北京国富安电子商务安全认证有限公司

证书策略

(CP)

版本1.0

生效日期： 2009 年 5 月 12 日

声明：

国富安CA证书策略（GFA CP）是由国富安公司安全策略管理委员会制定并发布，版权归国富安公司所有，未经国富安公司书面同意，本文件的任何部分不得以任何方式、任何途径转载、传播、使用。

已经国富安公司授权使用的，应在授权范围内使用，并注明"来源：北京国富安电子商务安全认证有限公司"。

如因作品内容、版权和其它问题需要同本公司联系的，请在30日内进行。公司名称：北京国富安电子商务安全认证有限公司。地址：北京经济技术开发区荣华中路11号中国国际电子商务中心709。电话：(8610-67800320),传真：（8610-67800318），电子邮件：gfacasupport@ec.com.cn

国富安CA证书策略

北京国富安电子商务安全认证有限公司版权

地址：北京经济技术开发区荣华中路11号

邮编：100176

电话：（8610）-67800320

公司网址：www.cacenter.com.cn

运营网址：www.gfapki.com.cn

目录

1. 简介

北京国富安电子商务安全认证有限公司成立于 1998 年 12 月，简称“国富安 CA”。 国富安 CA 是在公众网络（例如 CHINANET、CIETNET 等，以下简称公网）上进行电子商务活动的安全基础设施。该体系和与之配套的安全技术在整个公众电子商务平台中处于基础结构地位。

本文件是国富安CA证书策略（CP）。本CP是一个以公钥基础设施（Public Key Infrastructure，PKI）为基础的证书策略，它制定了各种应用的数字证书的策略，适合于广大的、对通信和信息安全方面有各种各样的需求的公众用户。

本CP是管辖国富安CA所有证书的主要策略说明。它严格按照《中华人民共和国电子签名法》和《电子认证服务管理办法》的要求，以及相关管理规定，为批准、签发、管理、使用、吊销和更新证书和相关的可信服务制定商务、法律和技术上的规范。这些规范应用于所有PKI参与者，保护证书的安全性和完整性，遵循本CP 的认证机构应根据本CP 制定认证业务声明（CertificationPractices Statement），及其他的管理规范和辅助协议。

北京国富安电子商务安全认证有限公司安全策略管理委员会PMA负责CP 的修改、更新、及评述整理工作。PMA还负责检查CP 要求的遵守情况。

本文档的编写遵从《中华人民共和国电子签名法》、《电子认证业务管理办法》等法律和行政法规、以及IETF RFC 3647 （ Internet X.509 Public KeyInfrastructure Certificate Policy and Certification Practices Framework，公钥基础设施证书策略和证书运行框架）标准。

1.1 概述

本证书策略为整个国富安CA签发的证书制定了要求，参与国富安CA证书活动的当事人以及第三方均在其合理合法的管辖范围内。本证书策略默认使用证书当事人及其第三方熟知《中华人民共和国电子签名法》及《电子认证业务规则》，如欲了解相关知识可在http://www.gfapki.com.cn获得。

1 1.1.1 证书类别

1.1.1.1 第 1 类证书

在国富安CA信任域中，第1 类证书是个人证书，提供较低级的安全保证，国富安CA签发的这类证书在满足《中华人民共和国电子签名法》及其他规定要求下，由其产生的电子签名符合《中华人民共和国电子签名法》的要求。个人证书，提供基本的安全保障，与个人在社会中的职务与地位没有关系，如同公安局发的身份证一样；只承担由个人行为所引发的责任。依据订户的要求，该类证书可以与自然人的电子名章相对应。自然人证书里可以包含职业资格要素，增加国家法定承认的职业资格鉴定。第1 类证书申请的验证过程是基于在国富安CA信任域中订户甄别名的唯一性和确定性，它们主要用于个人证书的数字签名、加密、非商业性的访问控制或无需提供身份证明的低额交易。

1.1.1.2 第 2 类证书

国富安CA签发的第2 类证书在满足《中华人民共和国电子签名法》的其他规定要求下，由其产生的电子签名符合《中华人民共和国电子签名法》的要求。第2 类证书包括组织机构、企业授权人证书；组织机构、企业法人证书；组织机构、企业部门证书；组织机构、企业身份证书。

1.1.1.2.1 组织机构授权人证书

组织机构、企业授权人证书，提供比自然人证书更高一级的安全保障，代表个人在组织机构、企业中的职务和地位，每一个人在不同的组织机构、企业中可以拥有不同的授权人证书，承担与所代表组织、机构内相应的责任。此证书的验证过程除了第1 类证书的验证过程外，还必须将证书申请者提交的信息与商业记录或数据库中的信息、或国富安CA批准的第三方身份验证服务数据库中的信息进行比较。

1.1.1.2.2 组织机构、企业法人证书

组织机构、企业法人证书，该证书代表组织机构、企业的注册法人，与组织机构、企业的唯一身份证书具有相同的用途，承担相同的责任与义务，依据订户的要求，该类证书可以与组织机构、企业的法人名章相对应。此证书的验证过程除了第1 类证书的验证过程外，还必须将证书申请者提交的信息与商业记录或数据库中的信息、或国富安批准的第三方身份验证服务数据库中的信息进行比较。

1.1.1.2.3 组织机构、企业部门证书

组织机构、企业部门证书，由组织机构、企业授权的部门，承担其所在部门内的责任和义务。依据订户的要求，该类证书可以与相应部门的电子业务章相对应。此证书的验证过程除了第1 类证书的验证过程外，还必须将证书申请者提交的信息与商业记录或数据库中的信息、或国富安批准的第三方身份验证服务数据库中的信息进行比较。

1.1.1.2.4 组织机构、企业身份证书

组织机构、企业身份证书，代表组织机构在中华人民共和国境内网络身份，直接或间接(通过委托授权人证书)承担企业网上行为责任。依据订户的要求，该类证书可以与组织机构、企业的电子公章或合同章相对应。此证书的验证过程除了第 1 类证书的验证过程外，还必须将证书申请者提交的信息与商业记录或数据库中的信息、或国富安批准的第三方身份验证服务数据库中的信息进行比较。

1.1.1.3 第 3 类证书

第 3 类证书包括个人服务器证书和组织机构、企业服务器证书。

1.1.1.3.1 个人服务器证书

个人服务器证书使浏览器可以鉴别个人网站服务器的身份，并创建 SSL 加

密通道以使双方进行加密会话。个人服务器证书是一种加强了的服务器证书，提供 128 位 SSL 会话加密强度。

1.1.1.3.2 组织机构、企业服务器证书

组织机构服务器证书使浏览器可以鉴别组织机构服务器的身份，并创建 SSL 加密通道以使双方进行加密会话。组织机构服务器证书是一种加强了的服务器证书，提供 128 位 SSL 会话加密强度。

1.2 文档名称与标识

本文档称为国富安CA证书策略（GFA CP），此为一个覆盖了三类数字证书的证书策略。目前版本号为V1.0，在国富安CA运营网站发布，网站地址为www.gfapki.com.cn。

1.3 电子认证活动参与者及其职责

2 1.3.1 认证机构（CA）

认证机构（Certification Authority，简称CA）作为可信第三方，对个人、实体及设备进行主题信息及其它属性与公钥绑定的确认。系统承担证书签发、审批、吊销、查询、证书及黑名单发布、密钥和证书管理、政策制定等工作，设在国富安CA北京经济技术开发区运营主机房，不直接面对用户证书，采用两层结构，第一层为根CA，负责制定国富安CA电子认证总体政策与策略，为下级运营CA签发并管理CA证书，负责与其他CA信任体系进行交叉认证。第二层为运营CA，直接为用户签发并管理数字证书，该层CA可以根据用户证书策略不同分为多个运营CA。

3 1.3.2 注册机构（RA）

注册机构（Registration Authority，简称RA）为CA 建立起注册过程，确认证书申请者的身份，批准或拒绝证书申请者。在用户获得证书前，它必须以申请者的身份来注册证书。证书申请者必须从CA 或RA 建立的注册过程来完成注

册，并将注册信息提交给CA 或RA。CA 或RA 将对申请者的身份及其它属性进行确认，然后决定是签发还是拒绝该请求。如果签发证书，则证书将被发送给申请者。RA 还可以根据用户需要吊销证书，尽管是CA 的系统完成最终的吊销工作，并将证书加入到证书吊销列表(CRL)中去，或是在CA 信息库中显示证书已吊销。

4 1.3.3 订户

从电子认证服务机构接收证书的实体。在电子签名应用中，订户即为电子签名人。

5 1.3.4 依赖方

信赖方指为某一应用而使用、信任其他方证书的个人或组织。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。

6 1.3.5 其他参入者

其他参与者指为国富安 CA 提供相关服务的其它实体，如提供第三方身份鉴定的机构和组织。

1.4 证书使用

7 1.4.1 合适的证书应用

本 CP 描述了在国富安CA信任域中规范使用1-5类证书的行为，每一类证书通常适用的应用。通过合同或在法律允许的范围内，PKI参与者可以将证书用于比本CP 描述的应用安全高的应用，但是任何这种用法，必须仅限于这些实体，并且这些实体须为这种用法带来的任何伤害和赔偿承担唯一的责任。

国富安CA证书允许信赖方验证数字签名，签名信息验证通过则标明该签名操作是合法的，并且不受签名操作或订户所处地理位置的限制。

1.4.1.1 1 类证书的应用

一类证书是个人证书，提供基本的安全保障，它主要用于提供个人的身份证明，能够用于数字签名、加密和访问控制。可应用于网上银行、电子支付、安全邮件、SSL安全代理等应用。

1.4.1.2 2 类证书的应用

1.4.1.2.1 2 类组织机构授权人证书的应用

组织机构授权人证书提供的订户身份保证是基于必须确认：订户组织机构确实存在，该组织机构授权证书申请，并且订户提交证书申请的人获得授权这么做。组织机构授权人证书适用于各类应用，包括但不限于代表组织机构进行网上交易、网上业务申报等，提供中高等担保级别的保证。组织机构授权人证书还适用于客户端的鉴别，可以提供诸如数据库或网站的访问控制，以及提供电子邮件的签名加密。

1.4.1.2.2 2 类组织机构法人证书的应用

组织机构法人证书提供的订户身份保证是基于必须确认：订户组织机构确实存在，该组织机构法人信息真实。组织机构法人证书适用于各类应用，包括但不限于代表组织机构进行网上交易、网上业务申报、签署文件等，提供高等担保级别的保证。组织机构法人证书还适用于客户端的鉴别，可以提供诸如数据库或网站的访问控制，以及提供电子邮件的签名加密。

