(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107147497 B
(45)授权公告日 2018.07.06

(21)申请号 201710302306.6

(22)申请日 2017.05.02

(65)同一申请的已公布的文献号
申请公布号 CN 107147497 A

(43)申请公布日 2017.09.08

(73)专利权人 北京海泰方圆科技股份有限公司
地址 100094 北京市海淀区东北旺西路8号中关村软件园9号楼国际软件大厦E座一层、二层

(72)发明人 姜海舟 叶家明 王烨

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 赵囡囡 褚敏

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

(56)对比文件
CN 103338215 A,2013.10.02,全文.
CN 106572109 A,2017.04.19,全文.
US 2015156025 A1,2015.06.04,全文.
CN 104094554 A,2014.10.08,说明书第[0002]-[0009]、[0027]-[0080]段.
CN 104539429 A,2015.04.22,说明书第[0002]-[0005]、[0091]-[0254]段.

审查员 吴龙

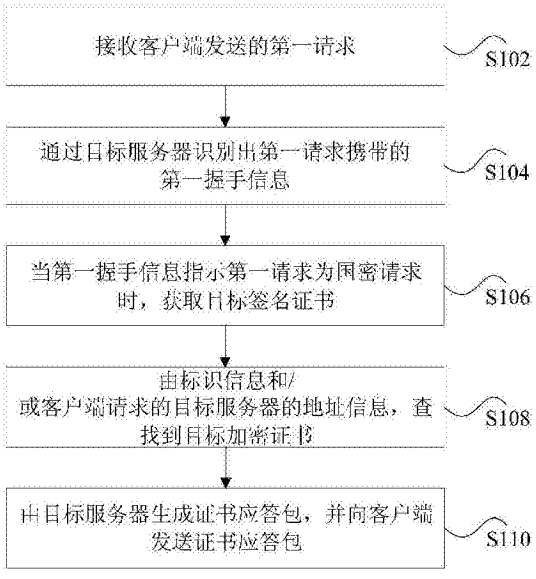
权利要求书2页 说明书7页 附图1页

(54)发明名称

信息处理方法和装置

(57)摘要

本发明公开了一种信息处理方法和装置。该信息处理方法包括：接收客户端发送的第一请求，其中，第一请求用于请求与目标服务器进行握手操作；通过目标服务器识别出第一请求携带的第一握手信息；当第一握手信息指示第一请求为国密请求时，获取目标签名证书，其中，目标签名证书中包括用于标识目标加密证书的标识信息；由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书；由目标服务器生成证书应答包，并向客户端发送证书应答包，其中，客户端根据证书应答包与目标服务器继续进行握手操作。通过本发明，达到了降低国密改造成本的效果。



CN 107147497 B

1.一种信息处理方法,其特征在于,包括:

接收客户端发送的第一请求,其中,所述第一请求用于请求与目标服务器进行握手操作;

通过所述目标服务器识别出所述第一请求携带的第一握手信息;

当所述第一握手信息指示所述第一请求为国密请求时,获取目标签名证书,其中,所述目标签名证书中包括用于标识目标加密证书的标识信息,所述目标签名证书预先配置在所述目标服务器的站点证书的配置项中;

由所述标识信息和/或所述客户端请求的所述目标服务器的地址信息,查找到所述目标加密证书;

由所述目标服务器生成证书应答包,并向所述客户端发送所述证书应答包,其中,所述客户端根据所述证书应答包与所述目标服务器继续进行握手操作;

其中,由所述标识信息和/或所述客户端请求的所述目标服务器的地址信息,查找到所述目标加密证书包括:

解析所述目标签名证书,得到目标签名证书信息;

从所述目标签名证书信息中提取出所述标识信息;

根据所述标识信息从预设证书库中查找所述目标加密证书,其中,所述预设证书库用于存储多个国密证书,所述多个国密证书包括所述目标加密证书。

2.根据权利要求1所述的方法,其特征在于,根据所述标识信息从所述预设证书库中查找所述目标加密证书包括:

获取所述第一请求携带的所述目标服务器的地址信息;

根据所述标识信息和所述地址信息从所述预设证书库中查找所述目标加密证书,其中,所述目标加密证书用于所述客户端与所述地址信息对应的所述目标服务器进行握手操作。

3.根据权利要求1或2所述的方法,其特征在于,在获取所述目标签名证书之前,所述方法还包括:

