Nation 国民技术

NS3300 方案简介 v1.0

目 录

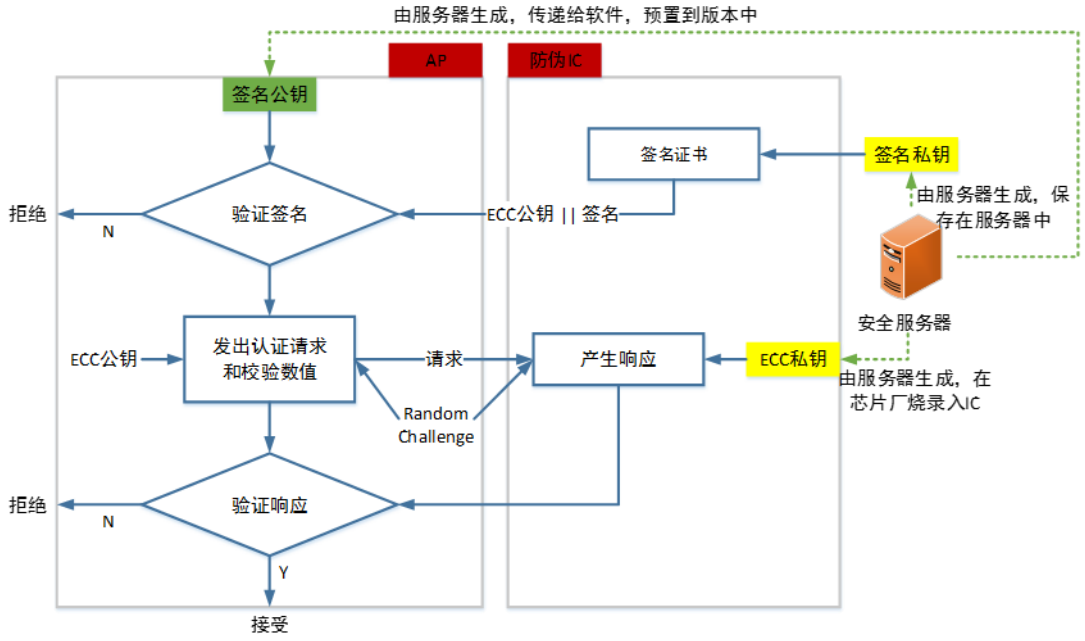
国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

1 方案简介

本文档介绍了 NS3300 认证方案的流程和实现细节，通过阅读该文档，用户可以对整个认证方案有总体的了解。

2 系统框图

主机通过 SWI 单线协议，与 NS3300 进行了一系列交互，最终完成对 NS3300 的身份认证。如下所示：



3 方案规格参数

生产阶段，服务器生成一对固定的签名 ECC 公/私钥（GFp-256）。其中，签名私钥保存在服务器中，签名公钥预置到主机中。同时，服务器为每个 NS3300 生成一对 ECC 公/私钥（GF2n-163）。服务器用签名私钥对 ECC 公钥（GF2n-163）及唯一的 UID（内置在 NS3300 中）等身份信息进行签名，并将结果烧录入 NS3300 中。

NS3300 在生产阶段已经烧录了如下信息：

- ***UID***
- ***ECC 公/私钥（GF2n-163）***
- ***ECC 私钥（GFp-256）对 UID 和 ECC 公钥（GF2n-163）一起签名的结果***

主机端需要验证 NS3300，则需要预置 ECC 公钥（GFp-256）。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

认证流程由主机发起，NS3300 根据指令响应，大致可分为三个阶段：

- **验证签名**

主机从 NS3300 中获取到 UID、ECC 公钥及签名证书等信息后，需验证签名的有效性。签名证书由签名私钥（GFp-256）对每个 NS3300 的 ECC 公钥（GF2n-163）及其唯一的 UID 做签名运算得到。签名验证通过身份认证保证获取的 UID 和 GF2n-163 公钥的有效性。

- **认证请求与挑战码**

主机通过随机数生成每次认证的挑战码，将挑战码及认证请求发给 NS3300，等待其响应。

- **验证响应**

NS3300 收到挑战码及认证请求后生成响应。响应由 ECC 私钥（GF2n-163）对随机挑战码做 GF2n-163 ECDSA 签名得到。主机验证响应可确保 NS3300 与签名中的芯片身份相符（即 UID 和 GF2n-163 ECC 公钥），同时保证通信的时效性。

4 方案特点和优势

- SWI 单线接口，占用资源少
- 96bit 全球唯一序列号
- 采用 ECC 非对称算法
- 每个芯片具有不同的 ECC 密钥对
- 每个芯片具有不同的数字证书（可与序列号绑定）
- 支持自毁功能，报废处理
- 支持 ECC 校验次数设置，超过次数拒绝认证
- 支持生命计数设置，超过次数拒绝认证
- 支持多种工作模式，降低总体功耗
- 提供 128bytes 的用户读写区域，锁定后无法写只能读取
- ROHS 标准
- 工作温度范围：-40℃ ~+85℃，存储温度范围：-55℃ ~+150℃，湿度范围：35~90%RH

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

5 应用场景

NS3300 是国民技术嵌入式安全芯片系列中的一员，主要用于防伪用途，可供用户用于身份识别或者配件认证等，保护自身知识产权。主要应用领域有：

- 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

6 修订历史记录

版本号	修订人	修订日期	修订内容
V 1.0	黄汉彬	2021-02-07	初版

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

7 声明

国民技术股份有限公司（以下简称国民技术）保有在不事先通知而修改这份文档的权利。国民技术认为提 供的信息是准确可信的。尽管这样，国民技术对文档中可能出现的错误不承担任何责任。在购买前请联系国民技术获取该器件说明的最新版本。对于使用该器件引起的专利纠纷及第三方侵权国民技术不承担任何责任。另外，国民技术的产品不建议应用于生命相关的设备和系统，在使用该器件中因为设备或系统运转失灵而导致的损失国民技术不承担任何责任。国民技术对本手册拥有版权等知识产权，受法律保护。未经国民技术许可，任何单位及个人不得以任何方式或理由对本手册进行使用、复制、修改、抄录、传播等。

国民技术股份有限公司 Nations Technologies Inc.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057