ICS 33.050
CCS M 30

团　体　标　准

T/TAF 191—2023

车联网服务用户身份认证安全技术要求

Security technical requirements for user authentication of connected vehicle services

2023-11-24 发布　　2023-11-24 实施

电信终端产业协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件中的某些内容可能涉及专利。本标准的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、博鼎实华（北京）技术有限公司、郑州信大捷安信息技术股份有限公司、安谋科技（中国）有限公司、百度在线网络技术（北京）有限公司、国民认证科技（北京）有限公司、天翼电信终端有限公司、北京豆荚科技有限公司。

本文件主要起草人：徐晓娜、袁琦、宁丹、王昱龙、董雾、刘献伦、李煜光、王骏超、郭建领、李俊、崔凯、刘为华、窦丽娟、孙科、王海兰。

引　言

近年来，包括《新能源汽车产业发展规划（2021-2035年）》、《智能汽车创新发展战略》等指导性文件出台，工信部也部署开展车联网身份认证和安全信任试点工作，都预示着国家高度重视车联网的网络安全工作，也将车联网网络安全的标准需求上升到了更高的层次。目前国内涉及车联网网络安全的相关标准仍在制定中，大部分标准均重点关注于车联网中通信系统与车辆自身的网络安全能力，而较少涉及车联网用户的网络安全保障能力。本标准旨在响应国家相关政策，积极构建车联网用户身份认证的安全技术要求相关内容。

本文件重点在于从接入车联网服务的用户身份认证角度，对车联网的网络安全能力进行规范，可用于指导协会内相关企业设计与部署车联网用户身份认证的技术架构，提升产品网络安全能力。

车联网服务用户身份认证安全技术要求

1 范围

本文件规定了适用于车联网服务的用户身份认证系统的安全技术要求，主要内容包括技术架构、认证流程、安全风险与目标、安全技术要求等方面。

本文件适用于车主实名认证、车主无感支付、车辆开锁等车联网服务场景中，用户身份认证相关的设计、部署和测试等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 40660-2021 信息安全技术 生物特征识别信息保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

车联网服务 connected vehicle services

通过人、车、路与网之间的实时感知与协同实现智能交通管理、智能动态信息服务和智能车辆控制服务，包括车主实名认证、车主无感支付、车辆开锁等应用场景。

3.2

车联网服务用户身份认证 user authentication of connected vehicle services

车联网服务应用场景中，用户、终端设备、车辆与车联网服务网络、车联网身份认证网络及第三方应用之间，通过数字身份标识进行身份认证，保证车辆开锁、无感支付等业务的安全进行。

4 缩略语

下列缩略语适用于本文件。

ETC：电子收费系统（Electronic Toll Collection）

NFC：近场通信（Near Field Communication）

SE：安全单元（Secure Element）

TEE：可信执行环境（Trusted Execution Environment）

TSP：汽车远程服务提供商（Telematics Service Provider）

UWB：超宽带（Ultra Wide Band）

5 总体架构

5.1 技术架构

车联网服务用户身份认证应用场景中，用户主要包括使用车联网服务用户身份认证服务的车主、用车人等车辆使用相关人员。车联网服务用户身份认证应用场景所具备的技术架构参考实现如图1所示。

