

中华人民共和国通信行业标准

YD/T [×××××]—[××××]  
[代替 YD/T]

基于 LTE 的车联网无线通信技术 安全证书  
管理系统技术要求

LTE-based vehicular communication — Technical requirement of security  
certificate management system

[点击此处添加与国际标准一致性程度的标识]

(报批稿)

[点击此处添加本稿完成日期]

[××××]-[××]-[××]发布

[××××]-[××]-[××]实施

中华人民共和国工业和信息化部 发布

## 目 次

前 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
4 概述.....	3
4.1 V2X 通信安全系统构成.....	3
4.2 V2X 通信安全服务架构.....	4
5 LTE-V2X 证书管理安全需求.....	7
5.1 概述.....	7
5.2 LTE-V2X 消息安全需求.....	7
6 LTE-V2X 通信安全认证机制总体技术要求.....	8
6.1 LTE-V2X 证书管理系统架构.....	8
6.2 LTE-V2X 安全证书.....	16
6.3 基本元素说明.....	20
6.4 安全协议数据单元.....	21
6.5 数字证书和证书管理数据格式.....	32
7 LTE-V2X 通信安全认证交互流程及接口技术要求.....	44
7.1 注册证书管理流程.....	44
7.2 假名证书申请流程.....	50
7.3 应用证书和身份证书管理流程.....	57
7.4 证书撤销列表管理流程.....	62
7.5 机构证书管理流程.....	71
7.6 异常行为检测上报流程.....	71
7.7 LA 管理架构和流程.....	72
8 LTE-V2X 通信安全认证 PKI 互信技术要求.....	75
8.1 概述.....	75
8.2 PKI 互信架构.....	75
8.3 PKI 互信管理过程.....	78
8.4 PKI 互信认证过程.....	79
8.5 可信根证书列表管理策略.....	80
8.6 可信域 CA 证书列表管理策略.....	80

8.7 可信域的异常行为检查 .....	80
附录 A (资料性附录) 车联网通信安全基本应用模式 .....	81
附录 B (资料性附录) 基于 OAUTH 的 token 授权机制 .....	83
附录 C (规范性附录) ASN.1 模板 .....	86
附录 D (规范性附录) 密码算法的输入与输出 .....	107
附录 E (规范性附录) V2X 设备与安全证书管理系统接口的数据格式 .....	111
附录 F (规范性附录) GBA 机制应用层会话密钥产生及使用方法 .....	146
附录 G (资料性附录) 证书生命周期及更新场景 .....	147
附录 H (资料性附录) 密钥衍生流程的一种算法建议 .....	150
附录 I (规范性附录) 链接值相关定义 .....	153
附录 J (规范性附录) 可信 CA 证书列表及互信认证流程 .....	155
附录 K (资料性附录) 算法编码示例 .....	158

行业标准信息服务平台