于异地。

4.1.9 入侵侦测与报警系统

外围是机房所在楼宇的大型综合监控报警系统，具有 24 小时对层楼及重点部位的不间断监控作用；内部采用了专用机房监控系统，对机房内所有通道和主要房间进行实时监控，确保无监控死角。

4.2 操作过程控制

4.2.1 可信角色

CA 机构、RA 机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。可信角色包括：

1. 系统管理员

系统管理员负责 CA 系统日常管理，执行系统的日常监控，并可根据需要签发服务器证书和下级操作员证书。

2. 安全管理员

安全管理员负责 CA 机构的物理、网络、系统的安全管理，拟订安全管理制度和操作流程，监督各岗位安全管理的执行情况。

3. 审计管理员

审计管理员控制、管理、使用安全审计系统，安全审计系统分布于 CA 系统的各个子系统中，负责各个子系统的运行和操作日志记录。

4. 密钥管理员

密钥管理员负责管理密钥相关设备，进行密钥的生成、备份、恢复、销毁等操作。

5. 证书业务管理员

证书业务管理员对 RA 机构操作员进行管理，并对 RA 机构业务进行管理。

6. 证书业务操作员

证书业务操作员进行录入、审核、制作等证书业务操作，直接对用户提供服务。

4.2.2 角色的识别与鉴别

所有在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。系统将独立完整地记录其所有的操作行为。

4.2.3 角色职责分离设置

对每个操作人员的责任和权限进行明确的划分，禁止进行超越安全权限的操作。不同角色由不同人员担任。

4.3 人员控制

4.3.1 可信人员要求

1. CA 机构对工作人员的资格、经历以及经验等情况进行严格审查和核实，工作人员必须无重大工作错误、无违法犯罪行为、无不良信用记录等。

2. CA 机构工作人员必须具有相应的安全意识，经过 PKI 培训和保密教育，签署员工保密协议后，方能录用。

4.3.2 人员培训及再培训

培训及考核工作人员是 CA 机构的责任。CA 机构对人员的培训包括 CA 系统运行维护、CA 系统操作过程、相关业务流程规范、安全管理规范等。此外，培训还包括安全意识和工作人员未来工作中将使用到的软件或工具。CA 机构组织对培训内容进行考核。

CA 机构根据工作人员对培训内容的掌握情况不定期安排再培训，如果 CA 机构升级 CA 系统软硬件或调整相关业务流程，应确保所有的相关工作人员受到适当的再培训。

根据人员岗位以及角色的不同对应不同的培训内容，主要包括：系统硬件安装与维护、系统软件安装与维护、系统软件运行管理、系统物理及数据安全、CA 中心运营管理、相关政策法规、CA 应用软件开发。

4.3.3 工作岗位轮换周期和顺序

对于可替换角色，CA 机构将根据业务安排进行工作轮换。轮换的周期和顺序，视业务的具体情况而定。

4.3.4 违规行为处罚

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

4.3.5 外包服务人员及要求

对非正式签约工作人员，不安排 CA 系统安全管理工作，其他要求与正式员工基本一致。

4.3.6 提供给员工的文档

CA 机构向其员工提供完成岗位工作所需的培训文档和相关操作文档。

4.4 审计日志

4.4.1 审计日志内容

审计日志包括 CA 系统记录与系统相关的事件以及 CA 机构记录与系统不直接相关的事件，主要包括：CA 密钥声明周期内的管理事件、证书生命周期中的各项操作、CA 机房人员访问记录以及人员岗位调整记录等。

CA 机构采用集中方式进行日志记录与管理，日志共分为两类：系统日志与本地日志。

1． 系统日志

系统日志不向外界发行，以避免黑客对系统事务流程的分析。

系统日志的事件记录可以达到通信级，对于系统中的任何细小异常或错误都会记录在案。

系统日志对事件分类共分为四类，分别是：正常、警告、安全及内部错误。通过对不同类型事件的整理可以分析出系统攻击的来源及危害性。对于严重的安全类型及错误型，将产生本地日志文件以防止数据库系统被破坏时的日志丢失。

