(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110557255 A
(43)申请公布日 2019.12.10

(21)申请号 201810552246.8

(22)申请日 2018.05.31

(71)申请人 北京京东尚科信息技术有限公司
地址 100195 北京市海淀区杏石口路65号西杉创意园四区11号楼东段1-4层西段1-4层
申请人 北京京东世纪贸易有限公司

(72)发明人 侯伟浩 吕军委 李硕

(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 张一军 张效荣

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

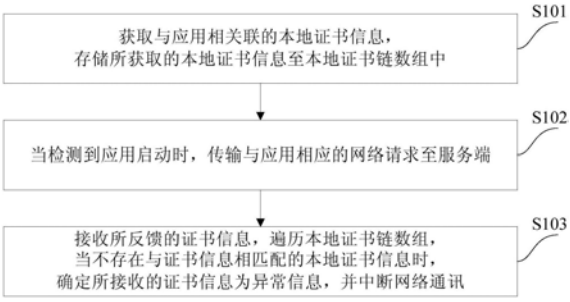
权利要求书3页 说明书12页 附图9页

(54)发明名称

一种证书管理的方法和装置

(57)摘要

本发明公开了一种证书管理的方法和装置，涉及计算机技术领域。该方法的一具体实施方式包括：获取与应用相关联的本地证书信息，存储所获取的本地证书信息至本地证书链数组中；当检测到应用启动时，传输与应用相应的网络请求至服务端；接收所反馈的证书信息，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。该实施方式实现了指定APP证书链校验机制，规避了中间人攻击，增强了APP的网络通讯安全性，同时可以保护了开发者权益。



CN 110557255 A

1.一种证书管理方法,其特征在于,包括:

获取与应用相关联的本地证书信息,存储所获取的所述本地证书信息至本地证书链数组中;

当检测到所述应用启动时,传输与所述应用相应的网络请求至服务端;

接收所反馈的证书信息,遍历所述本地证书链数组,当不存在与所述证书信息相匹配的本地证书信息时,确定所接收的所述证书信息为异常信息,并中断网络通讯。

2.根据权利要求1所述的方法,其特征在于,所述存储所获取的所述本地证书信息至本地证书链数组中还包括:

基于预定的转换规则,转换所获取的所述本地证书信息为预定标识,存储转换后的所述预定标识至所述本地证书链数组中。

3.根据权利要求1所述的方法,其特征在于,在所述确定所接收的所述证书信息为异常信息,并中断网络通讯之前,还包括:

传输与所述应用相应的第一网络请求至所述服务端,以接收所述服务端所反馈的最新证书信息;

基于所接收的所述最新证书信息,更新所述本地证书链数组;

所述确定所接收的所述证书信息为异常信息,并中断网络通讯还包括:

遍历更新后的本地证书链数组,当不存在与所述证书信息相匹配的本地证书信息时,确定所接收的所述证书信息为异常信息,并中断网络通讯。

4.根据权利要求1所述的方法,其特征在于,所述传输与所述应用相应的网络请求至服务端还包括:

传输与所述应用相应的第一网络请求至所述服务端,以接收所述服务端所反馈的最新证书信息;

基于所接收的所述最新证书信息,更新所述本地证书链数组;

所述遍历所述本地证书链数组,当不存在与所述证书信息相匹配的本地证书信息时,确定所接收的所述证书信息为异常信息,并中断网络通讯还包括:

遍历更新后的本地证书链数组,当不存在与所述证书信息相匹配的本地证书信息时,确定所接收的所述证书信息为异常信息,并中断网络通讯。

5.根据权利要求4所述的方法,其特征在于,所述传输与所述应用相应的第一网络请求至所述服务端还包括:

基于预定的加密方式,对所述第一网络请求进行加密,传输加密后的第一网络请求至所述服务端。

6.根据权利要求1所述的方法,其特征在于,还包括:

传输与所述应用相应的第二网络请求至所述服务端,以接收所述服务端所反馈的证书校验功能的执行状态;

所述遍历本地证书链数组,当不存在与所述证书信息相匹配的本地证书信息时,确定所接收的所述证书信息为异常信息,并中断网络通讯包括:

当所述证书校验功能为开启状态时,遍历所述本地证书链数组,当不存在与所述证书信息相匹配的本地证书信息时,确定所接收的所述证书信息为异常信息,并中断网络通讯;或

当所述证书校验功能为关闭状态时，确定所接收的所述证书信息为可信任信息。

7.根据权利要求1-6中任一项所述的方法，其特征在于，所述证书信息至少包括证书域名、证书公钥以及证书有效时间。

8.一种证书管理装置，其特征在于，包括：

存储模块，用于获取与应用相关联的本地证书信息，存储所获取的所述本地证书信息至本地证书链数组中；

传输模块，用于当检测到所述应用启动时，传输与所述应用相应的网络请求至服务端；

校验模块，用于接收所反馈的证书信息，遍历所述本地证书链数组，当不存在与所述证书信息相匹配的本地证书信息时，确定所接收的所述证书信息为异常信息，并中断网络通讯。

9.根据权利要求8所述的装置，其特征在于，所述存储模块，用于：

基于预定的转换规则，转换所获取的所述本地证书信息为预定标识，存储转换后的所述预定标识至所述本地证书链数组中。

10.根据权利要求8所述的装置，其特征在于，所述校验模块，还用于：

传输与所述应用相应的第一网络请求至所述服务端，以接收所述服务端所反馈的最新证书信息；

基于所接收的所述最新证书信息，更新所述本地证书链数组；

遍历更新后的本地证书链数组，当不存在与所述证书信息相匹配的本地证书信息时，确定所接收的所述证书信息为异常信息，并中断网络通讯。

11.根据权利要求8所述的装置，其特征在于，所述传输模块，还用于：

传输与所述应用相应的第一网络请求至所述服务端，以接收所述服务端所反馈的最新证书信息；

基于所接收的所述最新证书信息，更新所述本地证书链数组；

所述校验模块，还用于：

遍历更新后的本地证书链数组，当不存在与所述证书信息相匹配的本地证书信息时，确定所接收的所述证书信息为异常信息，并中断网络通讯。

12.根据权利要求11所述的装置，其特征在于，所述传输模块，还用于：

基于预定的加密方式，对所述第一网络请求进行加密，传输加密后的第一网络请求至所述服务端。

13.根据权利要求8所述的装置，其特征在于，还包括状态接收模块，用于：

传输与所述应用相应的第二网络请求至所述服务端，以接收所述服务端所反馈的证书校验功能的执行状态；

所述校验模块，还用于：

当所述证书校验功能为开启状态时，遍历所述本地证书链数组，当不存在与所述证书信息相匹配的本地证书信息时，确定所接收的所述证书信息为异常信息，并中断网络通讯；或

当所述证书校验功能为关闭状态时，确定所接收的所述证书信息为可信任信息。

14.根据权利要求8-13中任一项所述的装置，其特征在于，所述证书信息至少包括证书域名、证书公钥以及证书有效时间。

15.一种电子设备,其特征在于,包括:

一个或多个处理器;

存储装置,用于存储一个或多个程序,

当所述一个或多个程序被所述一个或多个处理器执行,使得所述一个或多个处理器实现如权利要求1-7中任一所述的方法。

16.一种计算机可读介质,其上存储有计算机程序,其特征在于,所述程序被处理器执行时实现如权利要求1-7中任一所述的方法。

一种证书管理的方法和装置

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种证书管理的方法和装置。

背景技术

[0002] 目前应用市场上大部分APP(Application，应用软件)都采用https(Hyper Text Transfer Protocol over Secure Socket Layer，网络协议)方式进行网络通讯，而https通讯是需要依赖安全证书的。

[0003] 现有开发者在做https网络通讯时，对于证书的处理方式通常有两种：

[0004] 1)不考虑证书信任及校验的问题，直接默认信任设备中已信任的所有证书；例如，对实现X509TrustManager(证书信任管理器)的方法checkServerTrusted(X509Certificate[]chain,String authType)不做任何处理；

[0005] 2)对证书做严格校验；例如，对于实现X509TrustManager的方法checkServerTrusted(X509Certificate[]chain,String authType)做证书严格校验。

[0006] 在实现本发明的过程中，发明人发现现有技术至少存在如下问题：

[0007] 1)APP进行https网络通讯时，如果默认信任设备中所有的证书，导致网络通讯数据包可能会被抓包，造成信息泄露；

[0008] 2)虽然可以对证书进行严格校验，但若没有合理的证书管理方案，当遇到服务器升级或更换https证书时，也会导致网络访问失败，出现业务中断的情况。

发明内容

[0009] 有鉴于此，本发明实施例提供一种证书管理的方法和装置，至少能够解决现有技术中不校验、直接信任所有证书，导致数据被抓包；校验情况没有合理的证书管理方案，导致APP网络访问失败的现象。

[0010] 为实现上述目的，根据本发明实施例的一个方面，提供了一种证书管理的方法，包括：

[0011] 获取与应用相关联的本地证书信息，存储所获取的本地证书信息至本地证书链数组中；

[0012] 当检测到应用启动时，传输与应用相应的网络请求至服务端；

[0013] 接收所反馈的证书信息，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0014] 可选的，存储所获取的本地证书信息至本地证书链数组中还包括：