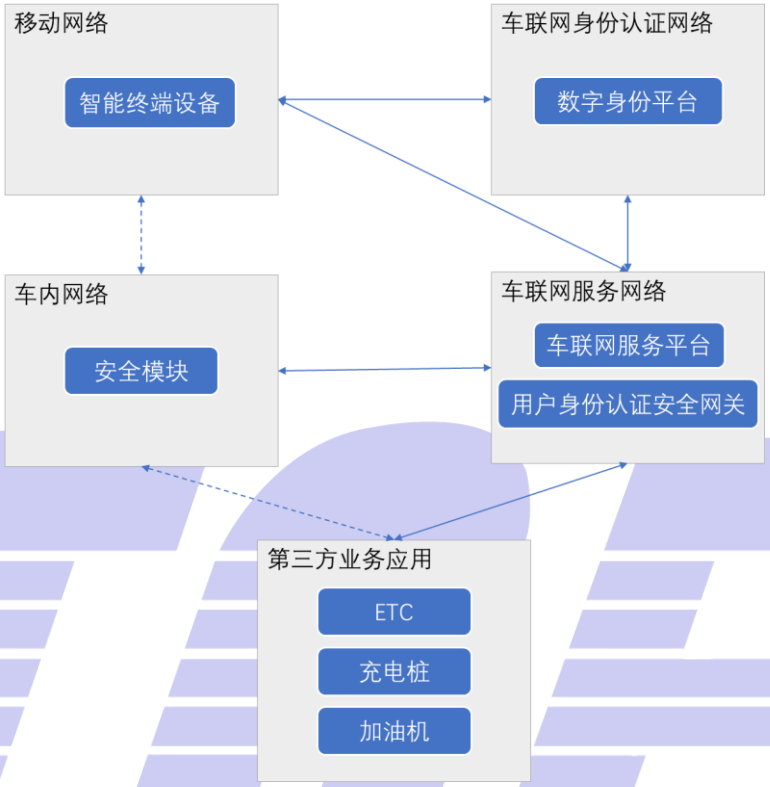

图 1 车联网服务用户身份认证技术架构参考实现

该技术架构参考实现主要包括移动网络、车联网身份认证网络、车内网络、车联网服务网络与第三方业务应用五个部分，不同部分之间通过短距离或远距离通信方式进行通信与数据交换。其中虚线表示短距离通信方式，例如NFC、UWB、蓝牙等；实线表示远距离通信方式，例如WiFi、蜂窝网等。

移动网络中主要包含智能终端设备及其通信网络，智能终端设备在系统中是用户与认证系统交互的唯一接口。

车联网身份认证网络主要包含车联网数字身份平台等，车联网数字身份平台对移动网络中产生的数字身份标识进行加解密、二次运算等操作。

车内网络主要包括车内安全模块，例如SE、TEE或其他具备相同安全功能的安全部件。车内网络主要对数字身份标识进行安全存储并提供硬件加解密接口，供车内应用调用。

车联网服务网络主要包括车联网服务平台、用户身份认证安全网关等。车联网服务网络主要为车企提供的应用服务，例如查询车辆唯一识别号、管理钥匙数据等。

第三方业务应用主要包括加油机、充电桩、ETC路侧单元等。

其中，将车联网数字身份平台和车联网服务平台统称为后台服务器。

5.2 应用场景

用户在注册开通车联网服务用户身份认证服务后，其主要应用场景包括车主实名认证、车主无感支付、车辆开锁等。

a) 车主实名认证：利用车联网数字身份平台，对车主或车辆使用者进行实名认证及电子证照验证等；
b) 车主无感支付：利用车联网数字身份平台，第三方业务应用（ETC、充电桩、加油机等）基于身份认证自动识别车辆和车主信息，实现自动结算、离场自动扣除等服务；
c) 车辆开锁：基于身份认证实现无钥匙开锁。

6 安全风险

6.1 概述

车联网服务用户身份认证是在用户、终端设备、车辆与车联网服务网络、车联网身份认证网络及第三方应用之间通过数字身份标识在各业务流程中进行的身份认证。身份认证过程中，可能存在非法用户使用车联网服务、用户数据被窃取、泄露或篡改等风险。车联网服务用户身份认证安全风险具体体现在身份识别、认证过程、后台服务器、网络和个人信息等方面。

