国汽（北京）智能网联汽车研究院有限公司证书策略

（生效日期：2020 年 12 月）

国汽（北京）智能网联汽车研究院有限公司

版本控制表

版本	修改状态	修改说明	修改人	审核人/批准人	生效期
1.0	初版发行			安委会	2020 年 12 月

1. 目录

1. 引言

1.1 概述

1.1.1 公司简介

国汽（北京）智能网联汽车研究院有限公司（以下简称“国汽智联”），由中国汽车工程学会、中国汽车工业协会及中国智能网联汽车产业创新联盟共同发起筹建，成立于 2018 年 3 月 19 日，注册地址为北京市经济技术开发区，注册资本 11 亿元。22 家股东单位均为整车、零部件、信息通信等领域的领军企业和科研机构。

2019 年 5 月 30 日，国家工业和信息化部正式批复同意由国汽（北京）智能网联汽车研究院有限公司组建国家智能网联汽车创新中心。

国汽智联致力于：聚集国内外高端专业人才，突破关键共性技术，提升创新能力，培育一批在智能网联汽车领域具有国际竞争力的企业，持续高效引领和支撑行业发展，提升我国智能网联汽车及相关产业在全球价值链中的地位，努力把国汽智联建设成为具有世界级影响力的研发平台。目前汽车行业的电子认证系统局限于内部使用，不同汽车企业的电子认证系统尚未实现相互认证，特别是在车联网通信中不能实现不同车企的车辆身份互认。因此，国汽智联建立车联网电子认证平台，为汽车制造商、车联网应用服务平台、车联网通信提供身份认证及安全防护服务，系统全面地保障车联网的安全。

1.1.2 证书策略

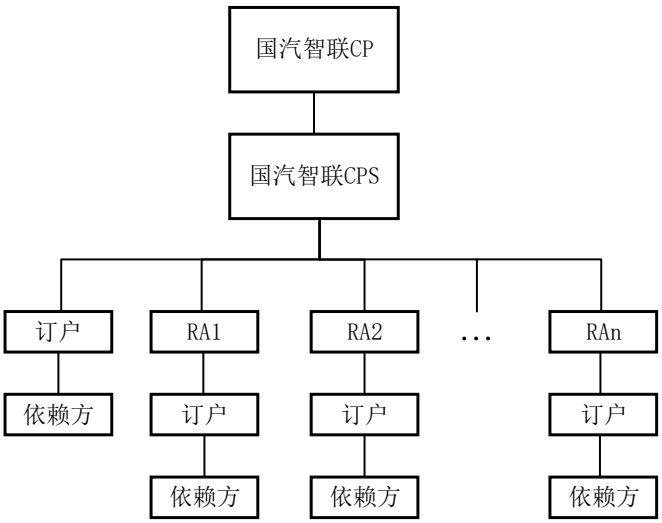
本文件描述的国汽智联的证书策略（CP），是国汽智联数字证书服务的策略声明，适用于所有由国汽智联签发和管理的数字证书及相关参与主体。为批准、签发、管理、使用、更新、吊销证书和相关的可信服务定制业务，法律和技术上的要求和规范。这些要求和规范保护国汽智联数字证书服务的安全性和完整性，包含一整套在国汽智联范围内一致适用的单一规则集，因此在整个国汽智联架构内能够提供同样的信任担保。本 CP 并不是国汽智联和各参与方之间的法律性协议，国汽智联和各参与方之间的权利义务依靠他们之间签署的各类协议构成。

本 CP 满足《互联网 X.509 公开密钥基础设施证书策略和证书业务框架》（Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework），即由互联网工程工作组 (The Internet Engineering Task Force, IETF) 制定的 RFC 3647 标准的结构和内容要求，同时也满足《GB26855-2011-T 信息安全技术公钥基础设施证书策略与认证业务声明框架》的结构和内容要求，并根据中国的法律法律和国汽智联的运营要求进行适当的改变。

国汽智联作为一个证书服务机构（CA），在本 CP 的约束下生成根证书和子 CA 证书，签发订户证书。基于不同的类型和应用范围，作为证书持有人的订户可以使用证书进行网络站点安全保护、代码签名、邮件签名、文档签名、身份认证等不同的应用。依赖方依照本 CP 中关于依赖方的义务要求，决定是否信任一张证书。国汽智联的电子认证业务规则（CPS）接 受本 CP 的约束，详细阐述了国汽智联作为电子认证服务机构提供的证书、如何提供证书以及相应的管理、操作和保障措施。所有国汽智联证书的订户及依赖方必须参照本 CP 及相关 CPS 的规定，决定对证书的使用和信任。

1.1.3 国汽智联架构

本 CP 是国汽智联最高的策略，国汽智联的证书服务机构（CA）按照本 CP 制定 CPS，RA 按照 本 CP 及相关 CPS 进行证书服务申请鉴别，订户、依赖方及其他相关实体按照本 CP 及相关 CPS 决定对证书的使用、信任并履行相关的义务。国汽智联包含了根 CA、子 CA、各相关注册机构、服务受理点，这些实体都是国汽智联认证体系内不同层次的服务主体。国汽智联认证体系所有和证书相关的服务和管理，都完整、正确、全面的贯彻和实施本 CP 以及相应 CPS 的要求。


国汽智联CP
国汽智联CPS
订户
RA1
RA2
...
RAn
依赖方
订户
订户
订户
依赖方
依赖方
依赖方

1.2 文档名称与标识

本文档的名称为《国汽（北京）智能网联研究院有限公司证书策略》。本CP中为每类证书的证书策略项没有分配唯一的对象标识符。

1.3 PKI 参与者

1.3.1 电子认证服务机构（CA）

国汽智联是根据《电子签名法》及《电子认证服务管理办法》规定依法设立的电子认证服务机构，是网上安全电子交易中具有权威性和公正性的可信赖的第三方机构。国汽智联为网上业务的各参与方签发标识其身份的数字证书，并对数字证书进行更新、注销等一系列管理。国汽智联设立安全管理委员会、安全管理小组等机构，进行相关管理活动。国汽智联下设服务中心、及业务受理点（RA），进行业务管理及实施活动。

1.3.2 注册机构（RA）

国汽智联的注册机构（以下简称“RA”），又称为业务受理点，是国汽智联设立或授权委托设立的数字证书业务受理机构。其业务范围包括：面向用户受理数字证书业务和销售数字证书产品业务。其中受理数字证书业务是指受理用户的证书注册申请、审核用户身份、批准证书申请、证书制作、发放证书、接受和处理证书更新、证书注销、密钥恢复以及其他需要直接面向用户的业务，其中密钥恢复业务仅由指定受理点开展。销售数字证书产品业务是指销售国汽智联的各类数字证书以及数字证书存储介质。

RA按照国汽智联制定的CP及相关业务受理点管理程序运营数字证书代理业务。在代理数字证书业务的运营活动中，应按照国汽智联的规定，执行符合政策规定的资费标准，向用户提供统一标准的服务。

国汽智联各RA点挂牌的名称为“数字证书业务受理点”。

1.3.3 订户

订户也称为证书持有者，也称为用户。是指拥有电子认证服务机构签发的有效证书的实体。包括从国汽智联处接受证书的任何个人或合法设立的组织。订户符合以下情况：

- 在接受的证书中指明或识别为证书接受者；
- 已接受该证书并遵守本 CPS 和相关协议；
- 拥有与接受的证书内公钥所对应的私钥。

1.3.4 依赖方

依赖方包括行为上依赖于国汽智联用户的证书及其数字签名的一方，与订户发生业务往来的个人或组织。依赖方可以是、也可以不是一个订户。

1.3.5 其他参与者

其他参与者是指为国汽智联的电子认证活动提供相关服务的其他实体。

1.4 证书使用

1.4.1 适合的应用

各个证书代表各自的身份进行使用。所有证书根据其颁发对象的不同，归为以下三种：

- 个人证书
- 机构证书
- 设备证书

国汽智联在开展业务时可能为某种对象的证书作特别的命名。

证书类型	用户性质	举例
个人证书	各级政务部门的工作人员和参与业务的社会公众，用以代表个体的身份。	如某局职员，参加纳税申报的个人。
机构证书	政务机关和参与业务的企事业单位，代表机构身份。	某部委、某局或参加政府招投标业务的投标企业。
设备证书	系统中的服务器或其他设备，用以代表设备身份的	服务器身份证书、SSL 服务器证书、

1.4.2 限制的证书应用

禁止将证书用于违反国家及地方相应法律法规用途。

禁止违反操作规程进行证书应用。

1.5 策略管理

1.5.1 策略文档管理机构

国汽智联 CP 由国汽智联安全管理委员会负责起草、注册、维护和更新，版权由国汽智联完全拥有。

1.5.2 联系人

联系地址：北京经济技术开发区荣华南路 13 号院 7 号楼中航国际广场 H5 办公楼。

邮箱：ca@china-icv.cn 网站：http://www.china-icv.cn

电话：010-57705900

1.5.3 决定 CP 符合策略的机构

本 CP 由国汽智联安全策略委员会批准，包括本 CP 的修订和版本变更。

国汽智联安全策略委员会负责评估国汽智联的 CPS 是否符合本 CP，是批准和决定国汽智联的 CPS 是否与本 CP 相适应的机构。

1.5.4 CP 批准程序

国汽智联将对国汽智联 CP 进行严格的版本控制，由国汽智联安全管理委员会指定专人负责版本控制及发布。

所有 CP 相关公告和通知需获得安全管理委员会批准后，通过国汽智联网站 www.china-icv.cn 进行公布。

根据《电子签名法》及《电子认证服务管理办法》等规定，国汽智联在公布 CP 后向国家工业和信息化部备案。

1.5.5 CP 修订

如果因为标准变化、技术提高，安全机制增强、运营环境的变化和法律法规的要求等对本 CP 进行修改，提交国汽智联安全策略委员会审核。经过该委员会批准后，国汽智联通过官方网站进行公布。

1.6 定义和缩写

1. CA（Certificate Authority）

电子认证服务机构的简称。CA 是网络身份认证的管理机构，是网上安全

电子交易中具有权威性和公正性的可信赖的第三方机构。CA 为电子事务的各参与方签发标识其身份的数字证书，并对数字证书进行更新、注销等一系列管理。

2. RA（Registration Authority）

注册机构的简称。RA 是 CA 认证体系的一个功能组件，负责对数字证书申请进行资格审核，并决定是否同意给该申请者发放数字证书，以及证书更新和注销工作。

3. KMC(Key Management Center)

密钥管理中心的简称。用于产生用户加密证书密钥对，并提供加密密钥对托管服务的管理机构。

4. CPS（Certification Practice Statement）

电子认证业务规则的简称。CPS 详细描述电子认证机构数字证书的发放、注销、更新、管理的规范，是认证体系各机构运营 CA 系统进行实际工作和运行应严格遵守的各种规范的综合，是数字证书管理、数字证书服务、数字证书应用、数字证书分类、数字证书授权和数字证书责任等政策集合。

5. CRL（Certificate Revocation List）

数字证书注销列表的简称。CRL 中记录所有在原定失效日期到达之前被注销的数字证书的序列号，供数字证书使用者在认证对方数字证书时查询使用，由 CA 周期性签发。CRL 通常又被称为数字证书黑名单、数字证书废止列表等。内容通常包含列表签发者、发行日期、下次注销列表的预定签发日期、被注销的数字证书序号，并说明被注销的时间与理由。

6. OCSP (Online Certificate Status Protocol)

在线数字证书状态查询协议的简称，用于支持实时查询数字证书状态。

7. 数字证书 （digital certificate）

数字证书是由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。它是用来标志和证明网络

通信双方身份的数字信息文件，与司机驾照或日常生活中的身份证相似。在网上进行电子商务等活动时，交易双方需要使用数字证书来表明自己的身份，并使用数字证书来进行有关交易操作。

