

(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



(10) 国际公布号

WO 2020/119037 A1

(43) 国际公布日
2020 年 6 月 18 日 (18.06.2020)

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2019/089183
- (22) 国际申请日: 2019 年 5 月 30 日 (30.05.2019)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201811518453.8 2018 年 12 月 12 日 (12.12.2018) CN
- (71) 申请人: 平安科技(深圳)有限公司(PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518033 (CN)。
- (72) 发明人: 吴春海(WU, Chunhai); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518033 (CN)。 谭智文(TAN, Zhiwen); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中

心 23 楼, Guangdong 518033 (CN)。 王峰(WANG, Feng); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518033 (CN)。 李国颂(LI, Guosong); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518033 (CN)。

(74) 代理人: 北京鸿元知识产权代理有限公司 (GRANDER IP LAW FIRM); 中国北京市朝阳区光华路 7 号汉威大厦东区 18A6 室, 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, 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, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: IDENTITY AUTHENTICATION CONFIGURATION METHOD AND DEVICE AND COMPUTER READABLE STORAGE MEDIUM

(54) 发明名称: 一种身份验证配置方法、装置及计算机可读存储介质

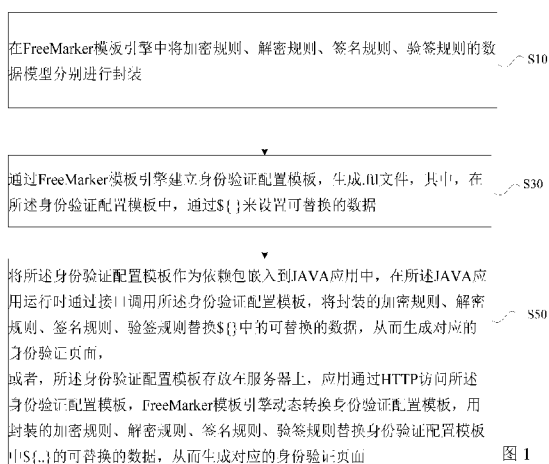


图 1

S10 Encapsulate data models for encryption, decryption, signature and signature verification rules respectively in a FreeMarker template engine
S30 Establish an identity authentication configuration template by means of the FreeMarker template engine, generate an .ftl file, wherein, in the identity authentication configuration template, replaceable data are configured by means of \${}
S50 Embed the identity authentication configuration template as a dependency package into a Java application, the Java application calling the identity authentication configuration template when running by means of an interface to replace the replaceable data in \${} with encryption rules, decryption rules, signature rules and signature verification rules, thereby generating a corresponding identity authentication page;
or, the identity authentication configuration template exists on a server, the application accesses the identity authentication configuration template by means of HTTP, and the FreeMarker template engine dynamically converts the identity authentication configuration template and replaces the replaceable data of \${} in the identity authentication configuration template with the encapsulated encryption, decryption, signature and signature verification rules, thereby generating the corresponding identity authentication page

(57) Abstract: The present solution relates to the field of information security, and provided thereby are an identity authentication configuration method and device and a computer readable storage medium. The method comprises: encapsulating data models for encryption, decryption, signature and signature verification rules respectively in a template engine; establishing an identity authentication configuration template, and configuring replaceable data by means of \${}; embedding the identity authentication configuration template as a dependency package into a Java application, and the Java application calling the identity authentication configuration template by means of an interface to replace the replaceable data in \${} with encryption rules, decryption rules, signature rules and signature verification rules to form identity authentication rules; or the identity authentication configuration template existing on a server, and the Java application accessing the identity authentication configuration template by means of HTTP and replacing the replaceable data of \${} in the identity authentication configuration template with the encapsulated encryption, decryption, signature and signature verification rules to form the identity authentication rules. The present application does not require repeated code development and reduces workload.

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))。

(57) 摘要: 本方案涉及信息安全领域, 提供一种身份验证配置方法、装置及计算机可读存储介质, 方法包括: 在模板引擎中将加密、解密、签名、验签规则的数据模型分别封装; 建立身份验证配置模板, 通过\${}设置可替换的数据; 将身份验证配置模板作为依赖包嵌入到JAVA应用中, 在JAVA应用通过接口调用身份验证配置模板, 使加密规则、解密规则、签名规则、验签规则替换\${}中可替换的数据, 形成身份认证规则, 或, 身份验证配置模板存在服务器上, JAVA应用通过HTTP访问身份验证配置模板, 用封装的加密、解密、签名、验签规则替换身份验证配置模板中\${}的可替换的数据, 形成身份认证规则。本申请不需要重复的代码开发, 减少工作量。

一种身份验证配置方法、装置及计算机可读存储介质

技术领域

本申请涉及信息安全技术领域，具体地说，涉及一种身份验证配置方法、装置及计算机可读存储介质。

背景技术

现在普遍采用数字签名的方式进行身份认证。对于一些较新的系统，一般采用标准 Basic Auth、OAuth、HMAC 等方式实现身份认证。但对于一些较旧的业务系统，很多都采用了自定义的身份认证方案。这使得这些业务系统之间的互相访问变得复杂——交互双方都需要按照对方的身份认证方式进行开发，而认证的规则往往与具体的业务相关。因此虽然身份认证的代码具有很大的相似度，但是又不是完全相同，几乎每次对接都需要进行身份认证的代码开发。因此虽然身份认证的代码具有很大的相似度，但是又不是完全相同，因此几乎每次对接都需要进行身份认证的代码开发。