[0015] 基于预定的转换规则，转换所获取的本地证书信息为预定标识，存储转换后的预定标识至本地证书链数组中。

[0016] 可选的，在确定所接收的证书信息为异常信息，并中断网络通讯之前，还包括：传输与应用相应的第一网络请求至服务端，以接收服务端所反馈的最新证书信息；基于所接收的最新证书信息，更新本地证书链数组；

[0017] 确定所接收的所述证书信息为异常信息，并中断网络通讯还包括：遍历更新后的本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0018] 可选的，传输与所述应用相应的网络请求至服务端还包括：传输与应用相应的第一网络请求至服务端，以接收服务端所反馈的最新证书信息；基于所接收的最新证书信息，更新本地证书链数组；

[0019] 遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯还包括：遍历更新后的本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0020] 可选的，传输与应用相应的第一网络请求至服务端还包括：基于预定的加密方式，对第一网络请求进行加密，传输加密后的第一网络请求至服务端。

[0021] 可选的，还包括：

[0022] 传输与应用相应的第二网络请求至服务端，以接收服务端所反馈的证书校验功能的执行状态；

[0023] 遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯包括：当证书校验功能为开启状态时，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯；或当证书校验功能为关闭状态时，确定所接收的证书信息为可信任信息。

[0024] 可选的，证书信息至少包括证书域名、证书公钥以及证书有效时间。

[0025] 为实现上述目的，根据本发明实施例的另一方面，提供了一种证书管理的装置，包括：

[0026] 存储模块，用于获取与应用相关联的本地证书信息，存储所获取的本地证书信息至本地证书链数组中；

[0027] 传输模块，用于当检测到应用启动时，传输与应用相应的网络请求至服务端；

[0028] 校验模块，用于接收所反馈的证书信息，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0029] 可选的，存储模块，用于：基于预定的转换规则，转换所获取的本地证书信息为预定标识，存储转换后的预定标识至本地证书链数组中。

[0030] 可选的，所述校验模块，还用于：传输与应用相应的第一网络请求至服务端，以接收服务端所反馈的最新证书信息；基于所接收的最新证书信息，更新本地证书链数组；遍历更新后的本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0031] 可选的，传输模块，还用于：传输与应用相应的第一网络请求至服务端，以接收服务端所反馈的最新证书信息；基于所接收的最新证书信息，更新本地证书链数组；

[0032] 校验模块，还用于：遍历更新后的本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0033] 可选的，传输模块，还用于：基于预定的加密方式，对第一网络请求进行加密，传输

加密后的第一网络请求至服务端。

[0034] 可选的，还包括状态接收模块，用于：

[0035] 传输与应用相应的第二网络请求至服务端，以接收服务端所反馈的证书校验功能的执行状态；

[0036] 校验模块，还用于：当证书校验功能为开启状态时，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯；或

[0037] 当证书校验功能为关闭状态时，确定所接收的证书信息为可信任信息。

[0038] 可选的，证书信息至少包括证书域名、证书公钥以及证书有效时间。

[0039] 为实现上述目的，根据本发明实施例的再一方面，提供了一种证书管理的电子设备。

[0040] 本发明实施例的电子设备包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现上述任一所述的证书管理的方法。

[0041] 为实现上述目的，根据本发明实施例的再一方面，提供了一种计算机可读介质，其上存储有计算机程序，所述程序被处理器执行时实现上述任一所述的证书管理的方法。

[0042] 根据本发明所述提供的方案，上述发明中的一个实施例具有如下优点或有益效果：实现了指定APP证书链校验机制，规避了中间人攻击，增强了APP的网络通讯安全性；中断网络请求，保护了开发者权益。

[0043] 上述的非惯用的可选方式所具有的进一步效果将在下文中结合具体实施方式加以说明。

附图说明

[0044] 附图用于更好地理解本发明，不构成对本发明的不当限定。其中：

[0045] 图1是根据本发明实施例的一种证书管理的方法的主要流程示意图；

[0046] 图2是根据本发明实施例的一种可选的证书管理的方法的流程示意图；

[0047] 图3是根据本发明实施例的另一种可选的证书管理的方法的流程示意图；

[0048] 图4是根据本发明实施例的又一种可选的证书管理的方法的流程示意图；

[0049] 图5是根据本发明实施例的再一种可选的证书管理的方法的流程示意图；

[0050] 图6是根据本发明实施例的一具体地证书管理的方法的流程示意图；

[0051] 图7是根据本发明实施例的另一具体地证书管理的方法的流程示意图；

[0052] 图8是根据本发明实施例的一种证书管理的装置的主要结构示意图；

[0053] 图9是本发明实施例可以应用于其中的示例性系统架构图；

[0054] 图10是适于用来实现本发明实施例的移动设备或服务器的计算机系统的结构示意图。

具体实施方式

[0055] 以下结合附图对本发明的示范性实施例做出说明，其中包括本发明实施例的各种细节以助于理解，应当将它们认为仅仅是示范性的。因此，本领域普通技术人员应当认识

到，可以对这里描述的实施例做出各种改变和修改，而不会背离本发明的范围和精神。同样，为了清楚和简明，以下的描述中省略了对公知功能和结构的描述。

[0056] 对于本发明所涉及的名词作解释如下：

[0057] 抓包：将网络传输发送与接收的数据包进行截获、重发、编辑、转存等操作，可用来检测网络安全性。

[0058] 硬编码：把输出或输入的相关参数直接以常量的方式书写在源代码中。

[0059] 证书链数组：可以理解为由证书链、证书信息所组成的库。

[0060] 证书域名：就是用电子证书的格式，标明了注册域名、注册人的名称、注册成功的时间和域名注册到期时间这几项内容。

[0061] 证书公钥：由服务端或中间人所生成，当用在签名系统时，公钥用于验证签名；当用于加密系统时，公钥用于加密。

[0062] 参见图1，示出的是本发明实施例提供的一种证书管理的方法的主要流程图，包括如下步骤：

[0063] S101：获取与应用相关联的本地证书信息，存储所获取的本地证书信息至本地证书链数组中。

[0064] S102：当检测到应用启动时，传输与应用相应的网络请求至服务端。

[0065] S103：接收所反馈的证书信息，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0066] 上述实施方式中，对于步骤S101，对于本地证书链数组中的证书信息，可以为首次写入该APP的证书信息，且是事先读取得到的，其具体实现方案，本发明在此不做限制。

[0067] 例如，事先将服务端/客户端的证书信息存储于本地文件系统中，该证书信息至少包括证书域名(SubjectDN)、证书公钥(PublicKey)以及有效时间。

[0068] 进一步的，还可以对证书信息进行硬编码操作，将其转换为预定标识，例如，转换为数字、字符等，便于后续存储。

[0069] 对于步骤S102，对于APP，需要用户主动触发才能开启。只有当监测到APP启动后，客户端才会传输相应的网络请求至服务端，该网络请求可以是https请求。

[0070] 进一步的，该https请求可以针对该应用生成，具体地，该应用具有应用标识，所发出的网络请求可以也携带该应用标识。

[0071] 对于步骤S103，在https请求传输过程中，服务端会反馈相应的证书信息至客户端；客户端接收到服务端所反馈的证书信息后，会传输到自定义的证书管理器中，例如X509TrustManager，以在证书管理器中执行证书校验逻辑。

[0072] 对于有效时间，客户端在收到所反馈的证书信息后，首先会依据有效时间判断其是否有效，如发现有问题，则直接会抛出异常，提示证书存有问题；若没有问题，直接进行后续证书校验过程，例如依据证书域名以及证书公钥进行对比。对于证书公钥，由服务端或中间人所生成。

[0073] 对于证书校验，可以是遍历本地证书链数组，将所接收的证书信息与存储的本地证书信息进行对比，具体地，依据checkServerTrusted方法进行证书校验：

[0074] 1)若对比成功，可以继续后续进程，并保证网络通讯的正常运行；

[0075] 2)若比对失败，则需要在checkServerTrusted方法中抛出异常，中断本次网络通

讯并做出友好提示等，例如，网络出了点问题…

[0076] 除上述信息外，对于证书校验逻辑，也可以基于证书的其他信息进行校验，例如证书签名、证书链(包括根证书、中级证书、子证书)的中级证书等。

[0077] 对于证书信息对比失败的情况，可以有两种：

[0078] 1)从服务端所接收的证书信息被中间人替换，该APP被中间人所攻击；

[0079] 2)证书管理器中的证书并未更新，导致客户端本地所存储的证书信息与接收自服务端的证书信息不同，造成证书校验失败。

[0080] 为保护APP中的用户信息以及开发者权益，可以中断该APP的网络通讯，降低信息泄露风险。

[0081] 需要说明的是，上述实施过程，均发生在该网络请求过程中。对于https请求，并不是请求发出去后，相应结果就会返回。该过程中还包括证书校验认证等流程，因此，客户端可以在证书校验失败时抛出异常，需要中断网络请求、切断该APP的网络通讯。

[0082] 上述实施例所提供的方法，实现了指定APP证书链校验机制，规避了中间人攻击，增强了APP的网络通讯安全性，同时保护了开发者权益。

[0083] 参见图2，示出了根据本发明实施例的一种可选的证书管理的方法流程示意图，包括如下步骤：

[0084] S201：获取与应用相关联的本地证书信息，存储所获取的本地证书信息至本地证书链数组中。

[0085] S202：当检测到应用启动时，传输与应用相应的网络请求至服务端。

[0086] S203：接收所反馈的证书信息，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，传输与应用相应的第一网络请求至服务端，以接收服务端所反馈的最新证书信息。

[0087] S204：基于所接收的最新证书信息，更新本地证书链数组，遍历更新后的本地证书链数组。

[0088] S205：当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0089] 上述实施方式中，步骤S201、S202可分别参见图1所示步骤S101、S102的描述，在此不再赘述。

[0090] 针对同一应用，相应仅会有一套证书信息，但该证书信息中的内容会有删除、增加、更新等操作。

[0091] 因此，当证书校验失败时，也可能是由于服务端中的证书做了更新/变更，但本地证书链并未更新所导致，因此，在初步判断到证书校验失败后，为防止用户使用APP时错过了更新证书信息的时机，可以执行证书更新逻辑。

[0092] 上述实施方式中，对于步骤S203，对于本地证书链数组的遍历，具体参见图1所示步骤S103的描述，在此不再赘述。

[0093] 当证书初步校验失败后，可以使用网络通讯的方式向服务端请求数据，以对本地https证书信息进行更新。

[0094] 对于证书更新逻辑中的第一网络请求，可以为HTTP(HyperText Transfer Protocol，超文本传输协议)方式。因为本地所存储的证书信息可能已过期，若此时同样使

用https方式,可能会再次导致证书校验失败而出现网络通讯中断的情况,而http方式不会触发证书校验逻辑。

[0095] 进一步的,在进行http网络请求时,为了防止数据被抓包篡改,可以使用AES256+RSA2048对请求体及响应体进行了加密认证。对于从服务端所反馈的证书信息,只有解密成功才可以继续后续流程。

[0096] 其中,AES(Advanced Encryption Standard,高级加密标准)以及RSA加密算法中,密钥越长,加密效果越好,本发明分别采用256字段以及2048字段。请求体位于http请求中,且该http请求至少还包括请求首行、请求头信息;响应体位于服务端反馈给客户端的响应信息中,响应信息还包括响应首行、响应头信息、空行,且每部分都代表了不同的含义。

[0097] 另外,对于最新证书信息的获取,也可以是客户端根据APP的应用标识,在服务端中查询与该应用标识相应的证书信息,并检测当前所查询的证书信息与上次所查询到的证书信息是否一致,若不一致,则证明本次所查询的证书信息为最新证书信息,并获取该最新证书信息,以对本地证书信息进行更新。

[0098] 进一步的,对于上次所查询的证书信息为本地所存储的证书信息,由于服务端对于证书信息可能只存储一份,即最新的,因此,判断当前与上次查询的证书信息是否一致时,需要先将本地所存储的证书信息传输至服务端,之后再进行比较判断。

[0099] 对于步骤S204,对于本次所获取的最新证书信息,可以无需对比,直接对本地所存储的证书信息进行替换更新。

[0100] 另外,也可以先和本地存储的证书信息进行比对,例如证书域名、证书公钥、有效时间等,若对比结果为不一致,则将本地存储的证书信息替换为本次所获取的证书信息;但若对比结果为一致,则无需更新,直接确定与https请求相应的证书信息为异常信息。

[0101] 对于步骤S205,在本地证书更新完毕之后,可以继续或重新执行证书校验逻辑,以判断与https请求相应的证书信息在更新后的证书链数组中是否可以查询到。

[0102] 若仍查询不到,证明所接收的与https请求相应的证书信息被中间人篡改,则抛出异常,中断网络请求,以保证APP的网络通讯安全。

[0103] 上述实施例所提供的方法,实现了证书校验升级机制,只有当初始证书校验失败时才会触发证书更新逻辑,避免由于服务端的证书更新导致本地APP证书校验失败而无法使用的情况,当证书校验失败时,可以向服务端请求更新证书信息。

[0104] 参见图3,示出了根据本发明实施例的另一种可选的证书管理的方法流程示意图,包括如下步骤:

[0105] S301:获取与应用相关联的本地证书信息,存储所获取的本地证书信息至本地证书链数组中。

[0106] S302:当检测到应用启动时,传输与应用相应的网络请求、第一网络请求至服务端。

[0107] S303:接收证书信息以及服务端所反馈的最新证书信息。

[0108] S304:基于所接收的最新证书信息,更新本地证书链数组。

[0109] S305:遍历更新后的本地证书链数组,当不存在与证书信息相匹配的本地证书信息时,确定所接收的证书信息为异常信息,并中断网络通讯。

[0110] 上述实施方式中,步骤S301可参见图1所示步骤S101的描述,步骤S303可参见图2

所示步骤S203的描述，步骤S304可参见图2所示步骤S204的描述，在此不再赘述。

[0111] 上述实施方式中，对于步骤S302，与图2所示实施例不同之处，https网络请求以及http第一网络请求，均为APP启动时，一同发送至服务端的。

[0112] 对于步骤S305，由于证书更新逻辑较之证书校验逻辑先一步进行，因此，此时的证书校验，仅针对更新后的本地证书链进行，若校验失败，可以直接确定所接收的证书信息为异常信息，无需再判断所对比的本地证书信息是否最新。

[0113] 上述实施例所提供的方法，实现了另一种证书校验升级机制，证书校验逻辑基于证书更新逻辑进行，且对于证书的校验只执行一次，较之图2所示方式，简化了执行流程，加快了证书校验速度。

[0114] 参见图4，示出了根据本发明实施例的又一种可选的证书管理的方法流程示意图，包括如下步骤：

[0115] S401：获取与应用相关联的本地证书信息，存储所获取的本地证书信息至本地证书链数组中。

[0116] S402：当检测到应用启动时，传输与应用相应的网络请求、第二网络请求至服务端。

[0117] S403：接收所反馈的证书信息以及服务端所反馈的证书校验功能的执行状态。

[0118] S404：当证书校验功能为关闭状态时，确定所接收的证书信息为可信任信息。

[0119] S404’：当证书校验功能为开启状态时，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0120] 上述实施方式中，对于步骤S401可参见图1所示步骤S101的描述，在此不再赘述。

[0121] 针对有些应用，可能由于用户所持设备、应用版本的原因，当证书信息一更新，可能出现无法使用本地APP的情况，针对这些应用，可以不执行证书校验逻辑，需要直接默认信任即可。

[0122] 上述实施方式中，对于步骤S402，所涉及的第二网络请求，同样可以为http请求，具体参见图2步骤S203的描述，在此不再赘述。

[0123] 对于步骤S403，所涉及的证书校验开关功能的设定，可以存储于服务端，便于同时对多个客户端进行证书校验功能的控制，客户端APP根据其开闭状态相应决定是否执行证书校验逻辑。

[0124] 另外，对于证书校验开闭状态的设置，也可以根据用户使用反映或者测试结果进行人工设定，例如，很多用户更新证书后，导致所持设备的APP不可用，针对这种情况，可以将设置校验功能为关闭状态。

[0125] 对于步骤S404以及S404’，针对证书校验开闭状态的不同，可以有相应不同的操作：

[0126] 1)若校验功能关闭，则直接默认证书信息可信任，并继续后续进程；

[0127] 2)若校验功能开启，即需要按照图1执行证书校验流程；若校验失败，即触发证书更新逻辑，具体参见图2以及图3所示。

[0128] 上述实施例所提供的方法，实现了对证书校验功能的降级策略，以在证书校验逻辑之前判断是否需要执行证书校验逻辑。另外，当APP端的证书校验出现逻辑错误时，服务端可以远程关闭APP的证书校验逻辑，以保证网络通讯正常。

[0129] 参见图5,示出了根据本发明实施例的再一种可选的证书管理的方法流程示意图,包括如下步骤:

[0130] S501:获取与应用相关联的本地证书信息,存储所获取的本地证书信息至本地证书链数组中。

[0131] S502:当检测到应用启动时,传输与应用相应的网络请求至服务端。

[0132] S503:接收所反馈的证书信息,传输与应用相应的第二网络请求至服务端,以接收服务端所反馈的证书校验功能的执行状态。

[0133] S504:当证书校验功能为关闭状态时,确定所接收的证书信息为可信任信息。

[0134] S504':当证书校验功能为开启状态时,遍历本地证书链数组,当不存在与证书信息相匹配的本地证书信息时,确定所接收的证书信息为异常信息,并中断网络通讯。

[0135] 上述实施方式中,步骤S501、S502可分别参见图1所示步骤S101、S102的描述,步骤S504、S504'可分别参见图4所示步骤S404以及S404'的描述,在此不再赘述。

[0136] 上述实施方式中,对于步骤S503,与图4所示实施例不同之处在于,对于校验功能执行状态的获取,需要依据获取证书信息之后进行触发得到。

[0137] 上述实施例所提供的方法,提供了另一种对证书校验功能的降级策略,只有在获取证书信息后才触发得到,较之图4所示实施例,具有一定的执行要求。

[0138] 参见图6,示出了根据本发明实施例的一具体地证书管理的方法流程示意图,包括如下步骤:

