(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112257119 B
(45)授权公告日 2022.10.28

(21)申请号 202011125907.2
(22)申请日 2020.10.20
(65)同一申请的已公布的文献号
申请公布号 CN 112257119 A
(43)申请公布日 2021.01.22
(73)专利权人 河北素数信息安全有限公司
地址 071052 河北省保定市惠阳街369号保定·中关村创新基地雨林空间1层
(72)发明人 李耀龙 朱剑 王建承 刘琦
(74)专利代理机构 石家庄中和昇知识产权代理事务所(特殊普通合伙) 13145
专利代理师 付会平
(51)Int.Cl.
G06F 21/72(2013.01)
G06F 21/34(2013.01)
审查员 李常亮

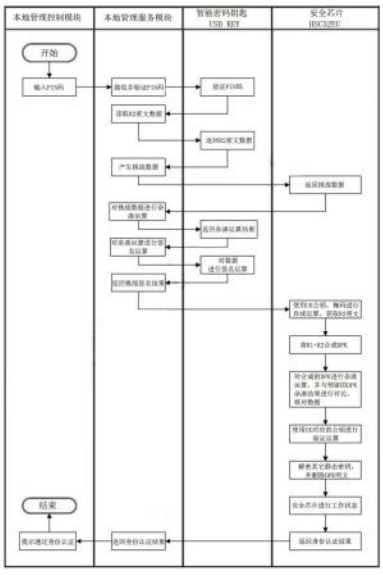
权利要求书2页 说明书11页 附图6页

(54)发明名称

一种身份认证方法及用于保证加密装置安全的保护方法

(57)摘要

本发明公开了一种身份认证方法及用于保证加密装置安全的保护方法,所述用于保证加密装置安全的保护方法包括以下步骤:S10、构建3层密钥体系,设定各层密钥体系之间的保护关系;S20、设定加密装置的安全状态转换方法;安全状态包括出厂态、就绪态、管理态、工作态;S30、依据步骤S1构建的密钥体系,对加密装置进行初装;S40、对智能密码钥匙进行身份认证。本发明有效提高了加密卫士的安全系数,设备故障率低,通过将密钥体系设置为3层,有效地提高了加密卫士的安全性,并采用对智能密码钥匙进行身份认证的方法,有效地提高本发明的抗冲击能力。



CN 112257119 B

1.一种身份认证方法,其特征在于,包括以下步骤:

S1、本地管理控制模块输入PIN码;本地管理服务模块接收并验证PIN码;再由智能密码钥匙验证PIN码;

S2、本地管理服务模块读取R2密文数据并传输至智能密码钥匙,智能密码钥匙返回R2密文数据至本地管理服务模块,本地管理服务模块产生挑战数据并传输至安全芯片;

S3、安全芯片返回挑战数据至本地管理服务模块,本地管理服务模块对挑战数据进行杂凑运算;

S4、智能密码钥匙返回杂凑运算结果至本地管理服务模块,本地管理服务模块对杂凑运算进行签名运算;

S5、智能密码钥匙对数据进行签名运算,返回挑战签名结果至本地管理服务模块;

S6、本地管理服务模块将挑战签名结果传输至安全芯片,安全芯片使用UK公钥、掩码进行异或运算,获取R2明文;将R1+R2合成DPK;

S7、安全芯片对合成的DPK进行杂凑运算,并与预留的DPK杂凑结果进行对比,核对数据;

S8、安全芯片使用UK对应的公钥进行验证运算;解密静态密钥,并删除DPK明文;

S9、安全芯片进行工作状态,返回身份认证结果至本地管理服务模块,本地管理服务模块返回身份认证结果至本地管理控制模块,由本地管理控制模块提示通过身份认证。

2.一种用于保证加密装置安全的保护方法,其特征在于,包括以下步骤:

S10、构建3层密钥体系,设定各层密钥体系之间的保护关系;所述密钥体系包括:设备保护密钥,用于加密加密装置内部的其它静态密钥;DPK产生后,将明文DPK进行杂凑运算,将杂凑运算结果存储于安全芯片内部的Flash;由设备保护密钥进行保护的设备管理密钥和设备应用密钥;以及由设备管理密钥及设备应用密钥的公钥加密导出的数据加密密钥和数据完整性密钥;

各密钥之间的保护关系如下所示:

1)$DPK_P=R1_P \oplus R2_P$,$R1_P$和$R2_P$为16字节随机数;

2)$H_{DPK}=H(DPK_P)$,H_{DPK}是对DPK_P进行摘要运算的结果,在安全芯片Flash中明文存储,H为摘要运算;

3)$DMK_C=E(DPK_P,DMK_P)$,其中E代表对称加密算法;DMK_P为明文设备管理密钥对,DMK_C为密文设备管理密钥对;

4)$DAK_C=E(DPK_P,DAK_P)$,其中E代表对称加密算法,DAK_P为设备应用密钥对明文,DAK_C为设备应用密钥对密文;

5)$R2_C= Rx \oplus R2_P \oplus UAK_{pub}$,$\oplus$为二进制数据异或运算,$UAK_{pub}$为智能密码钥匙对应鉴别密钥的公钥数据,Rx为安全芯片随机产生的掩码,Rx在安全芯片内部Flash中明文存储,$R2_C$存储于不同智能密码钥匙的安全存储区中,智能密码钥匙由PIN码进行访问控制;

S20、设定加密装置的安全状态转换方法;安全状态包括出厂态、就绪态、管理态、工作态;

S30、依据步骤S10构建的密钥体系,对加密装置进行初装;

S40、对智能密码钥匙进行如权利要求1所述的身份认证。

3.根据权利要求2所述的一种用于保证加密装置安全的保护方法,其特征在于,所述设

备保护密钥由R1和R2分量异或得到，其中R1在安全芯片内部Flash明文存储，R2分量在用户所属的UK中加密存储，每个UK中存储的R2密文数值不同，UK使用PIN码进行访问控制。

4.根据权利要求3所述的一种用于保证加密装置安全的保护方法，其特征在于，所述步骤S30中，对加密装置进行初装是对处于出厂态的设备进行初始化部署的过程，初始化完成后，设备进入就绪态；所述步骤S30包括以下步骤：

S301、设备上电后，按照可信链正常启动；

S302、安全控制芯片处于出厂态；

S303、生成设备保护密钥；

S304、生成设备管理密钥；

S305、生成设备应用密钥；

S306、创建1个或多个管理用户；

S307、创建1个或多个普通用户；

S308、安全芯片进入就绪态。

5.根据权利要求4所述的一种用于保证加密装置安全的保护方法，其特征在于，所述步骤S303，是通过本地管理控制软件发起生成设备保护密钥的流程，由安全控制芯片执行权利要求2中1)、2)步运算过程；

所述步骤S304，是通过本地管理控制软件发起生成设备管理密钥的流程，由安全控制芯片执行权利要求2中3)步运算过程；

所述步骤S305，是通过本地管理控制软件发起生成设备应用密钥的流程，由安全控制芯片执行权利要求2中4)步运算过程；

所述步骤S306和步骤S307，是通过本地管理控制软件发起创建管理用户和普通用户的流程，由安全控制芯片执行权利要求2中5)步运算过程。

6.根据权利要求5所述的一种用于保证加密装置安全的保护方法，其特征在于，在执行步骤S306和步骤S307过程中，需要将未使用的智能密码钥匙插入加密装置的USB接口。

7.根据权利要求2所述的一种用于保证加密装置安全的保护方法，其特征在于，所述步骤S20包括以下方法：

出厂态初始化完成后进入就绪态，就绪态销毁后进入出厂态；

就绪态登录1个普通用户后进入工作态，工作态注销用户后进入就绪态；

就绪态登录1个管理用户后进入管理态，管理态注销管理用户后进入就绪态；

管理态注销管理用户并登录普通用户后进入工作态，工作态登录1个管理用户后进入管理态；

工作态销毁后进入出厂态。

一种身份认证方法及用于保证加密装置安全的保护方法

技术领域

[0001] 本发明涉及数据传输加密技术领域，更具体涉及一种身份认证方法及用于保证加密装置安全的保护方法。

背景技术

[0002] 在数据通讯飞速发展的时代，越来越多的消息、信息和其它数字数据以位和字节通过电缆和空气传输，同时数字数据的拥有者要求保护数字数据的要求也在增多。网络传输加密系统的建设要严格遵循《中华人民共和国密码法》的相关规章制度，在加强技术建设的同时，也要制定相应的管理规章制度，通过制度规范系统运维和使用，通过技术约束运维和使用的操作。

