

权利要求书

1. 一种初始配置方法，应用于终端设备，包括：

安全模块建立与证书授权 CA 服务器之间建立的安全通道；

通过所述安全通道获取会话密钥，并从 CA 服务器获取数字证书；

其中，所述安全模块用于实现全球用户识别模块 USIM 的功能。

2. 根据权利要求 1 所述的初始配置方法，其中，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，所述从 CA 服务器获取数字证书，包括：

安全模块生成进行 EC 申请的密码公私钥对；

利用所述密码公私钥对，从 ECA 服务器获取 EC。

3. 根据权利要求 1 所述的初始配置方法，其中，在所述 CA 服务器为注册证书权威机构 ECA 服务器时，所述数字证书为注册证书 EC，所述从 CA 服务器获取数字证书之后，还包括：

存储 EC。

4. 根据权利要求 1-3 任一项所述的初始配置方法，其中，在所述 CA 服务器为匿名证书权威机构 PCA 服务器时，所述数字证书为匿名证书 PC，所述从 CA 服务器获取数字证书，包括：

安全模块使用注册证书 EC 对应的私钥对 PC 申请消息进行签名；

根据 PC 申请消息，从 PCA 服务器获取 PC。

5. 根据权利要求 4 所述的初始配置方法，其中，所述从 PCA 服务器获取 PC，包括：

接收 PCA 服务器发送的反馈消息，并利用 PCA 服务器的公钥对接收的所述反馈消息进行验签，获取 PC。

6. 根据权利要求 4 所述的初始配置方法，其中，在所述从 PCA 服务器获取 PC 之后，还包括：

安全模块使用 PC 对应的私钥对 PC5 接口直连通信业务消息进行签名；

将签名后的 PC5 接口直连通信业务消息发送给外部设备。

7. 根据权利要求 1 所述的初始配置方法，其中，在所述 CA 服务器为注

册证书权威机构 ECA 服务器时, 所述数字证书为注册证书 EC, 在所述从 CA 服务器获取数字证书之后, 还包括:

发送 EC 给硬件安全模块 HSM;

HSM 进行 EC 的存储。

8. 根据权利要求 7 所述的初始配置方法, 其中, 所述从 CA 服务器获取数字证书, 还包括:

HSM 生成进行 EC 申请的密码公私钥对;

HSM 将进行 EC 申请的密码公钥发送给安全模块;

安全模块利用所述密码公钥, 从 ECA 服务器获取 EC。

9. 根据权利要求 1、7 或 8 所述的初始配置方法, 其中, 在所述 CA 服务器为匿名证书权威机构 PCA 服务器时, 所述数字证书为匿名证书 PC, 所述从 CA 服务器获取数字证书, 包括:

发送 PC 给硬件安全模块 HSM;

HSM 进行 PC 的存储。

10. 根据权利要求 9 所述的初始配置方法, 其中, 所述从 CA 服务器获取数字证书, 包括:

HSM 生成进行 PC 申请的密码公私钥对;

HSM 将进行 PC 申请的密码公钥发送给安全模块;

安全模块利用所述密码公钥, 从 PCA 服务器获取 PC。

11. 根据权利要求 9 所述的初始配置方法, 其中, 所述从 CA 服务器获取数字证书之后, 还包括:

安全模块使用 PC 对应的私钥对 PC5 接口直连通信业务消息进行签名;

将签名后的 PC5 接口直连通信业务消息发送给外部设备。

12. 根据权利要求 1 所述的初始配置方法, 其中, 所述安全模块与 CA 服务器之间采用基于通用集成电路卡 UICC 的通用引导架构 GBA 的方式建立 GBA 安全通道。

13. 一种终端设备, 包括:

安全模块, 用于建立与证书授权 CA 服务器之间建立的安全通道;

通过所述安全通道获取会话密钥, 并从 CA 服务器获取数字证书;

其中，所述安全模块用于实现全球用户识别模块 USIM 的功能。

14. 一种终端设备，包括收发机和处理器；

所述处理器，用于：

控制安全模块建立与证书授权 CA 服务器之间建立的安全通道；

通过所述安全通道获取会话密钥，并从 CA 服务器获取数字证书；

其中，所述安全模块用于实现全球用户识别模块 USIM 的功能。

15. 一种计算机可读存储介质，其上存储有计算机程序，其中，该程序被处理器执行时实现如权利要求 1-12 任一项所述的初始配置方法中的步骤。