


ICS 33.050

M 30

团 体 标 准

T/TAF 074-2020



移动智能终端数字车钥匙 信息安全技术要求

Information security technical requirement for
digital vehicle key in smart mobile devices

2020 - 11 -26 发布

2020 - 11 -26 实施

电信终端产业协会 发布

目 次

前言	II
引言	III
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
下列缩略语适用于本文件。	2
4 技术架构	2
4.1 整体架构	2
4.2 车辆服务器	3
4.3 车辆	3
4.4 终端设备服务器	3
4.5 终端设备	3
5 安全威胁和安全目标	7
5.1 数字车钥匙应用软件	7
5.2 数字车钥匙执行环境	7
5.3 通信模块	8
6 安全技术要求	8
6.1 数字车钥匙应用软件	8
6.2 数字车钥匙执行环境	8
6.3 通信模块	11
7 安全能力分级	11

前 言

本标准按照 GB/T 1.1-2020 给出的规则起草。

本标准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这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、华为技术有限公司、蚂蚁科技集团股份有限公司、北京奇虎科技有限公司、OPPO广东移动通信有限公司、北京百度网讯科技有限公司、上海瓶钵信息科技有限公司、北京豆荚科技有限公司、北京雷森科技发展有限公司、北京中广瑞波科技股份有限公司、郑州信大捷安信息技术股份有限公司、上海果通通信科技股份有限公司。

本标准主要起草人：李煜光、国炜、魏凡星、路晔绵、常新苗、王思善、林冠辰、马志远、张屹、姚一楠、李根、潘蓝兰、李显杰、李笑如、程唐平、张智盛、窦丽娟、刘富洋、周鹏、连莉华、朱旭东、康亮、刘为华、李勋宏、彭成。



引 言

移动智能终端设备与相关技术在近几年迅速发展，承载了越来越多的与衣食住行相关的功能，此时移动智能终端产品不仅作为通信工具，还可作为银行卡、交通卡、智能家居控制终端等功能使用。移动智能终端设备作为车钥匙的功能是近几年的出现的热门技术之一，该功能也叫做数字车钥匙。与传统车钥匙不同数字车钥匙无需额外的实体车钥匙，而是将车钥匙功能集成在移动智能终端设备中，基于SE、TEE等安全技术，使用NFC、蓝牙、蜂窝网络、WIFI等技术实现车辆的开门、启动等功能。

数字车钥匙是智能网联车的重要革新功能之一，已经有部分车辆制造企业与移动智能终端设备厂商着手开发并提出数字车钥匙解决方案。然而现在业内还缺少相应的标准来保证开发过程的一致性与安全性，这将严重影响该技术的实际落地过程，也会使消费者的用户体验大打折扣。因此，本标准的立项旨在解决上述问题，重点解决移动智能终端设备数字车钥匙功能中的信息安全问题。本标准适用于移动智能终端设备商、移动智能终端应用商、智能网联车解决方案供应商与车辆制造企业等，可为我国相关产业提供产品安全技术依据，为行业市场做参考性指导。

对标准中的具体事项，法律法规另有规定的，需遵照其规定执行。



移动智能终端数字车钥匙信息安全技术要求

1 范围

本标准规定了基于移动互联网的数字车钥匙信息安全的技术要求，包括数字车钥匙执行环境、应用软件、通信模块和用户隐私等。由于现有数字车钥匙实现方案各异，因此本标准根据数字车钥匙的不同实现方案，提出了不同的信息安全技术要求。

本标准适用于各种制式的移动智能终端中实现的数字车钥匙功能。

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。凡是注日期的引用文件，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 32915—2016 信息安全技术 二元序列随机性检测方法

