北京数字认证股份有限公司

车联网（V2X）证书策略与电子认证业务规则

1.0.3 版

发布日期：2022 年 9 月 30 日

生效日期：2022 年 9 月 30 日

北京数字认证股份有限公司

版本控制表

版本	状态	修订说明	审核/批准人	生效时间
1.0.1	版本发布	新版本发布	公司安全策略管理委员会	2020 年 12 月 28 日
1.0.2	版本发布	根据车联网行业标准更新符合性描述	公司安全策略管理委员会	2022 年 8 月 17 日
1.0.3	版本发布	修订证书操作期和密钥对使用期限业务规则	公司安全策略管理委员会	2022 年 9 月 30 日

目录

1. 概括性描述

1.1. 概述

1.1.1. 公司简介

北京数字认证股份有限公司（Beijing Certificate Authority Co.,Ltd.，简称数字认证公司）于 2001 年 2 月开始运营，是权威、公正的电子认证服务机构。数字认证公司严格按照《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，提供数字证书签发、更新、撤销或管理等服务，并通过以 PKI 技术、数字证书应用技术为核心的车联网 V2X 应用安全解决方案，为车联网 V2X 领域构建安全、可靠的信任环境。

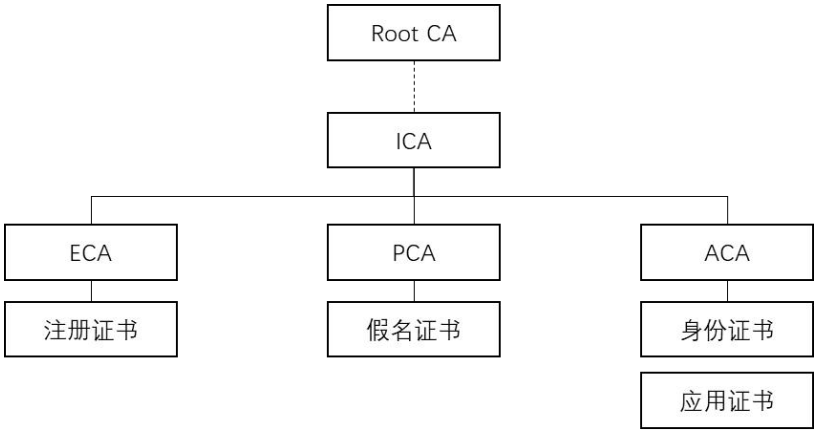
1.1.2. 证书策略与电子认证业务规则

北京数字认证股份有限公司车联网（V2X）证书策略与电子认证业务规则（以下简称《车联网证书策略与电子认证业务规则》）由数字认证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(试行)》制定，并报工业和信息化部备案。

本《车联网证书策略与电子认证业务规则》详细阐述了数字认证公司在实际工作和运行中所遵循的各项规范。本《车联网证书策略与电子认证业务规则》适用于数字认证公司、注册机构、认证授权机构、订户和依赖方，各参与方必须完整地理解和执行本《车联网证书策略与电子认证业务规则》所规定的条款，并承担相应的责任和义务。

1.1.3. 证书体系架构

本《车联网证书策略与电子认证业务规则》的证书体系有 1 个根证书，下设中级 CA 证书签发订户证书。



V2X证书体系示意图

Root CA 证书是本证书体系的根证书，Root CA 下设 ICA 证书，ICA 下设三级 CA 证书，其中：

（1）ECA 签发注册证书；

（2）PCA 签发假名证书；

（3）ACA 签发身份证书、应用证书。

1.2. 文档名称和标识

本文档的名称为《北京数字认证股份有限公司车联网（V2X）证书策略与电子认证业务规则》，简称《车联网证书策略与电子认证业务规则》。本文档的对象标识符为：1.2.156.112562.2.2.5。

1.3. 电子认证活动参与方及其职责

1.3.1. 电子认证服务机构

数字认证公司是根据《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（简称：CA 机构）。

CA 机构是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

1.3.2. 注册机构

注册机构（简称：RA 机构）是受理数字证书的申请、更新等业务的实体。

1.3.3. 认证授权机构

认证授权机构是车联网电子认证服务的组成部分，负责证书主体的身份认证和授权，为证书主体签发安全凭证，使其能够凭借获得的安全凭证与注册证书机构安全交互并获取注册证书。

CA 机构可以授权下属机构或委托外部机构（包括 VSP 服务商、汽车制造商、运营商等）作为认证授权机构，当 CA 机构授权下属机构作为认证授权机构时，VSP 服务商、汽车制造商、运营商等应向 CA 机构提供可信的身份标识，并保证其真实有效；当 CA 机构授权外部机构作为认证授权机构时，其应保证身份标识的真实有效，CA 机构应在与外部机构签署的合同中，明确双方的权利与义务，以及承担的法律责任。

1.3.4. 订户

订户即证书订户，是向 CA 机构申请数字证书的实体，通常为个人或机构。

需要明确的是，证书主体与证书订户是两个不同的概念。证书主体是指与证书信息绑定的实体，车联网证书中的证书主体通常是指受信任的车联网设备。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。

1.3.5. 依赖方

依赖方是指信赖于证书所证明的基础信任关系并开展业务活动的实体。

1.3.6. 其他参与者

其他参与者指为 CA 证书服务体系提供相关服务的其他实体。

1.4. 证书应用

1.4.1. 适合的证书应用

本规则下签发的数字证书适合应用在车联网领域，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等服务。

本规则下签发的数字证书类型包含注册证书、假名证书、身份证书和应用证书，具体如下：

a. 注册证书

面向车联网应用签发的一类特定通信证书，注册证书与设备唯一对应，适用于车载设备通过注册证书申请假名证书、身份证书；路侧设备、车联网服务提供商通过注册证书申请应用证书。

b. 假名证书

面向车联网应用签发的一类特定通信证书，假名证书签发给车载设备，用于签发其播发的主动安全消息。

c. 身份证书

面向车联网应用签发的一类特定通信证书，身份证书签发给车载设备，用于向路侧设备或车联网服务提供商证明其身份，以获得后者提供的某种车联网应用服务，例如警车与红绿灯进行交互，并控制后者的状态。

d. 应用证书

面向车联网应用签发的一类特定通信证书，应用证书签发给路侧设备或车联网服务提供商，用于签发其播发的某种应用消息，例如交通信号灯状态、交通信息、商业服务消息等。

1.4.2. 限制的证书应用

本 CA 机构发放的数字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。

1.5. 策略管理

1.5.1. 策略文档管理机构

本《车联网证书策略与电子认证业务规则》的管理机构是数字认证公司安全策略管理委员会。由数字认证公司安全策略管理委员会负责本《车联网证书策略与电子认证业务规则》的制订、发布、更新等事宜。

1.5.2. 联系人

本《车联网证书策略与电子认证业务规则》在数字认证公司网站发布，对具体个人不另行通知。

网站地址：http://www.bjca.cn

电子邮箱地址：cps@bjca.org.cn

联系地址:北京市海淀区北四环西路 68 号双桥大厦 15 层(左岸工社)(100080)

电话号码：8610-58045600

传真号码：8610-58045678

1.5.3. 决定 CPS 符合策略的机构

本《车联网证书策略与电子认证业务规则》由数字认证公司安全策略管理委员会组织制定，报数字认证公司安全策略管理委员会批准实行。

1.5.4. CP/CPS 批准程序

本《车联网证书策略与电子认证业务规则》由数字认证公司安全策略管理委员会，组织 CPS 编写小组。编写小组完成编写 CPS 草案后，由数字认证公司安全策略管理委员会组织对 CPS 草案进行初步评审。初步评审后，将 CPS 评审稿提交数字认证公司安全策略管理委员会审批。经数字认证公司安全策略管理委员会审批通过后，在数字认证公司的网站上对外公布。

本《车联网证书策略与电子认证业务规则》经数字认证公司安全策略管理委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