发明内容

为解决现有技术存在的不足，本申请提供一种身份验证配置方法，应用于电子装置，该方法包括：在 FreeMarker 模板引擎中将加密规则、解密规则、签名规则、验签规则的数据模型分别进行封装；通过 FreeMarker 模板引擎建立身份验证配置模板，生成.ftl 文件，其中，在所述身份验证配置模板中，通过插值符号\${ }来设置可替换的数据；将所述身份验证配置模板作为依赖包嵌入到 JAVA 应用中，在所述 JAVA 应用运行时通过接口调用所述身份验证配置模板，使封装的加密规则、解密规则、签名规则、验签规则替换插值符号\${ }中的可替换的数据，从而形成相应的身份认证规则，或者，所述身份验证配置模板存放在服务器上，JAVA 应用通过 HTTP 访问所述身份验证配置模板，FreeMarker 模板引擎动态转换身份验证配置模板，用封装的加密规则、解密规则、签名规则、验签规则替换身份验证配置模板中\${..}的可替换的数据，

从而形成相应的身份认证规则。

优选地，利用 FreeMarker 模板引擎建立身份验证配置模板的步骤包括：新建 Maven 项目；修改.xml 配置文件，增加 freemark 依赖；在 src/main/java 的包下添加目录，用于存放所有的 freemarker 模板；在 src/main/java/templates 目录下添加以.ftl 文件形式存在的 FreeMarker 模板。

优选地，JAVA应用设置有对应加密规则、解密规则、签名规则、验签规则的选择框。

优选地，加密规则、解密规则采用的算法至少包括MD5、RSA、DES、AES、Base64。

优选地，签名规则、验签规则采用的算法至少包括RSA、DSA和ECDSA。

优选地，AES具有CBC、CFB、ECB、OFB、PCBC5种模式，AES具有三种填充方式：NoPadding、PKCS5Padding、ISO10126Padding。

本申请还提供一种电子装置，所述电子装置包括存储器及与所述存储器连接的处理器，所述存储器中存储有可在所述处理器上运行的身份验证配置程序，所述身份验证配置程序被所述处理器执行时实现如下步骤：在 FreeMarker模板引擎中将加密规则、解密规则、签名规则、验签规则的数据模型分别进行封装；通过FreeMarker模板引擎建立身份验证配置模板，生成.ftl 文件，其中，在所述身份验证配置模板中，通过\${ }来设置可替换的数据；将所述身份验证配置模板作为依赖包嵌入到JAVA应用中，在所述JAVA应用运行时通过接口调用所述身份验证配置模板，将封装的加密规则、解密规则、签名规则、验签规则替换\${ }中的可替换的数据，从而生成对应的身份验证页面，或者，所述身份验证配置模板存放在服务器上，应用通过HTTP访问所述身份验证配置模板，FreeMarker模板引擎动态转换身份验证配置模板，用封装的加密规则、解密规则、签名规则、验签规则替换身份验证配置模板中\${.}的可替换的数据，从而生成对应的身份验证页面。

优选地，利用FreeMarker模板引擎建立身份验证配置模板的步骤包括：新建Maven项目；修改.xml配置文件，增加freemark依赖；在src/main/java的包下添加templates（模板）目录，用于存放所有的freemarker模板；在 src/main/java/templates目录下添加.ftl的FreeMarker模板。

优选地，加密规则、解密规则采用的算法至少包括MD5、RSA、DES、

AES、Base64；签名规则、验签规则采用的算法至少包括RSA、DSA和ECDSA。

本申请还提供一种计算机可读存储介质，所述计算机可读存储介质中包括身份验证配置程序，所述身份验证配置程序被处理器执行时，实现如上所述的身份验证配置方法的步骤。

采用本申请身份验证配置方法、装置及计算机可读存储介质，无论是客户端、开放平台还是服务方，都可以通过将各种加密规则、解密规则、签名规则、验签规则的数据模型的封装配置在应用中的形式，来选择对接双方都认可的加密规则、解密规则、签名规则、验签规则。不需要重复的代码开发，可以减少由于大量重复代码开发造成的出错率高的问题，可以避免版本发布的流程，实时进行更新。通过配置的方式，解决 API 开放平台在接入新的服务提供方过程中的开发问题，真正实现在线接入零开发。

附图说明

通过结合下面附图对其实施例进行描述，本申请的上述特征和技术优点将会变得更加清楚和容易理解。

图 1 是表示本申请实施例的身份验证配置方法的流程图；

图 2 是表示本申请实施例的电子装置的硬件架构示意图；

图 3 是表示本申请实施例的身份验证配置程序的模块构成图；

图 4 是表示本申请实施例的身份认证规则封装模块的单元构成图。

具体实施方式

下面将参考附图来描述本申请所述的身份验证配置方法、装置及计算机可读存储介质的实施例。本领域的普通技术人员可以认识到，在不偏离本申请的精神和范围的情况下，可以用各种不同的方式或其组合对所描述的实施例进行修正。因此，附图和描述在本质上是说明性的，而不是用于限制权利要求的保护范围。此外，在本说明书中，附图未按比例画出，并且相同的附图标记表示相同的部分。

一种身份验证配置方法，如图 1 所示，包括以下步骤：

步骤S10，在FreeMarker模板引擎中将加密规则、解密规则、签名规则、验签规则的数据模型分别进行封装，以便在后期替换插值符号\${ }中的内容，

从而生成对应的身份验证页面。

步骤 S30, 通过 FreeMarker 模板引擎建立身份验证配置模板, 生成.ftl 文件。FreeMarker 是一种基于模板和要改变的数据的模板引擎, 可以用来生成 HTML 网页、电子邮件、配置文件、源代码等输出文本。模板和数据模型是 FreeMarker 生成输出所需的组成部分, 其中, 在所述身份验证配置模板中, 通过插值符号\${ }来设置可替换的数据;

