ICS°35.080
L77

团　　体　　标　　准

T/JSHLW ###-####

基于区块链的车联网通信安全架构规范

Blockchain based Internet of Vehicles communication security architecture specification

（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/T1.2-2020《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，江苏智城慧宁交通科技有限公司，华设设计集团股份有限公司，江苏互联网创新联盟。

本标准主要起草人：戚湧、赵学龙、方越秀、郝冠亚、高宁波、刁含楼、周俊。

基于区块链的车联网通信安全架构规范

1 范围

本标准基于区块链技术架构描述基于区块链的车联网通信安全架构规范，规定基于区块链的车联网通信安全架构模型及相应要求。

本标准适用于基于区块链的车联网通信安全架构的相关设计、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 22239-2019 信息安全技术 网络安全等级保护基本要求。

GB/T35273-2017 信息安全技术个人信息安全规范

GB/T32399-2015 信息技术云计算

GB/T25069-2010 信息安全术语

GM/T 0024-2014 SSL VPN 技术规范

GM/T 0111-2021 区块链密码应用技术要求

T/CESA 6001-2016 区块链参考架构。

T/SHBTA 002-2019 区块链底层平台通用技术要求。

T/SIA 007-2018 区块链平台基础技术要求。

T/CESA 1049—2018 区块链隐私保护规范

T/GHDQ 76—2021 车内 CAN 通信安全合规性测试规范

3 术语、定义

下列术语和定义适用于本文件

3.1

控制器局域网总线 Controller Area Network

控制器局域网总线是一种用于实时应用的串行通讯协议总线。它常用于汽车中各种不同元件之间的通信，以此取代昂贵而笨重的配电线束

3.2

专用短程通信 Dedicated Short Range Communication

专用短程通信是一种高效的无线通信技术，可以实现小范围内图像、语音和数据的实时，准确和可靠的双向传输，将车辆和道路有机连接

3.3

前装智能车载终端 Telematic BOX

前装智能车载终端是指车联网系统中的智能车载终端，是直接与汽车 CAN 总线通信，

获取车身状态、车况信息，并上传至云端。

3.4

蜂窝车联网 Cellular Vehicle-to-Everything

C-V2X 是一种先进无线通讯技术，它能让车辆、信号灯、交通标识、骑行者和行人的通讯设备实现互联，并共享当前状态，位置及行动意图等信息。

3.5

防篡改装置 Tamper Proof Device

防篡改装置是一种集成安全模块，用来构建可信架构辅助完成车联网中身份认证，，用硬件确保身份认证的安全性和可靠性，防止篡改。

3.6

全球导航卫星系统 Global Navigation Satellite System

全球导航卫星系统又称全球卫星导航系统，是能在地球表面或近地空间的任何地点为用户提供全天候的3维坐标和速度以及时间信息的空基无线电导航定位系统。

3.7

安全套接层协议 Secure Socket Layer

安全套接层协议是一种网络安全协议，它位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持。SSL通过互相认证、使用数字签名确保完整性、使用加密确保机密性，以实现客户端和服务器之间的安全通讯。

3.8

无线射频识别技术 Radio Frequency Identification

无线射频识别技术是自动识别技术的一种，通过无线射频方式进行非接触双向数据通信，利用无线射频方式对记录媒体（电子标签或射频卡）进行读写，从而达到识别目标和数据交换的目的。

3.9

第五代移动通信技术 5th Generation Mobile Communication Technology

第五代移动通信技术是具有高速率、低时延和大连接特点的新一代宽带移动通信技术。

3.11

数字签名 Digital Signature

数字签名是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明，具有不可抵赖性

3.12

加密 encipherment / encryption

加密是对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

3.13

区块链 Blockchain

区块链是一个分布式的共享账本或数据库，存储于其中的数据或信息，具有去中心化、不可篡改等特点。

3.14

智能合约 Smart Contract

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。它基于区块链技术，作为一种旨在以信息化方式传播、验证或执行的计算机协议，为各类分布式应用服务提供了基础，是区块链的核心技术之一。

3.15

时间戳 Timestamp

时间戳是一个能表示一份数据在某个特定时间之前已经存在的、 完整的、 可验证的数据,通常是一个字符序列，唯一地标识某一刻的时间。

3.16

访问控制 Access Control

访问控制是指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源能力的手段。通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

4 缩略语

下列缩略语适用于本文件：

CAN	控制器局域网总线(Controller Area Network)
DSRC	专用短程通信（Dedicated Short Range Communication）
T-BOX	前装智能车载终端(Telematic BOX)
C-V2X	蜂窝车联网（Cellular Vehicle-to-Everything）
GNSS	全球导航卫星系统（Global Navigation Satellite System）
TPD	防篡改装置（Tamper Proof Device）
SSL	安全套接层协议（Secure Socket Layer）
RFID	无线射频识别即射频识别技术（Radio Frequency Identification）
5G	第五代移动通信技术（5th Generation Mobile Communication Technology）