6.2 身份鉴别

车联网服务用户身份认证应用场景中的用户身份识别可能存在的安全风险，主要包括口令泄露、口令被伪造、被重放、生物特征信息被窃取等。

6.3 后台服务器

车联网服务用户身份认证应用场景中，后台服务器可能受到的安全风险主要包括非授权物理访问、非授权远程访问、信息泄露、信息破坏等。

6.4 网络

车联网服务用户身份认证应用场景中，可能存在的网络风险包括网络传输数据被非法读取或篡改、网络数据包或报文被重放等。

6.5 数据和个人信息

车联网服务用户身份认证应用场景中，终端设备和车辆系统中存储和传输的身份认证相关的数据和个人信息可能受到的安全风险包括身份认证相关个人信息泄露、密钥泄露、身份伪造等。

7 安全技术要求

7.1 身份鉴别安全

7.1.1 基本要求

车联网服务用户身份认证应用场景中，各主体之间建立通信信道时，应具备双向认证机制，保证通信双方身份的真实性。

7.1.2 口令

车联网服务用户身份认证应用场景中，若使用口令，应满足以下要求：

a） 身份鉴别口令应具备一定的复杂度；
b） 应提供身份鉴别口令多次验证失败的处理功能；
c） 应采取措施保证各主体间传输口令的保密性、完整性和抗重放性。

7.1.3 生物特征识别

车联网服务用户身份认证应用场景中，若采用生物特征识别，应满足以下要求：
a） 应满足 GB/T 40660—2021 中对生物特征识别信息的要求；
b） 针对本地生物特征识别，应同时满足以下要求：
1） 应提供生物特征数据连续识别失败的处理机制；
2） 应加密存储生物特征数据。
c） 针对远程生物特征识别，应同时满足以下要求：
应加密传输生物特征识别数据，并具有重放保护能力。

7.2 后台服务器安全

车联网服务用户身份认证应用场景中，后台服务器应满足以下要求：
a） 后台服务器应具备访问权限控制功能，防止越权访问；
b） 后台服务器应保证密钥在生成、传输、存储、使用、注销和更新时的完整性与机密性；
c） 后台服务器应保证对密钥的相关操作过程不可复制、不可重放。

7.3 网络安全

车联网服务用户身份认证应用场景中，应满足以下网络安全要求：
a） 车联网服务用户身份认证应用场景中，应通过建立安全通信链路或采用密码机制对传输数据进行加密，以保证传输数据的机密性；
b） 车联网服务用户身份认证应用场景中，应采用密码机制保证数据传输完整性；
c） 车联网服务用户身份认证应用场景中，应采用机制防止数据包或报文的重排或重放，可使用序列码或时间戳实现抗重放攻击功能。

7.4 数据安全和个人信息保护

7.4.1 数据安全

车联网服务用户身份认证应用场景中，若对身份识别信息进行存储，应满足以下数据安全要求：
a） 应加密存储用户生物特征等敏感数据，用于加密的密钥应妥善保存，防止被直接获取；
b） 所采用的加密算法应支持国际主流的标准加密算法，若支持国密算法，则应符合国家密码管理机构的相关规定；
c） 对共享类应用（如共享汽车等应用场景），在当前用户退出后，应删除敏感个人信息。

7.4.2 个人信息保护

车联网服务用户身份认证应用场景中，应采取措施保护用户个人信息，具体应满足以下要求：
a） 对个人信息的手机应在提供相应服务的同时进行，若出于业务需要收集个人信息，应在收集前明示收集的目的和范围，并且只有在用户同意之后才可继续；
b） 当用户撤销授权同意后，应停止收集和使用用户数据，历史收集的个人数据应及时删除或进行匿名化处理；
c） 对外共享、转让个人信息前，应事先征得用户明示同意，并按照约定目的和用途进行，传输之