对于事件来源/产生者有详细的记录，对于动作发起人的证书序列号及 DN、时间、结果等都有清晰的记录，确保日志的完整性。

2． 本地日志

除系统日志外，每个子系统亦在本地存留日志文件。本地日志记录的内容重点是该子系统的日常操作及各项事件。对于这类日志亦分为正常、警告、安全及内部错误四种类型。操作员的一切动作（如登录、退出、审核、选择菜单等）都记录在本地日志中，如果子系统的安全性受到威胁可通过查阅本地日志的方法追踪管理员（或是假冒的管理员）的动作。

本地日志以文件的形式存在于子系统的本地存贮介质上（多是硬盘），本地日志文件达到一定大小后按其后缀尾数自动生成新的日志文件以防止前一日志被覆盖。

系统策略中规定管理员必须定期备份本地日志，以备日后审查。

4.4.2 审计日志处理

CA 机构每周对审计记录进行跟踪处理，如遇到警告、异常或日志满，则及时进行处理。

CA 机构通过日志收集分析系统，实时收集应用日志并归档保存。

4.4.3 审计日志保存期限

审计日志文档保存 10 年。

4.4.4 审计日志保护

审计日志处于严格的保护状态，CA 机构授权的人员才能对审计日志进行相应操作，严禁未经授权的任何操作。

4.4.5 审计日志备份

CA 系统审计日志备份采用数据库自身备份程序，根据记录的性质和要求，按照固定策略进行备份。

4.4.6 审计日志收集

审计日志收集系统涉及 CA 系统、RA 系统、网络和数据库系统等。

4.4.7 对导致事件主体的通告

对于审计日志中记录的事件，对导致该事件的个人、机构等主体，CA 机构不进行通告。

4.4.8 脆弱性评估

CA 机构定期对系统进行漏洞扫描等脆弱性评估，以降低运行风险。

4.5 规定事件记录的类型

1. 证书归档（主要是对已经过期的证书进行归档）；
2. 系统审计日志以及门禁监控日志归档；
3. 数据库归档；
4. 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）