根据多个服务器的地址信息在预设配置项中配置多张签名证书,其中,所述多张签名证书包括所述目标签名证书,所述多张签名证书分别包括用于标识加密证书的标识信息;

将所述多张签名证书配置在预设证书库中。

4.根据权利要求1或2所述的方法,其特征在于,所述目标签名证书为国密安全套接层SSL签名证书,所述目标加密证书为国密安全套接层SSL加密证书。

5.根据权利要求1或2所述的方法,其特征在于,所述证书应答包包括:所述目标签名证书、所述目标加密证书和所述目标服务器的信息。

6.一种信息处理装置,其特征在于,包括:

接收单元,用于接收客户端发送的第一请求,其中,所述第一请求用于请求与目标服务器进行握手操作;

识别单元,用于通过所述目标服务器识别出所述第一请求携带的第一握手信息;

获取单元,用于当所述第一握手信息指示所述第一请求为国密请求时,获取目标签名证书,其中,所述目标签名证书中包括用于标识目标加密证书的标识信息,所述目标签名证书预先配置在所述目标服务器的站点证书的配置项中;

查找单元，由所述标识信息和/或所述客户端请求的所述目标服务器的地址信息，查找到所述目标加密证书；

生成单元，用于由所述目标服务器生成证书应答包，并向所述客户端发送所述证书应答包，其中，所述客户端根据所述证书应答包与所述目标服务器继续进行握手操作；

所述查找单元包括：

解析模块，用于在生成所述目标服务器的所述证书应答包之前，解析所述目标签名证书，得到目标签名证书信息；

提取模块，用于从所述目标签名证书信息中提取出所述标识信息；

查找模块，用于根据所述标识信息从预设证书库中查找所述目标加密证书，其中，所述预设证书库用于存储多个国密证书，所述多个国密证书包括所述目标加密证书。

7.根据权利要求6所述的装置，其特征在于，所述查找模块包括：

获取子模块，用于获取所述第一请求携带的所述目标服务器的地址信息；

查找子模块，用于根据所述标识信息和所述地址信息从所述预设证书库中查找所述目标加密证书，其中，所述目标加密证书用于所述客户端与所述地址信息对应的所述目标服务器进行握手操作。

8.一种存储介质，其特征在于，所述存储介质包括存储的程序，其中，在所述程序运行时控制所述存储介质所在设备执行权利要求1至5中任意一项所述的信息处理方法。

9.一种处理器，其特征在于，所述处理器用于运行程序，其中，所述程序运行时执行权利要求1至5中任意一项所述的信息处理方法。

信息处理方法和装置

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种信息处理方法和装置。

背景技术

[0002] 目前，安全套接层(Secure Sockets Layer，简称为SSL)网关的服务器多为专有的网关设备。而对于SSL服务器软件，通常采用的算法为国际算法。

[0003] 服务器软件通常只能配置一张站点证书，比如，只支持签名证书的配置。不支持国密SSL，如Apache、Nginx等。如果重新改造国际常规的服务器软件，现有的云厂商以及服务器都需要重新部署，后期的部署工作量和工作难度都较大。因此在国密改造过程中，通常采用重新采购SSL硬件网关的方法。

[0004] 针对现有技术中在国密改造过程中，改造成本大的问题，目前尚未提出有效的解决方案。

发明内容

[0005] 本发明的主要目的在于提供一种信息处理方法和装置，以至少解决在国密改造过程中，改造成本大的问题。

[0006] 为了实现上述目的，根据本发明的一个方面，提供了一种信息处理方法。该信息处理方法包括：接收客户端发送的第一请求，其中，第一请求用于请求与目标服务器进行握手操作；通过目标服务器识别出第一请求携带的第一握手信息；当第一握手信息指示第一请求为国密请求时，获取目标签名证书，其中，目标签名证书中包括用于标识目标加密证书的标识信息；由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书；由目标服务器生成证书应答包，并向客户端发送证书应答包，其中，客户端根据证书应答包与目标服务器继续进行握手操作。