1.6. 定义和缩写

1.6.1. 定义

下列定义适用于本《车联网证书策略与电子认证业务规则》：

a） 车联网设备：本规则将车载设备（OBU）、路侧设备（RSU）和车联网服务提供商（VSP）的安全设备统称为车联网设备。

b） V2X 通信证书：本规则定义证书机构将签发给车联网设备的各种与 V2X 通信相关的证书，例如注册证书、假名证书、应用证书、身份证书等，统称为 V2X 通信证书。

c） 车载设备（OBU）：安装在车辆上，负责 V2X 通信的实体。

d） 路侧设备（RSU）：安装在路侧交通控制设备和交通信息发布设备中，负责 V2X 通信的实体。

e） 车联网服务提供商（VSP）：负责道路交通的管理机构和在车联网系统里提供某种商业服务的服务机构。

f） 公开密钥基础设施（PKI）：支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和不可否认性服务。

g） 证书策略与电子认证业务规则 (CPS)：关于电子认证服务机构在证书签发、证书更新(或密钥更新)、证书撤销或证书管理过程中所采纳的业务实践的声明。

h） 电子认证服务机构（CA）：受用户信任，负责创建和分配公钥证书的权威机构。

i） 根证书机构（Root CA）：负责 CA 系统根证书的管理与维护并对 V2X 证书机构进行注册审批，其签发管理机构的数字证书，使其成为系统内的有效实体。

j） 中间证书机构（ICA）：用于扩展 PKI 体系的层级，实现 CA 的多级部署和多级管理。

k） 注册证书机构（ECA）：负责向 OBU、RSU 和 VSP 等车联网设备签发注册证书。

l） 假名证书机构（PCA）：负责向 OBU 签发假名证书，OBU 使用假名证书对其播发的主动安全消息进行数字签名。

m） 应用证书机构（ACA）：负责向 OBU 签发身份证书，向 RSU 和 VSP 等车联网设备签发应用证书。

n） 注册机构（RA）：负责受理数字证书的申请、更新和注销等业务。

o） 异常行为管理机构（MA）：能够识别潜在的异常行为或故障，确定需要撤销的证书，生成证书撤销列表。

p） 数字证书(证书)：也称公钥证书，由电子认证服务机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期的一种数据结构。

q） 证书撤销列表(CRL)：一个经 MA 数字签名的列表，它指定了一系列证书颁发者认为无效的证书。

r） 证书可信列表（CTL）：一个经 Root CA 数字签名的列表，包含了所有机构证书的集合。

s） 私钥：非对称密码算法中只能由拥有者使用的不公开密钥。

t） 公钥：非对称密码算法中可以公开的密钥。

u） 身份标识（ID）：身份标识号是订户的唯一标识信息，在应用中相当于是一种“身份标识”，身份标识号一般是不变的。

1.6.2. 缩略语

缩写	英文全称	中文名称
AC	Application Certificate	应用证书
ACA	Application Certificate Authority	应用证书机构
CA	Certificate Authority	证书机构
CRA	Certificate Revocation Authority	证书撤销机构
CRL	Certificate Revocation List	证书撤销列表
CTL	Certificate Trust List	证书可信列表

EC	Enrolment Certificate	注册证书
ECA	Enrolment Certificate Authority	注册证书机构
ICA	Intermediate CA	中间证书机构
ID	IDentity	身份标识
MA	Misbehavior Authority	异常行为管理机构
OBU	On Board Unit	车载设备
PC	Pseudonym Certificate	假名证书
PCA	Pseudonym Certificate Authority	假名证书机构
PKI	Public Key Infrastructure	公钥基础设施
RA	Registration Authority	注册机构
RSU	Road Side Unit	路侧设备
TLS	Transport Layer Security	安全传输层性协议
VSP	V2X Service Provider	车联网服务提供商

2. 信息发布与信息管理

2.1. 认证信息的发布

数字认证公司通过网站公布以下信息：《车联网证书策略与电子认证业务规则》以及其他由数字认证公司不定时发出的信息。数字认证公司网址：http://www.bjca.cn。

本《车联网证书策略与电子认证业务规则》发布在数字认证公司的网站上，供相关方下载、查阅。

本 CA 机构的信息库面向订户及依赖方提供信息服务。提供信息服务包括但不限于以下内容：CPS、CP 以及数字认证公司不定期发布的信息。

2.2. 发布时间或频率

本 CA 机构的《车联网证书策略与电子认证业务规则》按照 1.5.4 所述的批准流程，一经发布到数字认证公司的网站，即时生效。

2.3. 信息库访问通知

对于公开发布的 CP、CPS 和 CA 证书等公开信息，本 CA 机构允许公众自行通过网站进行查询和访问。

只有经授权的 RA/CA 管理员可以查询 CA 机构和注册机构数据库中的其他数据。

3. 身份标识与鉴别

3.1. 命名

3.1.1. 名称类型

CA 机构颁发的数字证书含有颁发机构和证书主体标识名称，每个订户证书主体对应一个证书标识名称，是证书持有者的唯一识别名。

3.1.2. 对名称意义化的要求

在本规则下签发的数字证书，订户证书主体标识名称是唯一性元素，具有一定的代表意义，可识别证书用途。

3.1.3. 订户的匿名或伪名

在本规则下签发的证书可以接受匿名或者伪名。

3.1.4. 理解不同名称形式的规则

CA 机构签发的数字证书，其证书主体标识名称的命名规则由数字认证公司定义。

3.1.5. 名称的唯一性

在本规则下签发的数字证书，证书主体标识名称必须是唯一的。

3.1.6. 商标的承认、鉴别和角色

本 CA 机构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。

3.2. 初始身份确认

3.2.1. 证明持有私钥的方法

证明订户拥有私钥的方法是通过验证证书申请所包含的数字签名来完成的。

证明持有私钥的方法仅涉及订户申请注册证书的情况。CA 机构在为订户签发注册证书前，系统将自动使用订户的公钥验证其私钥签名的有效性和申请数据的完整性，以此来判断订户持有与所注册公钥相对应的私钥。

3.2.2. 个人身份的鉴别

个人订户在申请证书前应提供个人有效身份证件或证件的具体信息，包括但不限于：身份证、港澳台居民身份证、户口簿、护照、军官证等，提出证书申请。

CA 机构或授权的注册机构/认证授权机构将核实个人订户身份的真实性，鉴别方式可以采用面对面现场鉴别或远程鉴别。必要时，可以通过权威第三方数据库信息比对、手机短信验证等其他可靠的方式鉴别。

鉴别审核批准后，CA 机构或授权的注册机构/认证授权机构按照相关法律法规的要求妥善保存订户申请材料，CA 机构保存订户申请材料可以是纸质或电子数据形式。

本《车联网证书策略与电子认证业务规则》简要说明了如何进行个人身份鉴别。数字认证公司保留根据最新国家政策法规的要求更新个人身份鉴别方法与流程的权利。

3.2.3. 组织身份的鉴别

机构订户在申请证书前应提供组织有效身份证件或证件的具体信息，包括但不限于：营业执照、法人代码证、事业单位法人证书、社会团体登记证书、民办非企业登记证书、外国（地区）企业常驻代表机构登记证和政府批文等，提出证书申请。

CA 机构或授权的注册机构/认证授权机构将核实机构订户身份的真实性：

（1）订户提交的组织身份信息。鉴别方法包括核对订户提交的组织有效身份证件或证件的具体信息。必要时可以通过权威第三方数据库对身份证件信息进行比对。

（2）组织授予经办人的授权证明。鉴别方法包括但不限于检查组织或组织的法定代表人授权给经办人办理证书事宜的授权文件或授权条款，也可以通过银行对公账户打款附言或法定代表人手机短信验证方式核实。

（3）经办人的个人身份证明材料。

鉴别方式可以采用面对面现场鉴别或远程鉴别。当 CA 机构或授权的注册机构/认证授权机构认为有需要时，可以增加其他方式，包括但不限于鉴别组织的法定代表人身份或要求经办人提交法定代表人有效身份证件证明。

鉴别审核批准后，CA 机构或授权的注册机构/认证授权机构按照相关法律法规的要求妥善保存订户申请材料，CA 机构保存订户申请材料可以是纸质或电子数据形式。

本《车联网证书策略与电子认证业务规则》简要说明了如何进行组织身份鉴别。数字认证公司保留根据最新国家政策法规的要求更新组织身份鉴别方法与流程的权利。

3.2.4. 设备身份的鉴别

订户申请证书时，应提供真实有效的车联网设备身份信息，认证授权机构负责车联网设备身份鉴别、鉴别过程记录和证书申请信息的安全保管。

在请求注册证书时，应使用其规范的私钥和唯一身份标识信息进行初始认证，由认证授权机构进行认证。车联网设备在执行初始请求之前，通过车联网设备与

认证授权机构之间的安全通道将公钥和唯一身份标识信息带到认证授权机构。认证授权机构必须使用与订户相对应的公钥和第三方数据源来检查认证。

在请求假名证书、身份证书和应用证书时，车联网设备持有注册证书，使用其对应的私钥对请求进行签名，以证明自己的身份。签名由注册机构进行验证并确认验证结果。

3.2.5. 未经验证的订户信息

订户提交证书申请内容不属于鉴别范围内的信息，为没有验证的订户信息。

3.2.6. 授权确认

不适用。

3.2.7. 互操作准则

对于车联网设备与认证授权机构之间的通信，应确保车联网设备与认证授权机构之间连接的安全性。例如，可通过基于物理环境安全、TLS 安全协议或专用的端到端安全连接实现相关操作。RA 也必须支持这种安全通信。

