安全测试规范

以下标注可选的用例，若不支持该功能则无需测试，若支持则必测

1. 数据通信使用 TLS1.2[可选]

用例编号：

用例名称：数据通信使用 TLS1.2

测试目的：验证设备数据通信中是否使用 TLS1.2

用例属性：可选

测试步骤：

1.设备与 PC 处于同一个无线/有线网络环境

2.打开抓包软件，并开始监听局域网的数据包；

3.设备上电，并与云端通信；

预期结果：

1.能检测到设备端与云端 TLS 握手过程；

2.能检测到设备端与云端使用 TLS 传输数据过程；

3.TLS 版本号为 1.2；

备注：

1.TLS/iTLS/iDTLS 至少支持一种

2.本用例无需自测

2. 数据通信使用 iTLS/iDTLS[可选]

用例编号：

用例名称：设备数据通信使用 iTLS/iDTL

测试目的：验证设备数据通信中是否使用 iTLS/iDTLS

用例属性：可选

测试步骤：

1.设备与 PC 处于同一个无线/有线网络环境

2.设备上电，并与云端通信；

预期结果：

1.IoT 控制台显示设备在线，设备 log 显示连接云端的域名地址包含“itls”，如“itls-cn-shanghai.aliyuncs.com”；

备注：

1.TLS/iTLS/iDTLS 至少支持一种

2.本用例无需自测

3. 设备支持 ID2 认证[可选]

用例编号：

用例名称：设备支持 ID2 认证

测试目的：验证设备是否支持使用 ID2 与物联网平台认证连接

测试拓扑结构：设备与 PC 处于同一个无线/有线网络环境

用例属性：可选

测试步骤：

1.打开 WireShark 软件，并开始监听局域网的数据包；

2.设备上电，并与云端通信；

预期结果：

1.设备使用 ID2 认证连接成功

备注：

1.ID2 简介参考

2.若不支持 ID2，本用例无需测试

4. 设备连云多通道检测

用例编号：

用例名称：设备连云多通道检测

测试目的：

用例属性：必选

测试步骤：

1.抓包监听局域网的数据包；

2.设备上电，并与云端通信；

预期结果：

1.设备与云端通信前有 DNS 报文，且 DNS 报文中只包含阿里云 IoT 服务端的域名解析；

2.假定 DNS 解析出 IoT 服务端的 IP 为 IP1，设备与云端通信的数据报文中只包含与 IP1 的通信报文；

备注：

1.本用例无需自测

5. 设备安全启动[可选]

用例编号：

用例名称：设备安全启动

测试目的：验证设备是否具有安全启动能力

用例属性：可选

测试步骤：

1.获取固件分区图，明确代码区，数据区，固件签名区域；

2.获取固件包 BIN，烧录到设备并重启；

3.修改固件 BIN 的代码区域得到固件 BIN1，烧录到设备并重启；

4.修改固件 BIN 的数据区域得到固件 BIN2，烧录到设备并重启；

5.修改固件 BIN 的签名区域得到固件 BIN3，烧录到设备并重启；

6.烧录固件 BIN 到设备中，并重启设备；

预期结果：

1.步骤 2 设备重启成功；

2.步骤 3 设备重启失败；

3.步骤 4 设备重启失败；

4.步骤 5 设备重启失败；

5.步骤 6 设备重启成功；

备注：

1.若不支持安全启动，本用例无需测试

6. 设备支持密钥固化存储

用例编号：

用例名称：设备支持密钥固化存储

测试目的：验证设备是否支持密钥固化存储

用例属性：可选

测试步骤：

1.打开 IoT 控制台，找到当前设备；

2.设备上电，并与云端通信；

3.复位设备，重复步骤 2；

4.升级设备，重复步骤 2；

5.恢复出厂设置，重复步骤 2；

预期结果：

1.IoT 控制台显示设备为三元组认证设备，且设备离线；

2.执行步骤 2 后，IoT 控制台显示设备在线；

3.执行步骤 3 后，IoT 控制台显示设备在线；

4.执行步骤 4 后，IoT 控制台显示设备在线；

5.执行步骤 5 后，IoT 控制台显示设备离线；

备注：

1.不支持密钥固化，本用例无需测试

7. 设备日志不含敏感信息

用例编号：

用例名称：设备日志不含敏感信息

测试目的：验证设备日志中是否含有敏感信息

用例属性：必选

测试步骤：

1.设备配网、连接阿里云

2.检索日志，查看是否包含 deviceSecret 明文

3.检索日志，产看是否包含 productSecret 明文

3.检索日志，查看是否包含 AP password 明文（仅 Wi-Fi 支持）

预期结果：

1.日志不包含 deviceSecret、productSecret、AP password 明文

备注

8. 设备升级支持完整性和签名校验

用例编号：

用例名称：设备升级支持完整性和签名校验

测试目的：验证设备升级支持完整性和签名校验

测试步骤：

1.获取升级包分区图，明确代码区，数据区，固件签名区域；

2.获取升级包 BIN，设备升级；

3.修改升级包 BIN 的代码区域得到升级包 BIN1，升级设备；

4.修改升级包 BIN 的数据区域得到升级包 BIN2，升级设备；

5.修改升级包 BIN 的签名区域得到升级包 BIN3，升级设备；

预期结果：

1.步骤 2 升级成功

2.步骤 3 升级失败

3.步骤 4 升级失败

4.步骤 5 升级失败

备注：

9. 设备升级支持防回滚

用例编号：

用例名称：设备升级支持防回滚

测试目的：验证设备升级支持防回滚

测试步骤：

1.获取固件 BIN1，版本为 V1

2.获取固件 BIN2，版本为 V2，V1>V2

3.设备烧录固件 BIN1

4.使用 BIN2 升级设备

预期结果：

1.BIN2 升级失败

备注：