2 芯片简介

2.1 概述

NS3300 是国民技术嵌入式安全芯片系列中的一员，主要用于配件、耗材、防伪等用途。它可辅助用户进行身份识别或配件认证等操作，实现保护其知识产品的需求。

2.2 应用领域

- 配件和外设安全认证
- 耗材认证
- 物联网节点认证
- 安全存储
- 设备电池认证
- 防抄板保护

2.3 关键特性

- **安全方案**
  - 内置硬件加速引擎：163 位椭圆曲线密码算法（ECC163 2n 域）
  - 256 位椭圆曲线数字签名（ECDSA256 p 域）
  - 真随机数生成器（TRNG）
  - 挑战响应机制（主机 -> 从机）
  - 便于主机端集成的安全库
- **自毁功能**
  - 支持多种自毁触发条件：Kill 命令、生命周期计数器归零或 ECC 计数器归零
- **用户空间**
  - 1kBit 用户空间，存储客户信息
  - 具备锁定功能
  - 10 万次擦写次数及 10 年数据保持@25℃
- **单线接口(Single-Wire Interfaces, SWI)**
  - 高达 200 kBits/s 传输速率
  - 直接供电或由 SWI 间接供电
  - 支持 CRC 校验
  - 便于主机端集成的通信库

- **电源管理**
  - 直接供电或间接供电解决方案
  - 通过 SWI 接口实现上电和掉电控制
  - Power Down 功耗：1uA (Typ.)
  - Power Down 唤醒时间：10ms (Max.)
- **生命周期指示器**
  - 24-bit 计数器
  - 支持递减或递增功能
  - 客户设置初始值
  - 支持锁定功能
- **ECC 认证计数器**
  - 24-bit 递减计数器
  - 客户设置初始值
  - 支持锁定功能
- **硬件防护**
  - 达到 EAL4+安全等级，抗侧信道、抗故障注入、抗逻辑攻击、抗侵入式等攻击
- **96bit 唯一的器件 ID**
- **工作条件**
  - 供电电压范围：1.62~5.5V
  - 温度范围：-40~85℃
- **封装**
  - FCDFN6
- **ESD**
  - 2kV（HBM 模型），符合 EIA/JESD22-A114
  - 500V（CDM 模型），符合符合 EIA/JESD22-C101