前应对双方进行身份认证和授权；

d) 对收集、加工、转移阶段所使用的个人信息的缓存数据，应提供自动删除或授权用户手动删除功能。

7.5 业务安全

7.5.1 用户注册

车联网服务用户注册场景中，除满足 7.1-7.5 的要求，还应满足以下要求：

a) 生成的用户和车辆数字身份标识应具有唯一性；

b) 注册开通流程中，应采用措施保证各主体间传输数据的保密性和完整性；

c) 应对用户个人数据、车牌号码等敏感信息进行加密存储；

d) 用户取消注册时，应能够提供手段清除遗留数据。

7.5.2 无感支付

车联网服务无感支付场景中，除满足 7.1-7.5 的要求，还应满足以下要求：

a) 应对支付请求来源进行真实性验证；

b) 应采用措施保证无感支付流程中，各主体间传输支付指令时具有加密传输和重放保护能力。

7.5.3 车辆开锁

车联网服务车辆开锁场景中，除满足 7.1-7.5 的要求，还应满足以下要求：

a) 应对开锁指令进行完整性和来源可靠性校验；

b) 应采用措施保证车辆开锁流程中，各主体间传输开锁指令时具有加密传输和重放保护能力。

附 录 A
（资料性）
业务流程

A.1 注册流程

注册指车联网应用场景中的用户注册开通身份认证服务的基本流程，主要流程如图A.1所示。

a） 用户通过终端设备发起注册开通申请；
b） 数字身份平台接到申请后查询用户驾驶证，加密生成用户数字身份标识；
c） 数字身份平台将生成的用户数字身份标识返回终端设备；
d） 注册开通后，用户进行添加车辆申请；
e） 数字身份平台接到申请后向车联网服务网络发起车辆信息查询，确认用车权力等信息；
f） 车联网服务网络通过安全网关向数字身份平台返回车辆信息；
g） 数字身份平台进行驾驶证查询，加密生成车辆数字身份标识；
h） 数字身份平台将车辆数字身份标识下发到终端设备；
i） 同时，数字身份平台将用户和车辆数字身份标识下发到车联网服务网络；
j） 车联网服务网络最后将两种标识也下发到车内网络安全模块。

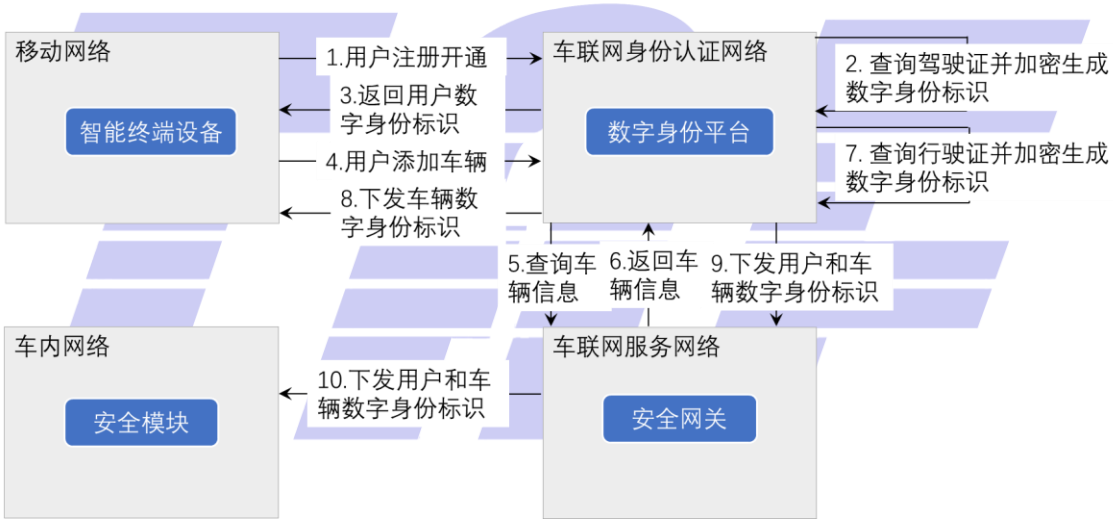

图 A.1 用户注册开通身份认证服务基本流程

A.2 认证流程

A.2.1 概述

认证指在不同车联网应用场景中对用户身份进行认证的特定流程，不同场景适用的认证流程有所不同。本文件中主要叙述适用于以下场景中的认证流程。

A.2.2 实名认证

车主实名认证基本流程如图A.2所示：

a） 车主通过终端设备发起实名认证申请；
b） 数字身份平台接到申请后进行行驶证/驾驶证查询，加密生成数字身份标识；
c） 数字身份平台数字身份标识下发到终端设备；
d） 同时，数字身份平台将数字身份标识也一并下发到车联网服务网络；