[0007] 可选地，在生成目标服务器的证书应答包之前，该信息处理方法还包括：解析目标签名证书，得到目标签名证书信息；从目标签名证书信息中提取出标识信息；根据标识信息从预设证书库中查找目标加密证书，其中，预设证书库用于存储多个国密证书，多个国密证书包括目标加密证书。

[0008] 可选地，由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书包括：获取第一请求携带的目标服务器的地址信息；根据标识信息和地址信息从预设证书库中查找目标加密证书，其中，目标加密证书用于客户端与地址信息对应的目标服务器进行握手操作。

[0009] 可选地，在获取目标签名证书之前，该信息处理方法还包括：根据多个服务器的地址信息在预设配置项中配置多张签名证书，其中，多张签名证书包括目标签名证书，多张签名证书分别包括用于标识加密证书的标识信息；将多张签名证书配置在预设证书库中。

[0010] 可选地，目标签名证书为国密SSL签名证书，目标加密证书为国密SSL加密证书。

[0011] 可选地，证书应答包包括：目标签名证书、目标加密证书和目标服务器的信息。

[0012] 为了实现上述目的，根据本发明的另一方面，还提供了一种信息处理装置。该信息处理装置包括：接收单元，用于接收客户端发送的第一请求，其中，第一请求用于请求与目标服务器进行握手操作；识别单元，用于通过目标服务器识别出第一请求携带的第一握手信息；获取单元，用于当第一握手信息指示第一请求为国密请求时，获取目标签名证书，其中，目标签名证书中包括用于标识目标加密证书的标识信息；查找单元，由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书；生成单元，用于由目标服务器生成证书应答包，并向客户端发送证书应答包，其中，客户端根据证书应答包与目标服务器继续进行握手操作。

[0013] 可选地，该查找单元包括：解析模块，用于在生成目标服务器的证书应答包之前，解析目标签名证书，得到目标签名证书信息；提取模块，用于从目标签名证书信息中提取出标识信息；查找模块，用于根据标识信息从预设证书库中查找目标加密证书，其中，预设证书库用于存储多个国密证书，多个国密证书包括目标加密证书。

[0014] 可选地，该查找模块包括：获取子模块，用于获取第一请求携带的目标服务器的地址信息；查找子模块，用于根据标识信息和/或地址信息从预设证书库中查找目标加密证书，其中，目标加密证书用于客户端与地址信息对应的目标服务器进行握手操作。

[0015] 为了实现上述目的，根据本发明的另一方面，还提供了一种存储介质。该存储介质包括存储的程序，其中，在程序运行时控制存储介质所在设备执行本发明中的信息处理方法。

[0016] 为了实现上述目的，根据本发明的另一方面，还提供了一种处理器。该处理器用于运行程序，其中，程序运行时执行本发明的信息处理方法。

[0017] 通过本发明，采用接收客户端发送的第一请求，其中，第一请求用于请求与目标服务器进行握手操作；通过目标服务器识别出第一请求携带的第一握手信息；当第一握手信息指示第一请求为国密请求时，获取目标签名证书，其中，目标签名证书中包括用于标识目标加密证书的标识信息；由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书；由目标服务器生成证书应答包，并向客户端发送证书应答包，其中，客户端根据证书应答包与目标服务器继续进行握手操作。由于通过算法自助查找国密的加密证书，实现了在不改造国际常用服务器软件的基础上，在服务器软件上依然支持国密证书的目的，解决了在国密改造过程中，改造成本大的问题，进而达到了降低在国密改造过程中的改造成本的效果。

附图说明

[0018] 构成本申请的一部分的附图用来提供对本发明的进一步理解，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0019] 图1是根据本发明实施例的一种信息处理方法的流程图；以及

[0020] 图2是根据本发明实施例的一种信息处理装置的示意图。

具体实施方式

[0021] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本发明。

[0022] 为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分的实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

