(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 109257328 B
(45)授权公告日 2021.03.02

(21)申请号 201710577022.8

(22)申请日 2017.07.14

(65)同一申请的已公布的文献号
申请公布号 CN 109257328 A

(43)申请公布日 2019.01.22

(73)专利权人 中国电力科学研究院
地址 100192 北京市海淀区清河小营东路15号
专利权人 国家电网公司

(72)发明人 盛万兴 史常凯 李二霞 李玉凌 樊勇华 刘海涛 孟晓丽 张波 杨红磊 孙智涛

(74)专利代理机构 北京安博达知识产权代理有限公司 11271
代理人 徐国文

(51)Int.Cl.
*H04L 29/06*(2006.01)
*H04L 9/32*(2006.01)
*H04L 9/08*(2006.01)
*H02J 13/00*(2006.01)

(56)对比文件
CN 104393993 A,2015.03.04

审查员 任盈之

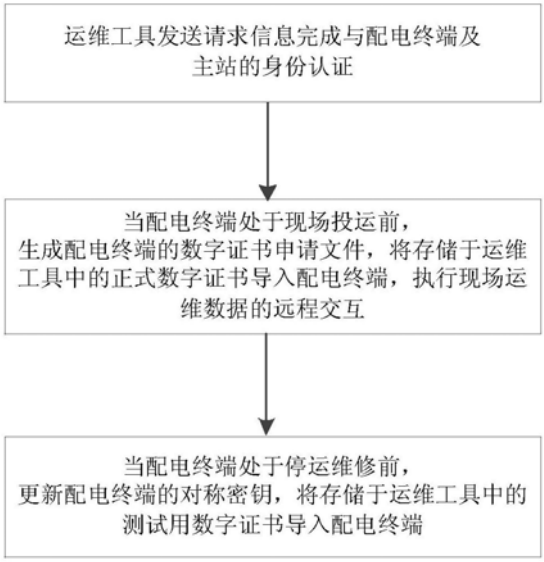
权利要求书4页 说明书11页 附图1页

(54)发明名称

一种现场运维数据的安全交互方法及装置

(57)摘要

本发明涉及一种现场运维数据的安全交互方法及装置，包括：运维工具发送请求信息完成与配电终端及主站的身份认证；当配电终端处于现场投运前，生成配电终端的数字证书申请文件，将存储于运维工具中的正式数字证书导入配电终端，执行现场运维数据的远程交互；当配电终端处于停运维修前，更新配电终端的对称密钥，将存储于运维工具中的测试数字证书导入配电终端。本方案的提出使现场终端数字证书和对称密钥的管理流程得到完善，弥补了配电终端现场运维过程中的安全防护漏洞，从而提高了配电终端现场应用与运维的安全防护水平。




CN 109257328 B

1.一种现场运维数据的安全交互方法,其特征在于,包括:

运维工具发送请求信息完成与配电终端及主站的身份认证;所述请求信息包括运维工具ID和数字证书;

当配电终端处于现场投运前,生成配电终端的数字证书申请文件,将存储于运维工具中的正式数字证书导入配电终端,执行现场运维数据的远程交互;

当配电终端处于停运维修前,更新配电终端的对称密钥,将存储于运维工具中的测试数字证书导入配电终端。

2.根据权利要求1所述的方法,其特征在于,所述运维工具发送请求信息完成与配电终端的身份认证包括:

所述运维工具接收配电终端生成的随机数R,将随机数R进行签名后发送至配电终端;

所述运维工具接收配电终端根据运维工具的数字证书验证签名有效性的结果,对于通过配电终端身份认证的运维工具,建立其与配电终端的现场运维报文传输。

3.根据权利要求1所述的方法,其特征在于,所述运维工具发送请求信息完成与主站的身份认证包括:

运维工具自动生成随机数$R_1$,将{$R_1$+运维工具数字证书}发送给主站;

主站从配电加密认证装置获取随机数$R_2$,对{$R_1$+$R_2$}签名获得$S_{mf}$,将{$R_2$+$S_{mf}$+签名密钥标识$I_{ask}$}发送给运维工具;

所述运维工具通过主站数字证书验证主站签名有效性,验证通过,则对主站随机数$R_2$进行签名,将{签名结果$S_{fm}$+签名密钥标识$I_f$}发送至主站;

主站通过运维工具数字证书验证运维工具签名的正确性,验证通过则认证运维工具身份,并返回认证结果信息;

双向认证成功后,主站发送读取运维工具ID的报文,运维工具返回其ID号以及用于计算消息认证码MAC的初始向量$IV_0$。

4.根据权利要求1所述的方法,其特征在于,所述生成配电终端的数字证书申请文件包括:

运维工具向配电终端发送终端序列号获取指令;

配电终端响应并返回终端序列号$N_t$;

运维工具向配电终端发送终端安全芯片序列号获取指令;

配电终端从安全芯片读取序列号$N_s$,并返回给运维工具;

运维工具向配电终端发送获取终端安全芯片公钥指令请求;

配电终端从安全芯片读取公钥$K_t$,并返回给运维工具;

运维工具生成包含$N_t$、$N_s$和$K_t$信息的证书请求字符串A,并将A发送给终端;

配电终端对A签名得到签名结果$S_a$,并将$S_a$返回给运维工具;

运维工具根据$N_t$、$N_s$、$K_t$、$S_a$和终端使用单位名称生成用于终端证书的申请文件。

5.根据权利要求1所述的方法,其特征在于,所述将存储于运维工具中的正式或测试数字证书导入配电终端包括:

运维工具将正式或测试数字证书以明文形式发送给配电终端,所述配电终端将数字证书下载到配电终端的安全芯片中,并向运维工具返回证书更新结果;其中,所述正式或测试数字证书的形式为{证书标识n+证书内容$C_n$},$C_n$包括CA二级应用证书、主站证书和网关证

书。

6.根据权利要求1所述的方法，其特征在于，所述更新配电终端的对称密钥包括：

配电终端收到所述终端安全芯片序列号获取指令，返回安全芯片序列号$N_s$；

运维工具向配电终端发送密钥版本号获取指令；

配电终端从安全芯片内读取对称密钥版本号$V_1$，获取随机数$R_3$，返回给运维工具；

运维工具对{$N_s$+$V_1$+$R_3$}签名获得签名结果$S_{rk}$，并将{$N_s$+$V_1$+$R_3$+$S_{rk}$+签名密钥标识$I_f$}发送给主站；

