设备发放

常见问题

文档版本	01
发布日期	2021-08-23

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

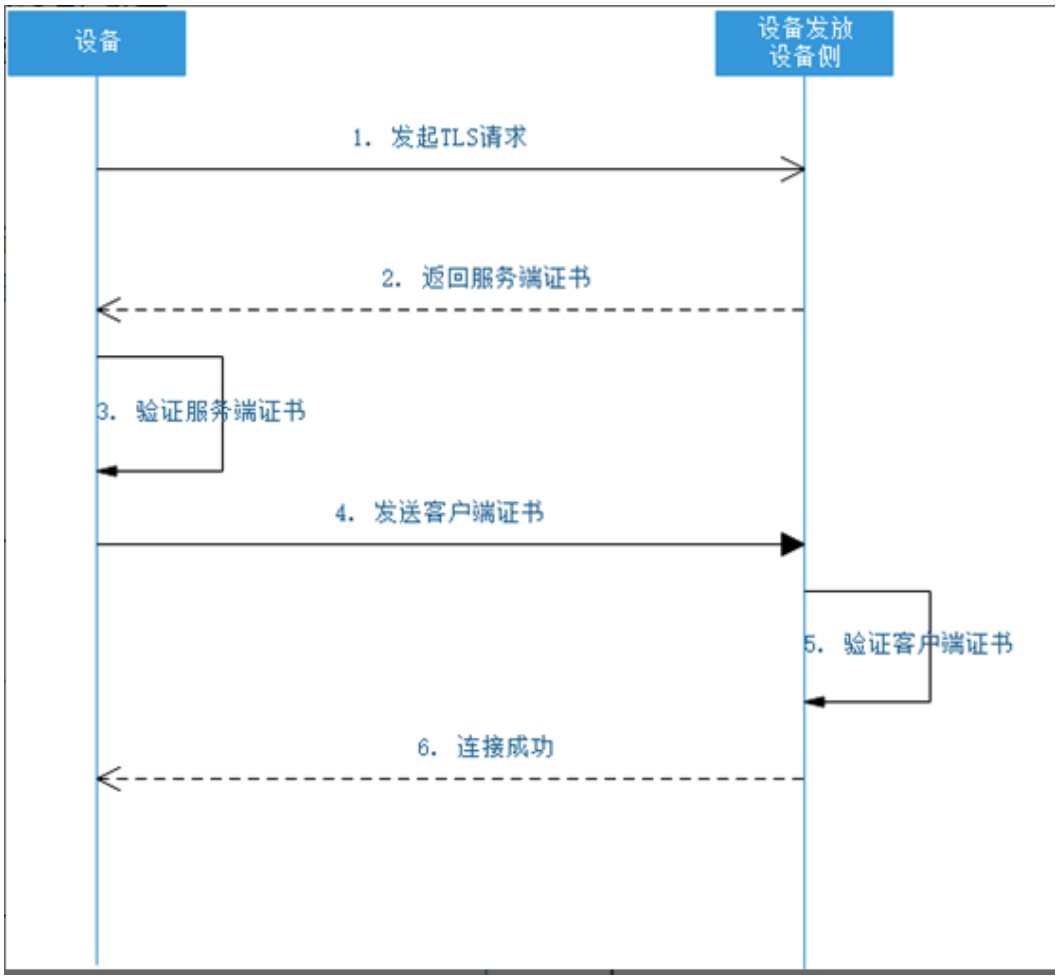
您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 常见问题 1：设备发放流程中使用到的证书都有哪些，它们有何区别?

设备发放提供证书认证方式，证书认证为双向认证过程，涉及到设备发放（平台）和设备两端，过程如下图所示。



双向证书认证过程使用到了如下几类证书：

表 1-1

证书	说明	证书及其私钥持有者	签发者
服务端证书	步骤2中，设备发放设备侧将该证书返回设备。	设备发放设备侧持有	权威CA（服务端证书的CA证书）签发
服务端CA证书	步骤3中，客户端使用该服务端CA证书验证服务端证书，通常为权威CA证书，获取方式见**MQTT CONNECT连接鉴权**。	权威CA机构持有	权威CA机构签发
设备证书（客户端证书）	步骤4中，设备将该证书发送给设备发放设备侧。	设备	CA证书
CA证书（设备CA证书/客户端CA证书）	步骤5中，设备发放设备侧使用该CA证书验证来自设备的客户端证书。用户通过应用侧上传该证书到设备发放平台。	用户	通常为自签发

样例中各类证书常用文件名：

表 1-2

证书	文件名	MQTT.fx中的字段名
服务端证书	-	-
服务端CA证书	如下其中之一： GlobalSignRSAOVSSLCA2018.bks（android） GlobalSignRSAOVSSLCA2018.crt.pem（c或java） GlobalSignRSAOVSSLCA2018.jks（java） bsca.jks（java） bsrootcert.pem（c）	CA File
设备证书（客户端证书）	client.crt	Client Certificate File
设备证书（客户端证书）私钥	client.key	Client Key File