[0023] 需要说明的是，本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0024] 实施例1

[0025] 本发明实施例提供了一种信息处理方法。

[0026] 图1是根据本发明实施例的一种信息处理方法的流程图。如图1所示，该信息处理方法包括以下步骤：

[0027] 步骤S102，接收客户端发送的第一请求。

[0028] 在本发明上述步骤S102提供的技术方案中，接收客户端发送的第一请求，其中，第一请求用于请求与目标服务器进行握手操作。

[0029] 该实施例的信息处理方法执行在服务器底层算法库中。客户端发送第一请求，该第一请求为SSL请求，用于与目标服务器进行握手操作。其中，目标服务器可以为网站(Web)服务器，该网站服务器为驻留于因特网上某种类型计算机的程序，可以向浏览器提供文档，可以为Web客户端放置网站文件，也可以放置数据文件。该实施例的目标服务器不仅能够存储信息，还能在用户通过Web浏览器提供的信息的基础上运行脚本和程序，具有多个站点，比如，百度站点、网易站点等，此处不做限制。不同的站点都有自己的证书。接收客户端发送的用于与目标服务器进行握手操作的第一请求。

[0030] 步骤S104，通过目标服务器识别出第一请求携带的第一握手信息。

[0031] 在本发明上述步骤S104提供的技术方案中，识别出第一请求携带的第一握手信息。

[0032] 第一请求携带第一握手信息，比如，第一握手信息为标准协议流程的信息ClientHello，该ClientHello中包括了请求版本。第一握手信息还可以包括客户端的随机数、第一请求的发送时间、请求进行握手操作的服务器信息等。

[0033] 在接收客户端发送的第一请求之后，通过目标服务器识别出第一请求携带的第一握手信息。

[0034] 步骤S106，当第一握手信息指示第一请求为国密请求时，获取目标签名证书。

[0035] 在本发明上述步骤S106提供的技术方案中，当第一握手信息指示第一请求为国密请求时，获取目标签名证书，其中，目标签名证书中包括用于标识目标加密证书的标识信息。

[0036] 国密SSL在握手过程中需要使用国密双证书。在通过目标服务器识别出第一请求携带的第一握手信息之后，判断第一握手信息指示的第一请求的版本，当第一握手信息指

示第一请求为国密请求时，获取目标签名证书。该目标签名证书为预先配置的签名证书，可以预先配置在Web服务器站点证书的配置项中，该目标签名证书包括用于标识目标加密证书的标识信息，为国密SSL站点证书中的一种。

[0037] 步骤S108，由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书。

[0038] 可选地，对目标签名证书进行解析，得到目标签名证书的签名证书信息，从签名证书信息中提取出用于标识目标加密证书的标识信息，根据标识信息在国密证书库中查找并识别目标加密证书。其中，国密证书库可以为国密证书存储库，为加密证书的存储位置，签名证书中包括加密证书的标识信息，如，在签名证书的文件扩展信息中记录加密证书的标识信息，该标识信息可以为加密证书的颁发信息、指纹信息、序列号、公钥信息等，其中，颁发信息可以为加密证书的颁发者，此处不做限定。

[0039] 可选地，对目标签名证书进行解析，得到目标签名证书的签名证书信息，从签名证书信息中提取出标识信息；获取客户端请求的目标服务器的地址信息；根据标识信息和客户端请求的目标服务器的地址信息在国密证书库中查找并识别目标加密证书。

[0040] 可选地，根据客户端请求的目标服务器的地址信息在国密证书库中查找并识别目标加密证书。

[0041] 需要说明的是，本发明实施例的获取目标加密证书的方法仅为本发明的优选实施方式，并不限定本发明的获取目标加密证书的方法仅为上述方式，任何可以获取目标加密证书的方法，且达到降低国密改造过程中的成本的方法都在本发明的保护范围之内，此处不再一一举例说明。

[0042] 步骤S110，由目标服务器生成证书应答包，并向客户端发送证书应答包。

[0043] 在本发明上述步骤S108提供的技术方案中，由目标服务器生成证书应答包，其中，客户端根据证书应答包与目标服务器进行握手操作。

[0044] 在由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书之后，由目标服务器生成证书应答包，证书应答包也即证书应答数据包，所述证书应答包包括目标签名证书、目标加密证书和目标服务器的信息，所述目标服务器信息为目标服务器与客户端在交互过程中产生的信息。