主站通过运维工具数字证书验证签名的有效性，若验证通过，根据密钥版本号$V_1$判断从加密认证装置中导出的对称密钥的版本号；

主站将终端随机数$R_3$作为计算消息认证码的初始向量，将终端安全芯片序列号$N_s$作为分散因子对$V_1$版本的主控密钥进行分散得到保护传输密钥，分散导出指定版本的对称密钥$P_k$；并基于SM2算法，利用主站私钥对$P_k$签名获得签名结果$S_k$，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}经所述运维工具发送给配电终端；

所述配电终端接收到密钥恢复报文后，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}发送到安全芯片，完成对称密钥的更新，并向运维工具返回更新结果信息。

7.根据权利要求6所述的方法，其特征在于，所述对称密钥$P_k$包括：密钥版本和密钥的密文与消息认证码。

8.根据权利要求3所述的方法，其特征在于，所述执行现场运维数据的远程交互的方法包括：

运维工具与主站身份认证成功后，采用现场运维数据保护加密密钥对发送的运维数据报文$M_{fm}$进行加密，并以$IV_0$为MAC初始向量，计算消息认证码，得到{密文$E_{fm}$+$MAC_{fm}$}，并将其发送给主站；

主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护解密密钥进行分散，并对{$E_{fm}$+$MAC_{fm}$}进行验证消息认证码和解密操作，获取明文报文数据；

主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护加密密钥进行分散，并对发送的运维数据报文$M_{mf}$进行加密；并以$IV_0$为消息认证码初始向量计算消息认证码得到{密文$E_{mf}$+$MAC_{mf}$}，将其发送给运维工具；

运维工具采用现场运维数据保护解密密钥对{$E_{mf}$+$MAC_{mf}$}进行验证消息认证码和解密操作，获取明文报文数据。

9.一种现场运维数据的安全交互装置，其特征在于，所述装置包括：

终端认证模块，用于运维工具发送请求信息完成与配电终端的身份认证；所述请求信息包括运维工具ID；

主站认证模块，用于运维工具发送请求信息完成与主站的身份认证；

远程交互模块，当配电终端处于现场投运前，生成配电终端的数字证书申请文件，将存储于运维工具中的正式数字证书导入配电终端，执行现场运维数据的远程交互；

更新模块，用于当配电终端处于停运维修前，更新配电终端的对称密钥，将存储于运维工具中的测试数字证书导入配电终端。

10.根据权利要求9所述的装置，其特征在于，所述终端认证模块包括：

第一随机数生成单元，用于运维工具接收配电终端生成的随机数R，将随机数R进行签

名后发送至配电终端；

第一签名有效性认证单元，用于运维工具接收配电终端根据运维工具的数字证书验证签名有效性的结果，对于通过配电终端身份认证的运维工具，建立其与配电终端的现场运维报文传输。

11.根据权利要求9所述的装置，其特征在于，所述主站认证模块包括：

第二随机数生成单元，用于运维工具自动生成随机数$R_1$，将{$R_1$+运维工具数字证书}发送给主站；主站从配电加密认证装置获取随机数$R_2$，对{$R_1$+$R_2$}签名获得$S_{mf}$，将{$R_2$+$S_{mf}$+签名密钥标识$I_{ask}$}发送给运维工具；

第二签名有效性认证单元，用于所述运维工具通过主站数字证书验证主站签名有效性，验证通过，则对主站随机数$R_2$进行签名，将{签名结果$S_{fm}$+签名密钥标识$I_f$}发送至主站；

第一数字证书正确性认证单元，用于主站通过运维工具数字证书验证运维工具签名的正确性，验证通过则认证运维工具身份，并返回认证结果信息；双向认证成功后，主站发送读取运维工具ID的报文，运维工具返回其ID号以及用于计算消息认证码的初始向量$IV_0$。

12.根据权利要求9所述的装置，其特征在于，所述远程交互模块包括：申请文件生成单元、正式证书导入单元和交互单元；其中，所述正式证书导入单元，用于运维工具将正式用数字证书以明文形式发送给配电终端，所述配电终端将数字证书下载到配电终端的安全芯片中，并向运维工具返回证书更新结果；

所述申请文件生成单元包括：

获取子单元，用于运维工具向配电终端发送终端序列号获取指令；配电终端响应并 返回终端序列号$N_t$；运维工具向配电终端发送终端安全芯片序列号获取指令；配电终端从安全芯片读取序列号$N_s$，并返回给运维工具；运维工具向配电终端发送获取终端安全芯片公钥指令请求；

读取子单元，用于配电终端从安全芯片读取公钥$K_t$，并返回给运维工具；

字符串生成子单元，用于运维工具生成包含$N_t$、$N_s$和$K_t$信息的证书请求字符串A，并将A发送给终端；

回执子单元，用于配电终端对A签名得到签名结果$S_a$，并将$S_a$返回给运维工具；运维工具根据$N_t$、$N_s$、$K_t$、$S_a$和终端使用单位名称生成用于终端证书的申请文件；

所述交互单元包括：

加密子单元，用于运维工具与主站身份认证成功后，采用现场运维数据保护加密密钥对发送的运维数据报文$M_{fm}$进行加密，并以$IV_0$为MAC初始向量，计算消息认证码，得到{密文$E_{fm}$+$MAC_{fm}$}，并将其发送给主站；

解密子单元，用于主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护解密密钥进行分散，并对{$E_{fm}$+$MAC_{fm}$}进行验证消息认证码和解密操作，获取明文报文数据；

密钥分散子单元，用于主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护加密密钥进行分散，并对发送的运维数据报文$M_{mf}$进行加密；并以$IV_0$为消息认证码初始向量计算消息认证码得到{密文$E_{mf}$+$MAC_{mf}$}，将其发送给运维工具；

明文报文数据获取子单元，用于运维工具采用现场运维数据保护解密密钥对{$E_{mf}$+$MAC_{mf}$}进行验证消息认证码和解密操作，获取明文报文数据。

13.根据权利要求9所述的装置，其特征在于，所述更新模块包括：更新单元和测试证书导入单元；

其中，所述测试证书导入单元，用于运维工具将正式用数字证书以明文形式发送给配电终端，所述配电终端将数字证书下载到配电终端的安全芯片中，并向运维工具返回 证书更新结果；

所述更新单元包括：

第一签名结果获取子单元，用于配电终端收到所述终端安全芯片序列号获取指令，返回安全芯片序列号$N_s$；运维工具向配电终端发送密钥版本号获取指令；配电终端从安全芯片内读取对称密钥版本号$V_1$，获取随机数$R_3$，返回给运维工具；运维工具对{$N_s$+$V_1$+$R_3$}签名获得签名结果$S_{rk}$，并将{$N_s$+$V_1$+$R_3$+$S_{rk}$+签名密钥标识$I_f$}发送给主站；

