(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
2017 年 1 月 5 日 (05.01.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/000676 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)

(21) 国际申请号: PCT/CN2016/081665

(22) 国际申请日: 2016 年 5 月 11 日 (11.05.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510381509.X 2015 年 7 月 2 日 (02.07.2015) CN

(71) 申请人: **西安西电捷通无线网络通信股份有限公司 (CHINA IWNCOMM CO., LTD.)** [CN/CN]; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。

(72) 发明人: **胡亚楠 (HU, Yanan)**; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。 **赖晓龙 (LAI, Xiaolong)**; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。 **李少锋 (LI, Shaofeng)**; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。 **张伟 (ZHANG, Wei)**; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。 **颜湘 (YAN, Xiang)**; 中国陕西省西安市高新区科技二路 68 号西安软件园秦风阁 A201, Shaanxi 710075 (CN)。

(74) 代理人: **北京集佳知识产权代理有限公司 (UNITALEN ATTORNEYS AT LAW)**; 中国北京市朝阳区建国门外大街 22 号赛特广场 7 层, Beijing 100004 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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,

[见续页]

(54) Title: METHOD FOR VERIFYING THE VALIDITY OF DIGITAL CERTIFICATE AND AUTHENTICATION SERVER THEREFOR

(54) 发明名称 : 一种验证数字证书有效性的方法及其鉴别服务器

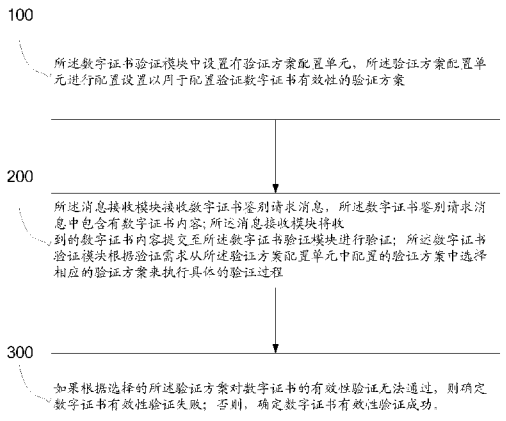

图 1

100 A VERIFICATION SCHEME CONFIGURATION UNIT IS PROVIDED IN THE DIGITAL CERTIFICATE VERIFICATION MODULE AND THE VERIFICATION SCHEME CONFIGURATION UNIT SETS A CONFIGURATION SO AS TO CONFIGURE A VERIFICATION SCHEME FOR VERIFYING THE VALIDITY OF A DIGITAL CERTIFICATE

200 THE MESSAGE RECEIVING MODULE RECEIVES A DIGITAL CERTIFICATE AUTHENTICATION REQUEST MESSAGE, THE DIGITAL CERTIFICATE AUTHENTICATION REQUEST MESSAGE CONTAINING A DIGITAL CERTIFICATE CONTENT; THE MESSAGE RECEIVING MODULE SUBMITS THE RECEIVED DIGITAL CERTIFICATE CONTENT TO THE DIGITAL CERTIFICATE VERIFICATION MODULE FOR VERIFICATION; AND THE DIGITAL CERTIFICATE VERIFICATION MODULE SELECTS A CORRESPONDING VERIFICATION SCHEME FROM VERIFICATION SCHEMES CONFIGURED IN THE VERIFICATION SCHEME CONFIGURATION UNIT ACCORDING TO A VERIFICATION REQUIREMENT, SO AS TO PERFORM A PARTICULAR VERIFICATION PROCESS

300 IF THE VERIFICATION OF THE VALIDITY OF THE DIGITAL CERTIFICATE ACCORDING TO THE SELECTED VERIFICATION SCHEME CANNOT BE PASSED, IT IS DETERMINED THAT THE VERIFICATION OF THE VALIDITY OF THE DIGITAL CERTIFICATE HAS FAILED; OTHERWISE, IT IS DETERMINED THAT THE VERIFICATION OF THE VALIDITY OF THE DIGITAL CERTIFICATE HAS SUCCEEDED

(57) **Abstract**: Provided is a method for verifying the validity of a digital certificate, which falls within the technical field of network security and solves the technical problem that the current method for verifying a digital certificate does not facilitate extension. The method relates to an authentication server comprising a message receiving module and a digital certificate verification module, wherein a verification scheme configuration unit is provided in the digital certificate verification module and sets a configuration so as to configure a verification scheme for verifying the validity of a digital certificate; the message receiving module receives a digital certificate authentication request message containing a digital certificate content, and submits the received digital certificate content to the digital certificate verification module for verification; if the verification of the validity of the digital certificate according to the selected verification scheme cannot be passed, it is determined that the verification of the validity of the digital certificate has failed; otherwise, it is determined that the verification of the validity of the digital certificate has succeeded. The method realizes the extension of a digital certificate verification scheme. Correspondingly, also provided is an authentication server.

(57) 摘要:

[见续页]

WO 2017/000676 A1

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))。

本申请提供的一种验证数字证书有效性的方法属网络安全技术领域，解决了当前对于数字证书验证方法不便于扩展的技术问题，该方法涉及包括消息接收模块和数字证书验证模块的鉴别服务器，其中数字证书验证模块中设置有验证方案配置单元，其进行配置设置以用于配置验证数字证书有效性的验证方案；所述消息接收模块接收包含有数字证书内容的数字证书鉴别请求消息，将收到的数字证书内容提交至所述数字证书验证模块进行验证；如果根据选择的所述验证方案对数字证书的有效性验证无法通过，则确定数字证书有效性验证失败；否则，确定数字证书有效性验证成功。该方法实现了数字证书验证方案的扩展。相应的，本申请同时还提供一种鉴别服务器。

一种验证数字证书有效性的方法及其鉴别服务器

本申请要求于 2015 年 7 月 2 日提交中国专利局、申请号为 201510381509.X、发明名称为“一种验证数字证书有效性的方法及其鉴别服务器”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

本发明涉及网络安全技术领域，尤其涉及一种验证数字证书有效性的方法及其鉴别服务器。

背景技术

目前在基于无线局域网鉴别和保密基础结构（WLAN Authentication and Privacy Infrastructure，简称 WAPI）协议的 WLAN 中，鉴别服务器实体（Authentication Service Entity, 简称 ASE）收到证书鉴别请求后，仅对收到的数字证书格式是否正确和是否被吊销的状态进行验证。验证过程涉及到使用对数字证书中数字签名验证等复杂的密码学技术，需要消耗大量的计算资源，如果黑客随意搜集一个无效的数字证书连续发送到 ASE，将会成功占用 ASE 大量的计算资源和时间，形成有效的拒绝服务攻击（Denial of Service，简称 DOS），导致其他合法用户无法正常和 ASE 进行通信。同时，由于验证内容对数字证书是否在数字证书颁发者颁发本数字证书时限定的业务范围内使用并不验证，黑客可能将一个领域合法授权的数字证书用于其他非授权领域，造成信息安全事故。

总之，当前通常对数字证书验证方法相对固定化、单一，没有考虑后续如何扩展，而且存在一定的安全风险。

发明内容

为了解决上述技术问题，本发明提供如下的技术方案：

一种验证数字证书有效性的方法，该方法涉及鉴别服务器，该鉴别服务器包括消息接收模块和数字证书验证模块，所述数字证书验证模块中设置有验证方案配置单元，所述验证方案配置单元进行配置设置以用于配置验证数字证书有效性的验证方案；

所述消息接收模块接收数字证书鉴别请求消息，所述数字证书鉴别请求消息中包含有数字证书内容；所述消息接收模块将收到的数字证书内容提交至所述数字证书验证模块进行验证；所述数字证书验证模块根据验证需求从所述验证方案配置单元中配置的验证方案中选择相应的验证方案来执行具体的验证过程；

如果根据选择的所述验证方案对数字证书的有效性验证无法通过，则确定数字证书有效性验证失败；否则，确定数字证书有效性验证成功。

此外，本发明同时提供一种用于验证数字证书有效性的鉴别服务器，其包括消息接收模块、数字证书验证模块，其特征在于，所述数字证书验证模块包括验证方案配置单元；

所述消息接收模块用于接收数字证书鉴别请求分组；

所述验证方案配置单元用于配置验证数字证书有效性的验证方案。

本发明提供的技术方案，很好的降低了鉴别服务器增加和删除验证方案的复杂度，通过验证方案配置单元实现了鉴别服务器在涉及多种验证方案时的有效配置和控制，有助于验证方案的扩展、修改及删除等操作；另外，通过选用已配置的验证方案验证数字证书的有效性，也提高了数字证书验证效率。

