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： 2026 年 8 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
2.0	修订	根据最新 CPS 以及政策变更修改	林立森	安委会	2021 年 06 月
2.1	修订	根据最新 CPS 以及政策变更修改，删除个人证书相关内容	林立森	安委会	2021 年 12 月
2.2	修订	据最新 CPS 以及政策变更修改	张相雨	安策委	2026年8月

目 录

1. 概括性描述

1.1 概述

证书策略（CP，Certificate Policy）是认证机构（CA,Certification Authority）制订的一组策略，表明国汽（北京）智能网联汽车研究院有限公司（以下简称“国汽智联”）PKI 体系中的各个参与者的划分与其义务，并包含国汽智联证书基本策略。

本证书策略的适用范围为国汽智联发放的证书。

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》，分配唯一对象标识符OID 1.2.156.115370.1.1。本CP 中为机构基础级电子签名认证证书分配唯一的对象标识符OID2.16.156.339.2.1.2.1。

1.3 PKI 参与者

本文中所包含的电子认证活动参与者有：电子认证服务机构、注册机构、订户、依赖方以及其它参与者，下面将分别进行描述。

1.3.1 电子认证服务机构（CA）

电子认证服务机构 CA（Certification Authority）承担证书签发、更新、吊销、密钥管理、证书查询、证书黑名单（又称证书吊销列表或 CRL）发布、政策制定等工作。

1.3.2 注册机构（RA）

注册机构（RA）作为电子认证服务机构授权委托的实体，负责受理证书的申请、审核、更新、恢复、撤销和下载等业务。国汽智联本身是 CA，也可承担 RA 职责。

1.3.3 订户

订户是向电子认证服务机构申请证书的实体。在电子签名应用中，订户即为电子签名人。

在国汽智联电子认证服务体系中，订户为具有确定身份标识的主体或实体。需要明确的是，证书订户与证书主体是两个不同的概念。“证书订户”是指向

国汽智联申请证书的实体，通常为机构；“证书主体”是指与证书信息绑定的实体，服务器证书中的“证书主体”通常是指受信任的服务器或用于确保与某一机构安全通信的其它设施。证书订户需要承担相应的责任与义务，而证书主体则是证书所要证明的可信赖方。。

1.3.4 依赖方

依赖方是指信赖于证书所证明的基础信任关系并依此进行业务活动的实体。

1.3.5 其他参与者

除国汽智联、订户和依赖方以外的参与者称为其它参与者。

1.4 证书应用

1.4.1 适合的应用

国汽智联证书支持相应的合法应用，具体应用场景在相应 CPS 1.4 节中说明。

1.4.2 限制的证书应用

各类证书的使用应符合证书内容对其用途的限定，如参与方未经国汽智联认可或不遵守相关约定，其对证书的应用超出限定的应用范围，将不受国汽智联的保护。

国汽智联签发的证书禁止在违反国家法律、法规或破坏国家安全的情况下使用，由此造成的法律后果由订户负责。

禁止使用证书的场景包括不限于：

a） 涉及人身关系的，如婚姻、收养、继承等；

b） 涉及停止公共事业服务的，如停止供水、供热、供气等；

c） 法律、行政法规规定的其他不适用电子签名的应用场景或类型；

d） 国家法律法规禁止的活动。

涉及生命健康、财产权益等高风险活动禁止使用基础级电子签名认证证书。

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。当需要编写或修订本 CP 时，由安全管理委员会牵头组织相关人员进行编写或修订，并应指定编写组负责人。

1.5.2 联系人

联系地址：北京市北京经济技术开发区融兴北三街39号国家智能网联汽车创新中心。

邮箱：cps@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。

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. 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。

10. 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）。

11. 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。

12. 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。

13. 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。

14. 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。

15. 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。

16. 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。

17. 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。

18. 鉴别

辨别认定证书申请者提交材料真伪的过程。

19. 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。

20. 证书主体 （ certificate subject）

证书主体是证书公钥对应的实体，它可以是机构、域名等。

21. 订户 （customer）

向 CA 申请证书的实体，包括机构订户。

22. 依赖方 （relying party）

使用证书中的数据进行决策的用户或代理。

24. 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。

25. 依赖方 （relying party）

使用证书中的数据进行决策的用户或代理。

26. 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。

27. 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。

28. 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。

29. 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。

30. 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。

31. 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。

32. 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。

33. 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

国汽智联信息库面向订户及证书应用依赖方提供信息服务。国汽智联信息库包括但不限于以下内容：证书、CRL、CPS、CP、证书服务协议、技术支持手册、国汽智联网站信息以及国汽智联不定期发布的信息。

2.2 认证信息的发布

国汽智联的 CPS、CP 以及相关的技术支持信息等在国汽智联网站上发布。用户证书可通过证书下载平台获取，已被吊销了的证书的信息可从 CRL站点查获，证书的状态（有效、吊销）可通过 OCSP 服务获得。。