4.6 规定事件记录的内容

1. 事件记录包括事件类型、发生时间、相关内容，以及操作身份的实体；
2. PKI系统的审计事件记录应确保不能被篡改。

4.7 记录归档要求

4.7.1 记录归档的保存期限

所有归档记录的保存期一般规定为十年。

4.7.2 记录归档的保护措施

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处理各种归档文件。

存档环境防水、防火、防潮、防盗。

对于光盘和硬盘等介质定期将数据更新到新介质上。

4.7.3 记录归档的备份程序

对于重要归档文件，采取备份存档，并且存放于不同的物理环境下。

4.7.4 记录归档时间戳要求

所有存档记录都需要按照时间进行分类存放，并且加上时间标识。

4.7.5 获得和检验归档信息的程序

只有被授权的可信人员才能获得归档信息。恢复归档信息后，先进行完整性校验。

4.8 认证机构密钥更替

完成一个CA密钥更新操作时，需要签发下面三个证书：

1. 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。

2. 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）。

3. 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。

4.9 数据备份

1. CA机构建立数据备份管理制度，制定数据备份计划，明确数据备份的内容、周期、备份方式等，定期开展数据备份。

2. CA机构制定容灾备份恢复计划和应急响应预案等，定期进行演练，减少对业务运营的影响。

3. CA机构根据业务需要，建立异地容灾备份。

4.10 损害与灾难恢复

4.10.1 事件和损害的列表

发生故障时，将按照灾难恢复计划实施恢复。

4.10.2 计算资源、软件和数据的损坏

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，将按照灾难恢复计划实施恢复。

4.10.3 实体私钥损害处理程序

当根证书被作废时，会通知订户。

当 CA 的私钥被攻破或需要作废时，根据灾难恢复计划规定的灾难恢复步骤进行操作。

4.10.4 灾难后的业务连续性能力

针对证书系统的核心业务系统，证书签发系统和密钥管理系统采用双机热备方式；对核心数据库，证书管理系统数据库采用磁盘阵列方式来确保证书系统的高可靠性和可用性。

发生自然或其它不可抗力性灾难后，采用异地备份系统对运营进行恢复。

4.11 认证机构或注册机构的终止

因各种情况，需要终止运营时，CA 机构将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。具体将采用以下措施：

1. 起草终止业务声明；
2. 停止认证中心所有业务；
3. 处理加密密钥；
4. 处理和存档敏感文件；
5. 清除主机硬件；
6. 管理系统管理员和安全官员；
7. 通知终止运营相关的实体。

5 认证系统技术安全控制规则

5.1 密钥对的生成和安装

5.1.1 密钥对的生成

订户的签名密钥对由订户的密码设备（如 USB KEY 或智能 IC 卡）生成，加密密钥对由 KMC 生成。

5.1.2 私钥传送给用户

订户的签名密钥对由自己的密码设备生成并保管。

加密密钥对由 KMC 产生，通过安全通道传到订户手中的密码设备中。

5.1.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经 RA 机构传递到 CA。

订户的加密证书公钥，由 KMC 通过安全通道传递到 CA。

从 RA 到 CA 以及从 KMC 到 CA 的传递过程中，采用国家密码管理局许可的通讯协议及密钥算法，保证了传输中数据的安全。

5.1.4 认证机构公钥传送给依赖方

依赖方可以从 CA 机构网站下载 CA 证书，从而得到 CA 的公钥。

5.1.5 密钥的算法

密码算法和长度符合国家密码管理部门的规定。

5.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可的硬件产生。

5.1.7 密钥使用目的

订户的签名密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等，加密密钥对可以用于信息加密和解密。

签名密钥和加密密钥配合使用，可实现身份认证、授权管理和责任认定等安全机制。

5.2 私钥保护和密码模块工程控制

5.2.1 CA 私钥保护方面要求

私钥采用国家密码管理局认定的硬件设备产生；

保存私钥的密码机设备采用 5 选 3 多人控制。；

私钥备份机制，备份操作和备份数据采用 5 选 3 多人控制；

将私钥的管理权限分散到 5 张管理员卡中，只有五人中的至少三人在场并许可的情况下，才能对私钥进行恢复操作。

5.2.2 用户私钥保护方面要求

电子政务的数字证书应用，数字证书对应私钥的生成、存储和使用应得到有效的安全保护；

签名密钥对为数字证书持有者专有，生成、存储和使用受数字证书持有者安全管控；

加密密钥对由密钥管理中心 KMC 提供密钥管理服务。

5.3 密钥对管理的其他方面

5.3.1 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥。他们由 CA 机构和密钥管理中心定期归档。

5.3.2 证书操作期和密钥对的使用期限

颁发给用户的数字证书的有效期与密钥有效期一致。结合业务系统应用需求，一般情况下，其有效期为 10 年，最长不超过根证书有效期。

5.4 激活数据

5.4.1 激活数据的产生和安装

激活数据是保护私钥的密码。证书存储介质出厂时设置了缺省密码。用户使用数字证书之前需要先修改缺省密码。

用于存放有 CA 私钥的密码设备激活信息（秘密分割）的产生过程安全可靠，符合相应的安全要求。

5.4.2 激活数据的保护

对于 CA 私钥的激活数据，CA 机构通过秘密分割将分割后的激活数据由不同的可信人员保管，签署协议确认他们知悉秘密分割保管者责任。

数字证书持有者使用密码保护私钥，数字证书持有者应妥善保管好密码，防止泄露或窃取。

5.4.3 激活数据的其他方面

A. 激活数据的传送

当私钥的激活数据进行传送时，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。

B. 激活数据的销毁

当私钥的激活数据不需要时，应予以销毁，并保护它们在此过程中免于丢失、偷窃、泄露或非授权使用，销毁的结果是无法通过残余信息、介质直接或间接获得激活数据的部分或全部，比如记录有口令的纸张必须粉碎。