[0139] S601:获取与应用相关联的本地证书信息,存储所获取的本地证书信息至本地证书链数组中。

[0140] S602:当检测到应用启动时,传输与应用相应的网络请求至服务端。

[0141] S603:接收所反馈的证书信息,传输与应用相应的第二网络请求至服务端,以接收服务端所反馈的证书校验功能的执行状态。

[0142] S604:当证书校验功能为关闭状态时,确定所接收的证书信息为可信任信息。

[0143] S604':当证书校验功能为开启状态时,遍历本地证书链数组,当不存在与证书信息相匹配的本地证书信息时,传输与应用相应的第一网络请求至服务端,以接收服务端所反馈的最新证书信息。

[0144] S605':基于所接收的最新证书信息,更新本地证书链数组,遍历更新后的本地证书链数组。

[0145] S606':当不存在与证书信息相匹配的本地证书信息时,确定所接收的证书信息为异常信息,并中断网络通讯。

[0146] 上述实施方式中,步骤S601、S602可分别参见图1所示步骤S101、S102的描述,步骤S603可参见图5所示步骤S503的描述,步骤S604可参见图4所示步骤S404的描述,步骤S604'可参见图4所示步骤S404'以及图2所示步骤S203的描述,步骤S605'以及S606'可分别参见图2所示步骤S204以及S205的描述,在此不再赘述。

[0147] 本发明实施例拖提供的方法,实现了指定证书链信任机制,基于证书校验逻辑触发证书降级机制,基于证书校验失败逻辑触发证书更新逻辑。所提供的实施方式,避免中间人攻击造成信息泄露的可能,极大增强了APP的安全性,且基于证书升级以及校验降级的方案,解决了证书过期后处理响应不及时的问题,成功避免了服务端证书的变更对该APP运行

的影响。

[0148] 参见图7,示出了根据本发明实施例的另一具体地证书管理的方法流程示意图,包括如下步骤:

[0149] S701:获取与应用相关联的本地证书信息,存储所获取的本地证书信息至本地证书链数组中。

[0150] S702:当检测到应用启动时,传输与应用相应的网络请求、第一网络请求至服务端。

[0151] S703:接收所反馈的证书信息、以及服务端所反馈的最新证书信息和证书校验功能的执行状态。

[0152] S704:当证书校验功能为关闭状态时,确定所接收的证书信息为可信任信息。

[0153] S704':当证书校验功能为开启状态时,基于所接收的最新证书信息,更新本地证书链数组。

[0154] S705':遍历更新后的本地证书链数组,当不存在与证书信息相匹配的本地证书信息时,确定所接收的证书信息为异常信息,并中断网络通讯。

[0155] 上述实施方式中,步骤S701可参见图1所示步骤S101的描述,步骤S702可参见图1所示步骤S102以及图3所示步骤S302的描述,步骤S703可参见图3所示步骤S303以及图4所示步骤S403的描述,步骤S704可参见图4所示步骤S404的描述,S704'、S705'可分别参见图3所示步骤S304以及S305的描述,在此不再赘述。

[0156] 本发明实施例拖提供的方法,实现了指定证书链信任机制,证书更新机制、证书降级机制以及证书校验机制,是基于APP的启动同时触发的,较之图6,简化了证书校验流程。

[0157] 参见图8,示出了本发明实施例提供的一种证书管理的装置800的主要模块示意图,包括:

[0158] 存储模块801,用于获取与应用相关联的本地证书信息,存储所获取的本地证书信息至本地证书链数组中;

[0159] 传输模块802,用于当检测到应用启动时,传输与应用相应的网络请求至服务端;

[0160] 校验模块803,用于接收所反馈的证书信息,遍历本地证书链数组,当不存在与证书信息相匹配的本地证书信息时,确定所接收的证书信息为异常信息,并中断网络通讯。

[0161] 本发明实施装置中,存储模块801,用于:基于预定的转换规则,转换所获取的本地证书信息为预定标识,存储转换后的预定标识至本地证书链数组中。

[0162] 本发明实施装置中,校验模块803,还用于:

[0163] 传输与应用相应的第一网络请求至服务端,以接收服务端所反馈的最新证书信息;基于所接收的最新证书信息,更新本地证书链数组;遍历更新后的本地证书链数组,当不存在与证书信息相匹配的本地证书信息时,确定所接收的证书信息为异常信息,并中断网络通讯。

[0164] 本发明实施装置中,传输模块802,还用于:

[0165] 传输与应用相应的第一网络请求至服务端,以接收服务端所反馈的最新证书信息;基于所接收的最新证书信息,更新本地证书链数组;

[0166] 所述校验模块803,还用于:

[0167] 遍历更新后的本地证书链数组,当不存在与证书信息相匹配的本地证书信息时,

确定所接收的证书信息为异常信息，并中断网络通讯。

[0168] 本发明实施装置中，传输模块802，还用于：基于预定的加密方式，对第一网络请求进行加密，传输加密后的第一网络请求至服务端。

[0169] 本发明实施装置中还包括状态接收模块804(图中未标出)，用于：

[0170] 传输与应用相应的第二网络请求至服务端，以接收服务端所反馈的证书校验功能的执行状态；

[0171] 校验模块803，还用于：当证书校验功能为开启状态时，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯；或

[0172] 当证书校验功能为关闭状态时，确定所接收的证书信息为可信任信息。

[0173] 本发明实施装置中，证书信息至少包括证书域名、证书公钥以及证书有效时间。

[0174] 另外，在本发明实施例中所述的证书管理装置的具体实施内容，在上面所述证书管理方法中已经详细说明了，故在此重复内容不再说明。

[0175] 本发明实施例拖提供的装置，实现了指定证书链信任机制，证书更新机制、证书降级机制以及证书校验机制，三者可以相互触发，也可以基于APP的启动同时触发。所提供的实施装置，避免中间人攻击造成信息泄露的可能，极大增强了APP的安全性，且基于证书升级以及校验降级的方案，解决了证书过期后处理响应不及时的问题，成功避免了服务端证书的变更对该APP运行的影响。

[0176] 图9示出了可以应用本发明实施例的证书管理方法或证书管理装置的示例性系统架构900。

[0177] 如图9所示，系统架构900可以包括终端设备901、902、903，网络904和服务器905(仅仅是示例)。网络904用以在终端设备901、902、903和服务器905之间提供通信链路的介质。网络904可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0178] 用户可以使用终端设备901、902、903通过网络904与服务器905交互，以接收或发送消息等。终端设备901、902、903上可以安装有各种通讯客户端应用，例如购物类应用、网页浏览器应用、搜索类应用、即时通信工具、邮箱客户端、社交平台软件等(仅为示例)。

[0179] 终端设备901、902、903可以是具有显示屏并且支持网页浏览的各种电子设备，包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。

[0180] 服务器905可以是提供各种服务的服务器，例如对用户利用终端设备901、902、903所浏览的购物类网站提供支持的后台管理服务器(仅为示例)。后台管理服务器可以对接收到的产品信息查询请求等数据进行分析等处理，并将处理结果(例如目标推送信息、产品信息--仅为示例)反馈给终端设备。

[0181] 需要说明的是，本发明实施例所提供的证书管理方法一般由服务器905执行，相应地，证书管理装置一般设置于服务器905中。

[0182] 应该理解，图9中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

[0183] 下面参考图10，其示出了适于用来实现本发明实施例的终端设备的计算机系统1000的结构示意图。图10示出的终端设备仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0184] 如图10所示，计算机系统1000包括中央处理单元(CPU)1001，其可以根据存储在只读存储器(ROM)1002中的程序或者从存储部分1008加载到随机访问存储器(RAM)1003中的程序而执行各种适当的动作和处理。在RAM 1003中，还存储有系统1000操作所需的各种程序和数据。CPU 1001、ROM 1002以及RAM 1003通过总线1004彼此相连。输入/输出(I/O)接口1005也连接至总线1004。

[0185] 以下部件连接至I/O接口1005：包括键盘、鼠标等的输入部分1006；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分1007；包括硬盘等的存储部分1008；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分1009。通信部分1009经由诸如因特网的网络执行通信处理。驱动器1010也根据需要连接至I/O接口1005。可拆卸介质1011，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器1010上，以便于从其上读出的计算机程序根据需要被安装入存储部分1008。

[0186] 特别地，根据本发明公开的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本发明公开的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分1009从网络上被下载和安装，和/或从可拆卸介质1011被安装。在该计算机程序被中央处理单元(CPU)1001执行时，执行本发明的系统中限定的上述功能。

[0187] 需要说明的是，本发明所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本发明中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本发明中，计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0188] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规

定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0189] 描述于本发明实施例中所涉及到的模块可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的模块也可以设置在处理器中，例如，可以描述为：一种处理器包括存储模块、传输模块、校验模块。其中，这些模块的名称在某种情况下并不构成对该模块本身的限定，例如，校验模块还可以被描述为“证书校验模块”。

[0190] 作为另一方面，本发明还提供了一种计算机可读介质，该计算机可读介质可以是上述实施例中描述的设备中所包含的；也可以是单独存在，而未装配入该设备中。上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被一个该设备执行时，使得该设备包括：