[0045] 客户端在接收到证书应答包之后，根据证书应答包与目标服务器继续进行SSL握手操作。

[0046] 该实施例采用接收客户端发送的第一请求，其中，第一请求用于请求与目标服务器进行握手操作；通过目标服务器识别出第一请求携带的第一握手信息；当第一握手信息指示第一请求为国密请求时，获取目标签名证书，其中，目标签名证书中包括用于标识目标加密证书的标识信息；由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书；由目标服务器生成证书应答包，并向客户端发送证书应答包，其中，客户端根据证书应答包与目标服务器继续进行握手操作。由于通过在服务器底层算法上实现上述方法，实现了自助查找国密的加密证书的目的，并且在不改造国际常用服务器软件的基础上，达到在服务器软件上依然支持国密证书的目的，解决了在国密改造过程中，改造成本大的问题，进而达到了降低在国密改造过程中的改造成本的效果。

[0047] 作为一种可选的实施方式，在由目标签名证书和由标识信息标识的目标加密证书

生成证书应答包之前，该信息处理方法还包括：解析目标签名证书，得到目标签名证书信息；从目标签名证书信息中提取出标识信息；根据标识信息从预设证书库中查找目标加密证书，其中，预设证书库用于存储多个国密证书，多个国密证书包括目标加密证书。

[0048] 在获取目标签名证书之后，在由目标签名证书和由标识信息标识的目标加密证书生成证书应答包之前，对目标签名证书进行解析，得到目标签名证书信息，该目标签名证书信息可以包括目标加密证书的标识信息，比如，目标加密证书的颁发信息、指纹信息、序列号、公钥信息等，其中，颁发信息包括加密证书的颁发者。在得到目标证书信息之后，从目标签名证书信息中提取出标识信息。

[0049] 该实施例的预设证书库用于存储根据不同站点配置的加密证书，该预设证书库用于确定加密证书的存储路径，可以为国密证书存储库，也即，为国密证书库。在从目标签名证书信息中提取出标识信息之后，根据标识信息从预设证书库中查找并通过目标服务器识别目标服务器对应的目标加密证书，从而实现了在服务器的底层算法库中，根据目标签名证书包括的标识信息获取目标加密证书的目的。

[0050] 作为一种可选的实施方式，由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书包括：获取第一请求携带的目标服务器的地址信息；根据标识信息和地址信息从预设证书库中查找目标加密证书，其中，目标加密证书用于客户端与地址信息对应的目标服务器进行握手操作。

[0051] 目标服务器信息包括目标服务器的地址信息，该地址信息可以为目标服务器对应的不同站点的地址信息，比如，该站点为百度站点、网易站点等，每个站点的地址信息不同。第一请求携带目标服务器的地址信息，根据目标签名证书的标识信息和目标服务器的地址信息从预设证书库中查找并识别目标加密证书，该目标加密证书用于客户端与地址信息对应的目标服务器进行握手操作，具体地，目标签名证书用于与目标服务器对应的站点进行握手操作。

[0052] 作为一种可选的实施方式，在获取目标签名证书之前，该信息处理方法还包括：根据多个服务器的地址信息在预设配置项中配置多张签名证书，其中，多张签名证书包括目标签名证书，多张签名证书分别包括用于标识加密证书的标识信息；将多张签名证书配置在预设证书库中。

[0053] 可选地，证书应答包包括：目标签名证书、目标加密证书和所述目标服务器的信息。

[0054] 需要说明的是，上述生成证书应答包的方式仅为本发明实施例的优选实施方式，并不限定本发明实施例只由目标签名证书、目标加密证书和目标服务器的信息生成证书应答包，任何可以结合目标签名证书、目标加密证书和目标服务器的信息生成证书应答包，且达到降低国密改造过程中的成本的方法都在本发明的保护范围之内，此处不再一一举例说明。

[0055] 该实施例的服务器可以为SSL Web服务器。在SSL Web服务器上，预先根据服务器的不同站点配置相应的两张国密SSL站点证书，其中，一张SSL站点证书为签名证书，一张站点证书为加密证书。可选地，签名证书的文件扩展信息中记录有加密证书的标识信息，比如，加密证书的颁发信息、指纹信息、序列号、公钥信息等，将国密SSL签名证书配置在Web服务器站点证书的配置项中，将加密证书配置在国密证书存储库中，从而实现了对不同站点