3.3. 密钥更新请求的身份标识与鉴别

3.3.1. 常规密钥更新的标识与鉴别

在订户注册证书到期前，订户需获得新证书以保持证书使用的连续性。本 CA 机构一般要求订户产生一个新密钥对代替过期的密钥对，即视为常规密钥更新。

对于常规情况下的密钥更新申请，订户须提交已有的注册证书及含该证书签名的更新请求。

对更新请求的鉴别基于：

（1）原证书存在并由 CA 机构签发；

（2）用原证书上的订户公钥对申请的签名进行验证。

假名证书、身份证书和应用证书没有密钥更新服务。

3.3.2. 撤销后密钥更新的标识与鉴别

证书撤销后的密钥更新等同于订户重新申请证书，则撤销后密钥更新的标识与鉴别使用初始身份确认相同的流程，其要求与 3.2 节所述的相同。

3.3.3. 证书变更的标识与鉴别

车联网 V2X 证书没有证书变更服务。

3.4. 撤销请求的标识与鉴别

若因订户未履行本《车联网证书策略与电子认证业务规则》所规定的义务或由于本《车联网证书策略与电子认证业务规则》第 4.9.1 节所述理由，由本 CA 机构申请撤销订户的证书时，无需对订户身份进行鉴别。

4. 证书生命周期操作要求

4.1. 证书申请

证书申请是指订户向 CA 机构发起数字证书签发请求的过程。签发的数字证书类型包含注册证书、假名证书、身份证书和应用证书。其签发对象及适用范围详见本《车联网证书策略与电子认证业务规则》第 1.4.1 节。

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(包括国家机关、企事业单位、社会团体等)。

4.1.2. 申请过程与责任

4.1.2.1. 申请过程

订户按照本《车联网证书策略与电子认证业务规则》所规定的要求，通过现场面对面或在线方式提交证书申请，包括相关的身份证明材料。CA 机构或授权的注册机构/认证授权机构受理证书申请，依据身份鉴别规范对订户身份进行鉴别，并决定是否签发证书。

1. 注册证书申请：订户持有认证授权机构签发的安全凭证申请注册证书

a. 在线验证安全凭证的有效性和申请数据的完整性，如果验证未通过，CA 机构将拒绝为订户发放注册证书，并将未通过的信息存档。

b. 验证通过后，CA 机构根据证书请求签发注册证书。

c. 订户下载注册证书。

2. 假名证书/身份证书/应用证书申请：订户持有 CA 机构签发的注册证书申请假名证书或身份证书或应用证书

a. 在线验证注册证书的有效性和申请数据的完整性，如果验证未通过，CA 机构将拒绝为订户发放证书，并将未通过的信息存档。

b. 验证通过后，CA 机构根据证书请求签发相应的证书。

c. 订户下载相应的证书。

4.1.2.2. 各参与实体的责任

订户：订户需要提供 3.2 所述的有效身份电子数据，并确保电子数据真实准确，配合认证授权机构或注册机构完成对身份信息的采集、记录和验证。

认证授权机构：认证授权机构参照 3.2 的要求对订户的身份信息进行采集、记录，验证。通过鉴证后，认证授权机构向订户签发安全凭证。

注册机构：注册机构对订户的注册证书进行采集、记录和验证。通过鉴证后，注册机构向 CA 机构提交证书申请，由 CA 机构向订户签发证书。注册机构须接受 CA 机构的监督管理和审计。

CA 机构：CA 机构对认证授权机构或注册机构提交的证书申请信息进行采集、

记录和验证。通过鉴证后，CA 机构向订户签发证书。

根据《中华人民共和国电子签名法》的规定，订户未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给 CA 机构或依赖方造成损失的，应承担相应的法律责任。

4.2. 证书申请处理

4.2.1. 执行识别与鉴别功能

认证授权机构和注册机构有权利和责任对订户的身份进行合理的鉴别。

1、注册证书申请处理

在接到订户的注册证书申请后，认证授权机构应完成以下鉴别工作，将其作为向该订户签发证书的先决条件：

a. 按照车联网 V2X 证书的要求对订户的身份进行验证。

b. 确认订户合法的拥有与证书申请中所含公钥配对的私钥。

c. 确认订户是否已得到了合法授权。

2、假名证书/身份证书/应用证书申请处理

在接到订户的假名证书或身份证书或应用证书申请后，注册机构应完成以下鉴别工作，将其作为向该订户签发证书的先决条件：

a. 确认订户合法的拥有有效的注册证书。

b. 使用已验证的注册证书验证相应证书的申请请求签名。

4.2.2. 证书申请批准和拒绝

认证授权机构或注册机构根据本《车联网证书策略与电子认证业务规则》所规定的身份鉴别流程对订户身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果订户通过本《车联网证书策略与电子认证业务规则》所规定的身份鉴别流程且鉴证结果为合格，认证授权机构或注册机构将批准证书申请，由 CA 机构为订户制作并颁发数字证书。

如果发生下列情形，认证授权机构或注册机构有权拒绝证书申请：

1)根据本《车联网证书策略与电子认证业务规则》第 3.2 节的规定，不能完成识别和认证所有必需的订户信息；

2)订户不能根据要求提供所需要的身份电子数据；

3)订户没有或者不能够按照规定支付相应的费用；

4)认为批准该申请将会对 CA 机构带来争议、法律纠纷或者损失；

5)其他认证授权机构或注册机构认为应拒绝证书申请的情形。

对于拒绝的证书申请，认证授权机构或注册机构通知订户证书申请失败，同时告知订户失败的原因(法律禁止的除外)。

4.2.3. 处理证书申请的时间

认证授权机构或注册机构将确认证书申请信息，一旦认证授权机构或注册机构收到了所有必须的相关信息，将及时处理证书申请。

认证授权机构或注册机构能否及时处理证书申请取决于订户是否真实、完整、准确地提交了相关信息和是否及时地响应了 CA 机构的管理要求。

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

CA 机构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正式地批准了证书申请。

4.3.2. 电子认证服务机构对订户的通告

CA 机构通过注册机构告知证书订户证书的签发结果和获取证书的方式，可通过网络下载或 CA 机构认为其他安全可行的方式告知订户。

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，订户通过 CA 机构所通告的方式获取证书，在订户发生以下任意一种行为后，CA 机构认为订户接受了证书：

1）订户下载或安装了证书；

2）在本 CA 机构将证书获取通知发送给订户后，在约定的时间内订户未表示拒绝。

4.4.2. 电子认证服务机构对证书的发布

CA 机构在签发证书后，将证书发给订户视为证书的发布。

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

CA 机构不对其他实体进行通告。

4.5. 密钥对和证书使用

4.5.1. 订户私钥和证书的使用

订户在提交了证书申请并接受了 CA 机构所签发的证书后，均视为已经同意遵守与 CA 机构、依赖方有关的权利和义务的条款。

订户只能在适用的法律、本《车联网证书策略与电子认证业务规则》指定的应用范围内使用私钥和证书，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。

4.5.2. 依赖方对公钥和证书的使用

当依赖方接收到加载数字签名的信息后，有义务进行以下确认操作：

1. 获得数字签名对应的证书及证书可信列表；

2. 确认该签名对应的证书是依赖方信任的证书；

3. 通过查询 CRL 确认该签名对应的证书未被撤销；

4. 证书的用途适用于对应的签名；

5. 使用证书上的公钥验证签名；

6. 确认证书的有效期未过期。

若不满足以上条件，依赖方有责任拒绝该签名信息。

4.6. 证书更新

CA 机构仅支持为注册证书提供证书更新服务。订户需在证书到期前 30 天进行证书更新，证书过期后，订户必须重新申请新注册证书。

证书更新等同于证书密钥更新。详见本《车联网证书策略与电子认证业务规则》第 4.7 节。

4.7. 证书密钥更新

4.7.1. 证书密钥更新的情况

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，CA 机构提供证书更新时，一般要求密钥同时更新。订户仅在申请更新注册证书的情况下会涉及密钥更新。

证书密钥更新的具体情况如下：

a) 当订户证书即将到期或已经到期时；

b) 当订户证书密钥遭到损坏时；

c) 当订户证实或怀疑其证书密钥不安全时；

d) 其它可能导致密钥更新的情况。

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. 证书密钥更新请求的处理

同本《车联网证书策略与电子认证业务规则》第 3.3 节。

4.7.4. 颁发新证书对订户的通告

同本《车联网证书策略与电子认证业务规则》第 4.3.2 节。

4.7.5. 构成接受密钥更新证书的行为

同本《车联网证书策略与电子认证业务规则》第 4.4.1 节。

4.7.6. 电子认证服务机构对密钥更新证书的发布

同本《车联网证书策略与电子认证业务规则》第 4.4.2 节。

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

同本《车联网证书策略与电子认证业务规则》第 4.4.3 节。

4.8. 证书变更

车联网 V2X 证书没有证书变更服务。

4.9. 证书撤销和挂起

4.9.1. 证书撤销的情形

发生下列情形之一的，CA 机构可以撤销其签发的数字证书：

1)订户提供的信息有误或变更时；

2)订户没有履行双方合同规定的义务，或违反本《车联网证书策略与电子认证业务规则》；

3)数字证书的安全性得不到保证；

4)法律、行政法规规定的其他情形。

4.9.2. 请求证书撤销的实体

CA 机构可以请求撤销订户证书。

4.9.3. 撤销请求的流程

撤销是指当 CA 机构确认发生本《车联网证书策略与电子认证业务规则》4.9.1 撤销证书情形时，对订户证书进行撤销。

4.9.4. 撤销请求宽限期

不适用。

4.9.5. 电子认证服务机构处理撤销请求的时限

异常行为管理机构接到撤销请求后将立即处理，处理撤销请求的周期为 24 小时。

4.9.6. 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 CRL 查询的方式对所依赖证书的状态进行查询。