e） 最后，车联网服务网络将接收到的数字身份标识下发给车内网络安全模块。

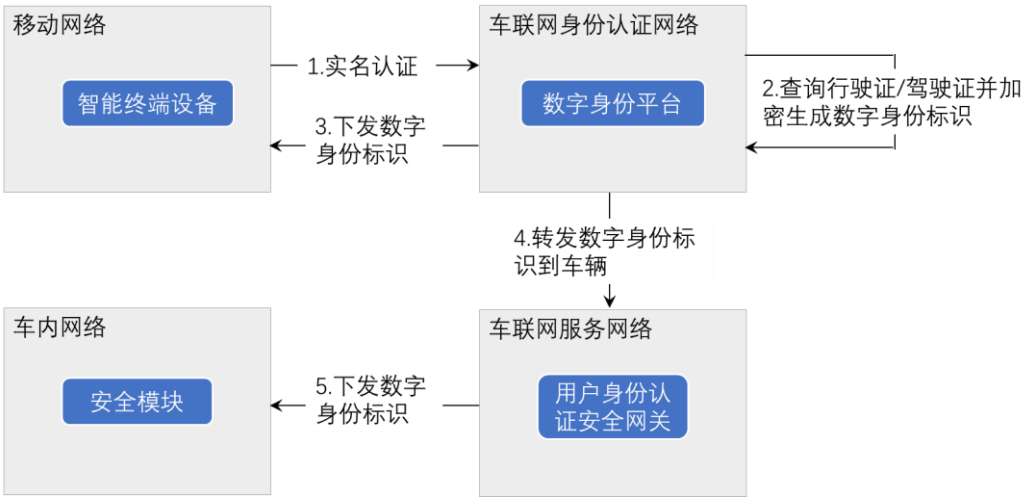

图 A.2 车主实名认证基本流程

A.2.3 无感支付

车主无感支付基本流程如图A.3所示：

a） 车主进行无感支付时，第三方业务应用向车内网络安全模块读取数字身份标识；

b） 同时，第三方业务应用向 TSP 提交支付请求；

c） TSP 接收到支付请求后，通过用户身份认证安全网关向数字身份平台申请数字身份认证；

d） 数字身份平台对数字身份标识进行解密验签；

e） 数字身份平台向用户身份认证安全网关返回验证结果；

f） 最后将验证结果返回 TSP，完成支付。

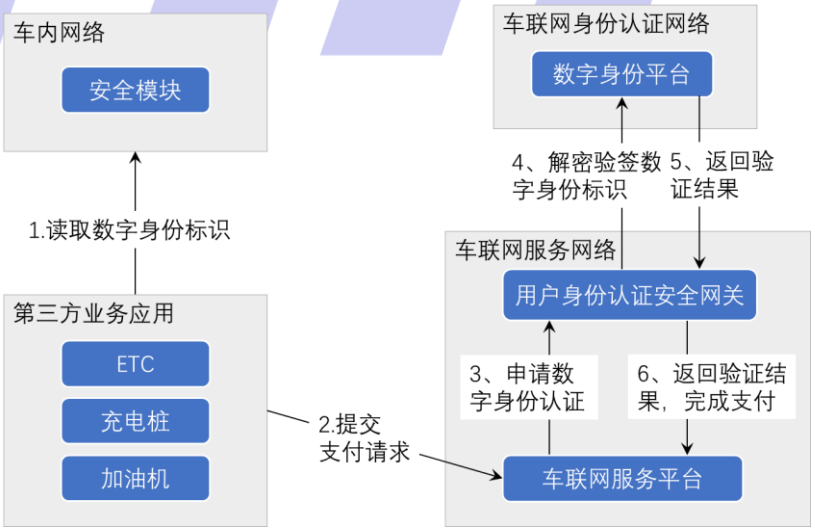

图 A.3 车主无感支付基本流程

A.2.4 车辆开锁

车辆开锁分为近距开锁和远程开锁。

近距开锁基本流程如图A.4所示：

a） 用户通过终端设备发起开锁指令，并加密签名数字身份标识；

