电子认证业务规则

(CPS)

版本 V1.4

发布日期：2026 年 6 月 29 日

生效日期：2026 年 8 月 17 日

国汽(北京)智能网联汽车研究院有限公司
China Intelligent and Connected Vehicles (Beijing) Research Institute Co.,Ltd

版本控制表

版本	状态	修改说明	变更人	审核/批准	生效期
1.0	新建	新建《国汽智联电子认证业务规则》	房骥 林立森 刘建行	国汽智联 安全策略 管理委员会	2020 年 12 月 10 日
1.1	修订	1) 1.4.1 根据现有 CA 系统调整了证书类型； 2) 5.4.2 明确了各类审计日志处理\归档周期； 3) 4.6、4.8 明确了证书更新及变更，必须更新密钥；	刘建行 林立森 杨广渊	国汽智联 安全策略 管理委员会	2021 年 06 月 03 日
1.2	修订	调整 CPS，不再提供“个人证书”相关业务。 1) 在以下章节中删除“个人证书”相关内容：1.3.3、1.4.1、3.2.4、3.3.2、3.4、4.1.1、4.6、4.8.3、4.9.3、4.9.5、9.9.3。 2) 删除原 3.2.3 节 个人订户身份的鉴别。	刘建行	国汽智联 安全策略 管理委员会	2021 年 12 月 1 日
1.3	修订	1） 更新 1.5.2 节 联系人； 2） 更新 2.1 节 LDAP 地址 3） 更新 5.1.1 节 场地位置与建筑； 4） 更新 5.1.4 节 水患防治	张相雨	国汽智联 安全策略 管理委员会	2025 年 9 月 28 日
1.4	修订	根据 T/CQAE 11034-2025 进行调整	张相雨	国汽智联 安全策略 管理委员会	2026 年 8 月 17 日

目　录

1 概括性描述

1.1 承诺

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”）开展经营和服务活动时，遵守法律、行政法规，树立以人民为中心的服务理念，承担社会责任；

与客户建立业务关系前，开展应用业务调研，建立应用接入风险评估及内部定责机制，严禁为存在违法违规风险的业务提供电子认证服务；

使用经过国家密码管理局审查的电子认证服务系统开展电子认证服务；

接受政府和社会监督，对主管部门检查发现的问题及时整改，建立问题纠治长效机制，持续符合整改要求。

1.2 基本信息

国汽（北京）智能网联汽车研究院有限公司，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，法定代表人张进华。国汽智联于 2020 年 7 月开始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、车联网通信实体提供身份认证及安全防护服务，系统全面地保障智能网联汽车/车联网的安全。

国汽智联已取得《电子认证服务许可证》等许可证书，证书编号：ECP11030222058，发证机关：中华人民共和国工业和信息化部，批准日期：2022 年 4 月 15 日，有效期起止日期：2022 年 4 月 15 日至 2027 年 4 月 14 日。

证书链-一级根证书信息。证书序列号：69e2fec0170ac67b，颁发机构名称：CN＝ROOTCA　O＝NRCAC　C＝CN，密码算法：SM2，密钥长度：256 位，有效期：2012 年 7 月 14 日 11:11:59 到 2042 年 7 月 7 日 11:11:59。

证书链-二级根证书信息。证书序列号：28265f9116cd73d731b2731219a1fa14，颁发机构名称：CN = ROOTCA　O = NRCAC　C = CN，密码算法：SM2，密钥长度：256 位，有效期：2020年12月30日 14:50:17 到2040年12月25日 14:50:17，计划服务时间：2020年12月30日 14:50:17 到2039 年12月25日 12:00:00。

电子认证业务规则（CPS，Certification Practice Statement）是电子认证服务机构（CA，Certificate Authority）对所提供的认证及相关业务的全面描述。

国汽智联严格按照《中华人民共和国电子签名法》、《电子认证服务管理办法》、《电子认证服务密码管理办法》等电子认证服务行业的相关法律法规和管理规定，遵循相关国家标准和规范的要求，制定了《国汽智联电子认证业务规则》，并报工业和信息化部备案。

《国汽智联电子认证业务规则》适用于国汽智联及其员工、注册机构、订户、依赖方和其他参与者。各参与方必须完整地理解和执行本 CPS 所规定的条款，并承担相应的责任和义务。

1.3 文档名称与标识

本文档名称是《国汽智联电子认证业务规则》，简称《国汽智联 CPS》。

国汽智联向国家 OID 注册管理中心注册了相应的对象标识符（OID）为 1.2.156.115370，在本 CPS 中分配 OID 规则如下：

1） 国汽智联电子认证证书策略 CP 对象标识符：1.2.156.115370.1.1；

2） 国汽智联电子认证业务规则 CPS 对象标识符：1.2.156.115370.1.2。

1.4 电子认证活动参与方及其职责

1.4.1 电子认证服务机构

电子认证服务机构（CA）是对证书的签发、发布、续期、撤销等证书全生命

周期进行管理的实体，本文中仅指国汽智联。

1.4.2 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，订户为机构这种具有确定身份标识的主体或实体。

1.4.3 依赖方

使用或信任国汽智联所签发的证书进行交易的证书订户，以及依照本 CPS 在某些应用中信任证书真实性的所有实体被称为国汽智联的依赖方。依赖方可以是证书订户也可以不是证书订户。

依赖方在信任某个证书前须验证该证书是否有效（如通过 CRL 判断）而且应考虑到与信任该证书真实身份的附加条件，做出判断后才能继续操作。

1.4.4 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。

1.5 证书应用

1.5.1 证书类型及适合的证书应用

国汽智联签发的数字证书适合应用在订户信息化和电子商务等领域，用于证明订户在电子化环境中所进行的身份认证和电子签名，以及数据加密等服务。

国汽智联的数字证书包含机构基础级电子签名认证证书，具体如下：

a.机构基础级电子签名认证证书

机构基础级电子签名认证证书，用于需要区分、标识、鉴别机构身份的场景，适用于机构身份认证和电子签名，以及数据加密等服务。证书扩展项包含主管部

门制定发布的电子签名认证证书策略 OID。

证书类型	主管部门证书策略 OID	含义
机构基础级电子签名认证证书	2.16.156.339.2.1.2.1	适用于低风险业务、符合《电子签名法》的机构电子签名认证证书

1.5.2 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。

1.6 策略管理

1.6.1 策略文档管理机构

国汽智联安全策略管理委员会是《国汽智联电子认证业务规则》的最高管理机构。国汽智联安全策略管理委员会由管理层、PKI 技术人员等组成，具体成员名单在《国汽智联安全策略委员会工作职责规范》中公示。安全策略管理委员会

明确工作职责并妥善保存安全策略委员会重大决议的相关文件和会议记录。安全策略管理委员会负责 CPS 和 CP 以及配套制度的维护，包括但不限于以下职责：

a） 确定维护 CPS 和 CP 等策略文档的职能分工，建立合理有效的修订和批准流程；

b） 对涉及信息安全策略、根证书密钥、证书签发自动审核等重要操作和流程进行审批；

c） 每年至少进行一次 CPS 和 CP 全面评审，根据实际需要及时修订策略文档；

d） 每年组织运营风险评估并形成报告。

1.6.2 联系人

本 CPS 在国汽智联网站发布，对具体人员不另行通知。

网站地址：http://www.china-icv.cn；

电子邮箱地址：cps@china-icv.cn；

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；

邮政编码：100176；

电话号码：010-57705900；

传真号码：010-57705907。

1.6.3 CPS 批准程序

国汽智联的 CPS 由安全策略管理委员会指定的专人或编写组起草拟定后，提

交安全策略管理委员会审核通过后批准发布。如 CPS 需要修改，由安全策略管理委员会指定专人或编写组对 CPS 内容进行修订，安全策略管理委员会对提供的变动建议进行研究分析，并征询法律顾问有关意见后，形成最终决议。国汽智联将在决议形成后，在网站公布变更后的《国汽智联电子认证业务规则》正式文档，并在发布之日起 30 天内向工业和信息化部备案。

