ICS **
CCS **

团 体 标 准

T/ITS ****—XXXX

车路协同路侧设施证书认证技术规范

Technical Specification of Certificate Authentication of Road Side Facilities on Vehicle Infrastructure Cooperation

（征求意见稿）

（本草案完成时间：2025 年 9 月）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国智能交通产业联盟　　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国智能交通产业联盟（C-ITS）提出并归口。

本文件起草单位：

本文件主要起草人：

引　言

为尽快构建车路协同系统化、整体性的证书认证体系，保障车路信息交互的安全性，规范车路协同路侧设施证书认证体系，编制组在深入调查研究、参考国内外标准，并广泛征求意见的基础上，制定本标准。

本标准可以为车路协同环境下路侧设施的证书认证系统的规划、设计、建设提供参考借鉴。

车路协同路侧实施证书认证技术规范

1 范围

本文件规定了车路协同环境下路侧设施各实体之间实现信息交互安全的证书体系、系统架构、设备证书管理、注册证书管理、应用证书管理、信息安全交互、跨域互信互认以及网络安全要求。

本文件适用于车路协同环境下路侧设施的证书认证系统的规划、设计、建设。

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 37376　　交通运输 数字证书格式

GM/T 0015　　基于SM2密码算法的数字证书格式规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

车路协同 vehicle infrastructure cooperation

车辆、基础设施、人等交通参与主体通过信息交互，实现交通行为的智能协同与配合。

3.2

路侧单元 road side unit

又称路侧设备，安装部署在道路沿线的信息终端，实现交通运行状态、交通事件、道路气象环境、基础设施状态等信息的采集、处理、传输，并实现与车载单元、管理平台、业务平台的信息交互。

3.3

车载单元 on board unit

部署在边缘侧的由计算设施、感知设备及相关附属设备所组成的用于对道路交通参与者、交通事件和交通运行状况、气象环境等进行实时监测、识别和定位的设施系统。

3.4

管理平台 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

3.5

业务平台 service platform

提供交通运行状态、交通事件、道路气象环境、高精度地图等车路协同所需业务服务的系统平台。

3.6

路侧设施 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

3.7

道路运营机构 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

3.8

车辆生产机构 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

3.9

数字证书 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

3.10

实体鉴别 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

3.11

真实性 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

3.12

完整性 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

3.13

机密性 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

3.14

不可否认性 management platform

管理路侧单元的系统平台，实现对路侧单元的策略配置、实时监测、安全管控等功能。

4 缩略语

以下缩略语适用于本文件：

AC：应用证书（Application Certificate）

ACA：应用证书系统（Application Certificate Authority System）

ARCA：应用根证书系统（Application Root Certificate Authority System）

CA：证书签发机构（Certificate Authority）

CRL：证书撤销列表（Certificate Revocation List）

DCA：设备证书系统（Device Certificate Authority System）

DRCA：设备根证书系统（Device Root Certificate Authority System）

EC：注册证书（Enrollment Certificate）

ECA：注册证书系统（Enrollment Certificate Authority System）

ERCA：注册根证书系统（Enrollment Root Certificate Authority System）

RA：注册机构（Registration Authority）

RSU：路侧单元（Road Side Unit）

MA：异常行为管理机构（Misbehavior Authority）

SCMS：安全证书管理系统（Security Credential Management System）

TCMF：可信证书管理功能（Trusted Certificate Management Function）

TDCL：可信域CA证书列表（Trusted Domain CA Certificates List）

TRCLA：可信根证书列表（Trusted Root Certificate List）

5 证书体系

5.1 概述

车路协同环境下路侧设施证书体系包括两部分，一是路侧设施各实体之间实现信息交互安全的证书体系，支持路侧单元之间、与管理平台、与业务平台之间信息交互的真实性、完整性、保密性、不可否认性，保障车路协同路侧设施的安全可靠；二是支持与车载单元信息交互安全的证书体系，实现与车载单元证书体系的互信互任，保障车路通信的安全可靠。

