小米产线服务器使用说明 - 证书签发

Miot 嵌入式

Exported on 12/25/2020

Table of Contents

本文描述了小米产线证书签发服务器的使用方法及部署要求。

1 环境要求

- **生产服务器**：部署了证书签发服务，小米提供
- **局域网**：LAN网线一根。局域网需要与服务器互通
- **外网**: 服务器能够连接外网 factoryman.io.mi.com[1] 端口：554，小米数据更新维护时使用

1 http://factoryman.io.mi.com

2 安装部署

1. 接通电源及网线（只有电源和网线，**不需要连接显示器、键盘或鼠标**）；
2. 分配固定IP地址（如路由器MAC绑定）；
3. 在局域网内web访问服务器IP，打开登录界面，输入口令（妥善保管，丢失得重置生产服务器），启动服务。这一步在服务器**每次上电时需且仅需执行一次**。

3 服务接口

3.1 证书签发

- **调用方法**
  GET
- **接口路径**
  http://server:port/getcertchain/{公钥}
- **参数**

字段	类型	描述
公钥	Hex String	128字节ASCII字符，表示64字节ECC256公钥

- **返回**
  *OK,DID,*根证书,生产服务器证书,设备证书,CRC32。（需要校验码增加传输可靠性）

字段	类型	描述
OK	String	表示正常，英文逗号分隔符
DID	Integer	十进制ASCII字符串，最大长度20
根证书	Hex String	DER编码
生产服务器证书	Hex String	DER编码
设备证书	Hex String	DER编码
CRC32	Hex String	CRC32之前所有字符的校验码，包含**所有逗号** 多项式: x^32+x^26+x^23+x^22+x^16+x^12+x^11+x^10+x^8+x^7+x^5+x^4+x^2+x+1

- **异常**

字段	描述
ERROR,PUBKEY ERROR	公钥格式错误
ERROR,NEED LOGIN	需要登录
ERROR,CERT ERRO	证书生成错误，联系小米
ERROR,NO MORE SN	没有更多可用序列号，联系小米

3.2 状态查询

- **调用方法**
  GET
- **接口路径**

http://server:port/[2]

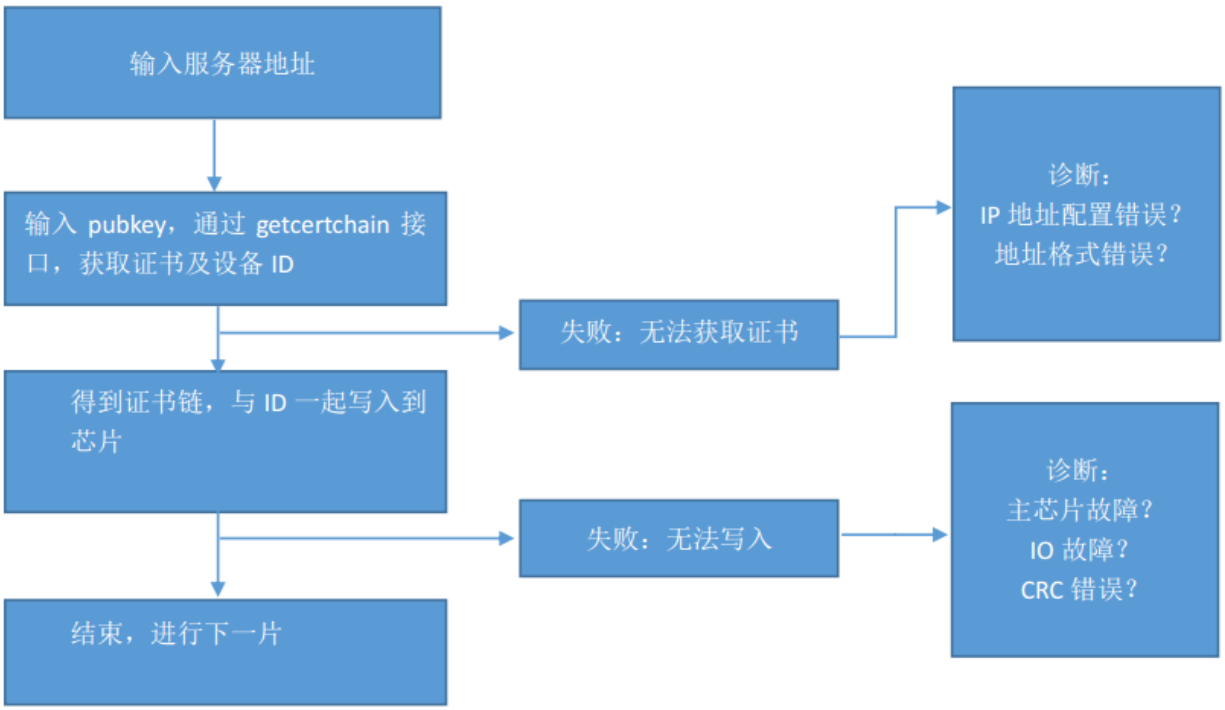
- **返回**
  固件服务器登录状态、已经签发的证书SN地址段及总数量。

2 http://serverport

4 产线机台要求

1. **去重**： 与历史数据库对比，确保DID没有重复；
2. **签名验签**： 确保证书与芯片匹配；
3. **检查证书SN**： 确保证书与DID匹配;
4. **验证证书链**： 确保证书链匹配。

5 典型使用流程


输入服务器地址
输入 pubkey，通过 getcertchain 接口，获取证书及设备 ID
失败：无法获取证书
诊断：
IP 地址配置错误？
地址格式错误？
得到证书链，与 ID 一起写入到芯片
失败：无法写入
诊断：
主芯片故障？
IO 故障？
CRC 错误？
结束，进行下一片

6 Q&A

- 服务器登录密码？
  不需要。
- 如何分配固定IP?
  服务器接通网线和电源启动时会主动获取IP，你可以登录到网关/路由器的管理后台进行MAC地址绑定操作。
- 如何关机？
  短按一下电源键等待电源指示灯熄灭即可。