4.9.7. CRL 和 CTL 的颁发频率

CA 机构采用定期的方式发布 CRL，发布 CRL 的频率根据证书策略确定，一般为 24 小时定期发布。

CTL 包含了 CA 证书的集合，当 CA 证书有更新时，Root CA 应发布新的 CTL，同时旧的 CTL 自动作废。

4.9.8. CRL 发布的最长滞后时间

CRL 发布的最长滞后时间为 24 小时。

4.10. 证书状态服务

4.10.1. 操作特点

证书状态可以通过 CA 机构提供的 CRL 服务查询。

4.10.2. 服务可用性

CA 机构提供 7*24 小时的证书状态查询服务。

4.11. 订购结束

订购结束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。

订购结束包含以下两种情况：

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，订户可以终止订购；

b)在证书有效期内，证书被撤销后，即订购结束。

4.12. 密钥生成、备份与恢复

4.12.1. 密钥生成、备份与恢复的策略和行为

订户证书的签名密钥由国家密码管理部门认可的密码模块生成，CA 机构不提供签名密钥的备份与恢复服务。

4.12.2. 会话密钥的封装与恢复的策略和行为

不适用。

4.13. 跨域互信准则

在车联网体系中，会有多个独立的 PKI 系统为订户提供证书服务，每个 PKI 的服务范围称为一个认证域。跨域认证是指位于一个认证域中的订户能够认证由其他认证域签发给该域订户的证书。

本 CA 机构可以与其他电子认证服务机构建立跨域互信的关系，通过获取另一个认证域签发的证书可信列表的方式，实现不同认证域订户的互相认证。要求该电子认证服务机构的 CP 及 CPS 必须符合本《车联网证书策略与电子认证业务规则》及相关标准的各项控制要求，并与本 CA 机构签署相关协议。

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

a）CA 机房的建筑物和机房建设按照下列标准实施：

1）GB 50174-93：《电子计算机机房设计规范》

2）GB 2887-89：《计算站场地技术条件》

3）GB 9361-88：《计算站场地安全要求》

4）GB 6650-1986：《计算机机房用活动地板技术条件》

5）GB 50034-1992：《工业企业照明设计标准》

6）GB 5054-95：《低压配电装置及线路设计规范》

7）GBJ 19-87：《采暖通风与空气调节设计规范》

8）GB 157：《建筑防雷设计规范》

9）GBJ 79-85：《工业企业通信接地设计规范》

b）CA 机房位于北京市西城区裕民东路 3 号 CA 机房，实行分层访问的安全管理：

CA 机房的功能区域划分为六个层次，四个区域。

六个层次由外到里分别是：入口、办公、敏感、数据中心、屏蔽机房和保密

机柜。

四个区域由外到里分别是：公共区域、DMZ 区域（非军事区）、操作区域和安全区域。

其中，入口之外的区域为公共区域，入口和办公层位于 DMZ 区，敏感层位于操作区，其他各层位于安全区。

5.1.2. 物理访问

为了保证本系统的安全，采取了一定的隔离、控制和监控手段。机房的所有门都足够结实，能防止非法的进入。机房通过设置门禁和侵入报警系统来重点保护机房物理安全。

物理访问控制包括如下几个方面：

a）门禁系统：控制各层门的进出。工作人员需使用身份识别卡结合指纹鉴定才能进出，进出每一道门应有时间纪录和信息提示。

b）报警系统：当发生任何非法闯入、非正常手段的开门、长时间不关门等异常情况都应触发报警系统。报警系统明确指出报警位置。

c）监控系统：与门禁和物理侵入报警系统配合使用的还有录像监控系统，对安全区域和操作区域进行 24 小时不间断录像。所有录像资料需要保留不少于 6 个月，以备查询。

门禁和物理侵入报警系统备有 UPS，并提供至少 8 小时的不间断供电。

CA 服务器与外部云服务器通过专用安全链路连接，以保障数据传输安全。

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。

使用不间断电源（UPS）来保证供电的稳定性和可靠性。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。

根据机房环境及设计规范要求，主机房和基本工作间，均设置了空气调节系统。空调系统使用中央空调，并采用独立空调作为备份。其组成包括精密空调、通风管路、新风系统。

CA 机房的要求参照电信设施管理的规定，而且每年对物理系统的安全性进行检查。

5.1.4. 水患防治

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。

CA 机房的系统有充分保障，能够防止水侵蚀。

目前机房内无上下水系统，空调间做了严格防水处理，由漏水检测系统提供（7*24）实时检测。

5.1.5. 火灾预防和保护

火灾预防：

a）敏感区（物理三层）、高度敏感区域（物理四、五、六层），其建筑物的耐火等级必须符合 GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级。

b）CA 机房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。

c）敏感区及高敏区配置独立的气体灭火装置，使用七氟丙烷（HFC-227ea）等洁净气体灭火系统，备有相应的气体灭火器，非敏感区根据实际情况可配置水喷淋灭火装置。CA 机房内除对纸介质等易燃物质进行灭火外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂。

d）火灾自动报警、自动灭火系统避开可能招致电磁干扰的区域或设备，同时配套设置消防控制室。还设有不间断的专用消防电源和直流备用电源，并具有自动和手动两种触发装置。

e）火灾自动灭火设施的区域内，其隔墙和门的耐火极限不低于 1 小时，吊顶的耐火极限不得低于 15 分钟。

f）在非敏感区及敏感区的办公区域内，须设置紧急出口，紧急出口必须设有消防门，消防门符合安全要求。紧急出口门外部不能有门开启的装置，且紧急出口门须与门禁报警设备联动外，需装配独立的报警设备。

g）紧急出口有监控设备进行实时监控，并保证紧急出口门随时可用。CA 机房采取适当的管理手段来保障非紧急避险状态下，紧急出口门不能被内部人员任意打开。

灭火系统采用电动，手动，紧急启动三种方式：

a）电动方式：防护区报警系统第一次火警确认后，发出声光警示信号，切断非消防电源（如：空调电源、照明电源等）。并送排风（烟），防火阀关闭。第二次火警确认后，经延时，同时发出气体释放信号，并发出启动电信号，送给对应的管网启动钢瓶，喷气灭火。

b）手动方式：人员对钢瓶或药剂瓶直接开启操作。

c）紧急启动：防护区外设有紧急启动按钮供紧急时使用。

CA 机房通过与专业防火部门协调，实施消防灭火等应急响应措施。

5.1.6. 介质存储

CA 机房的存储介质包括硬盘、软盘、磁带、光盘等，介质存储地点和 CA 机房系统分开并且保证物理安全，注意防磁、防静电干扰、防火、防水，由专人管理。

5.1.7. 废物处理

当 CA 机房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

CA 机构主机房位于北京市西城区裕民东路 3 号，同城异地备份机房位于北京市朝阳区工体北路 1 号，异地备份机房位于武汉市。主机房的电子认证数据实

时传输到容灾备份中心，用于容灾备份系统应急恢复。

5.2. 程序控制

5.2.1. 可信角色

电子认证服务机构、注册机构、依赖方等组织中与密钥和证书生命周期管理操作有关的工作人员，都是可信角色，必须由可信人员担任。

可信角色包括：

a）系统管理员

系统管理员负责对数字证书服务体系在本单位的系统进行日常管理，执行系统的日常监控，并可根据需要签发服务器证书和下级操作员证书。

b）安全管理员

安全管理员对 CA 中心的物理、网络、系统的安全全面负责。并且拟订安全管理制度和操作流程，监督各岗位安全管理的执行情况。

c）审计管理员

审计管理员控制、管理、使用安全审计系统，安全审计系统分布于证书管理系统的各个子系统中，负责各个子系统的运行和操作日志记录。

d）密钥管理员

密钥管理员负责管理 CA 中心的密钥相关设备，进行 CA 中心密钥的生成、备份、恢复、销毁等操作。

e）证书业务管理员

证书业务管理员对注册机构操作员进行管理，并对注册机构业务进行管理。

5.2.2. 每个角色的识别与鉴别

所有 CA 机构的在职人员，按照所担任角色的不同进行身份鉴别。进入机房需要使用门禁卡和指纹识别；进入系统需要使用数字证书进行身份鉴别。CA 机构将独立完整地记录其所有的操作行为。

