(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 2 月 22 日 (22.02.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/032939 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2017/094021

(22) 国际申请日: 2017 年 7 月 24 日 (24.07.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610692426.7 2016年8月19日 (19.08.2016) CN

(71) 申请人: 腾 讯 科 技 (深 圳) 有 限 公 司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(72) 发明人: 魏 伟 (WEI, Wei); 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(74) 代理人: 北 京 德 琦 知 识 产 权 代 理 有 限 公 司 (DEQI INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区知春路1号学院国际大厦7层, Beijing 100083 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,

WO 2018/032939 A1

(54) **Title:** NETWORK NODE ENCRYPTION METHOD AND NETWORK NODE ENCRYPTION DEVICE

(54) **发明名称:** 网络节点加密方法及网络节点加密装置

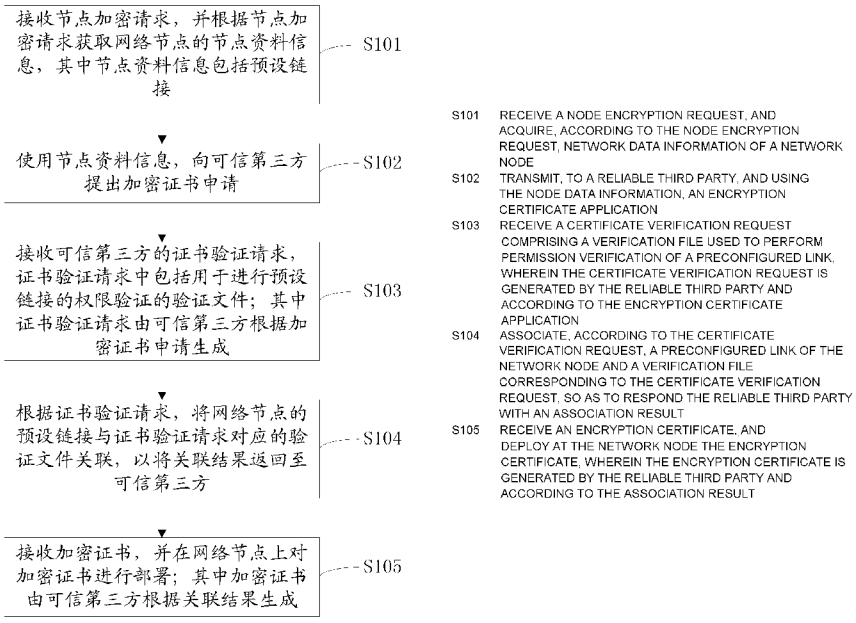

图 1

(57) **Abstract:** The application provides a network node encryption method comprising: receiving a node encryption request, and acquiring, according to the node encryption request, network data information of a network node; requesting, using the node data information, an encryption certificate application from a reliable third party; receiving a certificate verification request, and associating, according to the certificate verification request, a preconfigured link of the network node and a verification file corresponding to the certificate verification request, so as to respond the reliable third party with an association result; and receiving an encryption certificate,

[见续页]

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

and deploying at the network node the encryption certificate. The application also provides a network node encryption device.

(57) 摘要：本申请提供一种网络节点加密方法，其包括接收节点加密请求，并根据节点加密请求获取网络节点的节点资料信息；使用节点资料信息，向可信第三方提出加密证书申请；接收证书验证请求，并根据证书验证请求，将网络节点的预设链接与证书验证请求对应的验证文件关联，以将关联结果返回至可信第三方；接收加密证书，并在网络节点上对加密证书进行部署。本申请还提供一种网络节点加密装置。

网络节点加密方法及网络节点加密装置

本申请要求于 2016 年 08 月 19 日提交中国专利局、申请号为 201610692426.7、发明名称为“网络节点加密方法及网络节点加密装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及互联网领域，特别是涉及一种网络节点加密方法及网络节点加密装置。

背景技术

CDN（Content delivery network，内容分发网络）是一种通过互联网互相连接的电脑网络系统，可利用最靠近每位用户的服务器，更快、更可靠地将音乐、图片、视频、应用程序以及其他文件发送给其他用户，从而提供高性能、可扩展性以及低成本的网络内容。

为了提高 CDN 网络节点的安全性，网络内容提供者往往会对 CDN 网络节点进行加密操作。

发明内容

本申请实施例提供一种可自动对网络节点进行加密，从而提高网络节点的安全性的网络节点加密方法及网络节点加密装置。

本申请实施例提供一种网络节点加密方法，其包括:

接收节点加密请求，并根据所述节点加密请求获取网络节点的节点资料信息，其中所述节点资料信息包括预设链接;

使用所述节点资料信息，向可信第三方提出加密证书申请;

接收可信第三方的证书验证请求，所述证书验证请求中包括用于进行所述

预设链接的权限验证的验证文件；其中所述证书验证请求由所述可信第三方根据所述加密证书申请生成；

根据所述证书验证请求，将所述网络节点的预设链接与所述证书验证请求对应的验证文件关联，以将关联结果返回至所述可信第三方；以及

接收加密证书，并在所述网络节点上对所述加密证书进行部署；其中所述加密证书由所述可信第三方根据所述关联结果生成。

本申请实施例还提供一种网络节点加密装置，其包括：

存储器和处理器，所述存储器上存储有计算机可读指令，所述处理器执行所述计算机可读指令时实现以下步骤：

接收节点加密请求，并根据所述节点加密请求获取网络节点的节点资料信息，其中所述节点资料信息包括预设链接；

使用所述节点资料信息，向可信第三方提出加密证书申请；

接收可信第三方的证书验证请求，所述证书验证请求中包括用于进行所述预设链接的权限验证的验证文件；其中所述证书验证请求由所述可信第三方根据所述加密证书申请生成；

根据所述证书验证请求，将所述网络节点的预设链接与所述证书验证请求对应的验证文件关联，以将关联结果返回至所述可信第三方；以及

接收加密证书，并在所述网络节点上对所述加密证书进行部署；其中所述加密证书由所述可信第三方根据所述关联结果生成。

一种网络节点加密方法，包括：

接收网络节点加密装置发送的加密证书申请，并根据该加密证书申请生成证书验证请求，所述加密证书申请中包括有网络节点的节点资料信息，所述节点资料信息包括预设链接，所述证书验证请求中包括用于进行所述预设链接的权限验证的验证文件；

接收网络节点加密装置根据所述证书验证请求返回的关联结果；

在根据所述关联结果确定所述网络节点的预设链接与验证文件存在关联关

系时，生成相应的加密证书；

将该加密证书发送至网络节点加密装置。

一种用于可信第三方的网络节点加密装置，包括：

存储器和处理器，所述存储器上存储有计算机可读指令，所述处理器执行所述计算机可读指令时实现以下步骤：

接收网络节点加密装置发送的加密证书申请，并根据该加密证书申请生成证书验证请求，所述加密证书申请中包括有网络节点的节点资料信息，所述节点资料信息包括预设链接，所述证书验证请求中包括用于进行所述预设链接的权限验证的验证文件；

接收网络节点加密装置根据所述证书验证请求返回的关联结果；

在根据所述关联结果确定所述网络节点的预设链接与验证文件存在关联关系时，生成相应的加密证书；

将该加密证书发送至网络节点加密装置。

一种非易失性计算机可读存储介质，其中所述存储介质中存储有计算机可读指令，所述计算机可读指令可以由处理器执行以：

接收网络节点加密装置发送的加密证书申请，并根据该加密证书申请生成证书验证请求，所述加密证书申请中包括有网络节点的节点资料信息，所述节点资料信息包括预设链接，所述证书验证请求中包括用于进行所述预设链接的权限验证的验证文件；

接收网络节点加密装置根据所述证书验证请求返回的关联结果；

在根据所述关联结果确定所述网络节点的预设链接与验证文件存在关联关系时，生成相应的加密证书；

将该加密证书发送至网络节点加密装置。

一种非易失性计算机可读存储介质，其中所述存储介质中存储有计算机可读指令，所述计算机可读指令可以由处理器执行以：

接收节点加密请求，并根据所述节点加密请求获取网络节点的节点资料信

息，其中所述节点资料信息包括预设链接；

使用所述节点资料信息，向可信第三方提出加密证书申请；

接收可信第三方的证书验证请求，所述证书验证请求中包括用于进行所述预设链接的权限验证的验证文件；其中所述证书验证请求由所述可信第三方根据所述加密证书申请生成；

根据所述证书验证请求，将所述网络节点的预设链接与所述证书验证请求对应的验证文件关联，以将关联结果返回至所述可信第三方；以及

接收加密证书，并在所述网络节点上对所述加密证书进行部署；其中所述加密证书由所述可信第三方根据所述关联结果生成。

附图简要说明

图 1 为本申请的网络节点加密方法的实施例的流程图；

图 2 为本申请的网络节点加密方法的实施例的流程图；

图 3 为本申请的网络节点加密方法的实施例的步骤 S203 的流程图；

图 4 为本申请的网络节点加密方法的实施例的步骤 S204 的流程图；

图 5 为本申请的网络节点加密方法的实施例的步骤 S206 的流程图；

图 6 为本申请的网络节点加密装置的实施例的结构示意图；

图 7 为本申请的网络节点加密装置的实施例的结构示意图；

图 8 为本申请的网络节点加密装置的实施例的节点信息获取模块的结构示意图；

图 9 为本申请的网络节点加密装置的实施例的证书申请提出模块的结构示意图；

图 10 为本申请的网络节点加密装置的实施例的关联模块的结构示意图；

图 11 为本申请的网络节点加密方法及网络节点加密装置的具体实施例的实施时序图；

图 12 为本申请的网络节点加密装置所在的电子设备的工作环境结构示意

图。

实施本申请的方式

请参照附图，其中相同的组件符号代表相同的组件，本申请的原理是以实施在一适当的运算环境中来举例说明。以下的说明是基于所例示的本申请具体实施例，其不应被视为限制本申请未在此详述的其它具体实施例。

在以下的说明中，本申请的具体实施例将参考由一部或多部计算机所执行的作业的步骤及符号来说明，除非另有说明。因此，其将可了解到这些步骤及操作，其中有数次提到为由计算机执行，包括了由代表了以一结构化型式中的数据的电子信号的计算机处理单元所操纵。此操纵转换该数据或将其维持在该计算机的内存系统中的位置处，其可重新配置或另外以本领域技术人员所熟知的方式来改变该计算机的运作。该数据所维持的数据结构为该内存的实体位置，其具有由该数据格式所定义的特定特性。但是，本申请原理以上述文字来说明，其并不代表为一种限制，本领域技术人员将可了解到以下所述的多种步骤及操作亦可实施在硬件当中。