[0191] 获取与应用相关联的本地证书信息，存储所获取的本地证书信息至本地证书链数组中；

[0192] 当检测到应用启动时，传输与应用相应的网络请求至服务端；

[0193] 接收所反馈的证书信息，遍历本地证书链数组，当不存在与证书信息相匹配的本地证书信息时，确定所接收的证书信息为异常信息，并中断网络通讯。

[0194] 根据本发明实施例的技术方案，实现了指定证书链信任机制，避免中间人攻击造成信息泄露的可能，极大增强了APP的安全性，且基于证书升级以及校验降级的方案，解决了证书过期后处理响应不及时的问题，成功避免了服务端证书的变更对该APP运行的影响。

[0195] 上述具体实施方式，并不构成对本发明保护范围的限制。本领域技术人员应该明白的是，取决于设计要求和其他因素，可以发生各种各样的修改、组合、子组合和替代。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明保护范围之内。

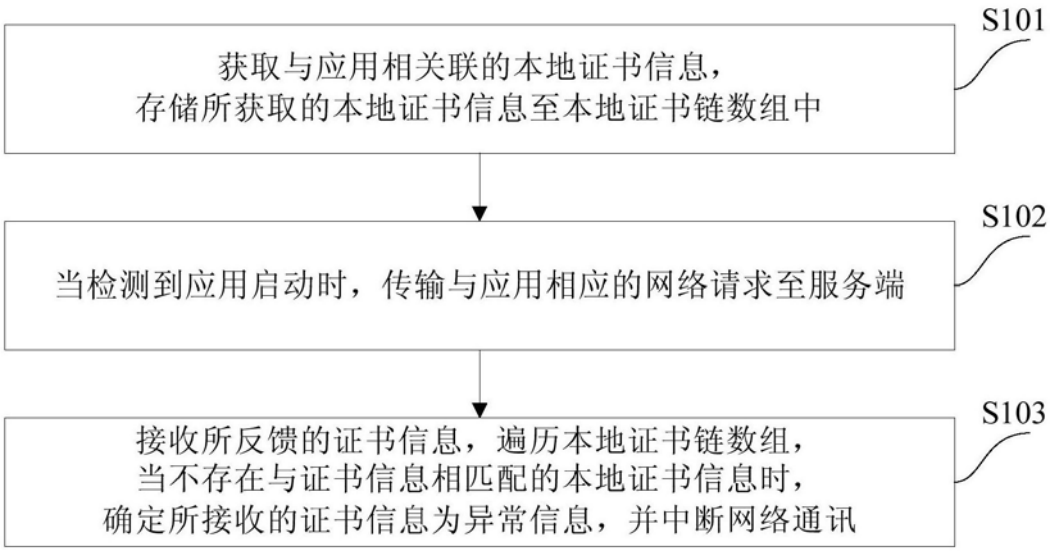

S101
获取与应用相关联的本地证书信息，
存储所获取的本地证书信息至本地证书链数组中
S102
当检测到应用启动时，传输与应用相应的网络请求至服务端
S103
接收所反馈的证书信息，遍历本地证书链数组，
当不存在与证书信息相匹配的本地证书信息时，
确定所接收的证书信息为异常信息，并中断网络通讯

图1

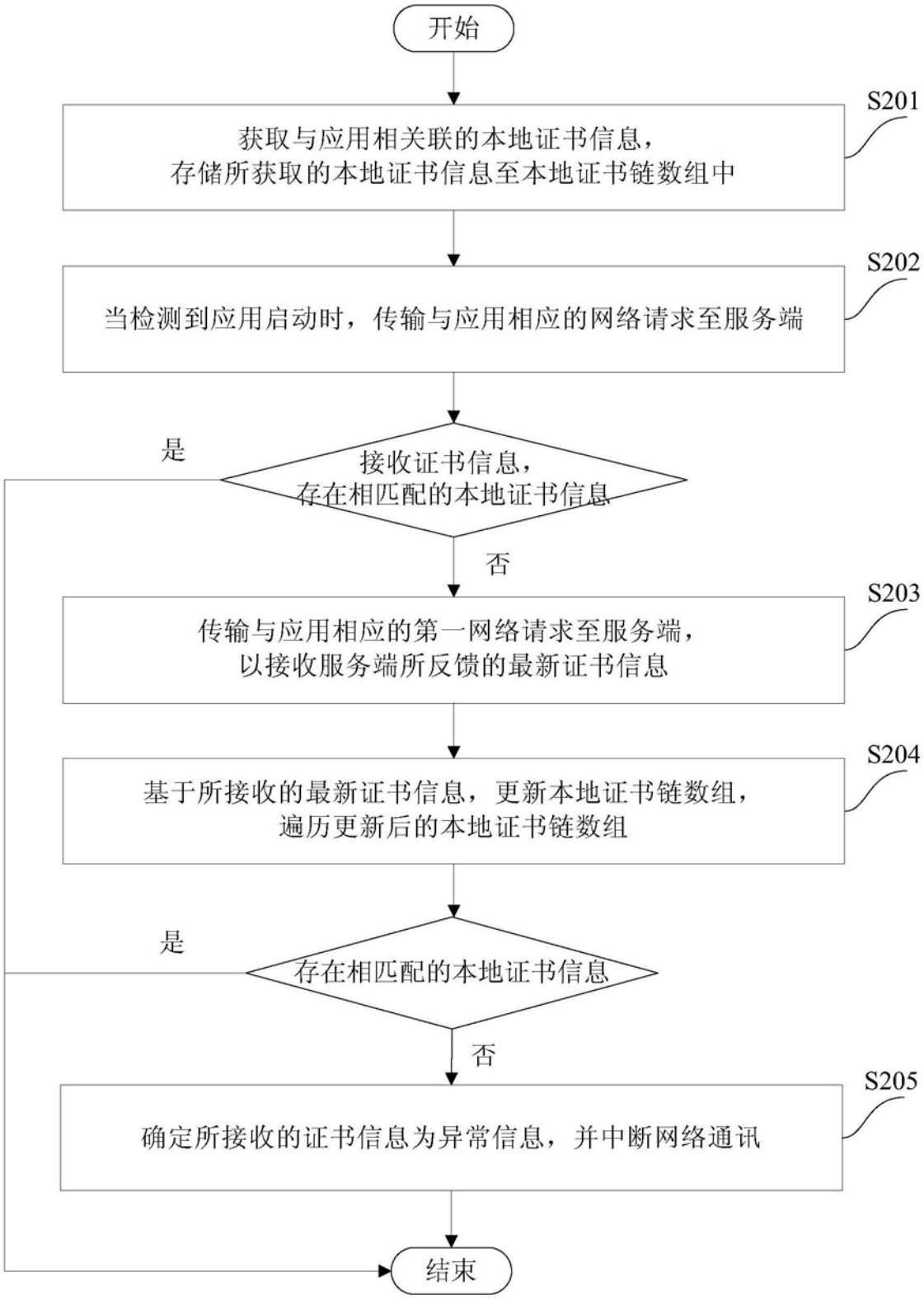

开始
S201
获取与应用相关联的本地证书信息，
存储所获取的本地证书信息至本地证书链数组中
S202
当检测到应用启动时，传输与应用相应的网络请求至服务端
是
接收证书信息，
存在相匹配的本地证书信息
否
S203
传输与应用相应的第一网络请求至服务端，
以接收服务端所反馈的最新证书信息
S204
基于所接收的最新证书信息，更新本地证书链数组，
遍历更新后的本地证书链数组
是
存在相匹配的本地证书信息
否
S205
确定所接收的证书信息为异常信息，并中断网络通讯
结束