1.7 定义和缩写

下列定义适用于本 CPS：

a) 公共密钥基础设施（PKI）Public Key Infrastructure

PKI 利用公钥密码理论和技术实施和提供信息安全服务的普适性安全基础设施，是硬件、软件、人员、策略和操作规程的总和，完成证书的发放、管理和使用，并基于证书提供信息安全服务。

b) 电子认证业务规则（CPS）Certification Practice Statement

电子认证业务规则是电子认证服务机构对所提供的认证及相关业务的全面描述。

c) 电子认证服务机构（CA）Certification Authority

对证书的签发、发布、续期、撤销等证书全生命周期进行管理的权威第三方机构。

d) 注册机构（RA）Registration Authority

国汽智联 CA 机构承担 RA 机构的职能，主要职能包括：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销证书，处理订户撤销其证书的请求，同意或拒绝订户更新其证书或密钥的请求。国汽智联 CA 未授权外部 RA 机构履行上述职能。。

e) 电子签名认证证书（证书）Digital Certificate

由电子认证服务机构（CA）签名的包含公钥拥有者信息、公钥、签发者信息、有效期以及扩展信息的一种电子文件。

f) 证书撤销列表（CRL）Certificate Revocation List

由电子认证服务机构（CA）签发并发布的被撤销证书的列表，也称黑名单服务。

g) 注销列表（ARL）Certificate Authority Revocation List

一个经电子认证服务机构数字签名的列表，标记已经被注销的 CA 的公钥证书的列表，表示这些证书已经无效。

h) 私钥（电子签名制作数据）Private Key

非对称密码算法中指只能由拥有者使用的不公开密钥。签名者使用私钥对待签名数据做数字签名，得到签名值。

i) 公钥（电子签名验证数据）Public Key

非对称密码算法中可以公开的密钥。验证者使用签名者的公开密钥对签名值进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

2 信息发布与信息管理

2.1 认证信息的发布

国汽智联信息库面向认证服务各参与方提供信息服务，包括但不限于以下内容：

1） CPS、CP 的所有版本；

2） 证书链；

3） 证书信息、状态信息等查询服务；

4） 详细的业务办理指南，包括不限于服务网点地址、营业时间、联系电话等；

5） 依赖方协议；

6） 投诉处理政策及投诉方式，包括不限于：投诉处理部门的地址、联系电话、电子邮件地址，以及内部监督部门名称。

国汽智联信息库不会改变任何从电子认证服务机构发出的证书和任何证书撤销的通知，而是准确描述上述内容。处理任何与国汽智联相关的事宜时，必须使用国汽智联信息库作为主要的和正式的依据。

国汽智联通过网站公布以下信息：本 CPS 修订以及其他由国汽智联不定时发出的信息。信息发布内容如有变化，在变化生效后 1 个工作日内更新。国汽智联网址：http://www.china-icv.cn。

国汽智联通过目录（LDAP）服务器发布订户的证书和 CRL，各参与方可以通过访问国汽智联的目录服务器获取证书的信息和撤销证书列表。LDAP 地址为：ldap://36.110.106.147:389。

国汽智联提供在线证书状态查询服务（OCSP）。OCSP 地址为：

https://ocsp.china-icv.cn:8083/ocsp/。

国汽智联按照国家电子认证服务管理平台的要求进行了备案。

国汽智联已与国家电子认证服务管理平台的技术对接，实现根据证书唯一编码、订户身份信息等维度查询本机构已签发证书列表的功能。

2.2 发布时间或频率

国汽智联应在 http://www.china-icv.cn 上及时发布 CPS 的最新版本；

国汽智联签发的证书在订户收到证书后应实时发布；

国汽智联的 CRL 最迟 24 小时发布一次；

国汽智联应在 http://www.china-icv.cn 上实时发布其他与电子认证服务相关的公告和通知。

2.3 信息库访问控制

对于公开发布的信息，国汽智联允许各参与方通过网站或目录服务器进行查询和访问。

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

3.1 身份查验通用要求

3.1.1 通用要求

国汽智联在受理证书申请时，对订户和/或受托人进行充分告知、身份确认、意愿记录和协议签署；

国汽智联身份查验义务未委托给外部机构或个人（非属同一法人主体的机构视为外部机构）。

3.1.2 订户告知

1.告知内容

国汽智联明确订户申请证书时，告知一下内容：

a） 订户的权利和义务；

b） 服务收费的项目和标准；

c） 电子签名认证证书、电子签名的使用条件；

d） 信息安全保障措施；

e） CA 和订户的责任划分；

f） 订户签名私钥的存储方式及安全要求；

g） 订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

2.告知方式

国汽智联告知方式如下：

基础级证书采用强制阅读、短信、邮件等方式告知，并保留告知记录。

3.2 初始身份确认

3.2.1 证明持有私钥的方法

国汽智联按照 6.2.2 私钥传送给订户规定的方式生成订户密钥对。

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 机构订户身份的鉴别

国汽智联受理机构证书申请时的身份信息查验方式及内容：

1.机构有效证件，包括但不限于工商营业执照等仅限法律法规和国家有关文件规定的证件；

2.法定代表人或受托人身份信息查验

a）要求法定代表人出示其有效身份证件或有效身份证件信息，有效证件类型仅限法律法规和国家有关文件规定的身份证件。

b)国汽智联通过证件机读工具、权威数据库查验订户身份证件的真实性和有效性。

c)受托人办理时，查验机构加盖公章的有效书面授权证明；受托人出示其有效身份证件或有效身份证件信息，并按照 b）款方式查验法人和受托人的身份证件或身份资料。

3.机构基础级证书的实人查验

国汽智联对订户开展实人查验采用下列方式之一：

a)法定代表人实人查验采用核验电信运营商三要素的方式：核对姓名、证件号码、手机号在电信运营商的一致性，并通过对应手机号的随机短信验证码核验。

b)受托人实人查验采用核验电信运营商三要素的方式：核对姓名、证件号码、

手机号在电信运营商的一致性，并通过对应手机号的随机短信验证码核验。

国汽智联会完整记录并保存身份查验过程和结果，每张证书建立独立的身份验证记录。

3.3 订户意愿记录

3.3.1 订户意愿记录内容

国汽智联对订户意愿记录，内容包括但不限于：

a） 订户身份信息；

b） CA 的信息；

c） 签名私钥保存方及保存义务；

d） 订户对电子签名的法律责任；

e） 订户对上述 a)至 d）项内容已充分知晓并同意的明确意愿表示。

3.3.2 机构基础级证书的意愿记录

订户意愿的确认采用下列方式之一：

1.法定代表人申请时，采用强制阅读、短信或邮件确认等电子方式确认机构法定代表人的意愿。

2.受托人申请时，查验加盖机构公章的授权文件，采用强制阅读、短信或邮件确认等电子方式确认受托人的意愿。

国汽智联将保留完整、可追溯的订户意愿记录。

3.4 订户协议

订户协议包含以下内容：

a) 订户的权利和义务；

b) 服务收费的项目和标准；

c) 电子签名认证证书、电子签名的使用条件；

d) 信息安全保障措施；

e) CA 和订户的责任划分；

f) 订户签名私钥的储存方式及安全要求；

g) 订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

3.5 未验证的订户信息

证书载明信息的查验方法、查验流程按 3.1、3.2 执行。

对于没有验证过的订户信息，国汽智联将不承诺此类信息的真实性，并不承担由于此类信息引起的任何责任和解决纠纷的义务。国汽智联证书中不包含未经验证的订户信息。

3.6 互操作要求

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。

3.7 命名

3.7.1 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。

3.7.2 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。

3.7.3 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。

3.7.4 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。

3.7.5 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。

4 证书生命周期操作要求

4.1 通用要求

1. 国汽智联承担建立、运营和维护注册通道的责任。
2. 国汽智联承担与订户签订电子认证服务协议的责任。
3. 订户承担提供准确信息的责任。
4. 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

包含企业、事业单位、政府机构、社会团体等各类组织机构。任何合法的机构和有明确身份归属的其他网络主体均可申请证书，以保证网络作业的安全和可靠。

4.2.2 申请过程与责任

证书申请实体按照本 CPS 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。国汽智联依据§3 身份标识与鉴别，完成对订户的告知、身份确认、意愿记录、协议签署等动作，并依据既定准则批准或拒绝该申请。

国汽智联确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在 5 个工作日内处理证书申请。国汽智联能否在上述时间期限内处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了国汽智联的管理要求。因特殊情况需超期处理的，国汽智联将与订户协商确定处理时限。

4.3 证书签发

4.3.1 证书签发过程中电子认证服务机构的行为

国汽智联在批准证书申请之后，将签发证书。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。

通常，国汽智联所签发的证书在 24 小时内生效。

4.3.2 电子认证服务机构对订户的通告

国汽智联对订户的通告有以下几种方式：

a) 通过面对面的方式，通知订户到国汽智联领取证书；

b) 通过电子邮件（e-mail）方式或短信通知；

c) 邮政信函通知；

d) 其他国汽智联认为安全可行的方式。

国汽智联不提供上门为订户安装证书的服务。国汽智联提供热线支持服务。热线支持电话由国汽智联公布。

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。如拒绝接受证书，国汽智联将对已签发证书进行撤销操作，撤销流程详见 4.9 证书撤销或冻结。

国汽智联保存证书申请人是否接受证书的记录，包括接受时间、方式、操作人等信息。

4.4.2 电子认证服务机构对证书的发布

国汽智联在签发完证书后，将证书发布到数据库和目录服务器中。

国汽智联采用主、从目录服务器结构来发布所签发证书。签发完成的数据直接写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动复制到从目录服务器中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

