

加密芯片生产工具 (atsha204a初始化)

<http://111.160.23.206:8081/gaowei/cryptoauthlib>

<http://111.160.23.206:8081/gaowei/crypto-dev>

一、加密芯片初始化

使用[crypto-init.sh](#)初始化加密芯片

----首先多个判断确认所在环境状态

1. 判断ZX_DIR="/home/zxsj/hd/EventTest"是否存在
2. 判断CFG_PATH=\${ZX_DIR}/crypto.cfg是否存在

----判断本地IP以获取板号 (A、B、C、D)

----获取参数 (SN与频道最大数)

----进行对crypto-dev的三次调用

1. 第一次调用附带参数: --gen-cfg \${CFG_NAME} --pcb-sn PCB\${PCB_SN} --core-pos CorePos\${CORE_POS} --channels \${CHANNELS}, 生成配置文件
2. 第二次调用附带参数: --init \${CFG_NAME}, 进行初始化
3. 第三次调用附带参数: --verify \${CFG_NAME}, 进行一次验证

二、项目中如何调用验证, 实现加密功能

调用std::vector<std::string> Verify(const char* cfgPath)方法进行验证

1. std::vector<std::string> fields = ReadCfg(cfgPath); // 读取先前生成的配置文件数据
2. Bytes32 key = cryptoDev.GenerateKey(fields); // 通过读取到的数据生成一个哈希值
3. cryptoDev.CheckMac(0, key); // 将读取到的哈希值与加密芯片中的哈希值进行对比以验证