5.5 系统安全控制

5.5.1 安全技术措施

计算机系统安全等级采用 TCSEC（受信计算机系统评测标准）安全标准。

5.5.2 安全技术要求

为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。另外，本系统采用增加冗余资源的方法，使系统在有故障时仍能正常工作。 对于设备有一套完整的保管和维护制度：

1. 专人负责设备的领取和保管，做好设备的领用、进出库和报废登记。
2. 对设备定期进行检查、清洁和保养维护。
3. 制定设备维修计划，建立满足正常运转最低要求的易损坏备件库。
4. 对设备进行维修时，必须记录维修的对象、故障原因、排除方法、主要维修过程及与维修有关的情况等。
5. 设备维修时，必须有派专人在场监督。

5.6 网络安全控制

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

CA 系统的网络环境满足密码和网络的安全运行要求，CA 机构制定安全事件管理和应急响应计划，并定期巡检、定期升级安全措施（如入侵检测、漏洞扫描、打补丁等），避免网络攻击和漏洞等带来的运营风险。

5.7 生命周期技术控制

5.7.1 CA 系统运行管理

A. CA 系统的操作流程文档化并进行维护。

B. CA 系统（包括软件、网络等方面）的变更经由 CA 机构运行管理部门批准，经批准的变更实行必须通过测试，并进行记录。

C. 可能对系统的安全性有影响的改动事先会进行风险评估，进行备份并经过批准之后方可实施。

D. CA 中心的测试系统、运营系统、网络设施等，具有专门的操作维护人员，并有相应明确的授权。

E. 操作维护人员定期检查系统及网络的稳定性、安全性及容量，确定符合服务水平。

F. 建立检测和防护控制来防止病毒和恶意软件，并提供适当的报警信息。

G. 建立监控流程，确保记录并报告发现的或怀疑的、对系统或服务有威胁的安全缺陷。建立并执行系统故障报告、处理流程。

H. 建立制度，对 CA 系统相关的媒介（包括设备、数字证书介质、文档等）进行妥善保管，避免非授权的访问。

5.7.2 CA 系统的访问管理

A. 制定 CA 系统的访问策略，内容包括：访问角色及相关权限，认证及鉴别的方法，分权机制，门限秘密共享机制（密钥生成时 m/n 规则）等。

B. 制定 CA 系统访问人员角色职能定义，确保合理的职责分割和权限控制，并明确授权及取消授权的操作流程和策略。

C. 制定网络安全策略，并制定访问网络的控制策略。

D. 制定操作系统及 CA 软件的安全访问的策略。

E. 建立各种对 CA 系统访问的审计措施。

5.7.3 CA 系统的开发和维护

A. 建立 CA 系统软件修订控制流程，对系统新增或修改进行管理。

B. 严格控制对 CA 系统的源代码及测试数据的访问。

C. 操作系统升级变更时，重新测试应用系统软件。

D. 在 CA 系统中，购买、使用或修改的软件，经病毒查杀之后方可部署。

5.8 时间戳

CA系统所有服务器使用同一时间源，证书、CRL、系统日志中的时间信息均保持一致。

6 法律责任和其他业务条款

6.1 费用

6.1.1 免费或收费策略

用户使用 CA 机构的电子认证服务，根据证书实际应用需求决定是否向 CA 机构缴纳证书服务费用。

6.1.2 证书签发和密钥更新费用

在证书有效期内，对该证书信息进行查询，不收取查询费用。

6.1.3 其他服务费用

CA 机构保留收取其他服务费用的权利。

6.2 财务责任

CA 机构保证具有维持其运作和履行其责任的财务能力。

6.3 业务信息保密

6.3.1 保密信息范围

保密的业务信息包括但不限于以下方面：

1. 在双方披露时标明为保密(或有类似标记)的；
2. 在保密情况下由双方披露的或知悉的；
3. 双方根据合理的商业判断应理解为保密数据和信息的；
4. 以其他书面或有形形式确认为保密信息的；
5. 或从上述信息中衍生出的信息。