其他实体可以通过从目录服务器中查询到国汽智联已经签发的证书。

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。

4.5.4 订户私钥和证书的使用

订户在提交了证书申请并接受了国汽智联所签发的证书后，均被视为已经同意遵守与国汽智联、依赖方有关的权利和义务的条款。订户接受了证书，应妥善保存其证书对应的私钥。

订户只能在指定的应用范围内，并按照证书内容对证书用途的约束（如密钥用途、密钥扩展用途）使用私钥和证书。并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

4.5.5 依赖方对公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份，并通过公钥验证对方电子签名的真实性和验证证书的有效性。在验证电子签名时，依赖方应准确知道签名的数据格式和信息范围，能确定什么数据已被签名。

验证证书的有效性包括三个方面的内容：

a) 用国汽智联的证书验证证书中的签名，确认该证书是国汽智联签发的，并且证书的内容没有被篡改；

b) 检验证书的有效期，确认该证书在有效期之内；

c) 查询证书状态，确认该证书没有被撤销。

4.6 证书续期

证书续期是指在不改变证书中订户的任何信息的情况下，为订户签发一张新证书。国汽智联不支持订户使用原有公钥进行证书续期，即订户对证书进行续期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续期请求。

证书续期申请人应为订户或其受托人。

证书续期须对订户身份标识和鉴别，若自申请人上次完成身份查验之日起至本次续期申请日未满三年，可使用有效的原证书进行电子签名验证的方式进行确认。否则应按照 3.2 的规定重新进行身份查验。

证书签发与接受的流程符合 4.3 和 4.4 的规定。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

a) 证书的有效期将要到期；

b) 因私钥泄漏而撤销证书；

c) 证书无法继续获得信任；

d) 证书无法正常使用；

e) 证书丢失；

f) 订户自主提出更新；

g) 国汽智联因法律法规、行业政策或自身策略要求更新。

4.7.2 请求证书密钥更新的实体

持有国汽智联证书的订户，都可以请求证书密钥更新。申请人为订户或其受托人。

4.7.3 证书密钥更新请求的处理

处理证书密钥更新请求采用人工方式，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，详见§3.2.2 机构订户身份的鉴别。由国汽智联来处理证书更新请求，为订户制作新的证书。订户注册信息没有发生变化的，国汽智联可以依据原注册信息对其签发新的证书。

证书签发流程符合§4.3 证书签发。

4.7.4 颁发新证书对订户的通告

人工更新方式，对订户的通告有以下几种方式：

a) 通过面对面的方式，通知订户到国汽智联领取证书；

b) 通过电子邮件（e-mail）方式或短信通知；

c) 邮政信函通知；

d) 其他国汽智联认为安全可行的方式。

4.7.5 构成接受密钥更新证书的行为

同§4.4.1 构成接受证书的行为。

4.7.6 电子认证服务机构对密钥更新证书的发布

同§4.4.2 电子认证服务机构对证书的发布。

4.7.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3 电子认证服务机构在颁发证书时对其他实体的通告。

4.8 证书变更

4.8.1 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。

4.8.2 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。申请人为订户或其受托人。

4.8.3 证书变更请求的处理

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，详见§3.2.2 机构订户身份的鉴别。若发起方不是证书订户，国汽智联需取得订户同意。

证书签发流程符合§4.3 证书签发。

4.8.4 构成接受更新证书的行为

同 § 4.4.1 构成接受证书的行为。

4.9 证书撤销或冻结

4.9.1 证书撤销的情形

a) 发生下列情形之一的，订户应当申请撤销证书：

证书私钥泄露；

证书中的信息发生重大变更；

认为本主体或实体不能实际履行国汽智联 CPS。

b) 发生下列情形之一的，国汽智联可以撤销其签发的证书：

订户申请撤销证书；

订户提供的信息不真实；

订户没有履行双方合同规定的义务；

证书的安全性得不到保证；

法律法规和行业政策规定的其他情形。

4.9.2 请求证书撤销的实体

根据不同的情况，订户、受托人、依赖方、国汽智联、司法机关及其他公权力机关可以请求撤销订户证书。

4.9.3 撤销请求和审核的流程

证书撤销请求的处理采用与原始证书签发相同的过程:

a) 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》，勾选“撤销”选项，记录影响证书或私钥安全的事件（如密钥遗失、泄露等）。国汽智联同时提供热线电话等便捷渠道。

b) 国汽智联对订户提交的撤销请求进行审核，详见§3.2.2 机构订户身份的鉴别。审核完成后做出是否受理的决定。

c) 国汽智联撤销订户证书后，国汽智联将通知订户证书被撤销。

d) 强制撤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撤销，撤销后将立即通知该订户。

e）证书撤销信息在 24 小时内发布。

f）国汽智联将保留处理流程的相关信息。

4.9.4 电子认证服务机构处理撤销请求的时限

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。

4.9.5 依赖方检查证书撤销的要求

在具体应用中，依赖方必须使用以下两种功能之一进行所依赖证书的状态查询：

a) CRL 查询：利用证书中标识的 CRL 地址，查询并下载 CRL 到本地，进行证书状态的检验。

b) 在线证书状态查询：服务系统接受证书状态查询请求，证书状态查询结果经过签名后，返回给请求者。

依赖方应验证 CRL 的可靠性和完整性，确保是经国汽智联发布并且签名的。

4.9.6 CRL 的颁发频率

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。

4.9.7 CRL 发布的最长滞后时间

发布的最长滞后时间为 24 小时。

4.9.8 证书冻结

国汽智联暂不提供证书冻结服务。

4.10 证书状态信息服务

4.10.1 证书状态信息服务方式

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。

4.10.2 服务可用性

国汽智联提供 7×24 小时的证书状态查询服务，服务响应时间在 1 秒以内，服务可用率不低于 99%。即在网络允许的情况下，各参与方能够实时获得证书状态查询服务。

当在线证书状态信息服务不可用时，提供备用查询机制，各参与方可通过电话形式查验，联系电话：010-57705900。

4.11 停止使用认证服务

1.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。

2.停止使用认证服务后，国汽智联将立即撤销证书，并在 24 小时内发布 CRL。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。

3.知识产权和保密条款继续有效；因未及时报告密钥丢失、未终止使用证书，非法使用证书或错误信赖证书造成损失的，订户或依赖方仍需承担赔偿责任。

4.国汽智联将完整记录操作过程。

4.12 密钥托管与恢复

4.12.1 密钥的托管

国汽智联根证书私钥不会托管给任何第三方机构或个人，保证在自身控制的安全环境中保管。

4.12.2 密钥的备份与恢复

国汽智联建立根证书密钥备份与恢复策略，对根证书密钥进行安全备份。

5 电子认证服务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

国汽智联电子认证服务系统的机房位于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日新楼 1 层。场地具有三道物理防护，以监控和管理国汽智联机房的物理通道。北京当地发生地震等自然灾害的概率较小，机房具备独立的防震、防火、防水、温控、门禁系统、视频监控系统和警报系统等，可以保证电子认证服务的连续性和可靠性。

机房采用高安全性的监控技术，包括视频、指纹、门禁等安全管理手段，以确保物理通道的安全。进入国汽智联机房时，有延时报警门禁系统。机房实行全天候自动监控。监控记录文件包括对机房通道上的所有踪迹的记录。所有进入国汽智联机房的来访者只有经过批准后，经由国汽智联人员陪同，才能在限制区域内活动。

国汽智联的建筑物和机房建设按照下列标准实施：

a) GB 50174-93：《电子计算机机房设计规范》；

b) GB 2887-89：《计算站场地技术条件》；

c) GB 9361-88：《计算站场地安全要求》；

d) GB 6650-1986：《计算机机房用活动地板技术条件》；

e) GB 50034-1992：《工业企业照明设计标准》；

f) GB 5054-95：《低压配电装置及线路设计规范》；

g) GHN 19-87：《采暖通风与空气调节设计规范》；

h) GB 157：《建筑防雷设计规范》；

i) GHN 79-85：《工业企业通信接地设计规范》。

5.1.2 分区管理与访问控制

为保证本系统的安全，采取了一定的隔离、控制、监控手段。机房通过设置门禁和侵入报警系统来保护机房物理安全。

安全区域划分为 6 个区域，包括：

（1）管理区：服务区服务器管理维护。

（2）屏蔽监控区：包括视频监控、门禁控制系统等。

（3）服务区：部署证书注册管理服务器（RA）及其数据库（RADB）、OCSP、从 LDAP 服务器、服务器加密机、入侵检测及防火墙等设备。

（4）CA 核心区：物理和逻辑上都高度隔离的安全区域，主要职责是管理数字证书的整个生命周期，包括证书的签发、续订、发布和吊销。

（5）KM 核心区：负责所有加密密钥的生命周期管理，包括密钥的生成、存储、分发、轮换、备份、恢复和销毁。

（6）缓冲区：屏蔽机房的物理缓冲隔离区域，核心区服务器管理维护。

物理访问控制包括如下几个方面：

a) 门禁系统：所有区域部署门禁系统，工作人员需使用门禁卡结合指纹鉴定才能进出，系统保留时间记录和信息提示，核心区和缓冲区物理访问实施“双人共管”和“双因素认证”的强制访问控制策略。

b) 报警系统：所有区域部署报警系统，当发生任何非法闯入、非正常手段开门、长时间不关门等异常情况都会触发报警系统。

c) 监控系统：所有区域部署监控系统，对国汽智联机房进行 24 小时不间断

录像，系统保留录像资料，以备查询。

5.1.3 电力与空调

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

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

根据机房环境及设计规范要求，均设置了空气调节系统。空调系统由空调、通风管路、新风系统组成。国汽智联保持相对湿度在 40%-60%范围内，保持温度在 18-28℃范围内。

