(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103248490 A
(43)申请公布日 2013.08.14

(21)申请号 201310194144.0

(22)申请日 2013.05.23

(71)申请人 天地融科技股份有限公司
地址 100083 北京市海淀区学清路38号B座1810

(72)发明人 李东声

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

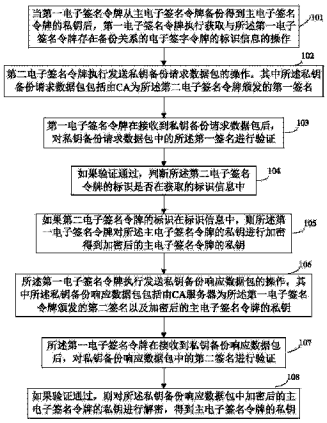
权利要求书5页 说明书14页 附图2页

(54)发明名称

一种备份电子签名令牌中信息的方法和系统

(57)摘要

本发明提供一种备份电子签名令牌中信息的方法和系统，所述方法包括：第一电子签名令牌执行获取标识信息的操作；第二电子签名令牌执行发送私钥备份请求数据包的操作；第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证；如果验证通过，判断第二电子签名令牌的标识是否在获取的标识信息中；如果在标识信息中，则第一电子签名令牌对主电子签名令牌的私钥进行加密；第一电子签名令牌执行发送私钥备份响应数据包的操作；第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证；如果验证通过，则对加密后的主电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥。



CN 103248490 A

1. 一种备份电子签名令牌中信息的方法，其特征在于，所述方法包括：

当第一电子签名令牌从主电子签名令牌备份得到主电子签名令牌的私钥后，第一电子签名令牌执行获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息的操作；

第二电子签名令牌执行发送私钥备份请求数据包的操作，其中所述私钥备份请求数据包包括由 CA 服务器为所述第二电子签名令牌颁发的第一签名；

第一电子签名令牌在接收到私钥备份请求数据包后，对私钥备份请求数据包中的所述第一签名进行验证；如果验证通过，判断所述第二电子签名令牌的标识是否在获取的标识信息中；如果所述第二电子签名令牌的标识在所述标识信息中，则所述第一电子签名令牌对所述主电子签名令牌的私钥进行加密，得到加密后的主电子签名令牌的私钥；

所述第一电子签名令牌执行发送私钥备份响应数据包的操作，其中所述私钥备份响应数据包包括由 CA 服务器为所述第一电子签名令牌颁发的第二签名以及加密后的主电子签名令牌的私钥；

所述第二电子签名令牌在接收到私钥备份响应数据包后，对私钥备份响应数据包中的第二签名进行验证；如果验证通过，则对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥。

2. 根据权利要求 1 所述的方法，其特征在于：

所述私钥备份响应数据包还包括所述第一电子签名令牌的标识；

所述第二电子签名令牌对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密之前，还包括：

所述第二电子签名令牌将所述私钥备份响应中的第一电子签名令牌的标识与本地存储的第二电子签名令牌对应的主电子签名令牌的标识进行比较；

如果第一电子签名令牌的标识与所述第二电子签名令牌对应的主电子签名令牌的标识相同，则执行对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密的操作。

3. 根据权利要求 1 所述的方法，其特征在于，第一电子签名令牌执行获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息的操作，包括：

所述第一电子签名令牌执行发送标识查询请求数据包的操作；

CA 服务器在接收到所述标识查询请求数据包后，获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息，并利用 CA 服务器私钥对所述标识信息进行签名，再执行通过标识查询响应数据包将签名处理后的标识信息发送给所述第一电子签名令牌的操作；

所述第一电子签名令牌对所述签名处理后的标识信息进行验证；如果验证通过，获取所述标识信息。

4. 根据权利要求 3 所述的方法，其特征在于，所述标识查询请求数据包包括所述第一电子签名令牌的第二签名；

所述 CA 服务器在接收到所述标识查询请求数据包之后，获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息之前，还包括：

