ICS°35.080
L77

团　体　标　准

T/JSHLW ###-####

基于区块链的车联网密钥管理规范

Internet of Vehicles Key Management Specification Based on Blockchain

（征求意见稿）

####-##-## 发布　　####-##-## 实施

江苏省互联网协会 发布

目录

前　　言

本标准依据 GB/T 1.1-2009《标准化工作导则》给出的规则起草。

本标准由江苏省互联网协会提出并归口。

本标准起草单位：南京理工大学、南京凌岳区块链科技有限公司、江苏智城慧宁交通科技有限公司。

本标准主要起草人：戚湧、赵学龙、陈弦霜、郝冠亚、徐志荣、高宁波。

基于区块链的车联网密钥管理规范

1 范围

本标准基于区块链技术架构描述了基于区块链的车联网密钥管理应用架构，规定了管理车联网密钥的随机性、安全性以及生成、使用的技术要求。

本标准适用于指导管理车联网密钥的区块链平台和应用中密钥生成、分发、使用系统的设计、实现和使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的应用文件，仅注日期的版本适用于本文件，凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式

GM/T 0002-2012 SM4 分组密码算法

GM/T 0003-2012 SM2 椭圆曲线公钥密码算法

GM/T 0004-2012 SM3 密码杂凑算法

GM/T 0044-2016 SM9 标识密码算法

GM/T 0054-2018 信息系统密码应用基本要求

GM/T 0028-2014 密码模块安全技术要求

GB/T 20271-2016 信息安全技术 信息系统安全通用技术要求

3 术语和定义

下列术语和定义适用本文件。

3.1

密钥 Cipher

密钥是一种在明文转换为密文或将密文转换为明文的算法中输入的参数。密钥分为对称密钥与非对称密钥。在对称加密算法中，加密运算和解密运算使用相同的密钥；而在非对称加密算法中，具有两个不同的密钥，即公钥和私钥。

3.2

区块链 Blockchain

区块链是一种对等网络环境下以块链式存储结构实现数据存储、共享、验证、计算等功能的多方共同维护的分布式账本技术。

3.4

智能合约 Smart Contract

智能合约是一种用计算机语言取代法律语言记录条款的合约。这种协议一旦制定和部署就能实现自我执行和自我验证,不再需要人为的干预。

3.5

数字证书 Digital Certificate

数字证书是由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.6

证书认证机构 Certificate Authority

证书认证机构是负责签发、验证数字证书和管理已颁发数字证书的机构。它承担公钥的合法性检验的责任，制定验证用户身份的策略，对数字证书进行签名以确保数字证书持有者的身份和公钥的拥有权。

3.7

密钥加密密钥 Key Encryption Key

密钥加密密钥是一个密钥，用于加解密主密钥。

3.8

传输层安全协议 Transfer Layer Secure

传输层安全协议是一种用于在两个通信应用程序之间提供保密性和数据完整性的协议。

3.9

安全套接字协议 Secure Socket Layer

安全套接字协议是一种在传输通信协议上实现的安全协议，采用公开密钥技术。

4 缩略语

下列缩略语适用于本文件：

CA	数字证书签发和管理机构（Certification Authority）
KEK	密钥加密密钥（Key Encryption Key）
SSL	安全套接字协议(Secure Sockets Layer)
TLS	传输层安全协议（Transfer Layer Secure）

