国富安 CA
电子认证业务规则 V3.2

北京国富安电子商务安全认证有限公司

2021 年 8 月

目录

1 概括性描述

1.1 概述

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。

国富安 CA 安全认证体系的设计和建设符合各项国际安全协议标准。国富安 CA 签发的证书格式遵循国际电联（ITU）X.509 标准。2006 年 2 月，国富安数字证书认证系统通过国家密码管理局安全性审查。

国富安 CA 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，提供数字证书的申请、颁发、存档、查询、废止等服务，并通过以 PKI 技术、数字证书应用技术为核心的应用安全解决方案。

国富安 CA 电子认证业务规则由北京富安电子商务安全认证有限公司按照工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范》制定。

本《电子认证业务规则》详细阐述了国富安 CA 在实际工作和运营中所遵循的各项规范。本《电子认证业务规则》适用于国富安 CA 及其员工、注册机构、证书申请方、订户和依赖方，各参与方必须完整理解和执行《电子认证业务规则》所规定的条款并承担相应的责任和义务。

1.1.1 证书类别

国富安 CA 证书策略根据社会活动中参与的实体不同定义了三类证书。在每类证书中又根据其承担的法律责任、安全保障级别、用途等又进行了细分，目的是为了更好的保障各参与方的权利和义务。

一类证书是个人证书，国富安 CA 签发的这类证书满足《中华人民共和国电子签名法》的规定，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。

个人证书是指自然人证书，提供基本的安全保障，代表法定公民在中华人民共和国

境内从事社会活动的网络身份，与个人在社会中的职务与地位没有关系，如同公安机关颁发发的身份证一样；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个人印章相对应。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。

二类证书是组织机构、企业证书，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》的规定下，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。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)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。

三类证书为设备、服务器证书，根据设备归属实体又分为个人服务器证书和组织机构、企业服务器证书。

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。

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，该证书不仅保障该域名或设备的身份，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》的规定下，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。

1.1.2 证书分发服务

国富安 CA 通过其承担相应责任的 RA 注册机构，包括在其 CA 认证机房和自建分布在全国各地、以及建立在其他组织机构中、遵从于本电子认证业务规则的 RA 注册机构进行证书批准、签发、管理、使用和吊销、更新等安全服务，国富安 CA 会在其运营网站公布各 RA 注册机构的有关信息。

1.2 文档名称与标识

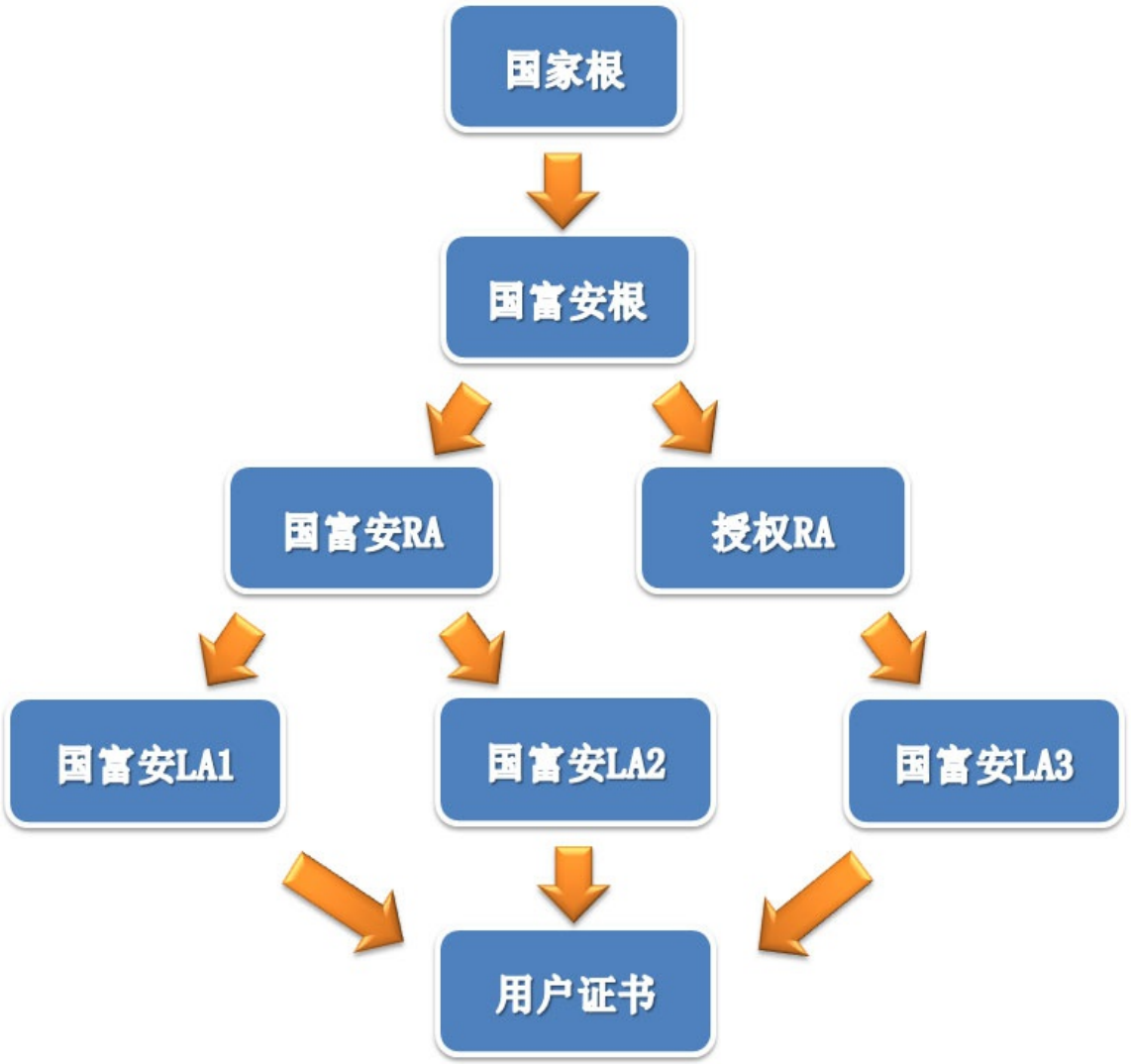
本文档名称为国富安 CA 电子认证业务规则（CPS），目前版本号为 V3.2，在国富

安 CA 运营网站发布，网站地址为 WWW.CACENTER.COM.CN。

1.3 电子认证活动参与方及其职责

国富安 CA 是根据《中华人民共和国电子签名法》和《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构。

国富安 CA 秉承国际领先的 PKI 技术，总体为两层，第一层为国家根 CA，第二层为国富安根 CA，国富安 CA 可以根据其电子认证业务规则依据其策略向不同行业和领域扩展其信任体系。国富安根 CA 由 CA 系统、RA 系统和 LA 受理点三部分组成，以下为其系统示意图：



1.3.1 电子认证服务机构

电子认证服务系统 CA（Certification Authority）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，不直接面对证书用户。国富安根 CA 负责制定国富安 CA 电子认证总体政策与策略，为下级子 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。

1.3.2 注册机构

注册机构作为电子认证服务机构授权委托的下属机构，包括注册系统（RA 系统），和证书受理点（LA），负责用户证书的申请、审批和证书管理，直接面向证书用户；一般情况下 LA 证书受理点进行用户身份鉴定和证书信息录入，提交到 RA 系统把证书申请信息传递到 CA。

国富安 CA 的 RA 系统分为自建 RA 和授权 RA，每个 RA 系统下面可以根据系统能力建立多个 LA 证书受理点。

自建 RA 指由国富安 CA 自己投资建设分布于全国各地的 RA 系统，归国富安 CA 所有，为证书总量在 500，000 张以下的地区或行业应用提供证书申请审批、证书信息录入以及证书发放并进行部分管理服务。

另一种为授权 RA，归授权的企业或组织所有，授权 RA 在遵循国富安 CA 电子认证业务规则的基础上负责为该区域或组织提供数字证书的申请，为证书总量相对较小（在 10000 以下，根据具体情况可以升级到 50，000 张以下），或证书审核严格或证书管理复杂的的区域和组织提供证书申请审批、证书信息录入以及证书发放并进行部分管理服务，适合于需要对 RA 系统功能进行客户化定制和需要自主管理 RA 系统的区域和组织使用。

RA 系统与 CA 系统根据其业务需求和特殊情况采用专线或 VPN 方式相连，之间的通信符合国家相关安全规范与标准。

LA 证书受理点是面向最终用户的注册审核机构，其主要功能是对用户提交的资料进行审核，以决定是否同意为该申请者发放证书。LA 的身份由 RA 审核，LA 的操作员证书由运行 CA 签发。LA 作为 RA 的下级机构，它不直接与 CA 进行数据交换，CA 不接收来自 LA 的证书签发请求，LA 的证书签发请求由 RA 转发给 CA。RA 服务器负责安全地和国富安 CA 服务器交换数据。

LA 证书受理点与 RA 系统一般采用 VPN 方式相连，之间的通信也符合国家相关安全规范与标准。

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。

1.3.4 依赖方

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、也可以不是一个订户。

1.3.5 其他参与者

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 证书应用

1.4.1 适合的证书应用

国富安 CA 所发证书能够满足不同的业务需要，如网上银行，电子商务，电子政务，安全电子邮件，SSL 安全代理，在线支付等应用。证书申请人根据实际需要和承担责任，自觉采用哪种数字证书类型。

1.4.2 限制的证书应用

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

由于证书的使用可能导致人员死亡、伤残的情形；由于证书的使用可能导致环境破坏的情形。

1.5 策略管理

1.5.1 策略文档管理机构

本《电子认证业务规则》的管理机构是国富安 CA 策略委员会。由国富安 CA 策略委员会负责对本《电子认证业务规则》的制定、发布、更新等事宜。

本《电子认证业务规则》由北京国富安电子商务安全认证有限公司拥有完全版权。

1.5.2 联系人

本《电子认证业务规则》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：gfacasupport@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