验证子单元，用于主站通过运维工具数字证书验证签名的有效性，若验证通过，根据密钥版本号$V_1$判断从加密认证装置中导出的对称密钥的版本号；

第二签名结果获取子单元，用于主站将终端随机数$R_3$作为计算消息认证码的初始向量，将终端安全芯片序列号$N_s$作为分散因子对$V_1$版本的主控密钥进行分散得到保护传输密钥，分散导出指定版本的对称密钥$P_k$；并基于SM2算法，利用主站私钥对$P_k$签名，获得签名结果$S_k$，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}经所述运维工具发送给配电终端；

返回子单元，用于配电终端接收到密钥恢复报文后，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}发送到安全芯片，完成对称密钥的更新，并向运维工具返回更新结果信息。

# 一种现场运维数据的安全交互方法及装置

## 技术领域

[0001] 本专利涉及配电自动化系统安全防护方法及装置，具体涉及一种现场运维数据的安全交互方法及装置。

## 背景技术

[0002] 配电自动化作为提高供电可靠性的必要手段和提升配网管理的重要工具，在提高供电可靠性与供电质量、提高配电网运检效率、降低运维人员现场操作和故障查找难度、提升配电网运维管控能力方面发挥了重要作用。近年来，国家发改委、国家能源局等主管部门加大了对电力信息安全的重点监督管控，相继颁布了国家发改委〔2014〕14号令《电力监控系统安全防护规定》和国能安全〔2015〕36号文《电力监控系统安全防护总体方案》等一系列法令、制度和标准，进一步明确了电网信息安全的重要性，对能源、电力等领域的关键信息基础设施的安全防护提出了更高要求，迫切需要全面升级配电自动化系统的安全防护体系，以满足国家对公司网络信息安全的各项要求。

[0003] 随着配电自动化工程建设的深入开展及实用化应用，相关部门对配电自动化终端的运行质量及现场运维安全防护能力提出了更高的要求。然而，目前配电终端现场运维过程中，运维人员通常采用便携式设备对终端进行运行状态巡视和软件功能维护，然而配电终端与现场运维工具之间的数据交互目前还没有任何安全措施与防护机制，运维软件极易被侵入篡改甚至复制模拟，形成安全防护漏洞；其次，终端无法认证现场运维工具的合法性，终端内部数据极易遭受非法运维工具的破坏；此外，现场配电终端的数字证书、对称密钥的管理流程还不够完善，对配电终端现场部署与应用工作的开展具有一定影响。

## 发明内容

[0004] 针对上述配电终端现场运维过程中的安全防护漏洞，以及现场终端数字证书、对称密钥的管理流程不够完善等问题，本发明提出一种现场运维数据的安全交互方法及装置。采用基于数字证书的身份认证、对称加密、数字签名等技术手段，提供了运维工具与配电终端、主站之间的安全交互方法，以及配电终端对称密钥恢复、数字证书申请与下载流程，从而提高了配电终端现场应用与运维的安全防护水平。

[0005] 本发明的目的是采用下述技术方案实现的：

[0006] 一种现场运维数据的安全交互方法，包括：

[0007] 运维工具发送请求信息完成与配电终端及主站的身份认证；其中，所述请求信息包括运维工具ID和数字证书；

[0008] 当配电终端处于现场投运前，生成配电终端的数字证书申请文件，将存储于运维工具中的正式数字证书导入配电终端，执行现场运维数据的远程交互；

[0009] 当配电终端处于停运维修前，更新配电终端的对称密钥，将存储于运维工具中的测试数字证书导入配电终端。

[0010] 优选的，所述运维工具发送请求信息完成与配电终端的身份认证包括：所述运维

工具接收配电终端生成的随机数R,将随机数R进行签名后发送至配电终端;

[0011] 所述运维工具接收配电终端根据运维工具的数字证书验证签名有效性的结果,对于通过配电终端身份认证的运维工具,建立其与配电终端的现场运维报文传输。

[0012] 优选的,所述运维工具发送请求信息完成与主站的身份认证包括:运维工具自动生成随机数$R_1$,将{$R_1$+运维工具数字证书}发送给主站;

[0013] 主站从配电加密认证装置获取随机数$R_2$,对{$R_1$+$R_2$}签名获得$S_{mf}$,将{$R_2$+$S_{mf}$+签名密钥标识$I_{ask}$}发送给运维工具;

[0014] 所述运维工具通过主站数字证书验证主站签名有效性,验证通过,则对主站随机数$R_2$进行签名,将{签名结果$S_{fm}$+签名密钥标识$I_f$}发送至主站;

[0015] 主站通过运维工具数字证书验证运维工具签名的正确性,验证通过则认证运维工具身份,并返回认证结果信息;

[0016] 双向认证成功后,主站发送读取运维工具ID的报文,运维工具返回其ID号以及用于计算消息认证码的初始向量$IV_0$。

[0017] 优选的,所述生成配电终端的数字证书申请文件包括:

[0018] 运维工具向配电终端发送终端序列号获取指令;

[0019] 配电终端响应并返回终端序列号$N_t$;

[0020] 运维工具向配电终端发送终端安全芯片序列号获取指令;

[0021] 配电终端从安全芯片读取序列号$N_s$,并返回给运维工具;

[0022] 运维工具向配电终端发送获取终端安全芯片公钥指令请求;

[0023] 配电终端从安全芯片读取公钥$K_t$,并返回给运维工具;

[0024] 运维工具生成包含$N_t$、$N_s$和$K_t$信息的证书请求字符串A,并将A发送给终端;

[0025] 配电终端对A签名得到签名结果$S_a$,并将$S_a$返回给运维工具;

[0026] 运维工具根据$N_t$、$N_s$、$K_t$、$S_a$和终端使用单位名称生成用于终端证书申请文件。

[0027] 优选的,所述将存储于运维工具中的正式或测试数字证书导入配电终端包括:

[0028] 运维工具将正式或测试数字证书以明文形式发送给配电终端,所述配电终端将数字证书下载到配电终端的安全芯片中,并向运维工具返回证书更新结果;其中,所述正式或测试数字证书的形式为{证书标识n+证书内容$C_n$},$C_n$包括CA二级应用证书、主站证书和网关证书。

[0029] 优选的,所述更新配电终端的对称密钥包括:

[0030] 配电终端收到所述终端安全芯片序列号获取指令,返回安全芯片序列号$N_s$;

[0031] 运维工具向配电终端发送密钥版本号获取指令;

[0032] 配电终端从安全芯片内读取对称密钥版本号$V_1$,获取随机数$R_3$,返回给运维工具;