所述 CA 服务器对所述第一电子签名令牌的第二签名进行验证；

如果验证通过，则所述 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

5. 根据权利要求 3 所述的方法，其特征在于：

所述第一电子签名令牌执行发送标识查询请求数据包的操作，包括：

所述第一电子签名令牌对标识查询请求数据包进行签名，并发送签名后的标识查询请求数据包；

所述 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息之前，还包括：

在接收到所述签名后的标识查询请求数据包后，所述 CA 服务器对签名后的标识查询请求数据包进行验证；

如果验证通过，则 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

6. 根据权利要求 3 所述的方法，其特征在于：

所述第二电子签名令牌执行发送私钥备份请求数据包的操作，包括：

所述第二电子签名令牌对私钥备份请求数据包进行签名，并发送签名处理后的私钥备份请求数据包；

所述第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证之前，还包括：

在接收到所述签名处理后的私钥备份请求数据包后，所述第一电子签名令牌对所述签名处理后的私钥备份请求数据包进行验证，如果验证通过，则第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证。

7. 根据权利要求 1 所述的方法，其特征在于：

所述第一电子签名令牌执行发送私钥备份响应数据包的操作，包括：

所述第一电子签名令牌对私钥备份响应数据包进行签名，并发送签名处理后的私钥备份响应数据包；

所述第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证之前，还包括：

在接收到所述签名处理后的私钥备份响应数据包后，所述第二电子签名令牌对签名处理后的私钥备份响应数据包进行验证，如果验证通过，则执行所述第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证的操作。

8. 根据权利要求 1 所述的方法，其特征在于：

所述第一电子签名令牌对所述主电子签名令牌的私钥进行加密得到加密后的主电子签名令牌的私钥，包括：

第一电子签名令牌和第二电子签名令牌获取匹配码；

第一电子签名令牌与第二电子签名令牌利用所述匹配码协商两者通信所使用的加密策略以及该加密策略对应的解密策略；

第一电子签名令牌利用所述加密策略对所述主电子签名令牌的私钥加密，得到加密后的主电子签名令牌的私钥；

其中，所述第二电子签名令牌对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥，包括：

所述第二电子签名令牌利用所述解密策略对所述加密后的主电子签名令牌的私钥进

行解密，得到所述主电子签名令牌的私钥。

9. 根据权利要求 8 所述的方法，其特征在于，第一电子签名令牌与第二电子签名令牌利用所述匹配码协商两者通信所使用的加密策略以及该加密策略对应的解密策略，包括：

将第二电子签名令牌获取到的匹配码作为待验证码，第二电子签名令牌执行发送该待验证码给第一电子签名令牌的操作；

第一电子签名令牌在获取到该待验证码后，判断所述待验证码与本地获取到的匹配码进行比较；

如果比较结果一致，则第一电子签名令牌生成两者通信所使用的加密策略以及该加密策略对应的解密策略；

第一电子签名令牌至少将解密策略发送给第二电子签名令牌。

10. 根据权利要求 8 所述的方法，其特征在于，第一电子签名令牌与第二电子签名令牌利用所述匹配码协商两者通信所使用的加密策略以及该加密策略对应的解密策略，包括：

第一电子签名令牌和第二电子签名令牌获取匹配码、加密策略和解密策略的对应关系；

第一电子签名令牌和第二电子签名令牌在所述对应关系中查找所述匹配码对应的加密策略和解密策略；

如果查找到，则将查找到的加密策略和解密策略作为两者通信所使用的加密策略以及该加密策略对应的解密策略。

11. 根据权利要求 1 所述的方法，其特征在于：

所述第一电子签名令牌对主电子签名令牌的私钥进行加密包括：

所述第一电子签名令牌获取密钥，该密钥与第一签名中存储的密钥相同，并利用密钥加密所述主电子签名令牌的私钥，得到加密后的主电子签名令牌的私钥；

所述第二电子签名令牌对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥，包括：

第一电子签名令牌从本地获取所述密钥，并利用所述密钥对加密后主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

12. 一种备份电子签名令牌中信息的系统，其特征在于，包括：

第一电子签名令牌中的第一获取模块，用于当第一电子签名令牌从主电子签名令牌备份得到主电子签名令牌的私钥后，执行获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息的操作；