1.5.3 决定 CPS 符合策略的机构

本《电子认证业务规则》由国富安 CA 策略委员会制定并执行。

1.5.4CPS 批准程序

国富安安全策略委员会负责 CPS 的管理，CPS 的修订只能由 CA 运营中心起草，并由国富安安全策略委员会对 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工业和信息化部备案。

1.6 定义和缩写

术语定义一览表

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。
证书政策（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。
政策管理中心（PMA）或政策中心（PA）	政策管理中心是有制定安全政策（如 CP）的最终权威和职责的实体。
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。

缩写词

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 认证信息的发布

国富安 CA 在其网站（http://www.gfapki.com.cn）公布以下信息：

①RA 系统、LA 证书受理点的基本情况；

②用户协议和依赖方协议；

③CP 和 CPS；

国富安 CA 应当在目录服务器中公布：

①用户的证书；

②CRL。

2.2 发布的时间或频率

国富安 CA 按照 CPS 的相关规定修订 CPS、用户协议、依赖方协议。证书一经签发就要在目录服务器公布，证书状态及 CRL 根据本 CPS 的相关规定公开。

国富安 CA 的 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。证书吊销列表至少每 24 小时更新一次。

2.3 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 CPS、证书、证书状态、CRL 等信息的任何人必须遵守本 CPS、依赖方协议和 CRL 使用协议。

国富安 CA 所颁发的证书及证书状态信息由系统自动生成并发布，无法通过其他渠道进行添加、修改和删除等操作。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

根据证书类型不同，国富安 CA 签发的证书实体名字可以是个人姓名、组织机构、企业名称、部门名、域名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），它由如下内容组成：

- 国家 （C） =CN或不用；
- 组织机构 （O） =组织机构属性如下：
  - 对于一类自然人证书为 GFA
  - 组织机构代码
- 机构部门 （OU1） =订户组织机构部门名称；
  （OU2） =职业资格证号、商标、订户签名或其他，或不用；
  （OU3） =订户证书类型；
- 省或城市 （S） =订户所在的省、城市或不用；
- 位置 （L） =订户所在具体地点或不用；
- 通用名 （CN） =通用名如下：
  - 一类证书为身份证号 +姓名
  - 二类证书为组织机构代码 +申请人姓名（或组织机构、企业名称或部门名称）
  - 三类证书为域名或服务器 DNS名
- 电子邮箱 （E） =电子邮件地址；

国富安 CA 可以根据自己的要求拥有对最终订户证书主题甄别名意义修改的权利，但修改的前提是不损害其他证书订户的权利和义务，并随时公布修改结果。

3.1.2 对名称意义化的要求

主题和签发者的 DN 遵循 PKIX 标准，并且在证书中标明。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

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。

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

在国富安 CA 证书信任域中，订户证书实体中主题甄别名必须是唯一的，除非订户申请签发双证书（签名证书和加密证书），两个证书因为属于同一实体，因此中 X.500 甄别名是一样的，但证书密钥用途不一样，签名证书密钥只能用于签名，加密证书密钥只用于加密。

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。

3.1.6 商标和订户签名信息

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

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。

3.2.2 组织机构身份及其授权的鉴别

对于与组织机构相关的证书，如一类证书中的组织机构授权人证书、组织机构法人证书，二类证书以及三类证书中的高级服务器证书，组织机构应指定和授权证书的申请代表，出具申请委托函，在证书的申请书上签字、盖章表示接受证书申请的有关条款，并承担相应的责任。国富安 CA 或 RA（包括受理点）当面或采用其他方式审核组织机构身份及其申请者的代表人是否符合要求。

国富安 CA 对证书组织机构身份及申请者代表的鉴证按以下方式进行：

①审核该组织机构身份的真实性：国富安CA或RA（包括受理点）必须检查组织机构相关的证明文件原件或复印件，申请者需向国富安CA提供组织机构确实存在的证明(如

工商执照、组织机构代码证、税务登记等，对于服务器证书需要出具域名拥有证书等)。

②代表人身份的授权：国富安CA或RA（包括受理点）必须检查组织机构的证书申请委托函，委托函需加盖组织机构公章和签名，通过对代表人身份证件的验证或其他渠道核实代表人已经由该组织授权。

如果国富安 CA 或 RA（包括受理点）已经预先明确了组织机构和授权或委托人的身份，那么国富安 CA 或 RA（包括受理点）可以信赖这些证明。

对于特殊情况，国富安 CA 或 RA（包括受理点）可以采用其他方式追加组织机构身份鉴证的权利。

3.2.3 个人身份的鉴别

对于与个人身份有关的证书，如一类证书中的自然人证书、三类个人服务器证书中所涉及到的个人身份，申请人需要正确填写申请表并书写签名，国富安 CA 或 RA（包括受理点）可以面对面或采用其他方式进行如下内容的鉴证：

①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，国富安 CA或 RA（包括受理点）需要申请人出示个人身份证，如果非本人申请需出具委托函和委托人个人证件；

②证书申请者是证书申请中所说的哪个人：国富安 CA或 RA（包括受理点）可以要求申请人出示代表申请人户籍证明的相关材料，也可以采用其他第三方数据库或有效手段进行验证；

③密钥拥有：按照 3.2.1中所述的方式确认证书申请者与证书中所列公钥相对应的私钥。

④职业资格或书写签名核实：国富安 CA或 RA（包括受理点）可以和第三方机构合作，核实个人所拥有的职业资格证书和书写签名信息；

⑤除未经验证的订户信息，包含在证书中的信息是准确的；

如果国富安 CA 或 RA（包括受理点）已经预先明确个人的身份，那么国富安 CA 或 RA（包括受理点）可以信赖这些证明。

对于特殊情况，国富安 CA 或 RA（包括受理点）可以采用其他方式追加个人身份鉴证的权利。

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。

3.2.5 互操作准则

不在此规定。

3.3 密钥更新请求的标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

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。以下为国富安 CA 例行密钥更新过程：

根密钥更新时，由所有密钥管理员在场，共同启动密钥管理程序，执行密钥更新指令，硬件加密设备重新生成根密钥，并做相应记录。

对于用户密钥，如果加密公钥或签名私钥已经或即将到期，订户要求产生一个新的密钥对代替过期的密钥对即为密钥更新。订户访问国富安 CA 或注册机构的证书服务站点进行密钥更新申请，系统会自动获取订户原证书的相关信息，如订户甄别名、证书序列号等，形成证书密钥更新申请信息，申请信息包含新公钥并由原证书的私钥签名。

国富安 CA 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证。

3.3.2 吊销后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

在国富安 CA 的证书业务中，证书吊销请求可以来自订户，也可以来自国富安 CA 或 RA（包括受理点）。证书吊销的方式可以是订户要求国富安 CA 或 RA（包括受理点）管理员吊销，国富安 CA 或 RA（包括受理点）在认为必须的时候，有权发起吊销订户证书。

对于来自订户要求的吊销，可以有如下方式：

① 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；

② 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）接到证书吊销申请后，根据其他途径和方式，如传真、电话、快递等方式核实吊销身份后进行吊销操作。

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

证书申请实体包括国家法定公民具有独立法人资格的组织机构（包括行政机关、事业单位、企业单位、社会团体和人民团体）。

服务器证书由域名拥有机构或获得域名使用授权的个人或组织授权申请。

4.1.2 注册过程与责任

证书申请人按照本《电子认证服务规则》所规定的要求，填写证书申请表，并准备相关的身份证明材料。CA 或 RA（包括受理点）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：订户要按照本《电子认证服务规则》所规定的要求准备证书申请材料，并确保申请材料的真实性。

CA 或 RA（包括受理点）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。

根据《中华人民共和国电子签名法》的规定，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

4.2.1 执行识别与鉴别功能

国富安 CA 或 RA（包括受理点）按照本《电子认证服务规则》所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体鉴别流程见 CPS §3.2.2、CPS §3.2.3 和 CPS §3.2.4 所描述的过程进行个人及组织机构身份鉴别和委托确认的鉴别。

4.2.2 证书申请批准和拒绝

在国富安 CA 或 RA（包括受理点）完成对证书申请的鉴别，有关鉴证获得通过并且证书申请者履行了其他应尽的责任（如付款）后，国富安 CA 或 RA（包括受理点）批准申请。如果鉴证未获通过或证书申请者拒绝履行了其他应尽的责任（如付款），国富安 CA 或 RA（包括受理点）将会拒绝申请。

4.2.3 处理证书申请的时间

国富安 CA 或 RA（包括受理点）将在合理时间内完成证书请求处理。在申请者提交资料齐全且符合要求的情况下，面对面处理证书申请的时间不超过 1 个工作日，其他处理证书的时间不超过 5 个工作日。

4.3 证书签发

证书签发过程是：国富安 CA 得到 RA 通过安全方式传来的用户公开信息身份，生成证书信息并通过 RA 通知用户的过程。

4.3.1 证书签发中注册机构和电子认证服务机构的行为

国富安 CA 在批准证书申请之后，将证书签发。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

国富安 CA 签发完证书后会在系统中及时通知下属 RA（包括受理点）机构，由 RA（包括受理点）下载证书（面对面申请），或者采用其他方法通知订户下载证书。

4.3.2 电子认证服务机构和注册机构对订户的通告

国富安 CA 或 RA（包括受理点）对订户的通告有以下几种方式：

①通过面对面的方式，通知订户到国富安 CA 或 RA（包括受理点）领取数字证书；

②邮政信函通知订户；

③电子邮件或其它国富安 CA认为安全可行的方式通知订户。

4.4 证书接受

4.4.1 构成接受证书的行为

国富安 CA 订户接受证书的方式可以有如下几种：

通过面对面的提交，订户从国富安 CA 的 RA（包括受理点）接受载有证书和私钥的介质。在这种情况下由国富安 CA 的 RA（包括受理点）替订户产生证书请求、证书密钥对、下载证书，订户接受载有证书和私钥的介质被视为同意接受证书。