附图说明

图 1 为本发明提供的方法流程示意图；

图 2 为本发明实施例一流程示意图；

图 3 为本发明实施例二流程示意图；

图 4 为本发明实施例三流程示意图;

图 5 为本发明实施例网络拓扑示意图;

图 6 为本发明实施例提供的鉴别服务器结构示意图。

具体实施方式

下面结合附图和实施例对本发明提供的验证数字证书有效性的方法及其鉴别服务器进行更详细地说明。

如图 1 及图 6 所示，本发明提供的验证数字证书有效性的方法，其涉及鉴别服务器，所述鉴别服务器包括消息接收模块和数字证书验证模块，该方法具体包括:

S100，所述数字证书验证模块中设置有验证方案配置单元，所述验证方案配置单元进行配置设置以用于配置验证数字证书有效性的验证方案;

S200，所述消息接收模块接收数字证书鉴别请求消息，所述数字证书鉴别请求消息中包含有数字证书内容; 所述消息接收模块将收到的数字证书内容提交至所述数字证书验证模块进行验证; 所述数字证书验证模块根据验证需求从所述验证方案配置单元中配置的验证方案中选择相应的验证方案来执行具体的验证过程;

S300，如果根据选择的所述验证方案对数字证书的有效性验证无法通过，则确定数字证书有效性验证失败; 否则，确定数字证书有效性验证成功。

优选的，所述鉴别服务器中还可以包括数字证书解析模块，用于解析数字证书鉴别请求分组以获取数字证书内容。

优选的，所述配置设置为创建验证方案数据库表，所述验证方案数据库表包括验证项目字段和开关值字段，所述验证项目字段用于标识验证方案; 所述验证方案的启用通过设置开关值来实现，当所述开关值为开启时，启用相应的验证方案; 当所述开关值设置为关闭时，不启用相应的验证方案。

优选的，S100 中所述验证方案可以是白名单列表验证、黑名单列表验证、数字证书格式和吊销状态验证以及数字证书使用范围验证等验证方案中的至少任意两种的组合。相应的验证方案由所述验证方案配置单元使用验证方案配置数据库表设置，配置有前述验证方案的验证方案配置单元进一步就包括了白名单列表验证子单元、黑名单列表验证子单元、数字证书格式和吊销状态验证子单元、数字证书使用范围验证子单元以及数字证书使用范围验证子单元。其中数字证书使用范围是指数字证书的颁发者是否有权限颁发在某个使用范围的数字证书或者数字证书的颁发者在某个使用范围内的可信度或者数字证书本身在颁发的时候是否限定某个使用范围内使用的权限。同时，所述验证方案配置单元中设置有开关值以确定相应验证子单元是否开启，通常情况下开关值设置为 1 时表示开启，开关值设置为 0 时表示关闭。所述验证方案配置单元具有建立验证方案配置数据库表、增加和删除验证方案和配置验证方案的功能。

具体的，如表一所示，所述验证方案配置单元创建验证方案配置数据库表，其中的验证方案配置数据库表包括序号字段、验证项目字段以及开关值字段。所述序号字段是主键，序号值自动递增，该序号字段可用于标识相应的验证方案的执行顺序（如 1 表示第一验证内容，2 表示第二验证内容等）；所述验证项目字段用于标识验证方案配置单元支持的数字证书验证方案，该验证项目字段标识的验证方案可根据本地验证策略要求的验证顺序调整到对应序号序号字段标识的位置。

序号	验证项目	开关值
1	白名单列表验证	0 或者 1
2	黑名单列表验证	0 或者 1

3	数字证书格式和吊销状态验证	0 或者 1
4	数字证书使用范围验证	0 或者 1
…	…	…

表一

优选的，所述数据库表中还可以包括验证顺序字段（在此情况下的序号字段仅仅是一个序号标识），如表二所示，通过在验证顺序字段中配置优先级顺序如 1,2,3 等，以用于标识相应验证方案的执行顺序。

序号	验证顺序	验证项目	开关值
1	2	白名单列表验证	0 或者 1
2	3	黑名单列表验证	0 或者 1
3	4	数字证书格式和吊销状态验证	0 或者 1
4	1	数字证书使用范围验证	0 或者 1
…		…	…

表二

所述数字证书验证方案具体可以包括白名单列表验证、黑名单列表验证、数字证书格式和吊销状态验证以及数字证书应用范围验证等中的至少任意两种的组合，即所述验证方案配置单元进一步包括了白名单列表验证子单元、黑

名单列表验证子单元、数字证书格式和吊销状态验证子单元以及数字证书应用范围验证子单元。所述开关值字段表示是否启用验证项目字段标识的验证方案。所述验证方案配置数据库表中验证项目字段标识的具体验证方案均可灵活的增加、修改和删除；其中每个对应的开关值字段的数值用于表示相应的验证方案是否开启，通常情况下，当开关值字段的值为 0 时代表对应的验证项目开启，当开关值字段的值为 1 时代表对应的验证项目关闭。当然，也可将开关值字段的值设置为 1 时代表对应的验证项目开启，当开关值字段的值为 0 时代表对应的验证项目关闭，本发明对于开关值字段的值的设置不做限制。

优选的，所述配置设置还可通过 XML 的方式配置验证方案。即验证方案配置单元以 XML 格式配置文件存在，该配置文件中包括序号元素、验证项目元素、验证顺序元素以及开关值元素。所述开关值元素用于确定相应验证子单元是否开启，通常情况下开关值元素设置为 1 时表示开启，开关值元素设置为 0 时表示关闭，所述验证方案配置单元可通过修改 XML 配置文件中元素的方式进行验证方案的增加、修改和删除。前述通过 XML 方式配置验证方案的配置文件示例如下:

<item>

<序号>1<序号/>

<验证项目>白名单列表验证</验证项目>

<验证顺序>2</验证顺序>

<开关值>0 或者 1</开关值>

</item>

<item>

<序号>2<序号/>

<验证项目>黑名单列表验证</验证项目>

<验证顺序>3</验证顺序>

<开关值>0 或者 1</开关值>

</item>

<item>

<序号>3<序号/>

<验证项目>数字证书格式和吊销状态验证</验证项目>

<验证顺序>4</验证顺序>

<开关值>0 或者 1</开关值>

</item>

<item>

<序号>4<序号/>

<验证项目>数字证书使用范围验证</验证项目>

<验证顺序>1</验证顺序>

<开关值>0 或者 1</开关值>

</item>

本发明正是利用了验证方案的配置设置实现了鉴别服务器中多种验证方

案的有效配置和控制，利用所述验证方案配置单元进行验证方案的配置设置有助于鉴别服务器验证方案的灵活的增加、修改和删除，

以下将结合图 2、图 3、图 4、图 5 就基于数据库表配置验证方案的方式对于本发明具体实施过程进行详细的阐述。

实施例一

如图 2 和图 5，在所述验证方案配置单元中开启数字证书使用范围验证子单元和数字证书格式和吊销状态验证子单元。具体验证过程详细说明如下。以 WAPI 网络架构为例，当所述消息接收模块接收到接入点 AP 发送的数字证书鉴别请求分组后，由所述数字证书解析模块对所述数字证书鉴别请求分组解析以获得数字证书内容，并将解析后的数字证书内容提交到所述数字证书验证模块，首先由所述数字证书验证模块中的数字证书使用范围验证子单元执行验证。具体是：所述数字证书使用范围验证子单元创建一个数字证书使用范围表，如表三所示，所述数字证书使用范围表包括序号字段、数字证书标识字段和使用范围字段，其中，序号字段是主键，序号值自动递增；数字证书标识字段表示是数字证书标识内容，数字证书标识可以为数字证书中证书序列号和颁发者名称的组合，也可以只为证书序列号。

序号	数字证书标识	使用范围
1	证书序列号 1+颁发者名称	范围 1/范围 2/范围 1/范围 4…
2	证书序列号 2+颁发者名称	范围 1/范围 2/范围 1/范围 4…
3	证书序列号 3+颁发者名称	范围 1/范围 2/范围 1/范围 4…
4	证书序列号 4+颁发者名称	范围 1/范围 2/范围 1/范围 4…
…	…	…