证书	文件名	MQTT.fx中的字段名
CA证书（设备CA证书/客户端CA证书）	server.crt	-

说明

双向认证，即双向证书认证，与单向认证中不同的是，不仅包含单向认证中的设备对平台的证书验证步骤，还包含了平台对设备的证书验证步骤。

2 常见问题 2：证书指纹是什么？如何获取？在业务中有何作用？

证书指纹

证书指纹，即证书哈希值，是用于标识较长公共密钥字节的短序列。通过使用哈希算法对证书内容进行计算获取指纹。

说明

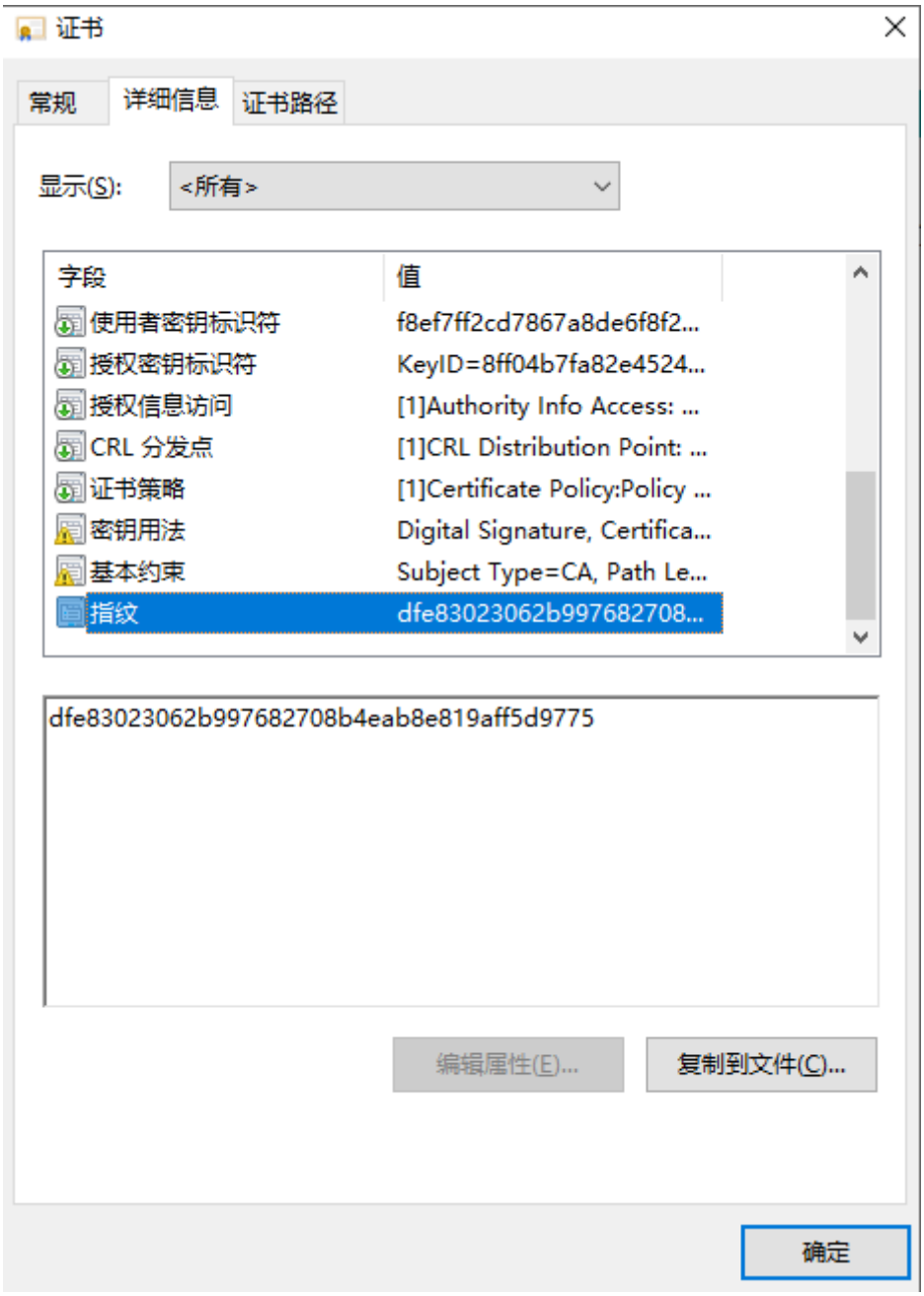
证书指纹通常使用sha1或sha256算法计算，算法不同，证书指纹的长度也不同。sha1算法得到40位长度的序列，sha256算法得到64位长度的序列。

无特别说明，物联网平台均使用sha1算法计算、存储和校验证书指纹，校验过程不区分大小写。

获取证书指纹

- 使用Windows自带的工具

  使用Windows自带的工具打开证书，单击详细信息，在显示的字段中选择指纹，即可获取该证书指纹。



- 使用openssl工具

```
# 使用sha1算法
openssl x509 -fingerprint -sha1 -in client.crt
# 使用sha256算法
openssl x509 -fingerprint -sha256 -in client.crt
```

说明

通过openssl工具计算出的指纹携带了“:”，使用前请删除，确保序列长度为40位或64位。

在业务中的用途

在证书认证方式中，平台存储设备CA证书，不存储设备证书完整内容，但会存储、计算和校验设备证书指纹。

为确保设备与平台通信的安全性，在双向认证过程中，平台不仅使用设备CA对设备证书进行验证，还会校验【 设备关联的证书指纹 】与【 双向认证使用的设备证书的指纹 】的一致性。