5.2.3. 需要职责分割的角色

为保证系统安全，遵循可信角色分离的原则，CA 机构进行职责分离的角色，包括但不限于证书业务受理、订户身份鉴别与审核、证书或 CRL 签发、系统工程与维护、CA 密钥管理、安全审计等。

对于根密钥的操作，必须有 3 名以上的根密钥管理员同时到场，才能进行有关的操作。CA 机构在系统遇到紧急情况需要联合抢修时，应至少有 1 名 CA 机构人员在场，抢修人员在 CA 机构人员的陪同下，执行许可的操作，所有操作、修改都保留记录。非 CA 机构员工因物理修理、消防、强电故障等情况，需要进入 CA 机房实施修理时，必须经同意后，首先认证修理者的身份，然后由 CA 机构指定的员工始终陪同和监护，完成约定部位的修理。

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 CA 机构签署保密协议。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，具体要求在人事管理制度中规定。CA 机构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 机构运行的其它兼职工作、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

CA 机构与有关的政府部门和调查机构合作，完成对 CA 机构可信任员工的背景调查。

所有目前的可信任员工和申请调入的可信任员工都必须书面同意对其进行背景调查。

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犯罪记录，社会关系和社会安全方面的调查。

调查程序包括：

a）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。

b）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鉴定。

c）用人部门通过现场考核、日常观察、情景考验等方式对其考察。

d）经考核，人事部门和用人部门联合填写《可信雇员调查表》，报主管领导批准后准予上岗。

5.3.3. 培训与考核要求

CA 机构对运营人员按照其岗位和角色安排不同的培训。培训有：系统硬件安装与维护、系统软件运行与维护、系统安全、应用软件的运行和维护、CA 中心的运行管理、CA 中心的内部管理、政策和规定及系统备份与恢复等。

对于运营人员，其 CA 的相关知识与技能，每年至少要总结一次并由 CA 机构组织培训与考核。技术的进步、系统功能更新或新系统的加入，都需要对相关人员进行培训并考核。

5.3.4. 再培训周期和要求

对于充当可信角色或其他重要角色的人员，每年至少接受 CA 机构组织的培训一次。

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

5.3.5. 工作轮换周期和顺序

对于可替换角色，CA 机构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 CA 机构员工被怀疑，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CA系统或进行越权操作,CA机构得知后将立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。对情节严重的，依法追究相应责任。

5.3.7. 独立合约人的要求

对不属于CA机构内部的工作人员，但从事CA有关业务的人员等独立签约者(如注册机构的工作人员)，CA机构的统一要求如下：

a) 正规劳务公司派遣人员；

b) 具有相关业务的工作经验；

c) 必须接受CA组织的岗前培训，达到5.3.3要求的技能要求。

5.3.8. 提供给员工的文档

为使得系统正常运行，CA机构向其员工提供完成其工作所必须的文档。

5.4. 审计日志程序

5.4.1. 记录事件的类型

CA机构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。

CA机构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。

CA机构不会记录与车联网V2X应用中私家车有关的隐私数据。

5.4.2. 处理或归档日志的周期

CA机构建有CA应用系统的日志收集分析系统，实时收集应用日志并归档保存。

审计日志处理包括对审计日志的审查、对日志未遭到篡改的验证、对所有日

志条目的检查以及对日志中任何警报或违规行为的调查。

审计日志至少每周存档一次。如果用于审计日志的可用磁盘空间低于一周内预期产生的审计日志数据量，则管理员应执行手动存档。

5.4.3. 审计日志的保存期限

CA 系统审计日志至少保存到证书失效后 5 年，法律法规另有规定的，按照相关法律法规执行。

5.4.4. 审计日志的保护

CA 机构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。审计日志的制作和访问进行岗位分离。对于包含可能导致个人身份识别等隐私信息的事件日志需加密保护，以确保仅允许获得特定授权的人员解密阅读。

5.4.5. 审计日志备份程序

CA 系统审计日志备份采用数据库自身备份程序，根据记录的性质和要求，按照实时、每日、每周等策略进行备份。

5.4.6. 审计日志收集系统

审计日志收集系统涉及：

- 证书管理系统；
- 证书注册系统；
- 证书签发系统（如注册证书机构、假名证书机构、应用证书机构等）；
- 认证授权管理系统；
- 网站和数据库系统；
- 网络安全系统；
- 其他 CA 机构认为有必要审查的系统。

CA 机构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

CA 机构发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，CA 机构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。

CA 机构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

CA 机构每年对系统进行漏洞扫描和渗透测试等脆弱性评估，以降低系统运行的风险。

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等。

5.5.2. 归档记录的保存期限

所有归档记录的保存期为证书失效后五年。

5.5.3. 归档文件的保护

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查询。CA 机构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. 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 CA 主机房的存储库，还在异地保存其备份。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。CA 机构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。

CA 每天增量备份归档文件，并每周执行完整备份。

5.5.5. 记录时间戳要求

所有记录都要在存档时添加准确的时间标识以表明存档时间。

5.5.6. 获得和检验归档信息的程序

由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。CA 机构每年会验证归档信息的完整性。

5.6. 电子认证服务机构密钥更替

CA 机构的根证书有效期最长不超过 15 年，任何由其签发的证书，包括下属 CA 证书和订户证书，其有效期都短于根证书的有效期，任何由下属 CA 证书签发的订户证书，其有效期都短于下属 CA 证书的有效期。

在证书到期以前，CA 机构将按照证书策略的规定对根密钥进行更换，生成新的证书。在进行密钥的生成时，严格按照 CA 机构关于密钥管理的规范。CA 密钥更替必须遵循以下原则：

1. 在 CA 证书生命周期结束前停止签发新的下级证书，确保在 CA 的证书到期时所有下级证书也全部到期。

2. 在停止签发新的下级证书后至证书到期时，继续使用 CA 私钥签发 CRL，直到最后一张下级证书过期。

3. 生成和管理 CA 密钥对时，严格遵守密钥规范。

4. 及时发布新的 CA 证书。

5. 确保整个过渡过程安全、顺利，不出现信任真空期。

电子认证服务机构密钥更替需要签发三个新证书：

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。

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信任。

5.7. 损害和灾难恢复

5.7.1. 事故和损害处理程序

发生故障时，CA 机构将按照灾难恢复计划实施恢复。

5.7.2. 计算资源、软件和/或数据被破坏

CA 机构遭到攻击，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，CA 机构将按照灾难恢复计划实施恢复。

5.7.3. 实体私钥损害处理程序

CA 机构应每年执行一次根密钥泄漏应急程序的演练。

当 CA 根证书被作废时，CA 机构通知订户。

当 CA 的私钥被攻破或需要作废时，CA 机构根据 CA 灾难恢复计划规定的灾难恢复步骤进行操作。

5.7.4. 灾难后的业务连续性能力

针对 CA 系统的核心业务系统，各证书机构应采用双机热备方式；对核心数据库，各证书机构数据库应采用磁盘阵列方式来确保证书系统的高可靠性和可用性。

发生自然或其它不可抗力性灾难后，CA 机构可采用远程热备站点对运营进行恢复。具体的安全措施按照 CA 灾难恢复计划实施。

5.8. 电子认证服务机构或注册机构终止

因各种情况，CA 机构需要终止运营时，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。

CA 机构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 CA 授权的注册机构和订户等。

在终止服务六十日前向工业和信息化部报告，按照相关法律规定的步骤进行操作。

根 CA 采用以下措施终止业务：

a）起草根 CA 终止业务声明；

b）停止根 CA 所有业务；

c）处理加密密钥；

d）处理和存档敏感文件；

e）清除主机硬件；

f）管理 CA 系统管理员和安全官员；

g）通知与 CA 终止运营相关的实体。

根据 CA 机构与注册机构签订的运营协议终止注册机构的业务。

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

6.1.1.1.CA 密钥对生成

CA 系统和 RA 系统的密钥对是在加密机内部产生，密码机具有商用密码产品认证证书。在生成密钥对时，CA 机构按照加密机密钥管理制度，执行详细的操作流程控制计划，选定并授权 5 个密钥管理员，采取五选三方式，密钥管理员凭借安全介质（如：USB-Key）对密钥进行控制。

6.1.1.2.订户密钥对生成

对于注册证书、身份证书、应用证书的密钥对由订户的密码设备生成。

对于假名证书，订户密钥由订户终端的密钥因子和私钥激活材料运算产生，其中订户的密钥因子由订户的密码设备（如 OBU 或 RSU 的安全密码模块中）生成；私钥激活材料由 CA 系统生成。