图2

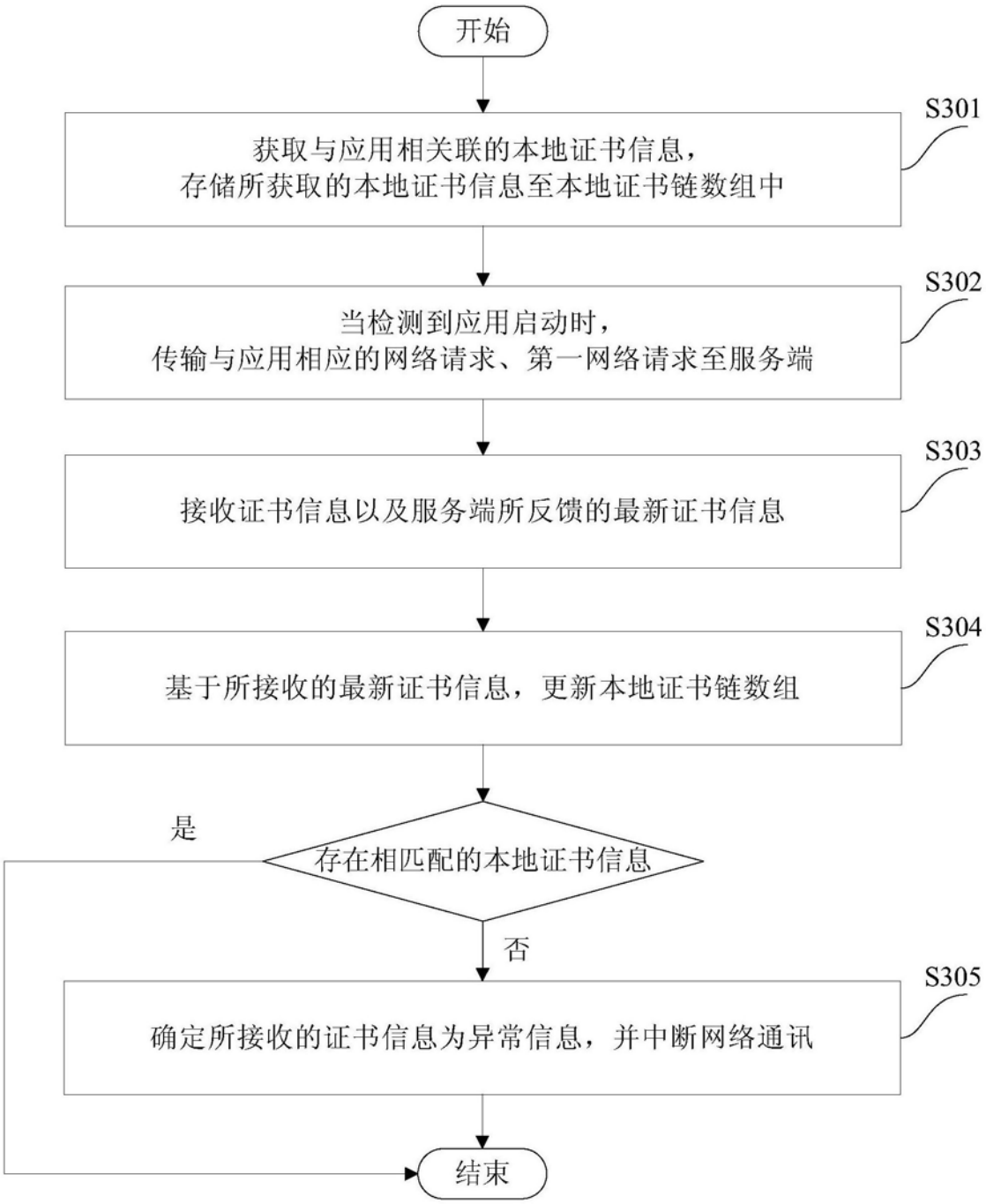

开始
S301
获取与应用相关联的本地证书信息，
存储所获取的本地证书信息至本地证书链数组中
S302
当检测到应用启动时，
传输与应用相应的网络请求、第一网络请求至服务端
S303
接收证书信息以及服务端所反馈的最新证书信息
S304
基于所接收的最新证书信息，更新本地证书链数组
是
存在相匹配的本地证书信息
否
S305
确定所接收的证书信息为异常信息，并中断网络通讯
结束

图3

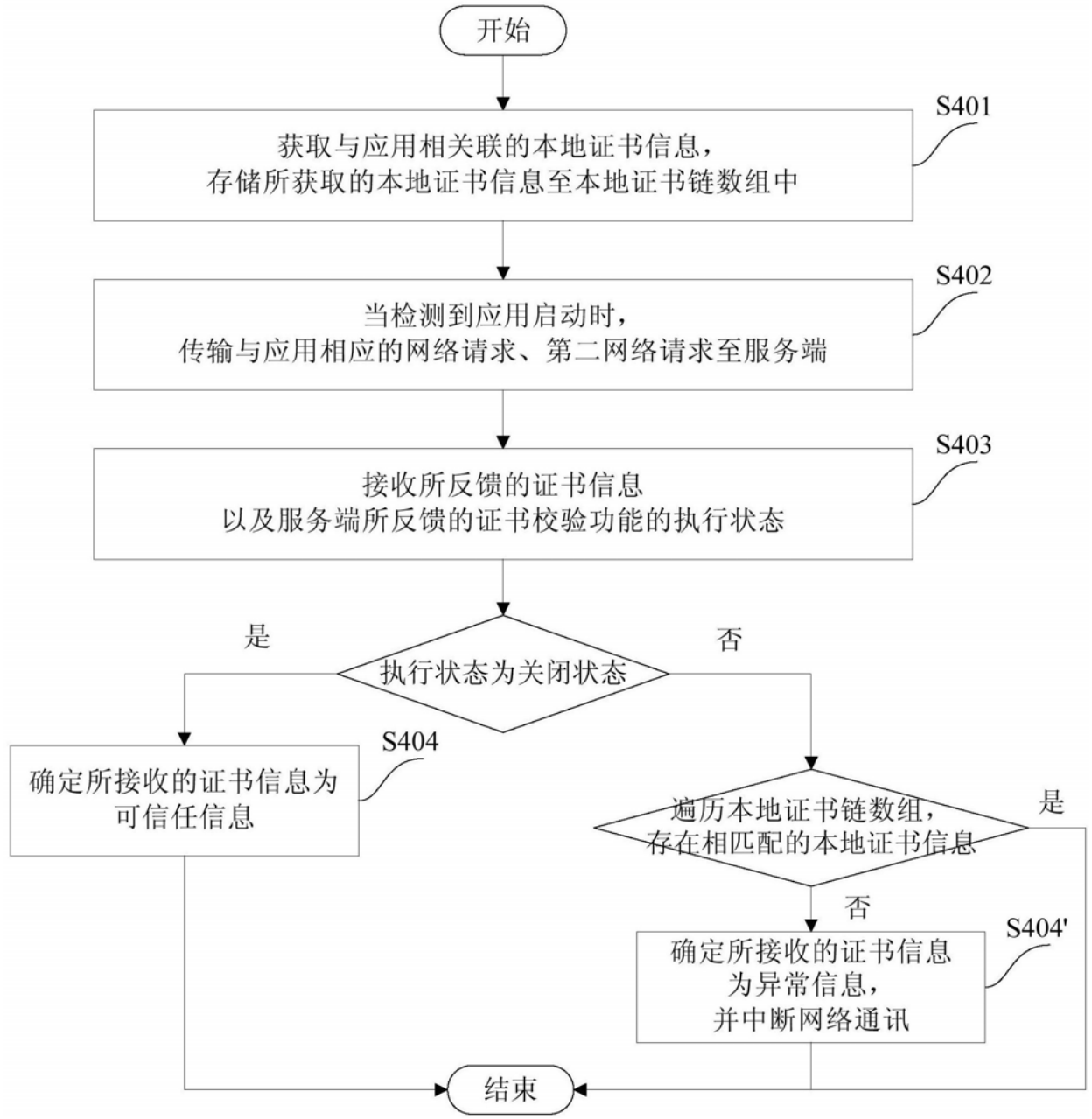

开始
S401
获取与应用相关联的本地证书信息，
存储所获取的本地证书信息至本地证书链数组中
S402
当检测到应用启动时，
传输与应用相应的网络请求、第二网络请求至服务端
S403
接收所反馈的证书信息
以及服务端所反馈的证书校验功能的执行状态
是
执行状态为关闭状态
否
S404
确定所接收的证书信息为
可信任信息
遍历本地证书链数组，
存在相匹配的本地证书信息
是
否
S404'
确定所接收的证书信息
为异常信息，
并中断网络通讯
结束