表三

所述数字证书使用范围验证子单元可执行 SQL 的查询语句对数字证书的使用范围是否在使用范围字段中进行查询，根据 SQL 查询语句的返回值判断；

如果在所述使用范围字段中可以查询到数字证书鉴别请求分组中包含的数字证书符合数字证书颁发时规定的使用范围，则所述数字证书使用范围验证子单元验证数字证书使用范围成功，否则，所述数字证书使用范围验证子单元验证数字证书使用范围失败。其中，数字证书使用范围记录可以增加或者删除。鉴别服务器增加或者删除数字证书使用范围记录的信息可来自于数字证书颁发实体或者网络管理员等，本发明对此不做限制。

换句话说，如果数字证书使用范围验证子单元判断数字证书鉴别请求分组中包含的数字证书不符合数字证书颁发时候规定的使用范围，则数字证书验证模块得到的数字证书验证结果为失败，然后通过消息发送模块构建证书鉴别响应分组发送至 AP 告知数字证书验证结果或者数字证书应该的使用范围；如果数字证书使用范围验证子单元判断数字证书鉴别请求分组中包含的数字证书符合数字证书颁发时候规定的使用范围，则继续下一步的验证。

然后由数字证书格式和吊销状态验证子单元进行验证，具体是：

所述数字证书解析模块解析所述数字证书鉴别请求分组获取数字证书的相关信息，所述数字证书格式和吊销状态验证子单元验证所述数字证书的信息格式是否与所述鉴别服务器已知的格式一致，如果不一致则数字证书格式和吊销状态验证失败，如果一致则数字证书格式和吊销状态验证成功；本发明中所述数字证书的信息格式依据的是 X.509 的数字证书标准；

或者，所述鉴别服务器利用其数字证书的公钥计算所述解析模块解析后的所述数字证书鉴别请求分组中的数字证书的签名值，所述数字证书格式和吊销状态验证子单元计算出的签名值和所述数字证书的签名值是否相同，如果不相同，则数字证书格式和吊销状态验证失败，如果相同，则数字证书格式和吊销状态性验证成功；

或者，所述数字证书格式和吊销状态验证子单元验证所述鉴别服务器当前时间和接收到的数字证书的有效时间范围，如果所述鉴别服务器当前时间不在接收到的数字证书的有效范围内，则数字证书格式和吊销状态验证失败；否则，数字证书格式和吊销状态验证成功；

或者，所述数字证书格式和吊销状态验证子单元验证所述鉴别服务器存储的接收到的数字证书的状态是否被标记为已吊销，如果被标记为已吊销，则数字证书格式和吊销状态验证失败，否则，数字证书格式和吊销状态验证成功。

在其他实施方式中，上述数字证书格式和吊销状态验证子单元执行的四种验证方式可做任意组合使用，此时，组合中的任意一种如果验证失败，则认为所述数字证书格式和吊销状态验证子单元判断证书鉴别请求分组中包含的数字证书格式不正确或者使用状态是无效，即数字证书验证失败；否则，数字证书验证成功。

基于上述的验证数字证书验证模块得到的数字证书验证结果为成功后，然后通过消息发送模块构建证书鉴别响应分组发送至 AP 告知数字证书验证结果。

该实施例述及的验证过程适用于在完全开放的网络环境中传输数字证书的情况，该验证方案能够很好地提高这种网络环境下的数字证书的验证效率。

实施例二

如图 3 和图 5，在所述验证方案配置模块中开启数字证书格式和吊销状态验证子单元、黑名单列表验证子单元和或白名单列表验证子单元。具体验证过程详细说明如下。

以 WAPI 网络架构为例，首先数字证书格式和吊销状态验证子单元开始执行验证具体验证过程同实施例一的表述，此处不再赘述。当数字证书格式和吊销状态验证通过后所述黑名单列表验证子单元和或白名单列表验证子单元开

始验证，具体包括:

所述白名单列表验证子单元创建一个白名单数据库表，如表四所示所述白名单数据库表包括序号字段和白名单值字段，其中序号字段是主键，序号值自动递增；白名单值字段表示数字证书标识，数字证书标识可以为数字证书中证书序列号和颁发者名称的组合，也可以只为证书序列号。

序号	白名单值
1	证书序列号 1+颁发者名称
2	证书序列号 2+颁发者名称
3	证书序列号 3+颁发者名称
4	证书序列号 4+颁发者名称
…	…

表四

所述白名单列表验证子单元执行 SQL 的查询语句对数字证书标识是否在白名单值字段中进行查询，根据 SQL 查询语句的返回值判断，如果返回值中包含有所查询的数字证书标识，则代表在白名单数据库表的白名单值字段中可以查询到数字证书鉴别请求分组中包含的数字证书的标识，否则，则代表在白名单数据库表的白名单值字段中不能查询到数字证书鉴别请求分组中包含的数字证书的标识;

如果在白名单数据库表的白名单值字段中可以查询到数字证书鉴别请求分组中包含的数字证书的标识，则所述白名单列表验证子单元执行白名单验证通过，说明白名单列表验证子单元判断证书鉴别请求分组中包含的数字证书在白名单内，从而确定数字证书有效性验证成功；否则，所述白名单列表验证子单元执行白名单验证失败，说明白名单列表验证子单元判断证书鉴别请求分组

换句话说，如果白名单列表验证子单元判断数字证书鉴别请求分组中包含

的数字证书不在白名单内，则数字证书验证单元得到的数字证书验证结果为失败，并通过消息发送模块构建证书鉴别响应分组发送至 AP 告知数字证书验证结果；如果白名单列表验证子单元判断数字证书鉴别请求分组中包含的数字证书在白名单内，则数字证书有效性验证成功。

上述执行过程中的白名单值可以增加或者删除。鉴别服务器增加或者删除白名单记录的信息可来自于数字证书颁发实体或者网络管理员等，本发明对此不做限制。

黑名单列表验证子单元的验证过程详细如下。

所述黑名单列表验证子单元创建一个黑名单数据库表，如表五所示，所述黑名单数据库表包括序号字段和黑名单值字段，其中，序号字段是主键，序号值自动递增；黑名单值字段表示是数字证书标识，数字证书标识可以为数字证书中证书序列号和颁发者名称的组合，也可以只为证书序列号。

序号	黑名单值
1	证书序列号 1+颁发者名称
2	证书序列号 2+颁发者名称
3	证书序列号 3+颁发者名称
4	证书序列号 4+颁发者名称
…	…

表五

所述黑名单列表验证子单元执行 SQL 的查询语句对数字证书标识是否在黑名单值字段中进行查询，根据 SQL 查询语句的返回值判断，如果返回值中包含有所查询的数字证书标识，则代表在黑名单数据库表的黑名单值字段中可以查询到数字证书鉴别请求分组中包含的数字证书的标识，否则，则代表在黑名单数据库表的黑名单值字段中不能查询到数字证书鉴别请求分组中包含的

数字证书的标识;

如果在黑名单数据库表的黑名单值字段中可以查询到数字证书鉴别请求分组中包含的数字证书的标识，则所述黑名单列表验证子单元执行黑名单验证不通过，说明黑名单列表验证子单元判断证书鉴别请求分组中包含的数字证书在黑名单内从而确定数字证书有效性验证失败；否则，所述黑名单列表验证子单元执行黑名单验证成功，说明黑名单列表验证子单元判断证书鉴别请求分组中包含的数字证书不在黑名单内，从而确定数字证书有效性验证成功。

换句话说，如果黑名单列表验证子单元判断证书鉴别请求分组中包含的数字证书在黑名单内，则数字证书验证模块得到的数字证书验证结果为失败，然后通过消息发送模块构建证书鉴别响应分组发送至 AP 告知数字证书验证结果；如果黑名单列表验证子单元判断证书鉴别请求分组中包含的数字证书不在黑名单则数字证书有效性验证成功。

上述执行过程中的黑名单值可以增加或者删除。鉴别服务器增加或者删除黑名单记录的信息可来自于数字证书颁发实体或者网络管理员等，本发明对此不做限制。

基于上述的验证数字证书验证模块得到的数字证书验证结果为成功后，然后通过消息发送模块构建证书鉴别响应分组发送至 AP 告知数字证书验证结果。

该实施例述及的验证过程适用于在一个特定的网络环境中，如一个企业内的局域网，传输的数字证书很大可能是企业内部的数字证书颁发者颁发，每一台企业内部网络中使用的设备中包含的数字证书数量有限，且根据设备本身的应用仅含有某个特定应用的证书，在这个封闭的特定应用环境中，由于数字证书来源和应用范围单一。该实施例提供的验证方案能够很好地提高这种网络环境下的数字证书的验证效率。

实施例三

如图 4 和图 5，在所述验证方案配置模块中开启黑名单列表验证子单元和或白名单列表验证子单元、数字证书使用范围验证子单元以及数字证书格式和吊销状态验证子单元。具体验证过程详细说明如下。