第二电子签名令牌中的第一发送模块，用于执行发送私钥备份请求数据包的操作，其中所述私钥备份请求数据包包括由 CA 服务器为所述第二电子签名令牌颁发的第一签名；

所述第二电子签名令牌中的第一验证模块，用于在接收到私钥备份请求数据包后，对私钥备份请求数据包中的所述第一签名进行验证；

所述第一电子签名令牌中的判断模块，用于如果验证通过，判断所述第二电子签名令牌的标识是否在获取的标识信息中；

所述第一电子签名令牌中的加密模块，用于如果所述第二电子签名令牌的标识在所述标识信息中，则对所述主电子签名令牌的私钥进行加密，得到加密后的主电子签名令牌的私钥；

所述第一电子签名令牌中的第二发送模块，用于执行发送私钥备份响应数据包的操作，其中所述私钥备份响应数据包包括由 CA 服务器为所述第一电子签名令牌颁发的第二签名以及加密后的主电子签名令牌的私钥；

所述第一电子签名令牌中的第二验证模块，用于在接收到私钥备份响应数据包后，对私钥备份响应数据包中的第二签名进行验证；

所述第二电子签字令牌中的解密模块，用于如果验证通过，则对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥。

13. 根据权利要求 12 所述的系统，其特征在于：

所述私钥备份响应数据包还包括所述第一电子签名令牌的标识；

所述第二电子签名令牌还包括：

比较模块，用于将所述私钥备份响应中的第一电子签名令牌的标识与本地存储的第二电子签名令牌对应的主电子签名令牌的标识进行比较；如果第一电子签名令牌的标识与所述第二电子签名令牌对应的主电子签名令牌的标识相同，则执行对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密的操作。

14. 根据权利要求 12 所述的系统，其特征在于：

所述第一获取模块，用于执行发送标识查询请求数据包的操作；

所述系统还包括 CA 服务器，其中所述 CA 服务器包括：

第二获取模块，用于在接收到所述标识查询请求数据包后，获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息；

签名模块，用于利用 CA 服务器私钥对所述标识信息进行签名；

第三发送模块，用于执行通过标识查询响应数据包将签名处理后的标识信息发送给所述第一电子签名令牌的操作；

其中，所述第一获取模块还用于对所述签名处理后的标识信息进行验证；如果验证通过，获取所述标识信息。

15. 根据权利要求 14 所述的系统，其特征在于，所述标识查询请求数据包包括所述第一电子签名令牌的第二签名；

所述 CA 服务器还包括：

第三验证模块，用于对所述第一电子签名令牌的第二签名进行验证，如果验证通过，则所述 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

16. 根据权利要求 14 所述的系统，其特征在于：

所述第一获取模块，用于对标识查询请求数据包进行签名，并发送签名后的标识查询请求数据包；

所述 CA 服务器还包括：

第四验证模块，用于在接收到所述签名后的标识查询请求数据包后，所述 CA 服务器对签名后的标识查询请求数据包进行验证；如果验证通过，则 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

17. 根据权利要求 13 所述的系统，其特征在于：

所述第一发送模块，用于对私钥备份请求数据包进行签名，并发送签名处理后的私钥备份请求数据包；

所述第一电子签名令牌还包括：

第五验证模块，用于在接收到所述签名处理后的私钥备份请求数据包后，对所述签名处理后的私钥备份请求数据包进行验证，如果验证通过，则第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证。

18. 根据权利要求 12 所述的方法，其特征在于：

所述第二发送模块，用于对私钥备份响应数据包进行签名，并发送签名处理后的私钥备份响应数据包；

所述第二电子签名令牌对还包括：

第六验证模块，用于在接收到所述签名处理后的私钥备份响应数据包后，对签名处理后的私钥备份响应数据包进行验证，如果验证通过，则执行所述第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证的操作。

19. 根据权利要求 13 所述的系统，其特征在于：

第一电子签名令牌和第二电子签名令牌均包括：协商模块，用于获取匹配码，并利用所述匹配码协商两者通信所使用的加密策略以及该加密策略对应的解密策略；

其中，所述加密模块利用所述加密策略对所述主电子签名令牌的私钥加密，得到加密后的主电子签名令牌的私钥；

其中，所述解密模块利用所述解密策略对所述加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

20. 根据权利要求 19 所述的方法，其特征在于，第一电子签名令牌与第二电子签名令牌中的协商模块通过如下方式得到两者通信所使用的加密策略以及该加密策略对应的解密策略，包括：