的签名证书和加密证书的预配置，以便于客户端与服务器的不同站点进行握手操作。

[0056] 需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0057] 实施例2

[0058] 下面结合优选的实施方式对本发明的技术方案进行说明。

[0059] 本发明实施例主要实现了一种使得Web服务器软件支持国密SSL证书的方法。可选地，通过如下技术手段来实现上述使得Web服务器软件支持国密SSL证书的方法。

[0060] 在SSL Web服务器端，预先根据SSL Web服务器的不同站点配置相应的两张国密SSL站点证书。其中，一张国密SSL站点证书为签名证书，另一张国密SSL站点证书为加密证书。可选地，国密SSL签名证书的文件扩展信息中记录有加密证书标识信息，比如，加密证书标识信息为加密证书的颁发信息、指纹信息、序列化、公钥信息等。将每个站点的国密SSL签名证书配置在Web服务器站点证书的配置项中，将每个站点的国密SSL加密证书配置在国密证书存储库中，从而实现了对每个站点的签名证书和加密证书进行预先配置，进而替换Web服务器的底层算法库。

[0061] 客户端在发起SSl请求时，请求ClientHello中包含了SSL(国密/国际)请求版本信息和请求进行握手操作的服务器信息。

[0062] 服务端接收并识别请求ClientHello中包含的请求版本信息以及请求的服务器信息。当服务器识别出客户端发送的SSL请求为国密请求时，进行国密SSL算法流程，向客户端发送ServerHello，同时获取Web服务器端预先配置的签名证书，解析签名证书，得到签名证书信息。根据解析出的签名证书信息和/或客户端请求的服务器地址信息在国密证书存储库中查找并识别国密SSL加密证书，通过国密SSL加密证书组织ServerCertificate数据包、ServerHelloDone数据包，向客户端发送ServerCertificate数据包、ServerHelloDone数据包和服务器相关信息。在客户端接收到ServerCertificate数据包、ServerHelloDone数据包和服务器相关信息之后，客户端根据Server包与服务器端进行SSL握手。最后，服务器使用国密算法证书与客户端完成国密SSL握手过程。

[0063] 由上述可知，该实施例实现了国密SSL服务端获取国密证书的方法，以及在不改造国际常用SSL软件的基础上使用国密SSL，上述步骤由底层算法库来实现，通过算法自助查找国密SSL加密证书，实现了在不改造国际常用SSL软件的基础上，在常规Web服务器软件上支持国密证书的目的，也避免了由于通常Web服务器只支持一张站点证书的配置，而导致重新改造国际常规软件，后期的部署工作较大，现有云厂商及服务器都需要重新部署的问题。

[0064] 实施例3

[0065] 本发明实施例还提供了一种信息处理装置。需要说明的是，该实施例的信息处理装置可以用于执行本发明实施例的信息处理方法。

[0066] 图2是根据本发明实施例的一种信息处理装置的示意图。如图2所示，该信息处理装置包括：接收单元10、识别单元20、获取单元30、查找单元40和生成单元50。

[0067] 接收单元10，用于接收客户端发送的第一请求，其中，第一请求用于请求与目标服务器进行握手操作。

[0068] 识别单元20，用于通过目标服务器识别出第一请求携带的第一握手信息。

[0069] 获取单元30，用于当第一握手信息指示第一请求为国密请求时，获取目标签名证书，其中，目标签名证书中包括用于标识目标加密证书的标识信息。

[0070] 查找单元40，由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书。

[0071] 生成单元50，用于由目标服务器生成证书应答包，并向客户端发送证书应答包，其中，客户端根据证书应答包与目标服务器继续进行握手操作。

[0072] 可选地，该查找单元包括：解析模块和提取模块。其中，解析模块，用于在由目标签名证书和由标识信息标识的目标加密证书生成证书应答包之前，解析目标签名证书，得到目标签名证书信息；提取模块，用于从目标签名证书信息中提取出标识信息；查找模块，用于根据标识信息从预设证书库中查找目标加密证书，其中，预设证书库用于存储多个国密证书，多个国密证书包括目标加密证书。

[0073] 可选地，查找模块包括：获取子模块和查找子模块。其中，获取子模块，用于获取第一请求携带的目标服务器的地址信息；查找子模块，用于根据标识信息和/或地址信息从预设证书库中查找目标加密证书，其中，目标加密证书用于客户端与地址信息对应的目标服务器进行握手操作。