YD/T 2844.1-2015 移动终端可信环境技术要求 第1部分：总体

YD/T 2844.2-2015 移动终端可信环境技术要求 第2部分：可信执行环境

YD/T 2844.3-2015 移动终端可信环境技术要求 第3部分：安全存储

YD/T 2844.4-2015 移动终端可信环境技术要求 第4部分：操作系统的安全保护

YD/T 2844.5-2016 移动终端可信环境技术要求 第5部分：与输入输出设备的安全交互

YD/T 2407—2017 移动智能终端安全能力技术要求

TAF-WG4-AS0008-V1.0.0:2017移动终端安全环境安全评估内容和方法

3 术语、定义和缩略语

3.1 术语和定义

3.1.1

移动智能终端 mobile intelligent terminal

能够接入移动通信网，具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行应用程序的移动终端。

3.1.2

数字车钥匙 digital key

在用户访问车辆时用于身份认证的数字凭证，可实现解锁、上锁车门，启动、关闭发动机引擎等功能。

3.1.3

钥匙追踪服务器 key tracking server

由车辆企业管理，用于记录数字车钥匙状态与储存相关隐私信息。

3.1.4

安全单元 secure element

位于设备中的一种防篡改硬件安全部件，用于保证设备的安全性与机密性，安全单元具有多种形态，包括eSE、inSE、SIM/UICC、智能卡、智能microSD卡等。

3.1.5

安全应用 applet

位于安全单元中实现相关安全功能的应用。例如数字车钥匙的SE实现中，数字车钥匙的加密、签名、密钥存储等核心安全功能在一个安全应用中实现。

3.2 缩略语

下列缩略语适用于本文件。

CA	代理应用	Client Application
DK	数字车钥匙	Digital Key
DoS	拒绝服务攻击	Denial of Service
ECU	电子控制单元	Electronic Control Unit
HCE	主机卡模拟	Host-based Card Emulation
KTS	钥匙追踪服务器	Key Tracking Server
NFC	近场通信	Near Field Communication
OTA	空中下载	Over The Air
REE	非可信执行环境	Rich Execution Environment
RPMB	重放保护内存块	Replay Protected Memory Block
SE	安全单元	Secure Element
TA	可信应用	Trusted Application
TEE	可信执行环境	Trusted Execution Environment
TLS	安全传输层协议	Transport Layer Security
TUI	可信用户界面	Trusted User Interface
UWB	超宽带	Ultra Wide Band

4 技术架构

4.1 整体架构

数字车钥匙系统架构如图1所示，其中主要包括车辆、车辆服务器、终端设备、终端设备服务器、移动服务提供商五个组件。其中移动服务提供商为非必须组件，可用于提供车队管理、数据分析等第三方服务。