在一些实例中，对 CDN 网络节点进行加密操作的过程包括:

一、首先网络内容提供者向可信第三方提供网络节点的基本资料，如网络节点名称、网络域名信息以及证书请求文件（CSR，Certificate Secure Request）等，以向该可信第三方申请证书。

二、可信第三方审核网络内容提供者的基本资料后，对该网络节点的网络域名信息进行验证，以确认网络内容提供者对该网络节点的所有权。

三、可信第三方对网络节点的网络域名信息验证完毕后，会将证书下载地址发送至网络内容提供者，以便网络内容提供者下载加密证书。

四、网络内容提供者将加密证书上传至 CDN 网络节点的控制台，使用该加密证书对 CDN 网络节点的控制台进行证书部署，控制台会对验证加密证书中公钥和私钥的匹配性，从而完成加密证书的部署。

在上述加密操作过程中，网络内容提供者需要对加密证书进行下载以及上传，在用户保管以及上传加密证书的过程中，极易发生加密证书泄露的风险，从而影响 CDN 网络节点的安全性。

本申请的网络节点加密方法及网络节点加密装置可用于各种进行网络节点管理的电子设备，如 CDN 节点服务器等。用户可使用上述电子设备自动完成向可信第三方申请加密证书，并使用加密证书对 CDN 节点进行加密操作的过程，从而避免了加密证书的泄露，提高了网络节点的安全性。

请参照图 1，图 1 为本申请的网络节点加密方法的实施例的流程图。本实施例的网络节点加密方法可使用上述的电子设备进行实施，本实施例的网络节点加密方法包括:

步骤 S101，接收节点加密请求，并根据节点加密请求获取网络节点的节点资料信息，其中节点资料信息包括预设链接;

步骤 S102，使用节点资料信息，向可信第三方提出加密证书申请;

步骤 S103，接收可信第三方的证书验证请求，证书验证请求中包括用于进行预设链接的权限验证的验证文件；其中证书验证请求由可信第三方根据加密证书申请生成;

步骤 S104，根据证书验证请求，将网络节点的预设链接与证书验证请求对应的验证文件关联，以将关联结果返回至可信第三方;

步骤 S105，接收加密证书，并在网络节点上对加密证书进行部署；其中加密证书由可信第三方根据关联结果生成。

下面详细说明本实施例的网络节点加密方法的各步骤的具体流程。

在步骤 S101 中，网络节点加密装置接收客户端的节点加密请求，该节点加密请求为客户端的用户请求向可信第三方对相应的网络节点申请加密证书，以对该网络节点进行加密操作的请求。

随后网络节点加密装置根据该节点加密请求，从预设数据库中获取该网络节点的节点资料信息。这里的预设数据库用于预存网络节点的节点资料信息;

节点资料信息包括但不限于网络节点的节点名称、网络域名信息、预设链接以及证书请求文件信息等；其中网络节点的预设链接是指网络节点加密装置中的与终端网络节点域名关联的链接。该预设链接可为一网络地址或网络存储空间等。可信第三方可根据该节点资料信息对该网络节点进行验证。随后转到步骤S102。

在步骤S102中，网络节点加密装置根据步骤S101获取的节点资料信息，向可信第三方提出加密证书申请。其中，所述节点资料信息包括所述预设链接。

这里的加密证书申请是指网络节点加密装置向可信第三方申请加密证书的请求。这里的可信第三方为PKI（Public Key Infrastructure，公钥基础设施）系统的通信双方均信任的实体。随后转到步骤S103。

在步骤S103中，可信第三方接收网络节点加密装置发送的加密证书申请，并根据该加密证书申请生成证书验证请求。该证书验证请求是指可信第三方对网络节点加密装置的申请加密证书的权限进行验证的请求。该证书验证请求应包括一验证文件，可信第三方通过相关链接下载该验证文件来确定网络节点加密装置对该相关链接的控制权。可信第三方将证书验证请求发送至网络节点加密装置。随后转到步骤S104。

在步骤S104中，网络节点加密装置接收该证书验证请求，并根据该证书验证请求将网络节点的预设链接与证书验证请求对应的验证文件关联，随后将关联结果返回至可信第三方，以便可信第三方进行网络节点加密装置的网络节点的权限验证。网络节点加密装置将网络节点的预设链接与证书验证请求对应的验证文件关联，即，网络节点加密装置将验证文件上传至所述网络节点的预设链接所对应的网络地址或网络存储空间处。关联结果表示验证文件已上传至所述网络节点的预设链接所对应的网络地址或网络存储空间。随后转到步骤S105。

在步骤S105中，可信第三方接收网络节点加密装置的关联结果，并根据该关联结果对网络节点的预设链接与验证文件的关联关系进行确认。即，可信第三方在收到网络节点加密装置返回的表示验证文件已上传至所述网络节点的预

设链接所对应的网络地址或网络存储空间的关联结果之后，对在步骤 S103 收到的加密证书申请中的网络节点的预设链接所对应的网络地址或网络存储空间进行访问，确认是否可以在该网络地址或网络存储空间下载所述验证文件。如网络节点的预设链接与验证文件确定存在关联关系，即，可信第三方可以在所述网络地址或存储空间访问并下载所述验证文件，则生成相应的加密证书，并将该加密证书发送至网络节点加密装置。

网络节点加密装置接收该加密证书，随后在网络节点上对加密证书进行部署，即完成了网络节点的加密操作。

这样即完成了本实施例的网络节点加密方法的网络节点的加密操作过程。

本实施例的网络节点加密方法使用网络节点的节点资料信息自动向可信第三方申请加密证书，且使用该加密证书对网络节点进行加密操作，避免了加密证书的泄露，提高了网络节点的安全性。

请参照图 2，图 2 为本申请的网络节点加密方法的实施例的流程图。本实施例的网络节点加密方法可使用上述的电子设备进行实施，本实施例的网络节点加密方法包括:

步骤 S201，接收网络节点的注册信息，并对网络节点的注册信息进行安全验证;

步骤 S202，根据安全验证后的网络节点的注册信息，生成并存储相应的节点资料信息;

步骤 S203，接收节点加密请求，并根据节点加密请求获取网络节点的节点资料信息，其中节点资料信息包括预设链接;

步骤 S204，使用节点资料信息，向可信第三方提出加密证书申请;

步骤 S205，接收可信第三方的证书验证请求，证书验证请求中包括用于进行预设链接的权限验证的验证文件；其中证书验证请求由可信第三方根据加密证书申请生成;

步骤 S206，根据证书验证请求，将网络节点的预设链接与证书验证请求对应的验证文件关联，以将关联结果返回至可信第三方；其中证书验证请求由可信第三方根据加密证书申请生成；

步骤 S207，接收加密证书，并在网络节点上对加密证书进行部署；其中加密证书由可信第三方根据关联结果生成；

步骤 S208，加密证书部署完毕后，生成加密证书部署反馈，并将加密证书部署反馈发送至相应的客户端。

下面详细说明本实施例的网络节点加密装置的各步骤的具体流程。

本实施例中的网络节点例如为 CDN 网络节点，内容提供者一般会在终端网络节点上制作内容，但是终端网络节点由于流量以及地域的限制，不利于内容的快速传播。因此内容提供者通常会注册一 CDN 网络节点，将该 CDN 网络节点与终端网络节点关联，这样可通过基本无流量和地域限制的 CDN 网络节点进行内容的快速传播。

在步骤 S201 中，网络节点加密装置接收相应客户端的网络节点的注册信息。这里的网络节点例如为 CDN 网络节点，这样即实现了终端网络节点与 CDN 网络节点的关联，当然这里也可直接提交终端网络节点的节点资料信息作为网络节点的注册信息。

随后网络节点加密装置对上述网络节点的注册信息进行安全验证，以保证该网络节点的注册信息的真实性。随后转到步骤 S202。

在步骤 S202 中，网络节点加密装置根据步骤 S201 中进行安全验证后的网络节点注册信息生成并存储该网络节点对应的节点资料信息。节点资料信息包括但不限于网络节点的节点名称、网络域名信息、预设链接以及证书请求文件信息等。其中网络节点的预设链接是指网络节点加密装置中的与终端网络节点域名关联的链接。这样网络节点加密装置可存储多个网络节点的节点资料信息，以形成预设数据库。随后转到步骤 S203。

在步骤 S203 中，网络节点加密装置接收客户端的节点加密请求，该节点加

密请求为客户端的用户请求向可信第三方对相应的网络节点申请加密证书，以对该网络节点进行加密操作的请求。

随后网络节点加密装置根据该节点加密请求，从预设数据库中获取该网络节点的节点资料信息。具体请参照图 3，图 3 为本申请的网络节点加密方法的步骤 S203 的流程图。该步骤 S203 包括:

步骤 S2031，网络节点加密装置接收节点加密请求，并根据节点加密请求，检测网络节点的预设链接是否与终端网络节点域名关联，即判断预设数据库中的节点资料信息是否有效；如通过网络节点的预设链接是否可以访问到终端网络节点域名上的相关内容。该预设链接可为一网络地址或网络存储空间等。

如网络节点的预设链接与终端网络节点域名关联，则转到步骤 S2032；如网络节点的预设链接未与终端网络节点域名关联，则转到步骤 S2033。

步骤 S2032，网络节点的预设链接与终端网络节点域名关联，网络节点加密装置判断预设数据库中的节点资料信息有效，并获取网络节点的其他节点资料信息。可信第三方可根据该节点资料信息对该网络节点进行验证。随后转到步骤 S204。

步骤 S2033，网络节点的预设链接未与终端网络节点域名关联，网络节点加密装置判断预设数据库中的该节点资料信息失效，向相应的客户端发出域名关联提示，以提示用户将终端网络节点域名与网络节点的预设链接进行关联，以便进行加密证书的自动申请操作。

在步骤 S204 中，网络节点加密装置根据步骤 S203 获取的节点资料信息，向可信第三方提出加密证书申请。其中，所述节点资料信息包括所述预设链接。这里的加密证书申请是指网络节点加密装置向可信第三方申请加密证书的请求。这里的可信第三方为 PKI（Public Key Infrastructure，公钥基础设施）系统的通信双方均信任的实体。具体请参照图 4，图 4 为本申请的网络节点加密方法的步骤 S204 的流程图。该步骤 S204 包括:

步骤 S2041，网络节点加密装置使用步骤 S203 获取的节点资料信息，在可

信第三方进行用户注册，以获取注册用户信息。

由于可信第三方只给注册用户提供加密证书申请服务，因此在本步骤中，网络节点加密装置使用节点资料信息，在可信第三方进行用户注册，由于节点资料信息已经经过安全验证以及有效性验证，因此在可信第三方进行用户注册的成功率很高。