5.2 路侧设施各实体间证书体系

路侧设施各实体间证书体系是三级证书体系，见图1所示。

业务平台证书：标识业务平台身份的机构证书，用于保障业务平台所发送信息的安全性。

管理平台证书：标识管理平台身份的机构证书，用于保障管理平台所发送信息的安全性。

路侧单元设备证书：标识路侧单元身份的设备证书，用于保障路侧单元所发送信息的安全性。

道路运营机构设备根证书：标识道路运营机构所运营的车路协同路侧设施各实体间网络信任锚点的机构证书。

行业车路协同设备根证书：标识交通运输行业车路协同路侧设施各实体间网络信任锚点的机构证书。

业务平台证书、管理平台证书、路侧单元设备证书由道路运营机构签发，通过道路运营机构设备根证书进行验证；道路运营机构设备根证书由交通运输行业电子认证机构签发，通过行业车路协同设备根证书进行验证；行业车路协同设备根证书由交通运输行业电子认证机构自签发，或由国家车路协同业务根证书签发并验证。

平台证书、设备证书格式应符合GM/T 0015要求。

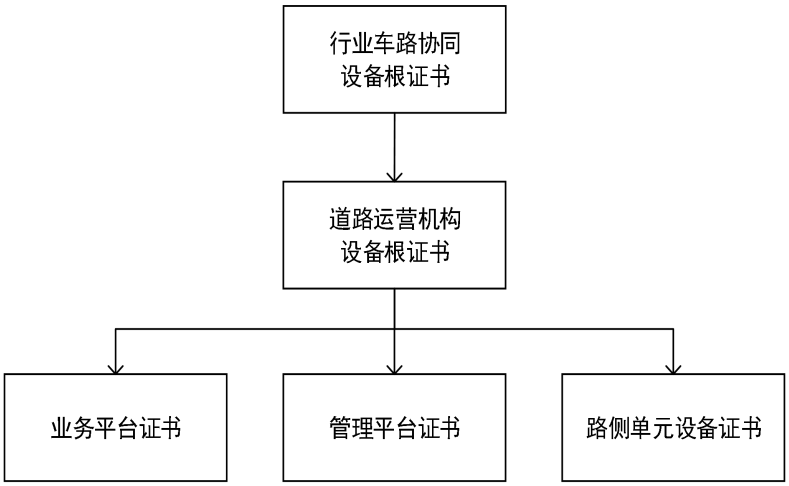

图1 路侧设施各实体间证书体系

5.3 路侧单元与车载单元间证书体系

路侧单元与车载单元间证书体系是三级证书体系，如图2所示。

路侧单元注册证书：标识路侧单元车路信息交互功能的身份证书，用于保障路侧单元应用证书申请、更新数据的安全性。

路侧单元应用证书：标识路侧单元车路协同业务应用的身份证书，用于保障车路协同业务应用消息的安全性。

车载单元应用证书：标识车载单元车路协同业务应用的身份证书，用于保障车路协同业务应用消息的安全性。

道路运营机构注册根证书：标识道路运营机构所运营的车路协同路侧设施与车载单元间信息交互功能网络信任锚点的机构证书。

道路运营机构应用根证书：标识道路运营机构所运营的车路协同路侧设施车路协同业务应用的网络信任锚点的机构证书。

行业车路协同注册根证书：标识交通运输行业车路协同路侧设施与车载单元间信息交互功能网络信任锚点的机构证书。

行业车路协同应用根证书：标识交通运输行业车路协同路侧设施车路协同业务应用的网络信任锚点的机构证书。

路侧单元注册证书、路侧单元应用证书由道路运营机构签发，分别通过道路运营机构注册根证书、应用根证书进行验证；道路运营机构注册根证书、应用根证书由交通运输行业电子认证机构签发，分别通过行业车路协同注册根证书、应用根证书进行验证；行业车路协同注册根证书、应用根证书由交通运输行业电子认证机构自签发，或由国家车路协同业务根证书签发并验证。车载单元应用证书由车辆生产机构签发。