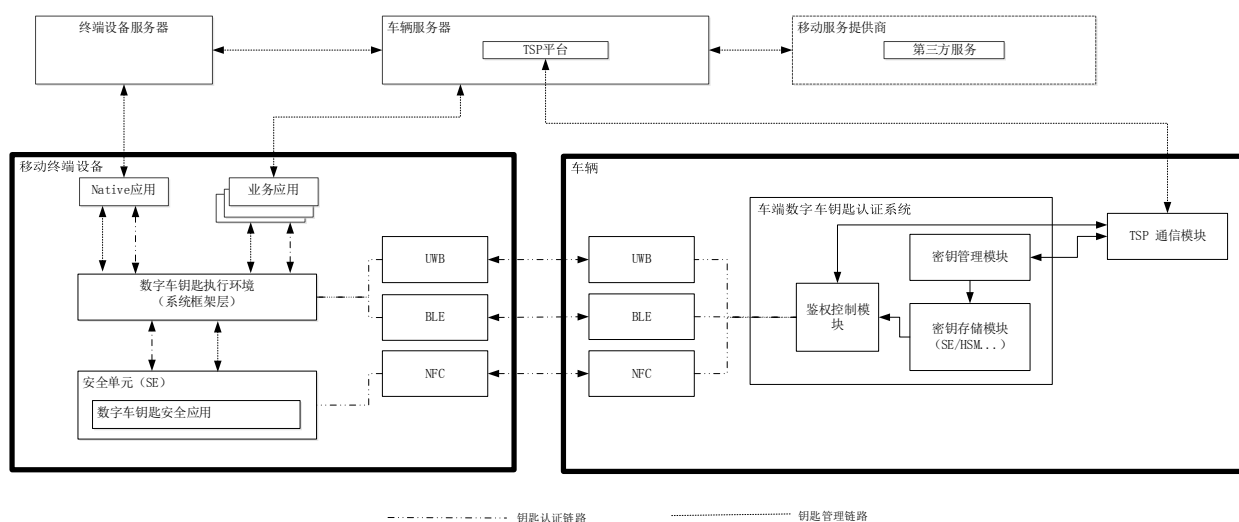


图1 数字车钥匙参考实现架构图

4.2 车辆服务器

车辆服务器负责储存数字车钥匙用户账号信息，对用户进行身份识别与验证、远程下发失效用户或设备信息到车辆端、管理数字车钥匙的开通、使用、分享与撤销等业务功能。

4.3 车辆

车辆负责与车辆服务器交互，对终端设备进行身份验证等功能。

4.4 终端设备服务器

终端设备服务器负责对移动智能终端内数字车钥匙生命周期进行管理，更新终端设备中相关证书，在终端设备丢失时暂停、恢复、擦除钥匙等功能。

4.5 终端设备

4.5.1 概述

终端设备中包括数字车钥匙应用软件、数字车钥匙执行环境与通信模块，共同构建数字车钥匙基本功能。通过使用终端设备中的数字车钥匙，可以实现解锁与上锁车门、启动与停止车辆发动机、开关后备箱功能的功能。