[0003] 为确保加密装置满足GM/T0028-2014《密码模块安全技术要求》以及GM/T0039-2015《密码模块安全检测要求》中安全等级二级的相关要求，能够通过国家密码管理局商用密码检测中心的安全检测，并取得检测认证报告，需要进行加密装置的安全体系设计。并且现有的加密装置故障率高、安全系数较低。为此，需要提供一种身份认证方法及用于保证加密装置安全的保护方法。

发明内容

[0004] 本发明需要解决的技术问题是提供一种身份认证方法及用于保证加密装置安全的保护方法，以解决现有的加密装置故障率高、安全系数较低的问题，以提高加密装置的安全性，降低加密装置的故障率。

[0005] 为解决上述技术问题，本发明所采取的技术方案如下。

[0006] 一种身份认证方法，包括以下步骤：

[0007] S1、输入PIN码；接收并验证PIN码；

[0008] S2、读取R2密文数据，返回R2密文数据，产生挑战数据；

[0009] S3、返回挑战数据，对挑战数据进行杂凑运算；

[0010] S4、返回杂凑运算结果，对杂凑运算进行签名运算；

[0011] S5、对数据进行签名运算，返回挑战签名结果；

[0012] S6、使用UK公钥、掩码进行异或运算，获取R2明文；将R1+R2合成DPK；

[0013] S7、对合成的DPK进行杂凑运算，并与预留的DPK杂凑结果进行对比，核对数据；

[0014] S8、使用UK对应的公钥进行验证运算；解密静态密钥，并删除DPK明文；

[0015] S9、安全芯片进行工作状态，返回身份认证结果。

[0016] 一种用于保证加密装置安全的保护方法，包括以下步骤：

[0017] S10、构建3层密钥体系，设定各层密钥体系之间的保护关系；

[0018] S20、设定加密装置的安全状态转换方法；安全状态包括出厂态、就绪态、管理态、工作态；

[0019] S30、依据步骤S1构建的密钥体系，对加密装置进行初装；

[0020] S40、对智能密码钥匙进行身份认证。

[0021] 进一步优化技术方案，所述密钥体系包括：

[0022] 设备保护密钥，用于加密加密装置内部的其它静态密钥；DPK产生后，将明文DPK进行杂凑运算，将杂凑运算结果存储于安全芯片内部的Flash；

[0023] 由设备保护密钥进行保护的设备管理密钥和设备应用密钥；以及

[0024] 由设备管理密钥及设备应用密钥的公钥加密导出的数据加密密钥和数据完整性密钥。

[0025] 进一步优化技术方案，所述设备保护密钥由R1和R2分量异或得到，其中R1在安全芯片内部Flash明文存储，R2分量在用户所属的UK中加密存储，每个UK中存储的R2密文数值不同，UK使用PIN码进行访问控制。

[0026] 进一步优化技术方案，各密钥之间的保护关系如下所示：

[0027] 1) $DPK_P = R1_P \oplus R2_P$，$R1_P$和$R2_P$为16字节随机数；

[0028] 2) $H_{DPK} = H(DPK_P)$，H_{DPK}是对DPK_P进行摘要运算的结果，在安全芯片Flash中明文存储，H为摘要运算；

[0029] 3) $DMK_C = E(DPK_P, DMK_P)$，其中E代表对称加密算法；DMK_P为明文设备管理密钥对，DMK_C为密文设备管理密钥对；

[0030] 4) $DAK_C = E(DPK_P, DAK_P)$，其中E代表对称加密算法，DAK_P为设备应用密钥对明文，DAK_C为设备应用密钥对密文；

[0031] 5) $R2_C = Rx \oplus R2_P \oplus UAK_{pub}$，$\oplus$为二进制数据异或运算，$UAK_{pub}$为智能密码钥匙对应鉴别密钥的公钥数据，Rx为安全芯片随机产生的掩码，Rx在安全芯片内部Flash中明文存储，$R2_C$存储于不同智能密码钥匙的安全存储区中，智能密码钥匙由PIN码进行访问控制。

[0032] 进一步优化技术方案，所述步骤S30中，对加密装置进行初装是对处于出厂态的设备进行初始化部署的过程，初始化完成后，设备进入就绪态；所述步骤S30包括以下步骤：

[0033] S301、设备上电后，按照可信链正常启动；

[0034] S302、安全控制芯片处于出厂态；

[0035] S303、生成设备保护密钥；

[0036] S304、生成设备管理密钥；

[0037] S305、生成设备应用密钥；

[0038] S306、创建1个或多个管理用户；

[0039] S307、创建1个或多个普通用户；

[0040] S308、安全芯片进入就绪态。

[0041] 进一步优化技术方案，所述步骤S303，是通过本地管理控制软件发起生成设备保护密钥的流程，由安全控制芯片执行1)、2)步运算过程；

[0042] 所述步骤S304，是通过本地管理控制软件发起生成设备管理密钥的流程，由安全控制芯片执行3)步运算过程；

[0043] 所述步骤S305，是通过本地管理控制软件发起生成设备应用密钥的流程，由安全控制芯片执行4)步运算过程；

[0044] 所述步骤S306和步骤S307，是通过本地管理控制软件发起创建管理用户和普通用户的流程，由安全控制芯片执行5)步运算过程。

[0045] 进一步优化技术方案，在执行步骤S306和步骤S307过程中，需要将未使用的智能密码钥匙插入加密装置的USB接口。

[0046] 进一步优化技术方案，所述步骤S20包括以下方法：

[0047] 出厂态初始化完成后进入就绪态，就绪态销毁后进入出厂态；

[0048] 就绪态登录1个普通用户后进入工作态，工作态注销用户后进入就绪态；

[0049] 就绪态登录1个管理用户后进入管理态，管理态注销管理用户后进入就绪态；

[0050] 管理态注销管理用户并登录普通用户后进入工作态，工作态登录1个管理用户后进入管理态；

[0051] 工作态销毁后进入出厂态。

[0052] 由于采用了以上技术方案，本发明所取得技术进步如下。

[0053] 本发明加密卫士的安全性按照GM/T 0028《密码模块安全技术要求》二级进行设计，有效提高了加密卫士的安全系数，设备故障率低，通过将密钥体系设置为3层，有效地提高了加密卫士的安全性，并采用对智能密码钥匙进行身份认证的方法，有效地提高本发明的抗冲击能力。

[0054] 本发明应用于无人值守领域，能够应用于环境恶劣的情况下，设备现场运维次数少，能够在网络做最小调整的情况下无缝接入现有网络，部署方便，简单易用。

[0055] 本发明加密卫士采用低功耗的ARM平台开发，内部采用硬件安全芯片作为密钥管理及密码运算的模块，支持双千兆网络接口，具有温湿度传感器、本地管理、远程管理等功能。

[0056] 本发明能够满足工业化、低功耗、易安装、免维护、高安全等各类要求，通过国家相关的安全检测认证，获取电力、能源、交通等各行业的机电或信息化相关认证。

附图说明

[0057] 图1为本发明一种身份认证方法的流程图；

[0058] 图2为本发明一种用于保证加密装置安全的保护方法的设备密钥保护关系图；

[0059] 图3为本发明一种用于保证加密装置安全的保护方法对加密装置进行初装的流程图；

[0060] 图4为本发明一种用于保证加密装置安全的保护方法中加密装置安全状态转换图；

[0061] 图5为本发明一种用于保证加密装置安全的保护方法的加密卫士硬件部分的原理框图；

[0062] 图6为本发明一种基于嵌入式技术的微型传输加密装置的对外接口图；

[0063] 图7为本发明一种基于嵌入式技术的微型传输加密装置的加密卫士软件部分的原理框图；

[0064] 图8为本发明一种基于嵌入式技术的微型传输加密装置中管理控制软件与加密卫士软件部分交互关系图；

[0065] 图9为本发明一种基于嵌入式技术的微型传输加密装置的启动流程图。

具体实施方式

[0066] 下面将结合附图和具体实施例对本发明进行进一步详细说明。

[0067] 一种基于嵌入式技术的微型传输加密装置，结合图5至图8所示，包括加密卫士硬件部分和加密卫士软件部分。

[0068] 加密卫士采用低功耗的ARM平台开发，内部采用硬件安全芯片作为密钥管理及密码运算的模块，支持双千兆网络接口，具有温湿度传感器、本地管理、远程管理等功能。

[0069] 加密卫士硬件部分包括：业务控制芯片、安全控制芯片、噪声源、算法协调处理器、多模定位模块、温湿度传感器、智能密码钥匙、DDR3存储器、eMMC Flash、复位按钮、指示灯和SPI Flash。