6.1.2. 私钥传给订户

私钥传给订户仅用于假名证书申请，CA 向订户以密文形式传递私钥激活材料，即用于派生签名私钥的秘密材料。

6.1.3. 公钥传送给证书签发机构

订户通过注册机构，将证书签名请求信息或其它数字签名的文件包，以电子文本的方式将公钥提交给本 CA 机构签发证书。当需要通过网络传送时将使用安全传输层协议（TLS）或其他安全加密方式。

6.1.4. 电子认证服务机构公钥传送给依赖方

依赖方可以从本 CA 机构指定的下载地址下载证书可信列表，从而得到 CA 的公钥。

6.1.5. 密钥的长度

本信任体系支持的根 CA 密钥长度：SM2 密钥长度至少应该是 256 位。

本信任体系支持的中级 CA 和订户证书密钥长度：SM2 密钥长度至少应该是 256 位。

6.1.6. 公钥参数的生成和质量检查

公钥参数由国家密码管理部门许可的密码设备生成，并遵从这些设备的生成

规范和标准。对生成的公钥参数的质量检查标准应符合国家密码管理部门要求。

6.1.7. 密钥使用目的

订户的证书密钥可以用于提供安全服务，例如身份认证、不可抵赖性和信息的完整性等。

6.2. 私钥保护和密码模块工程控制

6.2.1. 密码模块标准和控制

CA 机构所用的密码设备或密码模块都是经国家相关部门认可的产品，其安全性达到以下要求：

- 接口安全：不执行规定命令以外的任何命令和操作；
- 协议安全：所有命令的任意组合，不能得到私钥的明文；
- 密钥安全：密钥的生成和使用必须在硬件密码设备中完成；
- 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 系统的证书私钥的生成、更新、撤销、备份和恢复等操作采用多人控制机制，即采取五选三方式，将私钥的管理权限分散到 5 张管理员卡中，只有其中三人及以上在场并许可的情况下，才能对私钥进行上述操作。

订户证书的私钥应存储在硬件安全模块中，由订户通过访问控制使用操作。

6.2.3. 私钥托管

订户证书对应的私钥由自己保管或控制，CA 机构不负责托管。

6.2.4. 私钥备份

CA 机构不备份订户的私钥。

6.2.5. 私钥归档

CA私钥过期后，CA机构将对CA私钥归档保存至少十年。对CA私钥归档保存的方式为加密保存在外部存储介质中并存放在安全区域。

CA机构不对订户证书的私钥进行归档。

6.2.6. 私钥导入或导出密码模块

CA私钥在硬件密码模块中产生。在需要备份或迁移CA私钥时，从密码模块中导出的私钥必须由多人控制。

订户私钥不允许从硬件密码模块中导出，CA机构不提供订户私钥从硬件密码模块中导出的方法。

6.2.7. 私钥在密码模块中的存储

CA 系统采用国家密码管理部门认可的密码设备，这些设备内置的协议、算法等均符合国家密码行业的标准要求。

CA 私钥在硬件密码模块中加密存储。

订户私钥在密码设备或密码模块中存储。

6.2.8. 激活私钥的方法

CA私钥存放在硬件密码模块中，激活需要按本《车联网证书策略与电子认证业务规则》第6.2.2节使用加密设备的管理员权限实现，具有激活私钥权限的管理员使用安全介质（如：USB-Key）登录，启动密钥管理程序，进行激活私钥的操作，需要三名管理员以上同时在场。

订户在申请假名证书的情况下，需要使用CA传递的私钥激活材料，激活并派生签名私钥。

6.2.9. 解除私钥激活状态的方法

对于CA私钥，解除私钥激活状态需要按本《车联网证书策略与电子认证业务规则》第6.2.2节使用加密设备的管理员权限实现，具有解除私钥权限的管理员使用安全介质（如：USB-Key）登录，启动密钥管理程序，进行解除私钥激活状态的操作，需要三名管理员以上同时在场。

6.2.10. 销毁私钥的方法

当CA私钥生命周期结束后，将通过本《车联网证书策略与电子认证业务规则》第6.2.5节的方法进行CA私钥归档，其他的CA私钥备份将被安全销毁。在CA私钥归档期结束后，具有销毁密钥权限的管理员，启动密钥管理程序，进行销毁密钥的操作，需要3名或以上管理员同时在场。

订户的私钥不再被使用，或者与私钥相对应的公钥到期或者被撤销后，由订户决定其销毁方法，订户必须保证有效销毁其私钥，并承担有关的责任。涉及到密钥到期后保存和归档的，订户必须按照本《车联网证书策略与电子认证业务规则》的规定执行。

6.2.11. 密码模块的评估

CA 机构使用通过检测认证的服务器密码机，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：

a) 通信接口：符合国际 ITU Ethernet RJ45 标准；

b) 带宽控制：10M/100M/1000M 自适应，充分满足突发业务需要；

c) 并发容量：可支持同时并发 100 个的独立安全处理容量；

d) 密钥管理：密钥不以明文形式出现在服务器密码机以外；通信密钥通过身份鉴别后协商得到；

e) 身份鉴别：采用安全介质（如：USBKey）对用户进行身份鉴别管理，以控制对加密系统的使用；

f) 处理速度：数据加解密处理能力大于 100Mbps。

6.3. 密钥对管理的其他方面

6.3.1. 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《车联网证书策略与电子认证业务规则》第5.5节的相关规定。

6.3.2. 证书操作期和密钥对使用期限

本证书体系根证书的最长有效期不超过 30 年，其他 CA 证书的最长有效期不超过 25 年，订户证书的最长有效期不超过 6 年。

公钥和私钥的使用期限与证书的有效期相关但却有所不同。

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

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用期限不超过证书的有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限以外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内才可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

6.4. 激活数据

6.4.1. 激活数据的产生和安装

为了保护私钥的安全，证书订户产生和安装激活数据必须保证安全可靠，从而避免私钥被泄漏、被偷窃、被非法使用、被篡改、或者被非法授权的披露。

CA 私钥的产生遵循本《车联网证书策略与电子认证业务规则》第 6.2.2 节中的要求，严格进行生成、分发和使用。

6.4.2. 激活数据的保护

CA 私钥的激活数据，CA 机构按照可靠的方式将激活数据分割后由不同的可信人员掌管。

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：

a）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。

b）对设备定期进行检查、清洁和保养维护。

c）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。

d）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。

e）设备维修时，必须有派专人在场监督。

6.5.2. 计算机安全要求

CA 系统使用的涉及安全的网络设备、主机、系统软件等都属经正式验收测试合格的产品。

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

CA 机构对系统的维护保证操作系统、网络设置和系统配置安全。通过日志检查来检查系统和数据完整性和硬件的正常操作。

6.6.3. 生命周期安全控制

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

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。CA 机构采取防火墙、病毒防治、入侵检测、入侵防御、漏洞扫描、数据备份、灾难恢复等安全防护措施。

6.8. 时间信息

证书、CRL、CTL、电子认证服务系统日志均包含时间信息，该时间信息来源于国家的标准时间源。

7. 证书、证书撤销列表

7.1. 证书

本 CA 机构签发的证书包括注册证书、假名证书、身份证书和应用证书。其证书基本结构遵循 YD/T 3957-2021 《基于 LTE 的车联网无线通信技术 安全证

书管理系统技术要求》。

7.1.1. 版本号

CA 机构签发的证书格式版本为 V3。

7.1.2. 证书结构类型

对于显式证书，证书结构类型为 01；对于其他结构的证书，证书结构类型为 02。

7.1.3. 证书签发者

签发者 CA 证书的 HashedId8 值。

7.1.4. 证书签名数据

本规则签发的证书均为显式证书，对于显式证书，在生成或校验证书签名时，该字段是哈希函数的输入。

7.2. 证书撤销列表

7.2.1. 版本号

CA 机构签发的 CRL 版本信息在 CRL 版本格式一栏体现。

7.2.2. CRL 结构

CRL 的基本域内容参考如下表格。

域		是否必选	值或值的限制
版本	version	是	version 是 CRL 的版本号，本标准对应的版本号是 1；
CRL 序列号	crlSeries	是	代表 CRL 所属的 CRL 系列，用于确定 CRL 中的撤销信息是否与特定证书相

			关。
签发者	cracaId	是	签发此证书的 CRL CA 的证书的 HashedId8 值
CRL 签发时间	issueDate	是	CRL 的发布时间
预期下次 CRL 签发时间	nextCrl	是	包含预期发出具有相同 crlSeries 和 crlCraca 的下一个 CRL 的时间。
CRL 正文选择结构体	fullHashCrl		包含一个完整的基于散列值的 CRL，即包含所有已撤销证书的散列列表
	deltaHashCrl		包含基于增量散列的 CRL，即所有已撤销证书的散列列表
	fullLinkedCrl		包含一个完整的基于 Linkage ID 的 CRL，即包含所有已撤销证书的个体和/或群组链接数据的列表
	deltaLinkedCrl		包含基于增量 Linkage ID 的 CRL，即包含所有已撤销证书的个体和/或群组链接数据的列表

8. 电子认证服务机构审计和其他评估

8.1. 评估的频率或情形

审计是为了检查、确认 CA 机构是否按照《车联网证书策略与电子认证业务规则》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。审计分内部审计和外部审计。

内部审计是由 CA 机构自己组织内部人员进行的审计，审计的结果可供 CA 机构改进、完善业务，内部审计结果不需要公开。

外部审计由 CA 机构委托第三方审计机构来承担，审计的依据包括 CA 所有与业务有关的安全策略、《车联网证书策略与电子认证业务规则》、业务规范、管理制度，以及国家或行业的相关标准。

8.2. 评估者的资质

内部审计人员的选择一般包括：

- CA 的安全负责人及安全管理人员；

- CA 业务负责人；
- 各证书机构及信息系统负责人；
- 人事负责人；
- 其他需要的人员。

外部审计的审计人员的资质由第三方确定。

8.3. 评估者与被评估者之间的关系

评估者与被评估者应无任何业务、财务往来或其它利害关系足以影响评估的客观性。

8.4. 评估内容

审计内容包括但不限于：

- 人事审查；
- 物理环境建设及安全运营管理规范审查；
- 系统结构及其运行审查；
- 密钥管理审查；
- 客户服务及证书处理流程审查。

8.5. 对问题与不足采取的措施

对审计中发现的问题，CA 机构将根据审计报告的内容准备一份解决方案，明确对此采取的行动。CA 机构将根据国际惯例和相关法律、法规迅速解决问题。

8.6. 评估结果的传达和发布

除非法律明确要求，CA 机构一般不公开评估结果。

对 CA 关联方，CA 机构将依据签署的协议来公布评估结果。

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

CA 机构可根据提供的电子认证相关服务向证书订户收取费用，具体收费标准根据市场和管理部门的规定自行决定。CA 机构在不高于收费标准的前提下可以对证书价格进行适当调整。在订户向 CA 机构订购证书时，将提前告知证书的签发与更新费用。如果 CA 机构签署的协议中指明的价格和 CA 机构公布的价格不一致，以协议中的价格为准。

9.1.2. 证书查询费用

在证书有效期内，对该证书进行信息查询，CA 机构暂不收取此项费用，但保留对此项服务收费的权利。

9.1.3. 证书撤销或状态信息的查询费用

查询证书是否撤销，CA 机构不收取信息访问费用。

9.1.4. 其他服务的费用

CA 机构保留对其他服务收费的权利。

9.1.5. 退款策略

在实施证书操作和签发证书的过程中，CA 机构遵守并保持严格的操作程序和策略。一旦向订户颁发数字证书，CA 机构将不办理退证、退款手续。

如果订户在证书服务期内退出数字证书服务体系，CA 机构将不退还剩余时间的服务费用。

9.2. 财务责任

CA 机构保证其具有维持其运作和履行其责任的财务能力。它应该有能力承担对订户、依赖方等造成的责任风险，并依据《车联网证书策略与电子认证业务规则》规定，进行赔偿担保。

9.3. 业务信息保密

9.3.1. 保密信息范围

保密的业务信息包括但不限于以下方面：

a) 在双方披露时标明为保密(或有类似标记)的；

b) 在保密情况下由双方披露的或知悉的；

c) 双方根据合理的商业判断应理解为保密数据和信息的；

d) 以其他书面或有形形式确认为保密信息的；

e) 或从上述信息中衍生出的信息。

对于 CA 机构来说，保密信息包括但不限于以下方面：

a) 车联网 V2X 应用的各参与方的签名密钥都是保密的；

b) 保存在审计记录中的信息；

c) 年度审计结果也同样视为保密；

d) 除非有法律要求，由 CA 机构掌握的，除作为证书、CRL、CTL、认证策略被清楚发布之外的个人和公司的信息需要保密。

除非法律明文规定，CA 机构没有义务公布或透露订户数字证书以外的信息。

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。CA 机构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。

9.3.3. 保护保密信息的责任

a）各方有保护自己和其他人员或单位的机密信息并保证不泄露给第三方的责任。不将机密数据和信息(也不会促使或允许他人将机密数据和信息)用于协议项下活动目的之外的其他用途，包括但不限于将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；在披露当时，如果已明确表示机密数据和信息不得复印、复制或储存于任何数据存储或检索系统，接受方不得复印、复制或储存机密数据和信息。

b）当 CA 机构在任何法律、法规或规章的要求下，或在法院的要求下必须提供本《车联网证书策略与电子认证业务规则》中具有保密性质的信息时，CA 机构应按照要求，向执法部门公布相关的保密信息，CA 机构无须承担任何责任。这种提供不被视为违反了保密的要求和义务。

9.4. 用户隐私保护

CA 机构针对用户隐私信息提供如下保障措施。

9.4.1. 隐私保密方案

在数字证书生命周期中，CA 机构应在订户隐私信息的收集、使用、存储环节中，采取有效手段，保护订户隐私信息。

CA 机构应保护证书申请方所提供的、证明其身份的资料。CA 机构应采取必要的安全措施防止证书申请方资料被遗失、盗用与篡改。

CA 机构将实施信息安全管理制度以及行业通行的安全技术和程序来确保订户的信息不被丢失、泄露、篡改、毁损或滥用。

CA 机构将实施组织分离管理制度，防止单个管理员通过组合 PCA、RA、MA 的信息确定假名证书主体身份。

CA 机构使用密码技术对订户的身份信息进行加密；为避免泄露车辆行驶轨迹，车载设备可拥有多个假名证书，用于定期更换使用，确保订户的位置等信息不被泄露。

9.4.2. 作为隐私处理的信息

证书申请方提供的不构成数字证书内容的用户个人信息，被视为隐私信息。

9.4.3. 不被视为隐私的信息

订户持有的证书信息，以及证书状态信息不被视为隐私信息。

9.4.4. 保护隐私的责任

CA 机构有妥善保管本《车联网证书策略与电子认证业务规则》第 9.4.2 节中规定的订户隐私使用、共享、管理、查阅、删改等责任与义务。

在政府或执法机关根据合法程序要求 CA 机构向特定对象公布隐私信息的情况下，CA 机构无需承担由此造成的责任。

9.4.5. 使用隐私信息的告知与同意

本《车联网证书策略与电子认证业务规则》订户同意，在有关法律法规、执法机关或政府根据合法的程序要求下，CA 机构向特定对象披露隐私信息时，CA 机构无需告知订户。

9.4.6. 依法律或行政程序的信息披露

除非符合以下条件，CA 机构不会将订户的保密信息提供给其他第三人或第三方机构：

1）执法机关、政府或其他相关法律法规授权的部门依据法律、法规、规章、决定、命令等提出申请；

2）本《车联网证书策略与电子认证业务规则》规定的其他可以披露的情形。

9.5. 知识产权

除非额外声明，CA 机构享有并保留对证书以及 CA 机构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、著作权、专利权和利益分享权等。CA 机构有权决定关联机构采用的软件系统，选择采取的形式、方法、时间、过程和模型，以保证系统的兼容和互通。

按本《车联网证书策略与电子认证业务规则》的规定，所有由 CA 机构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 CA 机构所有，这些知识产权包括所有相关的文件和使用手册。认证授权机构应征得 CA 机构的同意使用相关的文件和手册，并有责任和义务提出修改意见。

9.6. 陈述与担保

9.6.1. 电子认证服务机构的陈述与担保

CA 机构在提供电子认证服务活动过程中的承诺如下：

a）CA 机构遵守《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的领导，对签发的数字证书承担相应的法律责任。

b）CA 机构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 CA 机构 CRL 发出了 CA 的私钥被破坏或被盗的通知，CA 机构保证其私钥是安全的。

d）CA 机构签发给订户的证书符合 CA 机构的《车联网证书策略与电子认证业务规则》所有实质性要求。

e）CA 机构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）CA 机构将及时撤销证书。

g）CA 机构拒绝签发证书后，将立即向证书订户归还所付的全部费用。

h）证书公开发布后，CA 机构向证书依赖方证明，数字证书中载明的订户信息都是准确的。

j）CA 机构不负责评估证书是否在适当的范围内使用。

k）所有证书不应用于、也不授权用于危险环境中的控制设备，或用于要求

防失败的场合，因为任何潜在的、或有的故障都可能导致死亡、人员伤害或环境破坏。

9.6.2. 注册机构的陈述与担保

CA 机构的注册机构在参与电子认证服务过程中的承诺如下：

a）提供给证书订户的申请过程完全符合 CA 机构的《车联网证书策略与电子认证业务规则》所有实质性要求。

b）在 CA 机构生成证书时，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方的信息不一致。

c）注册机构将按 CPS 的规定，及时向 CA 机构提交证书申请、更新等服务请求。当订户以书面形式通知注册机构其申请证书时提供的声明或信息发生改变时，注册机构无正当理由未及时提供相关证书服务的，由此给订户造成的损失由注册机构自行承担全部法律责任。