图4

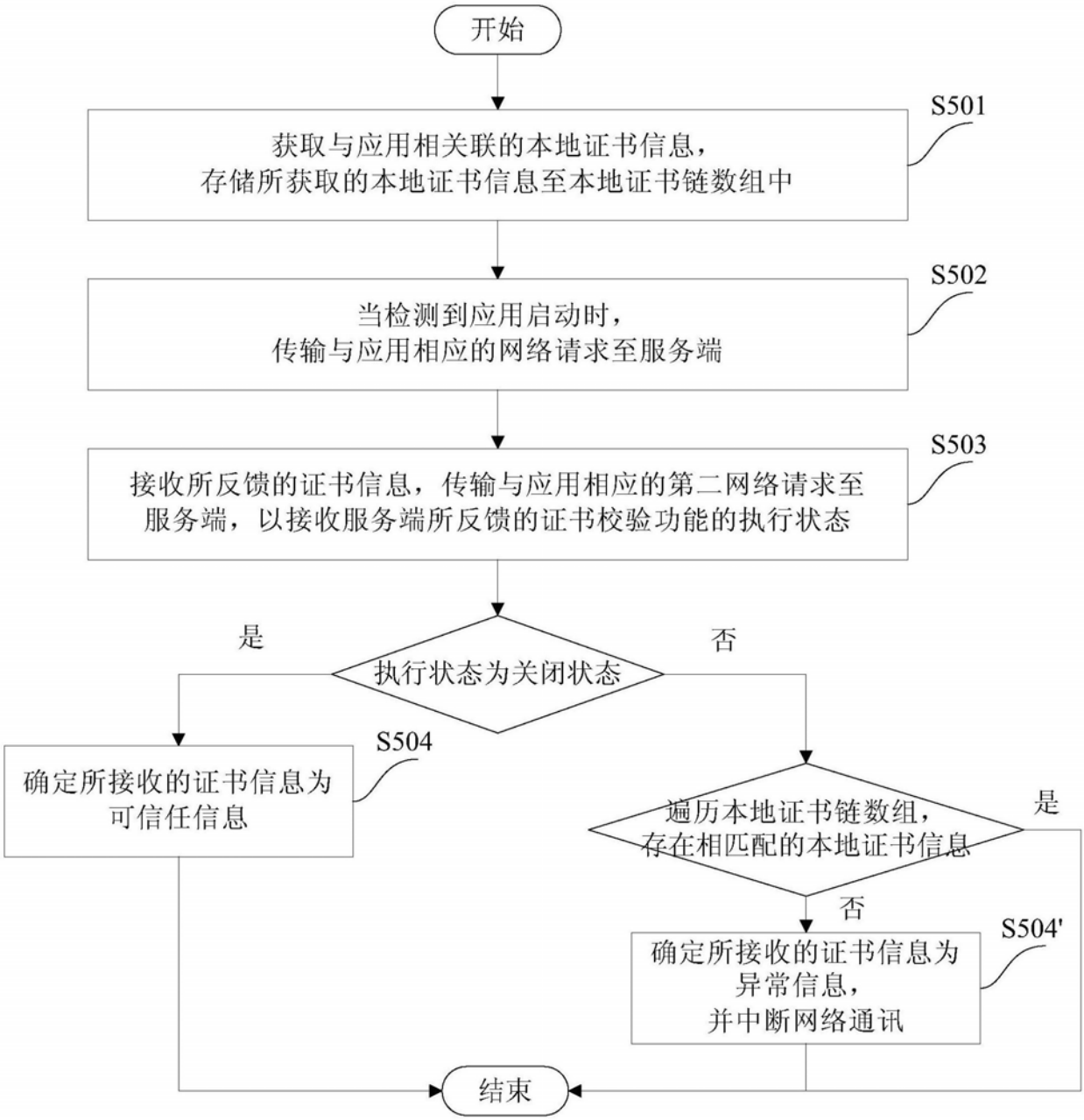

开始
S501
获取与应用相关联的本地证书信息，
存储所获取的本地证书信息至本地证书链数组中
S502
当检测到应用启动时，
传输与应用相应的网络请求至服务端
S503
接收所反馈的证书信息，传输与应用相应的第二网络请求至
服务端，以接收服务端所反馈的证书校验功能的执行状态
是
执行状态为关闭状态
否
S504
确定所接收的证书信息为
可信任信息
遍历本地证书链数组，
存在相匹配的本地证书信息
是
否
S504'
确定所接收的证书信息为
异常信息，
并中断网络通讯
结束

图5

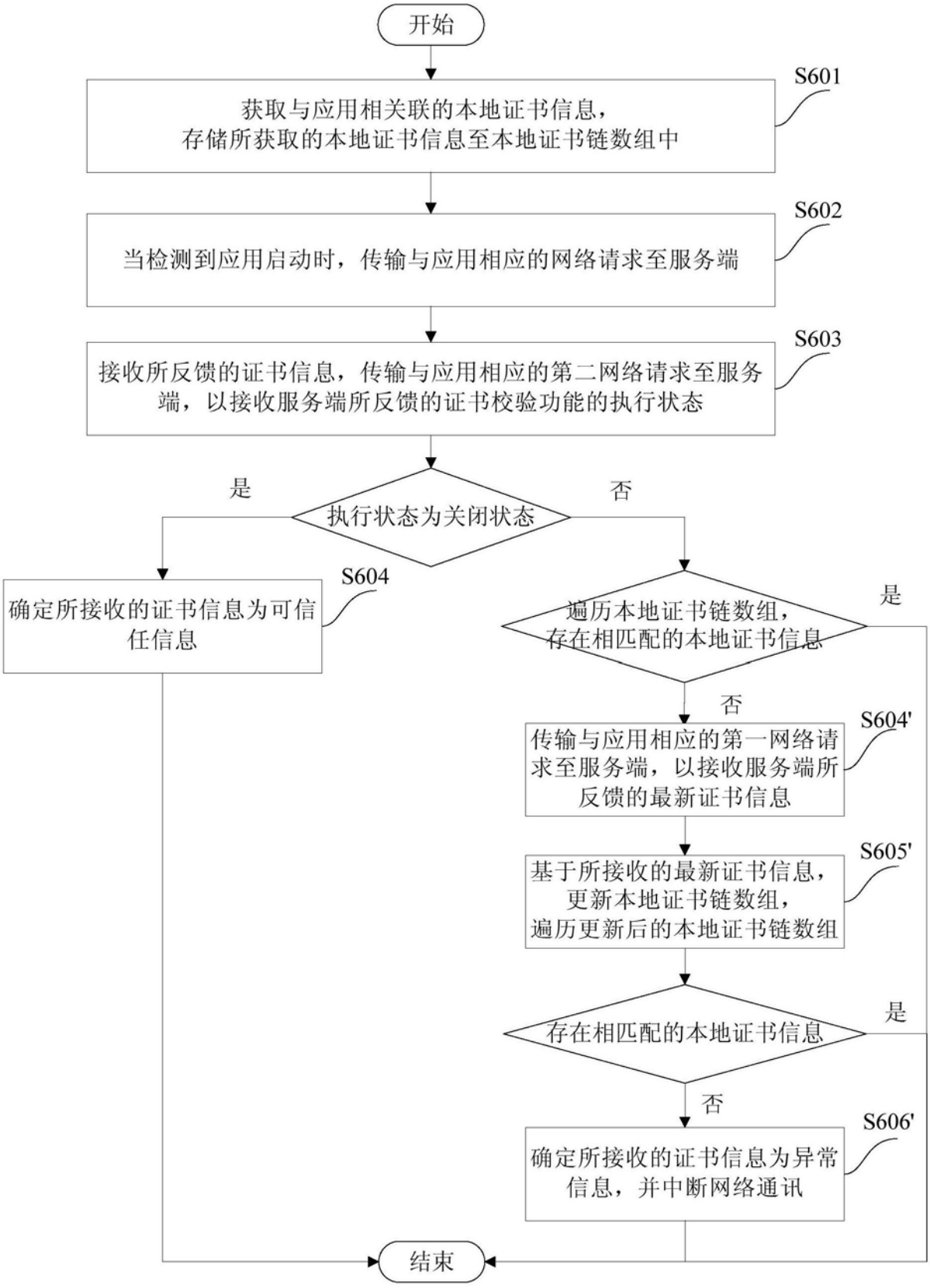

开始
S601
获取与应用相关联的本地证书信息，
存储所获取的本地证书信息至本地证书链数组中
S602
当检测到应用启动时，传输与应用相应的网络请求至服务端
S603
接收所反馈的证书信息，传输与应用相应的第二网络请求至服务端，以接收服务端所反馈的证书校验功能的执行状态
是
执行状态为关闭状态
否
S604
确定所接收的证书信息为可信任信息
遍历本地证书链数组，
存在相匹配的本地证书信息
是
否
S604'
传输与应用相应的第一网络请求至服务端，以接收服务端所反馈的最新证书信息
S605'
基于所接收的最新证书信息，
更新本地证书链数组，
遍历更新后的本地证书链数组
存在相匹配的本地证书信息
是
否
S606'
确定所接收的证书信息为异常信息，并中断网络通讯
结束