国汽智联参照电信设施管理的规定进行维护和保养。

5.1.4 水患防治

国汽智联机房位于建筑物 1 层，机柜架空离地，机房内无上下水系统，空调间做了严格防水处理，发生水患的可能性很小。

国汽智联机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

5.1.5 火灾预防和保护

机房所在建筑物的耐火等级符合 GHN 45《高层民用建筑设计防火规范》中规定的二级耐火等级，通过了国家权威部门的消防测试。国汽智联设施内设置火灾报警装置。在机房内、各物理区域内、活动地板下、吊顶里、主要空调管道中

及易燃物附近部位设置烟、温感探测器。每年进行一次消防安全检测。机房采用防火材料建设，配置独立的气体灭火装置，使用专业的灭火系统，备有相应的气体灭火器，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂，并配备专用氧气呼吸器。工作区配置水喷淋灭火装置。国汽智联通过与专业防火部门协调，建立了消防灭火等应急响应措施。

5.1.6 设备管理

国汽智联对机构内设备建立台账，设备台账包含每台设备的责任人、使用状态、维护周期和报废标准。定期进行设备盘点与核对，保持设备实际情况与设备台账相符。

5.1.7 存储媒体管理

数据的存储媒体包括硬盘、光盘、U 盘等，媒体存储地点保证物理安全，能够防磁、防静电干扰、防火、防水，由专人管理。制定详细的存储媒体使用、报废管理规定，规定包含使用权限、报废标准、销毁方法和审批流程。完整记录存储媒体领用、归还、报废等情况。

5.1.8 废物处理

当国汽智联存档的敏感数据或密钥已不再需要或存档期限已满时，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。

5.1.9 异地备份

国汽智联定期进行数据备份，备份数据保存于指定的保险箱。国汽智联对重要数据进行异地备份，异地备份地点位于天津市津南区海棠街道同德路 69 号开物芯港 4 号楼一层，直线距离约 109 公里。

5.2 操作过程控制

5.2.1 可信角色

基于认证服务的安全性需求，国汽智联 CA 及 RA 只有可信人员才能在安全性和敏感性高的岗位上工作，可信角色包括影响到以下操作的所有员工：

1.证书申请书中信息的鉴别。

2.证书申请、撤销请求、续期请求或其他业务的受理。

3.证书的发放、撤销和访问 CA 系统中受限制的部分。

4.对申请者信息和请求的处理。

国汽智联的可信人员包括但不仅限于：

1.系统维护管理员：负责系统策略配置、用户与权限管理等；

2.技术支持服务专员：负责物理环境、网络、服务器及系统软件的日常监控与维护等；

3.数据库管理员：负责数据库日常运维、性能优化及数据备份等；

4.系统审计员：负责系统和网络日志的审计、管理、审计报告生成等；

5.密钥管理员：负责根证书密钥材料管理、根证书密钥生存周期管理等；

6.业务操作员：负责证书申请的手里、审核，订户身份与意愿鉴证；

7.客户档案管理员：负责客户证书相关档案资料的归档与保密等；

8.运营审计员：负责对客户签发、客户服务等核心业务进行独立审计等；

9.网络安全管理员：负责网络设备维护、网络安全策略配置等。

5.2.2 职责分离

国汽智联遵循职责分离原则，所有涉及关键操作（密钥管理、审计、鉴证、系统管理）的角色实现双人操作或复核机制；涉及业务连续性的相关操作（运维、

鉴证、审计）的角色按工作量设置人员冗余，在任何一人缺岗时仍能实现双人操作；禁止同一人掌握可独立完成“发起、审批、执行、审计”全流程的任何组合，以下角色禁止相互兼任：

a)系统管理员、技术支持服务专员、数据库管理员、系统审计员之间不得兼任；

b）同一证书业务的录入与审核环节不得由同一业务操作员完成；

c）业务操作员、客户档案管理员、运营审计员之间不得兼任；

d）密钥管理员不得与系统管理员、技术支持服务专员兼任。

5.3 人员控制

5.3.1 资格、经历和无过失要求

所有的员工与国汽智联签订劳动合同和保密协议。对于充当可信角色或其他重要角色的人员，必须具备一定的资格，具体要求见相关人事管理制度。国汽智联要求充当可信角色的人员至少必须具备忠诚、可信赖及工作的热诚度、无影响CA 运行的其他兼职工作、无同行业重大错误记录、无违法记录等。

5.3.2 背景审查程序

背景调查分为：基本调查和全面调查。

基本调查包括对工作经历、职业推荐、教育、社会关系方面的调查。全面调查除包含基本调查项目外还包括对是否有无犯罪记录等调查。调查程序包括：

a) 用人部门通过面对面沟通互动、情景模拟等方式对其考察。

b) 人事部门负责对应聘人员的个人资料予以确认。提供如下资料：履历、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明。

c) 人事部门通过电话、信函、网络、走访等形式对其提供的材料的真实性进

行核查。

d) 核查合格后，经主管领导批准后准予上岗。

必要时，国汽智联可以与有关的政府部门和调查机构合作，对指定的可信人员进行背景调查。

5.3.3 培训要求

国汽智联对员工的一般培训内容为：证书基础知识、电子认证相关法律法规、国汽智联 CPS、规章制度、企业文化、岗位职责等。培训时长不少于 20 学时并通过考核。

针对特殊岗位员工，培训内容包括但不限于以下内容：国汽智联电子认证服务系统、身份验证和审核策略和程序、灾难恢复和业务连续性程序、电子认证服务项目管理、电子认证相关产品体系等。

5.3.4 再培训周期和要求

国汽智联策略调整、系统更新时，应组织员工进行继续培训，以适应新的变化。对于公司安全管理策略，每年至少进行 1 次培训；认证系统运营相关的人员，每年至少进行 1 次相关技能和知识培训。每人每年培训时长不少于 20 学时并通过考核。

国汽智联根据实际情况，对 PKI/CA 和密码技术的发展和演变，安排相应的培训。

培训内容至少包括：

1） 电子认证服务相关法律法规与标准；

2） 岗位通用职责要求及各角色特定的工作要求；

3） 内部管理政策、制度及流程等；

4） PKI 和密码技术基础知识；

5） CPS、CP；

6） 安全管理策略和机制；

7） 订户身份查验和审核策略、流程；

8） 电子认证服务运营体系构成；

9） 电子认证服务技术体系构成；

10） 灾难恢复和业务连续性管理。

5.3.5 工作轮换周期和顺序

对于可替换角色，国汽智联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。

5.3.6 对未授权行为的处罚

当国汽智联员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用国汽智联系统或进行越权操作，国汽智联得知后将立即对该员工进行工作隔离，并对该员工的未授权行为进行评估，根据评估结果按照公司规定进行相应处罚。对情节严重的，依法追究相应责任。