5 车联网密钥管理基本要求

在车联网架构系统中，密钥需要拥有不可篡改，隐私性高的特性，基于区块链的车联网密钥管理要求如下：

a） 用户的身份识别和权限控制

要求确认实体身份真实、合法，在区块链系统中进行的操作应符合其权限。

b） 密钥的保密性

要求密钥信息在注册、更新、存储、传输、撤销等过程中的安全，防止相关车辆信息被非法获取使用。

c） 密钥转移和使用记录的完整性

要求区块链网络中密钥提供方和使用方双方信息一致，确保信息在区块链系统中生成、存储、传输过程中的完整性。

d） 密钥的防篡改性

要求链上各方不能篡改已经产生的密钥。

6 基于区块链的车联网密钥管理架构

在基于区块链的车联网应用场景中，密钥管理应具备层次性，如图1所示：

图 1 区块链的车联网密钥管理架构图

一级：主密钥。用于加密二级密钥和三级密钥。

二级：密钥加密密钥。用于会话密钥的加密传送。

三级：会话密钥。对信道上传输的数据提供机密性、完整性保护等。

7 车联网密钥管理相关技术要求

基于区块链技术的车联网密钥管理规范包括：密钥生成、密钥注册、密钥更新、密钥存储、密钥使用、密钥备份和恢复、密钥归档和密钥清除。

7.1 密钥生成

在使用基于区块链的密钥管理服务时，首先需要按照区块链的数据格式生成密钥。密钥生成过程中应满足以下安全加密要求：

a) 密钥应在核准的密码产品内部生成。在密钥生成时，对应的密钥控制信息，包括但不限于密钥拥有者、密钥用途、密钥索引号、生命周期起止时间等，应进行完整性保护以确保被正确使用。

b) 对敏感信息使用加密方式进行保护，保证数据在传输、存储和使用过程中的安全。应使用较为安全的 HASH 算法，如国密算法 SM3、SHA256 等。

7.2 密钥注册

密钥注册中，车联网密钥所有权验证和达成区块共识过程中的安全加密要求应满足：

a） 数字证书有效性验证，包括 CA 签名验证、有效期验证、状态验证、策略验证，确保数字证书有效、密钥拥有方身份真实；

b） 密钥区块数据有效性验证，应确保区块中记录的上一个区块哈希值的有效性，有效数据通过共识算法在节点间达成共识，再被打包进区块中。

c） 应确保密钥分配过程的目标对象准确及路径安全。

7.3 密钥更新

应采用较为安全的 HASH 算法，如国密算法 SM3、SHA256 等，定期进行密钥更新

7.4 密钥存储

密钥应加密存储在外部介质中。若无法进行加密存储，则应采取一系列应急处理和响应措施，如停止原密钥使用、暂停业务系统服务、更新密钥等。

密钥在存储过程中，应防止密钥非授权的泄露和替换。私钥的存储要求保证机密性与完整性，公钥的存储要求保证真实性与完整性。

7.5 密钥使用

每个密钥都应该有明确的用途，信息系统应按照最初设定的用途使用不同的密钥。在第一次使用公钥前，应当对证书的有效性进行验证。如果密钥具有时限性，应当按照要求进行更换。

1) 一个密钥只能在预定的位置用于预期的功能。
2) 密钥周期结束或私钥泄露时，应停止密钥对的使用；
3) 应保护私钥的机密性和完整性，私钥不应在安全密码设备外使用。
4) 公钥的接收者应在使用前验证公钥的完整性和真实性。

7.6 密钥备份与恢复

备份的密钥只有恢复成激活状态后，才可以直接用于密码运算。

7.7 密钥归档

密钥生命周期结束后要求如下：

1）签名密钥对的私钥不应进行归档。

2）归档后的密钥应进行备份操作，并采用必要的访问控制措施保证密钥的安全性。

3）应确保公钥归档的安全级别与公钥存储的安全级别相同。

4）用于归档过程的密钥加密密钥不应与任何用于加密活动密钥的密钥加密密钥相同。

7.8 密钥清除

a）私钥不再需要处于激活状态时，则应将其清除。私钥清除后，相应的公钥不应再分发给相关各方。如果公钥存储在相关各方所在的位置，则应通知他们相应的私 钥已被清除。

b） 当安全密码设备从服务中永久删除时，设备中存储的全部私钥都应被清除。

7.9 智能合约部署

智能合约的容器与节点之间，应配有使用安全协议的安全通道。安全协议应采用符合国家密码标准的 SSL/TLS 协议。