步骤 S50, 将所述身份验证配置模板作为依赖包嵌入到 JAVA 应用中, 在所述 JAVA 应用运行时通过接口调用所述身份验证配置模板, 将封装的加密规则、解密规则、签名规则、验签规则替换插值符号\${ }中的可替换的数据, 从而进行不同形式的身份验证。例如, 通常需要身份认证的可能包括三方: 客户端(服务使用者)、开放平台(中间服务平台)、服务方(服务提供方), 客户端通过开放平台调用服务提供者的服务。在通讯过程中, 三方都需要解决身份认证与数据安全问题。客户端调用开放平台, 开放平台需要验签解密; 开放平台调用服务方, 需要加签加密; 开放平台调用服务方, 服务方返回结果后, 需要验签解密; 开放平台调用服务方, 服务方返回结果后, 开放平台将结果返回给客户端之前, 需要进行加签加密。

下面以开放平台和服务方之间的身份认证来说明。开放平台和服务方之间需要采用一种身份认证方式, 所述身份认证方式包括加密规则、解密规则、签名规则、验签规则。所述 JAVA 应用可以是该开放平台上的应用, JAVA 应用是通过建立.java 类形成。java 类中可以设置选择加密规则、解密规则、签名规则、验签规则的一些模块, 例如按钮、勾选框等。开放平台和服务方之间则可以通过开放平台上的 JAVA 应用选择适合的加密规则、解密规则、签名规则、验签规则。而在选择之后, java 应用则利用 API 接口调用以依赖包形式嵌入在 java 应用中的身份验证配置模板, 由于身份验证配置模板中设置有关于加密规则、解密规则、签名规则、验签规则的封装, 并且还通过\${ }设置有可替换的数据。Java 应用调用身份验证配置模板, 使得选择的加密规则、解密规则、签名规则、验签规则替换\${ }中的可替换数据, 从而形成适于开放平台和服务方之间的身份认证规则。服务方与开放平台之间的通讯则采用所配置的加密规则、解密规则、签名规则、验签规则来完成身份认证。

或者, 所述身份验证配置模板还可以是存放在独立的服务器上, JAVA应

用可以通过HTTP访问所述身份验证配置模板，例如，开放平台上的应用通过HTTP访问所述身份验证配置模板。JAVA应用可以设置选择加密规则、解密规则、签名规则、验签规则的一些模块，例如按钮、勾选框等。开放平台和服务方之间则可以通过开放平台上的应用选择适合的加密规则、解密规则、签名规则、验签规则。应用HTTP访问所述身份验证配置模板，FreeMarker模板引擎动态转换身份验证配置模板，用封装的加密规则、解密规则、签名规则、验签规则替换身份验证配置模板中\${..}的可替换的数据，从而形成适于开放平台和服务方之间的身份认证规则。

通过以上的身份验证配置方法，开发者可以免去繁杂的大量重复的代码开发工作，可以配置不同的身份验证规则，能够适用于开放平台、服务方、用户之间的身份验证。

下面说明一下FreeMarker模板引擎建立身份验证配置模板的具体步骤：

首先新建一个Maven项目；

修改.xml配置文件，增加freemark依赖；

在src/main/java的包下添加一个名为“templates”目录，用于存放所有的freemarker模板；

在src/main/java/templates目录下添加名为“product.ftl”的FreeMarker模板，其中，

模板的内容可以是包括如下内容：

加密规则：\${Encryption rules}

解密规则：\${Decryption rules}

签名规则：\${Signature rule}

验签规则：\${ Inspection rules}。

使用FreeMarker可以读取到模板内容，将选择的加密规则、解密规则、签名规则、验签规则替换对应的\${ }中的内容，FreeMarker将数据与身份验证配置模板绑定并渲染出对应的身份认证页面。

优选地，加密规则、解密规则采用的算法至少包括MD5（消息摘要算法第五版）、RSA（非对称加密算法）、DES（数据加密标准，是一种使用密钥加密的块算法）、AES（高级加密标准）、Base64（一种基于64个可打印字符来表示二进制数据的方法）。

优选地，签名规则、验签规则采用的算法至少包括RSA（非对称加密算法）、DSA（驾驶安全预警与导航系统）和ECDSA（椭圆曲线数字签名算法）。

将各种签名规则、加密规则、解密规则、验签规则分别对应封装。例如，签名规则的算法为SHA256WithRSA，加密规则的算法是RES，模式是CFB，填充方式是PKCS5Padding。通过在FreeMarker中设置插值符号\${}，利用正则表达式搜索插值符号\${ }，并将其中的内容替换为对应的封装的签名规则、加密规则、解密规则、验签规则。从而形成能够适用于不同应用场景的身份验证页面。

其中，AES具有CBC（密码分组链接模式）、CFB（密文反馈模式）、ECB（电子密码本模式）、OFB（输出反馈模式）、PCBC（填充密码块链接）5种模式。AES支持三种填充：NoPadding，PKCS5Padding，ISO10126Padding。则可以形成不同的封装，例如，签名规则的算法为RSA，加密规则的算法是AES，模式是ECB，填充方式是ISO10126Padding。

图2所示是本申请电子装置1的硬件架构示意图。所述电子装置1是一种能够按照事先设定或者存储的指令，自动进行数值计算和/或信息处理的设备。所述电子装置1可以是计算机、也可以是单个网络服务器、多个网络服务器组成的服务器组或者基于云计算的由大量主机或者网络服务器构成的云，其中云计算是分布式计算的一种，由一群松散耦合的计算机集组成的一个超级虚拟计算机。

在本实施例中，电子装置1可包括，但不仅限于，可通过系统总线相互通信连接的存储器13、处理器14、显示器15。需要指出的是，图2仅示出了具有部分组件的电子装置1，但是应理解的是，并不要求实施所有示出的组件，可以替代的实施更多或者更少的组件。