5 基于区块链的车联网通信安全架构

车联网通信安全架构分成五个部分：车与车通信、车与人通信、车内通信、车与路通信、车与云服务平台通信，如图 1 所示：

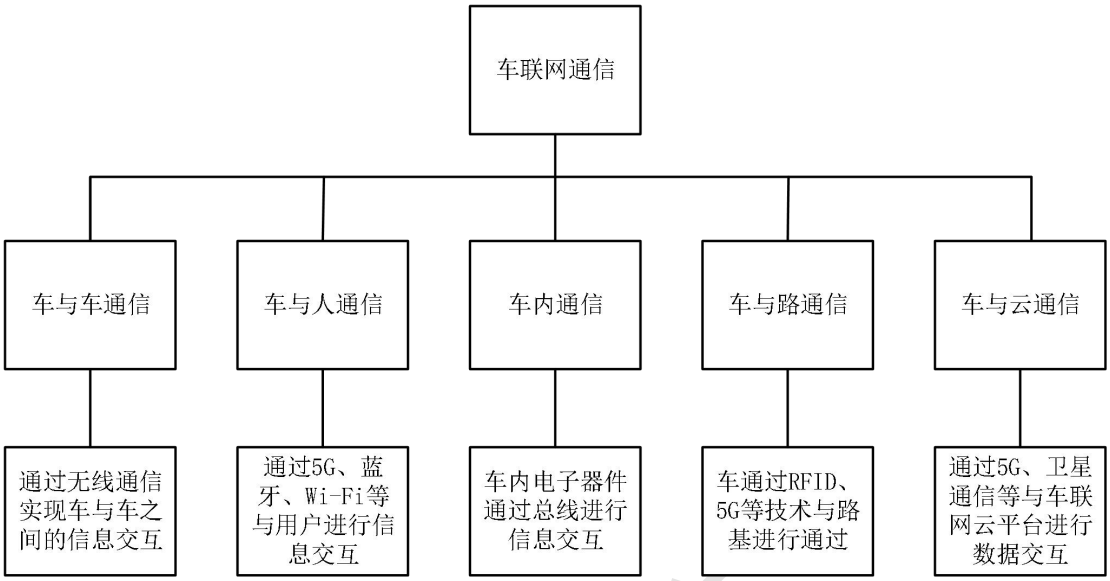

图 1　车联网通信安全架构图

5.1 车与车通信

车与车通信过程中应满足以下要求：

a)　应使用无线通信实现车与车之间的信息交互。

b)　应进行加密传输，有效保障通讯数据的机密性。

c)　应通过加密或签名来认证所传输信息的合法性及完整性，检测信息在传输过程中是否被恶意篡改。

5.2 车与人通信

车与人通信过程中应满足以下要求：

a)　通过5G、蓝牙、WIFI等与用户进行信息交互。

b)　应使用数字签名来保证信息的完整性、发送者的身份认证、防止交易中的抵赖发生。

c)　应通过密码技术将车辆的相关敏感信息或数据进行加密，保证信息机密性，防止信息被非法窃取。

d)　使用数字签名来保证数据真实性，防止数据被恶意篡改。

5.3 车内通信

车内通信过程应满足以下要求：

a)　车内电子器件通过 CAN 总线等技术进行信息交互。

b)　应对收发信息进行加密传输，有效保障通讯数据的机密性。

5.4 车与路通信

在车联网通信安全系统中，车与路通信过程中应满足以下要求：

a）应使用多种感知精度高的检测设备实时采集各种信息。

b) 应通过 WIFI、蓝牙、5G 等技术与路基进行通信。

c) 应将时间、速度、行驶路线和违章行为等车辆信息存储在防篡改设备中，避免违规车辆或用户否认其相关行为。

5.5 车与云通信

在车联网通信安全系统中，车与云服务平台应满足以下要求：

a） 应通过车载智能终端获取车辆信息，上传至云端。

b） 应在云服务器端部署 SSL 证书来实现传输通道加密，确保机密数据传输安全。

6 基于区块链的车联网通信安全架构技术要求

应用技术要求主要包括：高精度信息采集要求、数据交互传输要求、车联网云平台要求、智能合约要求、访问控制要求。

6.1 信息采集要求

在基于区块链的车联网通信安全系统中，高精度信息采集要求为：

a) 应通过多种技术的融合来实现车辆精准定位，包括GNSS、C-V2X、高精度地图等。

b) 应通过车载智能终端获取车辆周围路况信息。

6.2 数据交互传输要求

在基于区块链的车联网通信安全系统中，数据交互传输要求为：

a) 车、路、人、云平台之间的数据交互应当采用数字签名、加密算法等保密、防篡改技术，确保数据的机密性、完整性。

b) 应当将数据信息存入防篡改设备中，防止数据被篡改。

6.3 车联网云平台要求

在基于区块链的车联网通信安全系统中，车联网云平台要求

a） 应实现车、路、人之间的网络互联互通。

b） 应对平台使用者做出实时响应，即时接收、反馈信息。

c） 应实现多场景支撑功能，例如主动安全、路径规划、共享数据以及协同感知等。

6.4 智能合约要求

在基于区块链的车联网通信安全系统中，智能合约要求：

a)区块链上涉及到合约中修改状态变量的操作，必须对函数的调用权限进行严格控制。尤其涉及到一些重要属性修改时，应当配置仅合约拥有者可以调用的权限。

b)应使用适当的技术，使智能合约中使用的随机数尽量安全。

c) 应提防合约重入的可能性，使用无重入漏洞的合约。

d) 在合约中不使用区块时间戳作为判断对错或改变重要状态的决定性因素，尽量避免时间戳的依赖漏洞。

6.5 访问控制要求

在基于区块链的车联网通信安全系统中，访问控制要求：

a） 应当采用加密技术防止非法用户进入系统。

b） 应当采用权限认证技术阻止合法用户对系统资源的非法使用。

c） 应对系统中的用户权限应进行有效管理，防止系统的非授权使用。