注册证书、应用证书格式应符合GB/T 37376中6.2 ITS设备证书格式要求。

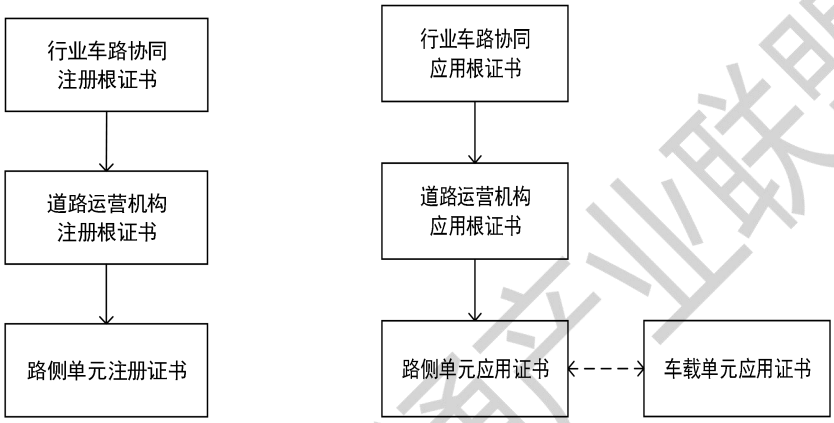

图2 路侧单元与车载单元间证书体系

6 系统架构

车路协同环境下路侧设施证书认证体系如图3所示。

行业车路协同设备根证书系统（TDRCA）：负责行业车路协同设备根证书的生成、更新，管理和维护行业车路协同设备证书体系的信任根；负责审核确认道路运营机构设备根证书系统的合法性，并为其签发、更新机构设备根证书。

行业车路协同注册根证书系统（TERCA）：负责行业车路协同注册根证书的生成、更新，管理和维护行业车路协同注册证书体系的信任根；负责审核确认道路运营机构注册根证书系统的合法性，并为其签发、更新机构注册根证书。

行业车路协同应用根证书系统（TARCA）：负责行业车路协同应用根证书的生成、更新，管理和维护行业车路协同应用证书体系的信任根；负责审核确认道路运营机构应用根证书系统的合法性，并为其签发、更新机构应用根证书。

道路运营机构设备证书系统（DCA）：负责机构设备根证书的申请，管理和维护机构设备根证书；负责审核确认路侧单元、管理平台、业务平台的合法性，并为其签发、更新平台设备证书、平台证书。

道路运营机构注册证书系统（ECA）：负责机构注册根证书的申请，管理和维护机构注册根证书；负责审核确认路侧单元的合法性，并为其签发、更新注册证书。

道路运营机构应用证书系统（ACA）：负责机构应用根证书的申请，管理和维护机构应用根证书；负责审核确认路侧单元的合法性，并为其签发、更新应用证书。

车辆生产机构证书管理系统（VCMA）：负责车辆车路协同业务相关证书的生成、更新，管理和维护车辆车路协同业务相关证书体系的信任根。车辆生产机构证书管理系统根据实际情况可为多级系统。

交通运输行业电子认证机构负责管理与运维行业车路协同设备根证书系统、注册根证书系统、应用根证书系统，应与车辆生产机构证书管理系统建立安全渠道，以实现双方根证书的安全交换；道路运营机构负责管理与运维其运营道路范围内的设备证书系统、注册证书系统、应用证书系统。