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。国富安 CA 认证系统记录订户已下载的信息即视为订户同意接受证书。

4.4.2 电子认证服务机构对证书的发布

国富安 CA 有基于 LDAP 协议的目录服务，除非与订户之间有特殊的约定，国富安 CA 通常将签发的证书及时发布到目录系统上。

4.4.3 电子认证服务机构对其他实体的通告

对于其签发的证书，国富安 CA 及 RA（包括受理点）不通知其他实体，其它实体可以通过目录服务器查询到国富安 CA 已签发的数字证书。

4.5 密钥对和证书的使用

密钥对和证书不应用于其规定、批准的用途之外的目的，否则其应用是不受相关法律和国富安 CA 策略保障的。

4.5.1 订户私钥和证书的使用

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。

4.5.2 信赖方公钥和证书的使用

当信赖方接受到经数字签名的信息后，应该：

① 获得数字签名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，并验证其证书的有效性。

③ 证书的用途适用于对应的签名。

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

4.6.1 证书更新的情形

对于国富安 CA 签发的任何最终订户证书，证书到期前 30 天系统将会自动提醒订户用户证书将到期，如继续使用可进行证书更新。到期前 30 天内或已到期后 30 天内，如果订户原来的注册信息继续有效，订户可访问国富安 CA 或注册机构的证书更新站点申请证书更新。申请证书更新时用户无需象初次申请那样填写注册信息，系统会自动获取所需的信息。

4.6.2 请求证书更新的实体

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。

4.6.3 证书更新请求的处理

接受到用户的证书更新请求后，国富安 CA 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 用原证书上的订户公钥对更新申请的签名进行验证。

在此基础上，国富安 CA 或注册机构一般会根据原有的信息通过电话等其他手段鉴定证书更新的实体是否是原来的实体，或者采取与初次证书申请一样的鉴证过程完成证书更新请求的鉴证，然后批准、签发证书。

4.6.4 颁发新证书时对订户的通告

同 CPS § 4.3.2。

4.6.5 构成接受更新证书的行为

同 CPS § 4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同 CPS § 4.4.2。

4.6.7 电子认证服务机构对其他实体的通告

同 CPS § 4.4.3。

4.7 证书密钥更新

证书密钥更新是为订户产生新的密钥对，使用与原证书一致的主题甄别名并签发一张新证书。

4.7.1 证书密钥更新的情形

对于国富安 CA 签发的任何最终订户证书，证书到期前 30 天系统将会自动提醒订户用户证书将到期，如用户希望继续使用证书并保持原有注册信息不变，但需要变更密钥对，可申请证书密钥更新。到期前 30 天内或已到期后 30 天内，如果订户原来的注册信息继续有效，订户可访问国富安 CA 或注册机构的证书密钥更新站点申请证书密钥更新。申请证书密钥更新时用户无需象初次申请那样填写注册信息，系统会自动获取所需的信息。

如果用户需要改变注册信息，或者用户证书到期超过 30 天、用户证书被吊销则不允许进行证书密钥更新。

4.7.2 请求证书密钥更新的实体

同 CPS § 4.1.1。

4.7.3 证书密钥更新请求的处理

证书密钥更新的请求包含新的公钥并且由新私钥签名，同时还包含有原证书私钥签名的更新请求信息。

在接收到证书密钥更新请求后，国富安 CA 认证系统将执行如下操作：

（1）申请对应的原证书存在，并且由认证机构签发；

（2）申请对应的原证书没有被注销，没有执行过证书更新，密钥更新请求在允许的期限；

（3）订户用原证书生成签名，在线更新系统验证其签名。

完成上述验证后，国富安 CA 或注册机构按与证书更新相同的方式和流程（参见 CPS § 4.6.3），完成证书密钥更新请求的鉴证，然后批准、更新密钥。

4.7.4 颁发新证书时对订户的通告

同 CPS § 4.3.2。

4.7.5 构成接受密钥更新证书的行为

同 CPS § 4.4.1。

4.7.6 电子认证服务机构对密钥更新证书的发布

同 CPS § 4.4.2。

4.7.7 电子认证服务机构对其他实体的通告

同 CPS § 4.4.3。

4.8 证书变更

证书变更是指在订户证书未到期之前，订户的关键信息有变更，导致证书内容有变化，但密钥对保持不变的情况。国富安 CA 不直接受理证书变更业务，订户要变更证书

中的内容时，视为申请一张新证书，国富安 CA 需先吊销原有证书，再签发新证书，并且证书变更的申请及处理流程与申请新证书一致（参见 CPS § 4.1、CPS § 4.2）。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

证书吊销分为主动吊销和被动吊销。主动吊销是指由用户提出吊销申请，由 RA 受理点 LA 进行审核并由具有相关权限的操作员对其要求进行处理，吊销证书；被动吊销是指当国富安 CA 及 RA（包括受理点）确认用户违反证书应用规定或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应尽的责任和义务。

在以下情况下，证书订户（主动吊销）应当要求吊销证书：

① 证书用户的私钥被泄露、丢失、盗窃、更改、滥用或遭到其它损害或者证书主体推测有这些情况发生；

② 证书不再需要用于原来的用途，如对于组织机构授权人证书，被授权人已经离开组织，不能代表该组织机构从事与组织有关的业务。

③ 证书包含的任何信息发生变化或容易引起误解。

国富安 CA及 RA（包括受理点）发现有下列情况下可决定撤销用户证书（被动吊销）：

① 证书用户不支付证书费用；

② 证书包含的信息发生变化；

③ CA的私钥泄露；

④ 证书用户已不再是国富安 CA客户；

⑤ 证书用户违反 CPS;

⑥ 因证书申请信息虚假等原因造成证书发放错误；

⑦ 证书用户对证书的使用有可能危及国富安 CA的安全；

⑧ 由于不可抗力、自然灾害、法律法规的变更、政府行为及其它人力无法控制的原因延误或阻止 CPS中的任一方当事人履行义务，并严重威胁或损害到另一方的利益；

此外，证书订户可以不需任何理由要求吊销证书，国富安 CA 应当应证书主体的要求吊销证书。国富安 CA 没有义务公开证书吊销的原因。

4.9.2 请求证书吊销的实体

能够要求吊销证书的实体有：

① 证书用户；

② 经证书用户合法授权的代表；

③ 在证书用户已经违反了协议法规或有效的法律情况下，国富安 CA授权的工作人员也有权要求作废。

④ 国家相关司法部门、政府职能部门及监管部门等，可以依据相应法律法规规定，有权要求吊销或挂起证书。

4.9.3 吊销请求的流程

当国富安 CA 及 RA（包括受理点）有充分的理由确信需要吊销订户的证书时，国富安 CA 及 RA（包括受理点）应严格根据其内部流程进行操作，在证书吊销后，国富安 CA 或 RA（包括受理点）将通过适当方式，包括邮件、传真等，通知最终订户证书已被吊销及吊销的理由。

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）接到证书吊销申请后，根据其他途径和方式，如传真、电话、快递等方式核实吊销身份后进行吊销操作。

4.9.4 吊销请求宽限期

如果出现私钥泄漏或组织机构授权人证书，被授权人已经离开组织，不能代表该组织机构从事与组织有关的业务等事件，吊销请求必须在发现泄漏或人员离职 8 小时之内提出。其它原因的吊销请求必须在 24 小时内提出。

4.9.5 电子认证服务机构处理吊销请求的时限

吊销申请一般在批准后 24 小时后生效，特殊紧急情况下可以立即生效（假使网络传输条件能够保证）。生效表示国富安 CA 将在证书黑名单库中公布被吊销的证书。对于测试证书的作废，不提供黑名单公布，但将在证书资源库中删除该测试证书。

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。很多的应用本身建有用户帐户数据库并基于用户帐户进行应用控制，数字证书在此只起身份鉴别的，在这种情况下检查证书是否吊销不一定是必须的。

4.9.7 CRL 发布频率

国富安 CA 至少每 24 小时更新和公布黑名单(CRL),依赖方根据国富安 CA 最新公布的 CRL 确认使用的证书是否被列入黑名单，国富安 CA 根据情况，有可能会实时公布黑名单。

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 上的滞后时间不超过 24 小时。

4.9.9 在线状态查询的可用性

国富安 CA提供证书状态的在线查询服务（OCSP），该服务 7X24 小时可获得。

4.9.10 在线状态查询要求

依赖方是否进行在线状态查询完全取决于应用的安全要求。很多的应用本身建有用户帐户数据库并基于用户帐户进行应用控制，数字证书在此只起身份鉴别的，在这种情况下在线状态查询不一定是必需的。对于安全保障要求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通过证书状态在线查询检查该证书的状态。

4.9.11 吊销信息的其他发布形式

除了 CRL、 OCSP 外，国富安 CA的 LDAP 提供 CRL 查询。

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。

4.9.13 证书挂起的情形

国富安 CA不直接受理证书挂起业务，证书挂起的情形、申请流程、处理流程及其相关操作规范与证书吊销一致。

4.10 证书状态服务

国富安 CA通过 CRL、 OCSP、 LDAP 提供证书状态服务。

4.10.1 操作特征

国富安 CA的证书状态查询以网络服务的形式提供。CRL 通过80 端口采用HTTP 协议提供。OCSP 符合RFC2560，反映证书的当前状态。证书目录LDAP 符合LDAP V2（RFC3377，2251-2256，2829-2830）