1.4.1.2.3 2 类组织机构部门证书的应用

组织机构部门证书提供的订户身份保证是基于必须确认：订户组织机构确实存在，该组织机构部门的授权证书申请，并且提交证书申请的人获得授权这么做。组织机构部门证书适用于各类应用，包括但不限于代表组织机构进行网上交易、网上业务申报、签署业务受理文件等，提供高等担保级别的保证。组织机构部门

证书还适用于客户端的鉴别，可以提供诸如数据库或网站的访问控制。

1.4.1.2.4 2 类组织机构身份证书的应用

组织机构身份证书提供的订户身份保证是基于必须确认：订户组织机构确实存在，并且提交证书申请的人获得授权这么做。组织机构身份证书适用于各类应用，包括但不限于代表组织机构进行网上交易、网上业务申报、签署文件、协议、合同等，提供高等担保级别的保证。组织机构证书还适用于客户端的鉴别，可以提供诸如数据库或网站的访问控制。

1.4.1.3 3 类证书的应用

1.4.1.3.1 3 类个人服务器的证书应用

个人服务器证书代表以个人申请的域名或其他设备证书，由于该域名或设备为个人拥有，根据法律不能从事经营活动，所以不承担由此引发的责任，该证书仅保障该域名或设备的身份，负责建立安全对话连接和身份证明。

1.4.1.3.2 3 类组织机构服务器的证书应用

组织机构、企业服务器证书，代表由组织机构、企业申请的域名或设备证书，由于该域名为企业拥有，代表组织机构、企业从事电子商务和其他经营活动，所以承担由此引发的责任。服务器证书使浏览器可以鉴别网站服务器的身份，并创建 SSL 加密通道以使双方进行加密会话。服务器证书是一种加强了的服务器证书，提供128 位SSL 会话加密强度。

8 1.4.2 受限的应用

一般而言，国富安CA证书是一般性目的的证书。国富安CA证书可以在全球范围内使用，并且可以和不同的信赖方之间相互操作。国富安CA证书的使用通常不只限于特定的商业环境，如导航、金融服务系统、行业市场环境或虚拟商场。尽

管如此，证书的受限使用是允许的，在他们自己环境中使用证书的客户可以对证书在这些环境中的使用增加更加严格的限制。但是认证机构不对实施这些环境中的这种限制负责。

国富安CA不适用于下列情况：

（1）订立或执行遗嘱；

（2）商业票据；

（3）创设、行使或执行一项契据、信托声明或除法定信托或推定信托以外的代理授权书；

（4）任何用于买卖不动产或其他方式处分不动产的契约及不动产下所发生利益的契约；

（5）不动产转移或不动产利益的转让；

（6）产权证书；

（7）其它任何危害国家，社会及他人人身与财产安全的范围

1.5 策略管理

9 1.5.1 策略文档管理机构

管理本 CP 的机构是国富安CA安全策略管理委员会，由国富安CA安全策略管理委员会负责对本CP的制定、发布、更新等事宜。其联系地址如下：

北京国富安电子商务安全认证有限公司

北京经济技术开发区荣华中路11号中国国际电子商务大厦7层

部门：CA运营部

电话号码：010－67800320

传真号码：010－67800318

邮箱地址：cabpm@ec.com.cn

10 1.5.2 联系人

本CP在国富安CA网站发布，对具体个人不另行通知。

网址：http://www.gfapki.com.cn

邮箱：cabpm@ec.com.cn

联系地址：北京经济技术开发区荣华中路 11 号中国国际电子商务大厦 7 层

邮编：100176

联系电话：010－67800320

传　　真：010－67800318

11 1.5.3 决定 CPS 符合策略的机构

本CP由国富安CA安全策略管理委员会制定并执行。

12 1.5.4 CPS 批准程序

国富安 CA 安全策略管理委员会负责 CP 和 CPS 的管理。国富安 CA 安全策略管理委员会对 CP 和 CPS 草案进行评审，如果符合证书策略，将批准 CPS，之后在国富安 CA 网站上对外公布。从对外公布之日起三十个工作日之内向信息产业部备案。

1.6 定义与缩写

13 1.6.1 定义

激活数据	不同于密钥的数据值 （如 PIN，验证短语，biometric 或是人工掌握的密钥份额），用来操作加密模块，须被保护
鉴定	核实实体（如个人，公司，或机构）所声称的身份
证书	是一种信息，包含的基本信息有：签发证书的认证中心，用户的名称，用户的公钥，证书的操作期，及签发证书的认证中心的数字签名。
证书策略（CP）	一套命名的规则，指定了证书对于特定群体的适用性和/或有共同安全要求的应用等级。

证书的密钥更新（Re-key）	有现成密钥对和证书的用户在新的密钥对产生之后接收了新的证书从而得到新的公钥。
证书的更新	用户得到了现有证书的一段新的有效期限
证书请求	RA 向 CA 呈交的确认的注册请求，注册证书中用户的公钥。
证书撤消列表（CRL）	被撤消的证书列表，由发证 CA 数字签名
认证中心(CA)	制作并签名证书的并被一个或多个依赖方信任的机构，CA 可取消它所制作并签发的证书。
认证实施声明（CPS）	认证机构应用于签发证书的实施声明。认证实施声明定义了 CA 为满足所支持的证书政策规定的要求而采用的设置，政策和程序。
损害	对安全系统的违反，因而可能导致敏感信息的未授权的泄露，修改，置换或使用
加密硬件(加密装置)	硬件加密模块
加密模块	一套硬件，软件，韧件或某种结合，在其中可执行密码逻辑，包括加密算法。一种可以实行密码功能（如加密，鉴定，密钥生成）的装置。
数字签名	数据的密码转换，当与数据单位相连时，提供鉴定起源，使数据完整和防止签名者抵赖的服务。
事件日志（审计日志或审计记录）	按照时间顺序对系统活动的记录，可以再现，评估和检查从事项的开始到最后结果的输出中每一事件周围的或导致每一事件的环境和活动序列。
密钥托管	私钥交由第三方保管，任何对被托管的密钥的访问，如法律实施官员的访问，都应符合事先定义的条件。

密钥恢复	当实体的私钥或对称的加密密钥丢失，被破坏，或不能获得时，从安全的存储库中恢复这些密钥能力。
目标重用	对包含一个或多个目标的介质主体（如页帧，磁盘扇区，磁带）的重新赋值。为安全的分配，该介质不应包含原先目标的剩余数据。
在线证书状态查询协议(OCSP)	可取代或补充定期的 CRL 的确定证书的当前状态的协议。该协议说明了检查证书状态的应用和提供该状态的服务器之间应交换的数据。
政策中心	政策中心有制定维护它自己的和下级机构操作的政策的职责。
公钥基础设施（PKI）	为了推动拥有非对称公钥的公共成分与拥有对应私钥的特定用户之间可证实的联系，采用数字签名技术的硬件，软件，人员，程序和政策的结构。公钥可被用来证实数字签名，鉴定通讯对话中的主体，和/或，交换或流通信息加密密钥。
注册中心（RA）	负责辨认和证明证书主体的实体，它不是 CA 因此不能签名或签发证书。RA 可以协助证书的申请，撤消或两者。
注册请求	某实体向 RA（或 CA）注册该实体在证书中的公钥的申请
注册回应	由 RA（或 CA）发出的回应注册申请的信息。
依赖方	证书的接受者，他信任证书中的信息或发证 CA 公布的其他信息，如 CRL（注：在此文件中，术语“证书使用者”和“依赖方”可互用。
资源库	分布或使证书或证书状态信息可利用的方法（如数据库或 X.500 目录）
根认证机构（根 CA）	CA 等级中地位最高的 CA
用户	公钥被公钥证书证实的实体

可信的计算系统（TCB）	计算机系统中的全体保护装置——包括硬件，韧件和软件——它们的结合负责执行安全政策。TCB 由一个或多个共同执行某个产品或系统的安全政策的成分组成。TCB 正确执行安全政策的能力完全由 TCB 内的装置和系统管理人员对安全政策的参数的正确输入所决定。
可信路径	终端人员可直接与可信的计算系统通信的机制。该机制只能由该人员或可信计算系统所激活，且不能被非置信的软件所效仿。
验证（Validation）	依赖方检查证书状态的过程。
确认（Verification）	为专有通信比较两种层次的系统规格的过程（如有最高规格的安全政策，有源码的 TLS，或有目标码的源码）。
查证（Verify）	是与数字签名相关的一种方法，为准确地确定：（1）数字签名是在有效证书的操作期内由对应于证书公钥的私钥制作的；（2）数字签名被制作后信息没有被改变。

14 1.6.2 缩写表

CA	安全认证机构 (Certification authority)
CPS	认证业务声明 (Certification practice statement)
CRL	证书黑名单 (Certificate revocation list)
CSR	证书签名请求 *（Certificate Signing Request）*

DAM	修改草本(ISO 标准) *（draft amendment(to an ISO standard)）*
FIPS	联邦信息处理标准 *(Federal Information Processing Standard)*
FTP	文件传输协议 *（File Transfer Protocol）*
GFA CA	北京国富安电子商务安全认证有限公司 (Beijing Guo Fu An Security Electronic Commerce CA Co.，Ltd.)
GMT	格林威治标准时间 *（Greenwich Mean Time）*
HTTP	超文本传输协议 (Hypertext Transfer Protocol)
HTTPS	安全套接层下的超文本传输协议 (Hypertext Transfer Protocol with SSL)
LRA	地方注册机构 (Local registration authority)
LRAA	地方注册机构管理员 (Local registration authority administrator)
NSI	未经证实的用户信息 (Nonverified subscriber information)
OCA	操作 CA (Operation Certification Authority)
PCA	政策 CA (Policy certification authority)
PCS	公共认证服务 (Public certification services)
PIN	个人识别码 (Personal identification number)

PKCS	公钥加密标准 *（Public Key Cryptography Standards）*
PKI	公钥基础设施 (Public key infrastrUCTure)
RCA	根 CA （Root Certification Authority）
RDN	相关区别名称 *（Relative Distinguished Name）*
RPA	信赖方协议 (Relying Party Agreement)
RSA	一种加密算法（见定义） (a cryptographic system (see definitions))
SET	安全电子交易 *（Secure Electronic Transaction）*
S/MIME	安全的多用途网络邮件延伸格式 (Secure Multipurpose Internet Mail Extensions)
SSL	安全协议层 *（Secure Sockets Layer）*
URL	单一资源地址 *（uniform resource locator）*
WWW or Web	万维网 （World Wide Web）
X.509	国际电信联盟认证体系的证书标准 （the ITU-T standard for certificates and their corresponding authentication framework）