以 WAPI 网络架构为例，当所述消息接收模块接收到接入点 AP 发送的数字证书鉴别请求分组后，由所述数字证书解析模块对所述数字证书鉴别请求分组解析以获得数字证书内容，并将解析后的数字证书内容提交到所述数字证书验证模块，首先由所述黑名单列表验证子单元和或白名单列表验证子单元执行验证，详细验证过程同实施例二的描述，此处不再赘述。

待所述黑名单列表验证子单元和或白名单列表验证子单元执行验证的结果为通过时，进一步由数字证书使用范围验证子单元执行验证，该验证过程同实施例一的描述，此处不再赘述。

待所述数字证书使用范围验证子单元执行验证的结果为在特定的范围内时，进一步由所述数字证书格式和吊销状态验证子单元执行验证，如验证执行通过则数字证书有效性验证成功，否则，数字证书有效性验证失败。

基于上述的验证数字证书验证模块得到的数字证书验证结果为成功后，然后通过消息发送模块构建证书鉴别响应分组发送至 AP 告知数字证书验证结果。

该实施例述及的验证过程适用于在一个网络通信系统中，如果某几个网络只限定给某些用户使用，其他的网络所有人都可以使用，则需要限定给某些用户使用的网络设备需要首先验证自己设备中的白名单和或黑名单，如果接收到的数字证书内容是白名单和或黑名单里面的成员，则可进行后续验证，如果接收到的数字证书内容不在设备的白名单内和或黑名单，不再进行后续的验证工作，节省时间。该验证方案能够很好地提高这种网络环境下的数字证书的验证效率。

除上述实施例描述的以外，所述验证方案配置单元中的验证项目字段标识的验证方案还可以是证书鉴别请求分组中包含的数字证书的颁发者是否满足使用的安全级别的验证等，鉴别服务器还可继续依据验证方案配置单元预置的验证方案对数字证书鉴别请求分组中包含的数字证书进行验证，然后通过消息发送模块构建证书鉴别响应分组发送给AP告知数字证书验证结果或者与验证相关的信息内容，本发明具体实施部分对此不再赘述。

此外，本发明提供的验证数字证书有效性的方法并不局限于上述实施例所述的 WAPI 架构。基于本发明提供的验证数字证书有效性的方法的相同的思路，本发明还提供了一种与之对应的鉴别服务器，参见图 6。具体是：

用于验证数字证书有效性的鉴别服务器，其包括消息接收模块、数字证书验证模块，其特征在于，所述数字证书验证模块包括验证方案配置单元；

所述消息接收模块用于接收数字证书鉴别请求分组；

所述验证方案配置单元用于配置验证数字证书有效性的验证方案。

优选的，所述鉴别服务器还可以进一步包括数字证书解析模块，用于解析数字证书鉴别请求分组中的数字证书内容。

优选的，所述验证方案配置单元进一步包括白名单列表验证子单元，所述白名单列表验证子单元用于验证所述数字证书鉴别请求分组中的数字证书是否包含在白名单内；

所述验证方案配置单元进一步包括黑名单列表验证子单元，所述黑名单列表验证子单元用于验证所述数字证书鉴别请求分组中的数字证书是否包含在黑名单内；

所述验证方案配置单元进一步包括数字证书格式和吊销状态验证子单元，所述数字证书格式和吊销状态验证子单元用于验证所述数字证书的信息格式是否与所述鉴别服务器已知的格式一致；

所述验证方案配置单元进一步包括数字证书使用范围验证子单元，所述数字证书使用范围验证子单元用以验证所述数字证书鉴别请求分组中包含的数字证书是否符合数字证书颁发时候规定的使用范围。

鉴别服务器所述各结构的功能及工作方式与前述方法中描述的工作过程相应，此处不再赘述。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种验证数字证书有效性的方法，该方法涉及鉴别服务器，该鉴别服务器包括消息接收模块和数字证书验证模块，其特征在于，

所述数字证书验证模块中设置有验证方案配置单元，所述验证方案配置单元进行配置设置以用于配置验证数字证书有效性的验证方案；

所述消息接收模块接收数字证书鉴别请求消息，所述数字证书鉴别请求消息中包含有数字证书内容;所述消息接收模块将收到的数字证书内容提交至所述数字证书验证模块进行验证；所述数字证书验证模块根据验证需求从所述验证方案配置单元中配置的验证方案中选择相应的验证方案来执行具体的验证过程；

如果根据选择的所述验证方案对数字证书的有效性验证无法通过，则确定数字证书有效性验证失败；否则，确定数字证书有效性验证成功。

2、根据权利要求 1 所述的方法，其特征在于，所述配置设置为创建验证方案数据库表，所述验证方案数据库表包括验证项目字段和开关值字段，所述验证项目字段用于标识验证方案；所述验证方案的启用通过设置开关值来实现，当所述开关值为开启时，启用相应的验证方案；当所述开关值设置为关闭时，不启用相应的验证方案。

3、根据权利要求 2 所述的方法，其特征在于，所述验证方案数据库表还包括序号字段和或验证顺序字段，所述验证顺序字段用于控制验证方案的执行顺序。

4、根据权利要求 1 或 2 或 3 所述的方法，其特征在于，所述验证方案为白名单列表验证方案、黑名单列表验证方案、数字证书格式和吊销状态验证方案以及数字证书使用范围验证方案中的至少任意两种的组合；

所述验证方案配置单元中相应的进一步包括：白名单列表验证子单元、黑名单列表验证子单元、数字证书格式和吊销状态验证子单元以及数字证书使用

范围验证子单元中的至少任意两种的组合。

5、根据权利要求 4 所述的方法，其特征在于，所述验证方案配置单元中启用数字证书使用范围验证子单元和数字证书格式和吊销状态验证子单元以验证数字证书有效性的方法，具体包括:

1）首先执行数字证书使用范围验证:

所述数字证书使用范围验证子单元创建一个数字证书使用范围表，所述数字证书使用范围表包括序号字段、数字证书标识字段和使用范围字段;

所述数字证书使用范围验证子单元执行 SQL 的查询语句对数字证书的使用范围否在使用范围字段中进行查询，根据 SQL 查询语句的返回值判断;

如果在所述使用范围字段中可以查询到数字证书鉴别请求分组中包含的数字证书符合数字证书颁发时规定的使用范围，则所述数字证书使用范围验证子单元验证数字证书使用范围成功，从而进一步执行数字证书格式和吊销状态验证;

否则，所述数字证书使用范围验证子单元验证数字证书使用范围失败，从而确定数字证书有效性验证失败;

2）执行数字证书格式和吊销状态验证:

所述数字证书格式和吊销状态验证子单元验证所述数字证书内容的信息格式是否与所述鉴别服务器已知的格式一致，如果不一致则数字证书格式和吊销状态验证失败，如果一致则数字证书格式和吊销状态验证成功;

或者，所述鉴别服务器利用其数字证书的公钥计算所述数字证书鉴别请求分组中的数字证书的签名值，所述数字证书格式和吊销状态验证子单元计算出的签名值和所述数字证书的签名值是否相同，如果不相同，则数字证书格式和吊销状态验证失败，如果相同则数字证书格式和吊销状态验证验证成功;

或者，所述数字证书格式和吊销状态验证子单元验证所述鉴别服务器当前时间和接收到的数字证书的有效时间范围，如果所述鉴别服务器当前时间不在

接收到的数字证书的有效范围内，则数字证书格式和吊销状态验证失败；否则，数字证书格式和吊销状态验证成功；

或者，所述数字证书格式和吊销状态验证子单元验证所述鉴别服务器存储的接收到的数字证书的状态是否被标记为已吊销，如果被标记为已吊销，则数字证书格式和吊销状态验证失败，否则，数字证书格式和吊销状态验证成功。

6、根据权利要求 4 所述的方法，其特征在于，所述验证方案配置单元中启用数字证书格式和吊销状态验证子单元、黑名单列表验证子单元和或白名单列表验证子单元以验证数字证书有效性的方法，具体包括：

1）首先执行数字证书格式和吊销状态验证：

所述数字证书格式和吊销状态验证子单元验证所述数字证书内容的信息格式是否与所述鉴别服务器已知的格式一致，如果不一致则数字证书格式和吊销状态验证失败，如果一致则数字证书格式和吊销状态验证成功；