[0074] 可选地，该装置还包括：第一配置单元和第二配置单元。其中，第一配置单元，用于在获取目标签名证书之前，根据多个服务器的地址信息在预设配置项中配置多张签名证书，其中，多张签名证书包括目标签名证书，多张签名证书分别包括用于标识加密证书的标识信息；第二配置单元，用于将多张签名证书配置在预设证书库中。

[0075] 可选地，上述目标签名证书为国密SSL签名证书，目标加密证书为国密SSL加密证书。

[0076] 可选地，该信息处理装置中的证书应答包包括：目标签名证书、目标加密证书和目标服务器的信息。

[0077] 实施例4

[0078] 本发明实施例还提供了一种存储介质。该存储介质包括存储的程序，其中，在程序运行时控制存储介质所在设备执行本发明实施例的信息处理方法。

[0079] 实施例5

[0080] 本发明实施例还提供了一种处理器。该处理器用于运行程序，其中，程序运行时执行本发明实施例的信息处理方法。

[0081] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0082] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

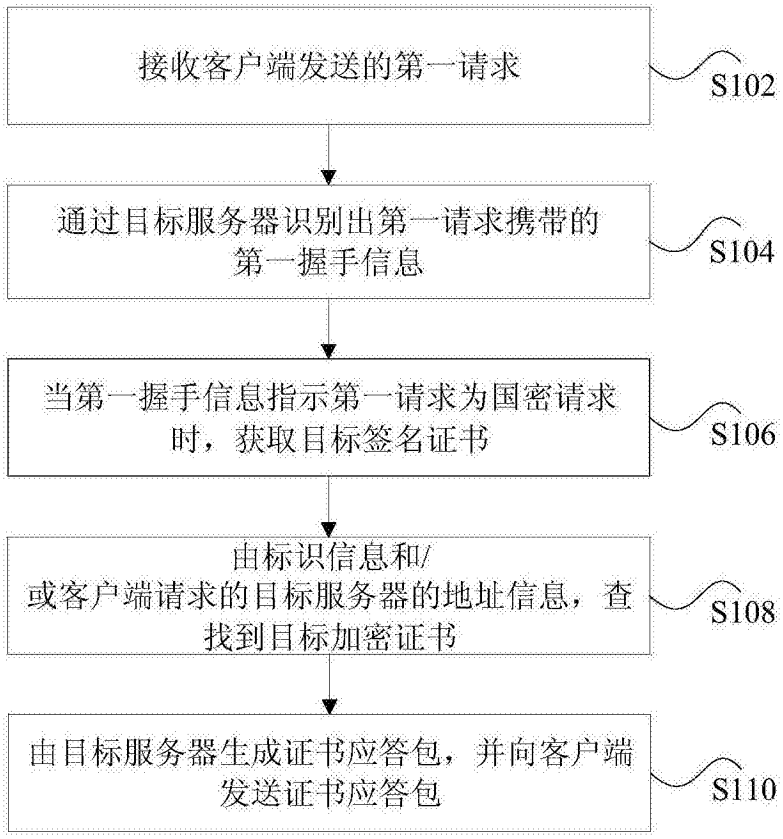

接收客户端发送的第一请求
S102
通过目标服务器识别出第一请求携带的第一握手信息
S104
当第一握手信息指示第一请求为国密请求时，获取目标签名证书
S106
由标识信息和/或客户端请求的目标服务器的地址信息，查找到目标加密证书
S108
由目标服务器生成证书应答包，并向客户端发送证书应答包
S110

图1

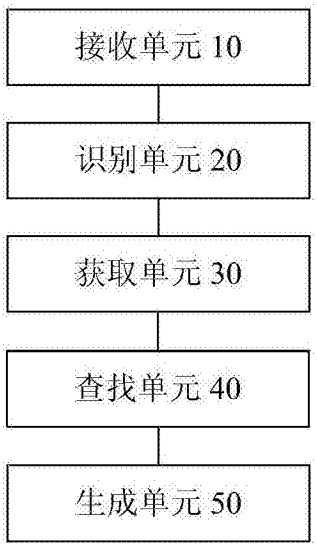

接收单元 10
识别单元 20
获取单元 30
查找单元 40
生成单元 50

图2