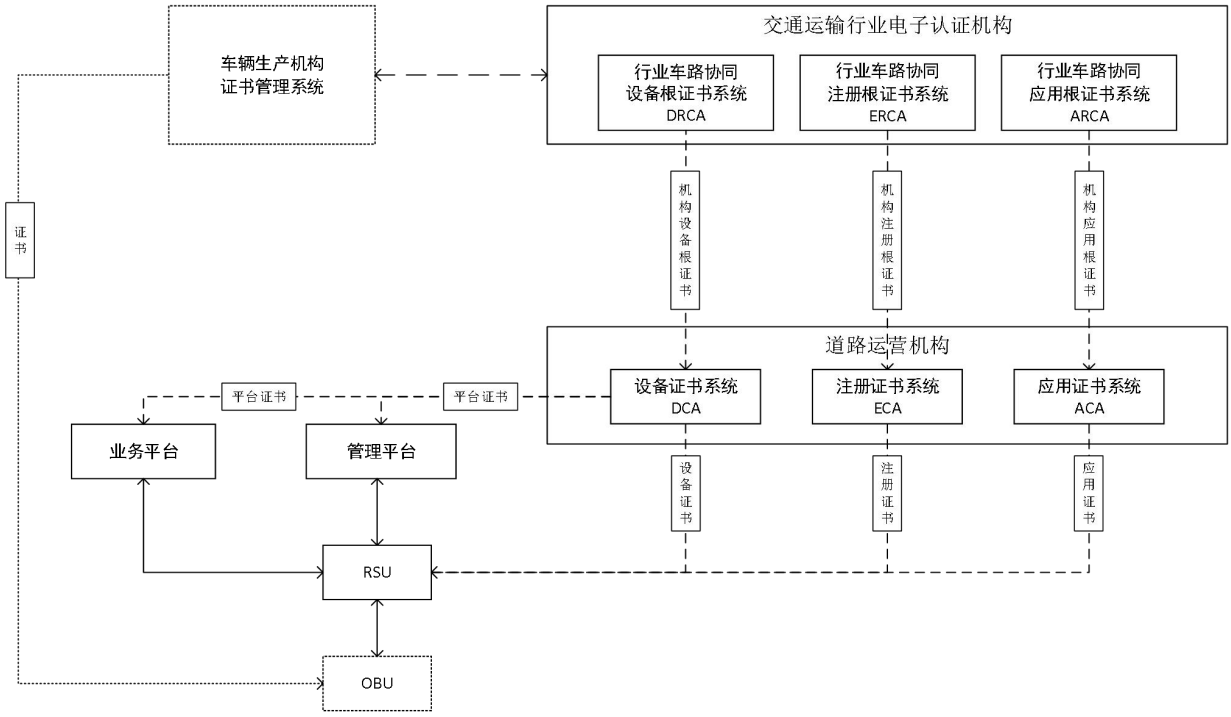

图3 证书管理系统架构图

7 设备证书管理

7.1 设备证书申请流程

路侧单元的设备证书在路侧单元生产过程中的安全环境下生成并写入其安全模块中，或者在安装部署的安全环境中生成并写入其安全模块。业务平台和管理平台的平台证书在其系统安装部署时生成并写入其安全模块。

设备证书中的设备标识应为设备全球唯一标识。

路侧单元设备证书申请流程如下：

a) 路侧单元生成自签名的证书申请数据；
b) 路侧单元将证书申请数据和签名值上传至设备证书系统；
c) 设备证书系统验证证书申请数据通过后，生成路侧单元设备证书；
d) 设备证书系统将路侧单元设备证书及机构设备根证书一起发放给路侧单元；
e) 路侧单元使用机构设备根证书验证路侧单元设备证书的有效性通过后，存储到路侧单元安全区域。

7.2 设备证书更新流程

路侧单元应在设备证书有效期到期前三个月发起设备证书更新流程。流程如下：

a) 路侧单元使用原设备证书对应的私钥对证书更新数据进行签名生成证书更新数据；
a) 路侧单元将证书更新数据和签名值上传至设备证书系统；
b) 设备证书系统使用原设备证书验证证书更新数据以及原设备证书的有效性后，生成更新后的路侧单元设备证书；
c) 设备证书系统将更新后的路侧单元设备证书发放给路侧单元；
d) 路侧单元使用机构设备根证书验证更新后的路侧单元设备证书的有效性通过后，存储到路侧单元安全区域。

7.3 设备证书撤销管理

管理平台实时监控路侧单元的行为状态，当路侧单元发生异常行为时，管理平台通知道路运营机构设备证书系统吊销此路侧单元的设备证书。路侧单元设备证书撤销列表应及时发送给管理平台、业务平台，以及相邻通信的路侧单元。

8 注册证书管理

8.1 注册证书申请流程

路侧单元的注册证书在路侧单元生产过程中的安全环境下生成并写入其安全模块中，或者在安装部署的安全环境中生成并写入其安全模块。

路侧单元中注册证书申请流程如下：

a) 路侧单元使用设备证书对应的私钥对证书申请数据进行签名；
b) 路侧单元将证书申请数据和签名值上传至注册证书系统；
c) 注册证书系统验证证书申请数据通过后，生成路侧单元注册证书；
d) 注册证书系统将路侧单元注册证书及机构注册根证书一起发放给路侧单元；
e) 路侧单元使用机构注册根证书验证路侧单元注册证书的有效性通过后，存储到路侧单元安全区域。

8.2 注册证书更新流程

路侧单元应在注册证书有效期到期前三个月发起注册证书更新流程。流程如下：

a) 路侧单元使用原注册证书对应的私钥对证书更新数据进行签名生成证书更新数据；
b) 路侧单元将证书更新数据和签名值上传至注册证书系统；
c) 注册证书系统使用原注册证书验证证书更新数据以及原注册证书的有效性后，生成更新后的路侧单元注册证书；
d) 注册证书系统将更新后的路侧单元注册证书发放给路侧单元；
e) 路侧单元使用机构注册证书验证更新后的路侧单元注册证书的有效性通过后，存储到路侧单元安全区域。

8.3 注册证书撤销管理

管理平台实时监控路侧单元的行为状态，当路侧单元发生异常行为时，管理平台通知道路运营机构注册证书系统吊销此路侧单元注册证书。

9 应用证书管理

9.1 应用证书申请流程

路侧单元应用证书在安装部署的安全环境中生成并写入其安全模块。路侧单元应用证书申请的安全性由注册证书进行保护；应用证书系统应管理和维护二级注册证书。

路侧单元应用证书申请流程：

a) 路侧单元使用其注册证书对应的私钥对应用证书申请数据进行签名；
b) 路侧单元将应用证书申请数据、签名值及其注册证书上传至应用证书系统；
c) 应用证书系统验证注册证书的有效性及证书申请数据的签名值的有效性后，生成路侧单元应用证书；
d) 应用证书系统将路侧单元应用证书及机构应用根证书一起发放给路侧单元；
e) 路侧单元使用机构应用根证书验证路侧单元应用证书的有效性通过后，存储到路侧单元安全区域。

9.2 应用证书更新流程

路侧单元应在应用证书有效期到期前三个月发起应用证书更新流程。流程如下：

a） 路侧单元使用原应用证书对应的私钥对证书更新数据进行签名生成证书更新数据；
b） 路侧单元将证书更新数据上传至应用证书系统；
c） 应用证书系统使用原应用证书验证证书更新数据以及原应用证书的有效性后，生成更新后的路侧单元应用证书；
d） 应用证书系统将更新后的路侧单元应用证书发放给路侧单元；
e） 路侧单元使用机构应用根证书验证更新后的路侧单元应用证书的有效性通过后，存储到路侧单元安全区域。

9.3 应用证书撤销管理

管理平台实时监控路侧单元的行为状态，当路侧单元发生异常行为时，管理平台通知道路运营机构应用证书系统吊销此路侧单元的应用证书。

道路运营机构应用证书系统及时将路侧单元应用证书吊销列表发送给车辆生产机构证书管理系统。

10 信息交互安全

10.1 路侧设施各实体间信息交互安全

道路运营机构应保障路侧单元之间、路侧单元与管理平台、路侧单元与业务平台、管理平台与业务平台之间信息交互的真实性、完整性、保密性、不可否认性。

路侧设施各实体间信息交互应使用基于设备证书的证书认证体系。

10.2 路侧单元与车载单元信息交互安全

路侧单元广播的消息应包括消息数据、由路侧单元应用证书对应的私钥签名值以及路侧单元应用证书。

车载单元广播的消息格式应符合 YD/T 3594—2019 的规定。

路侧单元证书体系和车载单元证书体系应满足跨域互认。

11 跨域互信互认

11.1 不同道路运营机构证书体系之间的互信互认

交通运输行业电子认证机构应统筹规划车路协同路侧设施的证书体系，生成并管理车路协同路侧设施的行业设备根证书、行业注册根证书、行业应用根证书，并为不同的道路运营机构签发机构设备根证书、机构注册根证书、机构应用根证书。道路运营机构为管理平台、业务平台和路侧单元签发设备证书、注册证书、应用证书。

不同道路运营机构的管理平台、业务平台和路侧单元之间的信息交互由行业根证书、机构根证书构成的根证书链进行安全保障。

11.2 路侧单元证书体系和车载单元证书体系之间的互信互认

交通运输行业电子认证机构应生成并管理车路协同路侧设施的可信根证书列表，并通过安全渠道发送给车辆生产机构，由其写入到车载单元的安全模块中。

车辆生产机构应生成并管理车载单元的可信根证书列表，并通过安全渠道发送给道路运营机构，由其写入到路侧单元的安全模块中。

11.3 可信根证书列表结构

可信根证书列表结构及各字段的用途应符合表1的规定。

表1 可信根证书列表结构

数据域 1	数据域 2	数据域 3	是否必选	说明
版本		version	是	描述列表结构的版本。与本标准对应的版本号为 1
颁发者		issuer	是	签发此列表的证书的 HashedId8 值
序列号		series	是	每次更新列表，序列号应较上一次更新加 1.
颁发时间		issueDate	是	颁发时间
下次颁发时间		nextRootCtl	是	预计下次颁发时间
根证书列表	某可信 PKI 系统相关的数据	rootCertificate	是	某 PKI 系统的可信根 CA 证书
		caListUrl	否	某可信 PKI 系统的可信域 CA 证书列表下载地址
	……	……	/	/
签名值		signature	是	可信根证书列表的签名值

11.4 跨域互信互认过程

以路侧单元与车载单元跨域互信互认为例，过程如下：

a) 车载单元接收路侧设备广播的签名消息；
b) 车载单元获取签名消息中携带的签名证书；
c) 车载单元获取签名证书中证书颁发者标识；
d) 车载单元利用获取的证书颁发者标识在车辆生产机构的可信根证书列表中查找对应的可信根证书或可信根证书链；
e) 车载单元利用可信根证书或可信根证书链验证消息中携带的签名证书；
f) 反之，路侧设备接收到车载单元广播的签名消息后，利用可信根证书或可信根证书链验证消息中携带的签名证书。

12 网络安全要求

12.1 密码应用要求

密码应用技术要求如下：

a) 应采用国家密码管理部门许可的密码算法；
b) 证书及其相关密钥数据应安全保存于物理安全模块中；
c) 应采用国产密码技术支持的鉴别机制实现设备身份认证，确保数据来源于正确的设备；
d) 通过加密和签名服务，保证发送消息的机密性和完整性；
e) 数据传输应支持抗重放攻击。

12.2 管理平台、业务平台网络安全要求

管理平台、业务平台网联安全要求如下：

a) 应对登录的用户进行身份标识和鉴别，用户的身份标识应具有唯一性，身份鉴别信息具有复杂度要求；
b) 用户首次登录时应修改系统设置的初始口令，并定期更换；
c) 宜采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术应使用密码技术来实现；
d) 应提供访问控制功能，对登录的用户分配账号和权限；
e) 应重命名或删除默认账号，修改默认账号的默认口令；

f） 应及时删除多余的、过期的账号。

12.3 路侧单元网络安全要求

路侧单元网联安全技术要求如下：

a） 具有唯一标识设备的 ID，保证整个生存周期设备标识的唯一性；
b） 应通过制定安全策略如访问控制列表，实现对路侧设备的访问控制；
c） 与其他设备通信时，根据安全策略对其他设备进行权限检查；
d） 更新配置时，根据安全策略对用户进行权限检查。
e） 支持使用安全运行环境、安全单元或安全处理器等对敏感信息的保护。