或者，所述鉴别服务器利用其数字证书的公钥计算所述数字证书鉴别请求分组中的数字证书的签名值，所述数字证书格式和吊销状态验证子单元计算出的签名值和所述数字证书的签名值是否相同，如果不相同，则数字证书格式和吊销状态验证失败，如果相同则数字证书格式和吊销状态验证成功；

或者，所述数字证书格式和吊销状态验证子单元验证所述鉴别服务器当前时间和接收到的数字证书的有效时间范围，如果所述鉴别服务器当前时间不在接收到的数字证书的有效范围内，则数字证书格式和吊销状态验证失败；否则，数字证书格式和吊销状态验证成功；

或者，所述数字证书格式和吊销状态验证子单元验证所述鉴别服务器存储的接收到的数字证书的状态是否被标记为已吊销，如果被标记为已吊销，则数字证书格式和吊销状态验证失败，否则，数字证书格式和吊销状态验证成功；

2）待所述数字证书格式和吊销状态验证执行成功后进一步执行黑名单列表验证和或白名单列表验证，具体包括：

所述黑名单列表验证子单元创建一个黑名单数据库表，所述黑名单数据库表包括序号字段和黑名单值字段，所述黑名单值字段为数字证书标识；

所述黑名单列表验证子单元执行 SQL 的查询语句对数字证书标识是否在白名单值字段中进行查询，根据 SQL 查询语句的返回值判断；

如果在黑名单数据库表的黑名单值字段中可以查询到数字证书鉴别请求分组中包含的数字证书的标识，则所述黑名单列表验证子单元执行黑名单验证失败；否则，确定所述黑名单列表验证子单元执行黑名单验证通过；和或，

所述白名单列表验证子单元创建一个白名单数据库表，所述白名单数据库表包括序号字段和白名单值字段，所述白名单值字段为数字证书标识；

所述白名单列表验证子单元执行 SQL 的查询语句对数字证书标识是否在白名单值字段中进行查询，根据 SQL 查询语句的返回值判断；

如果在白名单数据库表的白名单值字段中可以查询到数字证书鉴别请求分组中包含的数字证书的标识，则所述白名单列表验证子单元执行白名单验证通过；否则，确定所述白名单列表验证子单元执行白名单验证失败。

7、根据权利要求 4 所述的方法，其特征在于，所述验证方案配置单元中启用黑名单列表验证子单元和或白名单列表验证子单元、数字证书使用范围验证子单元以及数字证书格式和吊销状态验证子单元以验证数字证书有效性的方法，具体包括：

1）首先执行黑名单列表验证和或白名单列表验证，具体包括：

所述黑名单列表验证子单元创建一个黑名单数据库表，所述黑名单数据库表包括序号字段和黑名单值字段，所述黑名单值字段为数字证书标识；

所述黑名单列表验证子单元执行 SQL 的查询语句对数字证书标识是否在白名单值字段中进行查询，根据 SQL 查询语句的返回值判断；

如果在黑名单数据库表的黑名单值字段中可以查询到数字证书鉴别请求分组中包含的数字证书的标识，则所述黑名单列表验证子单元执行黑名单验证

失败；否则，确定所述黑名单列表验证子单元执行黑名单验证通过；和或，

所述白名单列表验证子单元创建一个白名单数据库表，所述白名单数据库表包括序号字段和白名单值字段，所述白名单值字段为数字证书标识；

所述白名单列表验证子单元执行 SQL 的查询语句对数字证书标识是否在白名单值字段中进行查询，根据 SQL 查询语句的返回值判断；

如果在白名单数据库表的白名单值字段中可以查询到数字证书鉴别请求分组中包含的数字证书的标识，则所述白名单列表验证子单元执行白名单验证通过；否则，确定所述白名单列表验证子单元执行白名单验证失败；

2）在黑名单列表验证和或白名单列表验证成功后，再执行数字证书使用范围验证，具体是：

所述数字证书使用范围验证子单元创建一个数字证书使用范围表，所述数字证书使用范围表包括序号字段、数字证书标识字段和使用范围字段；

所述数字证书使用范围验证子单元执行 SQL 的查询语句对数字证书的使用范围否在使用范围字段中进行查询，根据 SQL 查询语句的返回值判断；

如果在所述使用范围字段中可以查询到数字证书鉴别请求分组中包含的数字证书符合数字证书颁发时规定的使用范围，则所述数字证书使用范围验证子单元验证数字证书使用范围成功；

否则，所述数字证书使用范围验证子单元验证数字证书使用范围失败，从而确定数字证书有效性验证失败；

3）在数字证书使用范围验证成功后进一步执行数字证书格式和吊销状态验证，具体是：

所述数字证书格式和吊销状态验证子单元验证所述数字证书内容的信息格式是否与所述鉴别服务器已知的格式一致，如果不一致则数字证书格式和吊销状态验证失败，如果一致则数字证书格式和吊销状态验证成功；

或者，所述鉴别服务器利用其数字证书的公钥计算所述数字证书鉴别请求

分组中的数字证书的签名值，所述数字证书格式和吊销状态验证子单元计算出的签名值和所述数字证书的签名值是否相同，如果不相同，则数字证书格式和吊销状态验证失败，如果相同则数字证书格式和吊销状态验证成功；

或者，所述数字证书格式和吊销状态验证子单元验证所述鉴别服务器当前时间和接收到的数字证书的有效时间范围，如果所述鉴别服务器当前时间不在接收到的数字证书的有效范围内，则数字证书格式和吊销状态验证失败；否则，数字证书格式和吊销状态验证成功；

或者，所述数字证书格式和吊销状态验证子单元验证所述鉴别服务器存储的接收到的数字证书的状态是否被标记为已吊销，如果被标记为已吊销，则数字证书格式和吊销状态验证失败，否则，数字证书格式和吊销状态验证成功。

8、根据权利要求 1 所述的方法，其特征在于，所述配置设置还可以是 XML 格式的配置文件，其包括序号元素、验证项目元素、验证顺序元素以及开关值元素；

所述验证顺序元素用于控制验证方案的执行顺序；

所述开关值元素用于确定相应的验证方案是否开启。

9、一种用于验证数字证书有效性的鉴别服务器，其包括消息接收模块、数字证书验证模块，其特征在于，所述数字证书验证模块包括验证方案配置单元；

所述消息接收模块用于接收数字证书鉴别请求分组；

所述验证方案配置单元用于配置验证数字证书有效性的验证方案。

10、一种如权利要求 9 所述的鉴别服务器，其特征在于，所述验证方案配置单元进一步包括白名单列表验证子单元，所述白名单列表验证子单元用于验证所述数字证书鉴别请求分组中的数字证书是否包含在白名单内。

11、一种如权利要求 9 所述的鉴别服务器，其特征在于，所述验证方案配置单元进一步包括黑名单列表验证子单元，所述黑名单列表验证子单元用于验

证所述数字证书鉴别请求分组中的数字证书是否包含在黑名单内。

12、一种如权利要求 9 所述的鉴别服务器，其特征在于，所述验证方案配置单元进一步包括数字证书格式和吊销状态验证子单元，所述数字证书格式和吊销状态验证子单元用于验证所述数字证书的信息格式是否与所述鉴别服务器已知的格式一致。

13、一种如权利要求 9 所述的鉴别服务器，其特征在于，所述验证方案配置单元进一步包括数字证书使用范围验证子单元，所述数字证书使用范围验证子单元用以验证所述数字证书鉴别请求分组中包含的数字证书是否符合数字证书颁发时候规定的使用范围。

