- 方案介绍
- 方案优势
- 合作伙伴
- 基于可信根eSE的T-BOX 安全防护
- 基于TEE的IVI安全防护

Watchdata

# 智能网联汽车信息安全解决方案

# 方案介绍

握奇公司本着为每个信息处理设备打造可信计算环境的愿景，针对智能网联汽车的信息安全需求，开发出面向车联网的端-管-云全方位的安全解决方案。基于可信安全根(eSE)和可信执行环境（TEE）构建车联网的安全体系，在安全启动、安全升级、身份认证、安全通信、安全存储、安全监控、密钥管理等方面做到很好的支撑，做到易用性和安全性的最佳配置，提供客户最佳的安全解决方案。


# 方案优势

## 安全性

- 基于PKI、CA中心和证书体系，实现各项安全功能。
- eSE安全模块为EAL5+认证的车规级芯片，保证证书和私钥存储环境的安全性。
- WatchTrust TEE通过GP组织符合性认证，提供应用可信的运行。
- 保障车联网设备的固件的安全，在设备启动和更新时校验其完整有效。
- 在联网通讯时，可进行身份认证和建立安全链路。

## 一站式服务

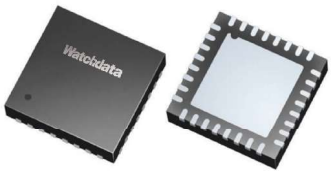
- 设备端提供符合OpenSSL接口的相关中间件，屏蔽底层实现，方便客户应用开发。
- 云端可提供基础安全服务平台，如：访问控制网关、KMS、TSM、TAM和CA中心等。
- 全面专业的定制开发能力，协助客户制定专用方案。
- 可协助客户建立eSE的个人化生产能力。