4.5.2 数字车钥匙执行环境

4.5.2.1 概述

数字车钥匙执行环境位于终端设备中，向用户提供数字车钥匙的基本功能，包括车辆与钥匙的配对、车辆开门、启动车辆引擎、钥匙分享等。

数字车钥匙执行环境可使用多种方式实现，包括使用TEE、SE等实现方式。不同实现方式的基本架构与安全要求有所差异，在本标准中分别叙述。

现有数字车钥匙执行环境实现方式包括REE实现，TEE实现，SE实现三种，三种实现方式安全级别依次递增。

数字车钥匙执行环境宜具备监测移动智能终端设备移动网络状态的功能，支持在设备长期不连网的情况下禁用数字车钥匙的功能。

4.5.2.2 REE 实现

该实现方式未使用TEE、SE及其他相关功能，仅通过终端设备操作系统之上的数字车钥匙应用软件实现相关功能。

该实现方式安全级别较低，无法以较高级别保证数字车钥匙的安全性，可能产生车辆被盗取或非法控制、用户隐私泄露等严重安全风险。

该实现方式的基本架构如图2所示。

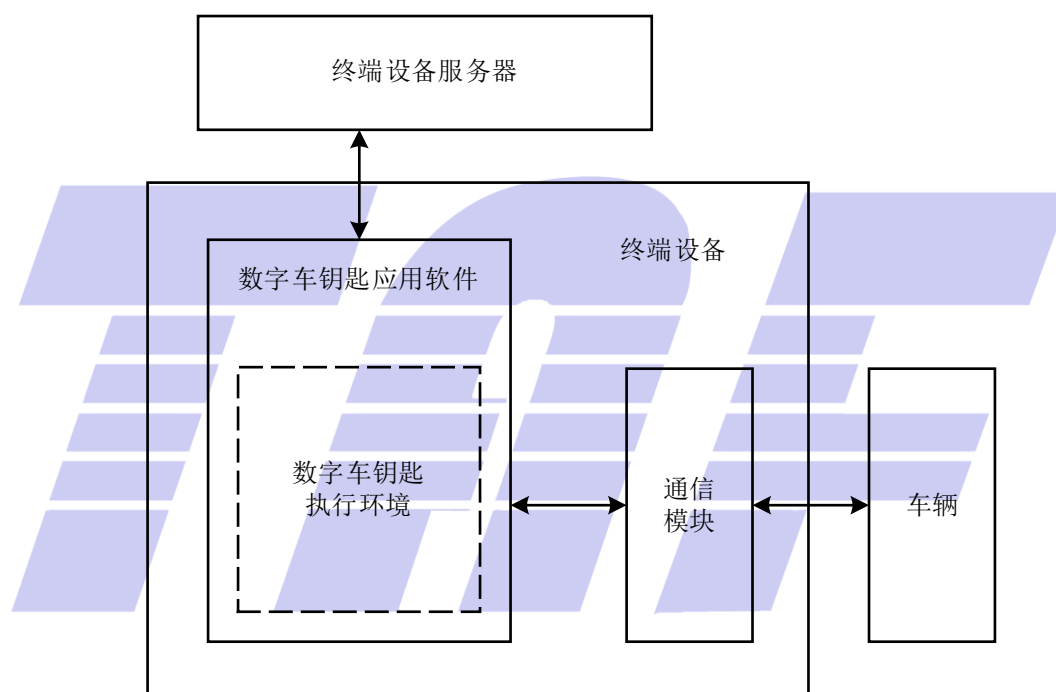


图2 数字车钥匙执行环境应用软件实现架构图

4.5.2.3 TEE 实现

4.5.2.3.1 基本架构

该实现方式使用TEE相关功能保证数字车钥匙的安全性。

该实现方式的基本架构如图3所示。

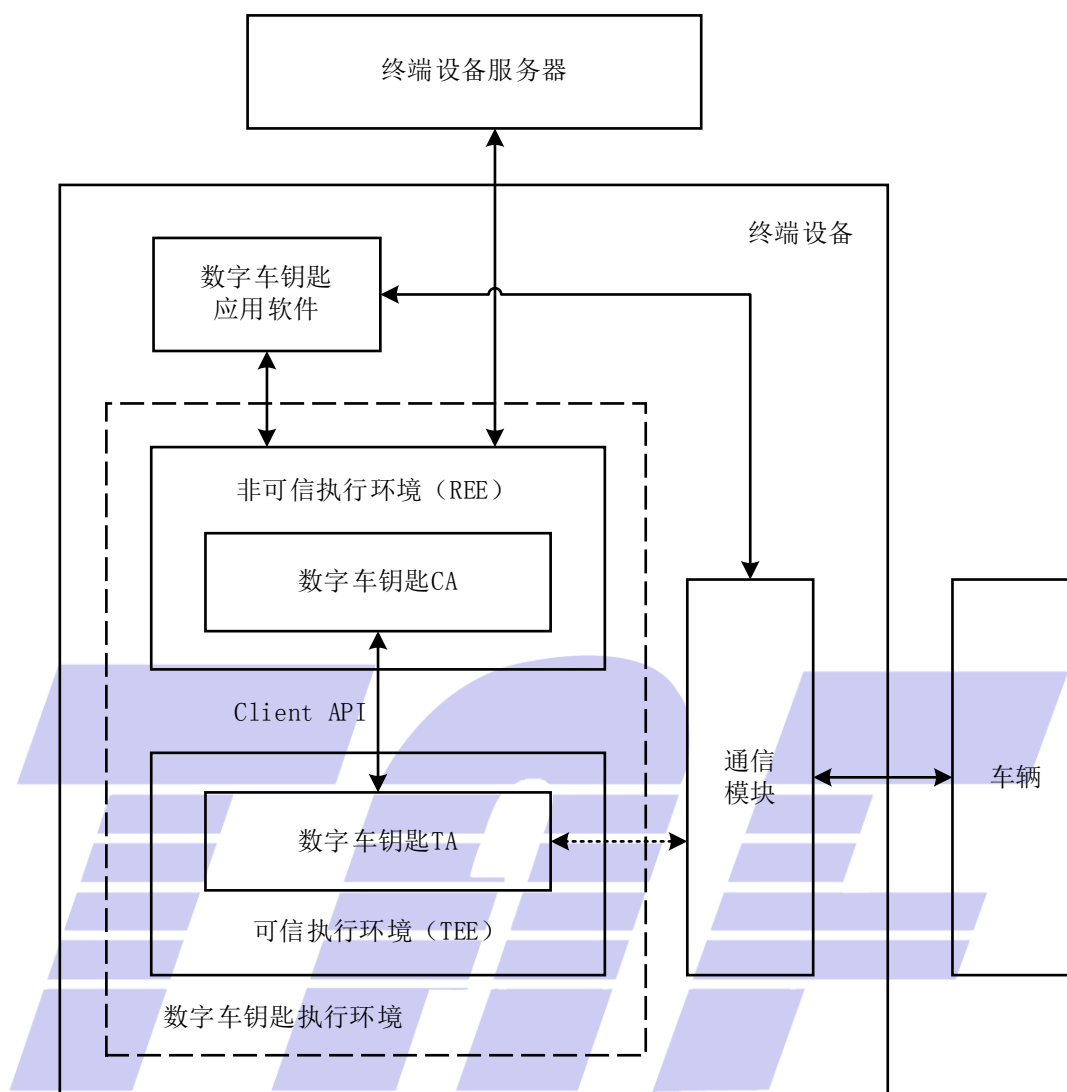


图3 数字车钥匙执行环境 TEE 实现架构图

4.5.2.3.2 可信执行环境（TEE）

可信执行环境是存在于移动终端设备内，与REE相分离的安全区域，具体实现可以是主处理器的一种安全模式，也可以是与主处理器相隔离的协处理器。可信执行环境可提供基本的安全功能，包括安全存储、安全启动、隔离机制等。