其中，主存储器13包括内存及至少一种类型的可读存储介质。内存为电子装置1的运行提供缓存；可读存储介质可为如闪存、硬盘、多媒体卡、卡型存储器（例如，SD或DX存储器等）、随机访问存储器（RAM）、静态随机访问存储器（SRAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、可编程只读存储器（PROM）、磁性存储器、磁盘、光盘等的非易失性存储介质。在一些实施例中，可读存储介质可以是电子装置1的内部存储单元，例如该电子装置1的硬盘；在另一些实施例中，该非易失性存储介质也可以是电子

装置 1 的外部存储设备，例如电子装置 1 上配备的插接式硬盘，智能存储卡(Smart Media Card)，安全数字(Secure Digital)卡，闪存卡(Flash Card)等。本实施例中，存储器 13 的可读存储介质通常用于存储安装于电子装置 1 的操作系统和各类应用软件，例如本实施例中的身份验证配置程序代码等。此外，存储器 13 还可以用于暂时地存储已经输出或者将要输出的各类数据。

所述处理器 14 用于运行所述存储器 13 中存储的程序代码或者处理数据。

另外，电子装置 1 还包括网络接口，所述网络接口可包括无线网络接口或有线网络接口，该网络接口通常用于在所述电子装置 1 与其他电子设备之间建立通信连接。

身份验证配置程序存储在存储器 13 中，包括至少一个存储在存储器 13 中的计算机可读指令，该至少一个计算机可读指令可被处理器执行，以实现本申请各实施例的方法；以及，该至少一个计算机可读指令依据其各部分所实现的功能不同，可被划为不同的逻辑模块。

在一个实施例中，上述身份验证配置程序被所述处理器 14 执行时实现如下步骤：

步骤S10，在FreeMarker模板引擎中将加密规则、解密规则、签名规则、验签规则的数据模型分别进行封装，以便在后期替换\${ }中的内容，从而生成对应的身份验证页面。

步骤 S30，通过 FreeMarker 模板引擎建立身份验证配置模板，生成.ftl 文件。FreeMarker 是一种基于模板和要改变的数据的模板引擎，可以用来生成 HTML 网页、电子邮件、配置文件、源代码等输出文本。模板和数据模型是 FreeMarker 生成输出所需的组成部分，其中，在所述身份验证配置模板中，通过\${ }来设置可替换的数据；

步骤 S50，将所述身份验证配置模板作为依赖包嵌入到 JAVA 应用中，在所述 JAVA 应用运行时通过接口调用所述身份验证配置模板，将封装的加密规则、解密规则、签名规则、验签规则替换\${ }中的可替换的数据，从而进行不同形式的身份验证。

或者，所述身份验证配置模板还可以是存放在独立的服务器上，应用可以通过HTTP访问所述身份验证配置模板，例如，开放平台上的应用通过HTTP访问所述身份验证配置模板。应用可以设置选择加密规则、解密规则、签名

规则、验签规则的一些模块，例如按钮、勾选框等。开放平台和服务方之间则可以通过开放平台上的应用选择适合的加密规则、解密规则、签名规则、验签规则。应用HTTP访问所述身份验证配置模板，FreeMarker模板引擎动态转换身份验证配置模板，用封装的加密规则、解密规则、签名规则、验签规则替换身份验证配置模板中\${.}的可替换的数据，从而形成适于开放平台和服务方之间的身份认证规则。

图3所示为身份验证配置程序50的程序模块图。在本实施例中，身份验证配置程序50被分割为多个模块，该多个模块被存储于存储器13中，并由处理器14执行，以完成本申请。本申请所称的模块是指能够完成特定功能的一系列计算机程序指令段。

所述身份验证配置程序50可以被分割为：身份认证规则封装模块501、模板建立模块502、身份验证配置模板处理模块503，

其中，身份认证规则封装模块501用于在FreeMarker模板引擎中将加密规则、解密规则、签名规则、验签规则的数据模型分别进行封装，以便在后期替换\${ }中的内容，从而生成对应的身份验证页面。

其中，模板建立模块 502 通过 FreeMarker 模板引擎建立身份验证配置模板，生成.ftl 文件。FreeMarker 是一种基于模板和要改变的数据的模板引擎，可以用来生成 HTML 网页、电子邮件、配置文件、源代码等输出文本。模板和数据模型是 FreeMarker 生成输出所需的组成部分，其中，在所述身份验证配置模板中，通过\${ }来设置可替换的数据。

其中，身份验证配置模板处理模块 503 将所述身份验证配置模板作为依赖包嵌入到 JAVA 应用中，在所述 JAVA 应用运行时通过接口调用所述身份验证配置模板，将封装的加密规则、解密规则、签名规则、验签规则替换\${ }中的可替换的数据，从而进行不同形式的身份验证。

下面以开放平台和服务方之间的身份认证来说明。开放平台和服务方之间需要采用一种身份认证方式，所述身份认证方式包括加密规则、解密规则、签名规则、验签规则。所述 JAVA 应用可以是该开放平台上的应用，JAVA 应用是通过建立.java 类形成。java 类中可以设置选择加密规则、解密规则、签名规则、验签规则的一些模块，例如按钮、勾选框等。开放平台和服务方之间则可以通过开放平台上的 JAVA 应用选择适合的加密规则、解密规则、签名

规则、验签规则。而在选择之后，java 应用则利用 API 接口调用以依赖包形式嵌入在 java 应用中的身份验证配置模板，由于身份验证配置模板中设置有关于加密规则、解密规则、签名规则、验签规则的封装，并且还通过\${ } 设置有可替换的数据。Java 应用调用身份验证配置模板，使得选择的加密规则、解密规则、签名规则、验签规则替换\${ } 中的可替换数据，从而形成适于开放平台和服务方之间的身份认证规则。服务方与开放平台之间的通讯则采用所配置的加密规则、解密规则、签名规则、验签规则来完成身份认证。