[0033] 运维工具对{$N_s$+$V_1$+$R_3$}签名结果$S_{rk}$,并将{$N_s$+$V_1$+$R_3$+$S_{rk}$+签名密钥标识$I_f$}发送给主站;

[0034] 主站通过运维工具数字证书验证签名的有效性,若验证通过,根据密钥版本号$V_1$判断从加密认证装置中导出的对称密钥的版本号;

[0035] 主站将终端随机数$R_3$作为计算消息认证码的初始向量,将终端安全芯片序列号$N_s$作为分散因子对$V_1$版本的主控密钥进行分散得到保护传输密钥,分散导出指定版本的对称密钥$P_k$;并基于SM2算法,利用主站私钥对$P_k$进行签名获得$S_k$,将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}经

所述运维工具发送给配电终端；

[0036] 所述配电终端接收到密钥恢复报文后，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}发送到安全芯片，完成对称密钥的更新，并向运维工具返回更新结果信息。

[0037] 进一步地，所述对称密钥$P_k$包括：密钥版本和密钥的密文与消息认证码。

[0038] 优选的，所述执行现场运维数据的远程交互的方法包括：

[0039] 运维工具与主站身份认证成功后，采用现场运维数据保护加密密钥对发送的运维数据报文$M_{fm}$进行加密，并以$IV_0$为MAC初始向量，计算消息认证码，得到{密文$E_{fm}$+$MAC_{fm}$}，并将其发送给主站；

[0040] 主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护解密密钥进行分散，并对{$E_{fm}$+$MAC_{fm}$}进行验证消息认证码和解密操作，获取明文报文数据；

[0041] 主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护加密密钥进行分散，并对发送的运维数据报文$M_{mf}$进行加密；并以$IV_0$为消息认证码初始向量计算消息认证码得到{密文$E_{mf}$+$MAC_{mf}$}，将其发送给运维工具；

[0042] 运维工具采用现场运维数据保护解密密钥对{$E_{mf}$+$MAC_{mf}$}进行验证消息认证码和解密操作，获取明文报文数据。

[0043] 一种现场运维数据的安全交互装置，所述装置包括：

[0044] 终端认证模块，用于运维工具发送请求信息完成与配电终端的身份认证；

[0045] 主站认证模块，用于运维工具发送请求信息完成与主站的身份认证；

[0046] 远程交互模块，当配电终端处于现场投运前，生成配电终端的数字证书申请文件，将存储于运维工具中的正式数字证书导入配电终端，执行现场运维数据的远程交互；

[0047] 更新模块，用于当配电终端处于停运维修前，更新配电终端的对称密钥，将存储于运维工具中的测试数字证书导入配电终端。

[0048] 优选的，所述终端认证模块包括：

[0049] 第一随机数生成单元，用于运维工具接收配电终端生成的随机数R，将随机数R进行签名后发送至配电终端；

[0050] 第一签名有效性认证单元，用于运维工具接收配电终端根据运维工具的数字证书验证签名有效性的结果，对于通过配电终端身份认证的运维工具，建立其与配电终端的现场运维报文传输。

[0051] 优选的，所述主站认证模块包括：

[0052] 第二随机数生成单元，用于运维工具自动生成随机数$R_1$，将{$R_1$+运维工具数字证书}发送给主站；主站从配电加密认证装置获取随机数$R_2$，对{$R_1$+$R_2$}签名获得$S_{mf}$，将{$R_2$+$S_{mf}$+签名密钥标识$I_{ask}$}发送给运维工具；

[0053] 第二签名有效性认证单元，用于所述运维工具通过主站数字证书验证主站签名有效性，验证通过，则对主站随机数$R_2$进行签名，将{签名结果$S_{fm}$+签名密钥标识$I_f$}发送至主站；

[0054] 第一数字证书正确性认证单元，用于主站通过运维工具数字证书验证运维工具签名的正确性，验证通过则认证运维工具身份，并返回认证结果信息；双向认证成功后，主站发送读取运维工具ID的报文，运维工具返回其ID号以及用于计算消息认证码的初始向量$IV_0$。

[0055] 优选的，所述远程交互模块包括：申请文件生成单元、正式证书导入单元和交互单元；其中，所述正式证书导入单元，用于运维工具将正式用数字证书以明文形式发送给配电终端，所述配电终端将数字证书下载到配电终端的安全芯片中，并向运维工具返回证书更新结果；

[0056] 所述申请文件生成单元包括：

[0057] 获取子单元，用于运维工具向配电终端发送终端序列号获取指令；配电终端响应并返回终端序列号$N_t$；运维工具向配电终端发送终端安全芯片序列号获取指令；配电终端从安全芯片读取序列号$N_s$，并返回给运维工具；运维工具向配电终端发送获取终端安全芯片公钥指令请求；

[0058] 读取子单元，用于配电终端从安全芯片读取公钥$K_t$，并返回给运维工具；

[0059] 字符串生成子单元，用于运维工具生成包含$N_t$、$N_s$和$K_t$信息的证书请求字符串A，并将A发送给终端；

[0060] 回执子单元，用于配电终端对A签名得到签名结果$S_a$，并将$S_a$返回给运维工具；运维工具根据$N_t$、$N_s$、$K_t$、$S_a$和终端使用单位名称生成用于终端证书申请文件；

[0061] 所述交互单元包括：

[0062] 加密子单元，用于运维工具与主站身份认证成功后，采用现场运维数据保护加密密钥对发送的运维数据报文$M_{fm}$进行加密，并以$IV_0$为MAC初始向量，计算消息认证码，得到{密文$E_{fm}$+$MAC_{fm}$}，并将其发送给主站；

[0063] 解密子单元，用于主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护解密密钥进行分散，并对{$E_{fm}$+$MAC_{fm}$}进行验证消息认证码和解密操作，获取明文报文数据；

[0064] 密钥分散子单元，用于主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护加密密钥进行分散，并对发送的运维数据报文$M_{mf}$进行加密；并以$IV_0$为消息认证码初始向量计算消息认证码得到{密文$E_{mf}$+$MAC_{mf}$}，将其发送给运维工具；

[0065] 明文报文数据获取子单元，用于运维工具采用现场运维数据保护解密密钥对{$E_{mf}$+$MAC_{mf}$}进行验证消息认证码和解密操作，获取明文报文数据。

[0066] 优选的，所述更新模块包括：更新单元和测试证书导入单元；

[0067] 其中，所述测试证书导入单元，用于运维工具将正式用数字证书以明文形式发送给配电终端，所述配电终端将数字证书下载到配电终端的安全芯片中，并向运维工具返回证书更新结果；

[0068] 所述更新单元包括：

[0069] 第一签名结果获取子单元，用于配电终端收到所述终端安全芯片序列号获取指令，返回安全芯片序列号$N_s$；运维工具向配电终端发送密钥版本号获取指令；配电终端从安全芯片内读取对称密钥版本号$V_1$，获取随机数$R_3$，返回给运维工具；运维工具对{$N_s$+$V_1$+$R_3$}签名获得签名结果$S_{rk}$，并将{$N_s$+$V_1$+$R_3$+$S_{rk}$+签名密钥标识$I_f$}发送给主站；

[0070] 验证子单元，用于主站通过运维工具数字证书验证签名的有效性，若验证通过，根据密钥版本号$V_1$判断从加密认证装置中导出的对称密钥的版本号；

[0071] 第二签名结果获取子单元，用于主站将终端随机数$R_3$作为计算消息认证码的初始向量，将终端安全芯片序列号$N_s$作为分散因子对$V_1$版本的主控密钥进行分散得到保护传输

密钥,分散导出指定版本的对称密钥$P_k$;并基于SM2算法,利用主站私钥对$P_k$签名,获得签名结果$S_k$,将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}经所述运维工具发送给配电终端;

[0072] 返回子单元,用于配电终端接收到密钥恢复报文后,将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}发送到安全芯片,完成对称密钥的更新,并向运维工具返回更新结果信息。

[0073] 与最接近的现有技术比,本发明的有益效果为:

[0074] 本发明提供一种现场运维数据的安全交互方法及装置,具备对配电终端运维数据机密性和完整性的安全防护能力,可有效防止运维数据被黑客恶意篡改、仿造或破坏。

[0075] 运维工具发送请求信息完成与配电终端及主站的身份认证;当配电终端处于现场投运前,生成配电终端的数字证书申请文件,将存储于运维工具中的正式数字证书导入配电终端,执行现场运维数据的远程交互;当配电终端处于停运维修前,更新配电终端的对称密钥,将存储于运维工具中的测试数字证书导入配电终端。通过以上操作完善了现场配电终端数字证书、对称密钥的安全管理机制。增加了配电终端对现场运维工具的身份鉴别能力,以及运维工具与主站之间双向身份鉴别能力,提高了终端现场运维业务的安全防护水平。

## 附图说明

[0076] 图1为本发明提供的配电终端运维工具安全交互方法流程图。

## 具体实施方式

[0077] 下面结合附图对本发明的具体实施方式作进一步详细的说明。

[0078] 本发明提供一种现场运维数据的安全交互方法,如图1所示,该方法包括如下步骤:

[0079] I、运维工具发送请求信息完成与配电终端及主站的身份认证;分别为与配电终端建立单向安全认证,与主站建立双向身份认证;其中,所述请求信息包括运维工具ID和数字证书。运维工具支持国密SM1、对称加密算法和国密SM2、SM3非对称加密算法。

[0080] 1)运维工具发送请求信息完成与配电终端的身份认证包括:所述运维工具接收配电终端生成的随机数R,将随机数R进行签名后发送至配电终端;

[0081] 运维工具接收配电终端根据运维工具的数字证书验证签名有效性的结果,对于通过配电终端身份认证的运维工具,建立其与配电终端的现场运维报文传输。

[0082] 2)运维工具发送请求信息完成与主站的身份认证包括:运维工具自动生成随机数$R_1$,将{$R_1$+运维工具数字证书}发送给主站;

[0083] 主站从配电加密认证装置获取随机数$R_2$,对{$R_1$+$R_2$}签名获得$S_{mf}$,将{$R_2$+$S_{mf}$+签名密钥标识$I_{ask}$}发送给运维工具;

[0084] 运维工具通过主站数字证书验证主站签名有效性,验证通过,则对主站随机数$R_2$进行签名,将{签名结果$S_{fm}$+签名密钥标识$I_f$}发送至主站;

[0085] 主站通过运维工具数字证书验证运维工具签名的正确性,验证通过则认证运维工具身份,并返回认证结果信息;

[0086] 双向认证成功后,主站发送读取运维工具ID的报文,运维工具返回其ID号以及用于计算消息认证码的初始向量$IV_0$。

[0087] Ⅱ、当配电终端处于现场投运前，生成配电终端的数字证书申请文件，将存储于运维工具中的正式数字证书导入配电终端，执行现场运维数据的远程交互；

[0088] 生成配电终端的数字证书申请文件包括：

[0089] 运维工具向配电终端发送终端序列号获取指令；

[0090] 配电终端响应并返回终端序列号$N_t$；

[0091] 运维工具向配电终端发送终端安全芯片序列号获取指令；

[0092] 配电终端从安全芯片读取序列号$N_s$，并返回给运维工具；

[0093] 运维工具向配电终端发送获取终端安全芯片公钥指令请求；

[0094] 配电终端从安全芯片读取公钥$K_t$，并返回给运维工具；

[0095] 运维工具生成包含$N_t$、$N_s$和$K_t$信息的证书请求字符串A，并将A发送给终端；

[0096] 配电终端对A签名得到签名结果$S_a$，并将$S_a$返回给运维工具；

[0097] 运维工具根据$N_t$、$N_s$、$K_t$、$S_a$和终端使用单位名称，即所属地市电力公司信息，生成用于终端证书申请的PCKS#10文件。

[0098] 将存储于运维工具中的正式或测试数字证书导入配电终端包括：运维工具将正式或测试数字证书以明文形式发送给配电终端，所述配电终端将数字证书下载到配电终端的安全芯片中，并向运维工具返回证书更新结果；其中，所述正式或测试数字证书的形式为{证书标识+证书内容}，包括CA二级应用证书、主站证书和网关证书。证书内容$C_n$包括用于表示是正式或测试数字证书的字段，配电终端的安全芯片可以通过该字段识别正式或测试数字证书。

[0099] Ⅲ、当配电终端处于停运维修前，更新配电终端的对称密钥，将存储于运维工具中的测试数字证书导入配电终端。

[0100] 更新配电终端的对称密钥包括：

[0101] 配电终端收到所述终端安全芯片序列号获取指令，返回安全芯片序列号$N_s$；

[0102] 运维工具向配电终端发送密钥版本号获取指令；

[0103] 配电终端从安全芯片内读取对称密钥版本号$V_1$，获取随机数$R_3$，返回给运维工具；

[0104] 运维工具对{$N_s$+$V_1$+$R_3$}签名结果$S_{rk}$，并将{$N_s$+$V_1$+$R_3$+$S_{rk}$+签名密钥标识$I_f$}发送给主站；

[0105] 主站通过运维工具数字证书验证签名的有效性，若验证通过，根据密钥版本号$V_1$判断从加密认证装置中导出的对称密钥的版本号；

[0106] 主站将终端随机数$R_3$作为计算消息认证码的初始向量，将终端安全芯片序列号$N_s$作为分散因子对$V_1$版本的主控密钥进行分散得到保护传输密钥，分散导出指定版本的对称密钥$P_k$；并基于SM2算法，利用主站私钥对$P_k$进行签名获得$S_k$，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}经所述运维工具发送给配电终端；

[0107] 配电终端接收到密钥恢复报文后，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}发送到安全芯片，完成对称密钥的更新，并向运维工具返回更新结果信息。

[0108] 对称密钥$P_k$包括：密钥版本和密钥的密文与消息认证码。

[0109] 执行现场运维数据的远程交互的方法包括：

[0110] 运维工具与主站身份认证成功后，采用现场运维数据保护加密密钥对发送的运维数据报文$M_{fm}$进行加密，并以$IV_0$为MAC初始向量，计算消息认证码，得到{密文$E_{fm}$+$MAC_{fm}$}，并

将其发送给主站；

[0111] 主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护解密密钥进行分散，并对{$E_{fm}$+$MAC_{fm}$}进行验证消息认证码和解密操作，获取明文报文数据；

[0112] 主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护加密密钥进行分散，并对发送的运维数据报文$M_{mf}$进行加密；并以$IV_0$为消息认证码初始向量计算消息认证码得到{密文$E_{mf}$+$MAC_{mf}$}，将其发送给运维工具；

[0113] 运维工具采用现场运维数据保护解密密钥对{$E_{mf}$+$MAC_{mf}$}进行验证消息认证码和解密操作，获取明文报文数据。

[0114] 具体应用的实施例如下：

[0115] 运维工具集成安全模块，支持国密SM1对称加密算法和国密SM2、SM3非对称加密算法。运维工具经发行后，内置1对非对称密钥及其数字证书$C_F$，用于与终端、主站之间的身份认证；内置的对称密钥包括现场运维数据保护解密密钥$K'_{14}$和现场运维数据保护加密密钥$K'_{15}$；内置正式的CA二级应用证书$C_0$、主站证书($C_1$,$C_2$,$C_3$,$C_4$)和安全接入网关证书$C_5$，内置用于测试的CA二级应用证书$C'_0$、主站证书($C'_1$,$C'_2$,$C'_3$,$C'_4$)和安全接入网关证书$C'_5$；运维工具的形式包括手持式运维终端、笔记本电脑等，通过串口等接口与配电终端通信，通过光纤以太网或无线公网等方式与配电主站通信。

[0116] 1)运维工具发送请求信息完成与配电终端及主站的身份认证，即运维工具与配电终端之间单向认证和运维工具与主站双向认证。

[0117] 运维工具与配电终端身份认证流程如下：

[0118] a.运维工具向终端发起认证请求，将运维工具ID和数字证书$C_F$发送给终端；

[0119] b.终端取随机数R发送给运维工具；

[0120] c.运维工具对随机数R进行签名，并将签名结果发送给终端；

[0121] d.终端用$C_F$验证签名有效性，并将认证结果返回给运维工具。运维工具通过终端的安全认证后，双方之间方可传输现场运维报文。

[0122] 运维工具与主站双向认证流程如下：

[0123] a.运维工具与主站之间建立网络连接后，如TCP连接；运维工具向主站发起双向身份认证请求。运维工具取随机数$R_1$，将{$R_1$+$C_F$}发送给主站；

[0124] b.主站从配电加密认证装置取随机数$R_2$，对{$R_1$+$R_2$}签名后得到$S_{mf}$，将{$R_2$+$S_{mf}$+签名密钥标识$I_{ask}$}发送给运维工具；$I_{ask}$可取1,2,3,4；

[0125] c.运维工具用主站证书(证书标识须与$I_{ask}$对应；例如$I_{ask}$＝1时，则使用主站证书$C_1$)验证主站签名有效性，验证通过完成运维工具对主站的身份；之后运维工具对主站随机数$R_2$签名，将{签名结果$S_{fm}$+签名密钥标识$I_f$}发送给主站；$I_f$可取1。

[0126] d.主站用$C_F$验证运维工具签名的正确性，验证通过完成主站对运维工具的身份认证并返回认证确认信息；

[0127] e.双向认证成功后，主站发送读取运维工具ID的报文，运维工具返回其ID号，以及用于计算消息认证码(MAC)的初始向量$IV_0$。

[0128] Ⅱ、当配电终端处于现场投运前，生成配电终端的数字证书申请文件，将存储于运维工具中的正式数字证书导入配电终端，执行现场运维数据的远程交互；

[0129] 1)生成配电终端的数字证书申请文件包括：

[0130] a.运维工具向配电终端发送获取终端序列号指令；

[0131] b.配电终端返回终端序列号$N_t$；

[0132] c.运维工具向配电终端发送获取终端安全芯片序列号指令；

[0133] d.配电终端从安全芯片读取序列号$N_s$，并返回给运维工具；

[0134] e.运维工具向配电终端发送获取终端安全芯片公钥指令；

[0135] f.配电终端从安全芯片读取公钥$K_t$，并返回给运维工具；

[0136] g.运维工具生成包含$N_t$、$N_s$和$K_t$信息的证书请求字符串A，并将A发送给终端；

[0137] h.配电终端对A签名得到$S_a$，并将$S_a$返回给运维工具；

[0138] i.运维工具利用$N_t$、$N_s$、$K_t$、$S_a$和终端所属地市电力公司信息生成用于终端证书申请的PCKS#10文件。

[0139] 现场运维数据远程安全交互包括：

[0140] a.运维工具与主站之间通过身份认证后，用现场运维数据保护加密密钥$K'_{15}$对发送的运维数据报文$M_{fm}$进行加密，并以$IV_0$为MAC初始向量计算MAC得到{密文$E_{fm}$+$MAC_{fm}$}，并将其发送给主站；

[0141] b.主站利用运维工具ID作为分散因子对配电加密认证装置中的现场运维数据保护解密密钥$K_{15}$进行1次分散得到$K'_{15}$，并对{$E_{fm}$+$MAC_{fm}$}进行验证MAC和解密操作，获取明文报文数据；主站利用运维工具ID作为分散因子对配电加密认证装置中的现场运维数据保护加密密钥$K_{14}$进行1次分散得到$K'_{14}$，对发送的运维数据报文$M_{mf}$进行加密并以$IV_0$为MAC初始向量计算MAC得到{密文$E_{mf}$+$MAC_{mf}$}，将其发送给运维工具；

[0142] c.运维工具用现场运维数据保护解密密钥$K'_{14}$对{$E_{mf}$+$MAC_{mf}$}进行验证MAC和解密操作，获取明文报文数据。

[0143] 现场运维数据远程安全交互包括：

[0144] a.运维工具与主站之间通过身份认证后，用现场运维数据保护加密密钥$K'_{15}$对发送的运维数据报文$M_{fm}$进行加密，并以$IV_0$为MAC初始向量计算MAC得到{密文$E_{fm}$+$MAC_{fm}$}，并将其发送给主站；

[0145] b.主站利用运维工具ID作为分散因子对配电加密认证装置中的现场运维数据保护解密密钥$K_{15}$进行1次分散得到$K'_{15}$，并对{$E_{fm}$+$MAC_{fm}$}进行验证MAC和解密操作，获取明文报文数据；主站利用运维工具ID作为分散因子对配电加密认证装置中的现场运维数据保护加密密钥$K_{14}$进行1次分散得到$K'_{14}$，对发送的运维数据报文$M_{mf}$进行加密并以$IV_0$为MAC初始向量计算MAC得到{密文$E_{mf}$+$MAC_{mf}$}，将其发送给运维工具；

[0146] c.运维工具用现场运维数据保护解密密钥$K'_{14}$对{$E_{mf}$+$MAC_{mf}$}进行验证MAC和解密操作，获取明文报文数据。

[0147] 将存储于运维工具中的正式或测试数字证书导入配电终端包括：运维工具将正式或测试数字证书以明文形式发送给配电终端，所述配电终端将数字证书下载到配电终端的安全芯片中，并向运维工具返回证书更新结果；其中，所述正式或测试数字证书的形式为{证书标识+证书内容}，包括CA二级应用证书、主站证书和网关证书。证书内容$C_n$包括用于表示正式或测试数字证书的字段，配电终端的安全芯片可以通过该字段识别正式或测试数字证书。

[0148] 配电终端现场投运前，运维工具将正式的CA二级应用证书$C_0$、主站证书($C_1$，$C_2$，$C_3$，

$C_4$)和安全接入网关证书$C_5$导入配电终端；

[0149] 其安全芯片内置正式的对称密钥包括：$K'_{10}$，$K'_{11}$，$K'_{12}$，$K_{13}$，$K_{14}$；配电主站侧加密认证装置经发行后，内置2组与终端安全芯片中功能相同的对称密钥；其中，第0组测试密钥为：$K_{00}$，$K_{01}$，$K_{02}$，$K_{03}$，$K_{04}$；第1组正式密钥为：$K_{10}$，$K_{11}$，$K_{12}$，$K_{13}$，$K_{14}$。

[0150] Ⅲ、当配电终端处于停运维修前，更新配电终端的对称密钥，将存储于运维工具中的测试数字证书导入配电终端。

[0151] 运维工具将用于测试的CA二级应用证书$C'_0$、主站证书($C'_1$，$C'_2$，$C'_3$，$C'_4$)和安全接入网关证书$C'_5$导入配电终端；运维工具将{证书标识n+证书内容$C_n$}(n可取0,1,2,3,4,5)以明文形式发送给配电终端；配电终端将证书内容下载到安全芯片。

[0152] 更新配电终端的对称密钥包括：

[0153] a.运维工具向配电终端发送获取终端安全芯片序列号指令；

[0154] b.配电终端返回安全芯片序列号$N_s$；

[0155] c.运维工具向终端发送取密钥版本号指令；

[0156] d.终端从安全芯片内读取对称密钥版本号$V_1$($V_1$可取1)，并获取随机数$R_3$，返回给运维工具；

[0157] e.运维工具对{$N_s$+$V_1$+$R_3$}签名得到$S_{rk}$，并将{$N_s$+$V_1$+$R_3$+$S_{rk}$+签名密钥标识$I_f$}发送给主站；

[0158] f.主站用$C_F$验证签名有效性，若验证通过，主站通过密钥版本号$V_1$判断需要从加密认证装置中导出的对称密钥的版本号$V_0$($V_0$取0)；

[0159] g.主站利用终端随机数$R_3$作为计算MAC的初始向量，利用终端安全芯片序列号$N_s$作为分散因子对$V_1$版的主控密钥$K_{10}$进行分散得到保护传输密钥$K'_{10}$，分散导出$V_0$版的对称密钥得到$K'_{00}$，$K'_{01}$，$K'_{02}$，$K_{03}$，$K_{04}$(对$K_{00}$，$K_{01}$，$K_{02}$的分散次数为1；对$K_{03}$，$K_{04}$的分散次数为0)的密文和MAC；导出的数据包$P_k$为：{$V_0$，$K'_{00}$的密文+MAC，$K'_{01}$的密文+MAC，…，$K_{04}$的密文+MAC}，并利用主站私钥对$P_k$进行签名得到$S_k$，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}发送给运维工具；

[0160] e.运维工具将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}发送给配电终端；终端接收到密钥恢复报文后，将{$I_{ask}$+$P_k$+$S_k$}发送到安全芯片，完成密钥更新，并向运维工具返回更新结果。

[0161] 基于上述发明构思，本实施例中还提供了一种现场运维数据的安全交互装置，包括：

[0162] 终端认证模块，用于运维工具发送请求信息完成与配电终端的身份认证；

[0163] 主站认证模块，用于运维工具发送请求信息完成与主站的身份认证；

[0164] 远程交互模块，当配电终端处于现场投运前，生成配电终端的数字证书申请文件，将存储于运维工具中的正式数字证书导入配电终端，执行现场运维数据的远程交互；

[0165] 更新模块，用于当配电终端处于停运维修前，更新配电终端的对称密钥，将存储于运维工具中的测试数字证书导入配电终端。

[0166] 其中：

[0167] 终端认证模块包括：

[0168] 第一随机数生成单元，用于运维工具接收配电终端生成的随机数R，将随机数R进行签名后发送至配电终端；

[0169] 第一签名有效性认证单元，用于运维工具接收配电终端根据运维工具的数字证书

验证签名有效性的结果，对于通过配电终端身份认证的运维工具，建立其与配电终端的现场运维报文传输。

[0170] 主站认证模块包括：

[0171] 第二随机数生成单元，用于运维工具自动生成随机数$R_1$，将{$R_1$+运维工具数字证书}发送给主站；主站从配电加密认证装置获取随机数$R_2$，对{$R_1$+$R_2$}签名获得$S_{mf}$，将{$R_2$+$S_{mf}$+签名密钥标识$I_{ask}$}发送给运维工具；

[0172] 第二签名有效性认证单元，用于所述运维工具通过主站数字证书验证主站签名有效性，验证通过，则对主站随机数$R_2$进行签名，将{签名结果$S_{fm}$+签名密钥标识$I_f$}发送至主站；