2. 信息发布与信息管理

2.1 信息库

认证机构应有信息库用于各类信息的发布，如证书策略、认证业务声明、协议、证书、证书吊销列表。认证机构应在其认证业务声明、信赖方协议等中指明有关信息发布、获取的位置。

2.2 认证信息的发布

认证机构需发布的认证信息包括，证书策略、认证业务声明、订户协议、信赖方协议、证书及证书状态。

2.3 发布的时间或频率

国富安 CA 的 CP、CPS、订户协议、依赖方协议，通过信息库 7X24 可获得。国富安 CA 签发的订户证书一经签发即发布到 LDAP 服务器供用户下载，同时订户可通过证书服务站点获得已签发的证书。通过 OCSP 对证书状态的查询是及时的。国富安 CA 对每个证书签发 CA 发布一个证书吊销列表，发布该 CA 签发的证书中的已吊销了的证书。证书吊销列表一般是每 24 小时更新一次。

2.4 信息库访问控制

在国富安CA网站或者目录服务器公布的信息属于公开信息，任何人可以免费查阅这些信息。国富安CA要求访问CP、证书、证书状态、CRL等信息的任何人必须遵守本CP、依赖方协议和CRL使用协议。这里的一个例外是OCSP，允许OCSP 作为一种付费服务。

3. 识别与鉴别

3.1 名称

15 3.1.1 名称类型

根据实体的类型不同，实体名字可以是姓名、组织机构、企业名称、部门名称、域名、商标名、IP 地址等或其相应的身份证号码和组织机构代码。

国富安CA最终订户证书的主题域中包含一个X.500甄别名（遵从关于X.500标准，并用X.501PrintableString格式）。

16 3.1.2 对名称有意义的要求

主题和签发者的DN遵循PKIX标准，并且在证书中标明。

最终订户证书包含的命名应具有通常理解的语义，用它可以确定证书主体中的个人、机构或设备的身份不允许使用假名或伪名。

17 3.1.3 订户的匿名或伪名

在国富安 CA 证书服务体系中，订户不能使用匿名、伪名或虚拟名申请证书。

18 3.1.4 解释不同命名的规则

依 X.500 甄别名命名规则解释。

19 3.1.5 名称的唯一性

认证机构应保证签发给某个实体的证书，其主题甄别名，在 CA 信任域内是唯一的。

20 3.1.6 名称解析

国富安CA免费向所有依赖方组织或个人、应用提供方提供证书解析字符串和解析方法。

21 3.1.7 商标和订户的信息与鉴证

国富安 CA 签发的证书的主题甄别名中可以包含商标名或订户签名信息。

3.2 初始身份确认

22 3.2.1 证明拥有私钥的方法

国富安 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，或其他国富安 CA 批准的方法，验证证书申请者拥有私钥。

23 3.2.2 组织机构身份的鉴别

在把证书签发给一个组织机构、组织机构拥有的设备或组织机构的代表人时，认证机构须对订户所在组织机构进行身份鉴别。对组织机构身份鉴别应该包括如下两个内容：

（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，如营业执照、组织机构代码证，或通过权威的第三方数据库确认。

（2）确认该组织机构知晓并授权证书申请，代表组织机构提交证书申请的人是经过授权的，如提交证书申请授权书，或者确认的方式可以是通过可靠的第三方实现。

对于特殊情况，国富安CA可以采用其他方式追加组织机构身份鉴证的权利。

24 3.2.3 个人身份的鉴别

对于个人证书的鉴别，需通过审核个人身份的真实性：证明证书申请者个人

身份确实存在，如出示个人身份证，如果非本人申请需出具委托函和委托人个人证件，也可以采用其他第三方数据库或有效手段进行验证。

对于特殊情况，国富安CA可以采用其他方式追加个人身份鉴证的权利。

25 3.2.4 没有验证的订户信息

用户提交鉴定文件以外的信息为没有验证的订户信息。

26 3.2.5 互操作准则

安全互操作性要求不同机构间使用不同的安全产品时，它们之间仍可以建立起信任关系。在本CP互操作准则中依据全球惯行的“功能等同原则”和“技术中立原则”，对符合上述原则的证书均采取相应合理的认证措施以保证证书间的可操作性。

3.3 密钥更新请求的标识与鉴别

27 3.3.1 常规的密钥更新的标识与鉴别

对于根密钥，国富安CA系统需要定期在有效期即将结束时或怀疑密钥遭到攻击的情况下进行密钥更新工作，并严格按照密钥管理程序进行。

对于一般正常情况下的密钥更新申请，订户须提交能够识别原证书的足够信息，如订户甄别名、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。对申请的鉴别须基于以下几个方面：

（1）确认申请更新对应的原证书存在并且由认证机构签发。

（2）使用原证书上的订户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。

28 3.3.2 吊销之后的密钥更新的标识与鉴别

国富安CA不对吊销后的密钥进行更新。

3.4 吊销请求的标识与鉴别

证书吊销请求可以来自订户，也可以来自认证机构、注册机构。证书吊销的方式可以是订户自己吊销，也可以订户要求认证机构、注册机构吊销。批准证书申请的实体（即认证机构、注册机构），在认为必须的时候，有权发起吊销订户证书。

在订户自己吊销时，可接受的鉴别过程如下：

订户在申请证书时需提交一个申请请求，在吊销证书时需提交一个吊销请求，如果请求相匹配，证书吊销自动完成。

订户通过认证机构、注册机构吊销时，可接受的鉴别过程如下：

订户通过一定的方式，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订户联系，确认要吊销证书的人或组织确实是订户本人。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

29 4.1.1 提交证书请求的主体

证书请求可由证书拥有实体或相应的授权人提交。

30 4.1.2 注册过程与责任

认证机构必须设定安全可靠的合法的证书申请方式和程序。注册过程必须做到：

（1） 提供必需的信息。

（2） 保证订户信息不被篡改、私密信息不被泄漏。

（3） 注册过程必须保证所有订户必须明确同意相关的订户协议，才能完成注册

过程。

（4） 按CP § 3.2.1 规定的产生一个密钥对，并将公钥传给认证机构、注册机构。

国富安CA必须严格按照操作流程进行身份鉴别和证书申请，并承担由此引发的责任和义务；另一方面申请者未向国富安CA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、国富安CA造成损失的，应承担相应的法律责任和经济赔偿。

4.2 证书申请处理

31 4.2.1 执行识别与鉴别功能

当认证机构、注册机构接受到订户的证书申请后，应按CP § 3.2 的要求，对订户进行身份识别与鉴别。

32 4.2.2 证书申请批准和拒绝

认证机构、注册机构应在鉴证的基础上，批准或拒绝申请。如果拒绝申请，则应该通过适当的方式、在合理的时间内通知证书申请者。

33 4.2.3 处理证书申请的时间

认证机构的认证业务声明和其他业务规范应规定合理的证书请求处理时间。

4.3 证书签发

34 4.3.1 证书签发中 RA 和 CA 的行为

在证书的签发过程中，国富安CA可以直接确认用户信息身份签发证书；或国富安CA得到RA通过安全方式传来的用户信息身份，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，证书签发系统签发证书。

35 4.3.2 CA 和 RA 对订户的通告

无论是拒绝还是批准订户的证书申请，CA或RA须通过适当的方式通知订户。

4.4 证书接受

36 4.4.1 构成接受证书的行为

订户接受证书的方式可以有如下几种：

（1）订户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

（2）通过面对面的提交，订户接受载有证书和私钥的介质。

完成以上行为表明订户接受证书。另外，在订户接受到证书后，应立即对证书进行检查和测试。

37 4.4.2 CA 对证书的发布

对于订户证书，国富安CA 根据用户的意愿将证书发布到目录系统上，或者不进行发布。

38 4.4.3 CA 对其他实体的通告

除证书订户和 RA 外，国富安CA 不需要通知其他实体证书的签发。

4.5 密钥对和证书使用

订户密钥对和证书须用于其规定的、批准的用途。否则，其应用是不受相关法律和国富安 CA 策略保障的。

39 4.5.1 订户私钥和证书使用

订户在接受了国富安 CA 所签发的证书后，即视为已经同意遵守与国富安 CA、

依赖方有关的权利和义务条款。证书持有人应妥善保管其证书私钥。

订户只能在指定的应用范围内使用证书和私钥，订户只能在接受了相关的证书之后才能使用对应的私钥，并且在证书到期或被吊销后停止使用该证书对应的私钥。

40 4.5.2 信赖方公钥和证书使用

当信赖方接受到签名的信息后，应该：

（1） 获得对应的证书及信任链；

（2） 确认该签名对应的证书是信赖方信任的证书；

（3） 证书的用途适用于相应的签名。

（4） 使用证书上的公钥验证签名。

以上任何一个环节失败，信赖方应该拒绝接受签名信息。

当信赖方需要发送加密信息给接受方时，须先通过适当的途径获得接受方的加密证书，然后使用证书上的公钥对信息加密。信赖方应将加密证书连同加密信息一起发送给接受方。

4.6 证书更新

41 4.6.1 证书更新的情形

每个证书都有其有效期，在一个订户的证书到期前30 天内或已到期后30 天内，如果订户的注册信息没有改变，订户可以申请证书更新，若证书已到期，但策略允许继续使用相同的密钥对，国富安CA将对其证书进行更新。