[0070] 业务控制芯片，业务控制芯片采用MARVELLARMADA 3720 SoC芯片，该款芯片内部集成Cortex®-A53处理器，具有丰富的外设接口。ARMADA 3720基于Marvell开创性的模块化芯片架构，即MoChi™架构，可通过增加MoChi模块扩展为虚拟SoC(Marvell VSoC™)，以支持定制互联方式以及各种I/O技术和接口；其紧凑的尺寸(11.5mm x 10.5mm)可实现尺寸更小、外形更简洁产品设计；Marvell VSoC集成了强大的双64位ARM® v8Cortex®-A53处理器，允许ARMADA 3720同时运行多种应用；ARMADA 3720为低功耗、小尺寸应用而优化，例如移动连接网络存储等电池供电设备，有助于将高性能、分布式云存储及网络管理平台快速、简便地推向市场；ARMADA 3720 SoC系列提供丰富的高速I/O，包括USB 3.0、SATA 3.0、千兆以太网(1GbE)和2.5GbE(NBASE-T)。此外，该系列器件采用了多种安全和数据加速引擎，适合创新性网络、存储和计算应用；ARMADA 3720支持先进的电源管理技术，可以单独接通每一个CPU内核以及针对每个内核动态调整电压和频率，这可以在不同工作负载时显著降低功耗。

[0071] 安全控制芯片，与业务控制芯片交互连接。安全控制芯片采用HSC32EU芯片，通过USB 2.0协议与业务控制芯片进行连接。该芯片是整机的安全控制中心，负责设备随机数生成、密钥安全存储、用户身份认证、安全状态转移等功能。该芯片支持SM2、SM3和SM4算法，支持多种外设接口。

[0072] 安全控制芯片数据加密密钥设置到算法协调处理器中，多个数据加密密钥通过KEY-ID进行区分，KEY-ID由密钥协商程序生成和维护，并通过KEY-ID调度算法协调处理器(T620)中的密钥进行加密、解密和完整性运算。

[0073] HSC32EU芯片是由北京宏思电子技术有限责任公司研制的一款具有多功能、高性能、高安全性、低功耗、低成本等特点的系统级密码安全芯片。

[0074] 芯片实现的主要功能包括：

[0075] 片上密钥管理(包括密钥生成、密钥存储、密钥更新等)；

[0076] 支持国密SM2/SM3/SM4/SSF33算法；

[0077] 支持国际AES/TDES/RSA/SHA算法；

[0078] 支持USB 2.0高速全速通信；

[0079] 支持SPI、UART、7816主接口、IIC等多种通信接口；

[0080] 支持U盘功能，支持外挂大容量NandFlash和eMMC存储芯片；

[0081] 支持IC卡读卡器和SD卡读卡器功能；

[0082] 支持高速数据流加密功能；

[0083] 支持多种安全管理控制。

[0084] 噪声源，与安全控制芯片通过接口交互连接，用于产生不可预测且密码学统计特性良好的真随机数，是信息安全级密码产品中不可缺少的基础部件。本发明中噪声源采用的是宏思电子设计生产的WNG-8物理噪声源芯片，主要应用于商用密码产品的密钥生成、初始向量设置，能够满足安全通信协议中真随机序列的广泛需求。

[0085] WNG-8与WNG-4、WNG-9产品管脚信息一致，保持产品向前兼容，支持DIP8和SOP8两种封装形式；为更好的适应不同的电源芯片，WNG-8提供3.3V和5.0V两类品种；WNG-8使用简单，采用单路穿行输出，输出速率为20Mbps。

[0086] 算法协调处理器，与业务控制芯片交互连接，并通过通讯接口连接于安全控制芯片的输出端，算法协调处理器用于SM4和SM3算法的加速处理。算法协调处理器采用方寸电子T620，业务控制芯片采用USB 3.0协议与算法协调处理器连接。

[0087] 该芯片内部硬件实现SM2、SM3、SM4等国密算法，支持USB 3.0全速、SPI、UART等多种通讯接口，具有抗DPA/SPA攻击、存储保护、主动屏蔽、电压频率温度检测等安全防护机制。

[0088] 该芯片主要用于SM4和SM3算法的加速处理，由HSC32EU通过UART接口将数据加密密钥设置到T620中，多个数据加密密钥通过KEY-ID进行区分，KEY-ID由密钥协商程序生成和维护，并通过KEY-ID调度算法协调处理器(T620)中的密钥进行加密、解密和完整性运算。

[0089] 算法协调处理器选择青岛方寸微电子科技有限公司的T620安全芯片(密码产品证书型号是SSX1929)，该芯片为商用密码产品1级，是由方寸微电子自主开发的新一代SoC网络终端安全芯片，具有安全性高、功能丰富、性能强、功耗低的特点。

[0090] 该芯片集成高性能32位国产RISC CPU，支持USB 3.0、SATA3.0、eMMC5.1等多种超高速接口，并集成多种商用密码算法(SM2、SM3、SM4)，可满足信息安全领域末端密码产品的安全需求。

[0091] 该芯片的SM4算法引擎性能约800Mbps，支持ECB、CBC、OFB、CFB、CTR、XTS等5类运算模式；SM2算法的密钥对生成速度月500对/秒。

[0092] 该芯片有512KB片内FLASH存储空间、32KB ROM空间、256KB SRAM空间，支持1路QSPI主接口、1路SPI主接口、2路UART接口、12位GPIO接口。

[0093] 在安全性上，支持抗电压检测、抗温度检测、支持物理探测防护等物理特性。

[0094] 多模定位模块，通过UART接口接入到业务控制芯片中，用于提供定位功能。为增强多模定位模块的定位能力，外壳需预留外置天线接口。

[0095] 温湿度传感器，与业务控制芯片交互连接，用于检测加密卫士硬件所处环境中的温度和湿度。本发明中的温湿度传感器选用SENSIRION公司的SHT30-DIS-B，该温湿度传感器具有体积小，精度高的特点，体积为3×3mm，湿度检测范围为0～100％RH，精度小于5％(0-90％RH时)，温度检测范围为-40℃～+125℃，精度小于1℃(-10℃～85℃)。

[0096] 智能密码钥匙，用于加密卫士启动时对管理用户或普通用户的身份认证。本发明中的智能密码钥匙采用天津赢达信科技有限公司研制生产的智能密码钥匙(USB KEY，简称“UK”)，采用全速/高速核心的高性能、高容量安全芯片，提供高速硬件运算能力，支持硬件的国际和国密算法。

[0097] 该UK采用USB接口设计，采用USB 2.0高速设计方案，其内部采用高安全性的安全

芯片，能有效防止物理攻击，采用免驱设计，在Windows操作系统自动识别。

[0098] 业务控制芯片交互连接有DDR3存储器、eMMC Flash、复位按钮和指示灯，DDR3存储器为1G容量，eMMC Flash为4G容量。业务控制芯片和安全控制芯片的输出端分别通过选择开关连接有SPI Flash，SPI Flash用于存储BootLoader程序，16M存储容量。

[0099] 加密卫士对外提供的物理接口如图6所示，该图中的Console口为单个物理接口，但是支持两路UART串口。指示灯采用1排4列方式布置，指示灯的含义另行设计，USB母口与PCB板平行连接，复位按钮为电源重启按钮功能。

[0100] 加密卫士软件部分包括：应用层、内核层、驱动层和系统层。

[0101] 应用层包括密钥协商模块、本地管理服务模块、远程管理代理模块、IP摄像机认证代理模块以及情报板安全代理模块。

[0102] 密钥协商模块主要负责实现满足GM/T0022-2014《IPSec VPN技术规范》的IKE协议以及自定义的密钥分发协议，协议中需要进行的密码运算由HSC32EU芯片实现，密钥协商模块的工作模式由本地管理控制软件设置。

[0103] 密钥协商支持的算法套件为：

[0104] 1)SM2-SM3-SM4

[0105] 2)RSA-SM3-SM4。

[0106] 远程管理代理模块用于实现与远程管理平台的通信交互。远程管理代理模块包括执行指令以及上报状态功能，远程管理指令包括：设备复位重启、设备软件升级、远程销毁密钥、获取安全状态、获取网络参数、设置网络参数；上报状态功能包括：上报温度数值、上报湿度数值、上报定位数值、上报流量信息、上报网络参数。

[0107] IP摄像机认证代理模块用于对摄像机的管理协议进行代理认证，实现GB 35114-2018的A级接入身份认证，由HSC32EU提供相关的密码运算以及证书管理功能。

[0108] 情报板安全代理模块用于对加密卫士被保护设备的在线探测工作，确保及时发现被保护设备的离线告警功能。

[0109] 内核层，包括数据加密封装模块以及防病毒模块。

[0110] 数据加密封装模块用于实现数据封包、数据拆包、ESP协议以及IP载荷加密。其中密码运算的功能由T620芯片实现。数据加密封装的策略由本地管理控制软件设置。