保密信息包括但不限于以下方面：

最终用户的私人签名密钥都是保密的。

6.3.2 不属于保密的信息

1. 与证书有关的申请流程、申请需要的手续、申请操作指南等信息是公开的。在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

2. 订户数字证书的相关信息可以通过目录服务等方式向外公布。

3. 在目录服务器中公布证书的吊销信息，供网上查询。

6.3.3 保护保密信息的责任

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

6.4 个人隐私保密

6.4.1 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄漏、使用或发布给第三方。

CA 机构将依法保护订户的个人隐私。任何人同意接受 CA 机构的任何服务，则其自动认可本规则关于隐私保密方案。

6.4.2 使用隐私信息的告知与同意

使用隐私信息，须获得本人同意。

6.4.3 依法律或行政程序的隐私信息的使用

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

6.4.4 不被视为隐私的信息

其他信息的披露遵循国家的相关规定处理。

6.5 知识产权

按本 CP 的规定，所有由 CA 机构运营的电子认证系统签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于 CA 机构所有，这些知识产权包括所有相关的文件和使用手册。

6.6 陈述和担保

6.6.1 认证机构的陈述与担保

1. 承诺建立健全 CPS、服务规则、以及其它制度或规则。

2. 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。

3. 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。

6.6.2 注册机构的陈述与担保

1. 为订户提供证书申请业务受理过程完全符合CA机构的CPS所有实质性要求；

2. 确保签发的证书信息与申请者提供的信息完全一致。

6.6.3 用户的陈述与担保

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：

1. 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，并愿意接受检查与核实，愿意无条件承担任何因虚假信息及或资料给 CA 机构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。

2. 保证遵守本规则所约定的条款，并愿意遵守申请、使用规则。

3. 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。

4. 一经接受证书，表示已经熟知本规则及有关协议的内容。

5. 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。

6. 一经接受证书，表示愿意遵守 CA 机构制定或修改的规则、规范或声明、更新、升级等。

6.6.4 依赖方的陈述与担保

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 CA 机构制定的规则、规定或声明或升级、更新等。

6.6.5 其它参与者的陈述与担保

应遵守本 CP 的规定。

6.7 有效期和终止

6.7.1 有效期限

CP 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。

6.7.2 终止

CA 机构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。

6.7.3 效力的终止与保留

CP 的某些条款在终止后继续有效，如知识产权承认和保密条款。另外，各参与方应返还保密信息到其拥有者。

6.8 对参与者的个别通告与沟通

参与者如需进一步了解本 CP 中提及的服务、规范、操作等信息，可以与 CA 机构联系。

6.9 修订

6.9.1 修订程序

网络和信息安全部定期对本 CP 进行适用性评估，评估结论为需要修订的，组织 CP 编写小组进行修订。

6.9.2 通知机制和期限

本 CP 版本更新时对具体个人不做另行通知。

6.9.3 必须修改业务规则的情形

1. 本 CP 所描述的规则、流程和相关技术已经不能满足 CA 机构业务时；
2. 本 CP 依据的法律法规和部门规章变更时。

6.10 与适用法律的符合性

电子认证服务活动参与者所需遵守的适用法律，主要有：

1. 中华人民共和国电子签名法
2. 中华人民共和国网络安全法
3. 商用密码管理条例
4. 电子认证服务密码管理办法
5. 电子政务电子认证服务管理办法

6.11 其他条款

CA机构对本CP拥有最终解释权。