步骤 S2042，网络节点加密装置根据步骤 S2041 获取的注册用户信息以及节点资料信息，将网络节点的证书请求文件提供给可信第三方，以向可信第三方提出加密证书申请。随后转到步骤 S205。

在步骤 S205 中，可信第三方接收网络节点加密装置发送的加密证书申请，并根据该加密证书申请生成证书验证请求。该证书验证请求是指可信第三方对网络节点加密装置的申请加密证书的权限进行验证的请求。该证书验证请求应包括一验证文件，可信第三方通过相关链接下载该验证文件来确定网络节点加密装置对该相关链接的控制权。可信第三方将证书验证请求发送至网络节点加密装置。随后转到步骤 S206。

在步骤 S206 中，网络节点加密装置接收该证书验证请求，并根据该证书验证请求将网络节点的预设链接与证书验证请求对应的验证文件关联。具体请参照图 5，图 5 为本申请的网络节点加密方法的步骤 S206 的流程图。该步骤 S206 包括:

步骤 S2061，网络节点加密装置从可信第三方上接收证书验证请求对应的验证文件;

步骤 S2062，网络节点加密装置将验证文件上传至预设链接对应的存储空间，以实现网络节点的预设链接与验证文件的关联。

随后将关联结果返回至可信第三方，以便可信第三方进行网络节点加密装置的网络节点的权限验证。关联结果表示验证文件已上传至所述网络节点的预设链接所对应的网络地址或网络存储空间。随后转到步骤 S207。

在步骤 S207 中，可信第三方接收网络节点加密装置的关联结果，并根据该

关联结果对网络节点的预设链接与验证文件的关联关系进行确认。即，可信第三方在收到网络节点加密装置返回的表示验证文件已上传至所述网络节点的预设链接所对应的网络地址或网络存储空间的关联结果之后，对在步骤S205收到的网络节点的预设链接所对应的网络地址或网络存储空间进行访问，确认是否可以在该网络地址或网络存储空间下载所述验证文件。如网络节点的预设链接与验证文件确定存在关联关系，即，可信第三方可以在所述网络地址或存储空间访问并下载所述验证文件，则生成相应的加密证书，并将该加密证书发送至网络节点加密装置。

网络节点加密装置接收该加密证书，随后在网络节点上对加密证书进行部署。随后转到步骤S208。

在步骤S208中，加密证书部署完毕后，网络节点加密装置生成加密证书部署反馈，并将加密证书部署反馈发送至相应的客户端，以提示用户该网络节点的加密操作已经完成。

这样即完成了本实施例的网络节点加密方法的网络节点的加密操作过程。

在上述实施例的基础上，本实施例的网络节点加密方法对节点资料信息进行安全验证以及有效性验证，降低了可信第三方验证失败的概率，进一步提高了网络节点加密操作的成功率。

本申请还提供一种网络节点加密装置，请参照图6，图6为本申请的网络节点加密装置的实施例的结构示意图，本实施例的网络节点加密装置可使用上述的网络节点加密方法的实施例进行实施，本实施例的网络节点加密装置60包括节点信息获取模块61、证书申请提出模块62、请求接收模块63、关联模块64以及证书部署模块65。

节点信息获取模块61用于接收节点加密请求，并根据节点加密请求获取网络节点的节点资料信息，其中所述节点资料信息包括预设链接；证书申请提出模块62用于使用节点资料信息，向可信第三方提出加密证书申请；请求接收模

块 63 用于接收可信第三方的证书验证请求，证书验证请求包括用于进行预设链接的权限验证的验证文件；其中证书验证请求由可信第三方根据所述加密证书申请生成；关联模块 64 用于根据证书验证请求，将网络节点的预设链接与证书验证请求对应的验证文件关联，以将关联结果返回至可信第三方；证书部署模块 65 用于接收加密证书，并在网络节点上对加密证书进行部署；其中加密证书由可信第三方根据关联结果生成。

本实施例的网络节点加密装置 60 使用时，首先节点信息获取模块 61 接收客户端的节点加密请求，该节点加密请求为客户端的用户请求向可信第三方对相应的网络节点申请加密证书，以对该网络节点进行加密操作的请求。

随后节点信息获取模块 61 根据该节点加密请求，从预设数据库中获取该网络节点的节点资料信息。这里的预设数据库用于预存网络节点的节点资料信息；节点资料信息包括但不限于网络节点的节点名称、网络域名信息、预设链接以及证书请求文件信息等；其中网络节点的预设链接是指网络节点加密装置中的与终端网络节点域名关联的链接。该预设链接可为一网络地址或网络存储空间等。可信第三方可根据该节点资料信息对该网络节点进行验证。

随后证书申请提出模块 62 根据节点信息获取模块 61 获取的节点资料信息，向可信第三方提出加密证书申请。其中，所述节点资料信息包括所述预设链接。这里的加密证书申请是指网络节点加密装置向可信第三方申请加密证书的请求。这里的可信第三方为 PKI（Public Key Infrastructure，公钥基础设施）系统的通信双方均信任的实体。

然后可信第三方接收证书申请提出模块 62 发送的加密证书申请，并根据该加密证书申请生成证书验证请求。该证书验证请求是指可信第三方对网络节点加密装置的申请加密证书的权限进行验证的请求。该证书验证请求应包括一验证文件，可信第三方通过相关链接下载该验证文件来确定网络节点加密装置对该相关链接的控制权。

可信第三方将证书验证请求发送至请求接收模块 63；请求接收模块 63 接收

该证书验证请求，随后关联模块 64 根据该证书验证请求将网络节点的预设链接与证书验证请求对应的验证文件关联，随后将关联结果返回至可信第三方，以便可信第三方进行网络节点加密装置的网络节点的权限验证。关联模块 64 将网络节点的预设链接与证书验证请求对应的验证文件关联，即，关联模块 64 将验证文件上传至所述网络节点的预设链接所对应的网络地址或网络存储空间处。关联结果表示验证文件已上传至所述网络节点的预设链接所对应的网络地址或网络存储空间。

随后可信第三方接收关联模块 63 的关联结果，并根据该关联结果对网络节点的预设链接与验证文件的关联关系进行确认。即，可信第三方在收到关联模块 63 的表示验证文件已上传至所述网络节点的预设链接所对应的网络地址或网络存储空间的关联结果之后，对收到的加密证书申请中的网络节点的预设链接所对应的网络地址或网络存储空间进行访问，确认是否可以在该网络地址或网络存储空间下载所述验证文件。如网络节点的预设链接与验证文件确定存在关联关系，即，可信第三方可以在所述网络地址或存储空间访问并下载所述验证文件，则生成相应的加密证书，并将该加密证书发送至证书部署模块 65。

最后证书部署模块 65 接收该加密证书，随后在网络节点上对加密证书进行部署，即完成了网络节点的加密操作。

这样即完成了本实施例的网络节点加密装置 60 的网络节点的加密操作过程。

本实施例的网络节点加密装置使用网络节点的节点资料信息自动向可信第三方申请加密证书，且使用该加密证书对网络节点进行加密操作，避免了加密证书的泄露，提高了网络节点的安全性。

请参照图 7，图 7 为本申请的网络节点加密装置的实施例的结构示意图，本实施例的网络节点加密装置可使用上述的网络节点加密方法的实施例进行实施。本实施例的网络节点加密装置 70 包括安全验证模块 71、节点信息存储模块

72、节点信息获取模块 73、证书申请提出模块 74、请求接收模块 75、关联模块 76、证书部署模块 77 以及反馈模块 78。

安全验证模块 71 用于接收网络节点的注册信息，并对网络节点的注册信息进行安全验证。节点信息存储模块 72 用于根据安全验证后的网络节点的注册信息，生成并存储相应的节点资料信息。节点信息获取模块 73 用于接收节点加密请求，并根据节点加密请求获取网络节点的节点资料信息。证书申请提出模块 74 用于使用节点资料信息，向可信第三方提出加密证书申请。请求接收模块 75 用于接收可信第三方的证书验证请求，证书验证请求中包括用于进行预设链接的权限验证的验证文件；其中证书验证请求由所述可信第三方根据加密证书申请生成。关联模块 76 用于根据证书验证请求，将网络节点的预设链接与证书验证请求对应的验证文件关联，以将关联结果返回至所述可信第三方。证书部署模块 77 用于接收加密证书，并在网络节点上对加密证书进行部署；其中加密证书由可信第三方根据所述关联结果生成。反馈模块 78 用于生成加密证书部署反馈，并将加密证书部署反馈发送至相应的客户端。

请参照图 8，图 8 为本申请的网络节点加密装置的实施例的节点信息获取模块的结构示意图。该节点信息获取模块 73 包括域名关联检测单元 81、节点信息获取单元 82 以及域名关联提示单元 83。

域名关联检测单元 81 用于接收节点加密请求，并根据节点加密请求，检测网络节点的预设链接是否与终端网络节点域名关联。节点信息获取单元 82 用于如网络节点的预设链接与终端网络节点域名关联，则获取网络节点的其他节点资料信息。域名关联提示单元 83 用于如网络节点的预设链接与终端网络节点域名关联，则发出域名关联提示。

请参照图 9，图 9 为本申请的网络节点加密装置的实施例的证书申请提出模块的结构示意图。该证书申请提出模块 74 包括注册单元 91 以及证书申请提出单元 92。

注册单元 91 用于使用节点资料信息，在可信第三方进行用户注册，以获取

注册用户信息。证书申请提出单元92用于根据注册用户信息以及节点资料信息，将网络节点的证书请求文件提供给可信第三方，以向可信第三方提出加密证书申请。

请参照图10，图10为本申请的网络节点加密装置的实施例的关联模块的结构示意图。该关联模块76包括验证文件接收单元101以及关联单元102。

验证文件接收单元101用于接收证书验证请求对应的验证文件。关联单元102用于将验证文件上传至预设链接对应的存储空间，以实现网络节点的预设链接与验证文件的关联。

本实施例的网络节点加密装置70使用时，安全验证模块71接收相应客户端的网络节点的注册信息。这里的网络节点例如为CDN网络节点，这样即实现了终端网络节点与CDN网络节点的关联，当然这里也可直接提交终端网络节点的节点资料信息作为网络节点的注册信息。