[0111] 驱动层，包括安全芯片驱动、网络接口驱动、USB驱动、UART驱动。

[0112] 系统层，包括操作系统。

[0113] 本地管理服务模块通过串口与本地管理控制软件连接，本地管理服务模块配合本地管理控制软件执行相关的指令，并将执行结果返回给本地管理控制软件。

[0114] 一种基于嵌入式技术的微型传输加密装置的启动方法，启动方法基于一种用于保证加密装置安全的保护方法进行，包括以下步骤：

[0115] S1、设备上电；安全控制芯片上电启动后，执行可信启动程序，设置业务控制芯片处于复位状态，通过复位信号延迟业务控制芯片启动。

[0116] S2、安全控制芯片对存放于SPI Flash芯片内部的启动引导程序进行数字签名校验。启动引导程序即为SPI Flash内部的Boot loader程序。

[0117] 若校验不通过执行步骤S3，若校验通过执行步骤S4。

[0118] S3、通过指示灯进行告警，红灯闪烁。

[0119] S4、校验通过后，再通过改变复位信号启动业务控制芯片，业务控制芯片加载启动引导程序并初始化各类外设。

[0120] S5、启动引导程序对eMMC Flash的操作系统内核镜像(Linux Kernel Image)软件进行数字签名校验；

[0121] 若校验不通过执行步骤S3，若校验通过执行步骤S6。

[0122] S6、校验通过后，业务控制芯片加载eMMC Flash中的操作系统内核程序，将Linux内核加载至CPU中运行。

[0123] 步骤S6中，在程序开发完成后，将应用程序(Linux Kernel)的所有文件打包为镜像文件(如Image、zImag等诸多格式文件)，使用厂商签名密钥对的私钥数据对镜像文件签名得到签名结果，将签名结果放入签名文件(后缀名为sig)中，签名文件名称与镜像文件名称相同，将镜像文件以及签名文件放入eMMC Flash的应用分区中。

[0124] S7、操作系统内核对应用程序镜像进行数字签名校验。

[0125] 若校验不通过执行步骤S3，若校验通过执行步骤S8。

[0126] S8、校验通过后，操作系统内核解压并启动应用程序，再将应用程序加载至CPU中运行。

[0127] SPI Flash的容量较小，内部用于存储业务控制芯片系统的启动引导(Boot Loader)程序，启动引导程序(Boot Loader)程序主要用于初始化硬件设备、建立内存空间映射图等工作，为嵌入式操作系统(通常为Linux系列)内核准备好启动环境；系统约定位于启动引导程序结束后绝对地址增加256字节为签名数据的存放起始位置。

[0128] 数字签名算法为:SM2，摘要算法为SM3。

[0129] 在启动过程中，安全控制芯片首先对SPI Flash的启动引导程序进行摘要运算，再从SPI Flash的签名位置区域读取签名数值，再读取内部存储的厂商签名公钥进行签名验证；若验证通过，则证明启动引导区的程序为厂商发布程序。

[0130] 当启动引导程序被正常加载后，启动引导程序读取eMMC Flash系统启动分区中的系统内核镜像文件，使用算法协调处理器进行摘要运算，摘要运算结束后再读取签名文件中的签名数据以及内部存储的厂商签名公钥，最后使用算法协调处理器对签名数据、摘要数据以及签名公钥进行验证；若验证通过，则证明操作系统内核为厂商发布程序。

[0131] 当操作系统内核被正常加载后，内核程序读取eMMC Flash应用分区中的应用程序镜像文件，使用算法协调处理器进行摘要运算，摘要运算结束后再读取签名文件中的签名数据以及内部存储的厂商签名公钥，最后使用算法协调处理器对签名数据、摘要数据以及签名公钥进行验证；若验证通过，则证明应用程序为厂商发布程序。

[0132] 上述流程中的签名及验签算法为:SM2，摘要算法为:SM3。

[0133] 一种用于保证加密装置安全的保护方法，包括以下步骤：

[0134] S10、构建3层密钥体系，设定各层密钥体系之间的保护关系。

[0135] S20、设定加密装置的安全状态转换方法；安全状态包括出厂态、就绪态、管理态、工作态。

[0136] S30、依据步骤S1构建的密钥体系，对加密装置进行初装。

[0137] S40、对智能密码钥匙进行身份认证。

[0138] 密钥体系包括：设备保护密钥、由设备保护密钥进行保护的设备管理密钥和设备

应用密钥、由设备管理密钥及设备应用密钥的公钥加密导出的数据加密密钥和数据完整性密钥。

[0139] 设备保护密钥,Device Protect Key,简称:DPK。在芯片初始化时随机产生密钥分量R1和R2,长度为128比特,DPK由R1和R2异或运算产生;DPK为对称密钥,长度128比特;该密钥为密钥加密密钥,用于加密设备内部的其它静态密钥。DPK产生后,将明文DPK进行杂凑运算,将杂凑运算结果(32字节/256比特)存储于安全芯片内部的Flash;其次,产生16字节随机数作为掩码,对R2与对UK对应的公钥数据进行异或运算,将运算结果存放于不同的USB KEY中,USB KEY由口令进行保护;R1明文存储于安全芯片内部的Flash中。

[0140] 设备保护密钥由R1和R2分量异或得到,其中R1在安全芯片内部Flash明文存储,R2分量在用户所属的UK中加密存储,每个UK中存储的R2密文数值不同,UK使用PIN码进行访问控制。

[0141] 设备管理密钥,Device Management Key,简称DMK,在HSC32EU安全芯片初始化时随机生成,为SM2非对称密钥,包含两组:加密密钥对和签名密钥对;DMK由DPK加密后在安全芯片内部Flash存储;两组密钥对主要用于与管理系统的身份验证和数据加密,其中加密密钥对支持外部加密导入;所有密钥对使用索引号码区分,DMK存储索引号为0。

[0142] 设备应用密钥,Device Application Key,简称DAK,由管理用户创建和销毁,为SM2非对称密钥,包含两组:加密密钥对和签名密钥对,其中加密密钥对支持外部加密导入;DAK由DMK加密后在安全芯片内部Flash存储,应用密钥对由加密卫士的软件调用,最大支持8组密钥,索引号为1～8。

[0143] 数据加密密钥,Data Encrypt Key,简称DEK,由安全芯片通过物理噪声源临时产生,或通过密钥协商方式派生产生,不支持明文导出,支持外部公钥加密后导出,仅在上电期间在安全芯片和协处理器的RAM中临时存储,掉电后销毁。

[0144] 数据完整性密钥,Data HMAC Key,简称DHK,由安全芯片通过物理噪声源临时产生,或通过密钥协商方式派生产生,不支持明文导出,支持外部公钥加密后导出,仅在上电期间在安全芯片和协处理器的RAM中临时存储,掉电后销毁。

[0145] 加密卫士中密钥的保护关系如图2所示,设备保护密钥作为最原始的保护密钥,设备保护密钥保护设备管理密钥和设备应用密钥,数据加密密钥和数据完整性密钥由设备管理密钥及设备应用密钥的公钥加密导出,数据加密密钥和数据完整性密钥为临时密钥,掉电后消失。

[0146] 各密钥之间的保护关系如下所示:

[0147] 1)$DPK_P = R1_P \oplus R2_P$,$R1_P$和$R2_P$为16字节随机数,本例由物理噪声源产生。

[0148] 2)$H_{DPK} = H(DPK_P)$,H_{DPK}是对DPK_P进行摘要运算的结果,在安全芯片Flash中明文存储,H为摘要运算(本例为SM3算法)。

[0149] 3)$DMK_C = E(DPK_P, DMK_P)$,其中E代表对称加密算法,本例为SM4算法;DMK_P为明文设备管理密钥对,DMK_C为密文设备管理密钥对。

[0150] 4)$DAK_C = E(DPK_P, DAK_P)$,其中E代表对称加密算法,本例为SM4算法;DAK_P为设备应用密钥对明文,本例由HSC32EU随机产生;DAK_C为设备应用密钥对密文。

[0151] 5)$R2_C = Rx \oplus R2_P \oplus UAK_{pub}$,$\oplus$为二进制数据异或运算,$UAK_{pub}$为智能密码钥匙对应鉴别密钥的公钥数据,Rx为安全芯片随机产生的掩码,Rx在安全芯片内部Flash中明文存储,

$R2_C$存储于不同智能密码钥匙的安全存储区中，智能密码钥匙由PIN码进行访问控制。

[0152] 各密钥之间的生命周期如下表：

[0153]