42 4.6.2 要求证书更新的主体

证书订户、证书订户的授权代表（组织机构证书）或证书对应实体的拥有者（比如服务器证书的拥有者）可以要求更新证书。同时，RA或CA可以依情况自动更新订户证书。

43 4.6.3 证书更新请求的处理

处理证书更新请求的过程，包括申请验证、鉴别、签发证书。对申请的验证和鉴别完成以下几个方面后才可签发证书：

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 用原证书上的订户公钥对更新申请的签名进行验证。

44 4.6.4 通知订户新证书的签发

无论是拒绝还是批准订户的证书申请，CA或RA须通过适当的方式通知订户。

45 4.6.5 构成接受更新证书的行为

订户接受证书的方式可以有如下几种：

（1）CA可以将证书发布到X.500或LDAP证书库；

（2）CA可能发送证书到RA，由RA发送给接受方；

（3）通过面对面的提交，订户接受载有证书和私钥的介质。

46 4.6.6 CA 对更新证书的发布

对于订户证书，CA 根据用户的意愿将证书发布到目录系统上，或者不进行发布。

47 4.6.7 CA 通知其他实体证书的签发

除证书订户和 RA 外，CA 不需要通知其他实体证书的签发。

4.7 证书密钥变更

48 4.7.1 证书密钥变更的情形

证书申请订户关键信息有变更，导致证书内容有变化，但密钥对保持不变的情况，订户可以申请证书密钥变更；或私钥泄漏而吊销证书之后，订户可以申请证书密钥变更。

49 4.7.2 请求证书密钥变更的实体

可以请求证书密钥更新的实体，如订户，RA或CA。

50 4.7.3 证书密钥变更请求的处理

处理步骤为：

① 由证书持有者本人持有效证件到申请证书的分支机构 RA（包括受理点）提出证书修改请求；

② RA（包括受理点）对有效证件进行审核；

③ 审核通过后在 RA 服务器的数据库中根据客户信息进行查询；

④ RA 修改本地审核数据库中的记录并发给国富安 CA 证书数据库。

对于非面对面申请证书变更的用户，国富安 CA 可以制定其他处理流程。

51 4.7.4 颁发新证书对订户的通告

同 CPS § 4.3.2。

52 4.7.5 构成接受密钥变更证书的行为

同 CPS § 4.4.1。

53 4.7.6 CA 对密钥变更证书的发布

同 CPS § 4.4.2。

54 4.7.7 CA 对其他实体的通告

同 CPS § 4.4.3。

4.8 证书吊销和挂起

55 4.8.1 证书吊销的情形

出现以下情况，最终订户证书必须吊销：

(1) 认证机构、注册机构或最终订户有理由相信或强烈的怀疑一个订户的私钥安全已经受到损害。

(2) 认证机构或注册机构有理由相信订户违背了订户协议下的义务、陈述或担保。

(3) 和订户达成的订户协议已经终止。

(4) 认证机构或注册机构有理由相信证书签发时没有依据CP 规定的有关程序，证书签发给了非证书主题的人员（1 类证书除外）或没有鉴证该人员在证书主题中的命名就签发了证书（1 类证书除外）。

(5) 认证机构或注册机构有理由相信证书申请中的信息有违背事实的错误。

(6) 认证机构或注册机构确定证书签发的一个必要前提条件既没有满足又没有豁免。

(7) 对于2 类证书，订户的组织机构名改变了。

(8) 除了未经鉴证的订户信息外，包含在证书中的信息不正确或已经改变。

(9) 订户请求吊销证书。

56 4.9.2 请求证书吊销实体

可以请求吊销证书的实体，例如对最终用户证书而言，可能是订户、

注册机构或电子认证服务机构。

57 4.9.3 吊销请求的流程

订户可以通过各种方式要求吊销自己的证书，包括：

（1）证书用户向国富安CA及RA（包括受理点）当面提出申请，要求作废其证书；

（2）证书订户在线访问国富安CA系统，根据证书申请时的保护密码进行在线吊销申请；

（3）证书订户通过电话或其他渠道通知国富安CA或RA（包括受理点）需要吊销证书，国富安CA或RA（包括受理点）需通过可靠方式核实请求确实来自最终订户。

认证机构确信出现CP § 4.9.1中的情况而需要立即吊销证书时，可立即吊销证书。

在撤销证书时，除特殊情况之外认证机构应立即通知登记人。

58 4.9.4 吊销请求的宽限期

订户必须在合理的时间内提出吊销请求：

（1）对于第2、3类证书不得超过8小时提出；

（2）其他证书不得超过24小时提出。

59 4.9.5 CA 处理吊销请求的时限

国富安CA从接到吊销请求到完成处理请求需要一定的合理的时间，一般在批准后24 小时后生效，特殊紧急情况下可以立即生效。

60 4.9.6 依赖方检查证书吊销的要求

依赖方是否检查证书吊销完全取决于应用的安全要求。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必须查询证书吊销列表确认该证书的状态。

61 4.9.7 CRL 发布频率

认证机构须定时发布最新的证书吊销列表。证书吊销列表更新的时间间隔不能超过24 小时。

62 4.9.8 CRL 发布的最大滞后时间

一个证书从它被吊销到它被发布到 CRL 上的滞后时间不能超过24 小时。

63 4.9.9 在线状态查询的可用性

认证机构须提供供证书状态的在线查询服务（OCSP），以供安全保障要求高的应用使用。

64 4.9.10 在线状态查询要求

基于合同的自愿原则，依赖方在信赖一个证书前必须通过证书状态在线查询检查该证书的状态。

65 4.9.11 吊销信息的其他发布形式

除了 CRL、OCSP 外，认证机构可以提供其他形式的吊销信息发布，但这不是必须的。

66 4.9.12 密钥损害的特别要求

无论是最终订户还是国富安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。

67 4.9.13 证书挂起的情形

无规定。

68 4.9.14 请求证书挂起的实体

无规定。

69 4.9.15 挂起请求的流程

无规定。

70 4.9.16 挂起的期限限制

无规定。

4.10 证书状态服务

认证机构应该通过 CRL、OCSP、LDAP 提供证书状态服务。

71 4.10.1 操作特征

认证机构提供的证书状态查询必须以网络服务的形式，让信赖方能够随时查询、下载。CRL 的发布频率和延迟必须符合CP § 4.9.7、4.9.8。OCSP 应能立即反映证书的当前状态。证书状态服务的提供应该使标准、通用的方式。对服务请求应该有合理的响应时间和并发处理能力。

72 4.10.2 服务可用性

国富安CA的CRL、OCSP 证书状态服务须保证7X24 可用，并且采用了冗余技术。

73 4.10.3 可选特征

无规定。

4.11 订购结束

当证书到期或证书被吊销或挂起则认证机构与订户关系结束。

4.12 密钥生成、备份与恢复

国富安CA依据国家管理规定或行业规则，提供加密证书密钥的集中管理和恢复。

74 4.12.1 密钥生成、备份与恢复的策略与行为

订户加密证书密钥对可以由国富安CA的密钥管理中心系统集中安全产生和保存，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）证书持有人提出申请；

2）国家执法、司法机构因执法、司法的需要；

3）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、资料。

75 4.12.2 会话密钥的封装与恢复的策略与行为

会话密钥根据其特性并依照国富安CPS §4.12规定对其进行合理的操作。

5. 设施、管理和操作控制

5.1 物理控制

国富安CA有详细的文件，描述CA 和RA 需遵守的物理控制和安全策略。对这些策略的符合性要求，在国富安CPS第五章中有详细的规定。

76 5.1.1 场地位置与控制

国富安CA中的所有CA 和RA 都将在物理上受保护的环境中运营，该环境能够防止、检测并阻止非授权的访问、使用或披露敏感信息和系统。

物理安全是基于物理层级的保护，每一物理层就是一个屏障，需要设置可以控制进出的带锁的门来控制每个人进出每一个区域。每一层区域必须有非常严格的控制方法防止未经授权的物理访问。而且要求每一个物理安全层在物理上必须能完全包含下一个物理安全层，而且要求内部的安全层不能与外部的安全层使用一样外部墙体，最外层的安全层应该是整个建筑物的外墙。

证书的认证等级决定了CA 或RA 的物理安全最小安全级别，例如：国富安CA签发了各类证书，因此他们运营在很高安全级别的系统环境下，CA 或RA 机构的证书管理签发程序被要求在相应的证书安全策略指导下，CA 或RA 机构需要在他们的CPS 中详细描述物理和环境的一些细节，其中包括：

（1）参照标准要求：

（2）机房设计指标的要求：

（3）机房区域划分。

77 5.1.2 物理访问控制

进出每一个物理安全层的行为都需要被记录、审计和控制，这样才可以保证进出每一个物理安全层的人都是经过授权的。

78 5.1.3 电力与空调

认证机构和注册机构须有安全、可靠的电力供电系统及电力备用系统以确保系统7X24 小时正常供电及在出现供电系统出现供电中断是能够提供正常的服务。认证机构应该有加热/通风/空调系统控制温度和湿度。

79 5.1.4 防水

认证机构和注册机构应采取预防措施以最大程度地减小水灾或其他水泄漏

对认证系统的影响和破坏。

80 5.1.5 火灾防护

认证机构和注册机构应采取预防措施,并制定相应的程序来消除和防止火灾的发生，这些防护方法应符合当地管理部门或机构的安全要求。

81 5.1.6 存储介质存放

储存产品软件和数据、归档、审计或备份信息的介质要保存在安全设施中，这些设施受到适当的物理和逻辑访问控制的保护，只允许授权人员的访问，并防止这些介质受到意外损坏（如水、火灾和电磁）。

82 5.1.7 废物处理

认证机构和注册机构应执行废物处理程序（如纸、电子介质或其他敏感信息）来控制未经授权的使用和访问，防止通过废物泄漏重要的公司商业信息和客户隐私信息。

83 5.1.8 异地备份

认证机构和注册机构应对关键系统数据、审计日志数据和其他敏感信息要进行日常备份和维护，这些备份信息要保存在安全的地方。

5.2 操作过程控制

84 5.2.1 可信角色

5.2.1.1 CA 系统管理人员

国富安CA系统管理人员负责CA系统的初始化、管理、审计等工作。

5.2.1.2 运营安全管理小组

根据安全管理策略和规范要求，安全管理小组由国富安CA领导和相关安全专家和顾问组成，安全官员对安全的三个关键领域负有全面的责任，即：开发与执行安全策略，维护与完善安全策略，保持安全审计的一致性。

85 5.2.2 每项任务需要的人数

认证机构和注册机构应建立、维护相应的策略和严格的控制程序，以保障敏感的操作进行了职责分工，确保多名可信人员共同参与完成一些敏感的任务。

职责分割的策略和控制程序是基于实际工作职责的要求。对于认证业务来讲，最敏感的任务是访问和管理CA 密码设备（如根密钥和加密卡）和涉及密码的相关材料，这些工作要求多名可信人员共同参与。

一些敏感的内部控制流程要求至少有两名可信人员参与，要求他们有各自独立的物理或逻辑控制设施，关于CA 的密钥设备的生命周期过程被严格的要求多名可信人员共同参加。关键的控制要进行物理和逻辑上的分割，如掌握关键设备的物理权限的人员不能再持有逻辑权限分割权力，反之易然。

其他的一些主要操作，如2类3类证书的鉴证和签发不能自动签发，要求至少 2 个可信人员的参与。

86 5.2.3 每个角色的识别与鉴别

认证机构和注册机构必须通过适当的方式，对有关人员的角色进行鉴别，并确认其可信，并且根据这些可信员工不同的权限功能要求定义不同鉴别方式；给与这些可信员工 CA 和RA 系统相应的管理权限。