4.5.2.3.3 数字车钥匙 TA

数字车钥匙TA为在TEE中执行的应用程序，TA可以调用TEE提供的安全接口，包括创建安全存储对象、生成随机数等。

4.5.2.3.4 非可信执行环境（REE）

非可信执行环境是存在于移动终端设备内，与TEE相分离的非安全区域。

4.5.2.3.5 数字车钥匙 CA

数字车钥匙CA为代理应用程序，可在REE中执行。数字车钥匙的上层功能可在CA中实现，包括车辆配对、钥匙分享等。CA可以通过调用Client API执行TEE中的TA，实现TEE提供的基本安全功能。

4.5.2.4 SE 实现

4.5.2.4.1 基本架构

该实现方式适用于终端设备有SE的情况，使用SE与TEE分别实现核心安全功能与附加安全功能，以保证数字车钥匙的安全性。该方式将数字车钥匙的加密、签名、密钥存储等核心安全功能在位于SE的数字车钥匙安全应用中实现，并使用安全通道与车辆通信；将数字车钥匙的TUI、免密认证机制等附加安全功能在TEE中实现。

该实现方式的基本架构如图4所示。

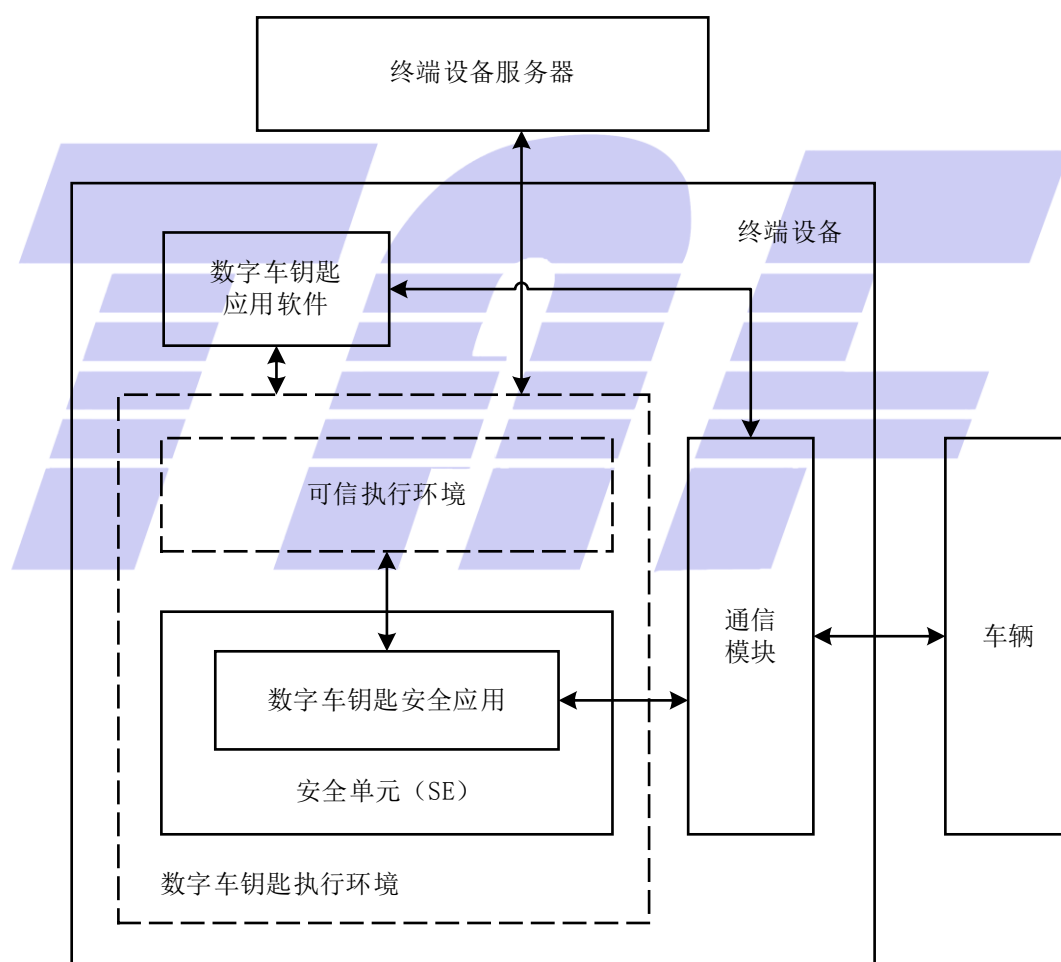


图4 数字车钥匙执行环境 SE 实现架构图

4.5.2.4.2 可信执行环境

可信执行环境中实现车钥匙非核心安全功能，包括TUI、免密认证机制（人脸识别、指纹识别、声纹识别、虹膜识别）、安全外设等。

4.5.2.4.3 安全单元

位于SE的安全应用中实现车钥匙核心安全功能，安全单元向安全应用提供安全函数调用接口，包括安全存储、安全启动、硬件加密、安全通道等。

4.5.2.4.4 数字车钥匙安全应用

数字车钥匙安全应用用于实现钥匙相关功能。所有车辆企业的数字车钥匙核心代码与数据预置在一个数字车钥匙安全应用中，包括密钥、防盗器令牌等。数字车钥匙安全应用使用SE相关功能创建安全通道并通过通信模块与车辆通信，通过终端设备中的数字车钥匙系统服务与终端设备服务器进行通信。

4.5.3 数字车钥匙应用软件

数字车钥匙应用软件位于终端设备中，根据数字车钥匙执行环境的不同实现方式，具备不同的功能。在使用应用软件实现方式时，数字车钥匙应用软件具备数字车钥匙的所有功能；而在使用其他方式实现时，数字车钥匙应用软件仅具备相关非安全功能，包括提供用户交互界面、展示车钥匙配对状态等。