随后安全验证模块71对上述网络节点的注册信息进行安全验证，以保证该网络节点的注册信息的真实性。

随后节点信息存储模块72根据安全验证模块71中进行安全验证后的网络节点注册信息，生成并存储该网路节点对应的节点资料信息。节点资料信息包括但不限于网络节点的节点名称、网络域名信息、预设链接以及证书请求文件信息等。其中网络节点的预设链接是指网络节点加密装置中的与终端网络节点域名关联的链接。这样网络节点加密装置可存储多个网络节点的节点资料信息，以形成预设数据库。

然后节点信息获取模块73接收客户端的节点加密请求，该节点加密请求为客户端的用户请求向可信第三方对相应的网络节点申请加密证书，以对该网络节点进行加密操作的请求。

随后节点信息获取模块73根据该节点加密请求，从预设数据库中获取该网络节点的节点资料信息。具体为：

节点信息获取模块73的域名关联检测单元81接收节点加密请求，并根据

节点加密请求，检测网络节点的预设链接是否与终端网络节点域名关联，即判断预设数据库中的节点资料信息是否有效。该预设链接可为一网络地址或网络存储空间等。

如网络节点的预设链接与终端网络节点域名关联，域名关联检测单元 81 判断预设数据库中的节点资料信息有效，节点信息获取单元 82 获取网络节点的其他节点资料信息，可信第三方可根据该节点资料信息对该网络节点进行验证。

如网络节点的预设链接未与终端网络节点域名关联，域名关联检测单元 81 判断预设数据库中的该节点资料信息失效，域名关联提示单元 83 向相应的客户端发出域名关联提示，以提示用户将终端网络节点域名与网络节点的预设链接进行关联，以便进行加密证书的自动申请操作。

然后证书申请提出模块 74 根据节点信息获取模块 73 获取的节点资料信息，向可信第三方提出加密证书申请。这里的加密证书申请是指网络节点加密装置向可信第三方申请加密证书的请求。这里的可信第三方为 PKI（Public Key Infrastructure，公钥基础设施）系统的通信双方均信任的实体。具体为：

证书申请提出模块 74 的注册单元 91 使用节点信息获取模块获取的节点资料信息，在可信第三方进行用户注册，以获取注册用户信息。

由于可信第三方只给注册用户提供加密证书申请服务，因此在本步骤中，证书申请提出模块使用节点资料信息，在可信第三方进行用户注册，由于节点资料信息已经经过安全验证以及有效性验证，因此该用户注册成功率很高。

证书申请提出模块 74 的证书申请提出单元 92 根据注册单元获取的注册用户信息以及节点资料信息，将网络节点的证书请求文件提供给可信第三方，以向可信第三方提出加密证书申请。其中，所述节点资料信息包括所述预设链接。

随后可信第三方接收证书申请提出模块 74 发送的加密证书申请，并根据该加密证书申请生成证书验证请求。该证书验证请求是指可信第三方对网络节点加密装置的申请加密证书的权限进行验证的请求。该证书验证请求应包括一验证文件，可信第三方通过相关链接下载该验证文件来确定网络节点加密装置对

该相关链接的控制权。

可信第三方将证书验证请求发送至请求接收模块 75; 请求接收模块 75 接收该证书验证请求，随后关联模块 76 根据该证书验证请求将网络节点的预设链接与证书验证请求对应的验证文件关联。具体为:

关联模块 76 的验证文件接收单元 101 从可信第三方上接收证书验证请求对应的验证文件;

关联模块 76 的关联单元 102 将验证文件上传至预设链接对应的存储空间，以实现网络节点的预设链接与验证文件的关联。

随后关联模块 76 将关联结果返回至可信第三方，以便可信第三方进行网络节点加密装置的网络节点的权限验证。关联结果表示验证文件已上传至所述网络节点的预设链接所对应的网络地址或网络存储空间。

然后可信第三方接收关联模块 76 的关联结果，并根据该关联结果对网络节点的预设链接与验证文件的关联关系进行确认。即，可信第三方在收到网络节点加密装置返回的表示验证文件已上传至所述网络节点的预设链接所对应的网络地址或网络存储空间的关联结果之后，对收到的网络节点的预设链接所对应的网络地址或网络存储空间进行访问，确认是否可以在该网络地址或网络存储空间下载所述验证文件。如网络节点的预设链接与验证文件确定存在关联关系，即，可信第三方可以在所述网络地址或存储空间访问并下载所述验证文件，则生成相应的加密证书，并将该加密证书发送至证书部署模块 77。

证书部署模块 77 接收该加密证书,随后在网络节点上对加密证书进行部署。

最后加密证书部署完毕后，反馈模块 78 生成加密证书部署反馈，并将加密证书部署反馈发送至相应的客户端，以提示用户该网络节点的加密操作已经完成。

这样即完成了本实施例的网络节点加密装置 70 的网络节点的加密操作过程。

在前述实施例的基础上，本实施例的网络节点加密装置对节点资料信息进

行安全验证以及有效性验证，降低了可信第三方验证失败的概率，进一步提高了网络节点加密操作的成功率。

下面通过一具体实施例说明本申请的网络节点加密方法及网络节点加密装置的具体工作原理。请参照图 11，图 11 为本申请的网络节点加密方法及网络节点加密装置的具体实施例的实施时序图。其中用户通过客户终端在 CDN 节点服务器上申请 CDN 网络节点，并通过该 CDN 节点服务器向可信第三方申请 CDN 网络节点加密。该 CND 网络节点的加密过程包括:

步骤 S1101，用户通过客户终端向 CDN 节点服务器注册 CDN 网络节点，即客户终端将该 CDN 网络节点的注册信息发送至 CDN 节点服务器。

步骤 S1102，CDN 节点服务器对该 CDN 网络节点的注册信息进行安全验证，随后将安全验证后的注册信息存储为该 CDN 网络节点的节点资料信息。这样 CDN 节点服务器可以形成包括多个 CDN 网络节点的节点资料信息的预设数据库。

步骤 S1103，用户通过客户终端向 CDN 网络服务器发送节点加密请求，以对 CDN 网络节点对应的网络内容进行加密操作。

步骤 S1104，CDN 网络服务器对该节点加密请求对应的 CDN 网络节点的节点资料信息进行有效性检测。

步骤 S1105，如该 CDN 网络节点的节点资料信息有效，则 CDN 节点服务器使用上述 CDN 网络节点的节点资料信息向可信第三方提出加密证书申请。

步骤 S1106，可信第三方根据上述加密证书申请，将证书验证请求发送至 CDN 网络服务器，以验证申请者身份与域名是否有效。该证书验证请求包括一验证文件。

步骤 S1107，CDN 节点服务器将证书验证请求对应的验证文件与 CDN 网络节点的预设链接进行关联。即，CDN 节点服务器将验证文件上传至所述 CDN 网络节点的预设链接所对应的网络地址或网络存储空间处。

步骤 S1108，CDN 节点服务器将关联结果返回给可信第三方。关联结果表示验证文件已上传至所述CDN网络节点的预设链接所对应的网络地址或网络存储空间。

步骤 S1109，可信第三方接收到关联结果后，通过 CDN 网络节点的预设链接对验证文件进行下载，从而确定 CDN 节点服务器对该 CDN 网络节点的控制权限，即确认了申请者身份与域名有效。随后可信第三方将相应的加密证书发送至 CDN 节点服务器。

步骤 S1110，CDN 节点服务器使用上述加密证书对 CDN 网络节点进行加密操作。

步骤 S1111，CDN 节点服务器对 CDN 网络节点加密操作完毕后，将相应的加密证书部署反馈发送至客户终端，以提示用户该 CDN 网络节点的加密操作已经完成。

这样即完成了本具体实施例的网络节点加密方法及网络节点加密装置的网络节点加密过程。

本申请的网络节点加密方法及网络节点加密装置可使用网络节点的节点资料信息自动向可信第三方申请加密证书，且使用该加密证书对网络节点进行加密操作，避免了加密证书的泄露，提高了网络节点的安全性。

如本申请所使用的术语“组件”、“模块”、“系统”、“接口”、“进程”等等一般地旨在指计算机相关实体：硬件、硬件和软件的组合、软件或执行中的软件。例如，组件可以是但不限于是运行在处理器上的进程、处理器、对象、可执行应用、执行的线程、程序和／或计算机。通过图示，运行在控制器上的应用和该控制器二者都可以是组件。一个或多个组件可以有在于执行的进程和／或线程内，并且组件可以位于一个计算机上和／或分布在两个或更多计算机之间。

图 12 和随后的讨论提供了对实现本申请所述的网络节点加密装置所在的电子设备的工作环境的简短、概括的描述。图 12 的工作环境仅仅是适当的工作环

境的一个实例并且不旨在建议关于工作环境的用途或功能的范围的任何限制。实例电子设备 1212 包括但不限于可穿戴设备、头戴设备、医疗健康平台、个人计算机、服务器计算机、手持式或膝上型设备、移动设备(比如移动电话、个人数字助理(PDA)、媒体播放器等等）、多处理器系统、消费型电子设备、小型计算机、大型计算机、包括上述任意系统或设备的分布式计算环境，等等。

尽管没有要求，但是在“计算机可读指令”被一个或多个电子设备执行的通用背景下描述实施例。计算机可读指令可以经由计算机可读介质来分布（下文讨论）。计算机可读指令可以实现为程序模块，比如执行特定任务或实现特定抽象数据类型的功能、对象、应用编程接口(API)、数据结构等等。典型地，该计算机可读指令的功能可以在各种环境中随意组合或分布。

图 12 图示了包括本申请的网络节点加密装置的一个或多个实施例的电子设备 1212 的实例。在一种配置中，电子设备 1212 包括至少一个处理单元 1216 和存储器 1218。根据电子设备的确切配置和类型，存储器 1218 可以是易失性的(比如 RAM)、非易失性的（比如 ROM、闪存等）或二者的某种组合。该配置在图 12 中由虚线 1214 图示。

在其他实施例中，电子设备 1212 可以包括附加特征和／或功能。例如，设备 1212 还可以包括附加的存储装置（例如可移除和／或不可移除的），其包括但不限于磁存储装置、光存储装置等等。这种附加存储装置在图 12 中由存储装置 1220 图示。在一个实施例中，用于实现本文所提供的一个或多个实施例的计算机可读指令可以在存储装置 1220 中。存储装置 1220 还可以存储用于实现操作系统、应用程序等的其他计算机可读指令。计算机可读指令可以载入存储器 1218 中由例如处理单元 1216 执行。

本文所使用的术语“计算机可读介质”包括计算机存储介质。计算机存储介质包括以用于存储诸如计算机可读指令或其他数据之类的信息的任何方法或技术实现的易失性和非易失性、可移除和不可移除介质。存储器 1218 和存储装置 1220 是计算机存储介质的实例。计算机存储介质包括但不限于 RAM、ROM、