5.3.7 提供给员工的文档

为保障认证系统的正常安全运行，国汽智联应该给相关员工提供有关的文档，至少包括国汽智联 CPS、公司规章制度、岗位说明、相关培训资料以及与岗位相关的文档资料等。

5.4 审计日志程序

5.4.1 记录事件的类型

国汽智联以手动或自动记录的方式记录以下事件，载体为纸张或电子文档：

1.CA 密钥整个生命周期的管理事件：

-密钥的产生、备份、存储、恢复、归档、销毁。

-密码设备整个生命周期的管理事件，包括启用、停用、转移和销毁等。

2.CA 和订户证书整个生命周期的管理事件：

-证书申请、审核、签发、续期、密钥替换、撤销等。

-成功或不成功的请求处理。

-签发证书和 CRL。

3.系统访问行为：

-包括所有对系统的访问企图。

-包括成功的和失败的登录、退出、权限使用行为等。

4.系统操作与变更，包括系统的各种关键查询、修改等操作，系统权限创建、删除、设置或密码修改。

5.网络安全事件：

-包括防火墙、路由器、入侵安全检测设备记录的告警信息。

-针对被攻击事件识别与相应处理过程、结果。

6.CA 设施的访问记录：

-包括授权人员和非授权人员进出 CA 设施的记录。

每个事件记录包含时间、类型、内容、操作人、作用对象及结果。对系统的关键操作由操作人员进行电子签名。

日志审计内容为核实系统和操作人员的合规性，包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

5.4.2 处理日志的周期

国汽智联每天对巡视场地监控系统产生的各类报警事件进行记录并及时采取补救行动。

每月对 CA 系统的操作记录、访问记录、事件记录、系统数据进行审查和处理，对来自网络的入侵行为进行检测、分析和记录。

每季度对系统产生的各类记录和日志进行审查和分析。

5.4.3 审计日志的保存期限

审计日志的保存期限不低于相关证书失效后 5 年，实施严格的访问控制以防止篡改或删除。

5.4.4 审计日志的保护

国汽智联通过物理或逻辑的访问控制防止电子或手写的审计日志文档被未经授权的浏览、篡改、删除和其他损坏。所有审计日志处于严格的保护状态。

5.4.5 审计日志收集系统

国汽智联的审计收集系统采用自动及手动的收集方式，主要涉及以下系统：

a) 证书签发系统；

b) 证书注册系统；

c) 证书目录系统；

d) 访问控制系统；

e) 网站、数据库安全管理系统；

f) 其他需要审计的系统。

5.4.6 对导致事件实体的通告

国汽智联发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，国汽智联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。

国汽智联有权决定是否对导致事件的实体进行通告。

5.5 记录归档

5.5.1 归档记录的类型

归档记录包括所有审计数据、证书申请信息、与证书申请相关的信息和证书信息等，具体包括：

1） 证书申请材料和订户意愿记录；

2） 所有审计日志；

3） 密设备全生命周期管理记录；

4） 密设备的日常操作与使用记录；

5） 根书或密钥生命周期管理相关的全部记录；

6） 证认证系统运行日志；

7） 已识别的安全事件及处理记录；

8） 证书认证系统关键操作日志；

9） 电子认证服务过程中的其他记录。

5.5.2 归档记录的保存期限

除了法律法规和管理部门提出的保存期限外，国汽智联对与证书相关的归档记录至少保存到证书有效期结束后 5 年。与法律政策的规定不一致时，选择两者中较长的期限予以保存。

此外，在不违反法律法规和管理部门的规定的前提下，国汽智联可以自主决定信息的存档期限，并不对此做出说明和解释。

5.5.3 归档文件的保护

存档内容采用物理安全措施或密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。国汽智联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。

国汽智联保存的申请者和订户基本情况资料和身份鉴别资料，非经政府主管机构或者司法机构经过合法的途径予以申请，任意无关的第三方均无法获知。

5.5.4 归档文件的备份程序

所有存档的文件和数据库除了保存在国汽智联指定的存储库，还可以在异地保存其备份。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。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。国汽智联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

所有记录都要在存档时加具体准确的时间标识以表明存档时间，可以是系统自动标识的时间，也可以是操作员手工标注的时间，国汽智联不采用时间戳技术表明存档时间。

5.5.6 归档收集系统

国汽智联电子认证服务系统的相关运营信息，由内部工作人员或具备安全控制措施的内部系统，依照人工和自动操作两部分进行产生和收集，并由专人进行管理和分类。

5.5.7 获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。归档记录的一致性在归档时进行验证。归档期间，所有被访问的记录在归还时必须验证其一致性。

5.6 电子认证服务机构根证书密钥更替

1.密钥更替程序

1）密钥生成：在颁发或更新根证书时，在安全可靠的环境中生成新密钥对，具体见 6.2；

2）根证书发布：将新的 CA 公钥证书发布给证书订户和依赖方；

3）旧密钥处理：在完成签名密钥更替后，按照 GB/T25056-2018 中 8.2.4.3 规定的方式销毁旧私钥及其备份，并保留相关操作记录。

2.密钥更替时间：

1）紧急更替：发现密钥泄露或存在安全隐患，立即启动密钥更替程序；

2）到期更替：国汽智联将在根证书密钥到期前二年完成密钥更替。

5.7 损害和灾难恢复

5.7.1 业务连续性目标

国汽智联灾难恢复的恢复时间目标(RTO)为 44min，恢复点目标（RPO）为 2min。

5.7.2 事故和损害处理程序

发生故障时，国汽智联将按照应急恢复计划实施恢复。

5.7.3 计算资源、软件和/或数据被破坏

国汽智联遭到攻击，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，国汽智联将按照灾难恢复计划实施恢复。

5.7.4 实体私钥损害处理程序

当国汽智联证实 CA 私钥泄露后，应：

a） 向管理部门汇报，并启动电子认证服务机构密钥更替流程；

b） 立即停止使用该私钥签发证书，并撤销该私钥颁发的所有订户证书；

c） 通过网站、短信、电话通知和邮件等方式，告知证书订户和依赖方；

d） 机构密钥更替完成后，为受影响的订户重新签发证书。

5.7.5 根私钥应急处理

国汽智联建立根私钥泄露的应急流程，当 CA 私钥发生泄露事件，立即启动应急事件处理程序，由安全策略委员会和相关的专家进行评估，制定行动计划。每年进行一次应急演练。

1） 立即吊销 CA 证书、由此私钥签发的公钥证书，停止签发新的用户证书；

2） 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；

3） 发布证书吊销状态到证书库；

4） 在公司网站或其他通信方式发布关于吊销 CA 证书的处理通报；

5） 重新签发新的 CA 证书。

5.7.6 事件报告

国汽智联建立应急事件上报机制，具体见 5.9 重大事项报告。

5.7.7 灾难后的业务连续性能力

国汽智联的核心证书业务系统均采用双机热备方式，数据库采用磁盘阵列方式来确保证书服务的高可靠性和可用性。

国汽智联有异地数据备份，发生自然灾害或其它不可抗力性灾难后，国汽智联将利用备份数据重建系统恢复业务。

5.7.8 定期验证

国汽智联定期验证备份的设备、数据可用性，包括备份恢复测试和功能验证，每年进行一次灾难恢复演练。

5.8 电子认证服务机构终止

因各种情况，国汽智联需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

国汽智联在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于订户、依赖方等。

在终止服务六十日前向管理部门报告，按照相关法律规定的步骤进行操作。并与其他具有资质的电子认证服务机构就业务承接进行协商，签订承接协议，明确约定承接机构的工作范围与责任。向承接方移交密钥及相关关键数据，协调承接方启动相关运营工作。

若国汽智联未能就业务承接事项与其他电子认证服务机构达成协议，将向管理部门申请安排其他电子认证服务机构承接相关业务。

同时，国汽智联采取以下措施终止业务：

a) 起草国汽智联终止业务声明；

b) 停止认证中心所有业务；

c) 停止密码设备并处理加密密钥；

d)及时撤销或冻结业务管理员和业务操作员的操作权限；

e) 处理和存档敏感文件，对所有存档文件记录进行整理和封存；

f) 清除主机和密码硬件设备中的敏感数据；

g) 通知与国汽智联终止运营相关的实体。

5.9 重大事项报告

在重大事件发生5个工作日内，向上级机构和主管部门报告事件类型、时间、具体事件内容、处置措施和事件总结结论。

重大事件类型包括：

1.证书认证系统迁移或改造：包括系统软件、网络、部署的重大改变。符合以下任意之一：

1）机房迁移，或机房内服务区、管理区或核心区划设范围改变；

2）变更电子签名认证证书签发逻辑；

3）新增远程证书注册子系统；

4）新增、更改或者删除用于签发电子签名认证证书的证书链；

5）其他对电子认证服务安全、用户资料安全有影响的改变。

2.重大安全事故：包括电子认证服务系统遭受黑客攻击、病毒入侵、数据泄露等，导致系统无法正常运行或数据安全性受到严重威胁的情形。符合以下任意之一：

1）证书签发及验证服务连续停机时间超24h；

2）发生根证书密钥等关键数据泄露；

3）持续或较大范围未授权的私钥访问记录或其他异常活动；

4）系统日志持续或较大范围显示异常操作（如非授权时间或网络地址访问敏感功能）。

3.订户信息泄露事件：包括订户身份信息、证书申请资料等敏感数据被泄露等。符合以下任意之一：

1）个人信息泄露事件影响范围较广，造成一定的经济损失或客户投诉；

2）数据丢失导致无法恢复证书状态信息。

4.合规性实践：包括不符合相关法律法规、标准或监管要求的情形。符合以下任意之一：

1）涉及电子认证服务的司法判定；

2）收到行政部门违规通知或处罚决定。

5.人力资源类事件：包括一个月内核心管理层基体离职、大规模劳动纠纷、重大职场安全事件等。符合以下任意之一：

1）涉及 2 名及以上管理层人员或 10%以上可信人员的离职；

2）劳动纠纷参与人数超过员工总数 10%，且经法院或仲裁机构生效裁决确认由 CA 承担法律责任。

6 认证系统技术安全控制

6.1 技术安全管理制度要求

国汽智联已建立并实施覆盖密钥管理、系统开发、网络防护等领域的技术安全管理制度，并定期接受安全策略委员会的评审，频率不低于每年一次。

6.2 密钥对的生成和安装

6.2.1 密钥对的生成

a) CA 密钥对生成

国汽智联的 CA 密钥对在物理隔离的安全环境中，采用通过国家密码主管部门批准和许可的硬件密码设备中生成并存放在该密码设备中，采用（3，5）秘密共享机制将密钥份额分享给 5 个密钥管理员保管。CA 密钥对生成时，必须 5 个密钥管理员在场，分别将密钥份额存放在自己保管的密码设备中。CA 密钥对生成、备份、恢复、销毁过程在安全策略委员会授权下进行，过程实施 5 选 3 多人控制机制，并通过录音录像方式全程记录，保存期限不少于操作完成后十年。

b) 订户密钥对生成

订户签名密钥对由订户自主生成，生成和存储于符合国家安全标准的密码模块中；加密密钥对由国汽智联密钥管理中心（KMC）生成。国汽智联将完整记录所有与订户签名私钥相关的操作日志，包括时间、方式、操作人员等信息，保存期限不少于证书失效后五年。

6.2.2 私钥传送给订户

订户的签名密钥对由订户自己生成并保管。

加密密钥对由国汽智联密钥管理中心（KMC）产生，通过安全通道传送给订户。

6.2.3 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经 RA 传送到国汽智联 CA。订户的加密证书公钥，由 KMC 通过安全通道传送给国汽智联 CA。

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

6.2.4 电子认证服务机构公钥传送给依赖方

依赖方可以从国汽智联网站 http://www.china-icv.cn 下载根证书和 CA 证书，从而得到 CA 的公钥。

6.3 私钥保护和密码模块工程控制

6.3.1 密码模块标准和控制

国汽智联电子认证服务系统所用的密码设备是经国家密码管理部门许可和批准的产品。国汽智联所采用密码模块符合国家密码行业相关技术标准。符合 GB/T37092-2018 第 5 章的要求。

6.3.2 私钥的多人控制

CA 私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，将私钥的管理权限分散到 5 张管理员卡中，只有其中 3 至 5 人在场并许可的情况下，才能对私钥进行操作。

6.3.3 私钥托管

国汽智联不向订户提供私钥托管服务。订户应采取预防措施防止签名私钥及其激活数据的丢失、泄露、更改或未授权的使用。

订户加密密钥对由国汽智联密钥管理中心（KMC）托管，其生命周期管理由国汽智联密钥管理中心（KMC）进行规范和规定。

6.3.4 私钥备份

为了保证业务持续开展，国汽智联创建 CA 私钥的备份，以备进行灾难恢复操作。国汽智联的 CA 私钥在加密机中生成，备份形式包括加密机双机备份和加密导出备份，加密备份导出将 CA 私钥以加密的形式保存在硬件密码模块中，并存储于保险柜中。

国汽智联不提供订户签名私钥备份服务。订户加密密钥对由国汽智联密钥管理中心（KMC）备份，其生命周期管理由国汽智联密钥管理中心（KMC）进行规范和规定。

6.3.5 私钥归档

国汽智联对已过期的 CA 密钥对进行归档，归档的 CA 密钥对保存期至少为 5 年。归档的 CA 密钥不能用于其他用途，在归档期结束后国汽智联会对密钥进行销毁处理。

国汽智联不对订户提供私钥归档服务。

6.3.6 私钥导入或导出密码模块

CA 私钥的导出和导入，由至少 3 个密钥管理员分别登录加密机，通过加密机进行加密导出和导入。

对于订户，国汽智联提供将加密私钥安全传送给订户的方法，不提供订户私钥导出的方法。

6.3.7 销毁密钥的方法

国汽智联的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，加密设备必须被清空。同时，所有用于激活私钥的 PIN 码、IC 卡、动态令牌等也必须被销毁或者收回。销毁时由 3 名以上的密钥管理员共同在场，由操作员负责

清空硬件加密设备，完成密钥销毁。私钥归档的操作按照本 CPS 的规定处理。

6.3.8 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，接受其颁布的各类标准、规范、评估结果、评价证书等各类要求。根据国汽智联对产品性能、工作效率、供应厂商的资质等方面的评估，选择需要的模块。

6.4 密钥对管理的其他方面

6.4.1 公钥归档

公钥的归档，其操作过程、安全措施、保存期限以及保存策略和证书保持一致。归档要求参照本 CPS 中 § 5.5 记录归档的相关规定。

6.4.2 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都是 1 年，证书到期后，签名私钥不可用于电子签名。

根证书密钥对有效期为 20 年。

6.5 激活数据

6.5.1 激活数据的产生和安装

激活数据是私钥保护密码，证书存储介质（如：智能 USB KEY）出厂时设置缺省的 PIN 值。

6.5.2 激活数据的保护

订户应及时修改证书存储介质的默认 PIN 值，以确保安全。CA、证书订户妥善保管各自的激活数据，并采用安全的技术措施传输激活数据。

6.5.3 激活数据的其他方面

订户只有在拥有证书介质并知道证书介质的 PIN 值时才能激活证书存储介

质，进而使用私钥。

6.6 计算机安全控制

6.6.1 特别的计算机安全技术要求

为保证系统的正常运行，建立并实施符合 GB/T 25056-2018 中 8.2 要求的计算机安全控制体系，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：

a)每半年检查一次系统升级补丁，记录系统升级审批及实施过程；

b)对无官方补丁支持的系统，制定网络隔离、功能限制等加强防护措施和系统更替计划；

c)对所有服务器和操作终端安装杀毒软件；

d)病毒库每周更新；

e)病毒扫描每天进行。

6.6.2 计算机安全评估

国汽智联电子认证服务系统已通过国家密码管理局组织的安全性审查和安全技术鉴定。

6.7 生命周期技术控制

国汽智联建立并实施符合 GB/T 25056-2018 中第 10 章证书认证中心运行管理要求、第 11 章密钥管理中心运行管理要求、第 12 章证书操作流程要求的生存周期安全控制体系。

6.8 网络的安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据

库运行的安全。国汽智联采取防火墙、病毒防治、入侵检测、数据备份、灾难恢复等安全防护措施。国汽智联明确建立并实施符合 GB/T25056-2018 中 5.3.8 要求的网络安全控制体系，包括但不限于：

1.网络结构满足 GB/T 25056-2018 附录 A 中的“B/S 模式 CA 网络结构”。

2.对所有 Web 服务配置防火墙、Web 应用防火墙、入侵检测系统和内容过滤等网络安全防护措施。

3.建立并维护网络拓扑图，包含所有网络设备、连接关系和安全边界，定期更新，与机房实际情况保持一致。

4.网络访问控制：

1）建立针对证书签发子系统及数据库的访问白名单机制，仅授权证书注册子系统的必要功能模块及必要的管理设备进行访问；

2）建立针对证书注册子系统和数据库的访问白名单机制。

5.网络监控：

1）定期对系统日志进行分析；

2）分析内容包括系统异常、未授权访问尝试、资源使用异常、配置变更等安全事件。

6.9 时间戳

国汽智联电子认证服务系统产生的各种日志、操作记录都具有时间标识，但尚未采用时间戳技术保留上述记录的时间信息。

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

国汽智联签发的证书格式，符合 GB/T 20518《信息安全技术 公钥基础设施数字证书格式》或 GM/T 0015-2023《基于 SM2 密码算法的数字证书格式规范》或 ITU-T X.509 V3。

7.1.1 版本号

符合 X.509 V3 证书格式，这一版本信息存放在证书版本属性栏内。

7.1.2 算法对象标识符

a) 签名算法

SM3withSM2Encryption 对象标识符为：OID：1.2.156.10197.1.501

b) 摘要算法

SM3 的对象标识符位：OID：1.2.156.197.1.401

c) 非对称算法：.

SM2 对象标识符为：OID： 1.2.156.10197.1.301

d) 对称算法

本 CPS 建议使用国家密码管理部门认可的对称算法。

7.1.3 名称形式

国汽智联签发的证书，其名称形式符合 X.500 的甄别名格式。

7.1.4 证书策略对象标识符

国汽智联签发的证书包含主管部门制定的相应等级证书策略 OID2.16.156.339.2.1.2.1。

7.1.5 证书序列号

国汽智联为每张证书分配唯一标识符，在所签发的所有证书中具有唯一性。

7.1.6 证书有效期

国汽智联签发的证书有效期均为 1 年。

7.1.7 订户的电子签名验证数据

订户的电子签名验证数据为为订户签发的签名证书中的公钥。验证者使用订户签名证书的公钥对签名值进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

7.1.8 CA 的电子签名

国汽智联为每张电子签名证书和加密证书进行电子签名，用于确认证书的真实性。

7.2 证书撤销列表

国汽智联定期签发 CRL，供各参与方查询使用，CRL 格式符合 GB/T 20518-2018 中 5.3 要求。

7.2.1 版本号

证书撤销列表符合 X.509 V2 格式，此版本号存放在 CRL 版本格式栏目内。

7.2.2 CRL 和 CRL 条目扩展项

CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。

CRL 条目扩展项：不使用 CRL 条目扩展项

7.3 在线证书状态协议

国汽智联为订户提供 OCSP（在线证书状态查询服务），OCSP 作为 CRL 的有效补充，方便各参与方及时查询证书状态信息。OCSP 符合 GB/T 19713-2025 中第 7 章的要求。

7.3.1 版本号

使用 OCSP 版本 1（OCSP v1）。

7.3.2 OCSP 扩展项

未使用 OCSP 扩展项。

8 电子认证服务机构审计及相关评估

审计评估是为了检查、确认国汽智联是否按照 CPS 及其业务规范、管理制度和安全策略开展业务，发现存在的可能风险。审计评估分内部审计评估和外部审计评估。同时，按规定接受管理部门的评估和检查。

8.1 审计评估制度

国汽智联制定审计评估制度，制度内容包括但不限于：

1.国汽智联审计评估类型包括认证业务审计和全面符合性评估。

2.国汽智联每执行一次审计。

3.国汽智联在进行内部审计评估时，要求评估人员至少具备认证机构、信息安全审计评估的相关知识，有两年以上的相关经验，并且熟悉本 CPS 的规范，以及应具备计算机、网络、信息安全等方面的知识和实际工作经验。内部审计评估由国汽智联安全管理部组织实施。

国汽智联在进行外部审计评估时，选择专业、公正、客观的专业审计评估机构，要求评估者具备以下的资质：

a) 必须是经许可的、有营业执照的评估机构，在业界享有良好的声誉；

b) 了解计算机信息安全体系、通信网络安全要求、PKI 技术、标准和操作；

c) 具备检查系统运行性能的专业技术和工具。

4.审计评估对国汽智联经营管理活动进行风险识别、评估、分析、控制，依据国汽智联 CPS、安全策略、业务规范、管理制度以及管理部门的相关要求及技术规范开展。

8.2 认证业务审计

国汽智联认证业务审计周期为每年一次。审计内容包括但不限于证书申请、

续期、密钥变更、更新、撤销等业务中订户告知、身份查验、意愿记录、协议签署、资料保存的合规性。审计采用全面审计的方式。对于审计发现的问题，通知相关部门和人员及时整改，并跟踪整改落实情况。

8.3 全面符合性评估

国汽智联全面符合性评估周期为每年一次。审计内容包括但不限于年度电子认证服务开展情况、电子认证服务许可条件符合性情况以及认证规则和证书策略符合性情况。审计采用全面审计的方式。对于审计发现的问题，通知被审计部门及时整改，并跟踪整改落实情况。国汽智联将在 1 月底前将上一年度符合性评估报告报送主管部门。

9 法律责任和其他业务条款

9.1 费用

国汽智联根据市场情况和提供的电子认证服务内容，开展服务成本核算，制定价格策略，并在证书业务受理前公布各项服务收费标准。

9.1.1 证书签发和续期费用

国汽智联收取合理的证书签发和续期费用，并在订户订购时提前告知。

9.1.2 证书访问查询费用

国汽智联对证书访问查询，目前不收取任何费用。

9.1.3 证书撤销或状态信息的查询费用

国汽智联对证书撤销和状态查询，目前不收取任何费用。

9.1.4 电子签名费用

国汽智联不提供签名密钥托管服务，不收取电子签名费用。

9.1.5 签名验证费用

国汽智联不对外提供签名验证服务，不收取签名验证费用。如因证书申请、续期、变更、撤销等业务发生的签名验证工作，不收取签名验证费用。

9.1.6 签名验证报告费用

国汽智联不对外提供签名验证报告服务，不收取签名验证报告费用。

9.1.7 其他服务的费用

国汽智联保留收取其他服务费的权利。

9.1.8 退款策略

国汽智联对订户收取的费用，除了证书申请和续期费用因为特定理由可以退还外，国汽智联均不退还订户任何费用。

9.2 财务责任

国汽智联确保具有赔付专项备用资金来保证相应义务的履行，资金保障额度不低于上一年度电子认证业务相关营业收入的 1.5%，资金来源于上一年度电子认证业务相关营业收入，采用专款专用方式管理，合理地承担对订户及对依赖方的责任。

9.3 业务信息保密

9.3.1 保密信息范围

1) 保密信息包括国汽智联与订户、国汽智联与其他各参与方之间的协议、往来函和商务协定等。除非法律明确规定和国汽智联明确进行了书面许可，一般不能在未经另一方许可的情况下擅自公开。

2) 订户应该遵照本 CPS 的规定妥善保管私钥，如果因订户泄露私钥，订户应自行承担一切责任。

3) 国汽智联的内部和外部审计评估结果及相关信息是机密信息，除了国汽智联授权和信任的人员，不能泄露给其他任何人。这些信息除了审查目的或法律规定的目的，不能用于其他用途。

4) 国汽智联所有涉及系统运营的信息，都在保密范围之内。

5) 除非法律明文规定，国汽智联不会公布或透露订户证书中已经包括的信息以外的任何信息。

9.3.2 不属于保密的信息

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

订户证书及撤销信息通过国汽智联目录服务等方式向外公布。

9.3.3 保护保密信息的责任

国汽智联、订户、依赖方和其他各参与方，都有义务按照本 CPS 的规定，承担相应的保护保密信息的责任。

当保密信息的所有者出于某种原因，要求国汽智联公开或披露他所拥有的保密信息时，应书面授权以表示其自身的公开或者披露意愿，国汽智联应满足其要求。如该披露行为涉及任何其他方的赔偿义务和所造成的损失，应由保密信息的所有者承担，国汽智联不予承担。

9.4 个人隐私保密

9.4.1 隐私保密方案

国汽智联尊重所有订户及其隐私，个人隐私信息保密方案遵守现行法律和政策规定，具体措施参照 GB/T 35273 的规定

订户选择使用国汽智联的服务，就表示已经同意接受国汽智联有关隐私保护的声明。

9.4.2 作为隐私处理的信息

申请者提供的不构成证书内容的资料被视为隐私信息。

9.4.3 不被视为隐私的信息

申请者提供的用来构成证书内容的资料不认为是隐私信息。证书是公开的，通过国汽智联目录服务等方式向外公布。

9.4.4 保护隐私的责任

接收到隐私信息的参与者有责任保护隐私信息不被泄漏、使用或发布给第三方。

9.4.5 使用隐私信息的告知或同意

使用隐私信息，须征得本人同意。

9.4.6 依法律或行政程序的信息披露

当国汽智联在任何法律法规要求或者法院以及其它公权力部门通过合法程序的要求下，必须披露本 CPS 中规定的保密信息时，国汽智联可以按照法律法规或相关政策以及法院判决的要求，向执法部门提交相关的保密信息。国汽智联不承担任何责任。这种披露不能被视为违反了保密要求和义务。

9.4.7 其他信息披露情形

其他信息的披露遵循国家的相关规定处理。

9.5 知识产权

除非额外声明，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，包括所有权、名称权和利益分享权等。

按本 CPS 的规定，所有由国汽智联签发的证书和提供的软件中使用、体现和相关的一切版权、商标和其他知识产权均属于国汽智联所有，这些知识产权包括所有相关的纸质和电子文档。国汽智联的知识产权可以授权相关实体使用。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