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。

4.10.3 可选特征

无

4.11 订购结束

订购结束包含以下两种情况：

（1）证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户自动终止与国富安 CA的服务关系；

（2）在证书有效期内，证书被吊销后，即订购结束，但这种情形国富安 CA或 RA（包括受理点）应及时通知订户。

一旦用户在证书有效期之内终止使用国富安 CA的认证服务，国富安 CA在批准终止请求后，将实时的把该订户证书吊销，并且按照 CRL发布策略进行发布。

4.12 密钥生成、备份与恢复

国富安 CA依据国家管理规定，提供加密证书密钥的集中管理和恢复。

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。

4.12.2 会话密钥的封装与恢复的策略与行为

无

5 认证机构设施、管理和操作控制

国富安 CA系统建设遵循了国家规定的技术性安全控制规范，这些规范对于国富安 CA的权威性是十分关键的，将最大限度的减少 CA遭受攻击的情况发生。

5.1 物理控制

系统的物理安全和环境安全是整个国富安CA系统安全的基础，它包括基础设施的处理、周边环境的监控、区域访问控制、设备安全及灾难预防等。为把国富安CA系统的危险减至最低限度，国富安CA选择设施的适当位置，充分考虑水灾、地震、电磁干扰与辐射、犯罪活动以及工业事故等的威胁。

国富安 CA物理场地满足以下安全要求，有效的控制风险：

① 防止物理非法进入，7-9层物理结构及完善的安全管理体系保护国富安 CA的运营设施和知识产权；

② 防止未经授权的物理访问，确保未经授权的人或仅被授权访问有限物理区域的人员不得访问国富安 CA机房的受限区域；

③ 维护国富安 CA系统服务的完整性、可用性，保障提供国富安 CA服务的系统、设施不受到破坏，保障认证服务不被中断。

5.1.1 场地位置与控制

5.1.1.1 参照标准要求

GB2887-89《计算站场地技术条件》

GB50174-93 《电子计算机机房设计规范》

GB6650— 86《计算机机房活动地板技术要求》

GBJ79— 85《通信接地设计规范建筑内部装修设计防火规范》

GBJ19-87《采暖通风与空气调节设计规范》

GB50222— 95《建筑内部装修设计防火规范》

GB6650— 95《高层民用建筑设计防火规范》

GB7450— 87 《电子设备雷击保护守则》

GBJ52-82 《工业与民用供电系统设计规范》

GBJ54-83《低压配电装置及线路设计规范》

GB232-82 《电气装置安装工程及验收规范》

JB16-83 《 建筑电气设计技术规范》

GBJ79-85 《工业企业通信接地设计规范》

GB50222-95《建筑内部装修设计防火规范》

GBJ116-88《火灾自动报警设计规范》

CECS89-97《建筑与建筑群综合布线系统施工及验收规范》

GBJ300-88《建筑安装工程质量检验评定统一标准》

GB115-87《工业电视监控系统工程设计规范》

GB— 12190《高性能室效能的测量方法》

GJBZ20219-94《军用电磁室通用技术要求和检测方法》 C级标准

5.1.1.2 机房设计指标的要求

温度：国家标准 B级 23℃± 5℃

相对湿度：国家标准 B级 55%± 15%

温度变化率小于 10%，不凝露

尘埃：粒径≥ 0.5um个数≤ 18000/dm3

噪音：计算机开机条件下，主机操作员位置 A≤ 68dB

接地：

计算机系统直流逻辑地电阻值≤ 0.9Ω

计算机系统交流工作地电阻值≤ 1Ω

计算机系统安全保护地电阻值≤ 1Ω

计算机系统防雷保护地电阻值≤ 4Ω

根据计算机系统的要求，建议计算机系统直流逻辑地独立设置。而计算机系统交流工作地、安全保护地、防雷保护地直接接在大楼综合地上。

零地电位差≤ 1V

电压：国家标准 B级 三相电压为 380V，波动不大于± 8%

单相电压为 220V，波动不大于± 8%频率：国家标准 B级 50Hz± 0.5Hz

谐波成份：在机器运行时≤ 3%

负荷分配：三相电流不平衡度≤ 20%三相电压不平衡度≤ 5

照度：离地面 0.8m处，照度 B不应低于 300LX，基本工作间和第一类辅助房间不低于 200LX，应急照明离地面 0.8m处不应低于 10LX。主要通道及有关房间的照度在距地面 0.8m处不应低于 2LX。

电磁干扰：

机房内无线电杂波干扰在频率范围 0.15MHz~1000MHz时不大于 126Db。

磁场干扰强度≤ 800A/m（相当于 10Oe）

主机房内绝缘体静电电位：≤ 1kV

在计算机系统停机条件下主机房地板表面垂直及水平向的振动加速度值，不应大于 500mm/s2

5.1.1.3机房区域划分

根据制定的安全策略，将机房分为三个区域，分别为公共管理区、 CA区和 KMC区。

CA区包括 CA核心区、 CA管理区、 RA服务区： 统称证书认证中心，简称 CA。

CA核心区屏蔽机房与外界区域利用通顶隔墙进行保护，防止通过天花板下面的假平顶进入。必须采用六面钢板进行屏蔽处理，以防止电磁干扰，增加系统的安全性。

CA中其他区域采用通顶隔墙进行隔离，便于维护管理。

CA所有出入门由门禁出入卡系统进行控制，并在安全区采用指纹识别与智能卡结合的方式实施。每个区域都安装视频监控系统、防侵入系统、机械组合锁等装置。

按防火管制的要求，最少设置两个出入口。

KMC区包括 KMC管理区、 KMC核心区：统称密钥管理中心，简称 KMC。它是一个相对独立的区域，整个区域必须用六面钢板进行处理。

KMC机房采用屏蔽专用室、门，以防止电磁干扰，增加系统的安全性。

KMC区域与外界区域利用通顶隔墙进行保护，防止通过天花板下面的假平顶进入。

KMC主机房与 KMC管理区采用通顶隔墙进行隔离，便于维护管理。

KMC 中的所有区域的进出采取指纹识别加智能卡进行控制。每个区域都安装视频监控系统、防侵入系统、机械组合锁等装置。

5.1.2 物理访问

机房内部一律禁止参观，只有经过国富安 CA授权的人员才能进入授权的部位和工作地点。机房采用高安全性的监控技术，包括生物活体探测、指纹、门警等监控技术，以确保物理通道的安全。国富安 CA机房实行 7*24小时自动监控。

监控记录文件包括对机房通道上的所有踪迹的记录。所有国富安 CA被授权的员工在限制区域活动都需要有国富安 CA人员的陪同。国富安 CA授权的人员清单会提供给国富安 CA，以保证只有经授权的国富安 CA员工才能进入机房，对于要进入机房的国富安 CA的来访者，他们需要有一位经国富安 CA授权的员工陪同。

5.1.3 电源和空调

CA 系统供电得到了充分保障，使用不间断电源（UPS），避免电源波动，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。

CA系统空调系统使用中央空调和冷却设备，并采用独立空调作为备份。

国富安 CA对 CA系统的电源、空调等物理要求，应该与机房所在地点的物业管理机构进行协调，使现有的要求得到满足。国富安 CA的要求参照《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》的规定，而且每年对是否符合要求进行检查。

5.1.4 防水

国富安 CA保证 CA系统能够防止水的侵蚀。

国富安 CA对 CA系统的防水要求，在机房建设时已经考虑了采取相应的措施。

5.1.5 防火

充分保障 CA系统避免火灾的威胁。

国富安 CA对 CA系统防火的要求，在机房建设之初已经加以考虑，并采取了有效措施。

5.1.6 存储介质保护

CA系统中使用的存储介质必须得到安全可靠的保护，避免诸如：温度、湿度和磁力等环境变化可能产生的危害和破坏。

5.1.7 废物处理

当国富安 CA存档的敏感数据或密钥已不再需要或存档的期限已满时，应当将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.1.8 异地备份

国富安 CA同时提供异地的备份，异地备份的使用在国富安 CA灾难恢复计划中规定。

5.1.9RA（包括受理点）的物理控制

国富安 CA注册机构即 RA（包括受理点）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，国富安 CA在遵循此 CPS的前提下有制定异地 RA（包括受理点）的建设和运营方案的权利和义务。

5.2 操作过程控制

5.2.1 CA 系统管理人员

（1）CA 系统用户：

由 CA初始化工具产生，由安全管理小组指定。

（2）CA 系统超级管理员、安全审计员：

CA超级管理员、安全审计员由三个 CA系统用户共同登录后方可生成。这些角色由安全管理小组指定。

（3）CA 业务管理员：

由 CA超级管理员产生

（4）CA 业务操作员：

由 CA业务管理员产生

（5）RA 超级管理员、RA 安全审计员：

由 CA超级管理员产生，由安全管理小组指定。

（6）RA 业务管理员：

由 RA超级管理员产生

（7）RA 业务操作员：

由 RA业务管理员产生

5.2.2 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，日常设置安全官员，其主要职责和义务如下：

① 制定 CA的安全策略；

② 指导 CA的安全管理；

③ 设计和指导 CA的安全策略实施；

④ 对 CA的安全管理进行定期的检查和评估；

⑤ 对安全策略和执行程序的日常维持；

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。

5.2.3 每一项任务需要的人数

国富安 CA确保单个人不能接触、导出、恢复、更新、撤销 CA存储的 CA证书对应的私钥。

至少三个人，使用一项对参加操作人员保密的密钥分割和合成技术，来进行任何密钥恢复的操作。

国富安 CA对于其运行和操作相关的职能有明确的分工，贯彻互相牵制的安全机制。

5.2.4 安全令牌控制

所有国富安 CA的在职人员，必须通过认证后，根据作业性质和职位权限的情况，发放

需要的系统操作卡、门禁卡、登录密码、操作证书、作业账号等安全令牌，对于使用安全令牌的员工， CA系统将独立完整地记录其所有的操作行为。

所有 CA在职人员必须确保：

① 发放的安全令牌只直接属于个人或组织所有；

② 发放的安全令牌不允许共享；

③ 国富安 CA的系统和程序通过识别不同的令牌对操作者进行权限控制。

5.3 人员控制

5.3.1 人员背景审查

国富安 CA员工的录取经过严格的审查，根据岗位需要，增加相应可信任的员工。员工需要有 3个月的考察期，关键部位的员工考察期为半年，核心部位的员工考察期为 1年。根据考察的结果安排相应的工作，或者辞退。国富安 CA根据需要，对员工进行职责、岗位、技术、政策、法律、安全等方面的培训。

国富安 CA会对其关键的 CA职员进行严格的背景调查， RA(包括 RA 受理点)操作员的审查可以参照国富安 CA对可信任员工的考察方式进行。 RA(包括 RA 受理点)责任单位可以在此基础上增加考察和培训条款，但不得违背国富安 CA证书受理的规程和国富安 CA CPS中的相关条款。

国富安 CA确立流程管理规则，据此， CA员工受到合同和章程的约束不许泄露国富安 CA证书服务体系的敏感信息，所有的员工与国富安 CA签订保密协议合同期满以后 3年内仍然不得从事与国富安 CA相类似的工作，由第三方公证机构对此加以公证。

5.3.2 背景审查的实现

国富安 CA与有关政府部门和调查机构合作，完成对国富安 CA可信任员工的背景调查。

5.3.3 培训要求

国富安 CA对国富安 CA员工进行以下内容的综合性培训：

① CA安全原则和机制；

② CA使用的软件介绍；

③ CA操作的系统和网络；

④ CA质量控制体系；

⑤ 岗位职责；

⑥ 政策标准和程序；

⑦ 相关法律、仲裁规则、管理办法等。

5.3.4 继续培训要求

根据国富安 CA策略调整、系统更新等情况，国富安 CA可能要求员工进行继续培训以适应新的变化。

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。

5.3.6 未授权行为的制裁

当国富安 CA员工被怀疑，或者已进行了未授权的操作，例如未经授权滥用权利或超出权限使用 CA系统或进行越权操作，国富安 CA在得到信息后立即暂停该员工进入国富安 CA证书服务体系。根据情节严重程度，实施包括提交司法机关处理等措施。

一旦发现上述情况国富安 CA立即撤销或终止该人员的安全令牌。

5.3.7 系统抢修的要求

国富安 CA在系统遇到紧急情况，需要联合抢修时，应至少有 1名国富安 CA安全事务专员在场，抢修人员在运行人员的陪同下，执行监督下许可的操作，所有操作修改都留有记录。

非国富安 CA员工因物理、修理、消防、强电故障等情况，需要进入国富安 CA数据中心实施修理时，必须报安全事务专员，经同意后，认证修理者的身份，由国富安 CA规定的可信任员工始终陪同和监护，完成约定部位的修理。

5.3.8 工作轮换周期和顺序

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。

5.3.9 独立合约人的要求

对不属于国富安 CA内部的工作人员，但从事国富安 CA有关业务的人员等独立签约者（如 RA机构包括受理点工作人员），国富安 CA的统一要求如下：

① 人员档案进行备案管理；

② 具有相关业务的工作经验；

③ 必须接受国富安 CA组织的为期一周的岗前培训。

5.3.10 提供给员工的文档

为使系统正常运行，必须提供给具有权限的相关人员各种文档，包括但不限于：

① 加密机用户手册；

② 机房设备管理办法；

③ 数字证书运营规范；

④ 灾难备份和恢复方案；

⑤ 目录服务器安装配置手册。

5.4 审计日志程序

5.4.1 记录事件的类型

国富安 CA记录与系统相关的事件，这些记录信息称为日志。对于这些日志，无论其载体是纸张还是电子文档的形式，必须包含事件发生的日期、事件的发生时间段、事件的内容和事件相关的实体等。

国富安 CA还可能记录与系统不直接相关的事件，例如：物理通道参观记录、人事变动等。

5.4.2 处理或归档日志的周期

国富安 CA每月对日志进行审查，并对审查日志的行为进行备案。

5.4.3 审计日志的保存期限

国富安 CA在数据库保存审计日志至少两个月，离线保存至少为五年。

5.4.4 审计日志的保护

国富安 CA执行严格的管理，确保只有国富安 CA授权的人员才能对审查日志进行相应

操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作，另外对日志要进行异地备份。审计日志的制作和访问进行岗位分离。

国富安 CA将审计日志保存到存储中，并存放到异地，实行安全保管。

5.4.5 审计日志备份程序

国富安 CA保证所有的审查记录和审查总结都按照国富安 CA备份标准和程序进行备份。根据记录的性质和要求，分为实时、按天、按周、按月和按年等多种形式的备份，可采用在线和离线两种方式的备份工具。

审计文档由管理员每周进行一次归档。所有档案安全存放在文档库内。

5.4.6 审计日志收集系统

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。

5.4.7 对导致事件实体的通告

国富安 CA发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，国富安 CA保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

国富安 CA有权决定是否对导致事件的实体进行通告。

5.4.8 脆弱性评估

国富安 CA每年对系统进行脆弱性评估，以降低系统运行的风险。

5.5 记录归档

5.5.1 存档记录类型

国富安 CA中心将实际操作中的的归档记录类型分为纸质记录和电子记录，纸质记录其主要内容为用户证书申请资料，主要由客户资料管理员和档案室资料管理员进行归档管理。对于电子记录（主要是数据库信息、日志、操作记录等），由 CA系统运营管理员进行管理维护。

国富安 CA的纸质归档记录：

- GFACA的系统建设和升级文档；
- 证书申请信息、证书服务批准和拒绝的信息、与证书订户的协议、证书等；
- 电子认证服务规则、证书策略、各类服务规范和合作协议等；
- 物理设施的访问记录，授权人员进出；非授权人员进出及陪同人；安全存储设施（离线密钥）的访问。授权人员进出物理设施由国富安物理场地的访问控制系统自动记录，非授权人员进出由陪同人员作纸质记录；

国富安 CA的电子归档记录：

- 证书归档（主要是对已经过期的证书进行归档）；
- 系统运行和认证服务的审计数据、认证系统密钥升级；
- 证书生命周期内的管理事件，包括证书的申请、批准、更新、吊销等；成功或失败的证书操作。这些记录由认证系统自动记录，保存在数据库；
- 国富安 CA会对 CA的数据库定期归档；

签名私钥原则上由用户本身保存。国富安 CA只保存用户请求保存的私钥，并承诺保证私钥数据库的安全性。有关私钥的责任应由用户本身承担。

5.5.2 存档的保留期限

国富安 CA规定除法律法规和认证主管机构提出的保存期限以外，所有归档记录保存期限为 5年。

5.5.3 档案的保护

存档内容既有物理安全措施的保证，也有密码技术的保证，只有经过授权的工作人员按照特定的安全方式才能接近这些档案。国富安 CA采用保护措施以保护相关的档案内容免遭恶劣环境的威胁，如温度湿度和强磁力等的破坏。

5.5.4 存档备份

所有存档的文件数据库除了保存在国富安 CA的主要数据库，还将在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互，只有授权的工作人员才能在监督的情况下，对档案进行读取操作，国富安 CA在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳要求

国富安 CA对每项日志都有时间记录，对于纸质记录，有操作人员按要求手工记录时间信息；对于电子记录，由系统自动生成时间信息，但这些时间信息未采用时间戳技术。

5.5.6 档案收集系统

国富安 CA的档案收集系统由人工和自动操作两部分组成。

5.5.7 验证档案信息

国富安 CA每年会验证存档信息的完整性。

5.6 密钥转换

5.6.1 密钥转换定义

在这里密钥转换是指当国富安 CA证书到期而需要更换 CA密钥对时所采取的措施。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。

5.6.2 CA 证书有效期

国富安 CA证书有效期按国家规定进行设置。在国富安 CA证书到期之前，国富安 CA将对 CA私钥进行更换。密钥转换程序在旧密钥对向新密钥对的转换起着过渡的作用。国富安 CA密钥转换采用以下方式：

① 国富安 CA将在证书到期前的 60天内停止颁发新的证书；

② 旧的国富安 CA证书到期后，国富安 CA将用新的 CA密钥对签发证书。

5.6.3 CRL

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 灾难恢复

5.7.1 国富安 CA 遭到攻击造成灾难时的恢复

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。

5.7.2 CA 证书公钥被撤销

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。

5.7.3 CA 证书私钥被攻破

当国富安 CA的证书私钥被攻破时，国富安 CA应根据国富安 CA灾难恢复计划规定的灾难恢复步骤进行操作。

5.7.4 自然灾难或其他灾难后采取的安全措施

按照国富安 CA灾难恢复计划实施。

5.8 国富安 CA 终止提供服务

当国富安 CA打算终止提供服务的情况下，国富安 CA会在终止提供服务前最少三个月的时间内给 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。

国富安 CA会按照相关法律的规定来安排好档案和证书的存档工作。

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

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。

国富安运营 CA的签名密钥对在本地的硬件加密设备中产生，除了加密设备许可的备份机制，私钥不能出此硬件加密设备。产生密钥的时候必须有 5个密钥管理人员的多数在场同时登陆系统后由加密设备产生，任何单独的一个人都无法进行签名私钥的操作，密钥管理人员的登陆采用 IC卡的形式。

对于订户签名密钥对，国富安 CA根据证书类型有如下规定：

一类证书中的组织机构法人证书、组织机构授权人证书需要采用硬件加密模块（USB Key或 IC卡），自然人证书推荐使用硬件加密模块的同时也允许使用其他软件密码模块生成密钥对；

二类证书，订户必须使用硬件加密模块（USB Key或 IC卡）产生签名密钥对；

对于三类证书，订户利用WEB服务器软件提供的密钥生成功能生成密钥对或采用专门的硬件加速模块产生密钥对；

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 CPS的前提下制定符合其应用的特殊证书策略。

6.1.2 私钥传送给订户

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。

6.1.3 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，经注册机构 RA(包括受理点) 传递到国富安 CA。

订户的加密证书公钥，由 KMC通过安全通道传递到用户，遵循国家密码管理局加密私钥不落地的要求。

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。

6.1.4 电子认证服务机构公钥传送给依赖方

国富安 CA可以通过如下方式传送 CA公钥给依赖方：

① 依赖方可以从国富安 CA的网站 (http://www.gfapki.com.cn)下载 CA证书，从而得到 CA的公钥；

② 依赖方访问国富安 CA目录服务器；

③ 通过电子签名邮件将 CA传送给依赖方；

④ 其他方式如软件绑定的形式等等；

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 2048比特。

6.1.6 公钥参数的生成和质量检查

① CA的签名密钥对采用国家密码管理局许可的硬件加密机生成。

② RA、受理点的密钥对采用国家密码管理局许可的硬件加密卡生成。

③ 所有其他证书用户的密钥对可以使用国富安 CA认可的软件或硬件模块生成。

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 私钥的安全保证

6.2.1 密码模块标准和控制

国富安 CA所用的密码设备都是经国家相关部门认可的产品，其安全性达到以下要求：

① 接口安全：不执行规定命令以外的任何命令和操作；

② 协议安全：所有命令的任意组合，不能得到私钥的明文；

③ 密钥安全：密钥的生成和使用必须在硬件密码设备中完成；

④ 物理安全：密码设备具有物理防护措施，任何情况下的拆卸均立即销毁在设备内保存的密钥。

6.2.2 私钥的多人控制

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。

6.2.3 私钥的托管

一般情况下 ,国富安 CA不向证书用户提供签名私钥托管服务。

国富安 CA可根据客户和法律的要求 ,对证书用户的加密密钥对提供托管服务。如果证书用户选择加密密钥对托管，国富安 CA将在非常严密的安全下提供密钥管理和恢复的服务。

国富安 CA承诺不泄露托管的加密密钥对，并且从技术上保证。

6.2.4 私钥备份

用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。

6.2.5 私钥归档

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，并通过数据库备份出来进行归档保存，归档后的密钥形成历史信息链，供查

询或恢复。

国富安 CA提供过期的托管加密密钥的归档服务。

6.2.6 私钥导入或导出密码模块

使用国富安 CA软件可以把私钥安全导入到密码模块中，私钥无法从硬件密码模块中导出。

6.2.7 私钥在密码模块中的存储

私钥在硬件密码模块中加密保存。

6.2.8 激活私钥的方法

根据订户证书存储介质的不同，国富安 CA有如下几种私钥激活方法：

私钥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计算机以防止在没有得到订户授权的情况下其他人员使用订户的计算机。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。如果该私钥有口令保护，软件密码模块加载后，还需要输入口令才能激活私钥。

对于订户必须使用 USBKey、智能卡等硬件密码设备存放私钥，私钥不能出卡，并且订户要使用 PIN 码（口令）或指纹鉴别等机制保护私钥。要激活私钥，用户计算机上需安装相应的驱动程序并将 USB Key 或智能卡插入相应的读卡设备，输入相应的 PIN 码（口令）或指纹鉴别信息，在通过密码验证后方可激活私钥。

对于国富安 CA签发的服务器证书，如果没有使用硬件密码模块产生、保存私钥，则私钥是存放在服务程序的软件密码模块中，这时订户应该使用口令对私钥进行保护。当服务程序启动，软件加密模块被加载，并输入相应的私钥保护口令后，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服务器上，服务程序启动，并输入相应私钥保护口令后，证书私钥被激活。

国富安 CA的 CA私钥存放在硬件密码模块中，并且其激活数据按 CPS § 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 5选 3的原则输入激活数据的分割。

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。

6.2.10 销毁密钥的方法

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。

6.2.11 密码模块的评估

国富安 CA使用山东得安信息技术有限公司的 SJJ0929服务器密码机，符合国家有关标准。密码机采用以分组密码体制为核心的高强度密码算法和非对称密码体制，密钥采取分层结构，逐层提供保护。主要技术指标如下：

① 通信接口：符合国际 ITU Ethernet RJ45标准；

② 带宽控制： 10M/100M自适应，充分满足突发业务需要；

6.3 密钥对管理的其他方面

6.3.1 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。它们由国富安 CA和密钥管理中心定期归档。

6.3.2 证书操作期和密钥对使用期限

所有订户证书的有效期和其对应的密钥对的有效期有其不一致的地方，在具体的使用过程中有如下的扩展：

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，直到私钥受到损害或密钥对存在被破解的风险，如加密算法被破解。当私钥受到损害或密钥对存在被破解的风险后，签名证书的公钥在技术上仍然可以用于验证数字签名，但这种验证在法律上不一定是有效的。

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。

6.4 激活数据

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。

6.4.2 激活数据的保护

国富安CA 私钥的激活数据的5 个IC 卡，由国富安CA5 个不同的可信人员掌管，存放在保险盒中。

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。如果因为激活数据丢失而造成私钥被盗，用户没有采用其他保护手段（吊销证书申请），由此带来的损失由订户自己承担。

6.4.3 激活数据的其他方面

6.4.3.1 激活数据的传送

存有国富安CA 私钥的激活数据的IC 卡，通常保存在国富安CA的安全设施中，不能携带外出或传送。如因某种特殊情况确实需要传送时，其传送过程需在国富安CA安全管理人员和密钥管理人员的监督下进行。

当订户证书私钥的激活数据需要进行传送时，订户应保护它们在传送过程中免于丢失、偷窃、修改、非授权泄露、或非授权使用。

6.4.3.2 激活数据的销毁

存有国富安CA私钥的激活数据的IC 卡，其销毁所采取的方法包括将IC 卡初始化，或者彻底销毁IC 卡，无论采取何种方式，都将保证不会残留有任何秘密信息。CA私钥激活数据的销毁是在国富安安全管理人员和密钥管理人员的监督下进行。

当订户证书私钥的激活数据不需要时应该销毁，订户应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的在纸页必须粉碎。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

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。

6.5.2 计算机安全评估

国富安 CA系统通过国家密码管理局的安全性审查。

6.6 生命周期技术控制

6.6.1 系统开发控制

系统开发采用先进的安全控制理念，同时应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。系统设计和开发运用软件工程的方法，做到系统的模块化

和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

6.6.2 安全管理控制

① 证书服务体系中的配置，以及任何修改和升级，会记录在案，并予以控制。

② 国富安 CA采用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。

6.6.3 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证的。完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

① 国富安 CA采用多级防火墙实施访问控制。

② 只有国富安 CA员工能够进入 CA系统服务器、资源库、操作中心等设备或系统，所有有权进入系统的员工必须有合法的安全令牌，并通过密码验证。

6.8 时间戳

国富安 CA的系统日志和记录等均可以根据标准时间源的时间戳进行记录，作为审计用。

7 证书、证书吊销列表和在线证书状态协议

7.1 证书

7.1.1 证书版本号

X.509v3 证书。

7.1.2 证书扩展项

针对特别的用户，国富安 CA签发的证书有可能包含私有扩展项，不能识别私有扩展项的应用、依赖方可以忽略该扩展项。

① 密钥用法（Key Usage）

该扩展项指定证书密钥对的用法，不同证书该扩展项不同。这个扩展项的 criticality 域通常设置为 FALSE。

② 证书策略扩展项（Certificate Policies）

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

③ 主题备用名（subjectAltName）

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

④ 基本限制扩展项（BasicConstraints）

国富安 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。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。

⑤ CRL 的分发点（cRLDistributionPoints）

国富安 CA签发的证书中包含 CRL 的分发点扩展项，依赖方可根据该扩展项提供地址和协议下载 CRL。此扩展项的 criticality 项应设为 FALSE。

⑥ 签发 CA 密钥标识符

国富安 CA最终订户证书及中级 CA 证书中有签发 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 SHA-1 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 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。

⑧ 名称限制

国富安CA签发的其他证书中的通用名不能使用假名、伪名。

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		SHA256RSA
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2048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		SHA256RSA
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 2048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		SHA256RSA
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 2048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

7.1.4 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

sha-1WithRSAEncryption	{ 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。

7.2.1 版本号

X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项

国富安 CA每天一次更新及公布如下的证书吊销列表（CRL），吊销列表上载有根据本规则吊销的证书。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		SHA256RSA
发行者		CN=ROOT CERTIFICATE FOR GFA TRUST NETWORK OU=GFA TRUST NETWORK O=CIECC L=BETDA S=BEIJING 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

7.3.1 版本号

使用OCSP版本（OCSP V2.0）。

7.3.2 OCSP 基本域

① 状态：响应状态，包括成功、请求格式错误、内部错误、稍候重试、请求没有签名和请求签名证书无授权，当状态为成功时必须包括以下各项。

② 版本 V1

③ 签名算法：签发 OCSP 的算法。使用 SHA256WithRSAEncryption (OID:1.2.840.113549.1.1.5)算法签名。

④ 颁发者：签发 OCSP 的实体。签发者公钥的 SHA256 数据摘要值和证书甄别名。

⑤ 产生时间： OCSP 响应的产生时间。

⑥ 证书状态列表：包括请求中所查询的证书状态列表。每个证书状态包括证书标识、证书状态以及证书吊销信息。

⑦ 证书标识：包括数据摘要算法 (SHA256, OID: 1.3.14.3.2.26)、证书甄别名数据摘要值、证书公钥数据摘要值和证书序列号。

⑧ 证书状态：证书的最新状态，包括有效、吊销和未知。

⑨ 证书吊销信息：当返回证书状态为吊销时包含吊销时间和吊销原因。

7.3.3 OCSP 扩展域

不使用OCSP扩展项。

8 认证机构审计和其他评估

8.1 评估的频率或情形

国富安 CA 应当至少每 12 个月按照 CPS 中规定的操作文档对 CA、RA 和受理点进行一次审计。

8.2 评估者的资质

执行审计的审计师必须是具有计算机安全专门技术知识的计算机安全专家（例如：认证信息系统审计师资格）。

8.3 评估者与被评估者之间的关系

审计师和 CA 必须有关于执行审计的契约关系，并且审计师在组织上和 CA 严格区分，以做出公正、独立的评估。

8.4 评估内容

采用国家相应审计标准，审计 CA RA及受理点的运作是否和本 CPS的规定相符合。

8.5 对问题与不足采取的措施

如果审计报告显示任何实质性的不符合要求时， CA RA 受理点必须制定改善计划。如果 CA RA 受理点没有针对审计报告采取适当的改进措施，国富安 CA必须有权利要求相关 CA RA 受理点暂时停止对公众提供服务。

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

除了一致性审计外，国富安 CA将定期进行内部审计评估，审计评估的内容与外部审计一致。

9 法律责任和其他业务条款

9.1 费用

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。

9.1.2 证书查询费用

国富安 CA 不对证书访问收费。

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。没有国富安 CA 书面授权，任何实体不得将国富安 CA 提供的 CRL 和 OCSP 等服务数据用作任何商业用途。

9.1.4 其他服务费用

任何人可以免费访问国富安 CA 在其资源库中公布的 CP 或 CPS。但是除了简单阅读之外的其他行为，诸如分发、修改、编译等行为，必须取的国富安 CA 的书面授权，国富安 CA 可对此类行为收取一定费用。

9.1.5 退款策略

除非由于国富安 CA 的原因，造成订户无法履行合同或证书无法使用，否则国富安 CA 订户数字证书一经申请，不办理退证、退款手续。

9.2 财务责任

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。

9.2.2 其他资产

无

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

国富安 CA 有专门的信息保密制度，保护自身和客户的敏感信息、商业秘密。

9.3.1 保密信息范围

① 证书申请记录，无论是否批准；

② 没有用户的事先同意，凡是涉及隐私、机密、以及本 CPS 确认的、国家相关法律规定的其它信息不能被披露；

③ 除了国家相关法律规定或法庭判决外，没有用户的书面同意，收集的信息不得出卖、租用、或披露给任何第三方；

④ 数字签名私钥必须保密。CA 保管的所有私钥的管理密钥必须严格保密。在任何情况下，私钥都不能以不被加密的形式出现在加密模块之外；

⑤ 灾难恢复计划；

⑥ 交易记录（包括所有记录和审计跟踪记录）；

⑦ 所有储存在 CA 和 RA 本地的信息必须被谨慎对待，并且对那些需要知道这些信息以执行管理职责的人的访问必须严格控制；

⑧ 审计信息将被谨慎对待，并且不能因为任何目的披露给任何人。除了为了审计、强制报告的目的、或依据法律的相关规定。

9.3.2 不属于保密的信息

① 证书和 CRL，以及在公开目录中公开的个人和机构信息，不被当作保密信息。

② 除本 CPS § 93.1 中规定的保密信息外的所有在网站或目录服务器中公布的信息均被视作不保密的信息。

本部分的规定必须遵守适用中国相关法律。

9.3.3 保护保密信息的责任

国富安CA不但有各种严格的管理制定、流程和技术手段保护自身的商业秘密，并且把保护客户信息作为自己应尽的义务。国富安CA的每个员工到要接受信息保密方面的培训。

9.4 个人隐私保密

9.4.1 隐私保密方案

国富安CA有客户隐私计划保护证书订户的个人信息。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括，最终订户注册申请证书中提交的信息，包括联系电话、地址等；个人与国富安 CA、注册机构签订的协议。

9.4.3 不被视为隐私的信息

不被认为是隐私信息包括，要出现在证书中的信息，证书及证书状态。

9.4.4 保护隐私的责任

除非执法、司法方面的强制需要，国富安 CA 及其注册机构在没有获得客户授权的情况下，不会将客户隐私信息透露给第三方。

9.4.5 使用隐私信息的告知与同意

国富安CA或其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，用户同意和授权信息以下列方式之一传送给国富安CA或其注册机构：

① 有手写签名的同意和授权文件，并将文件邮寄、快递到国富安CA或其注册机构，

② 将手写签名的同意和授权文件传真到国富安CA，

③ 以签名电子邮件的形式同意并授权。

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，国富安 CA及其注册机构有可能需要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，即使出现这种情形，国富安 CA及其注册机构也将尽可能地保护客户隐私信息。

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

国富安 CA 对网站及目录服务器上公布的所有资料享有知识产权，包括：

① CP 及 CPS；

② 证书用户协议；

③ 依赖方协议；

④ 证书；

⑤ CRL 中的信息；

⑥ 证书的状态信息。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

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。

根 CA主要责任包含：

① 制定 CA 总体政策的责任。作为根 CA，是责任审批的授权者，制定 CA 的总

体政策策略及执行这些策略的业务规则。

② 管理运营 CA 的责任。运营 CA 的管理包括审批其建设申请，包括资信审查、物理环境审查以及运营政策的审查，如果审批通过则发放运营 CA 证书。

③ 负责与其他国内外 CA 之间的交叉互信。当国富安 CA 需要与其他国内外 CA 互连互通时候，由根 CA 决定采用何种技术手段和措施及策略进行交叉论证。如果对方 CA 申请得到本 CA 的承认，则负责审核对方 CA 的证书策略、运营业务规则等等，评估其风险，如果审查通过则为其签发交叉证书。

④ 管理证书和吊销列表的责任。管理其签发的证书，包括根证书、运营 CA 证书的交叉认证证书和吊销证书列表。

以下情况根 CA不承担责任：

① 除根 CA 本身的钥被攻破以外，不承担由运营 CA 和交叉认证的其他 CA 私钥被攻破、泄露、损坏对用户造成的损失赔偿的责任。

② 不承担由于运营 CA 和交叉认证 CA 将证书用于本 CPS 之外用途造成用户损失赔偿。

③ 不承担运营 CA 和交叉认证 CA 因侵犯他人的专利、商标、著作权、商业秘密和其他知识产权而造成的用户赔偿和责任。

运营 CA有如下责任：

① 管理 RA 的责任。运营 CA 有决定下级 RA 运做模式的权利，并对 RA 的权限进行管理。

② 接受用户证书申请的责任。

③ 证书的签发与制作的责任。

④ 管理证书及吊销列表的责任。

⑤ 如对其业务规则进行调整，应提前通知 RA 并告知其更改的责任。

运营 CA不承担责任的情况：

① 除运营 CA 本身私钥被攻破或泄露对订户造成损害，不承担其他订户私钥泄露、破坏，或因其使用被取消、证书过期造成的损害赔偿。

② 不承担因国家强制要求使用的算法被攻破而造成的损害赔偿，除国富安 CA

全资拥有的 RA 和 LA 外，对其他 RA、LA 因没有按照其业务规则进行操作而造成订户损害进行赔偿，但有义务协助订户进行索赔的责任。

③ 如果证书内容与本 CPS 不符，将不为证书中表述的信息负责；

④ 如果订户证书用于本 CPS 规定之外的用途，则不承担由此引起的责任。

⑤ 若证书主体提交并列入了证书内的信息侵害了他人的专利、商标、著作权、商业秘密和其他知识产权，运营 CA 不承担其责任。

根 CA的义务有：

① 有义务定期对证书政策进行审计和评估，同时定时征求各种反馈意见，根据这些意见进行管理和完善。

② 有义务根据现行政策对运营 CA 申请进行审查或复查，并根据其结果决定运营 CA 是否继续运营。

③ 有义务提供交叉认证证书的查询手段和方法，有义务对其他需要交叉认证 CA 进行审查，或提供本 CA 与其他 CA 进行交叉认证所需的有关政策、操作管理规范和安全措施的文档及其他相关资料，并申请对方的交叉认证证书。

④ 有义务发布其签发的证书，以便用户查询；也必须根据其政策发布证书吊销列表。

⑤ 有义务在发生纠纷和争议时提供相关的材料。

运营 CA的义务：

① 有义务遵守国富安 CA CPS 中规定的管理要求、运营要求和系统安全设备要求，制定具体的步骤和程序来实施这些要求，并制定相应操作规程。

② 有义务维持国富安 CA 系统的正常运行，并为下级 RA、LA 提供及时、安全、可靠的服务。

③ 有义务为下级 RA、LA 提供与国富安 CA 有关产品和服务的技术支持、业务建议和培训服务。

④ 有义务提供相应的手段让订户填写证书申请表、更新和吊销表。

⑤ 有义务支持多种证书发放方式，业务受理点支持多种证书存储介质。

⑥ 有义务维护所发的证书及相关信息，并负责生成、维护和发放证书吊销列表。

国富安 CA的证书订户在申请证书前应同意国富安 CA的订户协议，国富安 CA和订户

及依赖方的责任与义务由其相应的订户协议和依赖方协议约束。

9.6.2 注册机构的陈述与担保

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 系统有如下责任：

① 自身密钥的管理，承担因 RA 自身私钥泄露导致用户损失的赔偿责任。
② 审批、设置 LA，并对 LA 进行管理和审计的责任，并承担由此带来的损失赔偿。
③ 承担在 CPS 规定之外使用 RA 内部管理员证书所造成的损失的责任；
④ 使用国富安 CA 规定的协议和通信标准来与国富安 CA 进行通信的责任。
⑤ 对国富安 CA 提供的国富安 CA 的专用软件有使用权，并有保密的责任。
⑥ RA 必须遵守所有的登记程序和安全保障措施，这些程序和保障措施由国富安 CA 决定。
⑦ RA 必须赔偿 CA 因 RA 没有遵守本 CPS 和与发证 CA 相关的其他的协议而发生的损失和索赔，保证 CA 不因此受到损害。

RA有如下义务：

① 有义务保障向运营 CA 提供正确的用户信息。
② 有义务承担因其提供的信息侵犯他人的权利而造成的后果的责任。
③ 有义务保障 LA 的合法性，接受并发送 LA 的各种请求，并及时提供其服务。

LA有如下义务：

① LA 有义务受理用户申请并录入用户申请信息，并保证其审核通过的用户信息真实、可靠，有义务对申请不通过的用户说明理由和原因。
② LA 有义务为审核通过的用户下载证书，有义务应用户的要求更新或吊销证书，所有这些操作必须遵守国富安 CA CPS。
③ LA 可以根据自身的特点，在遵守国富安 CA CPS 前提下制定具体的证书申请流程，在用户身份核实中可以酌情另外增加身份鉴别方法。
④ LA 必须接受上级 RA 的指导和监督，并对上级 RA 的评估作出整改。

⑤ 有义务承担因其提供的信息侵犯他人的权利而造成的后果的责任。

⑥ 按照对国富安 CA 的有关规定管理用户信息（包括纸面信息和电子信息），并承担其相应的责任。

⑦ LA 必须赔偿 RA 或 CA 因其没有遵守本 CPS 或相关的其他的协议而发生的损失和索赔，保证 CA、RA 不因此受到损害。

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，就被视为向国富安 CA、注册机构及信赖证书的有关当事人作出以下承诺：

① 同意接受订户协议，履行该协议规定应承担的义务确保在申请时所做的陈述、提供的信息准确无误，并承担不真实带来的责任。

② 订户在证书申请后，有责任将证书申请时的信息资料变更或授权人变更等等立即通知国富安 CA 或其受理机构。

③ 对于密钥对在用户端产生的订户，必须保障密钥对产生的系统是可信的，采取合理的措施保障密钥的安全，防止任何的密钥遗失、泄露和防止非授权使用。

④ 在用户接受到以用户名义申请的证书签发通知时，应当检查证书，以保证证书中所包含的用户的所有信息都是真实的，按照本 CPS 的相关规定以决定接受或不接受该证书。

⑤ 熟悉本 CPS的内容，了解证书的使用目的，保障按照本 CPS 规定的方式和用途使用证书和相应密钥对。

⑥ 当私钥面临任何事实上的丢失、泄漏、或其他危及私钥安全的情况时，应当迅速通知 CA(或 RA、受理点)撤销证书。

⑦ 订户在明知国富安 CA 根据其业务规则可能吊销证书的情况下，或订户已经作出吊销证书而国富安 CA 已经受理的情况下，均不得再使用该证书，并有通知仍有待完成的任何交易的依赖方的责任。

9.6.4 依赖方的陈述与担保

依赖方在信任和使用任何国富安 CA 证书的时候必须保证承担下列义务：

① 依赖方熟悉本 CPS的内容，了解证书的使用目的，依赖方必须保证证书的使用符合本 CPS的规定；

② 依赖方在信赖国富安 CA证书用户的证书前执行证书的路径验证和证书的有效性验证。

③ 依赖方在信赖国富安 CA证书用户的证书前必须检查最新的 CRL，或通过在线查询协议（Online Certificate Status Checking Protocol）检查证书的状态，只有确认该证书没有被作废时该证书才有效。

9.6.5 其他参与者的陈述与担保

对于为国富安 CA承担第三方身份验证的机构或组织，必须作出如下承诺：

① 是合法的、获得授权的组织机构；

② 在其管理和控制的范围内提供的数据是真实的、准确的；

③ 能够承担由此带来的责任赔偿。

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，为了表达明确，这些事件包括：罢工或其它劳动纠纷、暴动、国内骚动、供应商故意或无意的行为、不可抗力、战争、火灾、爆炸、地震、洪水或其它大灾难。

9.8 有限责任

在任何情况下，在国富安 CA 的信任链中，CA、RA 及受理点对所有当事人的关于每份证书最高赔偿限额如下所示：

证书类别	证书应用领域	赔付的额度说明

个人证书	符合《电子签名法》适用的电子签名所有应用领域	对所有当事人的关于每份证书最高赔偿限额总计不超过人民币 5000 元 (当事人包括但不限于证书用户、 证书申请者、接受或依赖方)；
机构证书	符合《电子签名法》适用的电子签名所有应用领域	对所有当事人的关于每份证书最高赔偿限额总计不超过人民币 20,000 元 (当事人包括但不限于证书用户、 证书申请者、接受或依赖方)；
设备证书	符合《电子签名法》适用的电子签名所有应用领域	对所有当事人的关于每份证书最高赔偿限额总计不超过人民币 30,000 元(当事人包括但不限于证书用户、 证书申请者、接受或依赖方)；

对于任何实体因使用或信任国富安 CA 所签发、管理、使用、撤销或过期的证书，而造成利益损失与损害赔偿，上述责任上限均适用，此类利益损失或损害包括但不局限于任何人所造成的直接的、间接的、特别的、必然的、偶然的、惩罚性的损害，前述的实体包括但不局限于用户、申请者、接受者或依赖方。此责任限制亦适用于因合同、侵权、或任何其他形式的赔偿请求所产生的责任。不论该证书的交易数量、数字签名的次数、或赔偿请求数量，该证书所适用的责任上限均无不同。如果赔偿金额超过此责任上限，除经过有司法管辖权的法院另有规定外，则应该以规定的责任上限支付最先的赔偿请求，以达成争议的最终解决。在任何情况下，对于每一证书而言，不论赔偿请求者之间如何分配责任上限的金额，国富安 CA 均无义务支付超过该证书责任上限的金额。

国富安 CA 在与订户和依赖方签定的协议中，对于因订户或依赖方的原因造成的损害不具有赔偿义务。

9.9 赔偿

对于由如下原因造成的订户或依赖方损失，国富安 CA 对订户或依赖方进行赔偿。

① 国富安 CA 在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发；

② 由于国富安 CA 的原因，使得证书中出现了错误信息；

③ 由于国富安 CA 私钥的泄漏。

在如下情况，订户对自身原因造成的国富安 CA、依赖方损失承担责任。

① 订户在证书申请中对事实的虚假或错误描述；

② 在证书申请中订户没有披露重要的事实，如果这种错误表述或遗漏是因为粗

心或故意欺骗任何一方；

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

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

在如下情况，依赖方对自身原因造成的国富安 CA 损失承担责任。

① 依赖方没有执行依赖方职责义务；

② 依赖方在不合理的环境下信赖一个证书；

③ 而依赖方没有检查证书状态确定证书是否过期或吊销。

9.10 有效期限与终止

9.10.1 有效期限

本《电子认证业务规则》自发布之日起正式生效。本《电子认证业务规则》中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的《电子认证业务规则》正式发布生效时，旧版本的《电子认证业务规则》自动终止。

当国富安 CA中止业务时，国富安 CA CPS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，对应的依赖方协议终止。

9.10.3 效力的终止与保留

《电子认证业务规则》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 对参与者的个别通告与沟通

国富安 CA 及其注册机构在必要的情况下，如在主动吊销订户证书、发现订户将证书用于规定外用途及订户其它违反订户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

9.12 修订

9.12.1 修订程序

在国富安 CA的《电子认证业务规则》作出任何修订之前，国富安 CA安全策略委员会将对提出的修订建议进行研究，作出变更的决定，在征求国富安 CA法律顾问有关法律上的意见后，形成决议；

修订后的《电子认证业务规则》在国富安 CA网站上重新发布后生效；

国富安 CA对国富安 CA《电子认证业务规则》作严格的版本控制；

适用《电子认证业务规则》时，以最新修订的版本为准。

9.12.2 通知机制和期限

本《电子认证业务规则》在国富安 CA的网站（http://www.gfapki.com.cn)上发布。

版本更新时，最新版本的《电子认证业务规则》在国富安 CA的网站发布，对具体个人不做另行通知。

9.12.3 必须修改业务规则的情形

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《电子认证业务规则》。

9.13 争议处理

涉及《电子认证业务规则》任一方面的或涉及由 CA 颁发的证书方面的争议，在采取任何解决途径之前，争议方应通知国富安 CA及其他当事人。

当事人可首先采用谈判的方式解决争议，如果争议在上述通知 10 天后未被解决，当事人可以将争议提交给国富安 CA，要求由国富安 CA 的专家小组调解，专家小组可以收取适当费用。认证中心将召集由 3名安全认证专家组成的专家小组，以协助解决争议为目的，搜集相关事实。争议提出方必须向所有其他当事人提供提交材料的复印件。在争议提交给专家小组后 7天内，未提出争议的当事人可向专家小组提供相关信息。专家小组应在接到争议材料后 3周内（除非当事人同意将此段时限延长至一特定时段）完成并向当事人传达其建议。专家小组的建议对当事人无任何约束力，仅供当事人参考。

当国富安 CA 其注册机构（包括 RA和 LA)、订户和依赖方之间的争议通过上述协商解决不了的，可通过法律解决。

9.14 管辖法律

本《电子认证业务规则》在各方面服从中国法律和法规的管制和解释，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

无论在任何情况下，本《电子认证业务规则》的执行、解释、翻译和有效性均适用中华人民共和国的法律和国家信息安全主管部门的要求。

9.16 一般条款

9.16.1 完整协议

本《电子认证业务规则》将替代先前的、与主题相关的书面或口头解释，本协议与订户协议、依赖方协议及其他补充协议构成了国富安 CA信任域中的完整协议。

9.16.2 分割性

当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。

9.16.3 强制执行

免除一方对合同某一项的违反应该承担的责任，不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。

9.16.4 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。不可抗力既可以是自然现象或者自然灾害，如地震、火山爆发、滑坡、泥石流、雪崩、洪水、海啸、台风等自然现象；也可以是社会现象、社会异常事件或者政府行为，如合同订立后政府颁发新的政策、法律和行政法规，致使合同无法履行，再如战争、罢工、骚乱等社会异常事件。

9.17 其他条款

本《电子认证业务规则》的解释权归北京国富安电子商务安全认证有限公司。