图6

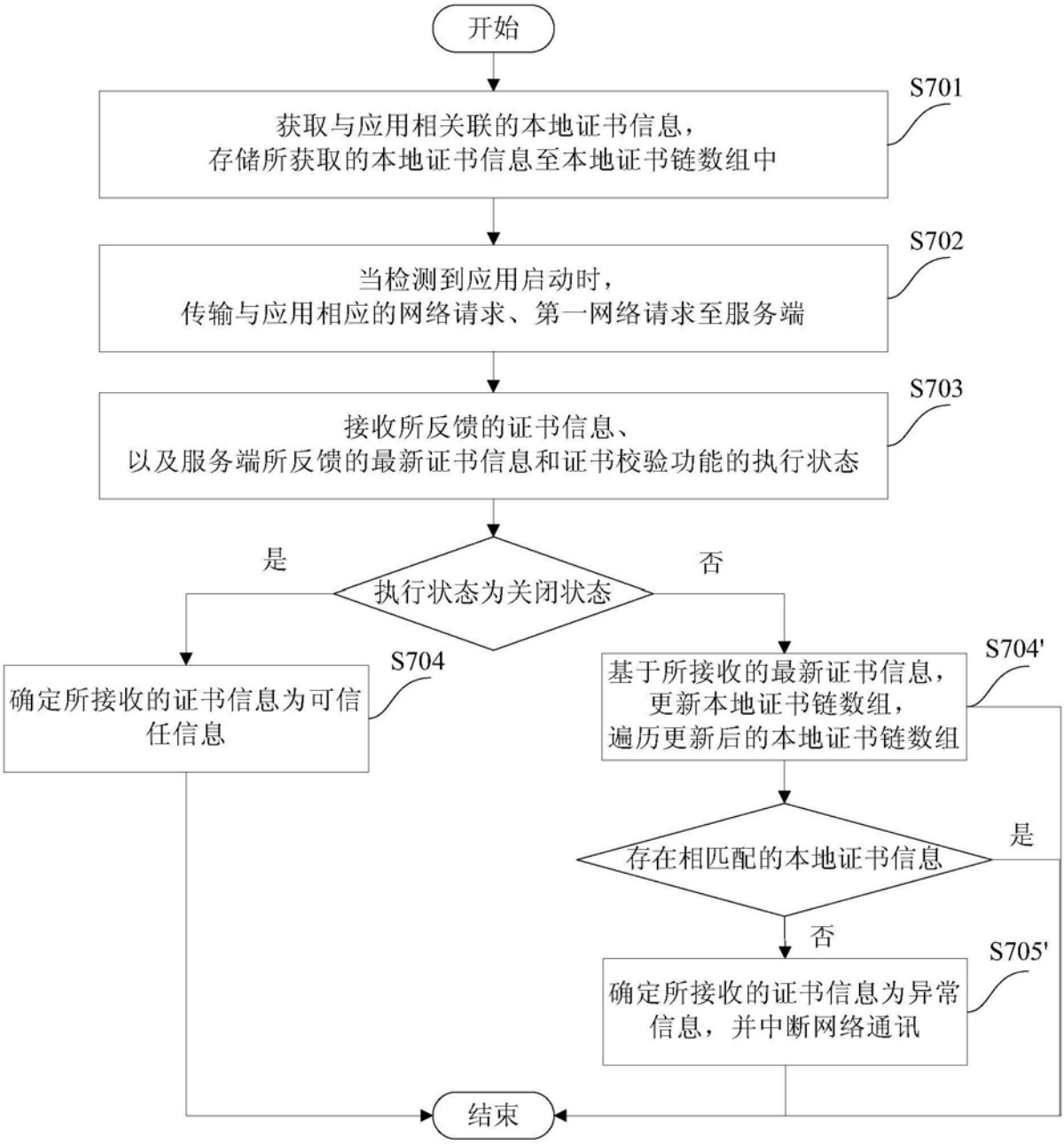

开始
S701
获取与应用相关联的本地证书信息，
存储所获取的本地证书信息至本地证书链数组中
S702
当检测到应用启动时，
传输与应用相应的网络请求、第一网络请求至服务端
S703
接收所反馈的证书信息、
以及服务端所反馈的最新证书信息和证书校验功能的执行状态
执行状态为关闭状态
是
否
S704
确定所接收的证书信息为可信任信息
S704'
基于所接收的最新证书信息，
更新本地证书链数组，
遍历更新后的本地证书链数组
存在相匹配的本地证书信息
是
否
S705'
确定所接收的证书信息为异常信息，并中断网络通讯
结束

图7

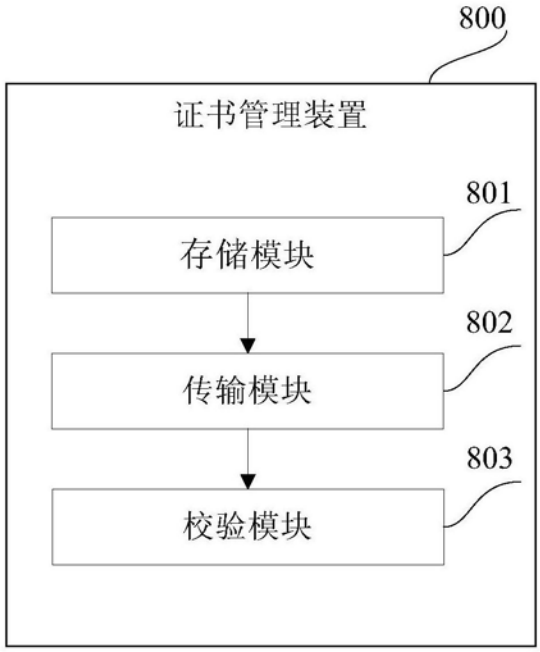


图8

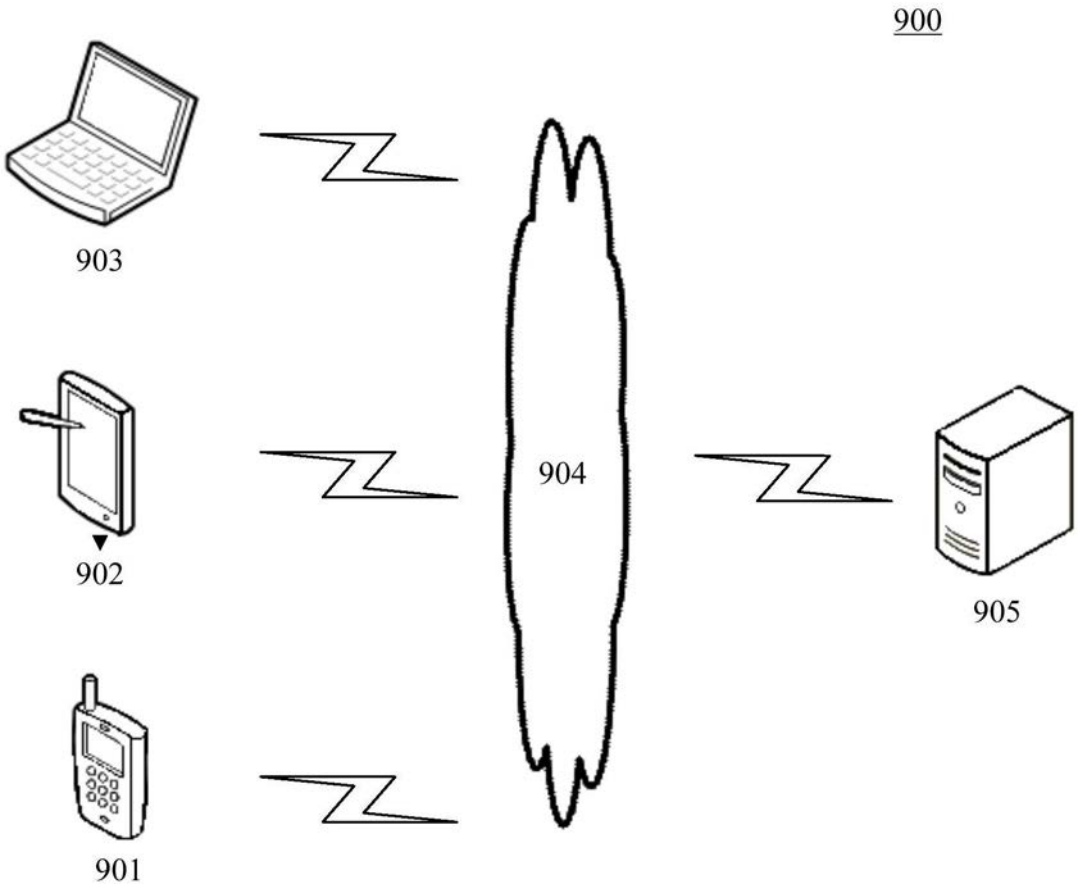


图9

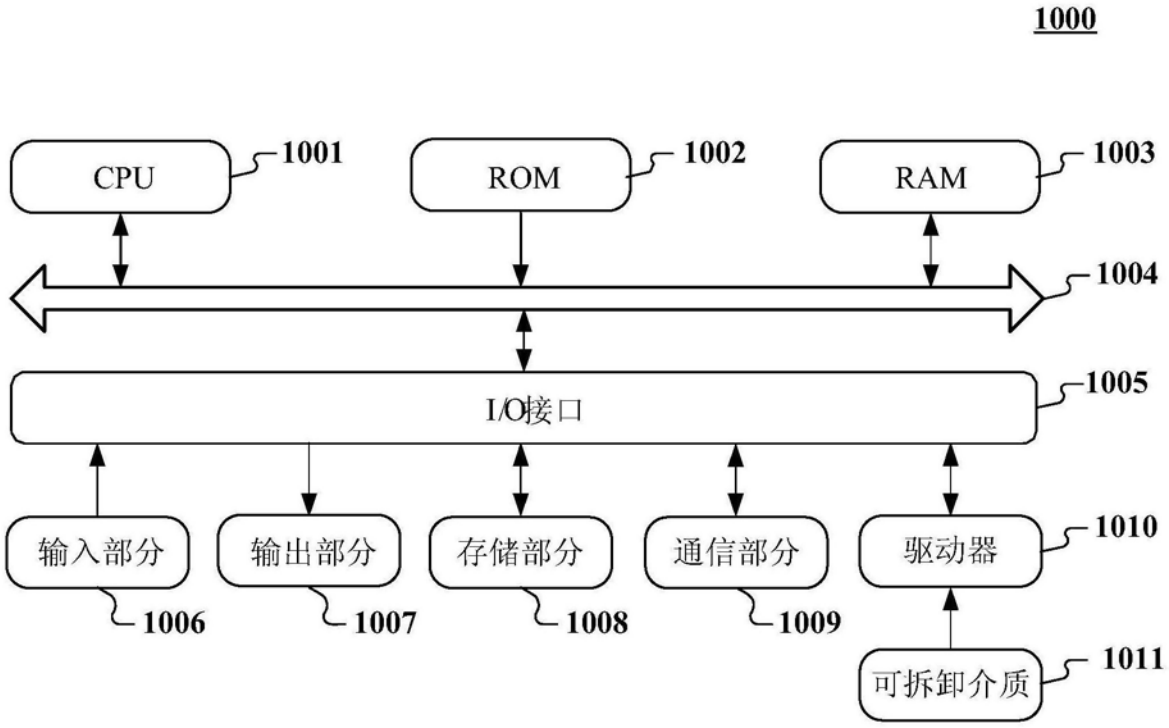

1000
CPU
1001
ROM
1002
RAM
1003
1004
I/O接口
1005
输入部分
输出部分
存储部分
通信部分
驱动器
1010
1006
1007
1008
1009
可拆卸介质
1011

图10