国汽智联在提供电子认证服务活动过程中的承诺如下：

a) 国汽智联遵守《中华人民共和国电子签名法》及相关法律的规定，接受工业和信息化部监管，对签发的证书承担相应的法律责任。

b) 国汽智联保证使用的系统及密码符合国家政策与标准，保证其 CA 本身的签名私钥在内部得到安全的存放和保护，建立和执行的安全机制符合国家政策的规定。

c) 除非已通过国汽智联证书库发出了国汽智联的私钥被破坏或被盗的通知，国汽智联保证其私钥是安全的。

d) 国汽智联签发给订户的证书符合国汽智联 CPS 的所有实质性要求。

e) 国汽智联将向证书订户通报任何已知的、将在本质上影响订户的证书的有效性和可靠性事件。

f) 国汽智联将及时撤销证书。

g) 国汽智联拒绝签发证书后，将立即向证书申请人归还所付的全部费用。

h) 证书公开发布后，国汽智联向证书依赖方证明，除未经验证的订户信息外，证书中的其他订户信息都是准确的。

9.6.2 注册机构的陈述与担保

国汽智联的注册机构在参与电子认证服务过程中的承诺如下：

a) 提供给订户的注册过程完全符合国汽智联 CPS 的所有实质性要求。

b) 在国汽智联生成证书时，不会因为注册机构的失误而导致证书中的信息与证书申请者的信息不一致。

c) 注册机构将按 CPS 的规定，及时向国汽智联提交证书申请、撤销、续期等服务请求。

9.6.3 订户的陈述与担保

订户一旦接受国汽智联签发的证书，就被视为向国汽智联及依赖方作出以下承诺：

a) 订户需熟悉本 CPS 的条款和与其证书相关的政策，还需遵守订户证书使用方面的有关限制。

b) 订户在证书申请表上填列的所有声明和信息必须是完整、真实和正确的，

可供国汽智联检查和核实。

c) 订户应当妥善保管私钥，采取安全、合理的措施来防止证书私钥的遗失、泄露和被篡改等事件的发生。

d) 私钥仅为订户本身访问和使用，订户对使用私钥的行为负责。

e) 一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘、泄密以及其他情况，订户应及时通知国汽智联，申请采取撤销等处理措施。

f) 订户已知其证书被冒用、破解或被他人非法使用时，应及时向国汽智联申请撤销其证书。

9.6.4 依赖方的陈述与担保

依赖方必须熟悉本 CPS 的条款以及和订户相关的证书政策，并确保订户的证书用于申请时预定的目的。

依赖方在信赖订户的证书前，必须采取合理步骤，验证订户证书及数字签名的有效性。

依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本 CPS 的有关条款。

9.6.5 其他参与者的陈述与担保

其他参与者的陈述与担保同 § 9.6.4 依赖方的陈述与担保。

9.7 担保免责

有下列情况之一的，应当免除国汽智联之责任：

1) 如果证书申请者故意或无意地提供了不完整、不可靠或已过期的信息，又根据正常的流程提供了必需的审核文件，得到了国汽智联签发的证书，由此引起的经济纠纷应由证书申请者全部承担，国汽智联不承担与证书内容相关的法律和

经济责任，但可以根据受害者的请求提供协查帮助。

2) 国汽智联不承担任何其他未经授权的人或机构以国汽智联名义编撰、发表或散布的不可信赖的信息所引起的法律责任。

3) 国汽智联不承担在法律许可的范围内，根据受害者或法律的要求如实提供网上业务中“不可抵赖”的数字签名依据所引起的法律责任。

4) 国汽智联不对任何一方在信赖证书或使用证书过程中引起的直接或间接的损失承担责任。

5) 国汽智联不是订户或依赖方的代理人、受托人、管理人或其他代表。国汽智联和订户间的关系以及国汽智联和依赖方间的关系并不是代理人和委托者的关系。订户和依赖方都没有权利以合同形式或其他方法让国汽智联承担信托责任。

6) 由于客观意外或其他不可抗力事件原因而导致证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。关于不可抗力的描述参见 § 9.16.4 不可抗力。

7) 因国汽智联的设备或网络故障等技术故障而导致证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。本项所规定之“技术故障”引起原因包括但不限于：

不可抗力；

关联单位如电力、电信、通信部门而致；

黑客攻击；

设备或网络故障。

8) 国汽智联已谨慎地遵循了国家法律、法规规定的证书认证业务规则，而仍有损失产生的。

9.8 偿付责任规则

9.8.1 国汽智联的赔偿责任范围

如因国汽智联过错，发生证书信息错误、被伪造、篡改的，国汽智联承担赔偿责任，范围如下：

a) 证书信息与订户提交的信息资料不一致，造成订户损失。

b) 因国汽智联原因，致使订户证书无法正常使用，造成订户损失。

c) 国汽智联只在证书有效期限内承担损失或损害赔偿。

9.8.2 其他方的赔偿责任范围

订户和依赖方在使用或信赖证书时，若有任何行为或疏漏而导致国汽智联产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任：

a) 未向国汽智联提供真实、完整和准确的信息，而导致国汽智联或有关各方损失。

b) 未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用，而导致国汽智联或有关各方损失。

c) 在知悉证书密钥已经失密或者可能失密时，未及时告知国汽智联，并终止使用该证书，而导致国汽智联或有关各方损失。

d) 订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个数字签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。

e) 证书的非法使用，即违反国汽智联对证书使用的规定，而导致国汽智联或有关各方损失。

9.8.3 对最终实体的赔偿担保

国汽智联对所有当事实体（包括但不限于订户、依赖方）的合计责任不超过证书适用的责任封顶。对于一份证书产生的所有数字签名和交易处理，国汽智联对于任何人有关该特定证书的合计责任应该限制在一个不超出赔偿责任上限的范围内。

国汽智联所颁发证书的赔偿责任上限如下：

机构证书：2000 元人民币。

国汽智联依据所提供的电子认证服务内容确定对应的赔偿责任上限，并及时予以公布。

本条款也适用于其他责任，如合同责任、民事侵权责任或其他形式的责任。每份证书的责任均有封顶而不考虑数字签名和交易处理等有关的其他索赔的数量。当超过责任封顶时，可用的责任封顶将首先分配给最早得到索赔解决的一方。

国汽智联没有责任为每个证书支付高出责任封顶的赔偿，而不管责任封顶的总量在索赔提出者之间如何分配的。

9.8.4 赔付监督机制

1.流程监督。在收到订户的索赔申请，赔付流程发生时，客户服务部组织成立赔付监督小组，小组成员由客户服务部、安全管理部和运营管理部人员组成。

2.财务监督。由财务管理部负责，每年对国汽智联电子认证服务中心产生的赔付资金情况进行监督审查，对赔付案件与赔付资金的支出情况作出总结。

9.9 赔偿

国汽智联赔偿受理流程及时限如下：

1.申请人提出申请，国汽智联在 2 个工作提内判断真实性；

2.如判断真实，则要求申请人 2 个工作日内填写并提交《国汽智联电子认证

中心赔付申请单》，如超期未提交则视为申请人主动放弃赔偿申请；如判断不真实，则告知申请人相关原因并结束赔付流程。

3.国汽智联在收到申请人提交的《国汽智联电子认证中心赔付申请单》10 个工作日内对赔付申请进行审核。

4.如果审核通过，则告知申请人并于 30 个工作日内支付，支付完成后自动结束赔付流程；如果审核不通过，则告知申请人相关原因并结束赔付流程。

9.10 有效期限与终止

9.10.1 有效期限

本 CPS 自生效日期起正式生效。

本 CPS 中将详细注明版本号、发布日期、生效日期。

9.10.2 终止

当新版本的 CPS 正式生效时，旧版本的 CPS 自动终止。

9.10.3 效力的终止与保留

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

9.11 对参与者的个别通告与沟通

除非法律法规或者协议有特别的规定，国汽智联将以合理的方式与相关各方进行沟通，不会采取个别的方式进行。

9.12 修订和发布

9.12.1 修订程序

当 CPS 不适用时，由国汽智联安全策略管理委员会指定专人或编写组对 CPS 进行修订，修订程序同 1.6.3CPS 批准程序。

9.12.2 发布机制和期限

本 CPS 在国汽智联网站 http://www.china-icv.cn 上发布。

版本更新时，最新版本的 CPS 在国汽智联的网站发布，对具体订户、依赖方、其他参与者不做另行通知。

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 CPS。

9.13 争议处理与举证

9.13.1 电子认证服务相关的争议解决机制

订户、依赖方等关联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 CPS 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) 任何因与国汽智联就本 CPS 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。

9.13.2 举证制度和能力体系

举证制度和能力体系覆盖证书全生命周期，包括但不限于：

1.证书签发环节，身份验证记录、材料审查记录、告知记录、意愿确认记录等；

2.签名环节，签名请求验证、签名操作日志、时间戳记录等；

3.验证签名环节，验证请求记录、验证结果记录、异常情况处理记录等；

4.国汽智联将在 15 个工作日内提供举证材料。

9.14 管辖法律

本 CPS 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 CPS 的执行、解释、翻译和有效性均适用中华人民共和国的法律，包括不限于《中华人民共和国电子签名法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《商用密码管理条例》《电子认证服务管理办法》《电子认证服务密码管理办法》。

9.16 一般条款

9.16.1 完整协议

本 CPS 共包含 9 个章节，本 CPS 替代所有先前或同时期的相关文档。

订户协议及依赖方协议中标明对应的 CPS 版本。

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。

在电子认证服务活动中，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，可根据不可抗力的影响而部分或者全部免除违约责任。其他认证各方（如订户）不得提出异议或者申请任何补偿。

9.17 其他条款

国汽智联的安全策略管理委员会对本 CPS 拥有最终解释权。