# 合作伙伴

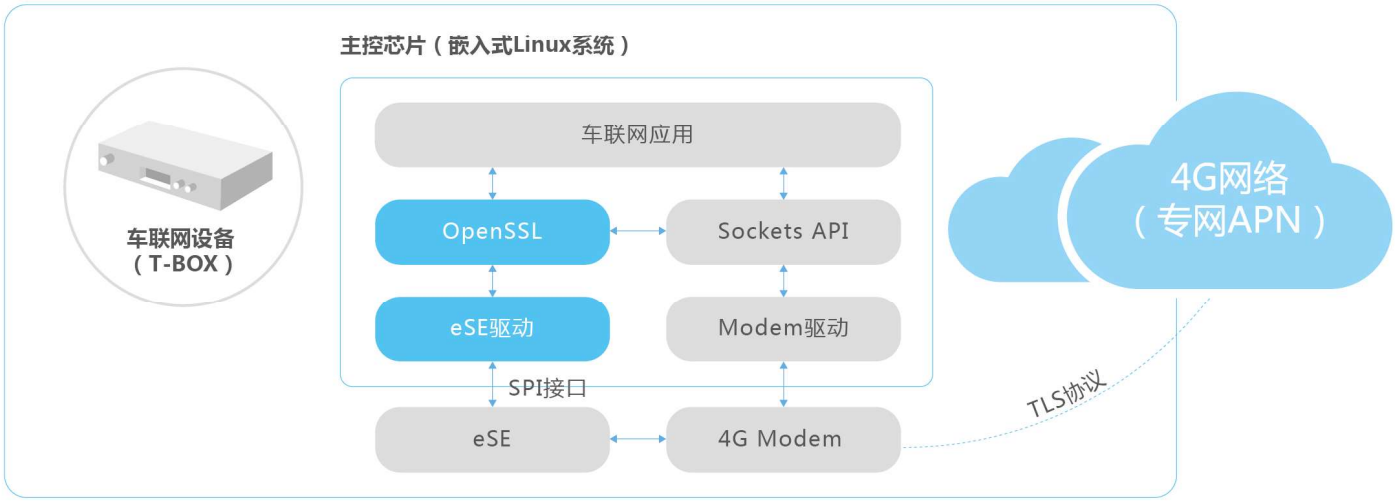
斯润天朗（北京）科技有限公司

北京航空航天大学

# 基于可信根eSE（WD-SAFE-A10）的T-BOX 安全防护




## 方案系统结构



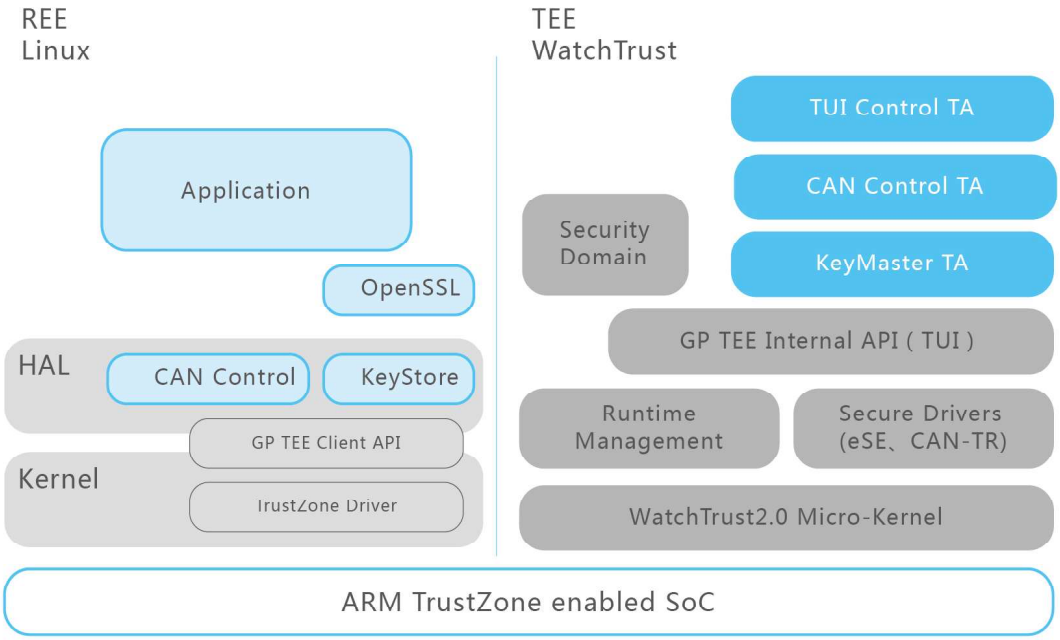

## 方案功能

- WD-SAFE-A10芯片可以与T-BOX主控芯片使用多种通信接口相连，并提供eSE驱动和符合OpenSSL标准的中间件。
- 可以本地生成RSA密钥对并支持申请证书的存储。
- 可以与远程服务器进行双向认证，建立基于安全传输层协议（TLS）的链接。
- 可支持安全启动和固件升级的签名验证，打包和解开数字信封。
- 可与TSM系统建立安全通道，支持下载应用、应用个人化和更新证书等功能。

## 车规级eSE参数

| | |
|---|---|
| 芯片认证 | AEC-Q100、CC EAL 5+ |
| 支持算法 | CRC16、CRC32、DES、Triple-DES、AES-128/256、MD5、SHA1、SHA256、RSA-2048、ECC-256、SM2、SM3、SM4。真随机发生器 |
| 通讯接口 | ISO7816、I2C、SPI |
| 物理参数 | -40 to +105°C；JESD22-B103；JESD22-A101 Humidity |
| 多应用 | 可同时支持eSIM和eSE功能 |
| 支持功能 | 支持X.509证书、TLS握手、签名验证服务（安全启动、固件更新）、片内生成密钥、数字信封处理、安全通道 |

# 基于TEE的IVI安全防护




WatchTrust方案（握奇公司自有知识产权的TEE解决方案）

## 方案功能

- 安全启动（Secure Boot）--防止篡改系统镜像，保证载入内存中的固件程序安全有效。
- 安全显示和触摸（TUI）--提供安全输入输出功能，保证应用界面和键盘操作不被操控，有效保护关键功能不被恶意软件控制，主要用于可直接向CAN总线发数据的操作，例如实现开车门、开灯光、开空调、车辆启动等操作可信。
- CAN总线控制--用于远程控制汽车的场景。远程控制指令在后台服务器签名后下发给REE应用，REE应用调用CAN Control接口把数据转发给CAN Control TA，签名信息在TEE中进行签名验证，验证成功后远程控制指令发给CAN总线控制器。
- 安全存储（Secure filesyetem）--包括SFS（Secure filesystem）和RPMB。保护个人信息、密码、证书、私钥等数据不被窃取和篡改。
- 安全加解密引擎--支持多算法API，可以用于有安全加解密要求的场景，如安全网络协议，网络传输、FOTA签名验证等。
- 应用管理（Admin）--提供全面管理安全域(SD)和可信应用(TA)的功能，包括SD，TA实体管理，安全数据存储管理，访问控制等，为Client App提供稳定安全的服务。

握奇官方网站　握奇官方微信

**握奇公司**

地址：北京市朝阳区望京利泽中园101号启明国际大厦7层
电话：（86 10）6472 2288
网址：www.watchdata.com.cn