87 5.2.4 需要职责分割的角色

所谓职责分割，是指如果一个人担任了完成某一职能的角色，就不能再担任完成另一特定职能的角色，但不限于国富安CA根据业务需要不限制的角色。

88 5.2.5 安全令牌控制

所有国富安 CA 的在职人员，对于使用安全令牌的员工，根据其权限发放相应的安全令牌，并且 CA 系统将独立完整地记录其所有的操作行为。

5.3 人员控制

89 5.3.1 资格、经历和无过错要求

认证机构和注册机构要求确认可信人员的程序需要有必备的背景调查。包括资格审查、工作经历调查、违法犯罪记录调查，确保这些人员能够胜任其工作。

90 5.3.2 背景审查程序

认证机构和注册机构应制定可信人员调查程序，调查程序必须符合我国的法律法规要求，关于人员的背景审查还要服从人员所在地域的政府或管理机构的要求。

背景审查的主要因素包括却不限于以下内容：

（1）身份证明，如个人身份证、护照、户口本等；

（2）学历、学位及其他资格证书；

（3）个人简历，包括教育、培训经历，工作经历及相关的证明人；

（4）无犯罪证明材料；

（5）是否有金融信贷不良记录；

（6）其他有关人员背景资料。

91 5.3.3 培训要求

为了使认证机构和注册机构的人员能胜任其承担的工作，认证机构应该提供岗前培训和必要的工作培训，和周期性的再培训。

92 5.3.4 继续培训的周期和要求

认证机构和注册机构应根据需要安排周期性的培训，以保证关键岗位的职员保持熟练的工作水平，顺利的完成其工作职责。

93 5.3.5 岗位分离

国富安CA的运行员工和负责CA设计开发维护的员工承担不同的职责,双方的岗位互相分离,为了保证安全,后者不能成为前者,即开发员工和运行员工分离的原则。

94 5.3.6 工作岗位轮换的周期和顺序

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

95 5.3.7 未授权行为的制裁

认证机构和注册机构应建立并维护一套管理办法来保障对于未授权行为或其他对认证机构及注册机构策略和程序的破坏行为应采取适当的纪律处罚。这些纪律处罚包含的措施包括中止员工相应工作并解除相应员工的劳动合同,纪律处罚程度与未经授权行为的频度和严重性相关。

96 5.3.8 系统抢修的要求

国富安CA系统需要抢修时,抢修人员需经过授权并由安全事务专员的陪同下进行，所有操作都要有记录。

97 5.3.9 独立合约人的要求

在有限制的情况下，独立合约人或顾问可以担任可信职位。任何合约人或顾问在某一职务的职能和安全标准应与相应职位的认证机构雇员一样。

98 5.3.10 提供给员工的文档

提供给认证机构和注册机构内部员工的文件应包括培训材料和与员工工作相关文档。

5.4 审计日志程序

99 5.4.1 记录事件的类型

认证机构和注册机构的审计日志和事件记录不管采用是电子的还是手动生成的,都应该记录事件相关信息及其他必要的信息。

100 5.4.2 处理或归档日志的周期

国富安CA定期对日志进行审查，对发现的安全事件采取相应的措施，并对审查日志的行为进行备案。

101 5.4.3 审计日志保存的期限

国富安CA在数据库保存审计日志至少两个月，离线保存至少为十年。

102 5.4.4 审计日志的保护

国富安CA将通过物理和逻辑的访问控制方法，防止未经授权而浏览、修改、删除或其他方式篡改电子或纸质审计日志文件。

103 5.4.5 审计日志备份程序

认证机构对审计日志应定期进行备份。

104 5.4.6 审计收集系统

审计日志收集系统涉及：

① 证书管理系统；

② 证书签发系统；

③ 证书目录系统；

④ 远程通信系统；

⑤ 证书受理系统；

⑥ 访问控制系统；

⑦ 网站、数据库安全管理系统；

⑧ 其他需要审计的系统。

国富安CA使用审计工具满足对上述系统审计的各项要求。

105 5.4.7 对导致事件主体的通知

审计日志报告一个事件时，应及时通知引起该事件的主体。

106 5.4.8 脆弱性评估

根据审计记录，认证机构应定期进行安全脆弱性评估，并根据评估报告采取措施。

5.5 记录归档

107 5.5.1 归档记录的类型

需要归档记录的类型如国富安CP§5.4.1，除此之外，存档的内容还包括国富安CA发行的证书和CRL、审计数据记录、证书申请审批资料等。

108 5.5.2 归档记录的保存期限

存档期限一般规定为七年。

109 5.5.3 归档文件的保护

国富安CA将通过适当的访问控制方法保护归档数据，只有授权的可信人员允许访问归档数据，国富安CA对任何未经授权的浏览、修改、删除或其它的篡改行为给予禁止访问的措施。

110 5.5.4 归档文件的备份

认证机构对归档文件应定期进行备份。

111 5.5.5 记录时间戳要求

每项记录必须有时间标识即时间戳，但这个证书时间戳不需要是基于密码技术的。

112 5.5.6 归档收集系统

各自实体应在内部建设归档收集系统，包括认证机构和外部独立实体的注册机构。

113 5.5.7 验证归档文件信息

只有可信人员才可以查看和获得归档信息，这些信息被归还时必须得到验证。

5.6 密钥变更

114 5.6.1 密钥有效期

国富安CA的密钥和所有终端用户的密钥对都有一个最终的生命期，当密钥对期满，旧密钥就应当自动撤销而使用新密钥，密钥的有效期根据安全级别的程度不同，有效期也有不同，但有效期都等于或大于一年。

115 5.6.2 密钥变更说明

国富安CA密钥对由加密机产生。证书到期更换密钥时将签发3张证书。

① 使用旧的私钥对新的公钥及信息签名生成证书；

② 使用新的私钥对旧的公钥及信息签名生成证书；

③ 使用新的私钥对新的公钥及信息签名生成证书。

④ 通过以上3张证书达到密钥更换的目的，使新旧证书之间互相认证、信任。

新的国富安CA将继续使用旧的CA私钥签发的CRL，直到由旧的CA私钥签发的证书到期为止。

5.7 损害与灾难恢复

认证机构必须通过实施物理和过程控制等有效的综合方案将密钥损害或其他灾难造成的风险和潜在影响降到最小。此外，认证机构必须建立灾难恢复方案和程序，并且在合理的期限内恢复业务运作。

116 5.7.1 事故和损害处理程序

国富安CA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，国富安CA将按照灾难恢复计划实施修复。具体由国富安CA灾难恢复计划决定。

117 5.7.2 实体公钥被撤销处理程序

当国富安CA证书被撤销时，国富安CA将通知证书用户，证书将被撤销。

118 5.7.3 实体私钥损害处理程序

当证书订户发现其私钥损害时，订户应立即通知认证机构吊销其证书，并尽可能地通知信赖方；认证机构应及时吊销订户证书并按CP 4.9 发布证书吊销信息。

当 CA 证书出现私钥损害时，认证机构应立即吊销CA 证书并及时通过广达的途径通知信赖方，然后生成新的CA 密钥对、签发新的CA 证书。

119 5.7.4 灾难后的业务存续能力

认证机构和注册机构在发生灾难后，按照国富安CA灾难恢复计划实施保证业务的正常运行。应有如下几个方面的业务存续能力：

（1）在尽可能短的时间内恢复业务系统 ，最多不超过24 小时。

（2）能够恢复客户信息。

（3）能够保证恢复后的运营场地符合安全要求。

（4）能够恢复对老客户、新客户的服务。

（5）有足够的人有继续业务并且不违反职责分割的要求

5.8 CA 终止服务

当国富安CA将要终止提供服务的情况下，国富安CA会在终止提供服务前一个合理的的时间内给RA(包括受理点)和证书用户书面通知，并会按照相关的法律规定的步骤进行操作。

6. 技术安全控制

6.1 密钥对的产生和安装

120 6.1.1 密钥对的产生

6.1.1.1 CA 密钥对的产生

国富安CA拥有签名密钥对，国富安CA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。

CA 密钥对的产生，必须由若干名接受过相关培训的可信雇员在密钥生成室按照严格的安全过程，在能够生成有足够安全强度密钥的可信系统上操作完成。

用于此类密钥生成的密码模块需通过国家密码主管部门鉴定、认证。对于CA 密钥对的产生，认证机构应该有严格的密钥生成流程。

6.1.1.2 最终订户密钥对的产生

国富安CA证书订户签名密钥对的产生遵循国家的法律，签名密钥对的产生即可在本地产生，也可以在受理点产生。不管何种类型，都必须保证签名密钥对产生的安全性，保护证书申请者的密钥的安全，要求不允许泄露申请者的私钥。国富安CA在技术、业务、流程和管理上已经实施了安全保密的措施。

对于特殊的应用，在依赖方许可的前提下，国富安CA在不损害本CP的前提下制定符合其应用的特殊证书策略。

121 6.1.2 私钥传输给订户

CA的私钥是在系统的初始阶段产生的,它保留在CA的系统中，不允许传送。

根据订户的要求，国富安CA证书服务体系支持在线传送加密密钥对给证书用户，并且保证传输的安全性。

对于订户的签名密钥对，必须在订户本地或受理点产生，不允许网络传送。

122 6.1.3 公钥传输给证书签发机构

最终订户的签名证书公钥从RA到CA传递，以及最终订户的加密证书公钥从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，保证证书传输过程中的安全性，完整性和可信性。

123 6.1.4 CA 公钥传输给依赖方

认证机构应该通过安全可靠的途径将 CA 公钥传给信赖方，包括从安全站点下载、面对面的提交、软件及操作系统预埋等方式。

124 6.1.5 密钥的长度

国富安CA用于加密和签名的非对称密钥对的模长是1024比特。

125 6.1.6 公钥参数的生成和质量检查

国富安CA公钥采用国家密码管理局许可的标准生成并检查证书的质量。

126 6.1.7 密钥使用目的

在国富安CA证书服务体系中的密钥使用与证书的种类有关。

① 国富安CA证书服务体系确保CA的签名私钥用于签发下级证书和所辖的黑名单CRL。

② 签名密钥可以用于提供安全服务，例如，身份认证不可抵赖和信息的完整性等。

③ 加密密钥可以用于信息加密时使用。

6.2 私钥保护和密码模块工程控制

认证机构必须通过物理、逻辑和过程控制的综合实现来确保CA 私钥的安全。订户合同会要求证书订户采取必要的预防措施防止私钥的丢失、泄露、更改或未经授权的使用。

127 6.2.1 密码模块的标准和控制

认证机构必须使用国家密码管理部门认可、批准的硬件密码模块生成根 CA、签发证书的CA 和其他CA 密钥对，并存储相关CA 私钥。

128 6.2.2 私钥多人控制

认证机构必须通过技术及过程上的控制机制来实现多名可信人员共同参与CA 加密设备的操作。

CA 私钥采用多人控制的策略(即 m 取 n 策略,m>n, n≥3),需要三个或三个以上的专员来共同完成生成程序。国富安 CA 的 CA 系统在技术上已经建立了相应安全机制，对生成操作进行限制。