或者，身份验证配置模板处理模块503还可以将所述身份验证配置模板存放在独立的服务器上，应用可以通过HTTP访问所述身份验证配置模板，例如，开放平台上的应用通过HTTP访问所述身份验证配置模板。应用可以设置选择加密规则、解密规则、签名规则、验签规则的一些模块，例如按钮、勾选框等。开放平台和服务方之间则可以通过开放平台上的应用选择适合的加密规则、解密规则、签名规则、验签规则。应用HTTP访问所述身份验证配置模板，FreeMarker模板引擎动态转换身份验证配置模板，用封装的加密规则、解密规则、签名规则、验签规则替换身份验证配置模板中\${..}的可替换的数据，从而形成适于开放平台和服务方之间的身份认证规则。

优选地，模板建立模块502通过FreeMarker模板引擎建立身份验证配置模板的具体步骤如下：

首先新建一个Maven项目；

修改.xml配置文件，增加freemark依赖；

在src/main/java的包下添加一个名为“templates”目录，用于存放所有的freemarker模板；

在src/main/java/templates目录下添加名为“product.ftl”的FreeMarker模板，其中，

模板的内容可以是包括如下内容：

加密规则：\${Encryption rules}

解密规则：\${Decryption rules}

签名规则：\${Signature rule}

验签规则：\${ Inspection rules}。

使用FreeMarker可以读取到模板内容，将数据与模板绑定并渲染出对应的

身份认证页面。具体说，根据不同的加密规则、解密规则、签名规则、验签规则的封装，替换\${ }的内容，从而实现不同的加密规则、解密规则、签名规则、验签规则。

优选地，如图4所示，身份认证规则封装模块501包括签名规则封装单元5011、加密规则封装单元5012、解密规则封装单元5013、验签规则封装单元5014。所述签名规则封装单元5011用于将各种签名规则进行封装，加密规则封装单元5012用于对各种解密规则进行封装。解密规则封装单元5013用于对各种解密规则进行封装、验签规则封装单元5014用于对各种验签规则进行封装。

优选地，加密规则、解密规则采用的算法至少包括MD5、RSA、DES、AES、Base64。

优选地，签名规则、验签规则采用的算法至少包括RSA、DSA和ECDSA。

优选地，身份验证配置模板处理模块503采用正则表达式搜索插值符号\${ }，并将所选择的签名规则、加密规则、解密规则、验签规则替换掉插值符号\${ }中的可替换内容。

优选地，FreeMarker模板引擎中的身份验证配置模板包括配置步骤，所述配置步骤通过性能数据采集任务配置为多个任务队列。

优选地，FreeMarker模板引擎中的身份验证配置模板包括验证步骤，所述验证步骤通过性能数据采集任务配置为多个任务队列。

优选地，所述加密规则通过循环队列位移规则配置为多个任务队列。

优选地，所述解密规则通过循环队列位移规则配置为多个任务队列。

优选地，所述验签规则通过轨迹与服务端内预存的核签轨迹进行拟合。

将各种签名规则、加密规则、解密规则、验签规则分别对应封装。例如，签名规则的算法为SHA256WithRSA，加密规则的算法是RES，模式是CFB，填充方式是PKCS5Padding。通过在FreeMarker中设置插值符号\${ }，利用正则表达式搜索插值符号\${ }，并将其中的内容替换为对应的封装的签名规则、加密规则、解密规则、验签规则。从而形成能够适用于不同应用场景的身份验证页面。

此外，本申请实施例还提出一种计算机可读存储介质，所述计算机可读存储介质可以是硬盘、多媒体卡、SD卡、闪存卡、SMC、只读存储器(ROM)、

可擦除可编程只读存储器(EPROM)、便携式紧致盘只读存储器(CD-ROM)、USB存储器等等中的任意一种或者几种的任意组合。所述计算机可读存储介质中包括身份验证配置程序等,所述身份验证配置程序被处理器12执行时实现如下操作:

步骤S10,在FreeMarker模板引擎中将加密规则、解密规则、签名规则、验签规则的数据模型分别进行封装,以便在后期替换 $\{ \}$ 中的内容,从而生成对应的身份验证页面。

步骤S30,通过FreeMarker模板引擎建立身份验证配置模板,生成.ftl文件。FreeMarker是一种基于模板和要改变的数据的模板引擎,可以用来生成HTML网页、电子邮件、配置文件、源代码等输出文本。模板和数据模型是FreeMarker生成输出所需的组成部分,其中,在所述身份验证配置模板中,通过 $\{ \}$ 来设置可替换的数据;

步骤S50,将所述身份验证配置模板作为依赖包嵌入到JAVA应用中,在所述JAVA应用运行时通过接口调用所述身份验证配置模板,将封装的加密规则、解密规则、签名规则、验签规则替换 $\{ \}$ 中的可替换的数据,从而进行不同形式的身份验证。

或者,所述身份验证配置模板还可以是存放在独立的服务器上,应用可以通过HTTP访问所述身份验证配置模板,例如,开放平台上的应用通过HTTP访问所述身份验证配置模板。应用可以设置选择加密规则、解密规则、签名规则、验签规则的一些模块,例如按钮、勾选框等。开放平台和服务方之间则可以通过开放平台上的应用选择适合的加密规则、解密规则、签名规则、验签规则。应用HTTP访问所述身份验证配置模板,FreeMarker模板引擎动态转换身份验证配置模板,用封装的加密规则、解密规则、签名规则、验签规则替换身份验证配置模板中 $\{ .. \}$ 的可替换的数据,从而形成适于开放平台和服务方之间的身份认证规则。

本申请之计算机可读存储介质的具体实施方式与上述库房监控方法以及电子装置1的具体实施方式大致相同,在此不再赘述。

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

之内。

权利要求书

1. 一种身份验证配置方法，应用于电子装置，其特征在于，该方法包括：
在 FreeMarker 模板引擎中将加密规则、解密规则、签名规则、验签规则的数据模型分别进行封装；

通过 FreeMarker 模板引擎建立身份验证配置模板，生成.ftl 文件，其中，在所述身份验证配置模板中，通过插值符号\${ }来设置可替换的数据；

将所述身份验证配置模板作为依赖包嵌入到JAVA应用中，在所述JAVA应用运行时通过接口调用所述身份验证配置模板，使封装的加密规则、解密规则、签名规则、验签规则替换插值符号\${ }中的可替换的数据，从而形成相应的身份认证规则，

或者，所述身份验证配置模板存放在服务器上，JAVA应用通过HTTP访问所述身份验证配置模板，FreeMarker模板引擎动态转换身份验证配置模板，用封装的加密规则、解密规则、签名规则、验签规则替换身份验证配置模板中\${..}的可替换的数据，从而形成相应的身份认证规则。

2. 根据权利要求 1 所述的身份验证配置方法，其特征在于，
利用FreeMarker模板引擎建立身份验证配置模板的步骤包括：
新建Maven项目；
修改.xml配置文件，增加freemark依赖；
在src/main/java的包下添加templates目录；
在src/main/java/templates目录下添加以.ftl文件形式存在的FreeMarker模板。

3. 根据权利要求1所述的身份验证配置方法，其特征在于，
JAVA应用设置有对应加密规则、解密规则、签名规则、验签规则的选择框。

4. 根据权利要求1所述的身份验证配置方法，其特征在于，
加密规则、解密规则采用的算法至少包括MD5、RSA、DES、AES、Base64。

5. 根据权利要求1所述的身份验证配置方法，其特征在于，
签名规则、验签规则采用的算法至少包括RSA、DSA和ECDSA。

6. 根据权利要求4所述的身份验证配置方法，其特征在于，
AES具有CBC、CFB、ECB、OFB、PCBC5种模式。

7. 根据权利要求3所述的身份验证配置方法，其特征在于，FreeMarker模

板引擎中的身份验证配置模板包括配置步骤，所述配置步骤通过性能数据采集任务配置为多个任务队列。

8. 根据权利要求3所述的身份验证配置方法，其特征在于，FreeMarker模板引擎中的身份验证配置模板包括验证步骤，所述验证步骤通过性能数据采集任务配置为多个任务队列。

9. 根据权利要求3所述的身份验证配置方法，其特征在于，所述加密规则通过循环队列位移规则配置为多个任务队列。

10. 根据权利要求3所述的身份验证配置方法，其特征在于，所述解密规则通过循环队列位移规则配置为多个任务队列。

11. 根据权利要求3所述的身份验证配置方法，其特征在于，所述验签规则通过轨迹与服务端内预存的核签轨迹进行拟合。

12. 一种电子装置，其特征在于，所述电子装置包括存储器及与所述存储器连接的处理器，所述存储器中存储有可在所述处理器上运行的身份验证配置程序，所述身份验证配置程序被所述处理器执行时实现如下步骤：

在FreeMarker模板引擎中将加密规则、解密规则、签名规则、验签规则的数据模型分别进行封装；

通过FreeMarker模板引擎建立身份验证配置模板，生成.ftl文件，其中，在所述身份验证配置模板中，通过\${ }来设置可替换的数据；

将所述身份验证配置模板作为依赖包嵌入到JAVA应用中，在所述JAVA应用运行时通过接口调用所述身份验证配置模板，将封装的加密规则、解密规则、签名规则、验签规则替换\${ }中的可替换的数据，从而生成对应的身份验证页面，

或者，所述身份验证配置模板存放在服务器上，应用通过HTTP访问所述身份验证配置模板，FreeMarker模板引擎动态转换身份验证配置模板，用封装的加密规则、解密规则、签名规则、验签规则替换身份验证配置模板中\${..}的可替换的数据，从而生成对应的身份验证页面。

13. 根据权利要求12所述的电子装置，其特征在于，

利用FreeMarker模板引擎建立身份验证配置模板的步骤包括：

新建Maven项目；

修改.xml配置文件，增加freemark依赖；

在src/main/java的包下添加目录，用于存放所有的freemarker模板；

在src/main/java/templates目录下添加.ftl的FreeMarker模板。

14. 根据权利要求12所述的电子装置，其特征在于，

加密规则、解密规则采用的算法至少包括MD5、RSA、DES、AES、Base64；
签名规则、验签规则采用的算法至少包括RSA、DSA和ECDSA。

15. 根据权利要求12所述的电子装置，其特征在于，

FreeMarker模板引擎中的身份验证配置模板包括配置步骤，所述配置步骤通过性能数据采集任务配置为多个任务队列。

16. 根据权利要求12所述的电子装置，其特征在于，

FreeMarker模板引擎中的身份验证配置模板包括验证步骤，所述验证步骤通过性能数据采集任务配置为多个任务队列。

17. 根据权利要求12所述的电子装置，其特征在于，

所述加密规则通过循环队列位移规则配置为多个任务队列。

18. 根据权利要求12所述的电子装置，其特征在于，

所述解密规则通过循环队列位移规则配置为多个任务队列。

19. 根据权利要求12所述的电子装置，其特征在于，

所述验签规则通过轨迹与服务端内预存的核签轨迹进行拟合。

20. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中包括身份验证配置程序，所述身份验证配置程序被处理器执行时，实现如权利要求1至11中任一项所述的身份验证配置方法的步骤。

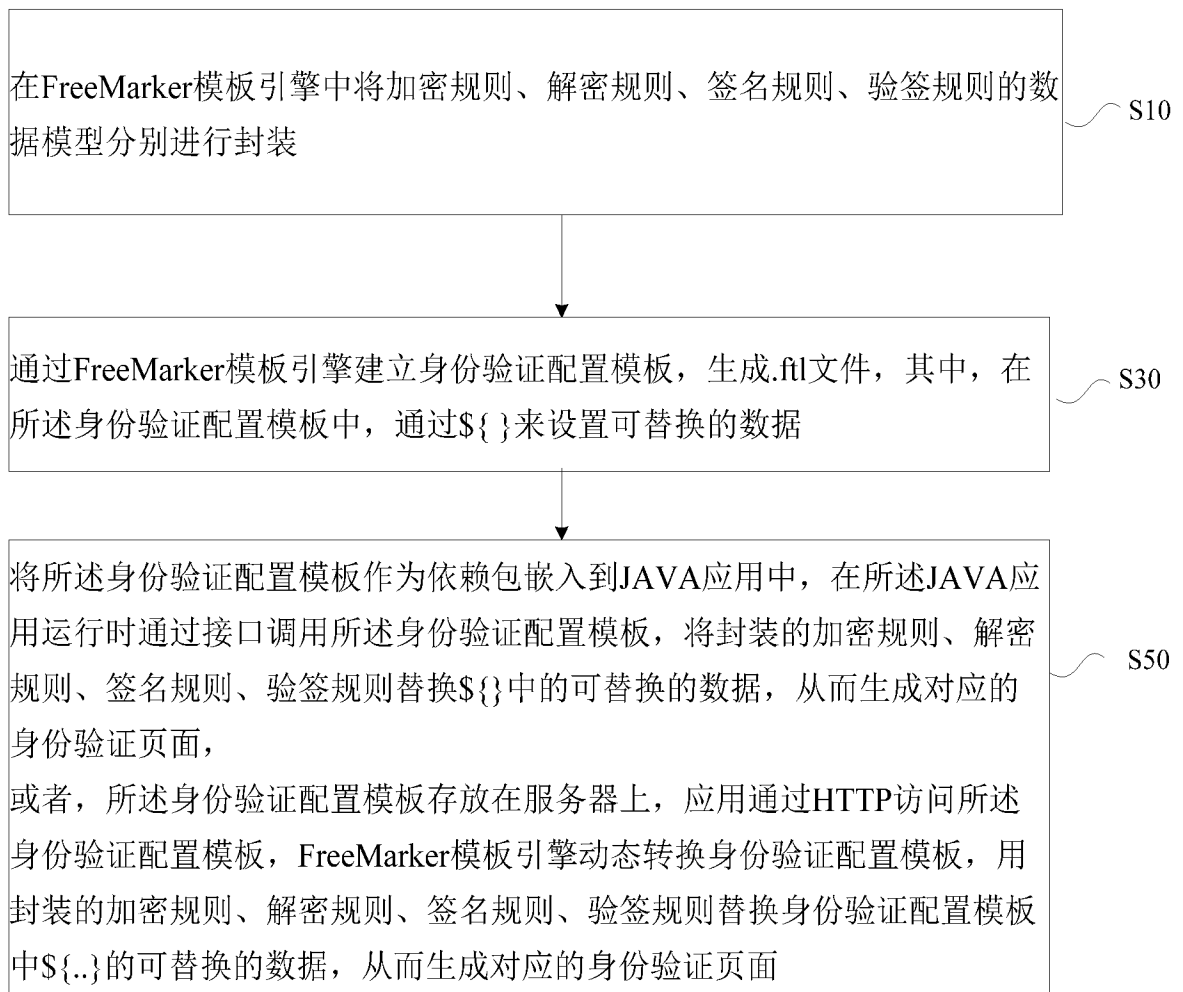


图 1

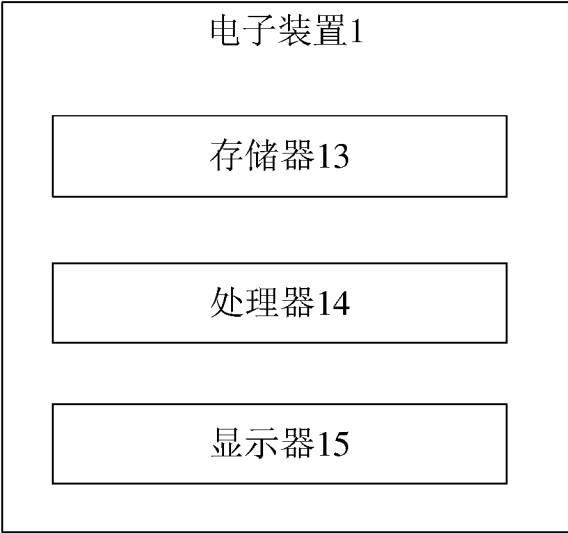


图 2

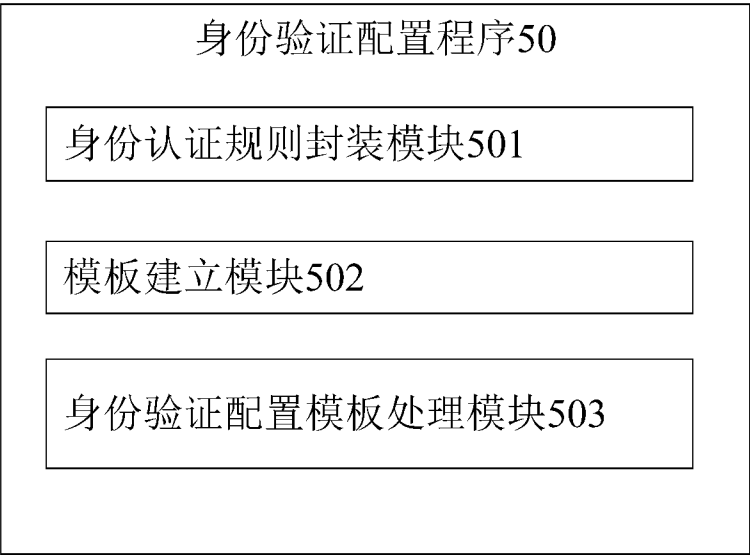


图 3



图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/089183

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)

CNPAT, CNKI, WPI, EPODOC, IEEE: 身份, 认证, 验证, 用户, 加密, 解密, 验签, 规则, 模板, 插值, 替换, 数据, 封装, 队列, 轨迹, 依赖包, Java, freemarker, FTL, Maven, template, MD5, RSA, DES, AES, Base64, RSA, CBC, CFB, ECB, OFB, status, identity, authenticate, verify, check, consumer, encrypt, decrypt, rule, template, replacement, data, encapsulate, queue, trace, jar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109787768 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 21 May 2019 (2019-05-21) claims 1-10	1-20
X	林钰杰等 (LIN, Yujie et al.). "基于FreeMarker的企业Web应用代码生成器研究 (Research and Design of Code Generator for Enterprise Web Application based on FreeMarker Template Engine)" 信息技术 (<i>Information Technology</i>), 30 September 2016 (2016-09-30), sections 1-3	1-20
A	CN 106453517 A (ZHENGZHOU YUNHAI INFORMATION TECH CO., LTD.) 22 February 2017 (2017-02-22) entire document	1-20
A	US 2014068552 A1 (SZOCS, V.) 06 March 2014 (2014-03-06) 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

20 August 2019

Date of mailing of the international search report

27 September 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/089183

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	谢满等 (XIE, Man et al.). "基于FreeMarker自定义访问控制的设计与实现 (The Design and Implementation of User-Defined Control Based on Free Marker)" 东莞理工学院学报 (<i>Journal of Dongguan University of Technology</i>), Vol. 22, No. 5, 31 October 2015 (2015-10-31), entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/089183

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	109787768	A	21 May 2019	None	
CN	106453517	A	22 February 2017	None	
US	2014068552	A1	06 March 2014	None	

国际检索报告

国际申请号

PCT/CN2019/089183

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)) CNPAT, CNKI, WPI, EPDOC, IEEE: 身份, 认证, 验证, 用户, 加密, 解密, 验签, 规则, 模板, 插值, 替换, 数据, 封装, 队列, 轨迹, 依赖包, Java, freemarker, FTL, Maven, template, MD5, RSA, DES, AES, Base64, RSA, CBC, CFB, ECB, OFB, status, identity, authenticate, verify, check, consumer, encrypt, decrypt, rule, template, replacement, data, encapsulate, queue, trace, jar																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 109787768 A (平安科技深圳有限公司) 2019年 5月 21日 (2019 - 05 - 21) 权利要求1-10</td> <td>1-20</td> </tr> <tr> <td>X</td> <td>林钰杰等. “基于FreeMarker的企业Web应用代码生成器研究” 《信息技术》, 2016年 9月 30日 (2016 - 09 - 30), 第1-3节</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 106453517 A (郑州云海信息技术有限公司) 2017年 2月 22日 (2017 - 02 - 22) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 2014068552 A1 (SZOCS, VOJTECH) 2014年 3月 6日 (2014 - 03 - 06) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>谢满等. “基于FreeMarker自定义访问控制的设计与实现” 《东莞理工学院学报》, 第22卷, 第5期, 2015年 10月 31日 (2015 - 10 - 31), 全文</td> <td>1-20</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 109787768 A (平安科技深圳有限公司) 2019年 5月 21日 (2019 - 05 - 21) 权利要求1-10	1-20	X	林钰杰等. “基于FreeMarker的企业Web应用代码生成器研究” 《信息技术》, 2016年 9月 30日 (2016 - 09 - 30), 第1-3节	1-20	A	CN 106453517 A (郑州云海信息技术有限公司) 2017年 2月 22日 (2017 - 02 - 22) 全文	1-20	A	US 2014068552 A1 (SZOCS, VOJTECH) 2014年 3月 6日 (2014 - 03 - 06) 全文	1-20	A	谢满等. “基于FreeMarker自定义访问控制的设计与实现” 《东莞理工学院学报》, 第22卷, 第5期, 2015年 10月 31日 (2015 - 10 - 31), 全文	1-20
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
PX	CN 109787768 A (平安科技深圳有限公司) 2019年 5月 21日 (2019 - 05 - 21) 权利要求1-10	1-20																		
X	林钰杰等. “基于FreeMarker的企业Web应用代码生成器研究” 《信息技术》, 2016年 9月 30日 (2016 - 09 - 30), 第1-3节	1-20																		
A	CN 106453517 A (郑州云海信息技术有限公司) 2017年 2月 22日 (2017 - 02 - 22) 全文	1-20																		
A	US 2014068552 A1 (SZOCS, VOJTECH) 2014年 3月 6日 (2014 - 03 - 06) 全文	1-20																		
A	谢满等. “基于FreeMarker自定义访问控制的设计与实现” 《东莞理工学院学报》, 第22卷, 第5期, 2015年 10月 31日 (2015 - 10 - 31), 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 2019年 8月 20日		国际检索报告邮寄日期 2019年 9月 27日																		
ISA/CN的名称和邮寄地址 中国国家知识产权局 (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		授权官员 张雪 电话号码 86-(10)-53961613																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/089183

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	109787768	A	2019年 5月 21日	无	
CN	106453517	A	2017年 2月 22日	无	
US	2014068552	A1	2014年 3月 6日	无	