

具有高级加密
加速器的安全系统

NCJ38A汽车级安全芯片

NCJ38A安全芯片(SE)是一款专用的硬件和软件安全架构产品，具有超强的抗物理攻击能力。它通常用于保护贵重资产，非常适合安全存储通过智能设备解锁和启动汽车所需的数字密钥。

概述

NCJ38A安全芯片系列是汽车级安全微控制器，具有高级加密加速器和抗物理及电气攻击能力。NCJ38A SE用于存储安全应用程序及其机密数据。

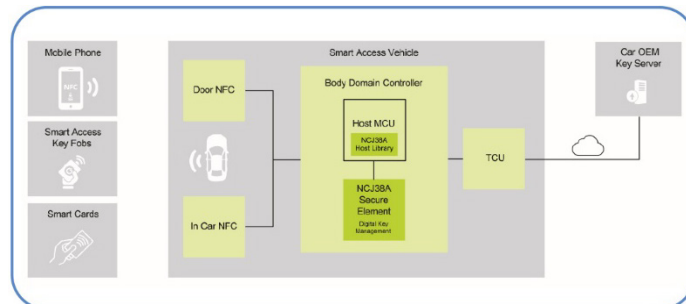
软件平台与恩智浦汽车JCOP 4.4操作系统一起，作为开放Java Card平台提供给客户。客户还可以选择订购通用身份验证小程序NCJ38xA，支持各种M2M验证方法、加密密钥和数据存储。

该器件基于高频时钟Arm® SC300内核，结合恩智浦新一代加密硬件协处理器和闪存模块，可全面提升安全应用的性能和安全性。

目标应用

- ▶ 用于智能汽车门禁的CCC数字钥匙管理
- ▶ Qi 1.3认证
- ▶ 保护互联汽车的外部 and 内部连接安全

NCJ38A安全元件应用框图



主要特性

内核:

- ▶ 采用Arm® SecurCore® SC300技术的恩智浦处理器

存储器:

- ▶ 高达750 kB的用户存储器

接口:

- ▶ SPI从机接口
- ▶ I²C总线从机接口

加密硬件协处理器

- ▶ 高速公共密钥协处理器(PKC), 支持主要的公共密钥加密系统, 例如RSA、ECC和相应机制
- ▶ 高速Triple-DES和AES协处理器
- ▶ 硬件中的随机数生成器, 符合AIS-31标准要求
- ▶ 两个高速循环冗余校验引擎

质量

- ▶ 符合AEC-Q100 2级标准
- ▶ 硬件认证: 通用标准EAL 5+

封装

- ▶ HVQFN32

开发支持

- ▶ 与恩智浦汽车JCOP® 4.4操作系统一起, 作为开放Java® Card平台提供给客户
- ▶ 客户还可以订购通用身份验证小程序NCJ38xA, 支持各种M2M验证方法、加密密钥和数据存储
- ▶ 软件堆栈: 恩智浦JCOP4.4安全Java Card操作平台
- ▶ 可选: 通用身份验证小程序
- ▶ NCJ38A主机库软件包
- ▶ JCOP工具链, 支持客户小程序开发

NCJ38A安全芯片



数字钥匙解决方案

恩智浦提供数字钥匙解决方案, 遵循车联联盟标准化规范版本2。该解决方案使用NCJ38A SE以及恩智浦NCF3320和NCF3340 NFC芯片组, 可通过支持NFC的智能手机、遥控钥匙或内含数字钥匙的NFC智能卡解锁并启动汽车。这款基于NFC技术解决方案, 使得当手机电池电量耗尽也可以触发汽车门禁和驾驶员授权成为可能, 而无需传统的物理钥匙。

其中采用NCJ38A汽车级安全芯片, 在手机、遥控钥匙和智能卡内以及汽车端均可配置恩智浦的这款安全芯片。

有关详细信息, 请访问www.NXP.com/NCJ38A

恩智浦、恩智浦标志和JCOP是NXP B.V.的商标。所有其他产品或服务名称均为其各自所有者的财产。Oracle和Java是Oracle和/或其关联公司的注册商标。Arm和SecurCore是Arm Limited (或其子公司) 在美国和/或其他地区的商标或注册商标。相关技术可能受任何或所有专利、版权、设计和商业机密的保护。保留所有权利。© 2020 NXP B.V.

文档编号: NCJ38ASECELFS REV 0