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》自完成审批流程后 15 个工作日之内发布到国汽智联网站上。

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

国汽智联的安全访问控制机制确保只有经过授权的人员才能编写和修改信息库中的信息，但不限制对这些信息的阅读权。

3. 身份标识与鉴别命名

3.1 命名

3.1.1 名称类型

国汽智联采用X.500定义的唯一甄别名DN（Distinguished Name）来标识订户身份信息，该甄别名包含于证书主体中。

3.1.2 对名称意义化的要求

订户的甄别名DN必须具有一定的意义，能够与证书主体所对应的实体建立确定联系。主体DN项中包含机构名称，扩展项中包含组织机构的有效证件类型及其编号。

3.1.3 商标的承认、鉴别和角色

国汽智联签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

3.1.4 自定义内容

在不影响证书通用性的前提下，可在证书中增加自定义的其他内容。

3.1.5 理解不同名称形式的规则

国汽智联所签发证书的甄别名DN符合GB/T16264.8的要求，命名规则如下：

编号	识别名称	说明	内容（示范性）
1	County（C）	国家名称	C=CN
2	State（S）	所在省	S=北京
3	Location（L）	所在城市	L=北京
4	Organization（O）	组织机构名称	O=国汽智联
5	Organization Unit（OU）	部门名称	OU=技术中心
6	Common Name（CN）	机构法定名称	CN=XX公司

如果有C项，则放在最后，且C=CN；如果有CN项，则放在DN的最前面；
如果同时存在OU和O项，则OU在O前面；如果同时存在S和L项，则L在S前面。

3.2 初始身份确认

3.2.1 证明拥有私钥的方法

订户持有的私钥由符合国家安全标准的密码模块产生和存储。

国汽智联通过包含数字签名的证书请求数据（如 PKCS#10）来证明订户持有私钥。国汽智联的电子认证服务系统使用订户的公钥验证由订户私钥签名的证书请求数据，来证明证书申请人持有与证书申请数据中公钥相对应的私钥。

3.2.2 证书订户信息鉴别

订户在申请国汽智联签发的证书前应指定并书面授权证书的申请代表，提供有效身份证明文件、证书申请文件或以国汽智联认可的安全方式提交订户真实有效信息，并接受证书申请的有关条款，同意承担相应的责任。

国汽智联或者国汽智联的注册机构接受订户的证书申请后，应对订户的身份真实性进行审核，并按照双方的约定妥善保存订户申请材料。具体鉴别内容参见 CPS3.2.2 章节。

3.2.3 互操作准则

互操作可能是交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的CA之间建立相互信任关系，从而使双方的订户可以实现互相认证。

国汽智联将根据业务需要，在遵循本CPS的各项控制要求的基础上，与国汽智联电子认证服务体系中未涉及的其他电子认证服务机构建立交叉认证关系。但交叉认证并不表示国汽智联批准了或赋予了其他CA或电子认证服务机构的权力。

。

3.3 密钥更新请求的标识与鉴别

证书密钥更新有两种情况：补发和换发。

1、证书补发

补发是指在证书有效期内，订户更新证书的操作。

当订户需要补发证书时，应主动向国汽智联的注册机构提出证书补发申请。国汽智联需对订户身份进行重新验证，验证流程及要求与初次申请相同。

服务器类证书补发操作成功时，新证书下载成功一个月后吊销老证书，其他类型的证书补发时立即吊销老证书。新证书有效期从补发成功之日起到原证书失效日止。

2、证书换发

换发是指在证书将要过期的三个月内或证书过期后，订户申请更新证书的操作。以下情况订户需要申请证书换发：订户证书即将到期或已经过期。

在订户证书到期前的三个月内，国汽智联将通过适当的方式通知用户对证书进行换发操作。订户证书换发时，需要对订户身份进行重新验证。

服务器类证书换发时需要对订户身份进行重新验证，重新验证订户身份的验证流程及要求与初次申请相同。

服务器类证书换发操作成功时，新证书下载成功一个月后吊销旧证书，其他类型的证书换发时立即吊销老证书。新证书有效期将从证书换发之日起至原证书到期为止再另加一个证书有效周期（已经过期的证书换证，其有效期仅为证书有效周期）。

3.3.1 常规密钥更新的标识与鉴别

同 3.2。

3.3.2 吊销后密钥更新的标识与鉴别

证书吊销后的密钥更新等同于订户重新申请证书，其要求与初次申请鉴别相同。

3.4 证书变更

证书变更是指订户在不改变现有公钥的情况下重新申请一张证书。国汽智联不提供证书变更服务，即订户对证书进行更新时其密钥对必须重新生成。

3.5 吊销请求的标识与鉴别

证书吊销请求的标识与鉴别流程见本 CP 的 4.8.3。

4. 证书生命周期操作要求

4.1 通用要求

国汽智联承担建立、运营和维护注册通道的责任。国汽智联承担与订户签订电子认证服务协议的责任。订户承担提供准确信息的责任。国汽智联承担妥善记录并保存相关信息的责任。

4.2 证书申请

4.2.1 证书申请实体

证书申请实体包括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)。

4.2.2 注册过程与责任

1. 最终订户

最终订户即申请证书的实体，最终订户须明确表示其愿意接受国汽智联 CPS 及相关的 CP 中所规定的相关责任与义务（CPS 及相关 CP 公布在国汽智联网站上），并需要按照 CPS3.2.2 的要求提供真实、准确的申请信息；根据《中华人民共和国电子签名法》的规定，申请者未向国汽智联提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、国汽智联或者国汽智联的注册机构造成损失的，订户应承担相应的法律及赔偿责任。订户有责任保护其拥有的证书私钥安全，并将证书应用于合法的场景。

2、注册机构

国汽智联既是一个 CA，同时也承担了部分注册机构的职能，如订户可以直接向国汽智联申请证书，由国汽智联审核订户信息并处理订户的请求。注册机构对订户提供的证书申请信息参照 CPS3.2.2 的要求进行鉴别，国汽智联对通过鉴别后的订户签发证书。同时应履行本 CP 中所规定的相关责任与义务。

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

证书签发完成后，国汽智联将证书本身或者证书获得的方式递送给证书申请人。

证书申请人在接收到证书后应及时验证证书所匹配的信息，如无异议需做确认接受证书登记。

国汽智联保存证书申请人接受证书的记录，包括接受时间、方式、操作人等信息。

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 密钥对和证书交付前安全

国汽智联在密钥对和证书交付前采取有效措施保障其安全性，包括：

1）采用技术手段和规范的操作流程保障签名私钥生成和传输过程的安全；

2）国汽智联审核订户密钥是否符合国家或行业相关安全标准要求，对不符合要求的（如RSA密钥长度小于2048为、使用MD5、SHA-1等不安全算法）将拒绝签发证书。

4.5.2 密钥管理服务

国汽智联不向订户提供签名私钥托管服务。

4.5.3 安全事件反馈

国汽智联建立外部安全事件反馈渠道，及时受理和处理证书信息错误、私钥失密或证书被盗用等异常情况。

渠道如下：

电子邮箱地址：cps@china-icv.cn；

电话号码：010-57705900；

传真号码：010-57705907。

4.6 证书密钥更新

证书密钥更新是指订户生成新密钥并申请为新公钥签发新证书。

4.6.1 证书密钥更新的情形

1、当订户证书即将到期或已经到期时；

2、当订户证书密钥遭到损坏时；

3、当订户证实或怀疑其证书密钥不安全时；

4、其它可能导致密钥更新的情形。

4.6.2 请求证书密钥更新的实体

请求证书更新的实体为已申请过国汽智联证书的订户。

4.6.3 证书密钥更新请求的处理

同 3.3。

4.6.4 颁发更新证书时对订户的通告

同 4.3.2。

4.6.5 构成接受密钥更新证书的行为

同 4.4.1。

4.6.6 CA 对密钥更新证书的发布

同 4.4.2。

4.6.7 CA 对其他实体的通告

同 4.4.3。

4.7 证书变更

4.7.1 证书变更的情形

证书变更是指证书订户的关键信息有变更，导致证书内容有变化，需要重新制作证书的情形。

4.7.2 请求证书变更的实体

持有国汽智联证书的订户，都可以请求证书变更。

4.7.3 处理证书变更的请求

国汽智联不支持订户使用原有公钥进行证书变更，即订户对证书进行变更时其密钥对必须重新生成，因此国汽智联使用证书密钥更新过程来处理订户的证书变更请求。证书变更须对订户身份标识和鉴别，使用原始证书身份验证相同的流程。

4.7.4 通知订户新证书的签发

同 4.3.2。

4.7.5 构成接受变更证书的行为

同 4.4.1。

4.7.6 CA 对变更证书的发布

同 4.4.2。

4.7.7 CA 对其他实体的通告

同 4.4.3。

4.8 证书吊销和挂起

4.8.1 证书吊销的情形

如有下列情况中的任何一种情况发生，则订户的证书将被吊销：

1)订户书面申请吊销数字证书；

2)订户通知 CA 最初的证书申请未经有效授权；

3)订户相信或怀疑密钥泄漏或遭受攻击，存放证书的服务器损坏或被锁定等情形；或者 CA 有证据表明订户证书私钥泄露的情形；

4）当 CA 有证据表明订户将证书使用于法律、行政法规定义为非法事项上，或者 CA 发现订户证书未恰当使用；

5）当 CA 有证据表明订户未履行国汽智联 CPS 或订户协议中约定的义务；或者订户证书不符合国汽智联 CPS 的相关要求；

6）当 CA 有证据表明订户已丧失证书中域名的使用权，或订户未能更新其域名使用权；

7）CA 获知通配符证书被用于验证具有欺诈误导性质的域名；

8）国汽智联取得了合理证据表明或意识到订户证书中的重要信息内容已经变更；

9）CA 正式签发时未能满足证书策略或证书标准中的要求和条件，或者证书中的任何信息不准确；

10）CA 认定证书中所显示的信息为不准确或具有误导性；或者订户申请证书时，提供的资料不真实；

11）国汽智联因某些原因停止业务，并且没有安排其他的 CA 提供证书吊销服务；

12）当国汽智联从事电子认证业务的资格被吊销后，国汽智联除继续维持 CRL/OCSP 信息库的情况外，将吊销或终结所有已签发的证书；

13）国汽智联用于签发证书的 CA 证书私钥可能被泄露时，将根据应急预案吊销所有已签发的证书；

14）国汽智联取得了合理证据表明或意识到订户已经被列在相关的黑名单中，或其经营地区被国汽智联所在国家的监管机构禁止；

15）证书的重要参数被国际国内主流标准认为有重大风险时；

16）法律、行政法规规定的其他情形。

4.8.2 请求证书吊销的实体

已申请国汽智联证书的订户可请求证书吊销。

同时，国汽智联也可在4.8.1 所述的情形下主动吊销订户的证书。

4.8.3 证书吊销请求的处理程序

证书吊销请求的处理采用与原始证书签发相同的过程:

a)证书吊销的申请实体到国汽智联按要求填写《国汽智联机构证书申请表》，勾选“撤销”选项；

b)国汽智联对订户提交的吊销请求进行审核；

c)国汽智联吊销订户证书后，国汽智联将通知订户证书被吊销；

d)强制吊销是指当国汽智联确认订户有违反本 CPS 的情况发生时，对订户证书进行强制吊销，吊销后将立即通知该订户；

e)证书吊销信息在 24 小时内发布。

4.8.4 吊销请求的宽限期

如果出现私钥泄露等事件，订户必须在发现泄露或有泄露嫌疑 8 小时内提出撤销请求。其他原因引起的撤销请求订户必须在 48 小时内提出。

4.8.5 CA 处理吊销请求的时限

证书撤销的申请实体到国汽智联按要求填写《国汽智联机构证书申请表》，国汽智联在对撤销请求审核通过后实时处理。国汽智联 24 小时内将最新的 CRL 发布到目录服务器指定的位置，供订户和依赖方查询下载。

4.8.6 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。

4.8.7 CRL 发布频率

国汽智联可采用实时或定期的方式发布 CRL。国汽智联一般每 24 小时签发一次 CRL。

4.8.8 CRL 发布的最大滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.8.9 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。

4.8.10 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。

4.8.11 密钥损害的特别要求

除本文 4.8.1 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。

4.8.12 证书挂起

国汽智联暂不提供证书挂起服务。

4.9 证书状态服务

4.9.1 操作特征

国汽智联通过目录服务器和证书在线状态查询服务系统为各参与方提供证书状态查询服务。

4.9.2 服务可用性

证书状态服务必须保证 7×24 小时可用。

4.10 停止使用认证服务

停止使用认证服务是指当证书有效期满或证书撤销后，该证书的服务时间结束。停止使用认证服务包含以下两种情况：

a) 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，视为停止使用认证服务；

b) 在证书有效期内，证书被撤销后，即停止使用认证服务。

停止使用认证服务后，订户不得继续使用证书及私钥。

停止使用认证服务后，国汽智联将归档用户数据。

4.11 密钥生成、备份与恢复

为保证订户密钥的安全性，订户应在安全的环境下独立生成密钥对，并将生产的密钥通过加密等手段存储在安全的介质中，订户应及时备份密钥，并确保备份密钥的安全性，以防密钥丢失。在生成密钥对之后与安装服务器证书之前的时期内不应更改服务器的任何配置，以防密钥丢失。在密钥丢失或可能泄漏后，需及时申请密钥更新。

在订户委托其他可信服务商代替订户生成密钥对的情况下，应要求服务商承担相应的保密责任。

5. 认证机构设施、管理和操作控制

本章节参见相关 CPS 第5章内容。

北京经济技术开发区融兴北

6. 认证系统技术安全控制

本章节参见相关 CPS 第6 章内容。

7. 证书、证书吊销列表和在线证书状态协议

本章节参见相关 CPS 第7章内容。

8. 认证机构审计及相关评估

本章节参见相关 CPS 第8章内容。

9. 法律责任和其他业务条款

本章节参见相关 CPS 第9章内容。

。