密钥名称	密码算法	长度	产生	存储	分发	更新	销毁
DPK	SM4	128 比特 / 16 字节	由分量 R1 和 R2 采用异或方式合成，R1 和 R2 由物理噪声源产生，均为 128 比特	R1 在 HSC32EU 内部 Flash 明文存储；R2 加密后在智能密码钥匙内部安全 Flash 中存储；明文状态在 RAM 中存在；	不分发	不更新	通过软件指令按需销毁
DMK	SM2	公钥 512 比特 私钥 256 比特	由 HSC32EU 芯片随机生成	由 DPK 加密后在 HSC32EU 的内部 Flash 中存储，明文状态在 RAM 中存在；	不分发	不更新	通过软件指令按需销毁
DAK	SM2	公钥 512 比特 私钥 256 比特	由 HSC32EU 芯片随机生成	由 DPK 加密后在 HSC32EU 的内部 Flash 中存储，明文状态在 RAM 中存在；	不分发	不更新	通过软件指令按需销毁
DEK	SM4	128 比特 / 16 字节	通过 IKE 或其它密钥协商协议生成	明文数据在 HSC32EU 中生成，在 HSC32EU 的 RAM 中存在，在 T620 的 RAM 中存在；	不分发	不更新	掉电销毁以及根据软件指令按需销毁
DHK	SM3	128 比特 / 16 字节	通过 IKE 或其它密钥协商协议生成	明文数据在 HSC32EU 中生成，在 HSC32EU 的 RAM 中存在，在 T620 的 RAM 中存在；	不分发	不更新	掉电销毁以及根据软件指令按需销毁
UAK	SM2	公钥 512 比特 私钥 256 比特	在智能密码钥匙中采用随机方式产生	在智能密码钥匙内部 Flash 加密存储，通过 PIN 码进行访问控制。	不分发	不更新	根据软件指令按需销毁

[0154] 步骤S30中，对加密装置进行初装是对处于出厂态的设备进行初始化部署的过程，初始化完成后，设备进入就绪态；

[0155] 加密卫士的固件分为：业务控制芯片系统内核；安全控制芯片固件程序；T620安全芯片固件程序；业务应用程序。

[0156] 其中，操作系统内核刷入eMMC存储芯片，应用程序在eMMC中存储。其中，安全芯片的固件中包含操作系统内核文件的完整性数值(SM3算法运算结果)；加密卫士初装流程如图3所示。

[0157] 步骤S30包括以下步骤：

[0158] S301、设备上电后，按照可信链正常启动；

[0159] S302、安全控制芯片处于出厂态；

[0160] S303、生成设备保护密钥；

[0161] S304、生成设备管理密钥；

[0162] S305、生成设备应用密钥；

[0163] S306、创建1个或多个管理用户；

[0164] S307、创建1个或多个普通用户；

[0165] S308、安全芯片进入就绪态。

[0166] 步骤S303，是通过本地管理控制软件发起生成设备保护密钥的流程，由安全控制芯片执行各密钥之间的保护关系的1)、2)步运算过程；

[0167] 步骤S304，是通过本地管理控制软件发起生成设备管理密钥的流程，由安全控制芯片执行各密钥之间的保护关系的3)步运算过程；

[0168] 步骤S305，是通过本地管理控制软件发起生成设备应用密钥的流程，由安全控制芯片执行各密钥之间的保护关系的4)步运算过程；

[0169] 步骤S306和步骤S307，是通过本地管理控制软件发起创建管理用户和普通用户的流程，由安全控制芯片执行各密钥之间的保护关系的5)步运算过程。

[0170] 在执行步骤S306和步骤S307过程中，需要将未使用的智能密码钥匙(USB KEY)插入加密装置的USB接口。

[0171] 步骤S20中，出厂态：出厂态是指硬件设备(本例为加密卫士)经过贴片和焊接完成后，电路信号通信正常；安全控制芯片(本例为HSC32EU)、算法协调处理器(本例为T620)以及业务控制芯片(本例为88F3720)刷入对应的二进制固件程序，设备可正常加电启动；设备内部除每机MAC地址不同外，未产生或存储用户个性化的密钥数据以及策略配置数据，设备处于原始生产完毕待实施安装状态。

[0172] 就绪态：当处于出厂态的设备经过初装步骤从而产生每机不同的密钥数据后，所有密钥数据处于安全加密静态存储状态，未恢复到明文密钥状态，设备暂时不能正常提供密码运算能力，此时设备处于就绪状态，设备的初始化过程参见步骤S30。

[0173] 工作态：当处于就绪态的设备经过普通用户身份认证后，设备的存储密钥已恢复至明文状态，设备可正常提供密码运算能力，但是不能对应用密钥对进行增加、更新或者删除操作，此时设备处于工作态。

[0174] 管理态：管理态是工作态中的一种特殊状态，处于管理状态的设备，其静态存储密钥已恢复至明文状态，但是不能正常提供密码运算能力，处于管理态的密码设备允许对应用密钥对进行增加、更新或者删除操作。

[0175] 步骤S20包括以下方法：

[0176] 出厂态初始化完成后进入就绪态，就绪态销毁后进入出厂态；

[0177] 就绪态登录1个普通用户后进入工作态，工作态注销用户后进入就绪态；

[0178] 就绪态登录1个管理用户后进入管理态，管理态注销管理用户后进入就绪态；

[0179] 管理态注销管理用户并登录普通用户后进入工作态，工作态登录1个管理用户后进入管理态；

[0180] 工作态销毁后进入出厂态。

[0181] 一种身份认证方法，结合图1所示，包括以下步骤：

[0182] S1、本地管理控制模块输入PIN码；本地管理服务模块接收并验证PIN码；再由智能密码钥匙验证PIN码；

[0183] S2、本地管理服务模块读取R2密文数据并传输至智能密码钥匙，智能密码钥匙返

回R2密文数据至本地管理服务模块，本地管理服务模块产生挑战数据并传输至安全芯片；

[0184] S3、安全芯片返回挑战数据至本地管理服务模块，本地管理服务模块对挑战数据进行杂凑运算；

[0185] S4、智能密码钥匙返回杂凑运算结果至本地管理服务模块，本地管理服务模块对杂凑运算进行签名运算；

[0186] S5、智能密码钥匙对数据进行签名运算，返回挑战签名结果至本地管理服务模块；

[0187] S6、本地管理服务模块将挑战签名结果传输至安全芯片，安全芯片使用UK公钥、掩码进行异或运算，获取R2明文；将R1+R2合成DPK；

[0188] S7、安全芯片对合成的DPK进行杂凑运算，并与预留的DPK杂凑结果进行对比，核对数据；

[0189] S8、安全芯片使用UK对应的公钥进行验证运算；解密静态密钥，并删除DPK明文；

[0190] S9、安全芯片进行工作状态，返回身份认证结果至本地管理服务模块，本地管理服务模块返回身份认证结果至本地管理控制模块，由本地管理控制模块提示通过身份认证。

[0191] 在身份认证流程中，本地管理服务软件是流程的调度者，密码运算主要由智能密码钥匙(USB KEY)和安全控制芯片(88F3720)负责，密码运算过程如下。

[0192] 第一步，安全芯片上电后，即可获取R1明文数据；等待本地管理服务模块提供R2密文。安全芯片产生32字节的挑战数据用于智能密码钥匙的数字签名。

[0193] 本地管理服务软件将安全芯片产生的32字节挑战数据先进行摘要运算，摘要运算过程如下：

[0194] $H_{Cha}=H(Cha+UAK_{Pub})$；

[0195] 然后使用UAK的私钥UAK_{Pri}对H_{Cha}进行数字签名，签名运算过程如下：

[0196] $S_{Cha}=S(UAK_{Pri},H_{Cha})$。

[0197] 第二步，本地管理服务模块通过智能密码钥匙的API获取R2密文和明文UK-ID；然后本地管理服务模块将UK-ID、R2密文以及SCha发送给安全芯片进行身份验证。

[0198] 第三步，安全芯片在收到校验身份请求后，首先将还原得到的R2明文和R1明文合成DPK，合成运算如下：

[0199] $DPK_P=R1_P \oplus R2_P$

[0200] 然后对合成的DPK进行摘要计算，计算过程如下：

[0201] $H_{DPK}=H(DPK_P)$，将新合成的H_{DPK}与安全芯片中保存的H_{DPK}进行对比，若两者数据一致，则证明提供的R2密文数据和UK-ID数据是匹配的；此时，已恢复出DPK明文数据。