4.5.4 通信模块

通信模块位于终端设备中，提供数字车钥匙执行环境与车辆的通信服务。通信模块可提供NFC、蓝牙、UWB等通信方式，其安全需求有所差异。

5 安全威胁和安全目标

5.1 数字车钥匙应用软件

数字车钥匙应用软件安全威胁包括应用软件受到篡改、逆向、动态调试等，泄露敏感数据或造成数字车钥匙功能失效。

数字车钥匙应用软件安全目标包括保护敏感数据与保障功能有效性。

5.2 数字车钥匙执行环境

5.2.1 钥匙数据

5.2.1.1 密钥

密钥安全威胁包括泄露、篡改与非法访问根密钥及其衍生密钥。

数字车钥匙执行环境安全目标包括提供可以抗侧信道攻击、错误注入攻击等物理攻击的安全密码算法。

5.2.1.2 随机数发生器

随机数发生器安全威胁包括外部条件干扰随机数发生器，导致其产生不可靠密钥。

数字车钥匙执行环境安全目标包括保证随机数发生器的可靠性。

5.2.1.3 数字车钥匙证书

数字车钥匙证书安全威胁包括泄露、篡改与非法访问证书。

数字车钥匙执行环境安全目标包括保证证书的机密性、完整性。

5.2.1.4 数字车钥匙用户数据

数字车钥匙用户数据安全威胁包括泄露、篡改与非法访问数字车钥匙中用户数据。

数字车钥匙执行环境安全目标包括保证数字车钥匙用户数据机密性、完整性。

5.2.2 钥匙代码

钥匙代码安全威胁包括恶意代码植入、代码非法访问等。

数字车钥匙执行环境安全目标包括保证钥匙代码的机密性、完整性。

5.2.3 钥匙系统功能

钥匙系统功能安全威胁主要包括以下几点：

- 1) 非法用户使用数字车钥匙，导致非法使用车辆。
- 1) 阻碍删除终端设备中数字车钥匙数据的过程，导致非法使用数字车钥匙功能。
- 2) 终端设备中并存多个车辆企业的数字车钥匙时，不安全的隔离机制可能产生安全风险。

数字车钥匙执行环境安全目标包括保证用户使用钥匙功能时具备用户身份认证（authentication）机制、已删除钥匙防恢复机制、钥匙迁移时不泄露隐私信息、终端设备中存在多个钥匙数据的安全隔离机制。