[0173] 第一数字证书正确性认证单元，用于主站通过运维工具数字证书验证运维工具签名的正确性，验证通过则认证运维工具身份，并返回认证结果信息；双向认证成功后，主站发送读取运维工具ID的报文，运维工具返回其ID号以及用于计算消息认证码的初始向量$IV_0$。

[0174] 远程交互模块包括：申请文件生成单元、正式证书导入单元和交互单元；其中，所述正式证书导入单元，用于运维工具将正式用数字证书以明文形式发送给配电终端，所述配电终端将数字证书下载到配电终端的安全芯片中，并向运维工具返回证书更新结果；

[0175] 申请文件生成单元包括：

[0176] 获取子单元，用于运维工具向配电终端发送终端序列号获取指令；配电终端响应并返回终端序列号$N_t$；运维工具向配电终端发送终端安全芯片序列号获取指令；配电终端从安全芯片读取序列号$N_s$，并返回给运维工具；运维工具向配电终端发送获取终端安全芯片公钥指令请求；

[0177] 读取子单元，用于配电终端从安全芯片读取公钥$K_t$，并返回给运维工具；

[0178] 字符串生成子单元，用于运维工具生成包含$N_t$、$N_s$和$K_t$信息的证书请求字符串A，并将A发送给终端；

[0179] 回执子单元，用于配电终端对A签名得到签名结果$S_a$，并将$S_a$返回给运维工具；运维工具根据$N_t$、$N_s$、$K_t$、$S_a$和终端使用单位名称生成用于终端证书申请文件；

[0180] 所述交互单元包括：

[0181] 加密子单元，用于运维工具与主站身份认证成功后，采用现场运维数据保护加密密钥对发送的运维数据报文$M_{fm}$进行加密，并以$IV_0$为MAC初始向量，计算消息认证码，得到{密文$E_{fm}$+$MAC_{fm}$}，并将其发送给主站；

[0182] 解密子单元，用于主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护解密密钥进行分散，并对{$E_{fm}$+$MAC_{fm}$}进行验证消息认证码和解密操作，获取明文报文数据；

[0183] 密钥分散子单元，用于主站将运维工具ID作为分散因子，对配电加密认证装置中的现场运维数据保护加密密钥进行分散，并对发送的运维数据报文$M_{mf}$进行加密；并以$IV_0$为消息认证码初始向量计算消息认证码得到{密文$E_{mf}$+$MAC_{mf}$}，将其发送给运维工具；

[0184] 明文报文数据获取子单元，用于运维工具采用现场运维数据保护解密密钥对{$E_{mf}$+$MAC_{mf}$}进行验证消息认证码和解密操作，获取明文报文数据。

[0185] 更新模块包括：更新单元和测试证书导入单元；

[0186] 其中，所述测试证书导入单元，用于运维工具将正式用数字证书以明文形式发送给配电终端，所述配电终端将数字证书下载到配电终端的安全芯片中，并向运维工具返回证书更新结果；

[0187] 所述更新单元包括：

[0188] 第一签名结果获取子单元，用于配电终端收到所述终端安全芯片序列号获取指令，返回安全芯片序列号$N_s$；运维工具向配电终端发送密钥版本号获取指令；配电终端从安全芯片内读取对称密钥版本号$V_1$，获取随机数$R_3$，返回给运维工具；运维工具对{$N_s$+$V_1$+$R_3$}签名获得签名结果$S_{rk}$，并将{$N_s$+$V_1$+$R_3$+$S_{rk}$+签名密钥标识$I_f$}发送给主站；

[0189] 验证子单元，用于主站通过运维工具数字证书验证签名的有效性，若验证通过，根据密钥版本号$V_1$判断从加密认证装置中导出的对称密钥的版本号；

[0190] 第二签名结果获取子单元，用于主站将终端随机数$R_3$作为计算消息认证码的初始向量，将终端安全芯片序列号$N_s$作为分散因子对$V_1$版本的主控密钥进行分散得到保护传输密钥，分散导出指定版本的对称密钥$P_k$；并基于SM2算法，利用主站私钥对$P_k$签名，获得签名结果$S_k$，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}经所述运维工具发送给配电终端；

[0191] 返回子单元，用于配电终端接收到密钥恢复报文后，将{签名密钥标识$I_{ask}$+$P_k$+$S_k$}发送到安全芯片，完成对称密钥的更新，并向运维工具返回更新结果信息。

[0192] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0193] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0194] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0195] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0196] 最后应当说明的是：以上实施例仅用以说明本申请的技术方案而非对其保护范围的限制，尽管参照上述实施例对本申请进行了详细的说明，所属领域的普通技术人员应当理解：本领域技术人员阅读本申请后依然可对申请的具体实施方式进行种种变更、修改或者等同替换，这些变更、修改或者等同替换，其均在其申请待批的权利要求范围之内。

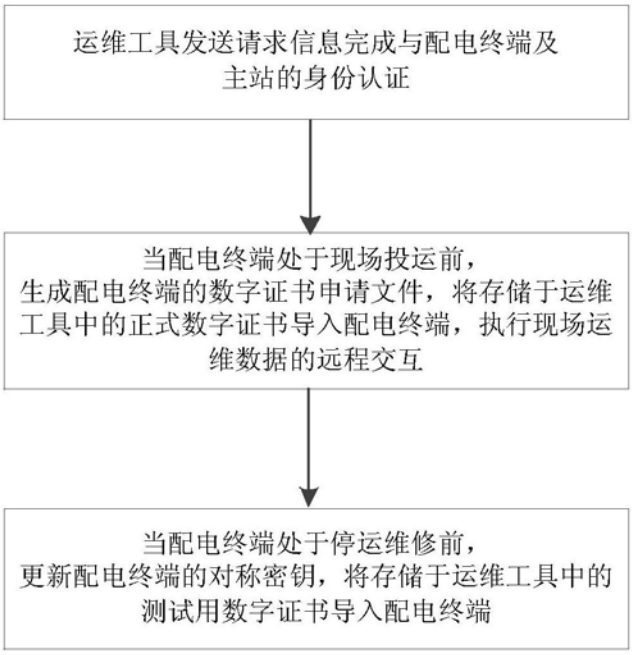

运维工具发送请求信息完成与配电终端及主站的身份认证
当配电终端处于现场投运前，生成配电终端的数字证书申请文件，将存储于运维工具中的正式数字证书导入配电终端，执行现场运维数据的远程交互
当配电终端处于停运维修前，更新配电终端的对称密钥，将存储于运维工具中的测试用数字证书导入配电终端

图1