证书申请者可以使用国富安 CA 认可的软硬件产生自己的私钥。

129 6.2.3 私钥托管

一般情况下,国富安CA不向证书订户提供签名私钥托管服务。

根据有法律规定或者双方约定的情况,国富安CA提供证书订户加密密钥对的托管服务，并且承诺、从技术上保证不泄漏托管的加密密钥对。

130 6.2.4 私钥备份

为了常规恢复和灾难恢复目的，认证机构必须创建 CA 私钥的备份。这种私钥备份以加密的形式保存在硬件密码模块中。存储CA 私钥的密码模块应符合CP § 6.2.1 的要求。CA 私钥复制到备份硬件密码模块中要符合CP § 6.2.6 的要求。备份的私钥要避免通过物理或加密方式进行的非授权的修改或泄露。

订户的签名密钥国富安CA和KMC都不备份。加密私钥由KMC备份，备份数据以密文形式存在。

131 6.2.5 私钥归档

当认证机构的 CA 密钥对到期后，这些CA 密钥对将会被使用满足CP § 6.2.1 要求的硬件密码模块安全存储设备保存一定合理的时间。

用户密钥对的归档是将已过生命周期或决定暂不使用的加密密钥以密文形式保存在数据库中并备份后归档保存，需提供查询或恢复服务。

国富安CA提供过期的托管加密密钥的归档服务。

132 6.2.6 私钥导入、导出密码模块

认证机构必须在硬件密码模块上生成CA 密钥对，该密钥对将在这个模块中使用，私钥无法从硬件密码模块中导出。

133 6.2.7 私钥在密码模块的存储

CA 私钥必须存放在硬件密码模块中。1类2类证书私钥在硬件密码模块（如USB Key、SmartCard）中存储和使用。3类服务器证书私钥可以存放在服务器程序特定的软件密码模块中，但最好使用带有硬件密码模块的加速卡。

134 6.2.8 激活私钥的方法

6.2.8.1 最终订户私钥

6.2.8.1.1 1 类证书私钥激活

1 类证书建议将私钥存放在诸如USB Key和智能卡硬件密码模块中，并且私钥可以通过PIN 码（口令）、指纹鉴别等保护。如果私钥没有PIN 码（口令）、指纹鉴别保护，那么，当用户计算机上安装了相应的驱动后，将USB Key 和智能卡插入相应的读卡设备中，则私钥被激活可以使用。如果私钥有PIN 码（口令）、指纹鉴别保护，那么，当用户计算机上安装了相应的驱动后并将USB Key 和智能卡插入相应的读卡设备后，只有输入通过相应的PIN 码（口令）、指纹鉴别，私钥才激活可以使用。

6.2.8.1.2 2 类证书私钥激活

对于2 类证书必须使用USB Key、智能卡等硬件密码设备存放私钥，私钥不能出卡，并且使用PIN 码（口令）、指纹鉴别保护私钥。要激活私钥，用户计算机上需安装相应的驱动后并将USB Key 和智能卡插入相应的读卡设备，通过相应的PIN 码（口令）、指纹鉴别，私钥才激活可以使用。

6.2.8.1.3 3 类证书私钥激活

对于3 类服务器证书，如果没有使用硬件密码模块，则私钥是存放在服务程序的软件密码模块中，这时应该使用口令对私钥进行保护。但服务程序启动，软

件加密模块被加载，输入相应私钥保护口令后，证书私钥被激活。

如果使用硬件密码模块，则私钥需要被口令保护。当硬件密码模块被安装到订户计算机上，服务程序启动，输入相应私钥保护口令后，证书私钥被激活。

6.2.8.1.4 4 类证书私钥激活

4 类证书的私钥可以存放在订户计算机的软件密码模块中，这时订户应该采用合理的措施从物理上保护订户的订户计算机以防止在没有得到用户授权的情况下，其他人员使用订户的订户计算机和相关的私钥。如果存放在软件密码模块中的私钥没有口令保护，那么，软件密码模块的加载意味着私钥的激活。如果使用口令保护私钥，软件密码模块加载后，还需要输入口令才能激活私钥。

6.2.8.1.5 5 类证书私钥激活

5 类证书的私钥激活类似于4 类证书。

6.2.8.2 CA 私钥

认证机构的私钥存放在硬件密码模块中，并且其激活数据按 CP 6.2.2 进行分割。当需要使用CA 私钥时，将硬件密码模块加载并按CP 6.2.2 规定的m选n 的原则输入激活数据的分割。

135 6.2.9 解除私钥激活状态的方法

对于存放在软件密码模块中的私钥，当软件密码模块被下载、用户退出登录状态、操作关闭或计算机断电时，私钥被解除激活状态。

对于存放在硬件密码模的私钥，当每次操作后注销计算机，或者把硬件密码模块从读卡器中取出时，私钥成为非激活状态。

对于服务器证书，当服务程序下载、系统注销或系统断电后私钥即进入非激活状态。

对于国富安CA系统私钥，当存放私钥的硬件密码模块断电或退出加密模块程

序，私钥进入非激活状态。

136 6.2.10 销毁私钥的方法

私钥不再使用、不需要保存时，应该将私钥销毁，从而避免丢失、偷窃、泄露或非授权使用。

对于最终订户加密证书私钥，在其生命周期结束后，应该妥善保存一定期限，以便于解开加密信息。对于最终订户签名证书私钥，在其生命周期结束后，如果无需再保存，可以通过私钥的删除、系统或密码模块的初始化来销毁。

认证机构CA 私钥，在生命周期结束后，需将CA 私钥的一个或多个备份进行归档，其他的CA 私钥备份被安全销毁。具有销毁密钥权限的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，进行销毁密钥的操作，需要三名管理员同时在场。

137 6.2.11 密码模块的评估

国富安CA将依据国家有关标准对密码模块进行评估。

6.3 密钥对管理的其他方面

138 6.3.1 公钥归档

CA 和最终订户证书将被归档于国富安CA和密钥管理中心，并进行定期的整理。

139 6.3.2 证书操作期和密钥对使用期限

公钥和私钥的使用期限与证书的有效期相关但却有所不同。

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内签名的信息可以验证，公钥的使用期限可以在证书的有效期限以外。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公

钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

另外需注意的是无论是订户证书还是CA 证书，有效期到了后，在保证安全的情况下，允许使用原密钥对对证书进行更新。但是密钥对不能无限期使用。

6.4 激活数据

140 6.4.1 激活数据的产生和安装

国富安CA 私钥的激活数据由硬件加密卡内部产生，并分割保存在5 个IC 卡中，需通过专门的读卡设备和软件读取。

如果订户证书私钥的激活数据是口令，国富安CA建议订户在使用前修改证书私钥的初始激活数据。这些口令必须有如下条件：

① 至少8 位字符或数字；

② 至少包含一个字符和一个数字；

③ 不能包含很多相同的字符；

④ 不能和操作员的名字相同；

⑤ 不能包含用户名信息中的较长的子字符串。

141 6.4.2 激活数据的保护

对于 CA 私钥的激活数据，认证机构必须通过秘密分割将分割后的激活数据由不同的可信人员掌管，而且掌管人员必须符合职责分割的要求，签署协议确认他们知悉秘密分割掌管者责任。

如果证书订户使用口令或PIN 码保护私钥，订户应妥善保管好其口令或PIN 码，防止泄露或窃取。如果证书订户使用生物特征保护私钥，订户也应注意防止其生物特征被人非法获取。

142 6.4.3 激活数据的其他方面

6.4.3.1 激活数据的传送

当私钥的激活数据进行传送时，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

当私钥的激活数据不需要时应该销毁，并保护它们在此过程中免于丢偷窃、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。

6.5 计算机安全控制

143 6.5.1 特别的计算机安全技术要求

认证机构应确保包含CA 软件和数据文件的系统是安全可信的系统，不会受到未经授权的访问。此外，认证机构应只允许有工作需求的必要人访问产品服务器，一般的应用用户在产品服务器上没有账户。

认证机构的生产系统网络与其它部分逻辑分离。这种分离可以阻止除指定的应用程序外对网络访问的访问。认证机构使用防火墙阻止从内网和外网入侵生产系统网络，限制访问生产系统的活动。只有认证机构系统操作与管理组中的、有必要工作需要、访问系统的可信人员可以直接访问认证系统数据库。

144 6.5.2 计算机安全评估

国富安CA根据国家计算机安全等级的要求，实现CA系统的安全等级标准。

6.6 生命周期技术控制

145 6.6.1 系统开发控制

系统开发采用先进的安全控制理念，同时兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。以保证系统的安全，稳定以及证书生成的完整性，可靠性。

146 6.6.2 安全管理控制

认证机构依照国家计算机管理规定等，制定策略、管理制度与流程对 CA 运营的各方面进行安全管理。

147 6.6.3 生命期的安全控制

国富安CA将依据《信息安全技术 公钥基础设施 特定权限管理中心技术规范》及《信息安全技术 公钥基础设施 时间戳规范》等规定，在证书的存续期间内保证证书的安全性以及整个系统的安全可靠。

6.7 网络的安全控制

认证机构应通过防火墙、入侵检测、防病毒、安全身份认证等安全技术，确保认证系统的安全运营。对于认证系统的网络安全，认证机构应制定专门的网络安全策略与实施方案，有关方案应符合国富安安全和审计要求指南。

6.8 时间戳

认证系统的各种系统日志、操作日志应该有对应的记录时间。

7. 有关证书、证书吊销列表和在线证书状态协议

7.1 证书

148 7.1.1 版本号

X.509v3 证书。

149 7.1.2 证书扩展项

依本证书策略签发的X.509v3 证书的扩展项满足CP§7.1.2.1-7.1.2.8私有扩展项的使用是允许的，但是除非由于特别应用而包含该项，不保证私有扩展项的使用。

7.1.2.1 密钥用法（Key Usage）

指定证书密钥对的用法。这个扩展项的 criticality 域通常设置为FALSE。

7.1.2.2 证书策略扩展项（Certificate Policies）

证书策略扩展项中有本 CP 中对应证书类的 CP 对象标识符及策略限定符。这个扩展项的criticality 域设置为FALSE。

7.1.2.3 主体备用名（subjectAltName）

扩展项的使用符合 RFC 3280。此扩展项的criticality 项应设为FALSE。

7.1.2.4 基本限制扩展项（BasicConstraints）

CA 证书的基本限制扩展项中的主题类型被设为CA。最终订户证书的基本限

制扩展项的主题类型设为最终实体（End-Entity）。这个扩展项的criticality 域设置为FALSE。将来，对于其它的证书，这个扩展项的criticality 域可以设置为TRUE。

CA 证书的基本限制扩展项中的路径长度设定为在证书路径中该证书之后的 CA 级数。对于最终订户证书签发CA，其CA 证书“pathLenConstraint”域的值设为0，表示证书路径中仅有一个最终订户证书可以跟在这个CA 证书后面。

7.1.2.5 扩展的密钥用法（Extended Key Usage）

对不同的证书，密钥用法根据证书安全等级不同而有所不同。

7.1.2.6 CRL 的分发点（cRLDistributionPoints）

证书中的 CRL 的分发点扩展项，它包含本地的一个链接，可以向信赖方提供CRL 的信息以便其查询证书状态。此扩展项的criticality 项应设为FALSE。

7.1.2.7 签发 CA 密钥标识符

最终订户证书及中级 CA 证书加入签发CA 密钥标识符扩展项，当证书签发者包含主题密钥标识扩展项时，签发CA 密钥标识符由160 位的签发证书的CA 的公钥进行SHA256散列运算后的值构成。否则，它将包含签发CA 的主题DN 和序列号。这个扩展项的criticality 域设置为FALSE。

7.1.2.8 主题密钥标识符

当证书包含主题密钥标识符扩展项时，该值由证书主题的公钥产生。使用该扩展项时，其扩展项的criticality 域设为FALSE。

150 7.1.3 证书格式

①一类证书（个人证书）

字段域名称	描述	内容

标准域		
版本		X．509V3
序列号		[由CA系统自动产生唯一号码]
签名算法ID		SHA256
发行者		CN=ROOT CERTIFICATE FOR GFA TRUST NETWORK OU=GFA TRUST NETWORK O=CIECC L=BETDA S=BEIJING C=CN
有效期		
	不早于	[国家标准时间]
	不迟于	[国家标准时间]
主题名称		CN=身份证号-姓名 OU（1）=无或部门名 OU（2）=无或职业资格证书、个人手写签名信息等 OU（3）=证书类型 O=GFA 或 组织机构代码 L=区域 S=城市 C=CN
主题公钥信息		算法ID：RSA 公钥信息：密钥长度为1024位
标准扩展域		
签发CA 密钥标识符		未使用
主题密钥标识符		未使用
密钥使用		数字签名、加密、不可否认 （此为“关键”位）

证书策略		PolicyIdentifier=[OID] PolicyQualifierID=CPS Qualifier=[cps 网址]
主题备用名		
	DNS	无
	RFC822	电子邮件地址
发行者其他名称		未使用
基本限制	主体类型	最终实体
	路径长度限制	无
扩展密钥用途		未使用
证书吊销分发点		分发点名称=[分发点URL]
NETSCAPE扩展位		
NETSCAPE证书类型		SSL client, S/MIME
NETSCAPE SSL服务器名称		未使用
NETSCAPE注释		未使用

②二类证书（组织机构证书）

字段域名称	描述	内容
标准域		
版本		X. 509V3
序列号		[由CA系统自动产生唯一号码]
签名算法ID		SHA256
发行者		CN=ROOT CERTIFICATE FOR GFA TRUST NETWORK OU=GFA TRUST NETWORK O=CIECC L=BETDA S=BEIJING

		C=CN
有效期		
	不早于	[国家标准时间]
	不迟于	[国家标准时间]
主题名称		CN=组织机构代码-组织机构名称 OU（1）=无、上级组织机构代码或部门名 OU（2）=无或企业商标名、行业资格号等 OU（3）=证书类型 O=组织机构代码 L=区域 S=城市 C=CN
主题公钥信息		算法ID：RSA 公钥信息：密钥长度为1024位
标准扩展域		
签发CA 密钥标识符		未使用
主题密钥标识符		未使用
密钥使用		数字签名、加密、不可否认 （此为“关键”位）
证书策略		PolicyIdentifier=[OID] PolicyQualifierID=CPS Qualifier=[cps 网址]
主题备用名		
	DNS	无
	RFC822	无
发行者其他名称		未使用
基本限制	主体类型	最终实体
	路径长度限制	无

扩展密钥用途		未使用
证书吊销分发点		分发点名称=[分发点URL]
NETSCAPE扩展位		
NETSCAPE证书类型		SSL client, S/MIME
NETSCAPE SSL服务器名称		未使用
NETSCAPE注释		未使用

③三类证书（设备、服务器证书）

字段域名称	描述	内容
标准域		
版本		X. 509V3
序列号		[由CA系统自动产生唯一号码]
签名算法ID		SHA256
发行者		CN=ROOT CERTIFICATE FOR GFA TRUST NETWORK OU=GFA TRUST NETWORK O=CIECC L=BETDA S=BEIJING C=CN
有效期		
	不早于	[国家标准时间]
	不迟于	[国家标准时间]
主题名称		CN=服务器名称或域名、IP地址名等 OU（1）=身份证号或部门名 OU（2）=无 OU（3）=证书类型 O=GFA 或 组织机构代码 L=区域

		S=城市 C=CN
主题公钥信息		算法ID：RSA 公钥信息：密钥长度为1024位
标准扩展域		
签发CA 密钥标识符		未使用
主题密钥标识符		未使用
密钥使用		数字签名、加密、不可否认 （此为“关键”位）
证书策略		PolicyIdentifier=[OID] PolicyQualifierID=CPS Qualifier=[cps 网址]
主题备用名		
	DNS	无
	RFC822	未使用
发行者其他名称		未使用
基本限制	主体类型	最终实体
	路径长度限制	无
扩展密钥用途		未使用
证书吊销分发点		分发点名称=[分发点URL]
NETSCAPE扩展位		
NETSCAPE证书类型		SSL client, S/MIME
NETSCAPE SSL服务器名称		未使用
NETSCAPE注释		未使用

151 7.1.4 名称形式

依本CP 签发的证书的甄别名符合X500 关于目录名的规定。对于证书主题甄

别名，O 代表证书持有者所在的组织机构，第一个OU 代表所在的部门。对于证书签发者甄别名，O 代表证书签发机构，第一个OU 签发机构中的部门。甄别名可以包含不止一个的OU 用于存放其他信息，如可将一个附加的组织部门(OU)域包含在最终订户证书中，该域指出证书对应的信赖方协议所在的URL。

152 7.1.5 名称限制

除有特别声明外，证书中的通用名一般是不能使用假名、伪名。

153 7.1.6 算法对象标识符

国富安CA的证书支持并使用下表中的算法来签名。

Algorithm	Object Identifier
SHA256WithRSA Encryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }

国富安CA的证书支持并使用下面的OID来识别产生主体密钥的算法。

Algorithm	Object Identifier
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.2 证书吊销列表

国富安CA签发的证书吊销列表符合X.509 V2格式。遵循RFC5280标准。

154 7.2.1 版本号

X.509 V2。

155 7.2.2 CRL 和 CRL 条目扩展项

与 X509 和PKIX 规定一致。吊销列表格式如下:

域名称		内容
标准域		
版本		V2
签名算法标示		SHA256
发行者		CN=OPERATION CA 01 OU=GFA TRUST NET O=CIECC C=CN
此次更新时间		[国家标准时间]
下次更新时间		[国家标准时间]
吊销证书	订户证书	序列号
	吊销日期	[国家标准时间]
	吊销清单号	
	吊销原因	[吊销原因识别号]
扩展域		
签发CA 密钥标识符	发行者	
	序列号	发行者证书序列号
证书吊销清单号		
发行者分发点		URL地址

7.3 在线证书状态协议

156 7.3.1 版本号

OCSP v1

157 7.3.2 OCSP 基本域

在线证书状态协议（OSCP）使得应用程序可以测定所需要检测证书的（撤销）状态，一个OSCP客户端发布一个状态查询给一个OSCP响应器直到响应器提供响

应。这个协议描述了在应用程序检查证书状态和服务器状态之间所需要交换的数据。

158 7.3.3 OCSP 扩展项

无规定。

8. 认证机构审计和其他评估

认证机构应定期对物理控制、密钥管理、操作控制、鉴证执行等情况进行审查，以确定实际发生情况是否与预定的标准、要求一直，并根据审查结果采取行动。

8.1 评估的频率和情形

评估应该至少12个月执行一次。

8.2 评估者的资格

评估者必须是：法律法规或行业规则认可的熟悉公钥基础设施技术、信息安全工具和技术、安全审计的人员；具有中华人民共和国注册会计师资格或类似资格，接受过专项培训，每年都接受了资格评估、测试、供职于权威机构和接受过持续的专业教育的人员。

8.3 评估者与被评估者之间的关系

评估者必须是独立于认证机构的会计事务所（或等同组织）。

8.4 评估的内容

评估的内容包括：CA 环境控制、密钥管理操作和CPS 的执行情况等。

8.5 对问题与不足采取的措施

若在评估当中出现重大事故或者任何实质性的问题时，采取行动的决定由认证机构管理层根据评估报告作出。认证机构的管理层负责根据审计结果制定和实施改正计划，如果认证机构确认审计中发现的意外或不作为对证书体系的安全或完整性会造成立即威胁，则认证机构必须在一个月内制定改正行动计划，并在合理的期限内执行它。

8.6 评估结果的传达与发布

国富安CA有权利决定是否将审计结果公开。

8.7 其他评估

除了一致性评估外，国富安CA将对其他有关于证书的领域进行必要的评估。

9. 法律责任和其他业务条款

9.1 费用

159 9.1.1 证书签发和更新费用

作为承担责任的第三方电子认证服务提供商，国富安CA有权利向证书订户收取签发证书、管理证书、更新证书的服务费用。

160 9.1.2 证书查询的费用

无规定。

161 9.1.3 证书吊销或状态信息的查询费用

国富安CA向公众免费提供CRL和证书状态查询服务。但若用户要求国富安CA

提供个性化的CRL查询、OCSP查询或其他增值服务，国富安CA将收取一定费用。

162 9.1.4 其他服务费用

有关认证机构的其他相关费用，若认证机构认为必须且必要或证书签发与接收双方有约定或法律有其他规定，认证机构可以收取必要的服务费用。

163 9.1.5 退款策略

证书是根据国家法律规定或者合同约定签发的，若证实接受方有证据证明证书违反法律规定或合同约定，有权向认证机构要求退款，但认证机构能够证明是第三方的过错导致或其本人导致的不承担退款义务。

9.2 财务责任

164 9.2.1 保险范围

国富安CA向证书订户提供证书使用保障。如果由于其本身原因造成用户使用证书过程中遭受损失，北京国富安电子商务安全认证有限公司将向证书订户、依赖方提供赔偿。

165 9.2.2 其他财产

无规定。

166 9.2.3 对最终实体的保险或担保

国富安CA财政状况良好，能够有效支持国富安CA的经营运作，承担因国富安CA责任而导致的经济损失。

9.3 业务信息保密

认证机构、注册机构应有专门的保密方案、计划，在符合法律的前提下，保

护自身和客户的敏感信息、商业秘密。

167 9.3.1 保密信息范围

认证机构、注册机构需要保密的信息包括但不限于系统方面、运营管理方面、客户信息等服务过程中获悉之任何信息。

168 9.3.2 不属于保密的信息

证书策略、认证业务声明、信赖方协议、订户协议等。

169 9.3.3 保护保密信息的责任

认证机构、注册机构须通过有效的技术手段和管理程序，保护商业的和客户的保密信息。

9.4 个人隐私保密

170 9.4.1 隐私保密计划

认证机构应制定隐私保密计划对证书订户的个人信息保密。

171 9.4.2 作为隐私处理的信息

作为隐私处理的信息包括但不限于，最终订户注册申请证书中提交的信息；与认证机构、注册机构签订的协议。

172 9.4.3 不被视为隐私的信息

不被认为是隐私信息包括但不限于，出现在证书中的信息；证书及证书状态。

173 9.4.4 保护隐私的责任

认证机构、注册机构在没有获得客户授权的情况下，不得将客户隐私信息透露给第三方。但不限于法律规定强制要求认证机构、注册机构提供。

174 9.4.5 使用隐私信息的告知与同意

认证机构、注册机构如果需要将客户隐私信息用于双方约定的用途以外的目的，则需要事先告知客户并获得客户同意和授权，而且这种同意和授权是要用可归档的方式。

175 9.4.6 依法律或行政程序的信息披露

由于法律执行、法律授权的行政执行的需要，认证机构、注册机构将有关信息在客户知晓或不知晓的情况下提供有关执法机关、行政执行机关是允许的，即使这样，认证机构、注册机构也应尽可能地保护客户隐私信息。

176 9.4.7 其他信息披露情形

对其他信息的披露受制于法律、订户协议。

9.5 知识产权

177 9.5.1 知识产权

国富安CA对它签发的证书及其中的信息拥有知识产权，包括专利，商标。

178 9.5.2 CRL 中的知识产权

认证机构对证书吊销列表及其中信息的拥有知识产权。

179 9.5.3 CP 及 CPS 中的知识产权

认证机构对本CP及CPS拥有知识产权。

180 9.5.4 命名中的知识产权

证书订户对证书注册信息及签发给他的证书中包含的商标、服务标志或商品名和甄别名拥有知识产权。

181 9.5.5 密钥和密钥材料的知识产权

证书中的密钥对是证书中主题对应实体或实体拥有者的知识产权。

9.6 陈述与担保

182 9.6.1 CA 的陈述与担保

国富安 CA 负责证书签发和管理的所有方面，包括控制实际的证书产生过程，证书的发布，证书的更新和吊销，负责确保根据本策略的要求说明做好与证书有关的服务、操作等各方面的工作。

国富安CA在签发证书和证书吊销列表之前，应该根据国家有关法律、主管机关的有关规定（例如电子签名法、电子认证服务管理办法）制定国富安CA总体认证政策，并受主管机关及相关法规管辖与监督。

国富安CA 不负责评估证书是否被恰当使用。订户和信赖方必须依订户协议和信赖方协议确保证书用于允许使的目的。

认证机构和订户之间的担保、免责和有限责任由他们之间的协议规定和约束。

认证机构需在下列几个方面做出声明和担保：

（1）根CA的主要责任；

（2）根CA不承担责任的情况：

（3）运营CA的责任：

（4）运营CA不承担责任的情况；

（5）根CA的义务：

（6）运营CA的义务。

183 9.6.2 RA 的陈述与担保

国富安CA通过RA系统为订户发放数字证书，并保证数字证书内容的真实性，RA系统通过LA最终面向订户证书申请，负责审核订户的真实身份并决定是否受理订户的申请，负责数字证书注册、审核、制证。RA应承担自身的责任和义务，其中包括LA的义务。

184 9.6.3 订户的陈述与担保

订户一旦接受国富安CA签发的证书，就被视为在证书申请时已阅读了订户协议并且同意订户协议条款，明确自身责任，防止密钥泄漏、遗失、非授权的使用，并遵循本CP与CPS的规定。

185 9.6.4 依赖方的陈述与担保

在任何信赖行为发生之前，依赖方必须阅读依赖方协议，并保证证书将会被恰当的使用，同时需熟悉本CP和CPS的条款并遵循条款规定。

186 9.6.5 其他参与者的陈述与担保

依据国家法律规定或双方协议约定。

9.7 担保免责

在适用法律允许范围内，国富安CA不对协议中已经存在的内容和现行法律规定的内容进行担保。

国富安CA不对由于客观意外或其它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。

9.8 有限责任

在法律允许的范围内，认证机构订户协议、信赖方协议和其他订户协议限制认证机构承担的责任，责任限制包括排除间接的、特殊意外造成的、偶然的和后续性的损失。

9.9 赔偿

认证机构对自身原因造成的订户损失对订户进行赔偿，或信赖方在履行了信赖方协议的情况下，由于认证机构或订户的原因造成的信赖方损失，认证机构对信赖方的赔偿。

订户对自身原因造成的认证机构、信赖方损失对认证机构进行赔偿。

信赖方对自身原因造成的认证机构损失对认证机构进行赔偿。

9.10 有效期限与终止

187 9.10.1 有效期限

作为认证机构的核心业务文件，CP 和CPS 在认证机构中止业务前一直有效，在发布新的CP 和CPS 版本后，新的CP 和CPS 版本将取代原CP 和CPS 版本。在新CP和CPS生效日之前，认证机构已经或正在进行证书签发的，即该认证机构在生效日前发布的所有证书，如能满足新CP和CPS及有关条例的规定，则应视为由该授权认证机构按照新CP和CPS发布。对于证书订户而言，证书签发时的CP、CPS和订户协议将起作用直到证书到期或吊销，除非法律相冲突的内容、与事实不符的错误描述。对某一特定证书而言，在公钥的有效使用期限内，信赖方协议有效。

188 9.10.2 终止

当认证机构终止业务时，CP 和CPS即终止。当证书到期或吊销后，订户协议即终止，公钥到了的有效使用期，对应的信赖方协议终止。

189 9.10.3 效力的终止与保留

认证机构认证业务的终止，不意味着认证机构责任的终止。认证机构在业务终止后应采取合理的措施，保证订户的利益，如证书可继续使用，对客户进行赔偿，或将认证服务转到其他认证机构。订户证书到期、证书吊销意味着订户协议的终此，认证机构不再对证书私钥（签名）或公钥（加密）的使用承担任何责任，信赖方不应再信赖证书对应的签名私钥或加密公钥。

当由于某种原因，如内容修改、与适用法律相冲突，CP、CPS、订户协议、信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。另外，各参与方需要归还或保障销毁从其他方得到的保密信息。

9.11 对参与者个别通告与沟通

认证机构在必要的情况下，如主动吊销订户证书、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，可通过适当方式，如电话、电邮、信函、传真等，个别通知订户、信赖方。

9.12 修订

190 9.12.1 修订程序

国富安CA保证本CP的稳定性和可信性，不定期地，国富安CA将对本CP 进行检查、评估，当国富安CA认为应该对本CP做出修改时，国富安CA安全安全策略管理委员会将对本CP及其他相关文档、协议的修改提出建议，在征求国富安CA法律顾问有关法律上的意见并获得国富安管理层批准后，由国富安CA安全安全策略管理委员会负责组织修改。修改后的CP及其他相关文档、协议经法律顾问及管理层批准后正式发布。

191 9.12.2 通知机制与期限

国富安CA将修改了的CP通过国富安网站（http://www.gfapki.com.cn）上发布，

一般情况下不对具体个人另行通知。对于特殊原因需要通过电子邮件、信件、媒体等方式通知的修改，国富安将在合理的时间内通知有关各方，合理的时间应保证有关方面受到的影响最小。

192 9.12.3 必须修改的情形

当管辖法律、适用标准及操作规范等有重大改变时，必须修改CP。

9.13 争议解决

当认证机构、订户和信赖方之间出现争议时，有关方面应依据协议通过协商解决，若协议有仲裁条款可进行仲裁裁定，否则可通过法律解决，订户协议、信赖方协议和其他订户协议都应该包含解决争执的相应条款。

9.14 管辖法律

中华人民共和国法律、规则、规章、法令和政令将管辖认证机构的业务活动。认证机构的任何业务活动必须受有关法律、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，受管辖法规包括但不限于《中华人民共和国电子签名法》及《电子认证服务管理办法》等。

9.15 与适用法律的符合性

认证机构的所有业务、活动、合同、协议必须符合中华人民共和国法律、法规和国家信息安全主管部门的要求。

9.15 一般条款

193 9.15.1 完整协议

CP、CPS、订户协议及信赖方协议及其补充协议将构成PKI参与者之间的完整协议。

194 9.15.2 分割性

在法律允许的范围内，认证机构的订户协议、信赖方协议和其他订户协议可以包含可分割性条款。

195 9.15.4 强制执行

国富安CA将依据国家法律法规规定行使强制执行能力，免除一方对某次合同违约的责任不意味着免除对其他合同违约的责任。

196 9.15.5 不可抗力

不可抗力是指不能预见、不能避免并不能克服的客观情况。自然灾害、政府行为或某些社会因素等属于不可抗力。认证机构可以免除或部分免除责任。

9.16 其他条款

遵守国家民法或行政等相关规定，保证国富安 CA 正常运作，本 CP 的解释权归北京国富安电子商务安全认证有限公司。