5.3 通信模块

通信模块安全威胁包括针对NFC、蓝牙等通信协议，进行协议降级、中间人攻击、中继攻击、嗅探攻击等，影响数字车钥匙系统的安全性。

通信模块安全目标包括防止协议降级、中间人攻击、中继攻击、重放攻击、嗅探攻击等。

6 安全技术要求

6.1 数字车钥匙应用软件

6.1.1 应用安全加固

数字车钥匙应用软件应进行安全加固，具备防篡改、防逆向、防动态调试等能力。

6.2 数字车钥匙执行环境

6.2.1 基本安全要求

6.2.1.1 终端安全能力

移动智能终端宜被ROOT后无法使用数字车钥匙相关功能。

移动智能终端应在数字车钥匙应用运行前对其完整性进行校验。

6.2.1.2 创建验证

在从移动智能终端侧创建新的数字车钥匙时，应对用户进行身份认证。

6.2.1.3 分享验证

在从移动智能终端侧使用钥匙分享功能向好友设备分享钥匙时，应对用户进行身份认证。

6.2.1.4 分组密码算法

数字车钥匙应使用安全分组密码算法，强度不应低于SM4-128、AES-128，加密模式宜采用GCM、CTR、CBC模式。

6.2.1.5 公钥密码算法

数字车钥匙应使用安全公钥密码算法与签名算法，强度不应低于SM2-256、ECC-256、RSA-2048、ECDSA-256。

6.2.1.6 密钥协商算法

数字车钥匙系统应使用安全密钥协商算法，强度应基于6.2.1.5中所叙述的安全公钥密码算法实现。

6.2.1.7 哈希函数

数字车钥匙应使用安全哈希函数，强度不应低于SM3-256、SHA-256。

6.2.1.8 TLS

数字车钥匙应使用TLS 1.2及以上版本或同等强度TLS协议。

6.2.1.9 密钥安全性

数字车钥匙应保证密钥在生成、存储、使用与删除时的完整性与机密性。

6.2.1.10 防复制

数字车钥匙应保证钥匙功能与移动智能终端设备的绑定，保证钥匙数据非法复制到其他设备之后，无法使用数字车钥匙相关功能。

6.2.1.11 安全环境

数字车钥匙应保证密钥和业务核心数据在生成、存储、使用、删除与更新时的完整性与机密性，还应保证对密钥和业务核心数据的相关操作过程不可重放。

移动智能终端应具备安全环境以实现安全启动、安全存储、隔离机制等功能，安全环境包括TEE、HSM或SE。

6.2.2 REE 实现增强要求

6.2.2.1 白盒密码算法库

数字车钥匙执行环境应具备白盒密码算法库，所支持的密码算法包括但不限于AES。

6.2.2.2 白盒密码算法调用

数字车钥匙工作过程对数据进行加解密时，应调用执行环境提供的白盒密码算法库。

6.2.3 TEE 实现增强要求

6.2.3.1 TEE 可信用户界面

数字车钥匙应使用TEE的TUI功能向移动智能终端提供可信用户界面，包括安全显示与安全输入机制。

6.2.3.2 TEE 安全存储

数字车钥匙TEE应具备安全存储机制，包括内容加密、防篡改、防回滚。

6.2.3.3 TEE 数据清除

数字车钥匙TEE应保证在清除敏感信息时，内存中的相应数据被有效清除且不可恢复。

6.2.3.4 TEE 随机数发生器

数字车钥匙TEE应具备随机数发生器，钥匙TA、钥匙CA应使用的TEE提供的随机数生成器生成随机数。

6.2.3.5 TA 代码完整性

数字车钥匙TA代码在被加载时应保证代码的完整性。

6.2.3.6 TA 安全隔离

数字车钥匙TEE应具备隔离机制，保证钥匙TA的数据与代码无法被REE与其他TA非法访问与篡改。

6.2.3.7 TA 安全存储

数字车钥匙TA应保证存储证书、密钥等核心敏感数据时的完整性与机密性。

6.2.3.8 TA 密码算法

数字车钥匙TA应使用TEE中提供的安全分组密码算法、安全公钥密码算法与安全哈希函数。

6.2.4 SE 实现增强要求

6.2.4.1 SE 密码算法

SE应提供可以抗侧信道攻击、错误注入攻击等物理攻击的硬件加密模块，密码算法包括但不限于AES、RSA。