[0202] 对挑战数据进行摘要运算，运算过程如下：

[0203] $H_{Cha}=H(Cha+UAK_{Pub})$

[0204] 然后使用该用户对应的公钥进行验签，验签计算过程如下：

[0205] $B=V(UAK_{Pub},H_{Cha},S_{Cha})$

[0206] 若验证未通过，则清除DPK明文数据，并返回错误码；若验证通过，则使用DPK对密文DMK、DAK等数据解密得到明文密钥数据，设备进入工作态；最后，返回正确结果。

[0207] 在此步骤中，本地管理服务程序在创建用户时已经将该用户对应的UAK_{Pub}存放于内部存储区。

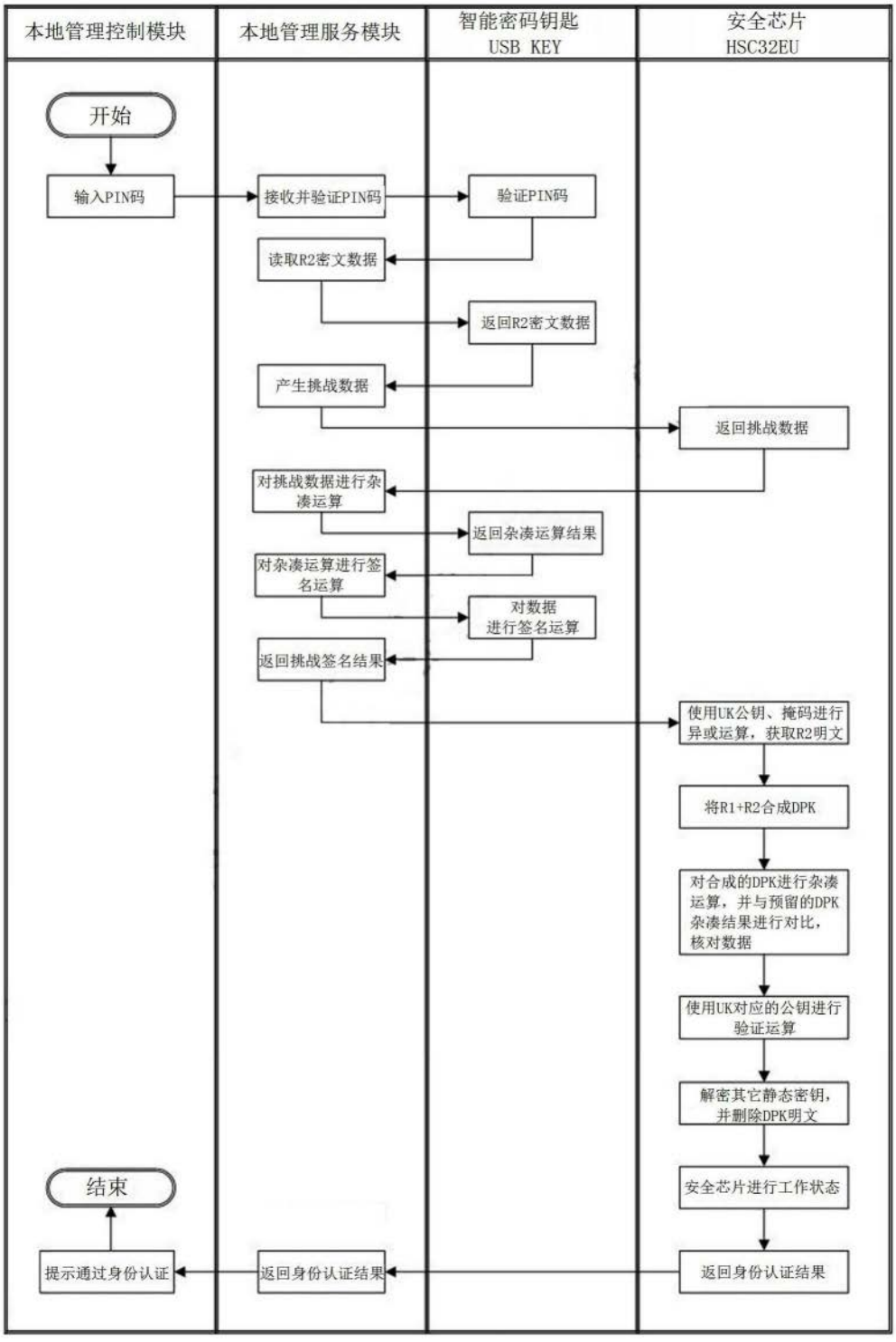

本地管理控制模块
本地管理服务模块
智能密码钥匙
USB KEY
安全芯片
HSC32EU
开始
输入PIN码
接收并验证PIN码
验证PIN码
读取R2密文数据
返回R2密文数据
产生挑战数据
返回挑战数据
对挑战数据进行杂凑运算
返回杂凑运算结果
对杂凑运算进行签名运算
对数据
进行签名运算
返回挑战签名结果
使用UK公钥、掩码进行异或运算，获取R2明文
将R1+R2合成DPK
对合成的DPK进行杂凑运算，并与预留的DPK杂凑结果进行对比，核对数据
使用UK对应的公钥进行验证运算
解密其它静态密钥，并删除DPK明文
安全芯片进行工作状态
结束
提示通过身份认证
返回身份认证结果
返回身份认证结果