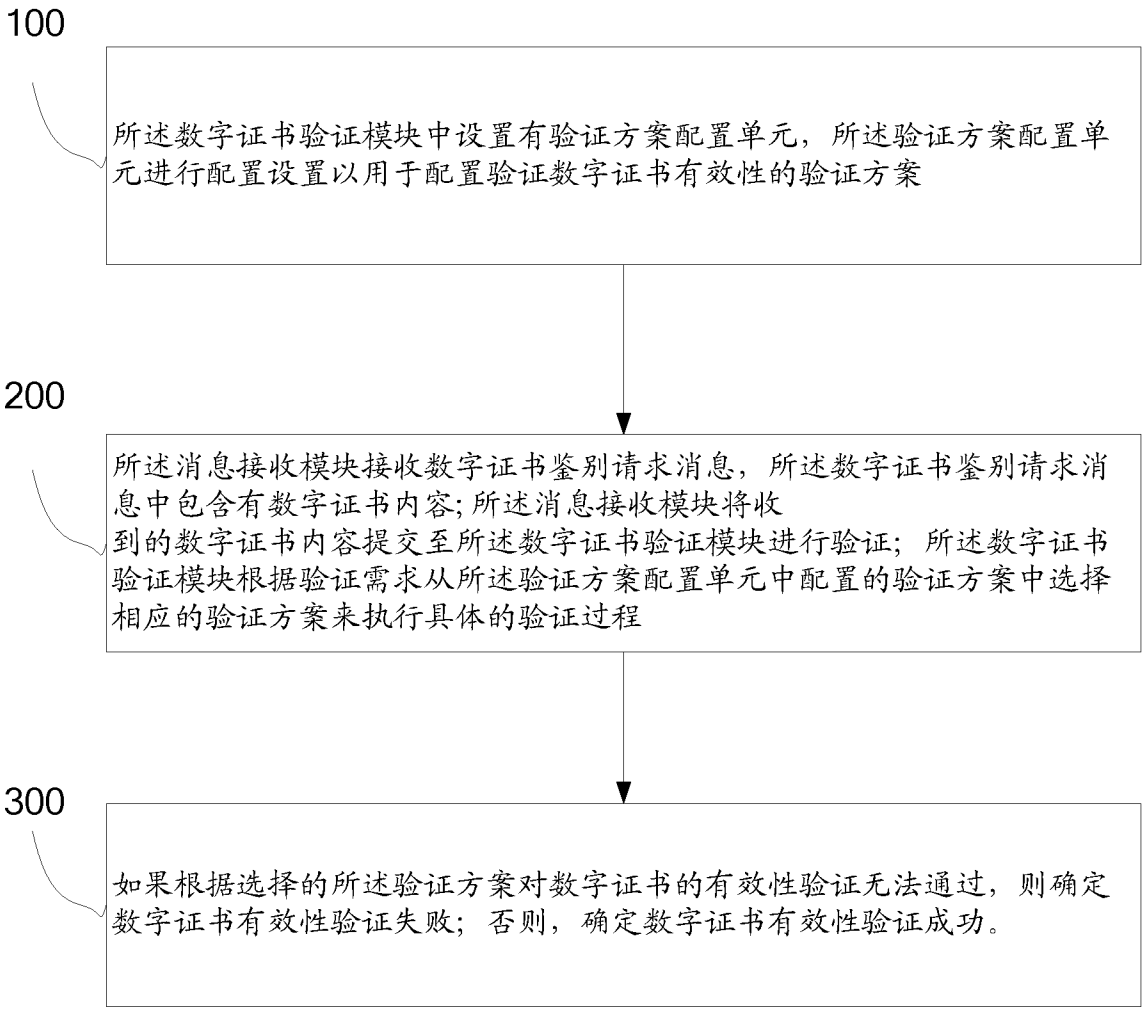
100
所述数字证书验证模块中设置有验证方案配置单元，所述验证方案配置单元进行配置设置以用于配置验证数字证书有效性的验证方案
200
所述消息接收模块接收数字证书鉴别请求消息，所述数字证书鉴别请求消息中包含有数字证书内容;所述消息接收模块将收到的数字证书内容提交至所述数字证书验证模块进行验证；所述数字证书验证模块根据验证需求从所述验证方案配置单元中配置的验证方案中选择相应的验证方案来执行具体的验证过程
300
如果根据选择的所述验证方案对数字证书的有效性验证无法通过，则确定数字证书有效性验证失败；否则，确定数字证书有效性验证成功。

图 1

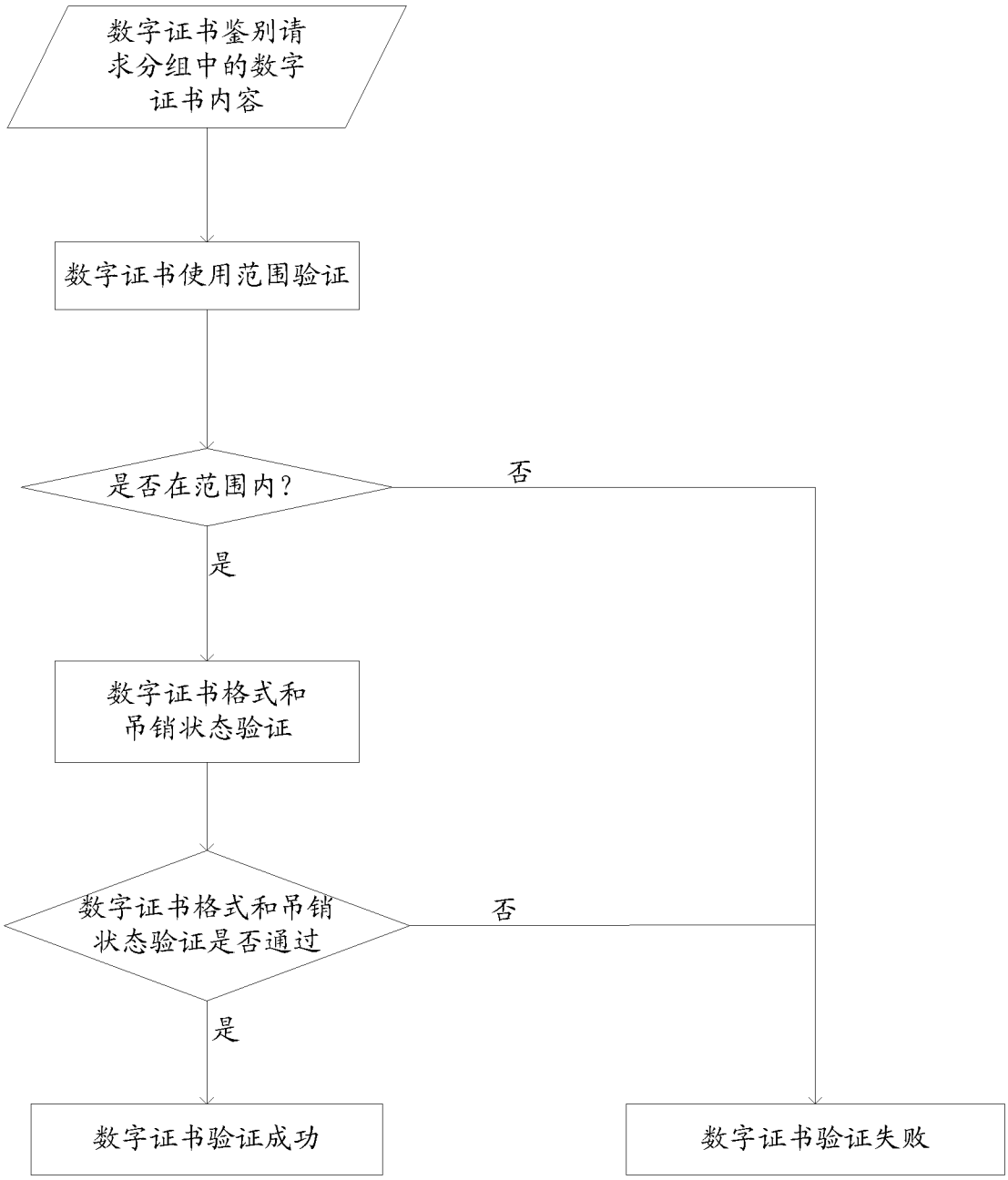
数字证书鉴别请求分组中的数字证书内容
数字证书使用范围验证
是否在范围内？
否
是
数字证书格式和吊销状态验证
数字证书格式和吊销状态验证是否通过
否
是
数字证书验证成功
数字证书验证失败