6.2.4.2 SE 数据清除

数字车钥匙所使用的SE应保证在清除敏感信息时，内存中的相应数据被有效清除且不可恢复。

6.2.4.3 SE 防篡改检测

数字车钥匙所使用的SE应具备检测固件与安全应用是否被恶意篡改的功能。若检测到被篡改，则SE应终止安全应用的相关操作。

6.2.4.4 SE 隔离机制

数字车钥匙所使用的SE应具备有效的隔离机制保证安全应用之间相互隔离。

6.2.4.5 SE 随机数发生器

数字车钥匙所使用的SE应提供满足GB/T 32915或NIST SP 800-22要求的随机数发生器。

6.2.4.6 安全应用密码算法

数字车钥匙安全应用执行加/解密、签名/验签操作时，应使用SE硬件加密模块中的安全算法。

6.2.4.7 安全应用敏感数据安全

数字车钥匙安全应用应使用SE的相关安全机制，保证数字车钥匙中的所有证书、密钥等核心敏感数据在生成、存储、使用和删除过程中的完整性和机密性。

6.2.4.8 安全应用随机数

数字车钥匙安全应用内部生成的所有随机数应使用SE中的随机数发生器生成。

6.3 通信模块

6.3.1 通信协议加密

数字车钥匙与车辆通信时，应对通信数据进行完整性和机密性保护。

若数字车钥匙执行环境使用TEE/SE实现，则应使用TEE/SE中的加解密模块、随机数发生器等相关安全机制实现该项安全要求。

6.3.2 双向认证

数字车钥匙与车辆建立通信信道时，应具备双向认证机制，保证通信双方身份的真实性。

6.3.3 通信协议抗攻击

数字车钥匙与车辆通信时所使用的通信协议应具备抵抗协议降级、中间人攻击、重放攻击、嗅探攻击的能力。

6.3.4 抗中继攻击

数字车钥匙与车辆通信时，宜具备缓和中继攻击的保护能力。

6.3.5 蓝牙通信安全

应使用强加密算法，配置加密密钥时建议选择允许的最大长度，并定期进行更换；

应使用具备防中间人攻击、防窃听、防重放的安全配对模式进行设备配对，且应在每次的配对中使用随机密钥。

7 安全能力分级

本标准依据移动智能终端数字车钥匙的实现方式与安全功能要求的差异，将安全能力级别划分为三级，其中一级、二级与三级安全能力依次递增，目前最高安全级别为三级。

具体安全能力分级详见表1。

表1 移动智能终端数字车钥匙安全能力分级表

安全能力		安全能力分级		
		一级	二级	三级
1.	应用安全加固	√	√	√
2.	终端安全能力	√	√	√
3.	创建验证	√	√	√

安全能力		安全能力分级		
		一级	二级	三级
4.	分享验证	√	√	√
5.	分组密码算法	√	√	√
6.	公钥密码算法	√	√	√
7.	密钥协商算法	√	√	√
8.	哈希函数	√	√	√
9.	TLS	√	√	√
10.	密钥安全性	√	√	√
11.	防复制	√	√	√
12.	安全环境	√	√	√
13.	白盒密码算法库	√		
14.	白盒密码算法调用	√		
15.	TEE可信用户界面		√	
16.	TEE安全存储		√	
17.	TEE数据清除		√	
18.	TEE随机数发生器		√	
19.	TA代码完整性		√	
20.	TA安全隔离		√	
21.	TA安全存储		√	
22.	TA密码算法		√	
23.	SE密码算法			√
24.	SE数据清除			√
25.	SE防篡改检测			√
26.	SE隔离机制			√
27.	SE随机数发生器			√
28.	安全应用密码算法			√
29.	安全应用敏感数据安全			√
30.	安全应用随机数			√
31.	通信协议加密		√	√
32.	双向认证		√	√
33.	通信协议抗攻击	√	√	√
34.	抗中继攻击			√
35.	蓝牙通信安全	√	√	√

电信终端产业协会团体标准

移动智能终端数字车钥匙信息安全技术要求

T/TAF 074-2020

*

版权所有 侵权必究

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