图1

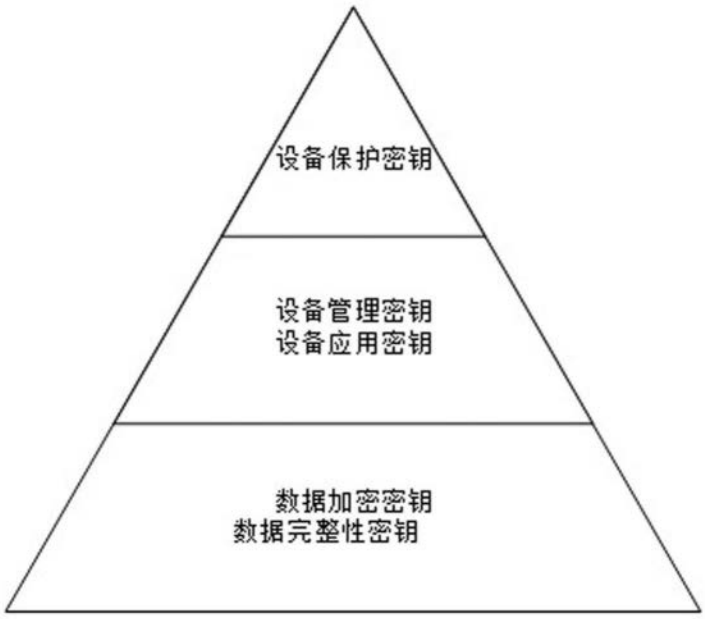

设备保护密钥
设备管理密钥
设备应用密钥
数据加密密钥
数据完整性密钥

图2

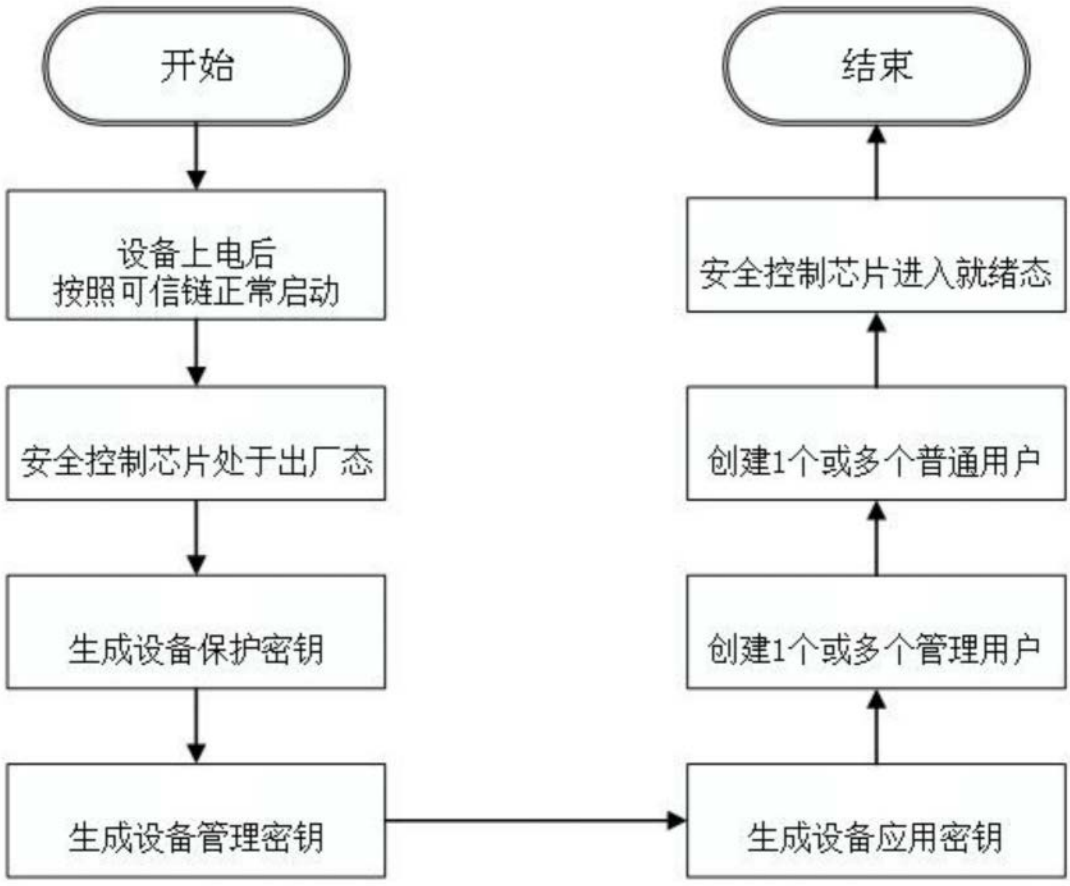

开始
设备上电后
按照可信链正常启动
安全控制芯片处于出厂态
生成设备保护密钥
生成设备管理密钥
生成设备应用密钥
创建1个或多个管理用户
创建1个或多个普通用户
安全控制芯片进入就绪态
结束

图3

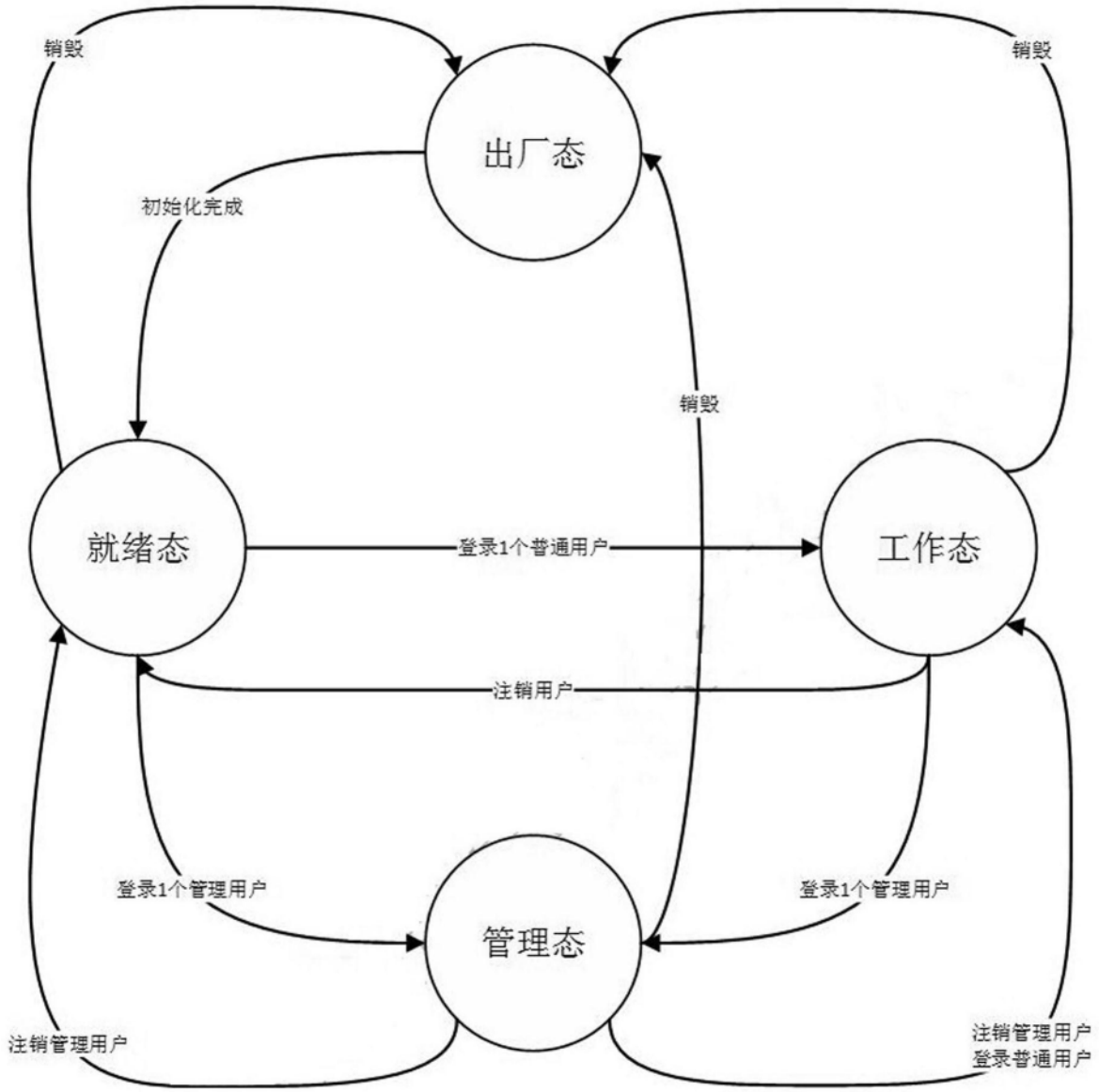

销毁
销毁
出厂态
初始化完成
销毁
就绪态
登录1个普通用户
工作态
注销用户
登录1个管理用户
登录1个管理用户
管理态
注销管理用户
注销管理用户
登录普通用户

图4

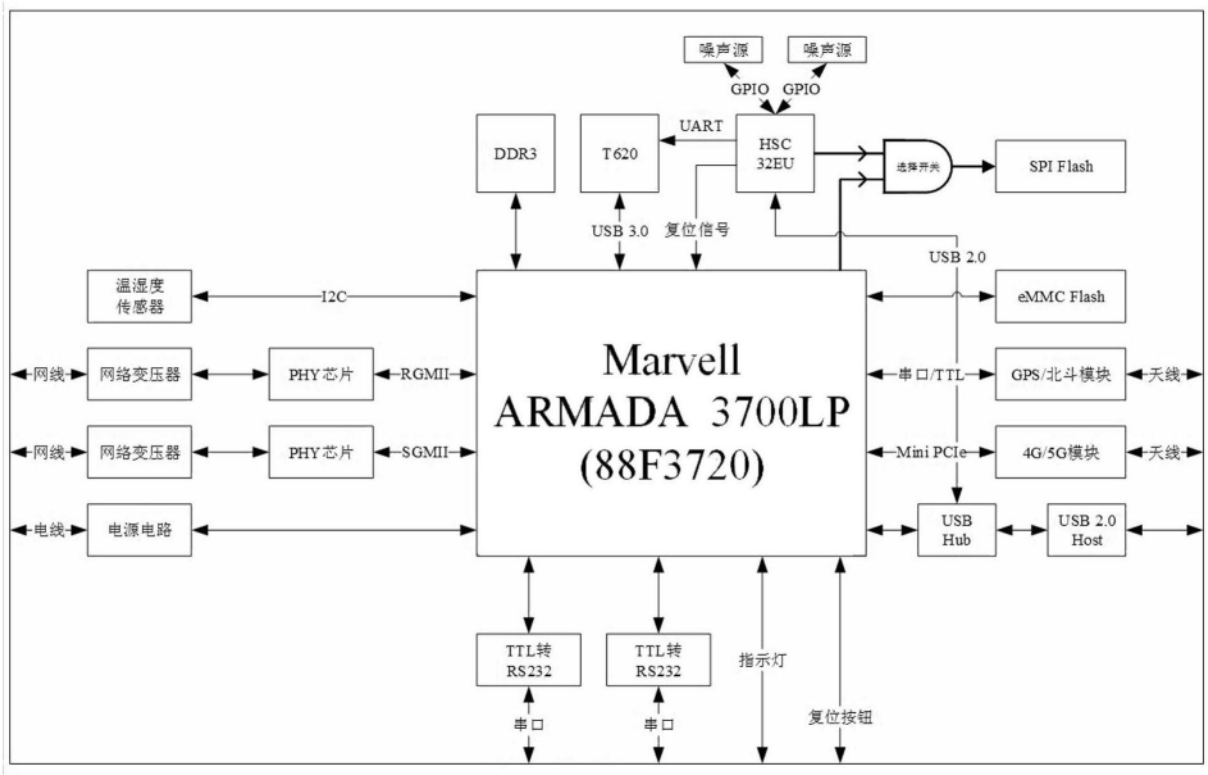

噪声源
噪声源
GPIO
GPIO
DDR3
T620
UART
HSC
32EU
选择开关
SPI Flash
USB 3.0
复位信号
USB 2.0
温湿度
传感器
I2C
eMMC Flash
网线
网络变压器
PHY芯片
RGMII
Marvell
ARMADA 3700LP
(88F3720)
串口/TTL
GPS/北斗模块
天线
网线
网络变压器
PHY芯片
SGMII
Mini PCIe
4G/5G模块
天线
电线
电源电路
USB
Hub
USB 2.0
Host
TTL转
RS232
TTL转
RS232
指示灯
串口
串口
复位按钮