EEPROM、闪存或其他存储器技术、CD-ROM、数字通用盘(DVD)或其他光存储装置、盒式磁带、磁带、磁盘存储装置或其他磁存储设备、或可以用于存储期望信息并可以被电子设备 1212 访问的任何其他介质。任意这样的计算机存储介质可以是电子设备 1212 的一部分。

电子设备 1212 还可以包括允许电子设备 1212 与其他设备通信的通信连接 1226。通信连接 1226 可以包括但不限于调制解调器、网络接口卡(NIC)、集成网络接口、射频发射器／接收器、红外端口、USB 连接或用于将电子设备 1212 连接到其他电子设备的其他接口。通信连接 1226 可以包括有线连接或无线连接。通信连接 1226 可以发射和／或接收通信媒体。

术语“计算机可读介质”可以包括通信介质。通信介质典型地包含计算机可读指令或诸如载波或其他传输机构之类的“已调制数据信号”中的其他数据，并且包括任何信息递送介质。术语“已调制数据信号”可以包括这样的信号：该信号特性中的一个或多个按照将信息编码到信号中的方式来设置或改变。

电子设备 1212 可以包括输入设备 1224，比如键盘、鼠标、笔、语音输入设备、触摸输入设备、红外相机、视频输入设备和／或任何其他输入设备。设备 1212 中也可以包括输出设备 1222，比如一个或多个显示器、扬声器、打印机和／或任意其他输出设备。输入设备 1224 和输出设备 1222 可以经由有线连接、无线连接或其任意组合连接到电子设备 1212。在一个实施例中，来自另一个电子设备的输入设备或输出设备可以被用作电子设备 1212 的输入设备 1224 或输出设备 1222。

电子设备 1212 的组件可以通过各种互连（比如总线）连接。这样的互连可以包括外围组件互连(PCI)(比如快速 PCI)、通用串行总线(USB)、火线(IEEE 1394)、光学总线结构等等。在另一个实施例中，电子设备 1212 的组件可以通过网络互连。例如，存储器 1218 可以由位于不同物理位置中的、通过网络互连的多个物理存储器单元构成。

本领域技术人员将认识到，用于存储计算机可读指令的存储设备可以跨越

网络分布。例如，可经由网络 1228 访问的电子设备 1230 可以存储用于实现本申请所提供的一个或多个实施例的计算机可读指令。电子设备 1212 可以访问电子设备 1230 并且下载计算机可读指令的一部分或所有以供执行。可替代地，电子设备 1212 可以按需要下载多条计算机可读指令，或者一些指令可以在电子设备 1212 处执行并且一些指令可以在电子设备 1230 处执行。

本文提供了实施例的各种操作。在一个实施例中，所述的一个或多个操作可以构成一个或多个计算机可读介质上存储的计算机可读指令，其在被电子设备执行时将使得计算设备执行所述操作。描述一些或所有操作的顺序不应当被解释为暗示这些操作必需是顺序相关的。本领域技术人员将理解具有本说明书的益处的可替代的排序。而且，应当理解，不是所有操作必需在本文所提供的每个实施例中存在。

而且，尽管已经相对于一个或多个实现方式示出并描述了本公开，但是本领域技术人员基于对本说明书和附图的阅读和理解将会想到等价变型和修改。本公开包括所有这样的修改和变型，并且仅由所附权利要求的范围限制。特别地关于由上述组件（例如元件、资源等）执行的各种功能，用于描述这样的组件的术语旨在对应于执行所述组件的指定功能（例如其在功能上是等价的）的任意组件（除非另外指示），即使在结构上与执行本文所示的本公开的示范性实现方式中的功能的公开结构不等同。此外，尽管本公开的特定特征已经相对于若干实现方式中的仅一个被公开，但是这种特征可以与如可以对给定或特定应用而言是期望和有利的其他实现方式的一个或多个其他特征组合。而且，就术语“包括”、“具有”、“含有”或其变形被用在具体实施方式或权利要求中而言，这样的术语旨在以与术语“包含”相似的方式包括。

本申请实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用

时，也可以存储在一个计算机可读取存储介质中。上述提到的存储介质可以是只读存储器，磁盘或光盘等。上述的各装置或系统，可以执行相应方法实施例中的方法。

综上所述，虽然本申请已以实施例揭露如上，上述实施例并非用以限制本申请，本领域的普通技术人员，在不脱离本申请的精神和范围内，均可作各种更动与润饰，因此本申请的保护范围以权利要求界定的范围为准。

权利要求书

1、一种网络节点加密方法，包括:

接收节点加密请求，并根据所述节点加密请求获取网络节点的节点资料信息，其中所述节点资料信息包括预设链接;

使用所述节点资料信息，向可信第三方提出加密证书申请;

接收可信第三方的证书验证请求，所述证书验证请求中包括用于进行所述预设链接的权限验证的验证文件；其中所述证书验证请求由所述可信第三方根据所述加密证书申请生成;

根据所述证书验证请求，将所述网络节点的预设链接与所述证书验证请求对应的验证文件关联，以将关联结果返回至所述可信第三方；以及

接收加密证书，并在所述网络节点上对所述加密证书进行部署；其中所述加密证书由所述可信第三方根据所述关联结果生成。

2、根据权利要求 1 所述的网络节点加密方法，其中，所述网络节点加密方法还包括:

接收网络节点的注册信息，并对所述网络节点的注册信息进行安全验证;以及

根据安全验证后的网络节点的注册信息，生成并存储相应的节点资料信息。

3、根据权利要求 2 所述的网络节点加密方法，其中，所述接收节点加密请求，并根据所述节点加密请求获取网络节点的节点资料信息的步骤包括:

接收节点加密请求，并根据所述节点加密请求，检测所述网络节点的预设链接是否与终端网络节点域名关联;

如所述网络节点的预设链接与所述终端网络节点域名关联，则获取所述网络节点的其他节点资料信息；以及

如所述网络节点的预设链接与所述终端网络节点域名关联，则发出域名关联提示。

4、根据权利要求 1 所述的网络节点加密方法，其中，所述使用所述节点资料信息，向可信第三方提出加密证书申请的步骤包括:

使用所述节点资料信息，在所述可信第三方进行用户注册，以获取注册用户信息；以及

根据所述注册用户信息以及所述节点资料信息，将所述网络节点的证书请求文件提供给所述可信第三方，以向所述可信第三方提出加密证书申请。

5、根据权利要求 1 所述的网络节点加密方法，其中，所述将所述网络节点的预设链接与所述证书验证请求的对应的验证文件关联的步骤包括:

接收所述证书验证请求对应的验证文件；以及

将所述验证文件上传至所述预设链接对应的存储空间，以实现所述网络节点的预设链接与所述验证文件的关联。

6、根据权利要求 1 所述的网络节点加密方法，其中，所述在所述网络节点上对所述加密证书进行部署步骤的之后还包括:

生成加密证书部署反馈，并将所述加密证书部署反馈发送至相应的客户端。

7、一种网络节点加密装置，包括:

存储器和处理器，所述存储器上存储有计算机可读指令，所述处理器执行所述计算机可读指令时实现以下步骤:

接收节点加密请求，并根据所述节点加密请求获取网络节点的节点资料信息，其中所述节点资料信息包括预设链接;

使用所述节点资料信息，向可信第三方提出加密证书申请;

接收可信第三方的证书验证请求，所述证书验证请求中包括用于进行所述预设链接的权限验证的验证文件；其中所述证书验证请求由所述可信第三方根据所述加密证书申请生成;

根据所述证书验证请求，将所述网络节点的预设链接与所述证书验证请求对应的验证文件关联，以将关联结果返回至所述可信第三方；以及

接收加密证书，并在所述网络节点上对所述加密证书进行部署；其中所述

加密证书由所述可信第三方根据所述关联结果生成。

8、根据权利要求 7 所述的网络节点加密装置，其中，所述处理器执行所述计算机可读指令时还实现以下步骤:

接收网络节点的注册信息，并对所述网络节点的注册信息进行安全验证;以及

根据安全验证后的网络节点的注册信息，生成并存储相应的节点资料信息。

9、根据权利要求 8 所述的网络节点加密装置，其中，所述接收节点加密请求，并根据所述节点加密请求获取网络节点的节点资料信息的步骤包括:

接收节点加密请求，并根据所述节点加密请求，检测所述网络节点的预设链接是否与终端网络节点域名关联;

如所述网络节点的预设链接与所述终端网络节点域名关联，则获取所述网络节点的其他节点资料信息；以及

如所述网络节点的预设链接与所述终端网络节点域名关联，则发出域名关联提示。

10、根据权利要求 7 所述的网络节点加密装置，其中，所述使用所述节点资料信息，向可信第三方提出加密证书申请的步骤包括:

使用所述节点资料信息，在所述可信第三方进行用户注册，以获取注册用户信息；以及

根据所述注册用户信息以及所述节点资料信息，将所述网络节点的证书请求文件提供给所述可信第三方，以向所述可信第三方提出加密证书申请。

11、根据权利要求 7 所述的网络节点加密装置，其中，所述将所述网络节点的预设链接与所述证书验证请求的对应的验证文件关联的步骤包括:

接收所述证书验证请求对应的验证文件；以及

将所述验证文件上传至所述预设链接对应的存储空间，以实现所述网络节点的预设链接与所述验证文件的关联。

12、根据权利要求 7 所述的网络节点加密装置，其中，在所述网络节点上

对所述加密证书进行部署步骤的之后还包括:

生成加密证书部署反馈，并将所述加密证书部署反馈发送至相应的客户端。

13、一种网络节点加密方法，包括:

接收网络节点加密装置发送的加密证书申请，并根据该加密证书申请生成证书验证请求，所述加密证书申请中包括有网络节点的节点资料信息，所述节点资料信息包括预设链接，所述证书验证请求中包括用于进行所述预设链接的权限验证的验证文件;

接收网络节点加密装置根据所述证书验证请求返回的关联结果;

在根据所述关联结果确定所述网络节点的预设链接与验证文件存在关联关系时，生成相应的加密证书;

将该加密证书发送至网络节点加密装置。

14、根据权利要求 13 的网络节点加密方法，其中，所述关联结果表示验证文件已上传至所述网络节点的预设链接所对应的网络地址或网络存储空间。

15、根据权利要求 14 的网络节点加密方法，其中，根据所述关联结果确定所述网络节点的预设链接与验证文件存在关联关系包括:

对所述网络节点的预设链接所对应的网络地址或网络存储空间进行访问，

如果可以在该网络地址或网络存储空间下载所述验证文件，则确定所述网络节点的预设链接与验证文件存在关联关系。

16、一种用于可信第三方的网络节点加密装置，包括:

存储器和处理器，所述存储器上存储有计算机可读指令，所述处理器执行所述计算机可读指令时实现以下步骤:

接收网络节点加密装置发送的加密证书申请，并根据该加密证书申请生成证书验证请求，所述加密证书申请中包括有网络节点的节点资料信息，所述节点资料信息包括预设链接，所述证书验证请求中包括用于进行所述预设链接的权限验证的验证文件;

接收网络节点加密装置根据所述证书验证请求返回的关联结果;

在根据所述关联结果确定所述网络节点的预设链接与验证文件存在关联关系时，生成相应的加密证书；

将该加密证书发送至网络节点加密装置。

17、根据权利要求 16 的网络节点加密方法，其中，所述关联结果表示验证文件已上传至所述网络节点的预设链接所对应的网络地址或网络存储空间。

18、根据权利要求 17 的网络节点加密方法，其中，根据所述关联结果确定所述网络节点的预设链接与验证文件存在关联关系包括:

对所述网络节点的预设链接所对应的网络地址或网络存储空间进行访问，

如果可以在该网络地址或网络存储空间下载所述验证文件，则确定所述网络节点的预设链接与验证文件存在关联关系。

19、一种非易失性计算机可读存储介质，其中所述存储介质中存储有计算机可读指令，所述计算机可读指令可以由处理器执行以完成如权利要求 1 至 7 中任一项的方法。

20、一种非易失性计算机可读存储介质，其中所述存储介质中存储有计算机可读指令，所述计算机可读指令可以由处理器执行以完成如权利要求 13 至 15 中任一项的方法。

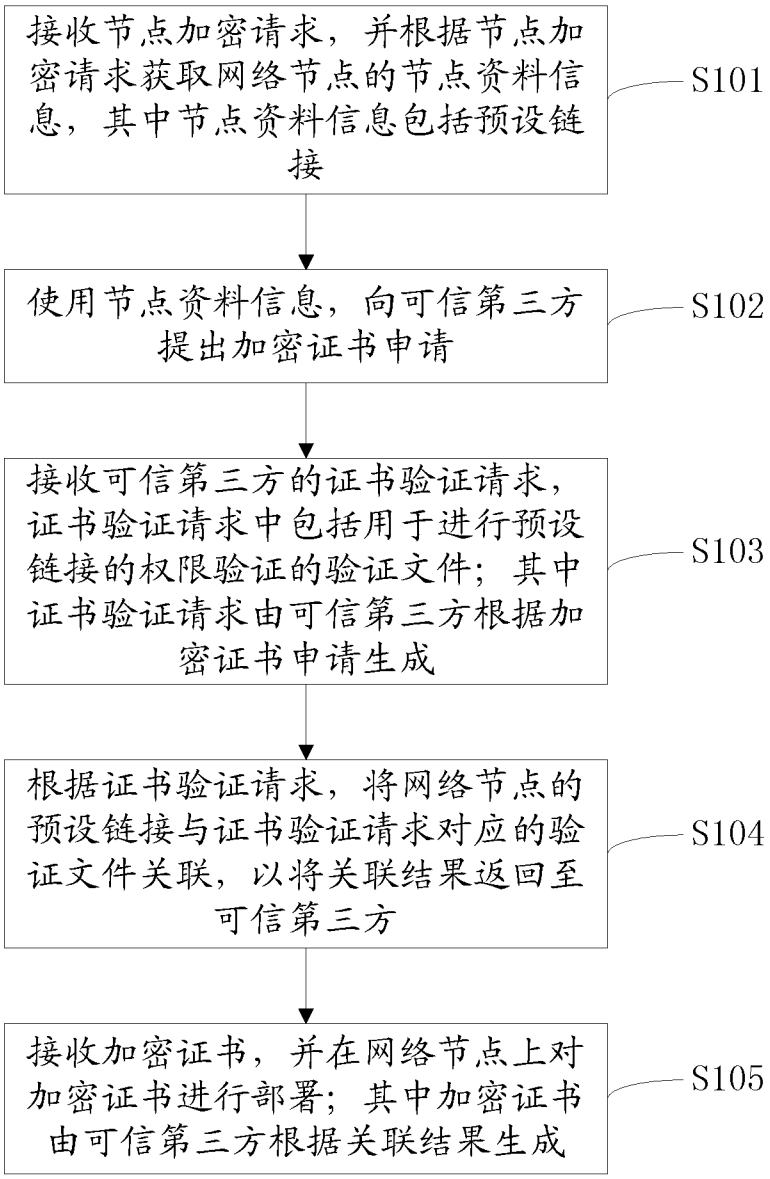
接收节点加密请求，并根据节点加密请求获取网络节点的节点资料信息，其中节点资料信息包括预设链接
S101
使用节点资料信息，向可信第三方提出加密证书申请
S102
接收可信第三方的证书验证请求，证书验证请求中包括用于进行预设链接的权限验证的验证文件；其中证书验证请求由可信第三方根据加密证书申请生成
S103
根据证书验证请求，将网络节点的预设链接与证书验证请求对应的验证文件关联，以将关联结果返回至可信第三方
S104
接收加密证书，并在网络节点上对加密证书进行部署；其中加密证书由可信第三方根据关联结果生成
S105

图 1

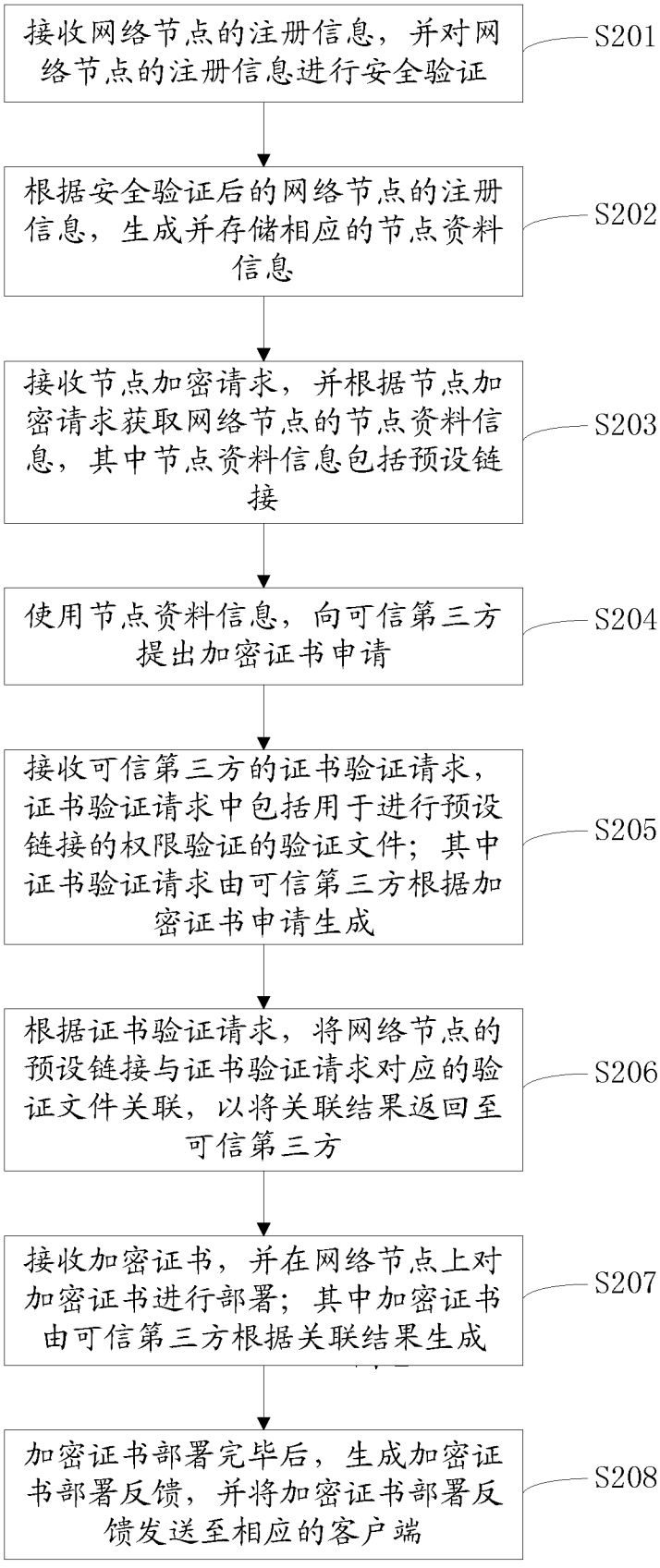
接收网络节点的注册信息，并对网络节点的注册信息进行安全验证
S201
根据安全验证后的网络节点的注册信息，生成并存储相应的节点资料信息
S202
接收节点加密请求，并根据节点加密请求获取网络节点的节点资料信息，其中节点资料信息包括预设链接
S203
使用节点资料信息，向可信第三方提出加密证书申请
S204
接收可信第三方的证书验证请求，证书验证请求中包括用于进行预设链接的权限验证的验证文件；其中证书验证请求由可信第三方根据加密证书申请生成
S205
根据证书验证请求，将网络节点的预设链接与证书验证请求对应的验证文件关联，以将关联结果返回至可信第三方
S206
接收加密证书，并在网络节点上对加密证书进行部署；其中加密证书由可信第三方根据关联结果生成
S207
加密证书部署完毕后，生成加密证书部署反馈，并将加密证书部署反馈发送至相应的客户端
S208

图 2

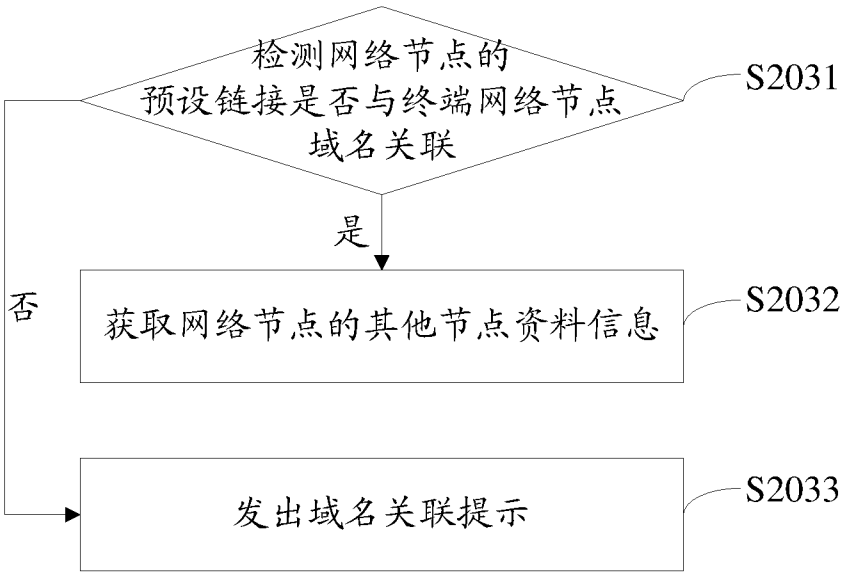
检测网络节点的预设链接是否与终端网络节点域名关联
S2031
是
否
获取网络节点的其他节点资料信息
S2032
发出域名关联提示
S2033

图 3

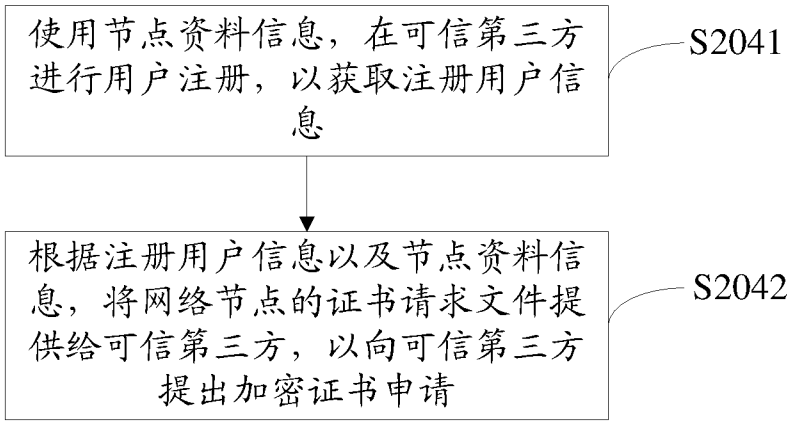
使用节点资料信息，在可信第三方进行用户注册，以获取注册用户信息
S2041
根据注册用户信息以及节点资料信息，将网络节点的证书请求文件提供给可信第三方，以向可信第三方提出加密证书申请
S2042

图 4

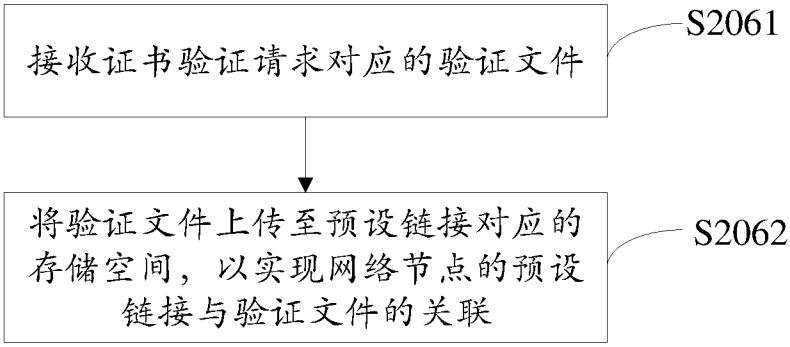
接收证书验证请求对应的验证文件
S2061
将验证文件上传至预设链接对应的存储空间，以实现网络节点的预设链接与验证文件的关联
S2062

图 5

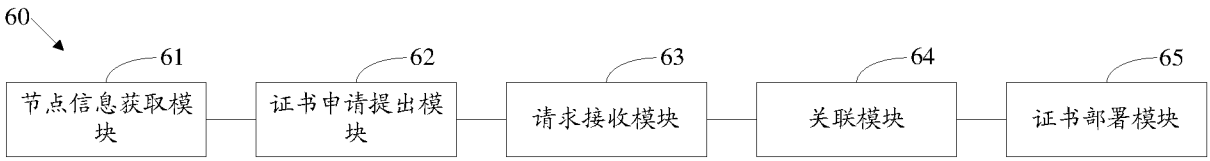
60
61
节点信息获取模块
62
证书申请提出模块
63
请求接收模块
64
关联模块
65
证书部署模块

图 6

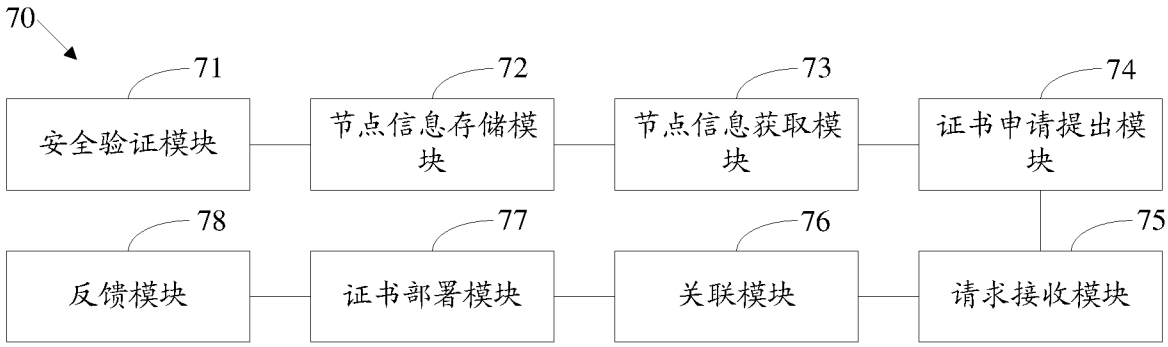
70
71
安全验证模块
72
节点信息存储模块
73
节点信息获取模块
74
证书申请提出模块
78
反馈模块
77
证书部署模块
76
关联模块
75
请求接收模块

图 7

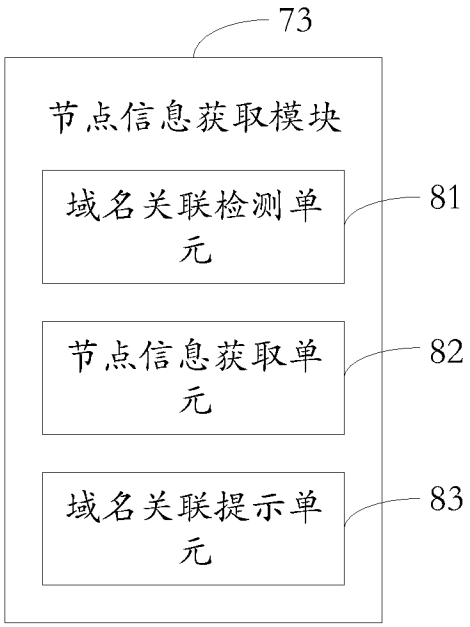
73
节点信息获取模块
域名关联检测单元
81
节点信息获取单元
82
域名关联提示单元
83

图 8

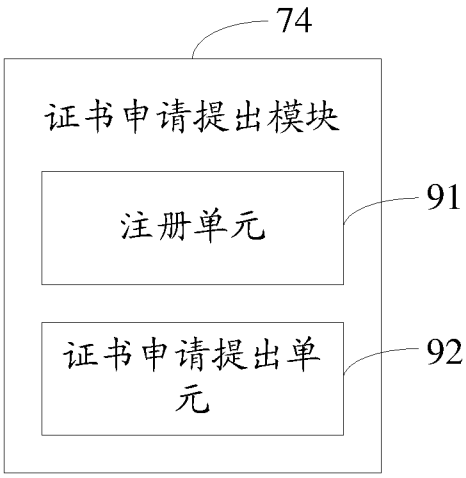
74
证书申请提出模块
注册单元
91
证书申请提出单元
92

图 9

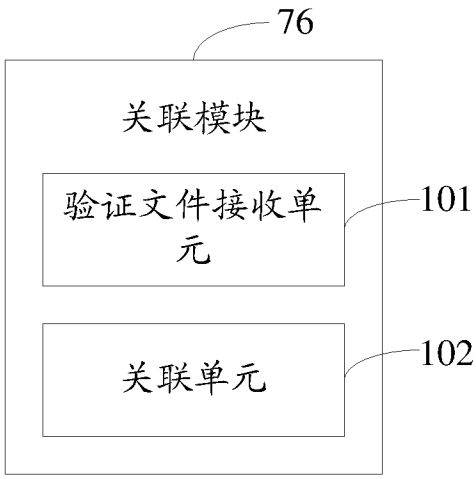
76
关联模块
验证文件接收单元
101
关联单元
102

图 10

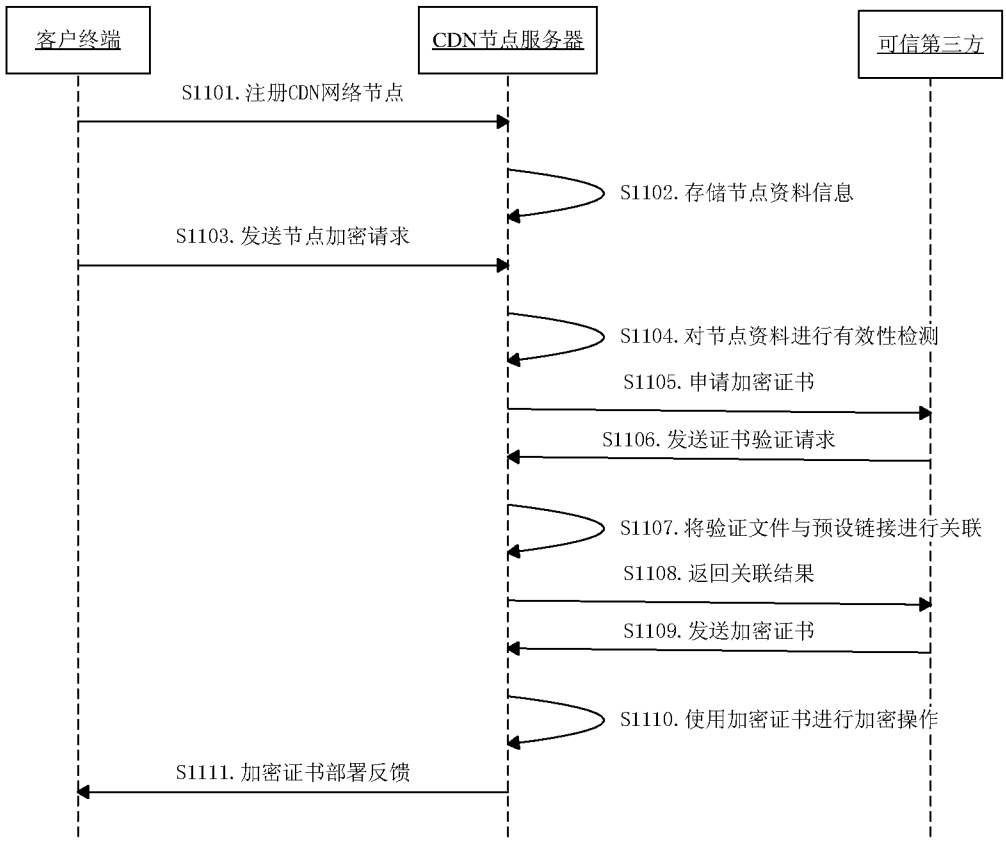
客户终端
CDN节点服务器
可信第三方
S1101. 注册CDN网络节点
S1102. 存储节点资料信息
S1103. 发送节点加密请求
S1104. 对节点资料进行有效性检测
S1105. 申请加密证书
S1106. 发送证书验证请求
S1107. 将验证文件与预设链接进行关联
S1108. 返回关联结果
S1109. 发送加密证书
S1110. 使用加密证书进行加密操作
S1111. 加密证书部署反馈