图 2

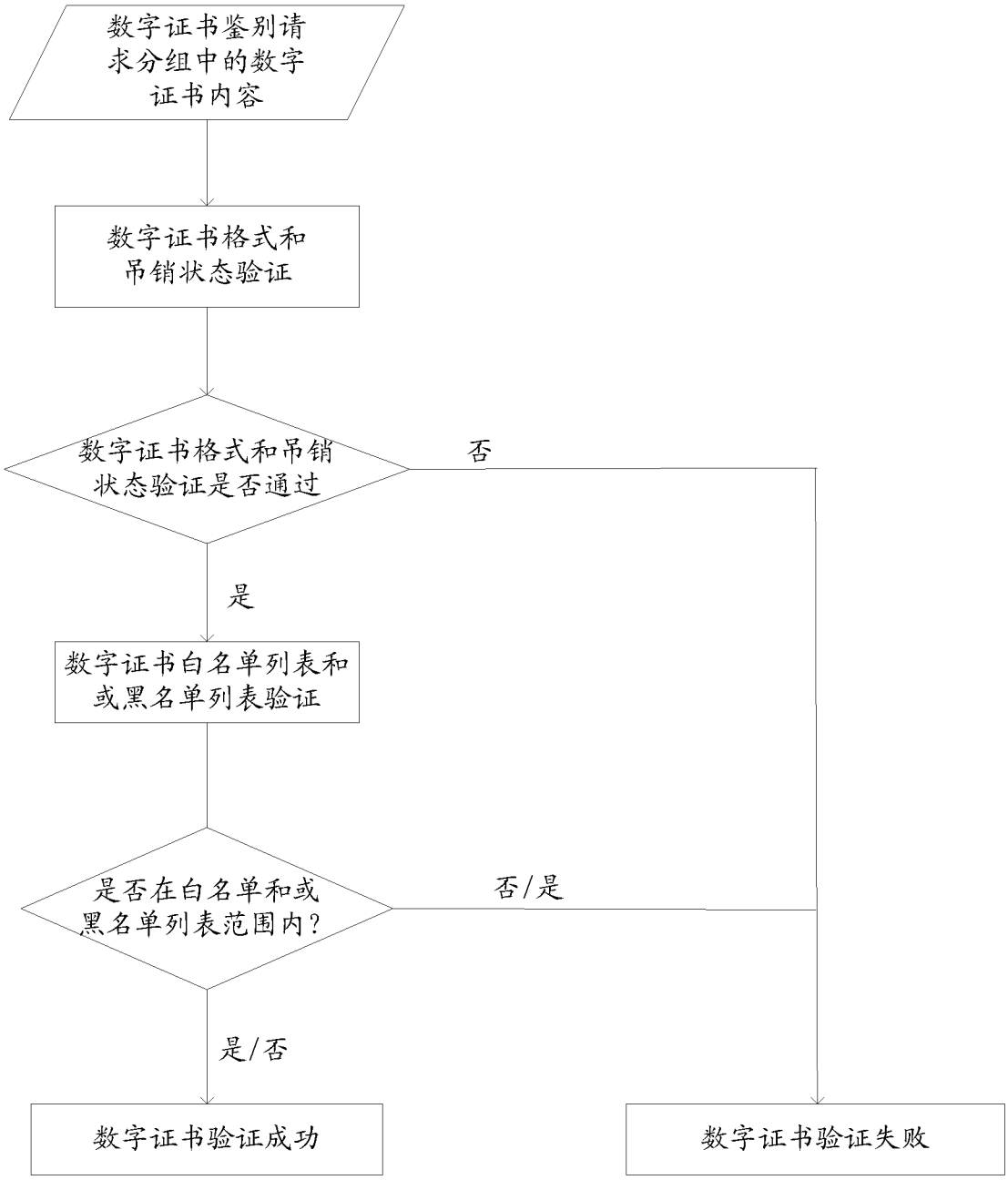
数字证书鉴别请求分组中的数字证书内容
数字证书格式和吊销状态验证
数字证书格式和吊销状态验证是否通过
否
是
数字证书白名单列表和或黑名单列表验证
是否在白名单和或黑名单列表范围内？
否/是
是/否
数字证书验证成功
数字证书验证失败

图 3

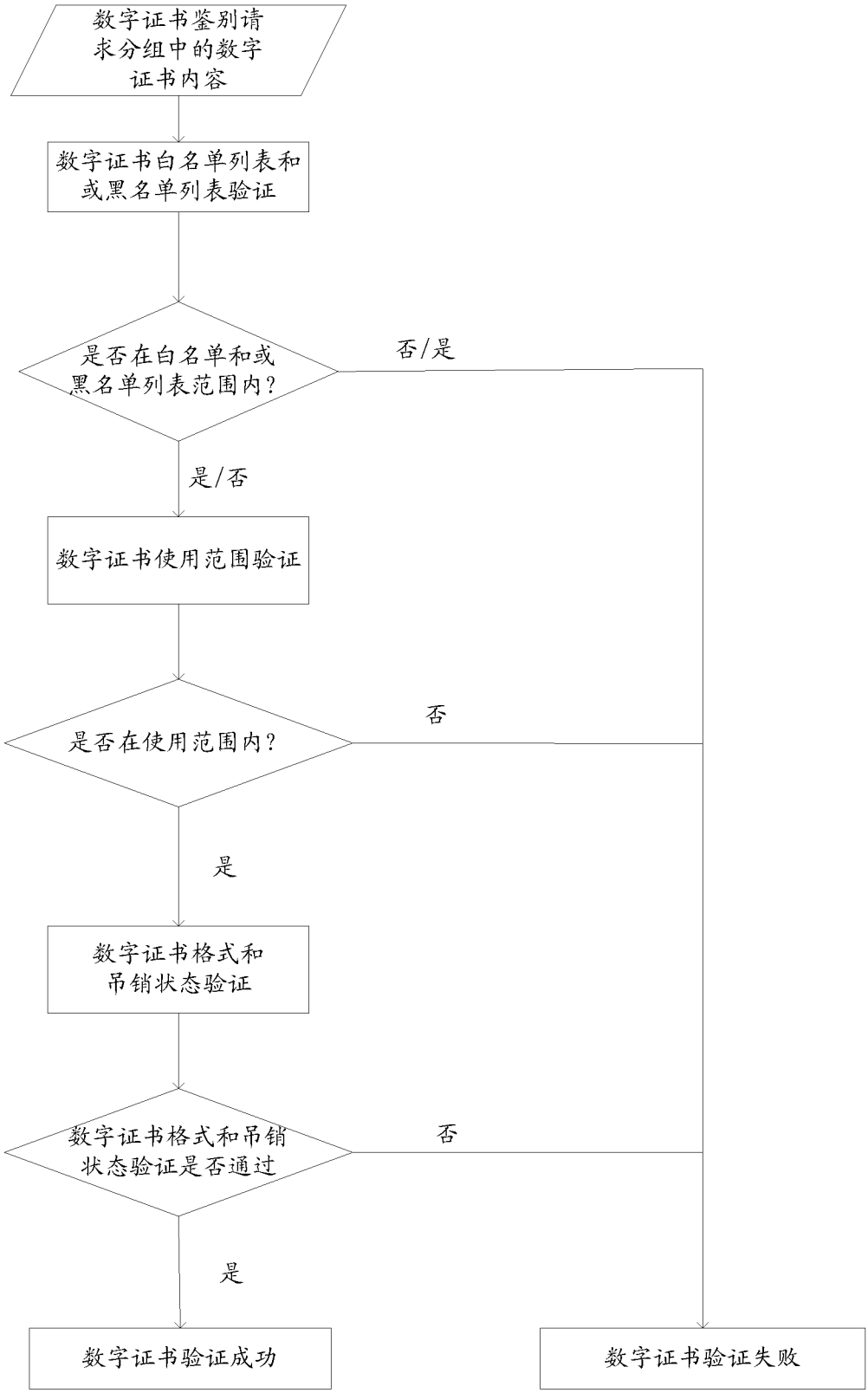
数字证书鉴别请求分组中的数字证书内容
数字证书白名单列表和或黑名单列表验证
是否在白名单和或黑名单列表范围内？
否/是
是/否
数字证书使用范围验证
是否在使用范围内？
否
是
数字证书格式和吊销状态验证
数字证书格式和吊销状态验证是否通过
否
是
数字证书验证成功
数字证书验证失败