图5

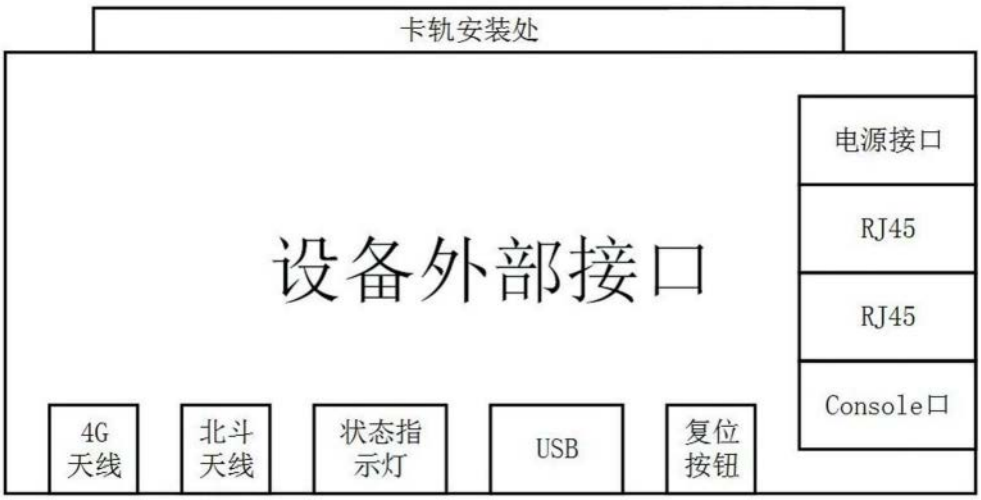

卡轨安装处
电源接口
RJ45
RJ45
Console口
设备外部接口
4G
天线
北斗
天线
状态指
示灯
USB
复位
按钮

图6

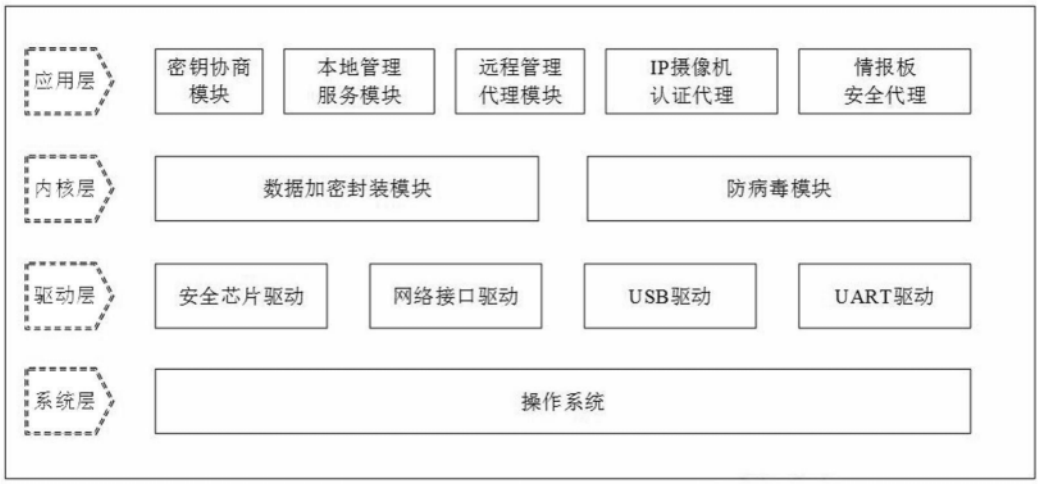

应用层
密钥协商模块
本地管理服务模块
远程管理代理模块
IP摄像机认证代理
情报板安全代理
内核层
数据加密封装模块
防病毒模块
驱动层
安全芯片驱动
网络接口驱动
USB驱动
UART驱动
系统层
操作系统

图7

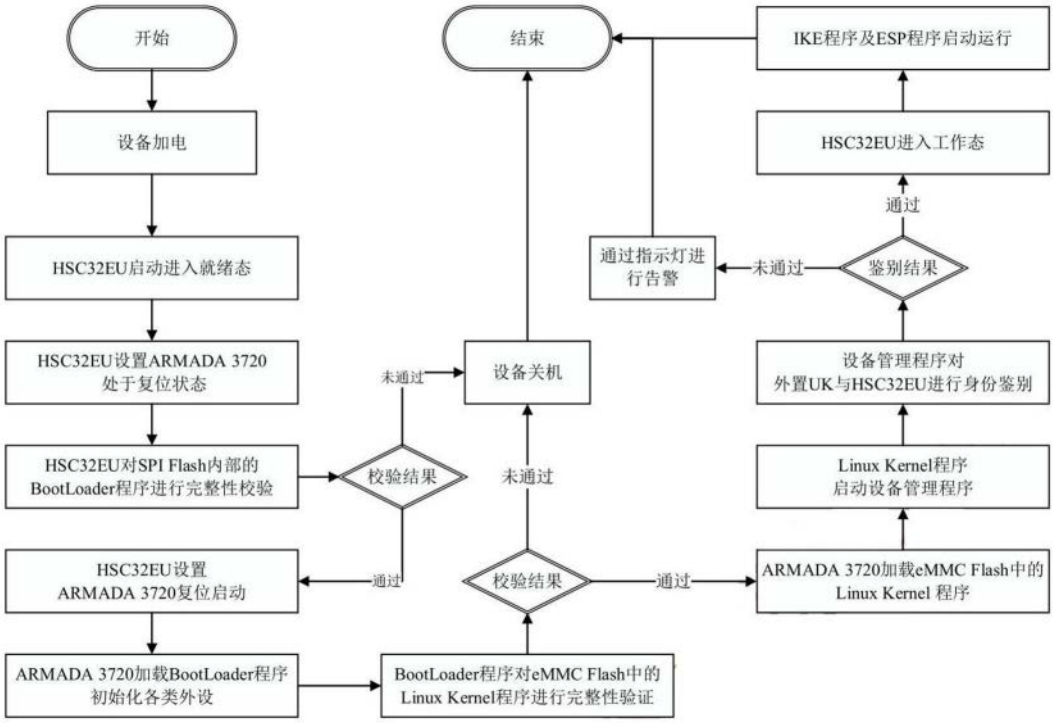

开始
设备加电
HSC32EU启动进入就绪态
HSC32EU设置ARMADA 3720处于复位状态
HSC32EU对SPI Flash内部的BootLoader程序进行完整性校验
校验结果
未通过
设备关机
通过
HSC32EU设置ARMADA 3720复位启动
ARMADA 3720加载BootLoader程序初始化各类外设
BootLoader程序对eMMC Flash中的Linux Kernel程序进行完整性验证
校验结果
未通过
结束
通过
ARMADA 3720加载eMMC Flash中的Linux Kernel 程序
Linux Kernel程序启动设备管理程序
设备管理程序对外置UK与HSC32EU进行身份鉴别
鉴别结果
未通过
通过指示灯进行告警
通过
HSC32EU进入工作态
IKE程序及ESP程序启动运行

图8

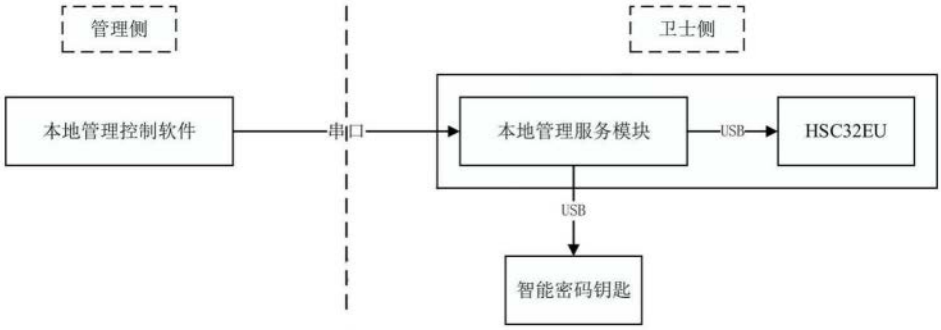


图9