(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 101751258 B
(45)授权公告日 2013.06.26

(21)申请号 200910244379.X

(22)申请日 2009.12.30

(73)专利权人 大唐微电子技术有限公司
地址 100094 北京市海淀区永嘉北路6号

(72)发明人 刘芳 任强 穆肇骊

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 栗若木 王漪

(51)Int.Cl.
G06F 9/44(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 101078992 A,2007.11.28, 说明书第4页第25行至第6页第17行, 图3-4.
CN 101505339 A,2009.08.12, 说明书第3页第19行至第4页第15行,图2.
CN 101216758 A,2008.07.09, 说明书第7页第2段.
CN 101042737 A,2007.09.26, 全文.

审查员 张坦

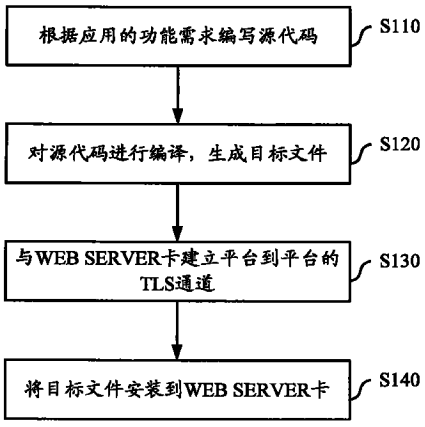
权利要求书2页 说明书9页 附图8页

(54)发明名称

智能卡与智能卡应用的开发方法、开发系统及部署方法

(57)摘要

本发明公开了一种智能卡、一种智能卡应用的开发方法、开发系统以及部署方法,用于智能卡应用的开发和部署,其中该开发方法主要包括:根据应用的功能需求编写源代码;对所述源代码进行编译,生成目标文件;与所述智能卡建立平台到平台的传输层安全通道;通过所述传输层安全通道将所述目标文件安装到所述智能卡。与现有技术相比,本发明针对智能卡的应用开发和部署提出了简易的解决方案,为应用开发人员提供了一种可视化、通用且安全可靠的智能卡应用开发和部署的技术。



CN 101751258 B

1. 一种智能卡应用的开发系统，其特征在于，该系统包括编辑模块、编译模块、连接模块以及安装模块，其中：

所述编辑模块，用于根据应用的功能需求编写源代码；

所述编译模块，用于对所述源代码进行编译，生成目标文件；

所述连接模块，用于与所述智能卡建立平台到平台的传输层安全通道；

所述安装模块，用于通过所述传输层安全通道将所述目标文件安装到所述智能卡，根据所述目标文件的各文件属性生成文件头信息，通过 HTTP 指令在所述智能卡内创建应用及其下文件；通过 HTTP 指令将所述应用及其下文件的文件体写入所述智能卡内；通过签名认证并完成所述应用的注册。

2. 如权利要求 1 所述的系统，其特征在于：

所述编辑模块采用 WEB 网页编写或者面向对象语言编写所述源代码。

3. 如权利要求 1 所述的系统，其特征在于：

所述编译模块生成的所述目标文件包括静态文本文件和动态数据处理目标文件，其中：

所述静态文本文件包括 HTML 文本文件、应用配置文件以及图像文件；

所述动态数据处理目标文件包括可执行文件。

4. 如权利要求 1 所述的系统，其特征在于，该系统进一步包括：

上传模块，用于将所述目标文件上传到网络，通过网络将所述目标文件安装到所述智能卡。

5. 一种智能卡，该智能卡支持 HTTP 协议，其特征在于，该智能卡包括部署模块，用于部署智能卡应用，该部署模块包括安全单元、创建单元、更新单元以及注册单元，其中：

所述安全单元，用于在所述智能卡与部署客户端之间建立传输层安全通道；

所述创建单元，用于通过所述传输层安全通道，从所述部署客户端获得所述应用的目标文件，通过 HTTP 指令创建应用及其下文件；

所述更新单元，用于通过 HTTP 指令将所述应用及其下文件的文件体写入所述智能卡；

所述注册单元，用于通过 HTTP 指令完成注册，所述注册过程包括签名认证过程。

6. 如权利要求 5 所述的智能卡，其特征在于，所述部署模块进一步包括注销单元以及删除单元，其中：

所述注销单元，用于通过 HTTP 指令完成所述应用的注销，所述注销过程包括签名认证过程；

所述删除单元，用于删除所述应用及其下文件的文件体。

7. 一种智能卡应用的开发方法，其特征在于，该方法包括：

根据应用的功能需求编写源代码；

对所述源代码进行编译，生成目标文件；

与所述智能卡建立平台到平台的传输层安全通道；以及

通过所述传输层安全通道将所述目标文件安装到所述智能卡；

根据所述目标文件的各文件属性生成文件头信息，通过 HTTP 指令在所述智能卡内创建应用及其下文件；

通过 HTTP 指令将所述应用及其下文件的文件体写入所述智能卡内；

通过签名认证后完成所述应用的注册。

8. 如权利要求 7 所述的方法，其特征在于：

编写所述源代码，包括采用 WEB 网页开发或者面向对象语言开发。

9. 如权利要求 7 所述的方法，其特征在于：

所述目标文件包括静态文本文件和动态数据处理目标文件，其中：

所述静态文本文件包括 HTML 文本文件、应用配置文件以及图像文件；

所述动态数据处理目标文件包括可执行文件。

10. 如权利要求 7 所述的方法，其特征在于，该方法进一步包括：

将所述目标文件上传到网络，通过网络将所述目标文件安装到所述智能卡。

11. 一种智能卡应用的部署方法，该智能卡支持 HTTP 协议，其特征在于，该方法包括：

在所述智能卡与部署客户端之间建立传输层安全通道；

通过所述传输层安全通道，从所述部署客户端获得所述应用的目标文件，通过 HTTP 指令创建应用及其下文件；

通过 HTTP 指令将所述应用及其下文件的文件体写入所述智能卡；

通过 HTTP 指令完成注册，所述注册过程包括签名认证过程。

12. 如权利要求 11 所述的方法，其特征在于，该方法进一步包括：

通过 HTTP 指令完成所述应用的注销，所述注销过程包括签名认证过程；

删除所述应用及其下文件的文件体。

智能卡与智能卡应用的开发方法、开发系统及部署方法

技术领域

[0001] 本发明涉及智能卡领域，尤其涉及一种智能卡、一种智能卡应用的开发方法、开发系统以及部署方法。

背景技术

[0002] 智能卡网络服务器(Smart Card WEB SERVER,SCWS)由移动开放联盟(OMA)组织提出的将WEB服务器嵌入智能卡平台的概念，它提出了通过HTTP协议访问卡上应用的方式。

[0003] 现有技术中，网络服务器(WEB SERVER)卡的应用开发以及部署(所谓部署是指发卡商或经发卡商授权的第三方在卡内对应的安全域内添加或删除应用的过程)，一般需要完成以下工作：

[0004] (1)通过更新卡操作系统，在卡操作系统中添加新的函数，以完成WEB SERVER卡动态数据处理功能；

[0005] (2)编写卡片能够识别的指令脚本，将静态文本数据发送给WEBSERVER卡，在WEB SERVER卡内的文件系统中创建文件，所创建的这些文件主要用于存储静态文本数据；