8. 数字签名 （电子签名 digital signature）

采用密码技术对数据进行运算得到的附加在数据上的签名数据，或是对数据所作的密码变换，用以确认数据来源及其完整性，防止被人（例如接收者）进行篡改或伪造。

9.金融网上系统 （financial internet system）

金融网上系统是指通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其用户提供各种金融服务的机构。

10. DTS （ Digital Time Stamp）

数字时间戳服务的简称。用于向用户提供可信的精确时间源，以证明某个特定时间某个行为或者文档确实存在。时间源采用的是国际标准时间 UTC，通过 GPS（全球卫星定位系统）卫星天线接收同步卫星原子钟的精确时间信号。

11. LDAP（Lightweight Directory Access Protocol）

轻量级目录访问协议的简称。LDAP 用于查询、下载数字证书以及数字证书注销列表（CRL）。

12. OID（Object Identifiers）

对象标识符的简称。OID 由国际标准化组织分配和发布，并形成一个层次关系。OID 是一串用点分开的十进制数（例如“1.2.3.4”）。OID 标准的定义来自 ITU-T 推荐 X.208(ASN.1)，企业（和个人）可以从国际标准化组织申请得到一个根对象标识符，并且可使用它分配根节点下的其他对象标识符。

13. PKI(PublicKeyInfrastructure)

公开密钥基础设施的简称。PKI 为支持基于证书的公开密钥算法技术的实现和运作的相关体系、组织、技术、操作和程序的集合。

14. 私钥(Private Key)

是一种不能公开、由持有者秘密保管的数字密钥，用于创建数字签名、解密报文或与相应的公开密钥一起加密机要文件。

15. 公钥(Public Key)

可以公开的数字密钥，用于验证相应的私钥签名的报文，也可以用来加密报文、文件，由相应的私钥解密。

16. SM2 算法

我国自主知识产权的商用密码算法，是 ECC（Elliptic Curve Cryptosystem）算法的一种，基于椭圆曲线离散对数问题，计算复杂度是指数级，求解难度较大，同等安全程度要求下，椭圆曲线密码较其他公钥算法所需密钥长度小很多。

17. URL(UniformResourceLocator)

统一资源位址的简称。URL 是在 Internet 的 www 服务程序上用于指定信息位置的表示方法。

18. X.509

一种由 ITU-T（InternationalTelecommunicationUnion-T：国际电信联盟）所发布的数字证书标准以及对应的验证架构。X.509 v3 则为一种具扩展栏位或可扩展的数字证书。

19. 鉴别

辨别认定证书申请者提交材料真伪的过程。

20. 验证

对证书申请材料和申请者之间的关联性进行确定的活动。

21. 证书主体 （certificate subject）

证书主体是证书公钥对应的实体，它可以是个人、机构、域名等。

22. 订户 （customer）

向 CA 申请证书的实体，包括个人用户和机构订户。

23. 依赖方 （relying party）

使用证书中的数据进行决策的用户或代理。

24. 个人证书 （individual certificate）

以个人用户名义向 CA 申请，用以表示个人身份信息的证书。

25. 机构证书 （organization certificate）

以机构用户名义向 CA 申请，用以表示机构身份信息的证书。

26. 依赖方 （relying party）

使用证书中的数据进行决策的用户或代理。

27. SSL 证书 （SSL（Secure Socket Layer) certificate）

SSL 服务器上需要配置的证书，包含服务器域名或 IP 地址信息，用于对服务器进行身份认证，并在服务器端与用户端之间建立 SSL（Secure Socket Layer，安全套接层)加密通道，对传送的数据进行加密，并确保数据在传输过程中不会被篡改。

28. 文件证书 （软证书 soft certificate）

指证书及对应私钥以文件形式存储在计算机文件系统中的证书，通常相对于证书及对应私钥保存在智能密码钥匙硬件中的证书而言（又称软证书）。

29. 智能密码钥匙 usb key

智能密码钥匙是一种内置 PKI 密码算法智能芯片、可以安全存储证书私钥和证书、并能进行签名和签名验证所需密码运算功能的硬件设备。

30. 证书更新 （certificate renewal）

证书更新是指在证书所载信息不变的情况下，延长证书的有效期。

31. 证书撤销 （certificate revocation）

证书撤销是指将用户的证书标记为 CA 永远不再信任的状态，并放置于证书撤销列表中供依赖方查询。

32. 证书冻结 （certificate suspension）

证书冻结是指将用户的证书标记为 CA 暂时不信任的状态，并放置于证书

撤销列表中供依赖方查询。

33. 证书解冻 （certificate dissuspension）

证书解冻是指将已经冻结的证书标记为CA重新信任的状态，并从证书撤销列表中删除其冻结信息供依赖方查询。

34. 证书策略 （certificate policy）

一套指定的规则集，用以指明证书对一个特定团体和（或）具有相同安全需求的应用类型的适用性；或用以指明证书对于具有相同安全需求的某类应用的适用性。

35. 密钥更新 （certificate rekey）

密钥更新是指在不改变证书中用户的其它任何信息的情况下，更换密钥对为用户签发一张新证书。

2.发布与信息库责任

2.1 信息库

国汽智联信息库是一个对外公开的信息库，它能够保存、取回证书及与证书有关的信息。国汽智联信息库内容包括但不限于以下内容：证书、CRL，证书状态信息，国汽智联 CP 最新的版本，以及其他由国汽智联不定期发布的信息。国汽智联证书库为信息库的子集，用来存放经国汽智联签发的证书和证书注销列表(CRL)，主要为用户和网络应用提供国汽智联证书查询及验证证书状态服务的信息库。用户可登录国汽智联网站（www.china-icv.cn）查询证书信息或下载证书。国汽智联信息库不会改变任何从发证机构发出的证书和任何证书挂起或注销的通知，而是准确描述上述内容。

国汽智联信息库将及时发布包括证书、CP 修订、证书挂起和注销的通知和其他资料等内容，这些内容保持与 CP 和有关法律法规一致。

除国汽智联授权者外，禁止访问信息库（或其他由 CA 或 RA 维护的数据）中任何被 CP 和/或国汽智联信息库宣布为机密信息的资料。

2.2 认证信息的发布

国汽智联需要发布的信息包括证书策略、电子认证业务规则、和证书使用和服务相关的协议、证书、证书吊销列表、证书在线状态查询等。

国汽智联提供明确的访问位置和方法，通过在线的方式对外发布证书、证书吊销列表和证书在线状态查询，这种信息的发布通常是证书服务的一部分。

此外，在其网站的固定位置 www.china-icv.cn 发布证书策略、认证业务声明、相关协议等。

2.3 发布的时间和频率

《国汽（北京）智能网联汽车研究院有限公司证书策略》自公布之日起的 15 天之后正式生效。

国汽智联在订户证书签发或者注销时，通过目录服务器或官方网站自动将证书和 CRL 发布，发布周期为不大于 24 小时，即在 24 小时内发布最新 CRL；在紧急的情况下，国汽智联可以自行决定证书和 CRL 的发布时间。国汽智联每年发布一次电子认证服务机构的 CA 证书撤销列表（ARL）。

信息库其他内容的发布时间和频率，由国汽智联独立做出决定，这种发布应该是即时的、高效的，并且是符合国家法律的要求的。

2.4 信息库访问控制

国汽智联在其网站上发布与其相关的公众信息。通过设置访问控制和安全审计措施，确保只有授权的国汽智联工作人员才能编写、修改和删除国汽智联在线发布的信息资料。同时国汽智联在必要时可自主选择是否实行信息的权限管理，以确保只有数字证书用户才有权阅读受国汽智联权限控制的信息资料。

对于国汽智联发布的 CP、CRL 和证书信息，证书订户和证书依赖方可以不受限制地进行只读访问。

3.身份标识与鉴别

3.1 命名

3.1.1 命名类型

国汽智联签发的数字证书符合 X.509 标准，分配给证书持有者的主体甄别名，采用 X.500 命名方式。

3.1.2 对命名有意义的要求

订户证书所包含的命名应具有一定的代表性意义，可以确定证书主题中的个人、机构或者设备的身份。

3.1.3 订户的匿名或伪名

订户不能使用匿名、伪名申请证书，证书中也不能使用匿名、伪名。

3.1.4 解释不同命名的规则

依 X.500 甄别名命名规则解释。

3.1.5 命名的唯一性

国汽智联应保证签发给某个订户的证书，其主体甄别名，在国汽智联信任域内是唯一的。当出现相同的名称时，以先申请者优先使用。

3.1.6 商标的识别、鉴别与角色

国汽智联签发的证书的主体甄别名中不包含商标名。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

国汽智联为证书申请者提供电子密匙或其他符合要求的密码设备，用于生成和保存密钥对，保证私钥不被泄露，并将此电子密匙安全地传递到用户手中。

国汽智联也可通过证书请求（如 PKCS #10）中的数字签名来确认证书申请者持有与注册证书对应的私钥。

证书申请者必需依据法律法规获取和使用密码。

3.2.2 机构身份的鉴别

国汽智联通过证书申请者提交申请材料的方式获取证书申请者信息。国汽智联通过查验能证明其机构身份的证件的原件，或通过第三方信息数据或服务，

或电话访问等。国汽智联采用认为恰当的查验方式来确定机构的身份是确实存在的，合法的实体。同时国汽智联也需对经过机构授权办理证书业务的代表的身份进行确认，确定该机构知晓并授权证书申请。

一般需提供以下资料到国汽智联或国汽智联的 RA 进行身份审核及确认：

1．申请表

2．申请机构的如下有效证件的正本或其副本。有效证件的类型如下：

- 组织机构代码证
- 营业执照
- 企业法人营业执照
- 事业机构登记证
- 事业机构法人登记证
- 税务登记证
- 社会团体登记证
- 社会团体法人登记证
- 人民团体登记证
- 人民团体法人登记证
- 政府批文
- 境外机构的有效证件
- 其他有效证件

3．经办人身份证明原件。有效证件的类型如下：

- 身份证
- 户口本
- 护照
- 回乡证
- 军人身份证明
- 授权委托书
- 其他有效证件

国汽智联在认为申请人的身份已经通过其他方式确认，则无需提交任何证件。是否需要提交及提交何种证件，国汽智联将在证书申请表中予以明示。

国汽智联或国汽智联的 RA 的业务受理人员在认为有必要的情况下，采取电话调查、实地考察或其他验证方式（包括第三方平台数据、互联网访问等）鉴定用户身份及其声明的 IP 地址和域名等信息，申请机构有配合业务受理员的调查工作的义务。

3.2.3 个人身份的鉴别

国汽智联对于通过证书申请者提交申请材料的方式获取证书申请者信息。国汽智联通过查验证明其个人身份的原件，或通过第三方信息数据或服务，或电话访问等国汽智联认为恰当的查验方式来确定个人的身份，一般情况下，个人申请者应提供以下资料到国汽智联或其 RA 进行身份审核及确认：

1．申请表。个人若需在证书中标明个人所属机构，其所属机构身份必须通过国汽智联的审核，并且其申请表必须由所属机构盖章。

2．个人身份证明原件。有效证件的类型如下：

- 身份证
- 户口本
- 护照
- 回乡证
- 军人身份证明
- 其他有效证件

3．如果是属于政府部门中的个人，申请人还需提供属于所在组织（所在部门）的证明（包括雇佣关系）。

国汽智联在认为申请人的身份已经通过其他方式确认，则无需提交任何证件。是否需要提交及提交何种证件，国汽智联将在证书申请表中予以明示。

国汽智联或其 RA 的业务受理人员在认为有必要的情况下，采取第三方信息数据或服务鉴定用户身份，申请人有配合业务受理员的调查工作的义务。

3.2.4 没有验证的订户信息

未在前面所列的，对于不影响用户身份追溯的信息，国汽智联一般不予验证。

3.2.5 授权确认

1．当 RA 所属单位必须为依法设立的机构，其身份审核依据本文 3.2.2 的要求进行，并由国汽智联进行实地的考察后可确认其身份。

- RA 的资格由国汽智联根据认证业务管理办法来审查批准，正式获得相应资格后，其运作遵循国汽智联的相关规定。

2．业务受理人员国汽智联的业务受理人员必须是国汽智联及所属 RA 机构的职员。

- 业务受理人员的身份除了必须符合个人证书申请者的条件外，还必须符合国汽智联的相关规定。

3.2.6 互操作准则

国汽智联通过可能存在的国家根 CA 或者通过交叉认证、证书交换中心等，与其他认证中心建立相互认证的关系。如国汽智联与其他 CA 进行了的相互认证，将在国汽智联的网站中公布。

国汽智联在进行相互认证时遵循相关法律法规的规定，如果相关法规未列明的要求则采取对等的方式，以不降低信任管理等级为标准。

3.3 密钥更新请求的标识与鉴别

数字证书用户申请更新数字证书（密钥）时，需要经过身份审核，才能够完成更新的过程。

国汽智联可以采用以下方式之一来对更新证书中的身份进行鉴别：

（1）用原证书提交合法有效的数字签名的更新申请，则身份审核通过，无需再次进行其他形式的身份审核；

（2）等同采用本文 3.2 身份的初始验证方法。

3.3.1 常规密钥更新的标识与鉴别

对于常规情况下的密钥更新，订户可访问国汽智联证书服务网站进行密钥更新申请，系统自动获取订户原证书信息，如甄别名、证书序列号等，形成证书密钥更新申请；国汽智联的证书认证系统将对密钥更新申请进行身份验证。订户也可以到国汽智联的注册机构申请密钥更新，国汽智联注册机构必须验证订户与经办人的有效文件。

密钥更新会造成使用原密钥对加密的文件或数据无法解密，因此，订户在申请密钥更新前，必须确认使用原密钥对加密的文件或者数据已经解密，由此造成的损失，国汽智联将不承担责任。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后不能进行密钥更新。

3.4 吊销请求的标识与鉴别

证书吊销请求可以来自订户，也可以来自国汽智联、注册机构。当国汽智联或者注册机构有充分的理由吊销订户的证书时，有权依法吊销证书，这种情况无须进行鉴证。

国汽智联或者注册机构的证书吊销请求，必须经过其管理机构或者监督机构进行确定才可以进行。如果订户主动请求吊销证书，则按照本文 3.2 节所述进行身份鉴别。如果是司法机关依法提出吊销，CA 或 RA 将直接以司法机关书面的吊销请求文件作为鉴别依据，不在进行其他方式的鉴别。

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

证书申请实体包括个人和具有独立法人资格的组织机构(包括行政机关、事业单位、社会团体和人民团体等)。

4.1.2 注册过程与责任

1. 注册过程

申请者将证书请求发送到 RA，RA 验证该请求，并对其签名，然后将其发送给 CA。

CA 接收到该请求后，验证 RA 的签名，签发订户证书。在整个注册过程中，必须采取措施保证：

- RA 必须对申请信息和申请者的资料进行鉴别；
- 在 RA 向 CA 发送证书请求时，保证传输信息过程安全、保密、完整。

2. 责任

- 国汽智联及注册机构有责任向订户告知数字证书和电子签名的使用条件；
- 国汽智联及注册机构有责任向订户告知服务收费的项目和标准；
- 国汽智联及注册机构有责任向订户告知保存和使用订户信息的权限和责任；
- 国汽智联及注册机构有责任向订户告知国汽智联的责任范围；
- 国汽智联及注册机构有责任向订户告知订户的责任范围；
- 订户负有在其证书申请中提供准确信息的责任；
- 注册机构承担对订户提供的证书申请信息与身份证明材料的一致性检查工作，同时承担相应审核责任。

4.2 证书申请处理

4.2.1 执行识别与鉴别

当国汽智联、注册机构接受到订户的证书申请后，应按本文 3.2 的要求，对订户进行身份识别与鉴别。

4.2.2 证书申请批准和拒绝

国汽智联或其 RA 对已通过身份审核的证书申请，并确认接收到相关费用款项，则给予接受该证书申请，并向国汽智联提交证书签发请求。

任何不能提供足够的身份证明材料，或被国汽智联或其 RA 怀疑提供虚假信息的，或未在约定时限内支付相关费用的，或未满足国汽智联其他申请要求条件的，国汽智联或其 RA 有权拒绝其申请。

4.2.3 处理证书申请的时间

一般情况下，国汽智联处理证书申请的时间不超出 48 小时，或按双方约定的处理时限。

国汽智联允许未能提供足够身份证明材料的申请继续给予补充，这时将相应延长证书申请的处理时间。

4.3 证书签发

4.3.1 证书签发中 RA 和 CA 的行为

在证书的签发过程中 RA 的管理员负责证书申请的审批，并通过操作 RA 系统将签发证书的请求发往 CA 的证书签发系统。RA 发往 CA 的证书签发请求信息须有 RA 的身份鉴别与信息保密措施，并确保请求发到正确的 CA 证书签发系统。

CA 的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，证书签发系统签发订户证书。

4.3.2 CA 和 RA 通知订户证书的签发

国汽智联的证书签发系统签发证书后，将直接或者通过 RA 通知订户证书已被签发，并向订户提供可以获得证书的方式，包括通过面对面、网络下载等方式，或者通过其它与订户约定的方式告知订户如何获得证书。

4.4 证书接受

4.4.1 构成接受证书的行为

根据不同的业务操作流程，以下任何一种情况均视为用户接受数字证书：

1. 经办人在证书领取记录上签字；
2. 用户获取数字证书及其 PIN 码或口令；
3. 用户从网上下载该数字证书；
4. 与用户约定的其他方式。

4.4.2 对证书的发布

订户接受证书后，国汽智联将该订户证书发布到可被公开访问的目录服务系统。

4.4.3 CA 通知其他实体证书的签发

除证书订户外，国汽智联及注册机构不需要通知其他实体证书的签发。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

用户只有接受了数字证书后方能使用证书对应的私钥。用户结合签名证书及加密证书的功能，在允许的应用范围内使用数字证书。用户使用数字证书时必须遵守国家相关法律法规、国汽智联 CPS 和签署的协议。

用户必须确保自己的私钥不被他人窃取。如果用户无法确定其私钥为安全的，请及时向国汽智联申请注销私钥对应的数字证书，以免因此造成损失。

用户必须按密钥的用途来使用相对应的证书，否则不被依赖方认可的责任由用户自行承担。

4.5.2 依赖方公钥和证书的使用

证书依赖方获得对方的数字证书和公钥后，可以通过查看数字证书来了解对方的身份，通过公钥验证对方数字签名的真实性。验证证书的有效性包括以下三个方面：

1. 验证该证书为国汽智联签发；
2. 检查该证书在有效期内；
3. 查验该证书没有被注销。

证书依赖方依据国汽智联的相关保障措施，确定自己对对方数字证书的信

赖程度。

在验证数字签名时，证书依赖方应参照国汽智联 CP，通过查看或判定证书使用目的和密钥的用途来评估决定是否接收用户的行为，对于不符合证书或密钥用途的证书使用，依赖方可以拒绝接收。

4.6 证书更新

4.6.1 证书更新的情形

1.证书将要到期或已到期或国汽智联其他策略要求原因，且密钥对处于安全状态并且策略允许继续使用。

2.用户或其授权代表提出证书的更新申请。

3.国汽智联的策略要求或相关法律法规引致其他更新。

4.6.2 请求证书更新的实体

请求证书更新的实体为证书订户。

4.6.3 处理证书更新请求

处理证书更新请求可以有以下两种方式：

1. 在线更新，只适合于证书未过期且未被注销的情形。即在证书即将过期前，通过国汽智联网站提交更新申请，经过国汽智联证实提交更新申请者拥有对应证书的私钥并收到相关款项后，由国汽智联签发新的证书。用户需在声明的处理时间之后，凭提交更新申请的证书公钥所对应的私钥下载新的证书。
2. 离线更新，适合所有证书更新情形。即用户或其授权代表提交证书更新申请表和身份证明材料，到国汽智联或其 RA 进行证书更新。其身份鉴别方式和处理过程与本文 4.2 的要求手段。

4.6.4 通知订户新证书的签发

同本 CP 4.3.2。

4.6.5 构成接受更新证书的行为

同本 CP 4.4.1。

4.6.6 CA 对更新证书的发布

同本 CP 4.4.2。

4.6.7 CA 通知其他实体证书的签发

同本 CP 4.4.3。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

证书密钥更新是指用户生成一对新密钥并申请为新公钥签发新证书，也就是说更新证书同时也会更新数字证书密钥。

4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体为证书订户。

4.7.3 处理证书密钥更新请求

同本 CP 4.6.3。

4.7.4 通知订户新证书的签发

同本 CP 4.3.2。

4.7.5 构成接受密钥更新证书的行为

同本 CP 4.4.1。

4.7.6 CA 对密钥更新证书的发布

同本 CP 4.4.2。

密钥更新证书应在 24 小时内发布。

4.7.7 CA 通知其他实体证书的签发

同本 CP4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

如果订户提供的注册信息发生改变，必须向国汽智联提出证书变更。如果证书内包含信息的变更可能影响订户权利义务的改变，则订户不能申请证书变更，只能吊销该证书，再重新申请新的证书。证书变更的申请和证书申请所需的流程、条件是一致的。

4.8.2 请求证书变更的实体

请求证书变更的实体为证书订户。

4.8.3 处理证书变更请求

证书变更按照初次申请证书的注册过程进行处理，同本文 3.2。

4.8.4 通知订户新证书的签发

同本 CP 4.3.2。

4.8.5 构成接受变更证书的行为

同本 CP 4.4.1。

4.8.6 CA 对变更证书的发布

同本 CP 4.4.2。

4.8.7 CA 通知其他实体证书的签发

同本 CP 4.4.3。

4.9 证书吊销和挂起

4.9.1 证书吊销的情形

发生下列情形，订户证书必须被吊销：

1. 政务机构的证书用户工作性质发生变化；
2. 政务机构的证书用户受到国家法律制裁；
3. 证书用户提供的信息不真实；
4. 证书用户没有或无法履行有关规定和义务；
5. 国汽智联、国汽智联 RA 或最终证书用户有理由相信或强烈怀疑一个证书用户的私钥安全已经受到损害；
6. 政务机构有理由相信或强烈怀疑其下属雇员的私钥安全已经受到损害；
7. 证书仅用于依赖主导的系统并由依赖方提出注销申请的；
8. 证书密钥泄漏或存储证书的电子密匙丢失；
9. 证书主体名称列明的从属关系改变；
10. 证书主体的变更；
11. 任何与提供证书服务相关的协议到期；
12. 用户或其授权代表提出证书注销申请；

13. 用户违反国汽智联 CP 或签订的相关证书协议；
14. 其他情况。例如因法律或政策等要求国汽智联进行临时或永久性的证书注销措施。

证书的注销既可以是用户提出申请，也可以是国汽智联因为用户的变更事实或违反约定事实而强行注销。

4.9.2 请求证书吊销的实体

以下实体可以请求吊销一个订户证书：

国汽智联或注册机构可以依据本文 4.9.1 要求吊销一个订户证书；

1. 对于个人证书，证书订户可以请求吊销他们自己的个人证书；
2. 对于机构证书，只有机构授权的代表有资格请求吊销已经签发给该机构的证书；
3. 对于设备证书，只有拥有设备的机构授权的代表有资格请求吊销已经签发的 证书；
4. 法院、政府主管部门及其他公权力部门可以依法吊销订户证书。 只有国汽智联可以吊销根证书或者子 CA 证书。

4.9.3 证书吊销请求的处理程序

在发生证书需注销的情形时，用户或其授权代表应及时填写证书注销申请表，并按本文 3.2 的要求携带身份证明材料，到国汽智联或其 RA 进行申请。

国汽智联或其 RA 按本文 3.2 的要求在 24 小时内进行身份审核通过后，在系统中完成证书的注销操作。

当国汽智联或其 RA 强制注销某一证书时，将在完成注销操作后按其登记的联系方式通知用户。

4.9.4 吊销请求的宽限期

在发生需要注销证书的情形时，用户应第一时间通知国汽智联或其 RA，如果用户未能在当天前往国汽智联或其 RA 进行注销登记，则需要通过电话挂失，先完成证书吊销。

4.9.5 CA 处理吊销请求的时限

国汽智联自接到吊销请求到完成吊销之间的间隔期限，不得超过 24 个小时。

4.9.6 依赖方检查证书吊销的要求

依赖方在依赖一个证书前必须查询国汽智联发布的 CRL 确认他们所信任的证书是否被吊销。

4.9.7 CRL 发布频率

国汽智联须定时发布最新的证书吊销列表。对于订户证书，证书吊销列表更新的时间间隔不能超过 24 小时。对于子 CA 证书，至少每 3 个月签发和公布一次，对于根 CA 证书，必须每年公布一次。

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。

4.9.9 在线状态查询的可用性

国汽智联须提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。

4.9.10 在线状态查询要求

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，依赖方在依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，国汽智联可以提供吊销信息的其他发布形式，但这不是必须的。

4.9.12 密钥损害的特别要求

除本文 4.9.1 规定的情形外，当订户或注册机构的证书密钥受到安全损害时，应立即向国汽智联提出证书吊销请求。如果 CA 的密钥（根 CA 或子 CA 密钥）安全被损害或者怀疑被损害，应该在合理的时间内用合式的方式及时通知订户和依赖方。

4.9.13 证书挂起的情形

用户在丢失电子密匙或其他密钥泄露的情况下而来不及到国汽智联或其 RA 进行注销时，可以先进行挂失，将证书挂起。

4.9.14 请求证书挂起的实体

以下实体可以请求挂起一个订户证书：

国汽智联或注册机构可以依据本文 4.9.1 要求挂起一个订户证书；

5. 对于个人证书，证书订户可以请求挂起他们自己的个人证书；
6. 对于机构证书，只有机构授权的代表有资格请求挂起已经签发给该机构的证书；
7. 对于设备证书，只有拥有设备的机构授权的代表有资格请求挂起已经签发的 证书；
8. 法院、政府主管部门及其他公权力部门可以依法挂起订户证书。

4.9.15 挂起请求的程序

所有证书挂起申请要求国汽智联或其 RA 受理人员核对申请人（或来电者）的身份，并确认申请人能正确回答证书申请时所登记的信息。必要时，受理人员可以再次通过已登记的联系方式再次确认。用户在申请办理证书挂起后，应在 72 小时内，按本文 3.2 的身份审核要求到国汽智联或其 RA 完成证书的挂起申请或取消挂起的申请。若用户未在 72 小时内来国汽智联办理挂起手续的，国汽智联将取消该挂失。

4.9.16 挂起的期限限制

国汽智联自接到挂起请求到完成挂起之间的间隔期限，不得超过 24 个小时。

4.10 证书状态服务

4.10.1 操作特征

订户可以通过 CRL、LDAP 目录服务、OCSP 查询证书状态，上述方式的证书状态服务应该对查询请求有合理的响应时间和并发处理能力。

4.10.2 服务可用性

证书状态服务必须保证 7×24 小时可用。

4.10.3 可选特征

无规定。

4.11 订购结束

订户证书出现下列情形时表明订户的订购行为正式结束：

1. 证书在有效期内被注销，并不再更换新的证书；
2. 证书有效期期满后，用户不再进行证书更新或证书密钥更新。与未到期的其他注销用户对比，其证书不会进入 CRL。

4.12 密钥托管与恢复

4.12.1 密钥托管与恢复的策略与行为

国汽智联要求订户必须使用本订户的数字证书载体生成签名密钥对。订户可以委托国汽智联代订户进行生成签名密钥对的有关操作。由于签名私钥遗失所造成的损失由订户自己承担，国汽智联对此不承担责任。

国汽智联颁发的用户证书中，含有签名用途的密钥对由用户生成或由国汽智联提供的电子密匙生成，国汽智联任何所属机构不对该密钥对进行备份；而加密用途的密钥对则由密钥管理中心（以下简称 KMC）产生，并在 KMC 备份托管，国汽智联的密钥管理中心由国家密码管理局进行管理。

4.12.2 会话密钥的封装与恢复的策略与行为

私钥在 KMC 生成后始终以加密的状态存储在密钥库中，且每个私钥由硬件加密设备生成不同的会话密钥进行加密。

对于每次密钥对的申请和恢复，KMC 使用用户或国汽智联提供的电子密匙产生的公钥对所申请（或恢复）的私钥进行加密传送，保持中间任何环节私钥都不会被获取。

5. 认证机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置与建筑

国汽智联机房的选址和建设按照《电子认证基础设施建设要求》避开易发生火灾危险程度高的区域、有害气体来源以及存放腐蚀区域；避开易燃、易爆物品的地方；避开低洼、潮湿、落雷区域和地震频繁的地方；避开强振动源和强噪音源；避开强电磁场的干扰；避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁；避开重盐害地区，将其置于建筑物安全区内。

国汽智联的主机房根据业务功能划分为服务区、核心区、密钥区，各功能区域对应的级别分别为控制区、限制区、敏感区、机密区，安全等级和要求逐级提高，并设置屏蔽室保护机密数据的存储和 CA 签名密钥的使用安全。机房的建设和管理将严格按照国家标准及国汽智联的规定要求执行。

5.1.2 物理访问控制

国汽智联将功能区域按低到高划分为不同的四个安全等级，为公共区、服务区、管理区和核心区，并采用高安全性的监控技术，包括 7×24 小时全天候动态监控的摄像、智能卡和指纹双因素控制、可控权限和时间的门禁系统等监控技术，以及人工监控管理，所有进入高一级的区域，必须首先获得低一级区域的访问权限。

国汽智联设置指纹和智能卡双因素门禁系统来提高访问授权的安全性，并在进入管理区和核心区时采用双人控制策略。

对于非业务管理和系统维护人员，只有经国汽智联安全管理小组授权的工作人员陪同下，并获得国汽智联安全管理小组负责人批准，才可进入相应限制区域活动，并且一切活动皆由摄像监控设备及系统监控软件记录。

5.1.3 电力与空调

国汽智联系统由两路不同高压下的双路电源提供供电，当单路电源发生故障时也能及时自动切换，提供紧急供电，维持系统正常运转；同时备有不间断电源（UPS），避免电压波动和持续 8 小时不间断电力供应。

国汽智联系统的空调系统使用独立的机房精密空调，达到机房温度和湿度的控制要求。

国汽智联对于电源和空调系统的要求，严格按照国家机房管理相关规定，并且定时对系统进行检查，确保其符合设备运行要求。

5.1.4 防水

国汽智联机房采用符合国家标准的防水材料建造。

5.1.5 火灾防护

国汽智联机房设置火灾自动报警系统和灭火系统，火灾报警系统包括火灾自动探测、区域报警器、集中报警器和控制器等，能够对火灾发生区域以声、光、邮件、短信等方式发出报警信号，并能以自动或手动的方式启动灭火设备。同时国汽智联制定了火灾事故专项应急预案，在国汽智联机房受到火灾威胁的时候启动应急预案，确保机房和 CA 系统的安全。

5.1.6 介质存放

国汽智联对存储有各类软件、运营数据和记录的各类介质妥善控制和保管。这些介质都会被存放在结构坚固的储存柜中，并对存放的地点设置安全保护，防止诸如潮湿、磁力、灾害以及人为可能造成的危害和破坏，同时记录介质的使用、库存、维修、销毁事件等。国汽智联对介质的存储地点进行监控，并且只有授权人员才能进入。

5.1.7 废物处理

对于存储或记录有敏感信息的介质，包括纸张、磁盘、磁带、光盘、加密设备等，国汽智联在它们作废前或保存期满后进行销毁。国汽智联制定相关的销毁程序，按信息不可恢复的原则，进行销毁。

5.1.8 异地备份

国汽智联采用异地备份机制，对用于 CA 系统恢复的相关软件、CA 密钥和日常的业务数据等进行异地防灾备份，以便 CA 系统在受到灾难性毁灭时能够启动灾难恢复程序恢复服务。

5.2 程序控制

5.2.1 可信角色

所有涉及 CA 及其 RA 业务操作和维护管理的人员，可能是国汽智联雇员或代理人员、承包人员、顾问等，都属于可信人员。这些可信人员担任的角色包括但不限于以下部分：

1. RA 业务操作员
2. RA 业务管理员
3. RA 超级管理员
4. CA 业务操作员
5. CA 业务管理员
6. CA 超级管理员
7. 系统管理员
8. 密钥管理员
9. 安全管理员
10. 安全审计员
11. 用户服务人员

5.2.2 每项任务需要的人数

国汽智联对于涉及敏感信息的操作任务，要求采取双人控制策略，并为担任该任务角色至少配置 3 人。某些涉及敏感信息的区域的进入也是采取双人控制策略（见本文 5.1.2 ）；核心秘密（如 CA 根密钥）分管者和操作的物理访问控制者由不同的人员担任角色。

5.2.3 每个角色的识别与鉴别

所有担任可信角色的人员需持有经授权的智能门禁识别卡或指纹进入相应的活动区域，或在有进入该区域权限的可信人员的陪同下进入，并持有经授权的智能 IC 卡和证书进入系统进行相应业务的操作和管理。

5.2.4 需要职责分割的角色

以下但不限于以下承担任务的角色必须分离开：

1. 证书业务受理；
2. 证书或 CRL 签发；
3. 系统工程与维护；

4. CA 密钥管理；

5. 安全审计

5.3 人员控制

5.3.1 资格、经历和清白要求

国汽智联在录用担任可信角色的人员之前，除需满足一般的技能和经验要求外，必须按国汽智联可信人员背景调查管理的相关操作指南要求，对录用岗位的可信人员进行对应调查级别的背景调查，符合要求方予录用。可信人员背景调查至少包括以下方面：

1. 学历、学位、职称；

2. 过往的就业情况；

对于较高可信等级的调查可能还包括社会关系、奖惩记录、犯罪记录、社会保险记录、交通违章记录、财务信贷记录等。

5.3.2 背景调查程序

首先先拟录用担任信任角色的人员需同意国汽智联作背景调查。国汽智联采取调阅人事档案、访问过往就读学校和就职单位的人事主管或同事、参阅政府相关部门的个人记录等方式，核实拟录用人所声明和未声明的信息，并作出评估。评估通过后需签署保密协议和就业限制协议，方可录用。

新入职的员工必须经过三个月的观察期，观察期通过后才可独立上岗。

国汽智联不定期进行可信人员背景调查，以便能够持续验证人员的可信程度和工作能力。

5.3.3 培训要求

为员工提供必要的培训，帮助员工胜任其目前的工作并为将来的发展做准备。国汽智联根据需要对员工进行职责、岗位、技术、政策、法律和安全等方面的培训。

国汽智联根据各岗位要求对员工进行相应的培训，包括但不限于：企业文化、规章制度、岗位职责等基本培训；《电子签名法》及《电子认证服务密码管理办法》、《电子认证服务管理办法》等相关法律法规的培训；国汽智联的 CP；国汽智联的安全原则和机制；国汽智联的系统运行、维护、安全；国汽智

联的政策、标准、程序；以及岗位技能、行为方式等其他必要的培训。

5.3.4 再培训的频度和要求

国汽智联定期对员工进行再培训，以不断提高员工业务素质和综合能力。同时根据国汽智联策略调整、系统更新升级或功能增加等情况，对员工进行继续培训，使其更快更好适应新的变化。

5.3.5 工作岗位轮换的频度和次序

国汽智联应依据安全管理策略制定在职人员的工作岗位轮换周期和顺序。

5.3.6 未授权行为的处罚

国汽智联员工所有涉及到业务操作安全的操作均有记录。记录由国汽智联系统管理员或安全审计员审查。当发现员工涉嫌未授权行为、未授予的权力使用和对系统的未授权使用等，一经发现，国汽智联将立即中止该员工进入国汽智联证书认证体系各系统。当事人的证书和操作权限即时冻结或注销，所做的未授权操作将立即被注销失效。同时根据情节严重程度，对当事人作出相应处罚，包括内部处分、辞退、开除等，涉及犯罪的将送司法机关处理。

5.3.7 独立合约人的要求

对于不属于国汽智联机构内部工作人员，但从事国汽智联业务有关工作的如业务分支机构的业务人员、管理人员等独立合约人，国汽智联的统一要求如下：

1. 具有 1 年以上相关业务工作经验；
2. 国汽智联提供统一的岗前培训和工作中的再培训，培训内容包括但不限于国汽智联证书受理规则和电子认证业务规则。

5.3.8 提供给人员的文件

国汽智联提供给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 审计记录程序

5.4.1 记录事件的类型

国汽智联日志记录的事件包括但不限于以下内容：

- 涉及 CA 密钥发生的事件。包括密钥生成、备份、存储、恢复、归档、撤销，密码设备的启用、停用、转移和撤销

- 涉及数字证书发生的事件。包括证书的申请、更新、密钥更新、密钥恢复、挂失/取消挂失、注销，证书业务申请的审核通过或拒绝，证书的签发、接受、CRL 的签发
- 涉及网络安全的事件，包括防火墙、路由器、入侵检测记录的信息，以及被攻击的相应处理记录。
- 其他安全事件。包括各系统的登录、退出，系统的各种配置及其修改，业务处理的成功或失败，系统部件的安装、升级、维修，人员在各区域的访问记录，敏感信息的取阅。

每个事件的记录至少包括以下信息

- 发生的日期和事件
- 事件的内容
- 事件相关的实体
- 事件的标识

5.4.2 处理日志的频度

国汽智联审计人员每月对日志进行一次审查，识别可疑的事件，核实系统和操作人员是否按规定操作，并记录和报告审查的结果。

5.4.3 审计日志的保留期限

对于纸质日志，现场保存至少 1 个月，归档保存期限为 10 年以上，满足本文 5.5.2 要求的档案保存期限。

对于系统自动记录的日志，分在线保存和离线保存，其中在线保存是把日志留在运行的数据库或文件中保存；离线保存则是把数据库或文件中某段时间的日志以文件转储的方式分开保存。在线保存期限为 1 年，离线保存的保存期限为 10 年以上，满足本文 5.5.2 要求的档案保存期限。

5.4.4 审计日志的保护

只有被国汽智联授权的人员才能对日志进行查看和处理，国汽智联对系统的日志设有访问控制权限。

5.4.5 审计日志的备份程序

国汽智联定期对纸质日志实施归档，对电子日志实施备份（周期参见本文 5.4.3）。归档或备份的日志都会被保存在异地，并需要授权才能取阅或恢复。

5.4.6 审计收集系统

国汽智联的审计日志分手工采集和自动采集两种方式。自动采集的主要是电子日志，通过 CA 系统（包括各子系统）、网络设备、各计算平台产生并记录；手工采集的主要是纸质日志，通过操作或出入人员的手工记录产生。

5.4.7 对导致事件主体的通知

国汽智联将依据法律、法规的监管要求，可能对一些恶意行为，如网络和病毒攻击等，通知相关的主管部门，并且国汽智联保留进一步追究责任的权利。

5.4.8 脆弱性评估

审计人员对日志进行日常审计，如发现引起安全事故的事件或可能的隐患，将写入审计报告。国汽智联安全管理小组将每月对审计报告进行评审，确定需要改进的安全措施。同时，国汽智联每年进行一次信息安全的风险评估。

5.5 记录归档

5.5.1 归档记录的类型

国汽智联归档的记录包括本文 5.4 所述的所有日志记录和证书数据库文件、CA 密钥备份、国汽智联发行的证书、CRL、ARL、证书各种业务申请资料等。

5.5.2 归档记录的保留期限

国汽智联的档案保存期限至少为档案相关证书或密钥失效后 10 年。

5.5.3 归档文件的保护

国汽智联的档案保存在设有安全防护和防盗的物理环境中，并由专人管理，防止档案被修改、删除、非法取阅，以及水、火、磁力、虫害等环境的损害。未经管理人员授权，任何人不得接近保存的档案。

5.5.4 归档文件的备份程序

国汽智联每天对 CA 系统产生的电子档案进行备份。每周进行一次全备份并异地保存；对于纸质档案，则依据使用要求，按及时保存原则分别制定归档流程。

5.5.5 记录时间戳要求

对于每一个国汽智联的档案，都给予适当标识，标识的内容包括：编号、归档时间、档案内容、经办人等。

5.5.6 归档收集系统

国汽智联的档案采集系统分为人工处理和自动处理两部分组成。

5.5.7 获得和检验归档信息的程序

国汽智联在取阅档案信息时，需检查存储的档案是否存在删改和破坏现象，对于作了数字签名的档案，则需验证签名。

5.6 密钥变更

国汽智联使用国家根。国家根的密钥更替遵循国家根的有关规定。当发生以下情况时，为保障用户证书使用的安全性和合法性，国汽智联将立即申请进行密钥更替：

- 密钥对已经被泄漏、被窃取、被篡改或者其他原因导致的密钥对安全性无法得到保证；
- 国家相关主管机构对密钥算法、密钥长度等有变更规定。

5.7 损害与灾难恢复

5.7.1 事故和损害处理程序

国汽智联备份所有 CA 运行所需的数据、软件和资料。当发生事故或受到攻击时，用于系统的复原。国汽智联制定相关的安全事件诊断和处理程序，包括业务连续性计划、灾难恢复程序等。

5.7.2 计算机资源、软件和/或数据的损坏

当出现计算资源或软件或数据被破坏，国汽智联启动安全事件的处理程序。评估事件的影响，防止事件扩大，并调查原因，作恢复处理。必要时可能启动 CA 私钥损害处理或灾难恢复程序。

5.7.3 实体私钥损害处理程序

当 CA 私钥被攻破或泄露，国汽智联启动应急事件处理程序，由安全管理小组和相关的专家进行评估，制定行动计划。如果需要注销 CA 证书，会采取

以下措施：

- 立即注销些 CA 证书、由此私钥签发的公钥证书，停止签发新的用户证书
- 立即通报运营监管机构和使用本 CA 服务的相关机构，要求相关机构通知证书用户及依赖方不得再使用原有的证书。
- 发布证书注销状态到证书库；
- 在国汽智联网站或其他通信方式发布关于注销 CA 证书的处理通报；
- 重新签发新的 CA 证书。

5.7.4 灾难后的业务存续能力

当现行 CA 运行系统地点发生灾难，致使 CA 系统不能运作时，国汽智联启动灾难应急处理程序，异地恢复 CA 系统的运行。

国汽智联在异地保存有用于 CA 系统恢复的最小资源和最新数据，并预选两个备用地点用于灾难恢复。灾难发生后，国汽智联会暂停业务受理，但证书及状态查询可以在 24 小时内恢复。

国汽智联每年最少进行一次灾难恢复和业务持续运作的演练，并对演练程序和结果进行记录，所包括的有关主要人员均参与演练。

5.8 CA 或 RA 的终止

因各种原因，在国汽智联计划暂停或终止电子认证业务情况下，国汽智联将按国家相关法律法规的要求进行业务终止操作。

国汽智联将努力寻找适合承接的认证机构，并在暂停或终止业务前六十个工作日前选择业务承接的认证机构，就业务承接有关事项通知有关各方，做出妥善安排，并在暂停或终止认证服务四十五个工作日前向主管部门报告。不能就业务承接事项做出妥善安排的，将在暂停或终止业务前六十个工作日前，向主管部门提出安排其他认证机构承接业务的申请。

无论如何，国汽智联继续按照本 CP 和国家法规的要求来处理档案和证书的续存工作。

6.认证系统技术安全控制

6.1 密钥对的生成与安装

6.1.1 密钥对的生成

国汽智联及其 RA、用户的所有密钥对，都是由国家密码主管部门许可使用的密码设备或模块生成。

国汽智联根密钥对及其下级 CA 密钥对的生成，是在预设定的程序下，由至少 3 名密钥管理员及 1 名监督人员参与下产生，并对每个环节进行记录和签名。

用户的签名密钥对由其持有的电子密匙或其他密码设备产生，而加密密钥对由 KMC 的密码设备产生。

6.1.2 私钥的传递

国汽智联的私钥只能保存在国汽智联控制的密码设备和采取秘密分割的备份介质中，禁止向外传递。

用户的签名私钥在用户的电子密匙或其他密码设备生成后随其实物通过离线方式传递到用户；而用户的加密私钥在 KMC 产生后，使用用户对应电子密匙或其他密码设备预生成的公钥加密后经过 CA、RA 传递回用户对应的电子密匙或其他密码设备中，保证传递中间环节加密私钥不泄露。

电子密匙或其他密码设备的离线传递，可以是 CA 或 RA 和用户面对面的交递，或采取邮寄等方式发送（如邮递）给用户。

6.1.3 公钥的传送

用户的公钥采用证书签发请求格式（PKCS#10）或其他专门的安全格式通过安全通道传递给国汽智联完成证书签发。用户证书签发后其公钥再随证书由国汽智联发布到国汽智联的证书库，证书依赖方可以从国汽智联证书库下载该公钥。

国汽智联的公钥或其直接生成证书的公钥，则直接由国汽智联签发证书后随证书发布到国汽智联证书库供用户和依赖方下载。

6.1.4 密钥的长度

现行国汽智联的根密钥对及其下级 CA RSA 密钥对为 2048 位的密钥对，SM2 密钥为 256 位的密钥对。

国汽智联要求用户的密钥对至少为 1024 位的 RSA 密钥对、256 位的 SM2 密钥对或与此强度相当的其他算法密钥对，否则证书申请不予批准。

6.1.5 公钥参数的生成和质量检查

公钥参数由国家密码主管部门许可的设备或模块产生，国汽智联不会专门安排其质量检查。

国汽智联认为这些设备和介质内置的协议、算法等已经具备了足够的安全等级要求。对于参数质量的检查，同样由通过国家密码主管部门批准许可的加密设备和硬件介质进行，例如加密机、加密卡、USB Key、IC 卡等。

6.1.6 密钥使用目的

在国汽智联认证体系中的密钥用途和证书类型紧密相关，被分为签名和加密两大类。

国汽智联的签名密钥用于签发下级 CA、用户证书和 CRL。

RA 的签名密钥用于确认 RA 所做的审核证书等操作。

用户的签名密钥用于提供网络安全服务，如信息在传输过程中不被篡改、接收方能够通过数字证书来确认发送方的身份、发送方对于自己发送的信息不能抵赖等。用户的加密密钥用于对需在网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。

更多与协议和应用相关的密钥使用限制请参阅 X.509 标准中的密钥用途扩展域。

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。订户协议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。

6.2.1 密码模块的标准和控制

国汽智联使用国家密码主管部门许可的密码产品，其密码模块符合国家规定的标准要求。

6.2.2 私钥多人控制（m 选 n）

国汽智联采用多人控制策略来管理（包括生成、激活、备份、恢复、停止、撤销）CA 的私钥。

国汽智联使用国家密码主管部门许可的硬件密码设备来生成和保护 CA 的私钥。通过密码设备支持的 M 选 N（其中 M 至少为 5，N 至少为 3 但不大于 M）方式进行私钥的分割，即将管理私钥的数据分割成 M 个部分，由密钥管理人员分别持有，并至少需要 N 个“秘密分享”持有者参与才能实现私钥的管理。

6.2.3 私钥托管

国汽智联的根和下级 CA 的私钥不进行托管，其他的签名私钥也都不进行托管。

根据国家相关法规的要求，国汽智联代用户向 KMC 申请加密密钥对的托管，其服务和安全保证参见本文 4.12 节。

用户的签名私钥自行管理，以保证其不可否认性。

6.2.4 私钥备份

国汽智联的私钥按本文 6.2.2 的管理方式备份到安全介质中（如 IC 卡），以作灾难恢复或密码设备更换时的恢复。

除第 6.2.3 的托管服务外，国汽智联不对用户的私钥进行备份。

6.2.5 私钥归档

国汽智联对过期的 CA 密钥对进行归档，保存期限按照本文 5.5.2 的要求。已归档的 CA 私钥不再利用，并在保存期过后进行销毁。

依据国家相关法规或国汽智联与用户的协议，KMC 可对不再托管的私钥进行归档。

6.2.6 私钥导出、导入密码模块

国汽智联的 CA 私钥可以在密码模块中导出，以实现私钥备份；国汽智联的 CA，也可以导入到其他由国家密码主管部门许可的密码模块中，以实现灾难

恢复和密码设备更新等。

用户可以使用国汽智联提供的电子密匙，使其私钥无法从电子密匙中导出，确保用户私钥的安全；但用户的加密私钥可以导入到电子密匙中。

6.2.7 私钥在密码模块的存储

私钥在硬件密码模块中是以密文的形式保存。

6.2.8 激活私钥的方法

国汽智联的私钥采用本文 6.2.2 的控制方式进行激活，并每次请求私钥运算时需提供口令。

用户的私钥保存在电子密匙或智能卡中，需要提供 PIN 码才能激活私钥。部分电子密匙或智能卡的私钥激活可配置成一定周期后自动失效（停止）。

6.2.9 冻结私钥的方法

一旦私钥被激活，除非这种状态被冻结，私钥总是处于活动状态。在某些私钥的使用当中，私钥每次被激活，只能进行一次操作，如果需要进行第二次操作，需要再次进行激活。

冻结私钥的方式包括退出登陆状态、切断电源、将硬件密码模块移开、注销用户或系统等。

对于 CA 私钥，当存放私钥的设备断电，私钥就被冻结。 订户冻结私钥由其自行决定，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，切断电源时，私钥就被冻结。

6.2.10 销毁私钥的方法

国汽智联对归档期过后的私钥进行销毁，包括保存在加密模块的中的副本及其使用备份，国汽智联确保这种销毁是不可复原的。国汽智联采用本文 6.2.2 的控制方式销毁密码模块中的私钥。

国汽智联对从用户中回收的电子密匙或智能卡进行私钥销毁。用户在停止使用证书加解密功能的情况下，为防止密钥泄漏及可能发生的密钥盗用情况，也可以使用国汽智联提供的证书管理工具的删除功能销毁私钥。

6.2.11 密码模块的评估

国汽智联使用国家密码主管部门批准和许可的密码产品，接受其颁发的各类标准、规范、评估结果、评价证书等各类要求，国汽智联可根据产品性能、

工作效率、供应厂商的资质等方面的条件，选择所需要的模块。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

国汽智联和国汽智联用户的公钥会随其证书作为国汽智联安全运行数据被存放或被归档在第三方的数据库中，并在其失效后仍会在国汽智联系统中保存至少 10 年。

6.3.2 证书操作期和密钥对使用期限

一般情况下密钥对的有效期视为与其对应的证书有效期相同。密钥对到期后不能再作为签名和加密使用，但可以继续用来验证签名和解密信息。

6.4 激活数据

6.4.1 激活数据的产生和安装

C 激活数据指用于激活私钥的口令、PIN 码或“秘密分享”数据等。

国汽智联的“秘密分享”数据由硬件加密模块产生（参见本文 6.2.2）。初始的口令或 PIN 码通常由国汽智联产生，或是预制的，或是由计算机随机产生的。国汽智联要求其业务人员或建议用户按以下规则设置或修改口令和 PIN 码：

- 长度不小于 8 个字符，除非系统或设备限制；
- 由数字、字母和特别符号（如“*&%$#@\~!”）组成；
- 不使用有含义的字串；
- 不能和操作员的名字相同；
- 不能包含用户名信息中的较长的子字符串；
- 不使用用过的口令或 PIN 码。

6.4.2 激活数据的保护

对于“秘密分享”，其持有者将遵守规定存放在具有物理保护的地方。口令和 PIN 码只有授权的私钥使用人员才能知悉。需要传递的口令和 PIN 一般使

用密码信封，防止泄露或被窃取。

激活数据被猜测或攻击时（如多次输入不正确的口令或 PIN 码），将被自动锁死。

国汽智联在任何时候发现其激活数据可能泄露的情况下，对激活数据进行更改，并销毁存在的记录，不对历史激活数据归档。

用户应自行评估其电子密匙的 PIN 码的泄露情况，建议用户定期更换 PIN 码。

6.4.3 激活数据的其他方面

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。

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，比如记录有口令的纸页必须粉碎。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

国汽智联用于运行认证系统和处理数据的生产用计算机由国汽智联的系统管理员维护，只有系统管理员或专门授权人员才能管理这些计算机（包括软件安装、卸载、系统优化、部件更换等），以保证系统处于安全可信的运行状态。

国汽智联生产用计算机安装有病毒保护程序，并定时更新防病毒软件的病毒库。任何维护时需接入生产网络的计算机均需进行病毒清查后才能使用。

国汽智联计算机的管理员账号口令有最小密码长度要求，而且必须符合复杂度要求，系统管理员定期更改这些口令。

国汽智联的生产系统网络采用多级不同厂家的防火墙逻辑隔离各安全区域，并部署有入侵防御系统。

国汽智联定期针对网络环境进行风险评估和审计，以检测有否被入侵的危险，尽可能降低来自网络的风险。

国汽智联在处理废旧设备时，将会清除影响认证业务安全性的信息存储并加以确认。

国汽智联定期聘请独立第三方机构进行包括计算机和网络安全在内的整体

评估。

6.5.2 计算机安全评估

国汽智联的计算机系统安全等级达到信息系统安全保护等级三级。

6.6 生命周期技术控制

6.6.1 系统开发控制

国汽智联的认证系统由商用密码产品生产定点单位研制，符合国家的相关标准和规范。

国汽智联要求其内部或外包的软件开发项目符合 ISO9001:2008 质量要求，并遵守国家的法规和签署的项目保密条款。

国汽智联的认证系统首次部署后经国家密码主管部门组织的专家组进行技术鉴定后启用。

6.6.2 安全管理控制

国汽智联认证系统的配置以及任何修改都会记录在案，并制定相关的管理程序和监督机制，包括确定认证系统的访问角色、制定网络安全策略、制定认证系统的访问机制、制定认证系统的审计机制等，来保障认证系统配置的安全，防止未授权的修改。

6.6.3 生命周期的安全控制

国汽智联对认证系统生命周期内的任何补丁和升级版本进行控制，并只有授权的工程实施人员才能访问；认证系统的升级需由安全管理小组批准。

国汽智联在实施补丁或升级之前对代码进行验证，包括测试和版本核对。

6.7 网络的安全控制

国汽智联认证系统根据信息敏感度的不同，划分为不同的区域，每个区域之间配备不同厂家的异构防火墙进行保护，并配置入侵防御系统，与防火墙联动。

CA 与 RA 的功能模块之间的通信采用安全通信协议连接，并采用安全身份认证技术。

国汽智联对网络安全设备的软件版本、规则及时更新，保持其有效的工作状态。只有系统管理员或专门授权人员才能管理这些网络设备。并且这些设备

的管理员账号口令有最小密码长度和复杂度要求，系统管理员定期更改这些口令。

6.8 时间戳

国汽智联认证系统的所有服务器都与时间服务器的时间同步，保证系统各电子记录需要的时间是准确的。

国汽智联还提供数字时间戳（DTS）服务，符合 RFC3161。

7.证书、证书吊销列表和在线证书状态协议

7.1 证书描述

国汽智联颁发的证书符合《GB/T20518-2006 信息安全技术 公钥基础设施数字证书格式》标准要求，并完全兼容 ITU-TX.509 和 RFC5280 等国际标准规范，支持大部分标准扩展，并支持自定义扩展项。

7.1.1 版本号

国汽智联订户证书符合 X.509 V3 证书格式，版本信息存放在证书版本信息栏内。

7.1.2 证书扩展项

国汽智联证书支持的标准扩展包括：

- 密钥用法（KeyUsage）
- 证书策略（CertificatePolicies）
- 主体替换名称（SubjectAlternativeNames）
- 基本限制（BasicConstraints）
- 扩展密钥用途（ExtendedKeyUsage）
- 证书注销列表分发点（CRLDistributionPoints）
- 颁发机构密钥标识符（AuthorityKeyIdentifier）
- 主体密钥标识符（SubjectKeyIdentifier）

国汽智联也支持 GB/T 20518 标准及数字证书格式标准中指定的标准扩展，并支持用户自定义私有扩展，可根据用户或应用的要求定制。私有扩展一般情况下为非关键项。

7.1.3 算法对象标识符

国汽智联使用 SM3withSM2 算法签发证书，算法 OID 为：1.2.156.10197.1.501。

7.1.4 名称形式

证书主体名称和颁发机构的名称形式遵循本文 3.1 要求，由 DN 表示。

另外，国汽智联颁发的证书支持主体替换名称扩展，在主体替换名称扩展中可以包含证书主体的其他相关名称信息，比如电子邮件地址、服务器的 IP 地址或域名等。

7.1.5 名称限制

订户的命名一定要有意义，应具有通常能够被理解的语义，可以明确确定证书主题中的个人、单位或者设备的身份，订户证书不被允许为匿名或者伪名。

7.1.6 证书策略对象标识符

由证书颁发机构制定并对外发布，并向国际标准化组织申请证书策略对象标识符（OID）以保证互操作性。证书策略 OID 代表证书颁发机构提供服务的相关策略（如国汽智联 CP）。证书依赖方在接受该证书行为时通过阅读证书策略以帮助确定是否信任该证书。用户必须在阅读并同意证书策略后才到证书颁发机构申请并使用证书。

7.1.7 策略限制扩展项的用法

无规定。

7.1.8 策略限定符的语法和语义

在国汽智联所颁发证书的证书策略扩展项中包含了 CP 策略限定符，提供了指向国汽智联 CP 的 URL，从中可以获取国汽智联的《国汽（北京）智能网联汽车研究院有限公司证书策略》。

7.1.9 关键证书策略扩展项的处理语义

与 X509 和 PKIX 规定一致。

7.2 证书吊销列表

国汽智联发布的 CRL 符合《GB/T 20518-2006 信息安全技术公钥基础设施数字证书格式》及 ITU-TX.509、RFC5280 标准规范定期签发 CRL，供用户查询

使用。

依本 CP 签发的 CRL 符合 RFC5280 标准。CRL 至少包含如下表所述基本域和内容。

7.2.1 版本

CRL 版本号为 X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项

国汽智联发布的 CRL 中，包含了以下扩展项：

- 颁发机构密钥标识符（AuthorityKeyIdentifier）
- CRL 编号（CRLNumber）
- DeltaCRL 指示符（DeltaCRLIndicator，仅用于 DeltaCRL，是关键扩展）如果有明确的被注销的原因，CRL 条目则会包含被注销的原因扩展（ReasonCode）。

应用如果遇到不认识的关键的 CRL 扩展或者 CRL 条目扩展，则不能使用该 CRL 来验证证书的注销状态。

7.3 OCSP 描述

国汽智联采用 OCSP 提供在线证书状态查询服务。应用户的要求，国汽智联可以将 OCSP 服务 URL 写到证书中。OCSP 作为 CRL 的有效补充，提供比 CRL 较为及时的证书状态查询机制，方便用户及时的获取证书状态信息。

国汽智联的 OCSP 服务系统符合 RFC2560 标准规范。

7.3.1 版本号

RFC2560 定义的 OCSP V1 版本。

7.3.2 OCSP 扩展项

国汽智联未使用 OCSP 相关扩展项。如果遇到 OCSP 响应返回 unauthorized 错误码、证书返回 unknown 状态或者不认识的扩展，则应该使用其他的机制去验证该证书的注销状态。

8.认证机构审计和其他评估

国汽智联建立内部审计机制，并组织信息安全风险评估活动。国汽智联还接受国家电子认证服务主管部门组织的年度审查。其他第三方的外部审计或评估依据用户协议或其他政策进行。

8.1 审计的依据

审计是为了检查和监督国汽智联及其下属机构或其他关联机构是否依据《电子签名法》、 《电子认证服务管理办法》、《国汽（北京）智能网联汽车研究院有限公司证书策略》的要求，依法开展电子认证服务业务，以及在开展业务过程中，是否存在违反其他法律法规以及国汽智联的业务规范、管理制度、安全策略等情况，以达到规避经营风险、提高服务质量、保障用户权益的目的。

8.2 审计的形式

审计分为外部审计与内部审计。

外部审计是由法律规定的主管部门、主管部门委托的第三方机构或国汽智联委托的第三方机构对自身的电子认证服务业务进行审计与评估。审计内容、评估标准及审计评估结果是否公开由主管部门确定。

内部审计是指国汽智联自行组织人员对机构内部、下属机构等进行审计评估，审计结果供内部用以完善管理、改进服务，不需对外公开。

8.3 审计或评估的频率

国汽智联的内部审计周期为每月一次，并且每年进行一次信息安全的风险评估。如果出现特殊情况则单独启动审计或风险评估，引发评估或审计事件的特殊情况包括疑似或真实的敏感信息泄密、用户反馈异常、重大的系统变更等。

国家电子认证服务主管部门组织的审查为每年一次。

8.4 审计或评估人员的资质

国汽智联的内部审计或评估人员要求熟悉电子认证业务和 PKI 技术体系，接受过内部信息安全 管理培训，并由安全管理小组任命。

外部审计或评估人员的资质由相关法规或主管部门确定。

8.5 审计或评估人员与国汽智联的关系

国汽智联内部审计人员要求与被审计对象无责任关系，为国汽智联雇员。

国汽智联内部风险评估的负责人要求与被评估对象无责任关系，可以是国汽智联雇员，也可以是非国汽智联雇员。

外部审计或评估人员应为与国汽智联无任何除审计或评估之外的业务、财务往来或其他足以影响评估客观性的利害关系。

8.6 审计或评估的内容

国汽智联内部审计或评估涉及的内容包括以下：

- 人员管理
- 物理环境建设及安全管理
- 系统结构及其运行管理
- 密钥管理
- 用户服务规范管理
- 综合运营规范（如法规、CP、风险控制等方面）

在特殊情况下的审计或评估内容可能只包括以上内容的一部分。

国家电子认证服务主管部门组织的年度审查内容遵照其发布的最新要求。

8.7 对问题与不足采取的措施

如果在审计或评估过程中发现执行规范有不足或存在问题，国汽智联将根据审计或评估报告制定和实施纠正措施，并由安全管理小组监督执行。

对于重大的安全隐患，国汽智联同样会启动应急事件处理程序，以迅速控制风险的影响范围。

8.8 审计或评估结果的传达与发布

国汽智联只按管理或协议要求将审计或评估结果传达到相应对象。

除非法律法规要求，国汽智联一般不公开审计或评估结果。

9.法律责任和其他业务条款

9.1 费用

国汽智联可根据提供的电子认证服务向本机构的证书订户收取费用，具体收费标准必须根据国家有关管理部门的批复文件执行，国汽智联不得擅自提高收费标准，扩大收费范围。

9.1.1 证书新增和更新费用

国汽智联对证书的签发、更新、密钥恢复和管理收取服务费用，费用标准执行国家或地方物价主管部门批准的价格。并根据实际情况，在批准价格之内调整。

9.1.2 证书查询费用

对于证书查询，目前国汽智联不收取任何费用。除非用户提出的特殊需求，需要国汽智联支付额外的费用，国汽智联将与用户协商收取应该收取的费用。如果证书查询的收费政策有任何变化，国汽智联将会及时在网站 www.china-icv.cn 上予以公布。

9.1.3 吊销和状态信息查询费用

国汽智联对发布到证书库中的 CRL 提供免费下载和使用服务。

国汽智联的 OCSP 服务和其他定制的证书状态查询服务根据用户的服务协议要求进行收费。

9.1.4 其他服务费用

国汽智联免费提供本 CP 和证书业务相关申请表格下载服务。

对于用户要求定制的服务，国汽智联酌情收取费用。

9.1.5 退款策略

国汽智联对订户收取的费用，除了证书申请和更新费用，因为特定理由可以退还外，国汽智联均不退还用户任何费用。

在实施证书操作和签发的过程中，国汽智联遵守严格的操作程序和策略。如果国汽智联违背了本 CP 所规定的责任或其它重大义务，订户可以要求国汽智联撤销证书并退款。在国汽智联撤销了订户的证书后，国汽智联将把订户剩余的证书使用费用并扣除相应税费后退还给订户。

此退款策略不限制订户得到其它的赔偿。

完成退款后，订户如果继续使用该证书国汽智联将追究其法律责任。

在业务受理过程中，发现申请者提供虚假材料，国汽智联中止受理，但不予退还已收取的各项费用。

9.2 财务责任

9.2.1 保险范围

保险范围主要针对 CP§9.9 中所规定的赔偿。

9.2.2 其他财产

无规定。

9.2.3 对最终实体的保险或担保范围

证书订户一旦接受国汽智联的证书，或者通过协议完成对证书服务的接受，那么就意味着该订户已经接受了本 CP 关于保险和担保的规定和约束。

9.3 业务信息保密

9.3.1 保密信息范围

国汽智联列入保密的信息包括但不限于以下内容：

- 用户的个人信息和（或）机构信息；
- 国汽智联及其代理机构的证书业务处理信息；
- 所有的私钥信息；
- 国汽智联的运行数据和记录，以及保障运行的相关计划；
- 国汽智联与业务代理机构间的商业信息，包括商业计划、销售信息、贸易秘密和在非公开协议下从第三方得到的信息；
- 国汽智联及其业务代理机构相关的审计报告、审计结果及其处理等信息；
- 除非法律明文规定，国汽智联没有义务公布或透露用户证书以外的任何信息；
- 其他书面或有形形式确认为保密的信息。

9.3.2 不属于保密的信息

以下信息国汽智联不列入保密范畴：

- 证书所载信息，以及证书状态信息；
- 由国汽智联网站或手册公布的信息。包括证书申请流程、证书使用指南、CP 等信息。

以上信息虽然是公开信息，但仅供下载查阅使用，任何人或组织不得转载或用于任何商业用途，国汽智联保留追究责任的权利。

9.3.3 保护保密信息的责任

国汽智联及其业务代理机构、用户、关联实体等所有保密信息掌握者均有义务承担信息保密的责任。

国汽智联执行严格的信息保密制度以确保只有经国汽智联授权的人员才能接近机密信息。严格禁止未授权的访问、阅读、修改和删除等操作。

当机密信息的所有者出于某种原因，要求国汽智联公开或披露其所拥有的机密信息，国汽智联应满足其要求。如果这种披露机密的行为涉及任何其他方的赔偿义务，国汽智联不应承担任何与此相关的或由于公开机密信息引起的所有损失、损坏的赔偿责任。

当国汽智联在国家的法律法规要求下，或在法院的要求下必须披露本文 9.3.1 中的保密信息时，国汽智联可以按照法律法规或法院判决的要求，向执法部门公布相关的保密信息。这种披露不能视为违反了保密的要求和义务，国汽智联无须承担任何责任。

9.4 个人隐私保密

9.4.1 隐私保密计划

国汽智联制定隐私保护策略，所有相关人员（包括国汽智联及其 RA 的工作人员、用户等）必须严格遵守相应的规章制度。

国汽智联根据国家相关法规的出台，及时调整隐私保护策略，以符合国家法规的要求。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括：

1. 订户的有效证件号码如身份证号码、单位机构代码；
2. 订户的联系电话；

3. 订户的地址；

4. 订户的银行帐号。

9.4.3 不被认为隐私的信息

订户持有的证书内包括的信息，以及该证书的状态等，是可以公开的，不被视为隐私信息。

9.4.4 保护隐私的责任

国汽智联对本文 9.4.2 所列的隐私信息进行保护，防止泄露。只有经国汽智联授权的人员才能接触隐私信息，禁止任何未授权的访问、阅读或转移。

9.4.5 使用隐私信息的告知与同意

国汽智联只在其业务范围内使用本文 9.4.2 所列的隐私信息，包括用户身份识别、管理、和服务的目的。这些使用，国汽智联没有告知用户的义务，也无需得到用户的同意。

任何超出以上范围的隐私信息使用，需得到其本人的同意。对违法、违规使用、发布以上隐私信息的，国汽智联承担由此造成的证书持有者、依赖方的损失，并负担相应的行政、经济责任。

9.4.6 依法律或行政程序的信息披露

当国汽智联在国家的法律、规章的要求下，或在法院的要求下必须披露本文 9.4.2 中的隐私信息时，国汽智联可以按照法律、规章或法院判决的要求，向执法部门公布相关的隐私信息。这种披露不能视为违反了保密的要求和义务，国汽智联无须承担任何责任。

9.4.7 其他信息披露情形

当隐私信息其本人出于某种原因，要求国汽智联公开或披露他的隐私信息，国汽智联可根据授权或协议进行披露。如果这种披露行为涉及任何其他方的赔偿义务，国汽智联不承担任何与此相关的或由于公开隐私信息引起的所有损失、损坏的赔偿责任。

9.5 知识产权

国汽智联享有并保留对证书以及国汽智联提供的全部软件的一切知识产权，包括但不限于所有权、名称权和利益分享权等。

国汽智联发行的证书及其状态信息，以及国汽智联提供的软件、系统、文档中，使用、体现和涉及到的一切版权、商标和其他知识产权均属于国汽智联，这些知识产权包括所有相关的文件、CP、规范文档和使用手册等。

在没有国汽智联预先书面同意的情况下，用户不能在任何证书到期、作废、或终止的期间或之后，使用或接受任何国汽智联使用的名称、商标、交易形式或可能与之相混淆的名称、商标、交易形式或商务称号。

9.6 陈述与担保

9.6.1 CA 的陈述与担保

国汽智联对证书订户必须做出如下担保：

- 在批准证书申请和颁发证书中没有国汽智联所知的或源自国汽智联的错误陈述；
- 在生成证书时，保证足够检测和审核，使证书中的信息与国汽智联所收到的信息保持一致；
- 除了未经验证的用户信息外,证书中的或证书中合并参考到的所有信息都是准确的；
- 签发给用户的证书符合本 CP 的所有实质性要求；
- 按本 CP 的规定，及时注销或挂起证书，并签发 CRL；
- 国汽智联将向用户和依赖方通报任何已知的，将在根本上影响证书的有效性和可靠性的事件；
- 其他的陈述与担保参见与用户的服务协议。

9.6.2 RA 的陈述与担保

国汽智联的 RA 担保如下：

- RA 遵循国汽智联制订的服务受理规范、系统运作和管理要求，保证其服务不影响到国汽智联的服务标准和承诺；
- 在审核和批准证书申请中没有 RA 所知的或源自 RA 的错误陈述；
- 在处理证书申请时，保证足够检测和审核，使证书中的信息与 RA 所收到的信息保持一致；
- 除了未经验证的用户信息外,证书中的或证书中合并参考到的所有信息都是准确的；

- 签发给用户的证书符合本 CP 的所有实质性要求；
- 按本 CP 的规定，及时处理证书的注销或挂起申请；
- 其他的陈述与担保参见与用户的服务协议。

9.6.3 订户的陈述与担保

订户的担保如下：

- 用与证书中所含公钥相对应的私钥所进行的每一次签名，都是用户自己的签名，并且在进行签名时，证书是有效的（没有过期、被挂起或注销）并已被用户接受；
- 用户的私钥得到很好的保护，未经授权的人员从未访问过其私钥；
- 用户在证书申请过程中向国汽智联及其 RA 陈述的所有信息是真实的；
- 用户提供给国汽智联及其 RA 用于申请证书的所有材料都是真实的；
- 如果存在代理人，那么用户和代理人两者负有连带责任。用户有责任就代理人所作的任何不实陈述与遗漏，通知国汽智联其 RA；
- 用户将按本 CP 的规定，只将证书用于经过授权的或其他合法的使用目的；
- 用户的证书是终端证书。用户保证不将其证书用于发证机构所从事的业务，例如：把与证书中所含的公钥所对应的私钥用于签发任何证书（或认证其他任何形式的公钥）或签发 CRL 之类；
- 其他的陈述与担保参见与国汽智联的服务协议。

9.6.4 依赖方的陈述与担保

依赖方的担保如下：

- 依赖方保证熟悉国汽智联 CP 以及和用户证书相关的证书政策，并了解和遵守证书的使用目的；
- 依赖方确保证书及其对应的密钥对的确用于预定的目的；
- 依赖方在信赖用户的证书前，需收集足够的信息，判明是否国汽智联签发的证书并在有效期内，根据最新的 CRL 检查证书的状态，查明证书是否还有效；
- 依赖方的信赖行为，表明其已同意本 CP 的有关条款。

9.6.5 其他参与者的陈述与担保

遵守本 CP 的所有规定。

9.7 担保免责

国汽智联在以下三种情况下免除责任：

1．不可抗力

在不可抗力情况下（内容见本文 9.16.5 和相关法律条款），国汽智联免除责任。

2．免责条款

免责条款是指当事人在合同中约定的免除将来可能发生的违约责任的条款。

免责条款不得违反法律的强制性规定和社会公共利益。

3．债权人过错

如果合约不履行或者不完全履行是由对方即债权人的过错造成的，不履行或者不完全履行的一方免除违约责任。在电子认证服务合同中也存在因债权人过错而免责的情况，包括但不限于以下内容：

- 申请者故意或无意的提供不完整、不可靠或已过期的，包括但不限于伪造、篡改、虚假的信息，而其又根据正常的流程提供了必须的审核文件，由此得到了国汽智联签发的数字证书；
- 用户或依赖方没有使用可信赖系统进行证书操作；
- 用户在国汽智联允许的目的范围之外使用或证书使用不当；
- 以上未尽事宜，依照中华人民共和国现行法律、法规执行。

9.8 有限责任

国汽智联是依《中华人民共和国公司法》、《电子签名法》设立的有限责任公司，国汽智联在承担任何责任和义务时，只承担法律范围内的有限责任。

国汽智联及其授权的发证机构，对于一份证书的所有当事人（包括但不限于用户、申请人或依赖方）的合计赔偿责任，不超过该证书的最高赔偿限额，这种限额可以由国汽智联改动。国汽智联声明的法律赔偿责任之最高限额为该证书相应的服务费用的 10 倍。当事人不能得到赔偿或有异议，可以向主管部

门进行反映，责令国汽智联履行赔偿责任。

国汽智联的赔偿责任范围：

➢ 证书信息与用户提交的资料信息不一致，导致用户或依赖方损失；

➢ 由于国汽智联的原因，导致依赖方或用户自身无法正常验证证书状态而蒙受损失；

➢ 国汽智联只有在国汽智联证书有效期限内承担以上损失或损害赔偿。

9.9 赔偿

9.9.1 认证机构的赔偿责任

如国汽智联违反了本 CP9.6.1 中的陈述，订户、依赖方等实体可申请国汽智联承担赔偿责任（法定或约定免责除外），包括以下情形：

1. 国汽智联将证书错误的签发给订户以外的第三方，导致订户或依赖方遭受损失的；
2. 在订户提交信息或资料准确、属实的情况下，国汽智联签发的证书出现了错误信息，导致订户或依赖方遭受损失的；
3. 在国汽智联明知订户提交信息或资料存在虚假谎报的情况，但仍然向订户签发证书，导致依赖方遭受损失的；
4. 由于国汽智联的原因导致 CA 私钥的泄露；
5. 国汽智联未能及时吊销证书，导致依赖方遭受损失的。

9.9.2 订户的赔偿责任

➢ 用户申请证书时，因故意、过失或者恶意提供不真实资料，造成国汽智联或者其他方遭受损害的；

➢ 用户因故意或者过失造成其私钥泄漏、遗失，明知私钥已经泄漏、遗失而没有告知国汽智联或其 RA，以及使用不安全系统或不当交付他人使用，造成国汽智联或其他方遭受损害的；

➢ 用户提供使用的命名信息，包括但不限于名称、域名、IP、电子邮箱等，存在任何侵犯他人知识产权，造成国汽智联或其他方遭受损害的。

9.9.3 依赖方的赔偿责任

➢ 未按国汽智联 CP 或其他相关协议承担依赖方义务，而造成国汽智联或其他方遭受损害的；

➢ 未能按国汽智联 CP 策略识别和信任证书及其行为，而造成国汽智联或其他方遭受损害的；

➢ 未查验证书的有效期和状态就冒然信任证书及其行为，而造成国汽智联或其他方遭受损害的。

9.10 有效期与终止

9.10.1 有效期

本 CP 及其更新版本自公布之日起的 15 天之后正式生效，CP 中将详细注明版本号及发布日期。

9.10.2 终止

当新版本的 CP 正式发布生效时，旧版本的 CP 将自动终止。

9.10.3 终止的效果与存续

国汽智联 CP 一旦终止后，用户和依赖方原则上不受其条款的约束，但涉及知识产权和保密的相关条款继续生效。

9.11 对参与者的个别通告及信息交互

除非参与者之间另有协议约定，否则各参与者之间必须采用书面的的方式（包括有数字签名的电子文书）进行通告和沟通。

信息发送者应确保信息被对方所接收，并能够理解。

9.12 修订

9.12.1 修订程序

国汽智联 CP 由国汽智联安全管理委员会根据情况进行审查，任何时候国汽智联安全管理委员会认为有必要时即组织修订。修订后的版本经国汽智联安全管理委员会审批后发布到国汽智联网站（http://cp.china-icv.cn:8089/cp/cicv_cp.pdf），并报送工业和信息化部备案。

9.12.2 通知机制和期限

国汽智联安全管理委员会有权作出对 CP 作任何修改的决定。如果 CP 的修改没有本质的变化，包括重新排版、勘误、重新表达，联系方式、发布地址变更等，则无需进行个别的通告。

国汽智联 CP 的修改结果在国汽智联的网站（http://www.china-icv.cn）上公布。

所有可能以书面形式提供给用户的 CP 修订结果，按以下规则发送：

1. 接受者是一个组织，则向其在国汽智联或其 RA 登记的联系地址发送信息；
2. 接受者是个人，则向其申请书上登记的地址发送信息；
3. 这些通知可能用快递或挂号信的方式发送。国汽智联也可以选择通过电子邮件（E-mail）向用户发送通知，该电子邮件地址在用户申请证书时已注明。

国汽智联 CP 的所有修正、修改和变化在公布后立刻生效。用户如不在修改结果公布之日起七天内作废证书，就视为同意这种修正、修改和变化。

9.12.3 必须修订的情形

如果出现下列情况，那么必须对 CP 进行修改：

- 采用了新的密码体系或技术，并影响现有 CP 的有效性；
- 认证系统和有关管理规范发生重大升级或改变；
- 法律法规的变化，并影响现有 CP 的有效性；
- 现有 CP 出现重要缺陷。

9.13 争议解决条款

证书用户、依赖方等实体在电子认证活动中产生争端可按照以下步骤解决：

a) 当事人首先通知，根据本《电子认证业务规则》中的规定，明确责任方；

b) 由相关部门负责与当事人协调；

c）若协调失败，可以通过司法途径解决；

d）任何因与国汽智联或授权机构就本《电子认证业务规则》所产生的任何争议而提起诉讼的，受国汽智联工商注册所在地的人民法院管辖。

9.14 管辖法律

国汽智联 CP 在各方面按照中国现行法律和法规执行和解释。包括但不限于《电子签名法》及《电子认证服务管理办法》、《电子认证服务密码管理办法》等。

9.15 符合适用法律

国汽智联电子认证业务各参与方必须遵守中国现行法律及相关行业规范的监管，包括但不限于《电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》及相关密码技术、产品标准规范等。

若要出口使用于国汽智联认证服务的相关产品，可能需要取得相关政府机关的许可。产品出口的当事人必须遵守中国进出口法律和法规。

9.16 一般条款

9.16.1 完整协议

国汽智联 CP 及国汽智联的相关业务管理办法、国家相关法律法规构成国汽智联的整体协议，各参与方的业务须遵循整体协议。

9.16.2 让渡

若国汽智联下属 RA 因故注销，则其管理的相应用户须接受国汽智联的业务调配，通过另一 RA 获得相应服务。

若国汽智联因政策性原因或其他不可抗力停止服务，国汽智联之所属用户须按国家规定，接受相应接管 CA 的证书服务条款。

9.16.3 分割性

在国汽智联的电子认证业务中，因某一原因导致法庭或其他仲裁机构判定协议中的某一条款无效或不具执行力时（由于某种原因），用户证书业务相关协议的其他条款仍然生效。

9.16.4 强制执行

国汽智联电子认证各参与方中，免除一方对合约某一条款违反应负的责任，不意味着免除这一方对其他条款违反或继续免除这一方对该条款违反应负的责任。

9.16.5 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。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。

在电子认证活动中，国汽智联由于不可抗力因素而暂停或终止全部或部分证书服务的，也可根据不可抗力的影响而部分或者全部免除违约责任。其他认证活动参与各方（如用户）不得就此提出异议或者申请任何补偿。

由于法律无法具体规定或者列举不可抗力的内容和种类，加上不可抗力本身的弹性较大，在理解上容易产生歧义，因而允许当事人在合同中订立不可抗力条款，根据交易的情况约定不可抗力的内容和种类。国汽智联电子认证合同中的不可抗力条款可以在与数字证书申请表一起提供给用户的服务协议中规定，也可被规定在国汽智联 CP 中。

9.17 其他条款

国汽智联对本 CP 具有最终解释权。