**证书**

# 1.应用场景

## 1.1置于HTTP服务器

用于客户端与HTTP服务器之间通信数据加密，确保HTTP服务器为合法服务器



## 1.2置于设备与MQTT服务器

证书放置于MQTT服务器上，用于设备验证MQTT服务器合法性，证书放置于设备中，用于MQTT服务器验证设备合法性。



# 2.证书制作介绍

## 2.1证书制作信息

证书公私密钥对生成算法：RSA

密钥大小：1024

证书格式：x509

证书版本：3

证书主题信息：可配置

证书有效期：3650天（可配置）

证书签名算法：SHA1withRSA

## 2.2服务器证书制作流程与配置

**流程：**

1. 生成公私密钥对root\_public\_key，root\_private\_key
2. 生成自签名证书 root\_cert
3. 生成服务器公私密钥对server\_public\_key, server\_private\_key
4. 生成服务器证书 server\_cert，并用root\_private\_key对服务器证书公钥server\_public\_key进行签名

**配置：**

服务端（EMQ）放置服务端证书server\_cert和服务端私钥server\_private\_key，并将根证书root\_cert安装于设备中。（让设备验证服务器的合法性）

## 2.3设备证书制作流程与配置

**流程：**

1. 生成公私密钥对device\_root\_public\_key，device\_root\_private\_key
2. 生成自签名证书 device\_root\_cert
3. 生成中间证书公私密钥对device\_immediate\_public\_key, device\_immediate\_private\_key
4. 生成中间证书 device\_ immediate \_cert，并用device\_root\_private\_key对中间证书公钥device\_immediate\_public\_key进行签名。
5. 生成设备公私密钥对device\_public\_key，device\_private\_key
6. 生成设备证书device\_cert，并用device\_immediate\_private\_key对设备证书公钥device\_public\_key进行签名。

**配置：**

服务端(EMQ)放置证书device\_root\_cert(服务器用于验证设备证书)， WEB服务端放置root\_cert，中间证书device\_ immediate \_cert与中间证书私钥device\_immediate\_private\_key，用于签发设备证书。将生成的设备私钥device\_private\_key以及设备证书device\_cert，下发至设备并安装于设备中。

# 3.设备证书安装

设备生产上电后，会通过http请求下载证书文件，安装证书，证书文件结构如下



设备证书安装完成后，即可与MQTT服务器进行通信