[0006] (3)针对WEB SERVER卡中网页的逻辑跳转的应用特点，需要统一处理新创建的文件名和处理动态数据的函数的入口地址，按照跳转逻辑关系更新静态文本数据中供浏览器跳转的URL地址；

[0007] 上述针对WEB SERVER卡的应用开发以及部署工作，对于一个不熟悉智能卡知识的开发人员而言是非常困难的。

发明内容

[0008] 本发明所要解决的技术问题，在于需要提供一种智能卡应用的开发方法及系统，用于智能卡应用的开发。

[0009] 为了解决上述技术问题，本发明首先提供了一种智能卡应用的开发系统，该系统包括编辑模块、编译模块、连接模块以及安装模块，其中：

[0010] 所述编辑模块，用于根据应用的功能需求编写源代码；

[0011] 所述编译模块，用于对所述源代码进行编译，生成目标文件；

[0012] 所述连接模块，用于与所述智能卡建立平台到平台的传输层安全通道；

[0013] 所述安装模块，用于通过所述传输层安全通道将所述目标文件安装到所述智能卡。

[0014] 优选地，所述编辑模块采用WEB网页编写或者面向对象语言编写所述源代码。

[0015] 优选地，所述编译模块生成的所述目标文件包括静态文本文件和动态数据处理目标文件，其中：

[0016] 所述静态文本文件包括HTML文本文件、应用配置文件以及图像文件；

[0017] 所述动态数据处理目标文件包括可执行文件。

[0018] 优选地，该系统进一步包括：

[0019] 上传模块，用于将所述目标文件上传到网络，通过网络将所述目标文件安装到所述智能卡。

[0020] 优选地，在所述智能卡中部署所述应用后，通过签名认证并完成所述应用的注册。

[0021] 为了解决上述技术问题，本发明还提供了一种智能卡应用的开发方法，该方法包括：

[0022] 根据应用的功能需求编写源代码；

[0023] 对所述源代码进行编译，生成目标文件；

[0024] 与所述智能卡建立平台到平台的传输层安全通道；以及

[0025] 通过所述传输层安全通道将所述目标文件安装到所述智能卡。

[0026] 优选地，编写所述源代码，包括采用 WEB 网页开发或者面向对象语言开发。

[0027] 优选地，所述目标文件包括静态文本文件和动态数据处理目标文件，其中：

[0028] 所述静态文本文件包括 HTML 文本文件、应用配置文件以及图像文件；

[0029] 所述动态数据处理目标文件包括可执行文件。

[0030] 优选地，在所述智能卡中部署所述应用的步骤，包括：

[0031] 对所述目标文件的各文件属性，生成文件头信息，通过 HTTP 指令在所述智能卡内创建应用及其下文件；

[0032] 通过 HTTP 指令将所述应用及其下文件的文件体写入所述智能卡内。

[0033] 优选地，该方法进一步包括：

[0034] 将所述目标文件上传到网络，通过网络将所述目标文件安装到所述智能卡。

[0035] 优选地，该方法进一步包括：

[0036] 在所述智能卡中部署所述应用，通过签名认证后完成所述应用的注册。

[0037] 本发明所要解决的另一技术问题是提出一种智能卡，用于完成应用的部署。

[0038] 为了解决这一问题，本发明还提供了一种智能卡，该智能卡支持 HTTP 协议，该智能卡包括部署模块，用于部署智能卡应用，该部署模块包括安全单元、创建单元、更新单元以及注册单元，其中：

[0039] 所述安全单元，用于在所述智能卡与部署客户端之间建立传输层安全通道；

[0040] 所送创建单元，用于通过所述传输层安全通道，从所述部署客户端获得所述应用的目标文件，通过 HTTP 指令创建应用及其下文件；

[0041] 所述更新单元，用于通过 HTTP 指令将所述应用及其下文件的文件体写入所述智能卡；

[0042] 所述注册单元，用于通过 HTTP 指令完成注册，所述注册过程包括签名认证过程。

[0043] 优选地，所述部署模块进一步包括注销单元以及删除单元，其中：

[0044] 所述注销单元，用于通过 HTTP 指令完成所述应用的注销，所述注销过程包括签名认证过程；

[0045] 所述删除单元，用于删除所述应用及其下文件的文件体。

[0046] 本发明所要解决的还一技术问题是提出一种智能卡应用的部署方法，用于在智能卡中部署应用。

[0047] 为了解决这一问题，本发明还提供了一种智能卡应用的部署方法，该智能卡支持 HTTP 协议，该方法包括：

[0048] 在所述智能卡与部署客户端之间建立传输层安全通道；

[0049] 通过所述传输层安全通道，从所述部署客户端获得所述应用的目标文件，通过HTTP指令创建应用及其下文件；

[0050] 通过HTTP指令将所述应用及其下文件的文件体写入所述智能卡；

[0051] 通过HTTP指令完成注册，所述注册过程包括签名认证过程。

[0052] 优选地，该方法进一步包括：

[0053] 通过HTTP指令完成所述应用的注销，所述注销过程包括签名认证过程；

[0054] 删除所述应用及其下文件的文件体。

[0055] 与现有技术相比，本发明针对智能卡的应用开发和部署提出了简易的解决方案，为应用开发人员提供了一种可视化、通用且安全可靠的智能卡应用开发和部署的技术方案，使得应用开发人员不需要了解智能卡相关知识及实现细节，即可像在PC机上开发传统WEB应用一样开发智能卡的新应用或者升级原有的应用；且可将调试成功后的目标文件像在PC机上安装软件一样将该应用安装到智能卡上，从而为智能卡应用的升级扩展提供了广阔的空间。另外，本发明所提供的智能卡，包含一个功能模块，实现智能卡应用的部署。

[0056] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0057] 附图用来提供对本发明的进一步理解，并且构成了说明书的一部分，与本发明的实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

[0058] 图1是本发明智能卡应用的开发方法实施例的流程示意图；

[0059] 图2为本发明技术方案在WEB SERVER卡上安装应用的流程示意图；

[0060] 图3为本发明技术方案在WEB SERVER卡上删除应用的流程示意图；

[0061] 图4为本发明智能卡应用的开发方法实施例中进行源代码开发的界面示意图；

[0062] 图5为本发明智能卡应用的开发方法实施例中目标文件的文件树结构示意图；

[0063] 图6为本发明智能卡应用的开发系统实施例的组成示意图；

[0064] 图7为本发明智能卡实施例的组成示意图；

[0065] 图8为本发明智能卡应用的部署方法实施例的流程示意图。

具体实施方式

[0066] 以下将结合附图及实施例来详细说明本发明的实施方式，借此对本发明如何应用技术手段来解决技术问题，并达成技术效果的实现过程能充分理解并据以实施。

[0067] 需要说明的是，如果不冲突，本发明实施例以及实施例中的各个特征可以相互结合，均在本发明的保护范围之内。另外，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，可以以不同的顺序执行所示出或描述的步骤。

[0068] 以WEB SERVER卡为例的智能卡，其应用所包含的功能可以划分为两类：一是文本、图片等静态文件；二是数据处理操作。其中数据处理操作需要操作卡上资源，文本、图片

等静态文件虽可以以文件形式存储在卡上，但智能卡操作系统属于嵌入式系统，其文件系统和文件命名机制不同于常见的 Windows 等操作系统。如何使新的应用有机嵌入到智能卡系统，以及如何使应用开发人员在不需要了解智能卡的专业知识背景下即可完成开发部署应用也决定了这项技术的普及和应用推广程度。

[0069] 以下对 WEB SERVER 卡上的文件命名机制进行简要说明。但是需要说明的是，该命名机制并不是本发明相比现有技术作出改进的重点内容，因此该命名机制的说明并不对本发明技术方案构成限制。

[0070] 卡上的文件系统是以主文件 (Master File，MF) 为根的一个文件树结构。在 MF 下，包含有基本文件 (Element File，EF)、专用文件 (Dedicated File，DF) 和应用文件 (Application DF，ADF) 等类型的文件；DF 和 ADF 下可包含 EF 及 DF 文件，依次类推。在 WEB SERVER 卡上添加一个新应用，实际上就是在卡上添加一个新的 ADF 及其下的 DF、EF。

[0071] 卡上文件是以文件标识符 (File Identifier) 的方式进行命名，即用 2 个字节识别文件。在常见的 Windows 系统中，文件有扩展名，以表示文件类型；而在 WEB SERVER 卡中，文件不支持扩展名，文件类型分为 DF(MF、ADF 属于特殊的 DF) 和 EF(分为透明、线性及循环类型等)。

[0072] 另外，在常见的 Windows 系统中，文件的安全属性有只读、存档，而在 WEB SERVER 卡中的文件安全属性是通过 PIN 机制控制；每个文件都通过设置相应的 PIN 控制其读写权限。

[0073] 图 1 为本发明智能卡应用开发方法实施例的流程示意图。如图 1 所示，该智能卡应用开发方法实施例主要包括如下步骤：

[0074] 步骤 S110，根据应用的功能需求编写源代码，其中的源代码包括静态文件和数据处理操作的源代码；本发明方法实施例中的源代码编写，支持 WEB 网页开发和面向对象语言开发；

[0075] 步骤 S120，对源代码进行编译，生成目标文件，其中该目标文件包括静态文本文件和动态数据处理目标文件，其中的静态文本文件比如包括 HTML 文本文件、应用配置文件以及图像文件等等，其中的动态数据处理目标文件比如包括可执行文件等等；

[0076] 步骤 S130，与 WEB SERVER 卡建立平台到平台的传输层安全 (TransportLayer Security，TLS) 通道；本实施例中的智能卡以 WEB SERVER 卡为例；

[0077] 步骤 S140，通过该 TLS 通道将该目标文件安装到 WEB SERVER 卡，完成应用的开发；在 WEB SERVER 卡中部署应用，通过签名认证后完成该应用的注册。

[0078] 上述步骤 S130 中是在部署客户端与卡端建立 TLS 通道，并完成步骤 S140 中所述的内容。在调试阶段，也可以是在部署客户端与 WEB SERVER 卡模拟器建立平台到平台的 TLS 通道，然后将目标文件安装到 WEBSERVER 卡模拟器，并在 WEB SERVER 卡模拟器进行部署应用的调试。

[0079] 上述方法实施例中，还可以将目标文件上传到网络，以提供该目标文件的网络下载，便于用户从网络上将该目标文件安装到 WEB SERVER 卡，完成应用的部署。

[0080] 上述步骤 S140 中将该目标文件安装到该网络服务器卡过程，主要是根据该目标文件中各文件的属性自动生成文件头信息，通过 HTTP 指令传输给 WEB SERVER 卡在卡内创建文件。根据目标文件中文件树结构在卡内创建类似的文件系统，其中目标文件中的一级

目录映射为ADF，其下子目录映射为DF，文件映射为EF。成功创建文件系统后，通过HTTP指令将文件内容写入该网络服务器卡相应文件体。智能卡在完成上述操作后，发送注册应用的指令，注册应用需要提供该应用的签名认证，最后通过签名认证完成该应用的注册。通过这样的运行机制保证了只有授权的第三方才可以在WEBSERVER卡上添加/删除应用。

[0081] 本发明上述方法实施例，其相比现有技术的优势之一，体现在安全性方面，具体地：应用部署前在卡端和部署客户端建立平台到平台的传输层安全(Transport Layer Security，TLS)通道；应用部署中需要进行注册或者注销才能顺利完成应用的安装或者删除。

[0082] 图2和图3分别为在WEB SERVER卡上安装和删除应用的流程示意图。结合图1所示本发明应用开发方法实施例，图2所示应用的安装流程主要包括如下步骤：

[0083] 步骤S210，部署客户端与WEB SERVER卡建立平台到平台的安全通道；

[0084] 步骤S220，向卡内添加挂起的应用，添加的方式是在卡内创建一个新的ADF，其AID在Description.xml文件中有说明；其中，所述挂起是指此时的应用作为卡内的一个ADF已经创建，但还不能被外界识别；

[0085] 步骤S230，向卡内添加应用下的文件(DF和EF)，方式是根据Description.xml文件记录的文件属性、文件在文件树的位置以及文件大小构建文件FCP(File Control Parameter)，通过HTTP指令将FCP传输给WEBSERVER卡，在卡内创建ADF下的DF和EF文件，且将文件内容写入到其在卡内相应的EF文件体中；

[0086] 步骤S240，向卡内发送注册命令以注册应用(ADF)，通过验证签名确认安装方的合法身份，验证通过后才将应用的状态由挂起更新为可选，签名文件是针对该应用ADF及相关信息所作的签名。

[0087] 需要说明的是，在安装过程中，部署客户端会根据图5所示的文件树结构在WEB SERVER卡上映射为以CUP_APP1为应用ADF的类似的文件树结构。

[0088] 结合图1所示本发明开发方法实施例，图3所示应用的删除流程主要包括如下步骤：

[0089] 步骤S310，部署客户端与WEB SERVER卡建立平台到平台的安全通道；

[0090] 步骤S320，注销应用(ADF)，步骤S240的反向过程；

[0091] 步骤S330，删除应用(ADF)下的文件(DF和EF)；

[0092] 步骤S340，删除应用(ADF)。

[0093] 在图2所示的应用安装流程中以及图3所示的应用删除流程中，部署客户端以符合HTTP协议的格式将数据(如FCP、文件体)传输给WEB SERVER卡完成应用的安装或删除，WEB SERVER卡返回HTTP响应。在本发明系统实施例中，应用表1所示的管理命令列表来完成图2及图3所示的两个流程：

[0094]

命令名称	HTTP 方法	适用文件类型	文件定位信息	功能描述
create	PUT	ADF	空	创建应用根目录 ADF
		DF	URL	创建 DF
		EF	URL	创建 EF
delete	DELETE	ADF	空	删除 ADF。
		DF	URL	删除 DF
		EF	URL	删除指定 EF 文件
update	PUT	EF	URL	更新 EF 文件体
register	PUT	ADF	空	注册应用
deregister	PUT	ADF	空	注销应用

[0095] 图 4 为源代码编写的界面示意图。本发明开发方法实施例中的源代码编写支持以下类型代码开发：标准的 Web 网页开发，符合 HTML 和 CSS 的语法规范、JavaScript 语法规范，支持 ajax 技术，还支持面向对象如 Java 语言开发，并提供通用的 API 库文件。

[0096] 图 5 为在 WEB SERVER 卡模拟器中进行调试时生成的目标文件的文件树结构示意图。在图 5 所示的文件树结构中，目录 bin 及 script 由开发人员根据需要创建，用于区分不同类型文件。一般情况下，目录 bin 存储编译后的 java 目标文件，目录 html 存储 WEB 文本文件，signature.dat 为应用安全域的签名文件。需要特别说明的是文件 Description.xml（应用描述文件）通常由编译器解析文本文件产生，也可以由开发人员自己编写，符合标准的 XML 规范。应用描述文件用于描述应用的属性信息，例如：包括应用标识 AID 名称，应用安全域 AID 和指定应用安全域的签名文件。除此之外，还包括应用 ADF 及其下目录的读写权限，文件创建和删除权限等等。对于任一个应用来说，应用描述文件是必不可少的。

[0097] 在本发明开发方法实施例中，应用描述文件位于应用包的根目录下，供应用安装时按照该信息安装文件使用。应用在运行阶段，WEB SERVER 卡解析 Description.xml 文件，获得重定向 HTTP 请求的 URL。综上所述，Description.xml 中描述了下列几类信息：

[0098] (1) 应用、目录和文件的安全属性

[0099] 在用户默认情况下，文件继承其父目录的安全属性；但用户可根据需要在部署客户端界面窗口中设置文件的安全属性，这些信息都记录在 Description.xml 文件中。

[0100] (2)URL 的重定向信息

[0101] 部署客户端在安装应用时，按照卡文件树结构及文件名更新文件体中 URL 重定向信息。

[0102] (3) 指定应用 AID 的签名文件

[0103] 应用在安装的注册阶段和删除的注销阶段将使用该路径指定的签名文件作为卡内安装应用的合法性认证。只有签名认证通过的应用才能顺利完成安装或者删除操作。保

证了只有授权用户才可以在卡上安装、删除应用。

[0104] 以上列举了应用描述文件描述的常用信息，其包含的信息仍可根据应用开发的需要适当调整和添加，要求符合 XML 格式即可。

[0105] 图 1 所示的本发明开发方法实施例，在具体应用时主要包括编辑、编译、连接以及安装等阶段。图 6 为本发明开发系统实施例的组成示意图，以下结合图 1 所示的本发明开发方法实施例，对本发明开发系统进行详细说明。图 6 所示的本发明开发系统实施例 600，主要包括编辑模块 610、编译模块 620、连接模块 630 以及安装模块 640，其中：

[0106] 编辑模块 610，用于根据 WEB SERVER 卡应用的功能需求，调用功能模块和应用接口编写该应用的源代码，该源代码包括静态文件和数据处理操作的源代码；该源代码的编写，支持 WEB 网页开发和面向对象语言开发；

[0107] 编译模块 620，用于对该编辑模块 610 所编写的源代码进行编译，生成目标文件；

[0108] 连接模块 630，用于与该 WEB SERVER 卡建立平台到平台的传输层安全 (TLS) 通道；

[0109] 安装模块 640，用于为 WEB SERVER 卡或者 WEB SERVER 卡模拟器提供目标文件的安装功能，也即将编译模块生成的目标文件安装到 WEBSERVER 卡，或者 WEB SERVER 卡模拟器。在本发明系统实施例中，通过安装模块 640 可以将目标文件安装到 WEB SERVER 卡进行部署以及注册，或者安装到 WEB SERVER 卡模拟器中调试。

[0110] 上述编辑模块 610 采用面向对象的程序语言（如 Java 等）及脚本语言（如 JavaScript 等）的设计开发，并提供通用的应用开发模板和 API 接口，开发人员根据具体应用的功能需求，调用相应的应用开发模板，并在应用开发模板中添加相应的核心代码即可完成代码编辑。编辑模块 610 提供图形化的人机界面，图 4 为编辑模块 610 进行源代码开发的界面示意图。其支持以下类型代码开发：标准的 Web 网页开发，符合 HTML 和 CSS 的语法规范、JavaScript 语法规范，支持 ajax 技术；另外，支持面向对象如 Java 语言开发，并提供通用的 API 库文件。

[0111] 上述连接模块 630 为部署客户端与 WEB SERVER 卡建立传输层安全 (Transport Layer Security，TLS) 通道，保证了数据传输的安全。

[0112] 根据前述内容，即可在上述系统实施例中完成一个新应用的开发、安装以及册除。

[0113] 图 6 所示开发系统实施例中，还可以包含压缩模块 650 及上传模块 660，其中：

[0114] 该压缩模块 650，用于将该目标文件打包成 zip 格式的目标文件，其中该目标文件包括静态文本文件和动态数据处理目标文件；

[0115] 该上传模块 660，应用开发人员（一般为服务提供商或授权组织）通过该上传模块 660，可将编译生成的目标文件打包上传到网络上，有需要加载该应用的持卡人即可通过网络下载目标文件压缩包，并自行解压缩并将应用安装到 WEB SERVER 卡上。熟悉开发 WEB 应用的持卡人甚至可根据个人兴趣在 WEB SERVER 卡片上开发部署个人应用。WEB SERVER 卡可以针对不同群体开放不同的操作权限。

[0116] 当然，压缩模块 650 进行文件压缩采用的是 zip 格式，在其他系统实施例中，也可以采用其他文件格式对目标文件进行打包并生成相应文件格式的压缩文件。在本发明的技术方案中，上述应用描述文件格式也不做具体限定，甚至可将应用描述文件所记录的属性功能安排到各个具体文件中。

[0117] 另外，本发明技术方案中也可以直接将目标文件安装到WEB SERVER卡中而不需要压缩模块650的压缩打包过程。

[0118] 图7为本发明WEB SERVER智能卡中增加部署模块实施例的组成示意图。结合图6所示的本发明开发系统实施例，图7所示智能卡中的部署模块实现的功能主要有应用安装和应用删除，其中的应用安装主要用于响应部署客户端安装应用的请求，在卡内安装一个新的应用，而应用删除主要用于响应部署客户端删除应用的请求，在卡内已存在的某个应用删除。

[0119] 如图7所示，该智能卡中的部署模块主要包括安全单元710、创建单元720、更新单元730、注册单元740、注销单元750以及删除单元760，其中：

[0120] 安全单元710，用于在卡端（WEB SERVER卡）和部署客户端之间建立TLS安全通道，以确保数据传输的完整性以及真实性等；

[0121] 创建单元720，用于通过该安全单元710建立的TLS安全通道，从部署客户端获得应用的目标文件的文件头信息，通过HTTP指令在WEB SERVER卡内创建应用文件；在本实施例中为接收HTTP指令create命令，根据指令中的FCP数据在卡内创建ADF及其下DF、EF文件；

[0122] 更新单元730，用于通过HTTP指令将该应用文件的文件体写入WEBSERVER卡内，在本实施例中为接收HTTP指令update命令，根据指令中指向的EF及文件体数据更新相应EF文件；

[0123] 注册单元740，用于在更新单元730更新文件（即将该文件体写入该WEB SERVER卡中）之后，通过HTTP指令完成注册过程中的签名认证，在本实施例中为接收HTTP指令register命令，从卡内安全密钥区取出注册密钥，对新创建ADF的AID进行签名算法，得出的结果与HTTP指令中的签名数据进行比较；相等则更新ADF状态为可见，否则返回错误状态；

[0124] 注销单元750，用于通过HTTP指令完成注销过程中的签名认证，在本实施例中为接收HTTP指令deregister命令，从卡内安全密钥区取出注销密钥，对即将删除ADF的AID进行签名算法，得出的结果与HTTP指令中的签名数据进行比较；相等则更新ADF生命周期状态为EASABLE；否则返回错误状态；

[0125] 删除单元760，用于删除该应用的专用文件，在本实施例中为接收DELETE指令，用于删除EF、DF或ADF。当删除DF，要删除DF及其下的所有文件树结构。当删除应用ADF时，应删除ADF下所有文件树结构。在进行删除操作前，检查应用的生命周期状态，只有当应用处于EASABLE状态时，文件删除方可进行。

[0126] 图8为本发明智能卡应用部署方法实施例的流程示意图。结合结合图1所示本发明开发方法实施例、图6所示的本发明开发系统实施例以及图7所示的本发明智能卡实施例，图8所示的智能卡应用部署方法实施例主要包括如下步骤：

[0127] 步骤S810，在该智能卡与部署客户端之间建立传输层安全通道；

[0128] 步骤S820，通过该传输层安全通道，从该部署客户端获得该应用的目标文件，通过HTTP指令创建应用及其下文件；

[0129] 步骤S830，通过HTTP指令将该应用及其下文件的文件体写入该智能卡；

[0130] 步骤S840，通过HTTP指令完成注册，该注册过程包括签名认证过程。

[0131] 如图 8 所示的流程中，还可以包括删除智能卡中该应用的方法，具体参见以下步骤：

[0132] 步骤 S850，通过 HTTP 指令完成该应用的注销，该注销过程包括签名认证过程；

[0133] 步骤 S860，删除该应用及其下文件的文件体。

[0134] 本发明的技术方案在部署 WEB SERVER 卡应用时采用开发、安装部署的模式，提供通用的应用开发模版和 API 接口，采用将文本文件、可执行文件等按文件树目录结构存储的模式，并采用描述文件记录各文件属性及逻辑关系的方式，还将开发的文件目录树结构映射为 WEB SERVER 卡的文件系统。在应用的安装和删除过程中，本发明技术方案采用建立安全通道的方式建立安全连接。在应用的注册和注销机制中，采用应用签名的方式验证合法应用。

[0135] 与现有技术相比，本发明技术方案针对 WEB SERVER 卡的应用开发提供了可视化接口，应用开发人员不需关注卡的实现细节及平台模式，即可在集成环境中像开发 PC 端的传统 WEB 应用一样开发卡端应用，使得 WEBSERVER 卡应用的扩展具备通用性。本发明技术方案，在部署客户端中可将整个应用功能所需的操作、数据通过编写静态文本、数据处理等一系列功能代码实现，通过安装将传统的 WEB 应用自动映射转化为 WEB SERVER 卡应用，之后将该应用有机集成到 WEB SERVER 卡内。本发明技术方案中，在应用的安装过程中，首先部署客户端与卡之间建立安全的数据连接通道，其次使用签名方式处理应用的注册 / 注销，只有签名验证通过的应用才能彻底完成安装过程并且被外界实体选择使用；同理，只有签名验证通过的应用才能被彻底删除的操作，这种机制充分考虑了添加 / 删除应用所必须的安全级别。本发明技术方案，对安装应用时，建立安全通道和签名的算法并不做具体限定。

[0136] 而且，本发明技术方案，包括前述的开发方法、开发系统、部署方法以及智能卡等的实施例，均是以 WEB SERVER 卡为例进行说明的。实际上，本发明技术方案适用于任何支持 HTTP 协议的智能卡，而并不限于 WEBSERVER 卡。

[0137] 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。另外，本领域的技术人员应该明白，本发明的上述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。

[0138] 虽然本发明所揭露的实施方式如上，但所述的内容只是为了便于理解本发明而采用的实施方式，并非用以限定本发明。任何本发明所属技术领域内的技术人员，在不脱离本发明所揭露的精神和范围的前提下，可以在实施的形式上及细节上作任何的修改与变化，但本发明的专利保护范围，仍须以所附的权利要求书所界定的范围为准。

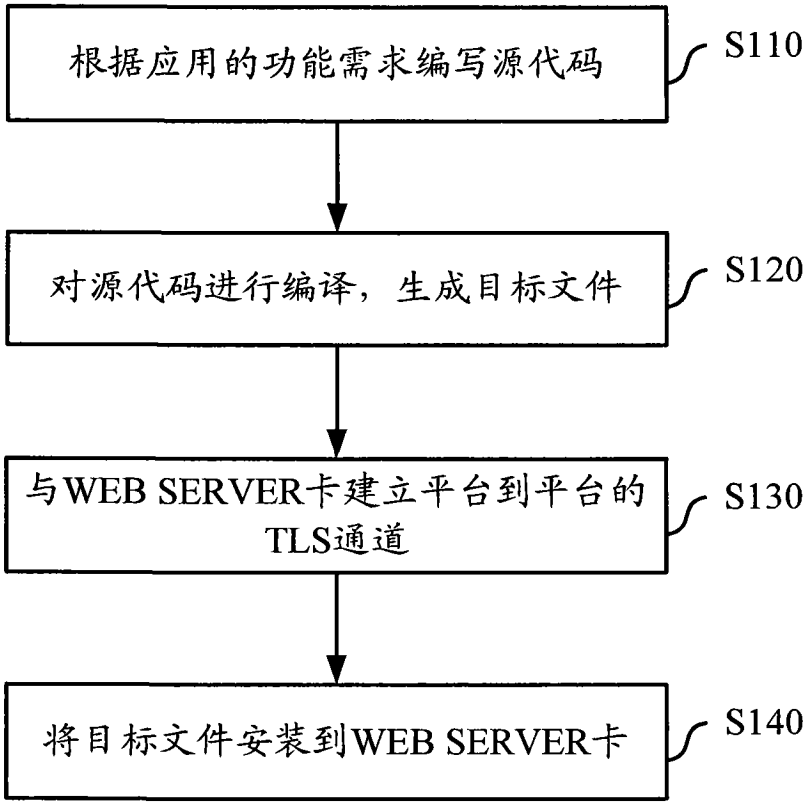

根据应用的功能需求编写源代码
S110
对源代码进行编译，生成目标文件
S120
与WEB SERVER卡建立平台到平台的TLS通道
S130
将目标文件安装到WEB SERVER卡
S140

图 1

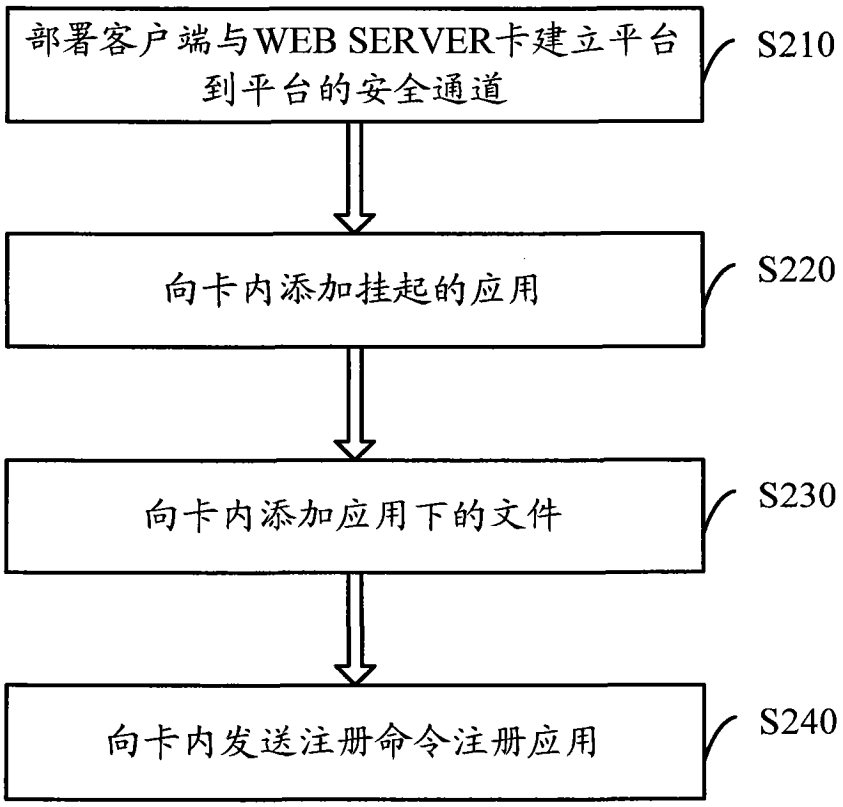

部署客户端与WEB SERVER卡建立平台到平台的安全通道
S210
向卡内添加挂起的应用
S220
向卡内添加应用下的文件
S230
向卡内发送注册命令注册应用
S240

图 2

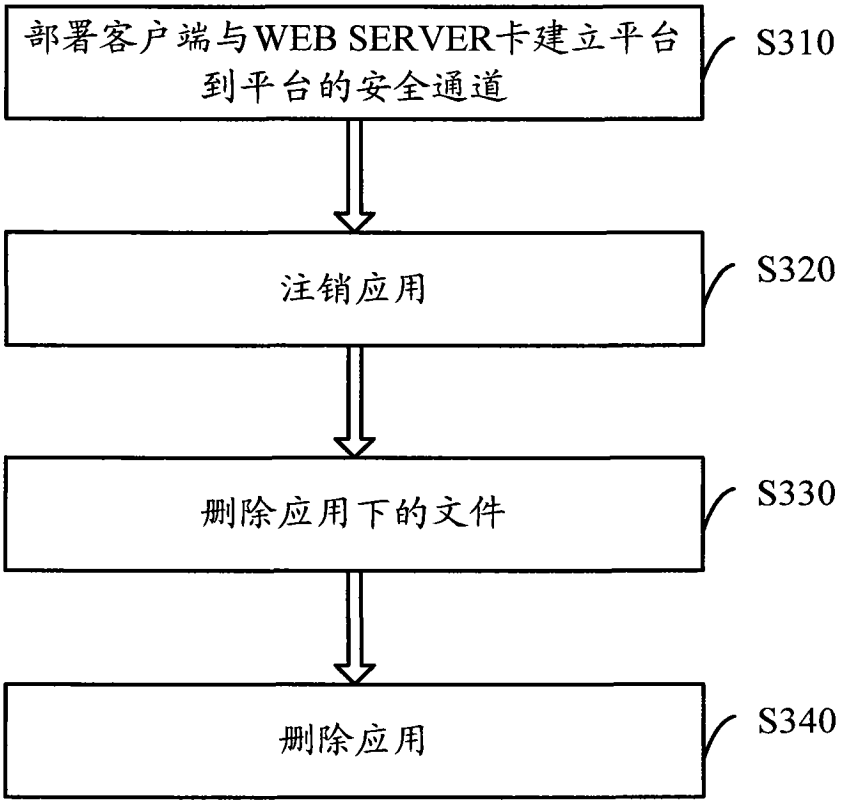

部署客户端与WEB SERVER卡建立平台到平台的安全通道
S310
注销应用
S320
删除应用下的文件
S330
删除应用
S340

图 3

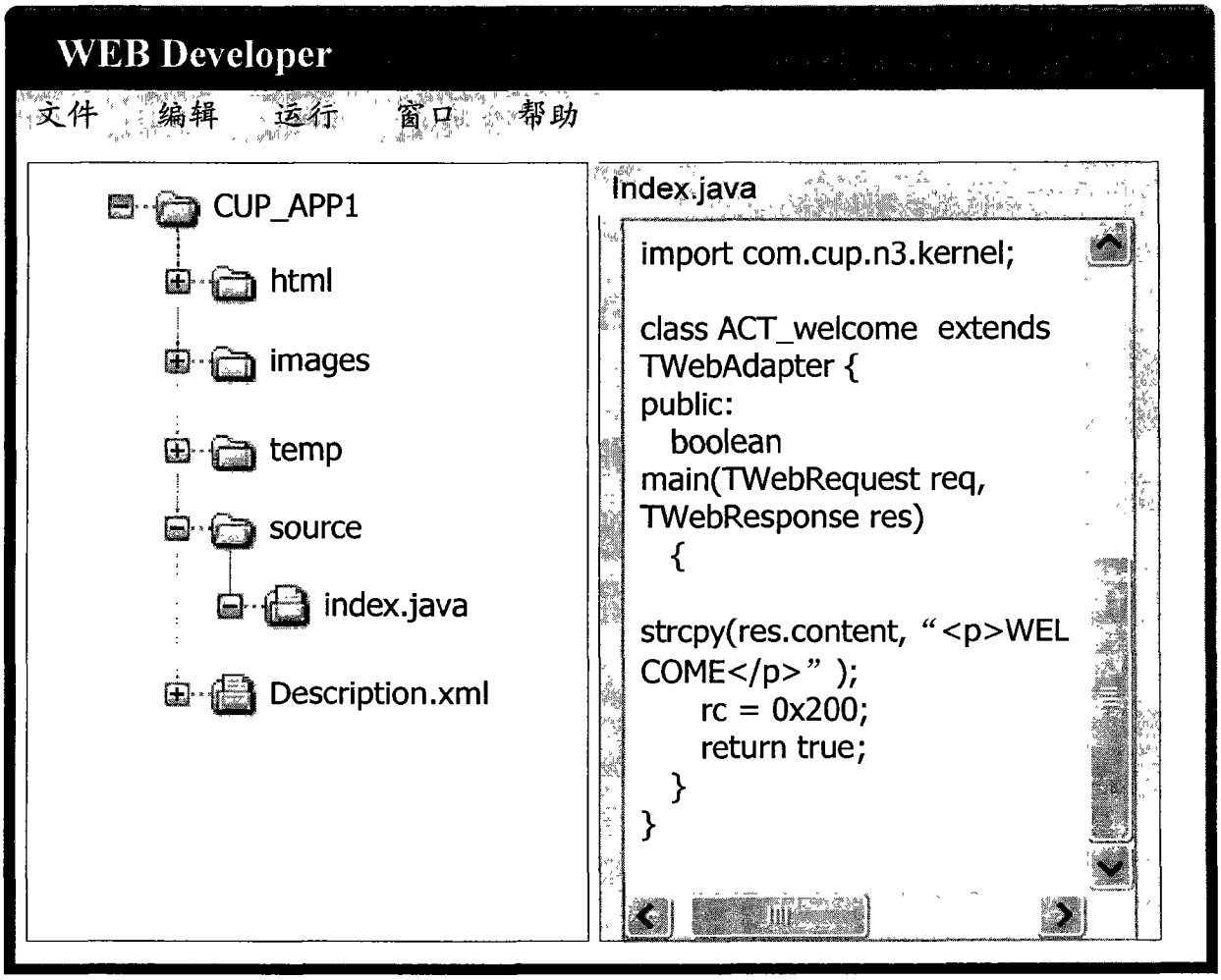

WEB Developer
文件 编辑 运行 窗口 帮助
CUP_APP1
html
images
temp
source
index.java
Description.xml
index.java
import com.cup.n3.kernel;
class ACT_welcome extends TWebAdapter {
public:
boolean
main(TWebRequest req, TWebResponse res)
{
strcpy(res.content, " WELCOME ");
rc = 0x200;
return true;
}
}

图 4

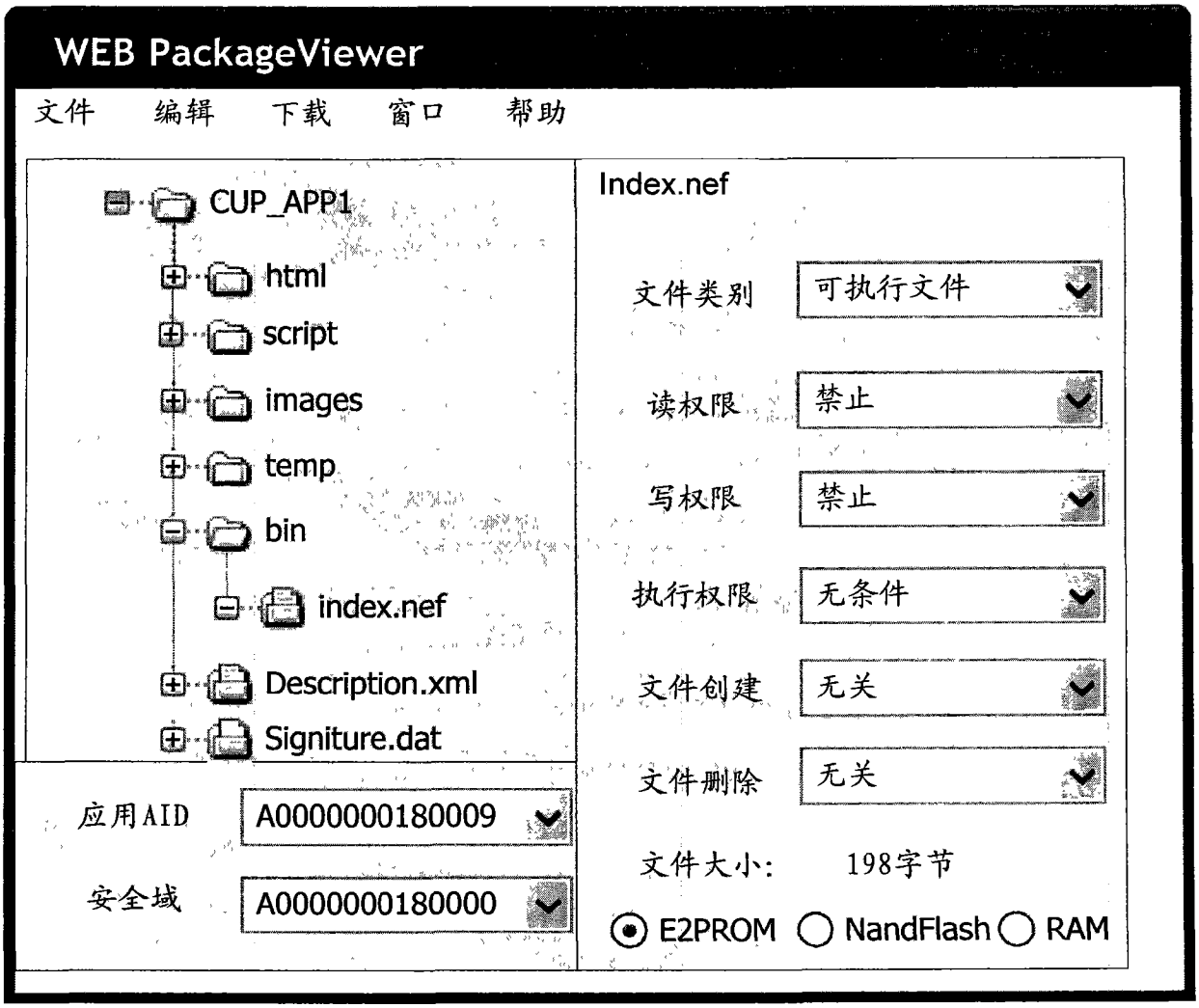

WEB PackageViewer
文件
编辑
下载
窗口
帮助
CUP_APP1
html
script
images
temp
bin
index.nef
Description.xml
Signiture.dat
应用AID
A0000000180009
安全域
A0000000180000
Index.nef
文件类别
可执行文件
读权限
禁止
写权限
禁止
执行权限
无条件
文件创建
无关
文件删除
无关
文件大小:
198字节
E2PROM
NandFlash
RAM

图 5

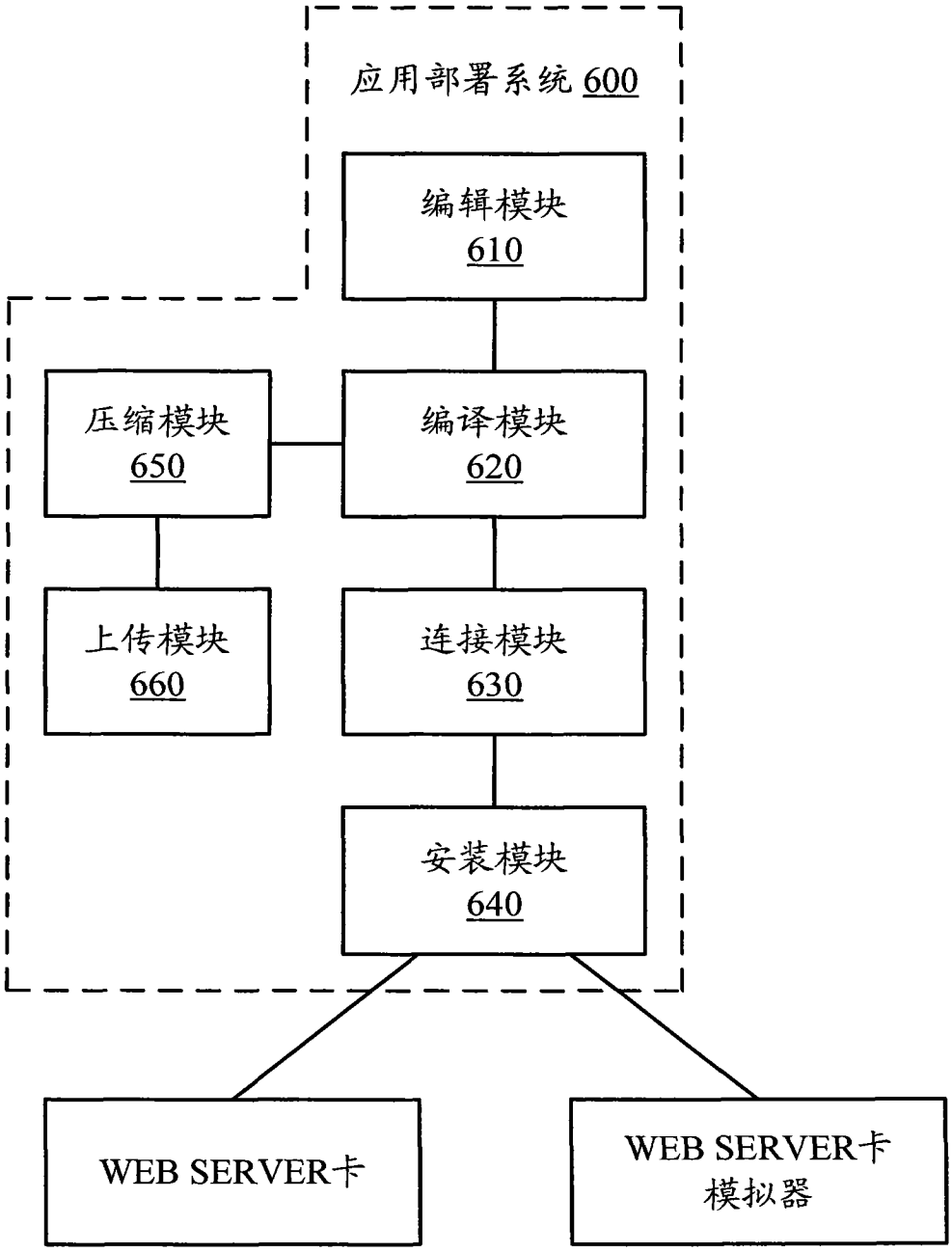

应用部署系统 600
编辑模块
610
压缩模块
650
编译模块
620
上传模块
660
连接模块
630
安装模块
640
WEB SERVER卡
WEB SERVER卡
模拟器

图 6

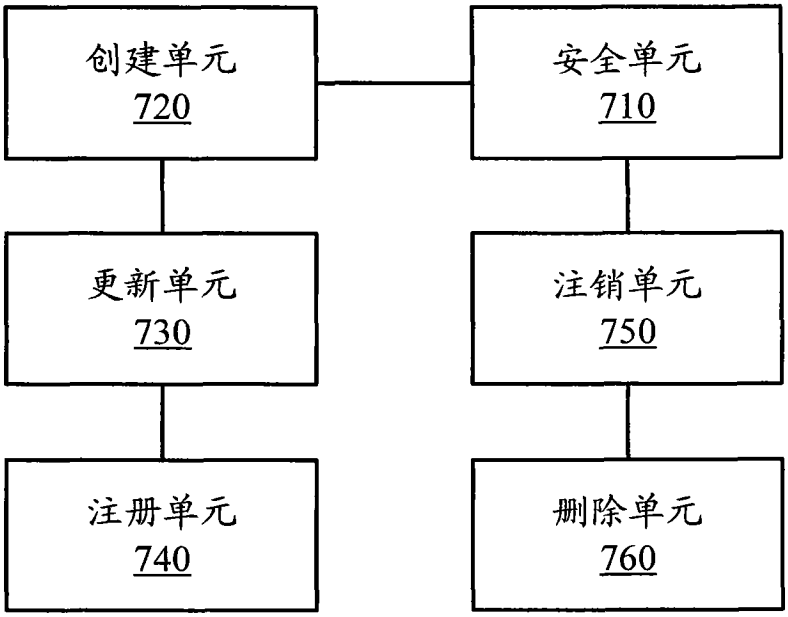


图 7

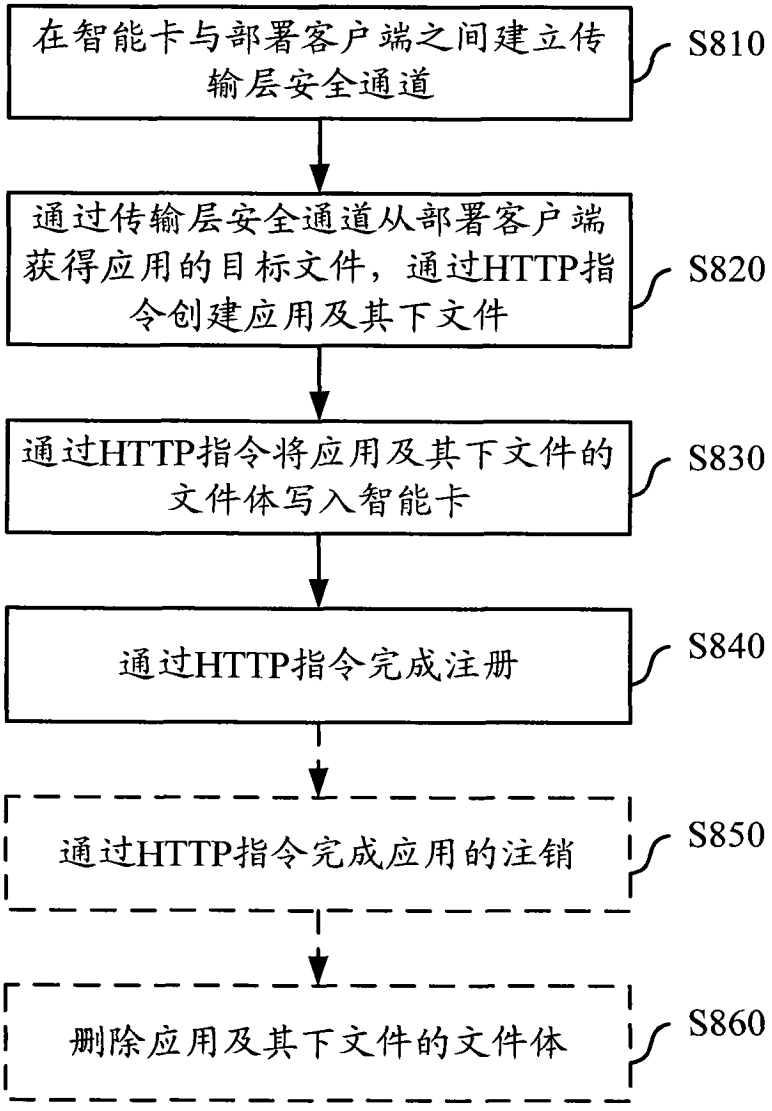

在智能卡与部署客户端之间建立传输层安全通道
S810
通过传输层安全通道从部署客户端获得应用的目标文件，通过HTTP指令创建应用及其下文件
S820
通过HTTP指令将应用及其下文件的文件体写入智能卡
S830
通过HTTP指令完成注册
S840
通过HTTP指令完成应用的注销
S850
删除应用及其下文件的文件体
S860

图 8