图 4

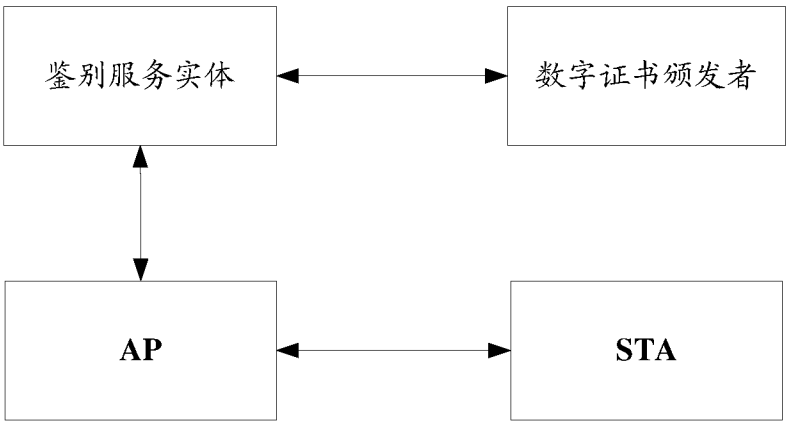
鉴别服务实体
数字证书颁发者
AP
STA

图 5

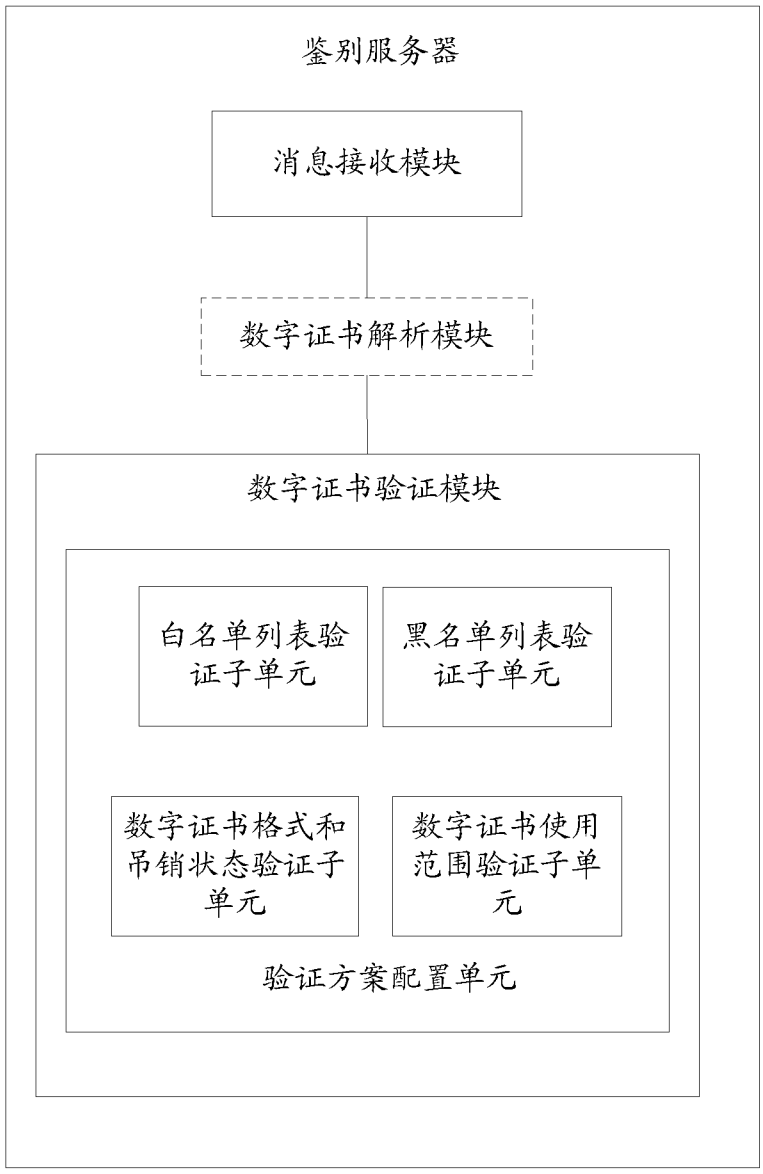
鉴别服务器
消息接收模块
数字证书解析模块
数字证书验证模块
白名单列表验证子单元
黑名单列表验证子单元
数字证书格式和吊销状态验证子单元
数字证书使用范围验证子单元
验证方案配置单元

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/081665

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i; H04L 29/06 (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 G06F

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)

WPI, EPODOC, CNKI, CNPAT, GOOGLE: CA, PKI, validation, validate, verification, verify, authentication server, authentication service entity, AS, revocation, certificate, valid, invalid, CRL, level, domain, scheme, mode, model, policy, hierarchical, cancel, white, black, list, range, rank, iwncomm

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102638346 A (HANGZHOU DPTECH TECHNOLOGIES CO., LTD.) 15 August 2012 (15.08.2012) description, paragraphs [0001]-[0004], [0015]-[0036] and figure 1	1-13
A	CN 102811218 A (JIANGSU ELECTRONIC COMMERCE SERVICE CENTER CO., LTD.) 05 December 2012 (05.12.2012) description, paragraphs [0030]-[0050] and figures 1 and 2	1-13
A	CN 102439898 A (MICROSOFT CORP) 02 May 2012 (02.05.2012) the whole document	1-13
A	US 2004030888 A1 (ROH JONG HYUK et al.) 12 February 2004 (12.02.2004) the whole document	1-13
A	US 2006200854 A1 (SAITO SHINICHI) 07 September 2006 (07.09.2006) the whole document	1-13
A	HE, Guofeng et al. "High Performance CA Authentication Solution" Applications of The Computer Systems, 30 June 2001 (30.06.2001) sections 2-4	1-13

☐ 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
18 July 2016	26 July 2016
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 LIU, Yi Telephone No. (86-10) 62413400

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/081665

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102638346 A	15 August 2012	CN 102638346 B	10 September 2014
CN 102811218 A	05 December 2012	CN 102811218 B	31 July 2013
CN 102439898 A	02 May 2012	JP 2012527703 A	08 November 2012
		AU 2010249698 B2	30 October 2014
		EP 2433390 A2	28 March 2012
		RU 2011147179 A	27 May 2013
		CA 2758579 A1	25 November 2010
		BR PI1014776 A2	19 April 2016
		KR 20120023679 A	13 March 2012
		AU 2010249698 A1	03 November 2011
		CN 102439898 B	20 April 2016
		WO 2010135292 A2	25 November 2010
		US 2010299716 A1	25 November 2010
		WO 2010135292 A3	03 February 2011
US 2004030888 A1	12 February 2004	KR 100431210 B1	12 May 2004
		KR 20040013668 A	14 February 2004
		US 7478236 B2	13 January 2009
US 2006200854 A1	07 September 2006	JP 2006244081 A	14 September 2006
		CN 1829148 A	06 September 2006

国际检索报告

国际申请号
PCT/CN2016/081665

A. 主题的分类

H04L 9/32(2006.01)i；H04L 29/06(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 G06F

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））

WPI, EPODOC, CNKI, CNPAT, GOOGLE: 验证，认证，鉴别，鉴权，证书，CA，PKI，有效，无效，失效，注销，吊销，白名单，黑名单，范围，级别，等级，分级，方案，策略，西电捷通，validation，validate，verification，verify，authentication server，authentication service entity，AS，revocation，certificate，valid，invalid，CRL，level，domain，scheme，mode，model，policy，hierarchical

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
X	CN 102638346 A (杭州迪普科技有限公司) 2012年 8月 15日 (2012 - 08 - 15) 说明书第[0001]-[0004]，[0015]-[0036]段，图1	1-13
A	CN 102811218 A (江苏省电子商务服务中心有限责任公司) 2012年 12月 5日 (2012 - 12 - 05) 说明书第[0030]-[0050]段，图1-2	1-13
A	CN 102439898 A (微软公司) 2012年 5月 2日 (2012 - 05 - 02) 全文	1-13
A	US 2004030888 A1 (ROH JONG HYUK 等) 2004年 2月 12日 (2004 - 02 - 12) 全文	1-13
A	US 2006200854 A1 (SAITO SHINICHI) 2006年 9月 7日 (2006 - 09 - 07) 全文	1-13
A	何国锋 等. "高性能CA认证解决方案" 计算机系统应用，2001年 6月 30日 (2001 - 06 - 30)， 第2-4节	1-13

☐ 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
2016年 7月 18日	2016年 7月 26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 刘毅 电话号码 (86-10)62413400

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/081665

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	102638346	A	2012年 8月 15日	CN	102638346	B	2014年 9月 10日
CN	102811218	A	2012年 12月 5日	CN	102811218	B	2013年 7月 31日
CN	102439898	A	2012年 5月 2日	JP	2012527703	A	2012年 11月 8日
				AU	2010249698	B2	2014年 10月 30日
				EP	2433390	A2	2012年 3月 28日
				RU	2011147179	A	2013年 5月 27日
				CA	2758579	A1	2010年 11月 25日
				BR	PI1014776	A2	2016年 4月 19日
				KR	20120023679	A	2012年 3月 13日
				AU	2010249698	A1	2011年 11月 3日
				CN	102439898	B	2016年 4月 20日
				WO	2010135292	A2	2010年 11月 25日
				US	2010299716	A1	2010年 11月 25日
				WO	2010135292	A3	2011年 2月 3日
US	2004030888	A1	2004年 2月 12日	KR	100431210	B1	2004年 5月 12日
				KR	20040013668	A	2004年 2月 14日
				US	7478236	B2	2009年 1月 13日
US	2006200854	A1	2006年 9月 7日	JP	2006244081	A	2006年 9月 14日
				CN	1829148	A	2006年 9月 6日