9.6.3. 认证授权机构的陈述和担保

认证授权机构在参与电子认证服务过程中的承诺如下：

a）提供给证书订户的注册过程完全符合 CA 机构的《车联网证书策略与电子认证业务规则》所有实质性要求。

b）在 CA 机构生成证书时，不会因为认证授权机构的失误而导致证书中的信息与证书申请方的信息不一致。

c）认证授权机构将按 CPS 的规定，及时向 CA 机构提交证书申请服务请求。

9.6.4. 订户的陈述与担保

订户一旦接受 CA 机构签发的证书，就被视为向 CA 机构、注册机构及信赖证书的有关当事人作出以下承诺：

a）订户确认已知悉并接受了本《车联网证书策略与电子认证业务规则》及相关规定的全部内容，且同意受本《车联网证书策略与电子认证业务规则》条款的约束，同意其中赔偿责任限制的规定。

b）订户在申请证书时提供的所有声明和信息必须是完整、真实和正确的，可供 CA 机构或注册机构检查和核实。如果前述声明或信息发生任何改变应及时通知 CA 机构或注册机构。如因订户故意或过失提供虚假、伪造等信息资料或陈述，或前述提供的声明或信息发生改变时未及时以书面形式通知 CA 机构或注册机构的，由订户自行承担全部法律责任。

c）订户应当妥善保管私钥，订户的密码安全设备必须符合安全技术标准，具备足够的安全防护能力来防止证书私钥的遗失、泄露和被篡改等事件的发生。

d）私钥为订户本身访问和使用，订户对使用私钥的行为负责。

9.6.5. 依赖方的陈述与担保

依赖方必须熟悉本《车联网证书策略与电子认证业务规则》的条款以及和订户数字证书相关的证书政策，并确保本身的证书用于申请时预定的目的。

依赖方在信赖订户的数字证书前，必须采取合理步骤，查证订户数字证书及数字签名的有效性。当依赖方未尽到前述查证义务时，依赖方愿意赔偿由此给 CA 机构造成的全部损失，并且自行承担由此给自身或他人造成的损失。

所有依赖方必须承认，他们对证书的信赖行为就表明他们承认了解本《车联网证书策略与电子认证业务规则》的有关条款，同意其中赔偿责任限制的规定。

9.6.6. 其他参与者的陈述与担保

其他参与者的陈述与担保同 9.6.5。

9.7. 赔偿责任限制

a）除非有另行的规定或约定，对于非本 CPS 下的认证服务而导致的任何损失，CA 机构不向订户或依赖方承担任何赔偿和/或补偿责任。

b）订户或依赖方进行车联网应用因 CA 机构提供的认证服务而遭受的直接损失，数字认证将依据本 CPS 的相关条款给予相应的赔偿。

c）如果 CA 机构能够证明其提供的服务是按照《电子签名法》、《电子认证服务管理办法》、CA 机构向主管部门备案的 CPS 实施的，则视为 CA 机构不具有

任何过错，CA 机构将不对订户或依赖方承担任何赔偿或补偿责任。

d）无论本 CPS 是否有相反或不同规定，就以下损失或损害，CA 机构不承担任何赔偿和/或补偿责任。

1. 订户和/或依赖方的任何间接损失、直接或间接的利润或收入损失、信誉或商誉损失、任何商机或契机损失、失去项目、以及失去或无法使用任何数据、无法使用任何设备、无法使用任何软件；

2. 由上述第 1 项所述的损失相应生成或附带引起的损失或损害；

3. 非 CA 机构行为而导致的损失；

4. 因不可抗力而导致的损失，如罢工、战争、灾害、恶意病毒代码等；

d）无论本 CPS 是否有相反或不同规定，如果 CA 机构根据本 CPS 或任何法律规定，以及司法判定须承担赔偿和/或补偿责任的，CA 机构将按照相关法律法规的规定、仲裁机构的裁决或法院的裁判承担相应的赔偿责任。

e）CA 机构对于任何证书或依赖方等实体的证书赔偿合计责任不得超出证书市场购买价格。

9.8. 担保免除

有下列情况之一的，应当免除 CA 机构之责任，包括但不限于赔偿责任及补偿责任。

a）如果订户故意或过失地提供了不完整、不可靠、已过期或无效的信息，又根据正常的流程提供了必须的审核文件，得到了 CA 机构签发的数字证书，由此引起的经济纠纷应由订户全部承担，CA 机构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。

b）CA 机构不承担任何其他未经授权的人或组织以本 CA 机构名义编撰、发表或散布的不可信赖的信息所引起的法律责任。

c）CA 机构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。

d）CA 机构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。

e）CA 机构和注册机构不是证书持有人或依赖方的代理人、受托人、管理人

或其他代表。CA 机构和证书持有人间的关系以及 CA 机构和依赖方间的关系并不是代理人和委托者的关系。证书持有人和依赖方都没有权利以合同形式或其他方法让 CA 机构承担信托责任。

f）CA 机构与授权的认证授权机构签署合同，合同条款中明确认证授权机构负责并承担订户身份核实责任。对于由认证授权机构的行为所产生的法律与赔偿责任由 CA 机构授权的认证授权机构承担，并且认证授权机构应当使 CA 机构免于第三方的索赔。

g）若数字证书被超出范围或者以非预期的方式使用（如应用领域不被 CA 机构认可等），CA 机构不向任何方承担赔偿和/或补偿责任。

h）由于客观意外或其他不可抗力事件原因而导致数字证书签发错误、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。

i）CA 机构因下列情况而导致数字证书签发延迟、中断、无法签发，或暂停、终止全部或部分证书服务的，该情况包括但不限于：（1）不可抗力；（2）关联单位如电力、电信、通讯部门而致；（3）黑客攻击；（4）设备或网络故障；（5）系统停机维护。

j）CA 机构已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.9. 有限责任

订户、依赖方因 CA 机构提供的电子认证服务从事民事活动遭受到的直接损失，CA 机构根据本《车联网证书策略与电子认证业务规则》向订户、依赖方承担有限责任。

9.10. 赔偿

CA 机构按照本《车联网证书策略与电子认证业务规则》第 9.7 节中的条款承担赔偿责任。

证书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 CA 机构和注册机构产生损失，订户和依赖方应承担赔偿责任。

订户或其管理者接受证书就表示同意在以下情况下承担赔偿责任。

a）未向 CA 机构提供真实、完整和准确的信息，而导致 CA 机构或有关各方损失。

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时。

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

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 CA 机构对证书使用的规定，造成了 CA 机构或有关各方的利益受到损失。

9.11. 有效期限与终止

9.11.1. 有效期限

本《车联网证书策略与电子认证业务规则》自发布之日起正式生效。

本《车联网证书策略与电子认证业务规则》中将详细注明版本号及发布日期。

9.11.2. 终止

当新版本的《车联网证书策略与电子认证业务规则》正式发布生效时，旧版本的《车联网证书策略与电子认证业务规则》自动终止。

9.11.3. 效力的终止与保留

《车联网证书策略与电子认证业务规则》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。

9.12. 修订

9.12.1. 修订程序

当本《车联网证书策略与电子认证业务规则》不适用时，由数字认证公司安全策略管理委员会组织 CPS 编写小组进行修订。

修订完成后，数字认证公司安全策略管理委员会进行审批，审批通过后将在数字认证公司的网站(http://www.bjca.cn)上发布新的《车联网证书策略与电子认证业务规则》。

《车联网证书策略与电子认证业务规则》将进行严格的版本控制。

9.12.2. 通告机制和期限

本《车联网证书策略与电子认证业务规则》在数字认证公司的网站(http://www.bjca.cn)上发布。

版本更新时，最新版本的《车联网证书策略与电子认证业务规则》在数字认证公司的网站发布，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《车联网证书策略与电子认证业务规则》。

9.13. 争议处理

CA 机构、订户、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 CA 机构，根据本《车联网证书策略与电子认证业务规则》中的规定，明确责任方；

b) 由 CA 机构相关部门负责与当事人协调；

c) 协调不成，当事人因与 CA 机构或授权机构在电子认证活动中产生的任何

争端及或对本《车联网证书策略与电子认证业务规则》所产生的任何争议，均应提请北京仲裁委员会按照其仲裁规则在北京进行仲裁。仲裁裁决是终局的，对双方均有约束力。

9.14. 管辖法律

本《车联网证书策略与电子认证业务规则》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. 与使用法律符合性

无论在任何情况下，本《车联网证书策略与电子认证业务规则》的执行、解释、翻译和有效性均适用中华人民共和国大陆地区的法律。

9.16. 一般条款

9.16.1. 完整规定

本《车联网证书策略与电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

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。

在数字证书认证活动中，CA 机构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

数字认证公司对本《车联网证书策略与电子认证业务规则》拥有最终解释权。