b） 车内网络安全模块对数字身份标识进行解密验签，若比对成功即完成开锁；

c） 车内网络安全模块向终端设备返回开锁结果。

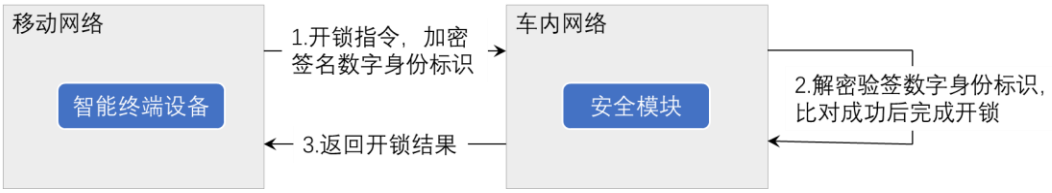

图 A.4　车辆近距开锁基本流程

远程开锁基本流程如图A.5所示：

a） 用户通过终端设备发起远程开锁指令，并加密签名数字身份标识；

b） 用户身份认证安全网关将远程开锁指令转发给车内网络安全模块；

c） 车内网络安全模块将数字身份标识进行解密验签，若对比成功即可完成开锁；

d） 车内网络安全模块将开锁结果返回用户身份认证安全网关；

e） 最后，开锁结果返回到终端设备。

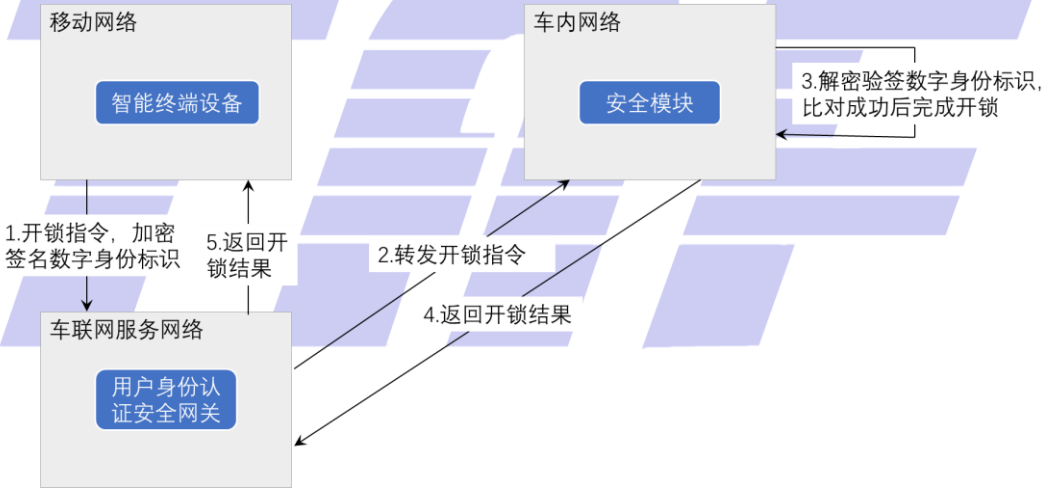

图 A.5　车辆远程开锁基本流程

电信终端产业协会团体标准

车联网服务用户身份认证安全技术要求

T/TAF 191—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn