(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 101783800 B
(45)授权公告日 2012.12.19

(21)申请号 201010104404.7
(22)申请日 2010.01.27
(73)专利权人 华为终端有限公司
地址 518129 广东省深圳市龙岗区坂田华为基地 B 区 2 号楼
(72)发明人 吴勇锋
(74)专利代理机构 北京凯特来知识产权代理有限公司 11260
代理人 郑立明 焦丽
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 101043338 A,2007.09.26,
US 7035830 B1,2006.04.25,
CN 101115060 A,2008.01.30,
CN 1507733 A,2004.06.23,

审查员 董振兴

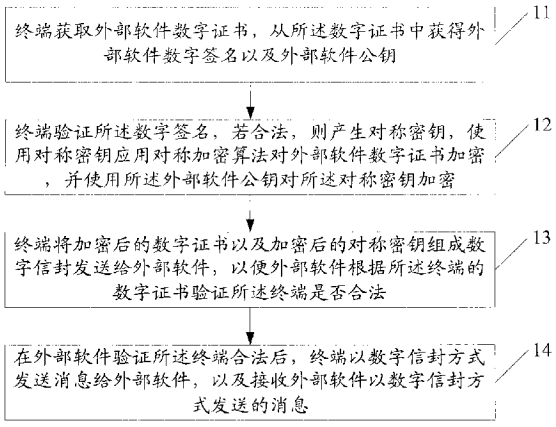
权利要求书 2 页 说明书 8 页 附图 5 页

(54)发明名称

一种嵌入式系统安全通信方法、装置及系统

(57)摘要

本发明实施例涉及通信领域一种嵌入式系统安全通信方法、装置及系统，终端获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥；终端验证所述数字签名，若合法，则产生对称密钥，使用对称密钥应用对称加密算法对外部软件数字证书加密，并使用所述外部软件公钥对所述对称密钥加密；终端将加密后的数字证书以及加密后的对称密钥组成数字信封发送给外部软件；在外部软件验证所述终端合法后，终端以数字信封方式发送消息给外部软件。本发明实施例实现了嵌入式系统通信终端和 PC 软件之间的通信进行双向认证和加密传输，保证了传输接口上的数据安全；使嵌入式通信终端与相应的外部软件之间的通信更加安全、可靠。



CN 101783800 B

1. 一种嵌入式系统安全通信方法，其特征在于，包括：

终端获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥；

终端验证所述数字签名，若合法，则产生对称密钥；使用对称密钥应用对称加密算法对外部软件数字证书加密，并使用所述外部软件公钥对所述对称密钥加密；

终端将加密后的数字证书以及加密后的对称密钥组成数字信封发送给外部软件，以便外部软件根据所述终端的数字证书验证所述终端是否合法；

在外部软件验证所述终端合法后，终端以数字信封方式发送消息给外部软件，以及接收外部软件以数字信封方式发送的消息。

2. 如权利要求 1 所述的方法，其特征在于，所述终端获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥包括：

终端获取外部软件加密数字证书，使用存储的根密钥的公钥解密所述数字证书获得外部软件数字签名以及外部软件公钥。

3. 如权利要求 1 或 2 所述的方法，其特征在于，终端获取外部软件数字证书后，所述方法还包括：

检查数字证书内容，获得数字证书允许的功能和范围以及数字证书有效时间。

4. 如权利要求 2 所述的方法，其特征在于，所述根密钥与使用根密钥的终端的种类对应，不同种类的终端使用不同的根密钥。

5. 如权利要求 1 所述的方法，其特征在于，所述外部软件根据所述终端的数字证书验证所述终端是否合法包括：

使用外部软件的私钥解密出对称密钥，使用解密出的对称密钥解密出所述终端的数字证书，根据所述终端的数字证书验证所述终端是否合法。

6. 如权利要求 1 所述的方法，其特征在于，所述终端以数字信封方式发送消息给外部软件包括：

产生对称密钥，使用对称密钥应用对称加密算法对消息加密，并使用所述外部软件公钥对所述对称密钥加密；将加密后的消息以及加密后的对称密钥组成数字信封发送给外部软件。

7. 如权利要求 1 或 6 所述的方法，其特征在于，终端以数字信封方式发送消息给外部软件过程中，所述产生对称密钥的步骤包括：

每间隔预定时间切换所述对称密钥；或每次产生不同的对称密钥。

8. 如权利要求 1 所述的方法，其特征在于，接收外部软件以数字信封方式发送的消息后，所述方法还包括：

使用终端的私钥解密出对称密钥，使用解密出的对称密钥解密出消息。

9. 一种嵌入式系统安全通信终端，其特征在于，包括：

获取单元，用于获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥；

验证单元，用于验证所述数字签名是否合法；

加密单元，用于产生对称密钥，使用对称密钥应用对称加密算法对发送给外部软件的消息加密，并使用所述外部软件公钥对所述对称密钥加密；

发送单元，用于将加密单元加密后的消息以及加密后的对称密钥组成数字信封发送给外部软件，以便外部软件根据所述终端的数字证书验证所述终端是否合法；

接收单元，用于在外部软件验证所述终端合法后，接收外部软件以数字信封方式发送的消息。

10. 如权利要求 9 所述的终端，其特征在于，还包括：

存储单元，用于安全存储数字证书、根密钥、本终端私钥以及指定的其他终端的数字证书。

11. 如权利要求 9 所述的终端，其特征在于，还包括：

第一解密单元，用于使用存储的根密钥的公钥解密所述数字证书获得外部软件数字签名以及外部软件公钥。

12. 如权利要求 9 所述的终端，其特征在于，还包括：

第二解密单元，用于使用本终端的私钥解密出所接收的数字信封方式发送的消息的对称密钥，使用解密出的对称密钥解密出所接收的消息。

13. 一种嵌入式系统，其特征在于，包括：个人电脑 PC 以及如权利要求 9 － 12 中任一项所述的终端，所述 PC 安装有外部软件；

所述外部软件，用于验证所述终端是否合法，若合法，则采用数字信封方式发送消息给所述终端。

14. 如权利要求 13 所述的系统，其特征在于，所述采用数字信封方式发送消息给所述终端包括：产生对称密钥，使用对称密钥应用对称加密算法对发送给终端的消息加密，使用终端的公钥对所述对称密钥加密，将加密后的消息和对称密钥组成数字信封发送给所述终端。

15. 如权利要求 13 所述的系统，其特征在于，所述外部软件还用于安全存储数字证书、根密钥、本软件私钥以及指定的其他终端的数字证书。

一种嵌入式系统安全通信方法、装置及系统

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种嵌入式系统安全通信方法、装置及系统。

背景技术

[0002] 嵌入式系统在无线通信终端中得到了广泛的应用，如无线手机、无线网关、无线数据卡等。在一定情况下，用户希望终端能够受控使用，如无线 Modem，常接入个人电脑 (PC，personal computer) 上的通用串行总线 (USB，Universal Serial Bus)，通过 PC 上的应用程序 (Application) 提供基本的拨号上网服务。除此之外，还可能提供特殊的业务，如应用类的增值业务，网络规划需要的特殊支持，以及 Modem 的改制 (rework)。这类业务不同于基本业务，应在一定的条件下进行使用，即对 PC 软件（业务）和终端要求满足一定的关系才能正常使用，一般地将 PC 软件与终端的特定关系定义为捆绑使用，即一对一或一对多的关系，此时双方需进行互相认证，确保满足预先定义的匹配关系。然而发明人在实施本发明过程中发现，现有技术至少存在如下缺点：

[0003] 现有嵌入式系统中，PC 软件与终端之间的通信过程中的数据采用明文传输，存在很大的安全隐患。

发明内容

[0004] 本发明实施例提供一种嵌入式系统安全通信方法、装置及系统，解决现有的嵌入式系统终端与外部软件之间通信过程中存在的安全隐患。

[0005] 本发明实施例是通过以下技术方案实现的：

[0006] 本发明实施例提供一种嵌入式系统安全通信方法，包括：

[0007] 终端获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥；

[0008] 终端验证所述数字签名，若合法，则产生对称密钥；使用对称密钥应用对称加密算法对外部软件数字证书加密，并使用所述外部软件公钥对所述对称密钥加密；

[0009] 终端将加密后的数字证书以及加密后的对称密钥组成数字信封发送给外部软件，以便外部软件根据所述终端的数字证书验证所述终端是否合法；

[0010] 在外部软件验证所述终端合法后，终端以数字信封方式发送消息给外部软件，以及接收外部软件以数字信封方式发送的消息。

[0011] 本发明实施例提供一种嵌入式系统安全通信终端，包括：

[0012] 获取单元，用于获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥；

[0013] 验证单元，用于验证所述数字签名是否合法；

[0014] 加密单元，用于产生对称密钥，使用对称密钥应用对称加密算法对发送给外部软件的消息加密，并使用所述外部软件公钥对所述对称密钥加密；

[0015] 发送单元，用于将加密单元加密后的消息以及加密后的对称密钥组成数字信封发

送给外部软件。

[0016] 本发明实施例提供一种嵌入式系统，包括：外部软件以及上面所述的终端；

[0017] 所述外部软件，用于验证所述终端是否合法，若合法，则采用数字信封方式发送消息给所述终端。

[0018] 由上述本发明实施例提供的技术方案可以看出，本发明实施例实现了嵌入式系统通信终端和 PC 软件之间的通信进行双向认证和加密传输，通过数字证书确认对方的合法身份，通过数字信封保证信息的安全传输，加密密钥由发送方独立选择切换，保证了传输接口上的数据安全；使嵌入式通信终端与相应的外部软件之间的通信更加安全、可靠。

附图说明

[0019] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0020] 图 1 为本发明实施例一种嵌入式系统安全通信方法流程图；

[0021] 图 2 为本发明实施例一种嵌入式系统安全通信方法场景一流程图；

[0022] 图 3 为本发明实施例一种嵌入式系统安全通信方法场景二流程图；

[0023] 图 4 为本发明实施例一种嵌入式系统安全通信终端结构示意图；

[0024] 图 5 为本发明又一实施例一种嵌入式系统安全通信终端结构示意图；

[0025] 图 6 为本发明另一实施例一种嵌入式系统安全通信终端结构示意图；

[0026] 图 7 为本发明实施例一种嵌入式系统结构示意图。

具体实施方式

[0027] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，可以理解的是，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0028] 本发明一个实施例提供一种嵌入式系统安全通信方法，以图 1 中所示为例，包括如下步骤：

[0029] 步骤 11：终端获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥；

[0030] 步骤 12：终端验证所述数字签名，若合法，则产生对称密钥，使用对称密钥应用对称加密算法对外部软件数字证书加密，并使用所述外部软件公钥对所述对称密钥加密；

[0031] 步骤 13：终端将加密后的数字证书以及加密后的对称密钥组成数字信封发送给外部软件，以便外部软件根据所述终端的数字证书验证所述终端是否合法；

[0032] 步骤 14：在外部软件验证所述终端合法后，终端以数字信封方式发送消息给外部软件，以及接收外部软件以数字信封方式发送的消息。

[0033] 本发明实施例终端和外部软件采用同一认证中心 (CA，CertificationAuthority) 发布的数字证书，对于终端的数字证书，CA 中心使用指定的不对称加密算法，对每个终端产

生一对公钥、私钥对 (key pair)。CA 选择某一根密钥 ROOT-KEYx，对产生的终端公钥，加上 IMEI 或其他标识符数据通过 HASH 算法生成摘要 Digest，再用根密钥 ROOT-KEYx 的私钥对摘要 Digest 值进行签名产生相应的数字证书。CA 将终端的数字证书及相应的 ROOT-KEYx 发给终端作为保密数据进行安全存储。

[0034] 对于外部软件的数字证书，采用 CA 中心指定的不对称加密算法，CA 中心为外部软件产生一对公私钥 (key pair)，CA 使用外部软件的版本信息及其他数据，通过 HASH 算法产生消息摘要，再选择某一 ROOT-KEYx，用其私钥进行签名，“证书头 + 所有数据 + 签名”组成数字证书，再用已选择的 ROOT-KEYx 的私钥对整个数字证书进行加密，形成外部软件的加密数字证书 ；CA 将加密数字证书 +ROOT-KEY 的公钥一起发给外部软件作为保密数据进行安全存储 ；本发明实施例所述外部软件包括 PC 软件或其他使用终端接入无线网络的系统，如网关 (Gateway)，机顶盒等外部软件。对于 PC 软件来说，CA 可以针对 PC 软件的某种特征，如 PC 软件所安装的 PC 机硬件配置，或针对 PC 软件特有的数据产生有时间期限 (时间戳) 的数字证书。本发明实施例所述的 PC 软件的安全存储方法可以采用常用的 USB key，也可以采用 PC 上已有的硬件、软件方法，例如新技术文件系统 (NTFS，New Technology File System) 中提供的安全文件系统。

[0035] CA 中心产生多个公私钥对 (POOT-KEYx，x ＝ 1，2，…N) 作为根密钥 ROOT-KEY，ROOT-KEY 的密钥应使用 1024 位或 2048 位，CA 中心负责管理根密钥的私钥安全性 ；在生成终端和外部软件数字证书过程中使用的所述 ROOT-KEYx 为从多个根密钥 ROOT-KEY 中选择的一个根密钥。所述根密钥与使用根密钥的终端的种类对应，不同种类的终端使用不同的根密钥，降低了因一个根密钥失密而所有相关产品被破解的概率。

[0036] 所述终端和外部软件中除安全保存所述 CA 分配的根密钥、数字证书外，还安全保存有所述 CA 分配的本终端的公私钥对，以及指定的其他终端的数字证书。例如，在终端中还保存有终端的私钥及外部软件的数字证书，在外部软件中还保存有外部软件的私钥及终端的数字证书。

[0037] 在步骤 11 中，一个实施例所述终端获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥的方法包括 ：终端获取外部软件加密数字证书，使用存储的根密钥的公钥解密所述数字证书获得外部软件数字签名以及外部软件公钥。

[0038] 在步骤 11 中，终端获取外部软件数字证书后，所述方法还包括 ：

[0039] 检查数字证书内容，获得数字证书允许的功能和范围以及数字证书有效时间。在数字证书中对功能和使用范围作了限制，在数字证书中预置许可的功能和使用范围，结合数字证书有效时间，可以用来防止数字证书被滥用和非法扩大化使用。例如，将终端支持的功能分类为 A、B、C 和 D，而外部软件发来的证书中仅写了 A 和 B，则终端只允许外部软件使用功能 A、B，如这时外部软件要求终端提供 C 或 D 的功能，则终端有权拒绝，即回复要求超出范围，或不予处理。

[0040] 在步骤 12 中，终端验证所述数字签名是否合法，即验证所述数字签名是否有效，具体验证方法为现有技术，本发明对此不做限定。

[0041] 在步骤 12 中，对于对称密钥的产生算法，可以由终端和外部软件之间预先协商确定，也可以由 CA 指定。终端与外部软件使用同样的随机数、时间信息等作为输入参数，使用约定的或 CA 指定的算法产生单次会话使用的对称密钥，也可以称为会话密钥。所述对称加

密算法可以由终端和外部软件之间预先协商确定，也可以由 CA 指定。

[0042] 在步骤 13 中，一种实施例所述外部软件根据所述终端的数字证书验证所述终端是否合法包括：使用外部软件的私钥解密出对称密钥，使用解密出的对称密钥解密出所述终端的数字证书，根据所述终端的数字证书验证所述终端是否有效。

[0043] 在步骤 14 中，所述终端以数字信封方式发送消息给外部软件包括：产生对称密钥，使用对称密钥应用对称加密算法对消息加密，并使用所述外部软件公钥对所述对称密钥加密；将加密后的消息以及加密后的对称密钥组成数字信封发送给外部软件。

[0044] 所述产生的对称密钥可以每间隔预定时间更换；或也可以每次都产生不同的对称密钥。

[0045] 在步骤 14 中，接收外部软件以数字信封方式发送的消息后，所述方法还包括：使用终端的私钥解密出对称密钥，使用解密出的对称密钥解密出消息。

[0046] 从上述描述可知，本发明实施例在通信双方互相验证对方合法后，双方采用各自独立的数字信封方式发送消息，不但省略了密钥交换过程，降低了密钥交换环节的风险，而且数字信封的使用保证了各个传输方向上的信息安全；每个发送方可按照自己的规则独立切换对称密钥，进一步增强了安全性。本发明实施例对数字证书的安全存储及传输方案减少了破解数字证书和公钥的机会，增强了通信过程的整体安全性。

[0047] 为进一步理解本发明，下面以不同场景对嵌入式系统安全通信方法进行详细介绍，

[0048] 场景一：嵌入式系统中终端与 PC 软件交互，PC 软件使用 USB key，PC 软件的私钥存储于 USB key 内，加解密操作仅在 USB key 内进行，具体操作流程如图 2 中所示，包括如下步骤：

[0049] 步骤 20：PC 软件发送连接请求消息 (PC Request)，同时携带 PC 软件当前的通用协调时间 UTC；

[0050] 本步骤中 PC 软件可使用明文发送该连接请求消息。

[0051] 步骤 21：终端收到该连接请求消息后，发送本终端标识信息作为响应消息给该 PC 软件；

[0052] 本发明实施例中终端的标识信息可以为单板的 IMEI 或 CA 为终端分配的唯一的公私钥对作为终端的唯一标识信息。

[0053] 步骤 22：PC 软件从 USB key 中取出相应的加密数字证书发给终端；

[0054] PC 软件接收到连接响应消息后，确定与终端连接成功，则可以判断是否有 USB key，如有 USB key，则从 USB key 中取出相应的加密数字证书 Pse，发送给终端；

[0055] 步骤 23：终端收到数字证书后，用已存储的 ROOT-KEYx 的公钥对加密数字证书进行解密，解密成功后再对数字证书中的数字签名验证是否有效，包括有效周期的检验，同时取出 PC 软件的公钥 Ps1 备用；

[0056] 终端检查数字证书允许的功能和范围，如发现是针对“PC 软件非特定终端”的证书，即 PC 软件与某一类的所有终端均可通信，终端则准备发送自己的数字证书 D1（包含公钥）给 PC 软件，一种实施例发送自己的数字证书给 PC 软件的方法包括：

[0057] 首先，产生一个会话密钥 Ku1，通过 Ku1 采用对称加密算法对 D1 进行加密生成 D1’，再用 PC 软件的公钥 Ps1 对 Ku1 加密生成 Ku1’，将 Ku1’+D1’组成数字信封 E1 发给 PC

软件；该会话密码是一种对称密钥。

[0058] 步骤 24：PC 软件收到终端发来的数字信封 E1 后，先用本身的私钥解密 Ku1’得到 Ku1，然后用 Ku1 解密 D1’得到 D1，再对 D1 证书验证是否有效，包括有效周期的检验，有效则取出 D1 中终端的公钥 Pu1 备用；

[0059] 所有解密和验证均在 USB Key 中进行。

[0060] PC 软件与终端之间的互相验证通过后，PC 软件可以和终端之间执行进一步的操作。

[0061] PC 软件可按照同样的方法产生数字信封发送命令或请求给终端，例如：产生对称密钥 Kp1，用 Kp1 及对称加密算法对发送给终端的命令 \ 请求的消息进行加密生成 CR’，再用终端的 Pu1 对 Kp1 加密生成 Kp1’，Kp1’+CR’组成数字信封 S1 发给终端。

[0062] 步骤 25：终端解密出 PC 软件发来的数字信封 S1 后，根据命令 \ 请求消息的要求准备回复数据 R1，终端对发送给 PC 软件的数据通过数字信封方式发送；

[0063] 例如，终端可选择新的会话密钥 Ku2 加密 R1，也可选择使用上次的 Ku1。也就是说，终端可按照一定的规则自行选择切换会话密钥 Ku。

[0064] 步骤 26：PC 软件使用数字信封给终端发送命令或请求；

[0065] 同样，PC 软件可按照一定的规则自行选择切换会话密钥 Kp。

[0066] 上述处理流程中，任一验证过程失败将导致流程终止。

[0067] 终端和 PC 软件间可以通过定时器来维护链路的连续性 (HeartbeatTimer)，如定时器超时仍未收到对方数据，则本次加密通信过程结束。下次通信需重新启动以上所述的双向认证和加密传输过程。

[0068] 本实施例终端和 PC 软件之间的通信进行双向认证和加密传输，通过数字证书确认对方的合法身份，通过数字信封保证信息的安全传输，加密密钥由发送方独立选择切换，保证了传输接口上的数据安全；使嵌入式通信终端与相应的外部软件之间的通信更加安全、可靠。

[0069] 场景二：嵌入式系统中终端与 PC 软件交互，PC 软件未使用 USB key，私钥由 PC 软件加密存储，具体操作流程如图 3 中所示，包括如下步骤：

[0070] 步骤 30：PC 软件发送连接请求消息 (PC Request)，同时携带 PC 软件当前的通用协调时间 UTC；

[0071] 本步骤中 PC 软件可使用明文发送该连接请求消息。

[0072] 步骤 31：终端收到该连接请求消息后，发送本终端标识信息作为响应消息给该 PC 软件；

[0073] 本发明实施例中终端的标识信息可以为单板的 IMEI 或 CA 为终端分配的唯一的公私钥对作为终端的唯一标识信息。

[0074] 步骤 32：PC 软件根据终端的唯一标识信息查找相应的数字证书（包含 PC 软件的公钥、终端的公钥）和 ROOT-KEYx，将相应的数字证书发给终端；PC 软件同时取出终端对应的公钥 P1 备用；本发明一个实施例所述 PC 软件根据终端的唯一标识信息查找相应的数字证书的方法包括：PC 软件预先存储一个或多个将用于通信的终端的证书，并对这些证书建立一个索引表，索引表以终端的特定标识信息作为索引值，如每个终端都有唯一值的 IMEI，则 PC 软件以该终端的唯一作为索引来查找相应的数字证书。

[0075] PC 软件接收到连接响应消息后，确定与终端连接成功，则可以判断是否有 USB key，如没有 USB key，则根据终端的唯一标识信息查找数字证书 Pse，发送给终端；

[0076] 步骤 33：终端收到数字证书后，用已存储的 ROOT-KEYx 的公钥对加密数字证书进行解密，解密成功后再对数字证书中的数字签名验证是否有效，包括有效周期的检验；

[0077] 终端检查数字证书允许的功能和范围，如发现是针对自己的公钥及 IMEI，则回复 PC 软件 UE Confirm，同时取出 PC 软件的公钥 Ps1 备用以及证书的许可功能及使用范围。

[0078] 步骤 34：PC 软件收到终端发来的 UE Confirm，使用数字信封的方式向终端发送命令或请求 (command、Request) 开始进一步的操作。

[0079] 例如，该以数字信封方式发送命令或请求的方法包括：首先产生会话密钥（对称密钥）Kp1，用 Kp1 及对称加密算法对 command/request 进行加密生成 CR'，再用终端的 Pu1 对 Kp1 加密生成 Kp1'，Kp1'+CR' 组成数字信封 S1 发给终端 (PC Command)。

[0080] 步骤 35：终端解密 PC 软件发来的数字信封 S1 后，根据命令 \ 请求消息判断其是否有效（证书中已许可）后并准备回复数据 R1，终端以数字信封方式发送回复的内容；一个实施例所述根据命令 \ 请求消息判断其是否有效的方法包括：如前面所述，在数字证书中会指明终端可接受 PC 哪些类功能，而该条命令 \ 请求消息可归类到某一类功能的其中一条，终端判断这一具体命令 \ 请求消息是否在证书已指明可接受的类别中，如果在，则命令有效，否则命令无效。

[0081] 该终端自行选择发送方向的会话密钥（对称密钥）Ku1 对 R1 加密生成 R1'，再用 Ps1 对 Ku1 加密生成 Ku1'，Ku1'+R1' 组成数字信封发给 PC 软件，该终端可按照一定的规则自行选择切换对称密钥 Ku。

[0082] 步骤 36：PC 软件使用数字信封给终端发送命令或请求；

[0083] 同样，PC 软件可按照一定的规则自行选择切换会话密钥 Kp。

[0084] 上述处理流程中，任一验证过程失败将导致流程终止。

[0085] 终端和 PC 软件间可以通过定时器来维护链路的连续性 (HeartbeatTimer)，如定时器超时仍未收到对方数据，则本次加密通信过程结束。下次通信需重新启动以上所述的双向认证和加密传输过程。

[0086] 本实施例终端和 PC 软件之间的通信进行双向认证和加密传输，通过数字证书确认对方的合法身份，通过数字信封保证信息的安全传输，加密密钥由发送方独立选择切换，保证了传输接口上的数据安全；使嵌入式通信终端与相应的外部软件之间的通信更加安全、可靠。

[0087] 本发明实施例还提供一种嵌入式系统安全通信终端，如图 4 所示，包括：获取单元 40、验证单元 41、加密单元 42、以及发送单元 43；

[0088] 所述获取单元 40，用于获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥；

[0089] 所述验证单元 41，用于验证所述数字签名是否合法；

[0090] 所述加密单元 42，用于产生对称密钥，使用对称密钥应用对称加密算法对发送给外部软件的消息加密，并使用所述外部软件公钥对所述对称密钥加密；该产生的对称密钥可按照一定的规则自行选择切换，例如，每次产生不同的对称密钥或每间隔预定时间更换产生的对称密钥。该发送给外部软件的消息包括本终端的数字证书、请求或命令等。将本

终端的数字证书加密传输给外部软件以便于外部软件对本终端进行合法性验证，实现双向身份验证的目的。

[0091] 所述发送单元 43，用于将加密单元加密后的消息以及加密后的对称密钥组成数字信封发送给外部软件。

[0092] 如图 5 所示，所述终端还可以包括 ：

[0093] 存储单元 44，用于安全存储数字证书、根密钥、本终端私钥以及指定的其他终端的数字证书。和 / 或

[0094] 第一解密单元 45，用于使用存储的根密钥的公钥解密所述数字证书获得外部软件数字签名以及外部软件公钥。

[0095] 如图 6 所示，所述终端还可以包括 ：

[0096] 接收单元 46，用于接收以数字信封方式发送的消息 ；

[0097] 第二解密单元 47，用于使用本终端的私钥解密出所接收的数字信封方式发送的消息的对称密钥，使用解密出的对称密钥解密出所接收的消息。

[0098] 本实施例所述安全通信终端和 PC 软件之间的通信进行双向认证和加密传输，通过数字证书确认对方的合法身份，通过数字信封保证信息的安全传输，加密密钥由发送方独立选择切换，保证了传输接口上的数据安全 ；使嵌入式通信终端与相应的外部软件之间的通信更加安全、可靠。

[0099] 本发明实施例还提供一种嵌入式系统，如图 7 所示，该系统包括 ：外部软件 71 以及如上面实施例所述的安全通信终端 70 ；

[0100] 所述安全通信终端 70，用于获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥，验证所述数字签名是否合法，若合法，则产生对称密钥，使用对称密钥应用对称加密算法对发送给外部软件的消息加密，并使用所述外部软件公钥对所述对称密钥加密，将加密单元加密后的消息以及加密后的对称密钥组成数字信封发送给外部软件。具体功能及结构同上面实施例中所述，此处不再赘述。

[0101] 所述外部软件 71，用于验证所述终端是否合法，若合法，则采用数字信封方式发送消息给所述终端。所述采用数字信封方式发送消息给所述终端包括 ：产生对称密钥，使用对称密钥应用对称加密算法对发送给终端的消息加密，使用终端的公钥对所述对称密钥加密，将加密后的消息和对称密钥组成数字信封发送给所述终端。

[0102] 所述外部软件 71，还用于安全存储数字证书、根密钥、本软件私钥以及指定的其他终端的数字证书。

[0103] 所述终端 70 与所述外部软件 71 之间可通过 USB 等物理接口承载，本发明实施例对于 USB 接口的承载及驱动不做限定。

[0104] 本实施例所述嵌入式系统，终端和 PC 软件之间的通信进行双向认证和加密传输，通过数字证书确认对方的合法身份，通过数字信封保证信息的安全传输，加密密钥由发送方独立选择切换，保证了传输接口上的数据安全 ；使嵌入式通信终端与相应的外部软件之间的通信更加安全、可靠。

[0105] 综上所述，本发明实施例实现了嵌入式系统的安全通信，也就是嵌入式通信终端和 PC 软件之间的通信进行双向认证和加密传输，通过数字证书确认对方的合法身份，通过数字信封保证信息的安全传输，加密密钥由发送方独立选择切换，保证了传输接口上的数

据安全；使嵌入式通信终端与相应的外部软件之间的通信更加安全、可靠。

[0106] 本领域普通技术人员可以理解，实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一计算机可读存储介质中，例如只读存储器（简称 ROM）、随机存取存储器（简称 RAM）、磁盘、光盘等。

[0107] 以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

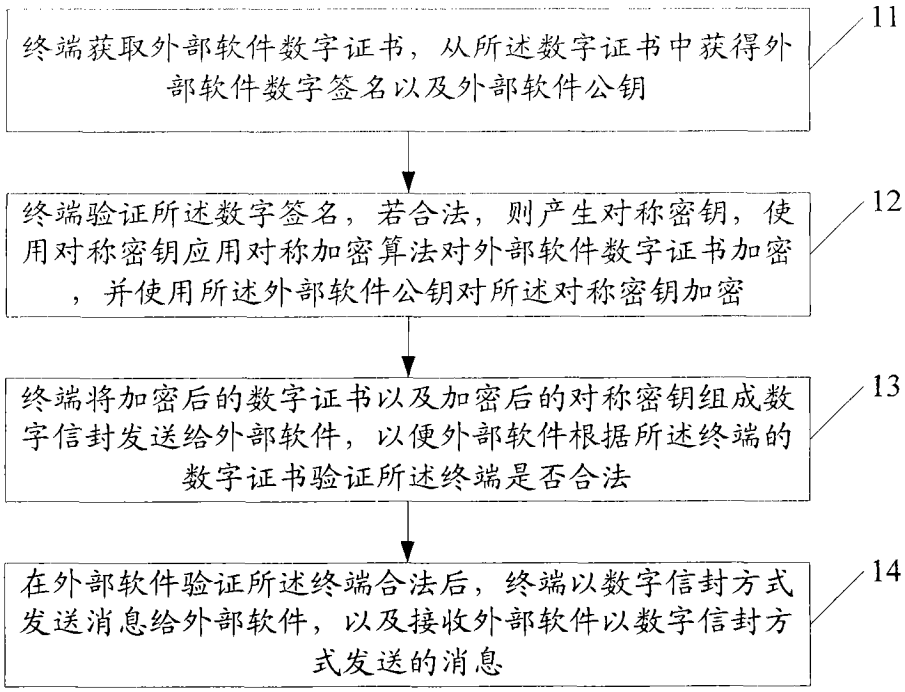

终端获取外部软件数字证书，从所述数字证书中获得外部软件数字签名以及外部软件公钥
11
终端验证所述数字签名，若合法，则产生对称密钥，使用对称密钥应用对称加密算法对外部软件数字证书加密，并使用所述外部软件公钥对所述对称密钥加密
12
终端将加密后的数字证书以及加密后的对称密钥组成数字信封发送给外部软件，以便外部软件根据所述终端的数字证书验证所述终端是否合法
13
在外部软件验证所述终端合法后，终端以数字信封方式发送消息给外部软件，以及接收外部软件以数字信封方式发送的消息
14

图 1

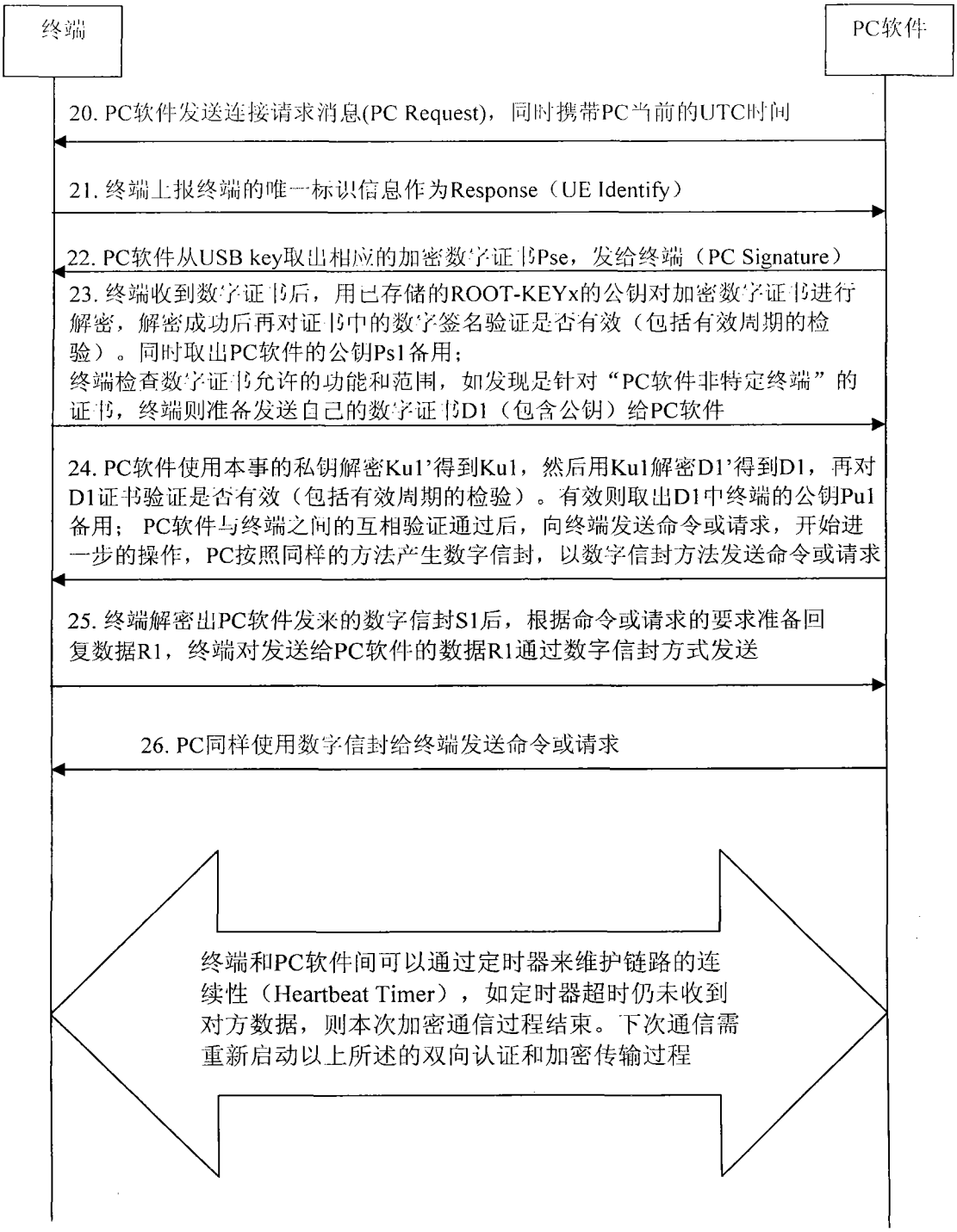

终端
PC软件
20. PC软件发送连接请求消息(PC Request)，同时携带PC当前的UTC时间
21. 终端上报终端的唯一标识信息作为Response（UE Identify）
22. PC软件从USB key取出相应的加密数字证书Pse，发给终端（PC Signature）
23. 终端收到数字证书后，用已存储的ROOT-KEYx的公钥对加密数字证书进行解密，解密成功后再对证书中的数字签名验证是否有效（包括有效周期的检验）。同时取出PC软件的公钥Ps1备用；
终端检查数字证书允许的功能和范围，如发现是针对“PC软件非特定终端”的证书，终端则准备发送自己的数字证书D1（包含公钥）给PC软件
24. PC软件使用本事的私钥解密Ku1'得到Ku1，然后用Ku1解密D1'得到D1，再对D1证书验证是否有效（包括有效周期的检验）。有效则取出D1中终端的公钥Pu1备用； PC软件与终端之间的互相验证通过后，向终端发送命令或请求，开始进一步的操作，PC按照同样的方法产生数字信封，以数字信封方法发送命令或请求
25. 终端解密出PC软件发来的数字信封S1后，根据命令或请求的要求准备回复数据R1，终端对发送给PC软件的数据R1通过数字信封方式发送
26. PC同样使用数字信封给终端发送命令或请求
终端和PC软件间可以通过定时器来维护链路的连续性（Heartbeat Timer），如定时器超时仍未收到对方数据，则本次加密通信过程结束。下次通信需重新启动以上所述的双向认证和加密传输过程

图 2

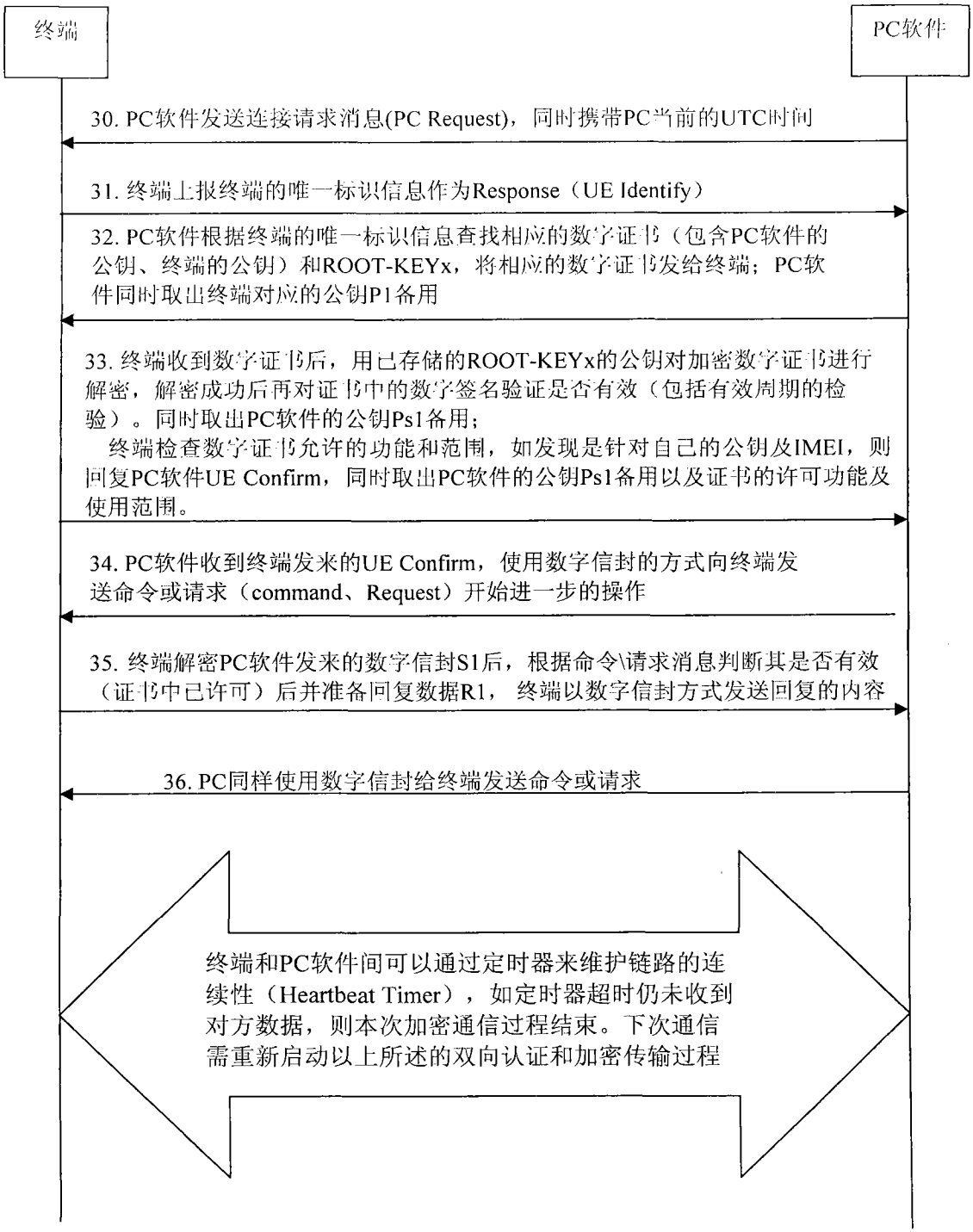

终端
PC软件
30. PC软件发送连接请求消息(PC Request)，同时携带PC当前的UTC时间
31. 终端上报终端的唯一标识信息作为Response（UE Identify）
32. PC软件根据终端的唯一标识信息查找相应的数字证书（包含PC软件的公钥、终端的公钥）和ROOT-KEYx，将相应的数字证书发给终端；PC软件同时取出终端对应的公钥P1备用
33. 终端收到数字证书后，用已存储的ROOT-KEYx的公钥对加密数字证书进行解密，解密成功后再对证书中的数字签名验证是否有效（包括有效周期的检验）。同时取出PC软件的公钥Ps1备用；
终端检查数字证书允许的功能和范围，如发现是针对自己的公钥及IMEI，则回复PC软件UE Confirm，同时取出PC软件的公钥Ps1备用以及证书的许可功能及使用范围。
34. PC软件收到终端发来的UE Confirm，使用数字信封的方式向终端发送命令或请求（command、Request）开始进一步的操作
35. 终端解密PC软件发来的数字信封S1后，根据命令\请求消息判断其是否有效（证书中已许可）后并准备回复数据R1，终端以数字信封方式发送回复的内容
36. PC同样使用数字信封给终端发送命令或请求
终端和PC软件间可以通过定时器来维护链路的连续性（Heartbeat Timer），如定时器超时仍未收到对方数据，则本次加密通信过程结束。下次通信需重新启动以上所述的双向认证和加密传输过程

图 3

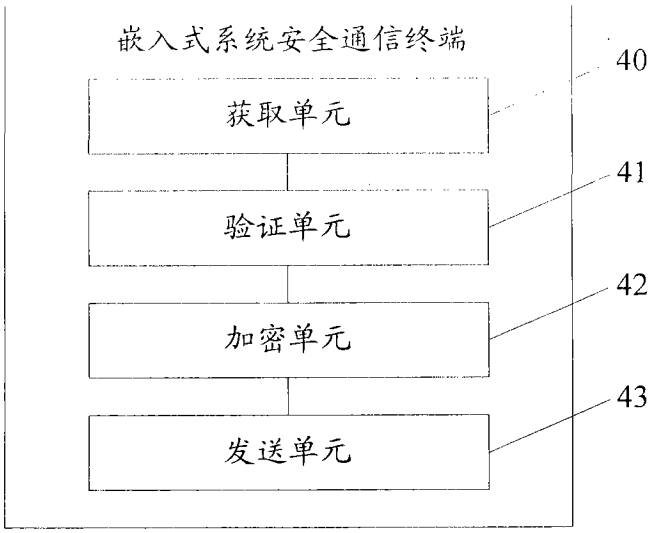

嵌入式系统安全通信终端
40
获取单元
41
验证单元
42
加密单元
43
发送单元

图 4

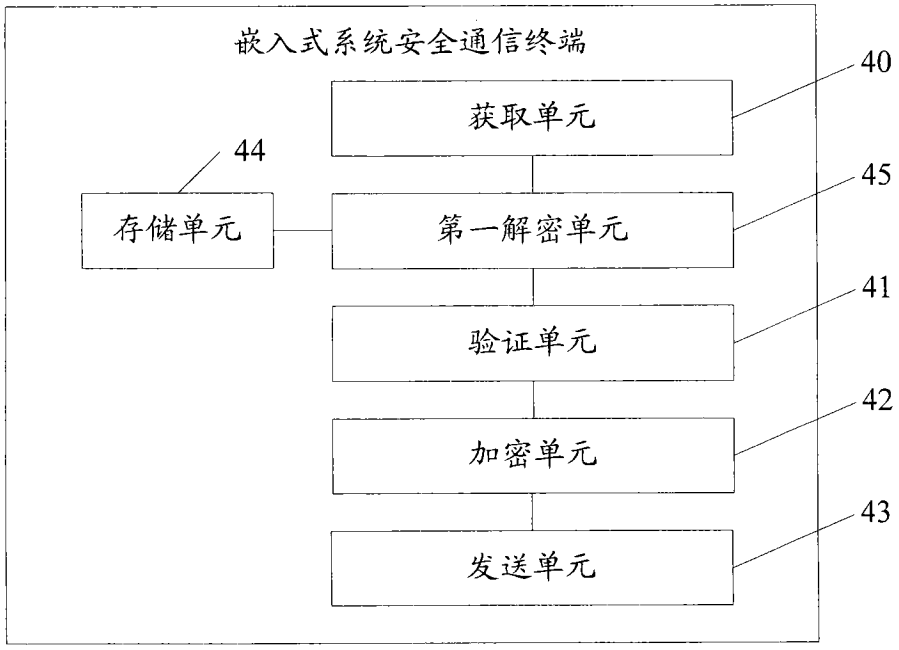

嵌入式系统安全通信终端
40
获取单元
44
存储单元
45
第一解密单元
41
验证单元
42
加密单元
43
发送单元

图 5

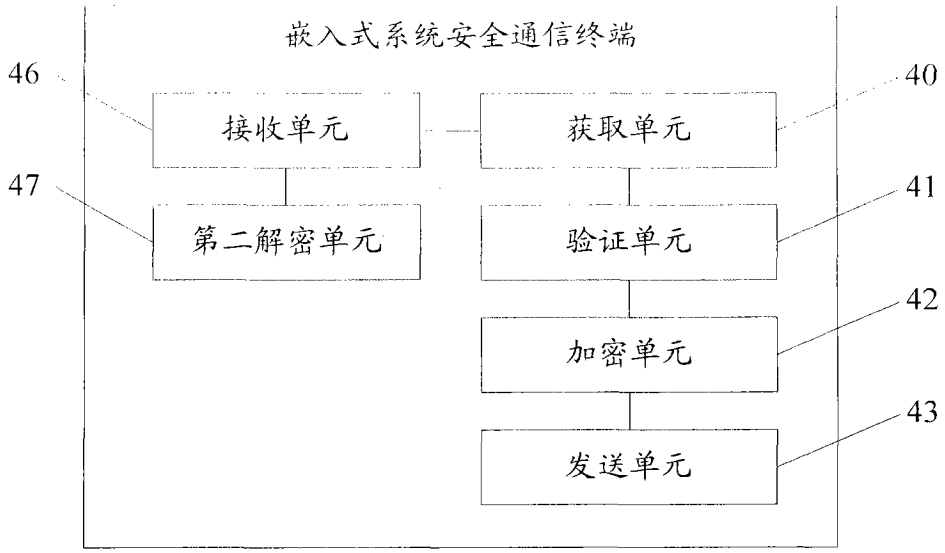

嵌入式系统安全通信终端
46
40
接收单元
获取单元
47
41
第二解密单元
验证单元
42
加密单元
43
发送单元

图 6

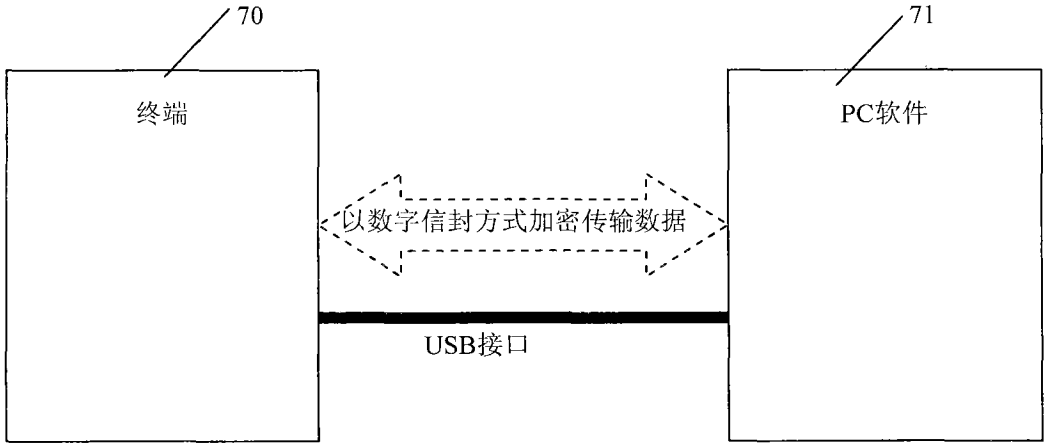

70
71
终端
PC软件
以数字信封方式加密传输数据
USB接口

图 7