图 11

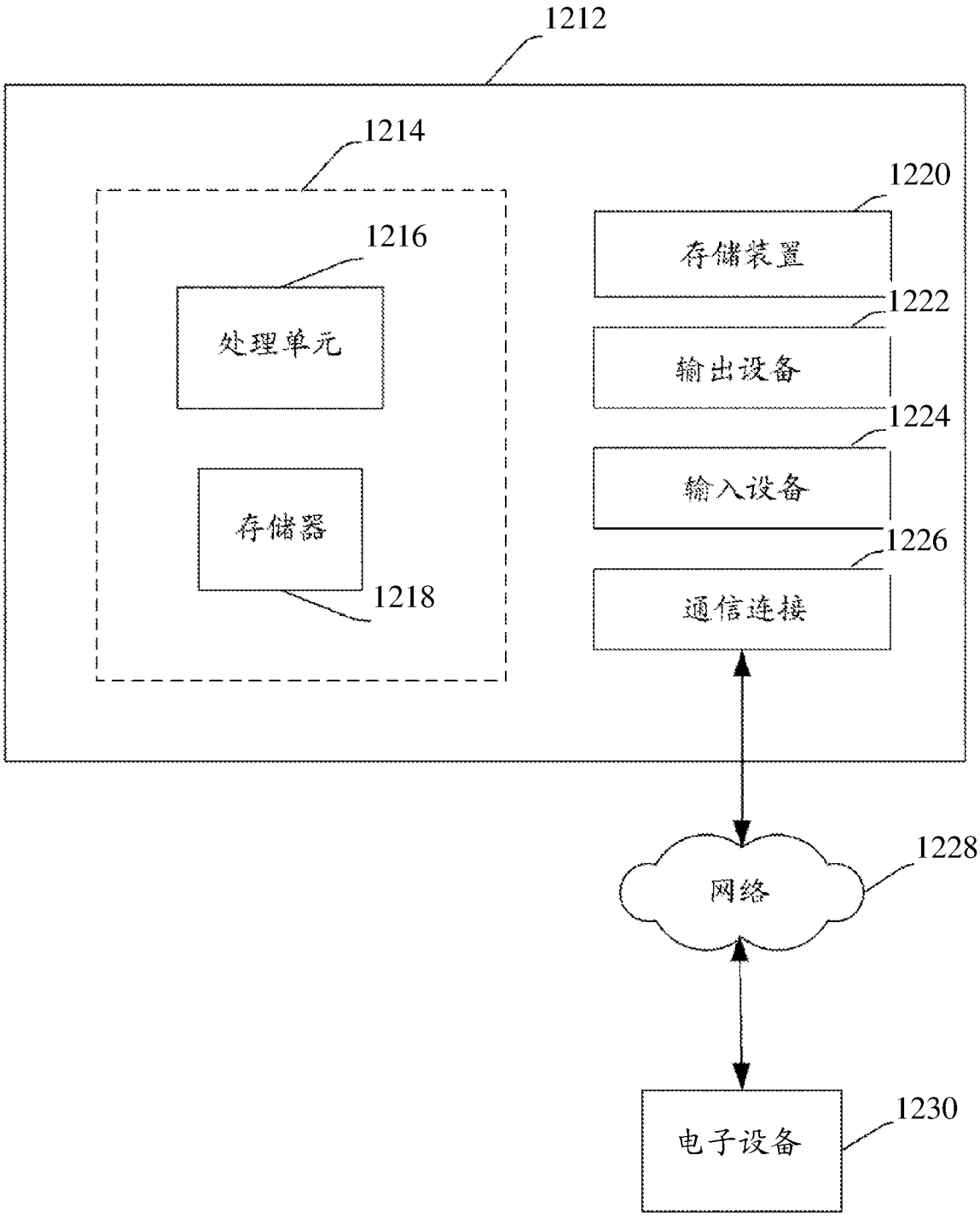
1212
1214
1216
处理单元
存储器
1218
1220
存储装置
1222
输出设备
1224
输入设备
1226
通信连接
网络
1228
电子设备
1230

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/094021

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; CNKI; VEN; WOTXT; EPTXT; USTXT: 加密, encrypt+, 证书, certificat+, 可信, 信任, trust+, 第三方, third party, 验证, verificat+, 链接, link, 域名, domain name, 地址, address, H04L63/0428/cpc, H04L63/0823/cpc

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 106302476 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 04 January 2017 (04.01.2017), claims 1-12	1-20
A	US 2014269431 A1 (VIRNETX INC.) 18 September 2014 (18.09.2014), entire document	1-20
A	CN 101527634 A (BEIJING FEITIAN TECHNOLOGIES CO., LTD.) 09 September 2009 (09.09.2009), entire document	1-20
A	US 2016241405 A1 (CRUCIALTEC CO., LTD.) 18 August 2016 (18.08.2016), entire document	1-20
A	CN 102932762 A (WUXI CINSEC INFORMATION TECHNOLOGY CO., LTD.) 13 February 2013 (13.02.2013), entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 October 2017	01 November 2017

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer
REN, Ling
Telephone No. (86-10) 62088423

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/094021

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106302476 A	04 January 2017	None	
US 2014269431 A1	18 September 2014	US 7986688 B2	26 July 2011
		US 7209479 B2	24 April 2007
		US 2015358168 A1	10 December 2015
		US 2007022477 A1	25 January 2007
		US 2002093915 A1	18 July 2002
		EP 2264951 A2	22 December 2010
		US 8780905 B2	15 July 2014
		US 9673988 B2	06 June 2017
		EP 2264952 A2	22 December 2010
		US 2008040794 A1	14 February 2008
		US 8571025 B2	29 October 2013
		EP 2264951 A3	21 March 2012
		US 8780906 B2	15 July 2014
		US 7944915 B2	17 May 2011
		EP 2264952 A3	21 March 2012
		US 2013014246 A1	10 January 2013
		EP 1360803 A1	12 November 2003
		US 2013067087 A1	14 March 2013
		US 8761168 B2	24 June 2014
		AT 536020 T	15 December 2011
		EP 1360803 A4	16 March 2005
		EP 2264951 B1	31 July 2013
		US 2012036359 A1	09 February 2012
		US 2012131665 A1	24 May 2012
		WO 02058339 A1	25 July 2002
		EP 2264952 B1	09 October 2013
		US 9143490 B2	22 September 2015

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/094021

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
		EP 1360803 B1	30 November 2011
		AU 2002249950 A1	30 July 2002
CN 101527634 A	09 September 2009	CN 101527634 B	17 August 2011
US 2016241405 A1	18 August 2016	KR 101666374 B1	14 October 2016
		KR 20160099922 A	23 August 2016
CN 102932762 A	13 February 2013	CN 102932762 B	25 March 2015

国际检索报告

国际申请号
PCT/CN2017/094021

A. 主题的分类

H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;CNKI;VEN;WOTXT;EPTXT;USTXT: 加密，encrypt+，证书，certificat+，可信，信任，trust+，第三方，third party，验证，verificat+，链接，link，域名，domain name，地址，address，H04L63/0428/cpc，H04L63/0823/cpc

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 106302476 A (腾讯科技深圳有限公司) 2017年 1月 4日 (2017-01-04) 权利要求1-12	1-20
A	US 2014269431 A1 (VIRNETX INC.) 2014年 9月 18日 (2014-09-18) 全文	1-20
A	CN 101527634 A (北京飞天诚信科技有限公司) 2009年 9月 9日 (2009-09-09) 全文	1-20
A	US 2016241405 A1 (CRUCIALTEC CO., LTD.) 2016年 8月 18日 (2016-08-18) 全文	1-20
A	CN 102932762 A (无锡华御信息技术有限公司) 2013年 2月 13日 (2013-02-13) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 10月 14日	2017年 11月 1日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 任玲 电话号码 (86-10)62088423

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/094021

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	106302476	A	2017年 1月 4日	无			
US	2014269431	A1	2014年 9月 18日	US	7986688	B2	2011年 7月 26日
				US	7209479	B2	2007年 4月 24日
				US	2015358168	A1	2015年 12月 10日
				US	2007022477	A1	2007年 1月 25日
				US	2002093915	A1	2002年 7月 18日
				EP	2264951	A2	2010年 12月 22日
				US	8780905	B2	2014年 7月 15日
				US	9673988	B2	2017年 6月 6日
				EP	2264952	A2	2010年 12月 22日
				US	2008040794	A1	2008年 2月 14日
				US	8571025	B2	2013年 10月 29日
				EP	2264951	A3	2012年 3月 21日
				US	8780906	B2	2014年 7月 15日
				US	7944915	B2	2011年 5月 17日
				EP	2264952	A3	2012年 3月 21日
				US	2013014246	A1	2013年 1月 10日
				EP	1360803	A1	2003年 11月 12日
				US	2013067087	A1	2013年 3月 14日
				US	8761168	B2	2014年 6月 24日
				AT	536020	T	2011年 12月 15日
				EP	1360803	A4	2005年 3月 16日
				EP	2264951	B1	2013年 7月 31日
				US	2012036359	A1	2012年 2月 9日
				US	2012131665	A1	2012年 5月 24日
				WO	02058339	A1	2002年 7月 25日
				EP	2264952	B1	2013年 10月 9日
				US	9143490	B2	2015年 9月 22日
				EP	1360803	B1	2011年 11月 30日
				AU	2002249950	A1	2002年 7月 30日
CN	101527634	A	2009年 9月 9日	CN	101527634	B	2011年 8月 17日
US	2016241405	A1	2016年 8月 18日	KR	101666374	B1	2016年 10月 14日
				KR	20160099922	A	2016年 8月 23日
CN	102932762	A	2013年 2月 13日	CN	102932762	B	2015年 3月 25日