将第二电子签名令牌获取到的匹配码作为待验证码，第二电子签名令牌执行发送该待验证码给第一电子签名令牌的操作；第一电子签名令牌在获取到该待验证码后，判断所述待验证码与本地获取到的匹配码进行比较；如果比较结果一致，则第一电子签名令牌生成两者通信所使用的加密策略以及该加密策略对应的解密策略；第一电子签名令牌至少将解密策略发送给第二电子签名令牌。

21. 根据权利要求 19 所述的方法，其特征在于，第一电子签名令牌与第二电子签名令牌中的协商模块通过如下方式得到两者通信所使用的加密策略以及该加密策略对应的解密策略，包括：

第一电子签名令牌和第二电子签名令牌获取匹配码、加密策略和解密策略的对应关系；第一电子签名令牌和第二电子签名令牌在所述对应关系中查找所述匹配码对应的加密策略和解密策略；如果查找到，则将查找到的加密策略和解密策略作为两者通信所使用的加密策略以及该加密策略对应的解密策略。

22. 根据权利要求 13 所述的系统，其特征在于：

所述加密模块，用于获取密钥，该密钥与第一签名中存储的密钥相同，并利用密钥加密所述主电子签名令牌的私钥，得到加密后的主电子签名令牌的私钥；

其中，所述解密模块，用于从本地获取所述密钥，并利用所述密钥对加密后主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

一种备份电子签名令牌中信息的方法和系统

技术领域

[0001] 本发明涉及一种电子技术领域，尤其涉及一种备份电子签名令牌中信息的方法和系统。

背景技术

[0002] 现有技术中，电子签名令牌中存储用户的私钥以及数字证书，利用USB Key内置的公钥算法实现对用户身份的认证。在现有的电子签名令牌中用户私钥理论上使用任何方式都无法读取，以保证了用户认证的安全性。然而，一旦电子签名令牌丢失，就无法得到原有的私钥，用户就必须重新办理电子签名令牌，私钥和序列号等关键信息都得重新分发和获取，需要触发电子签名令牌的更新流程，使得电子签名令牌的维护成本提高。即使有主电子签名令牌和备电子签名令牌，一旦主电子签名令牌丢失后，剩下的备电子签名令牌升级为主，那么如何对新的备电子签名令牌进行维护是亟待解决的问题。

发明内容

[0003] 本发明旨在解决上述问题 / 之一，提供一种备份电子签名令牌中信息的方法和系统。

[0004] 本发明提供如下技术方案：

[0005] 一种备份电子签名令牌中信息的方法，所述方法包括：当第一电子签名令牌从主电子签名令牌备份得到主电子签名令牌的私钥后，第一电子签名令牌执行获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息的操作；第二电子签名令牌执行发送私钥备份请求数据包的操作，其中所述私钥备份请求数据包包括由CA服务器为所述第二电子签名令牌颁发的第一签名；第一电子签名令牌在接收到私钥备份请求数据包后，对私钥备份请求数据包中的所述第一签名进行验证；如果验证通过，判断所述第二电子签名令牌的标识是否在获取的标识信息中；如果所述第二电子签名令牌的标识在所述标识信息中，则所述第一电子签名令牌对所述主电子签名令牌的私钥进行加密，得到加密后的主电子签名令牌的私钥；所述第一电子签名令牌执行发送私钥备份响应数据包的操作，其中所述私钥备份响应数据包包括由CA服务器为所述第一电子签名令牌颁发的第二签名以及加密后的主电子签名令牌的私钥；所述第二电子签名令牌在接收到私钥备份响应数据包后，对私钥备份响应数据包中的第二签名进行验证；如果验证通过，则对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥。

[0006] 其中，所述私钥备份响应数据包还包括所述第一电子签名令牌的标识；所述第二电子签名令牌对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密之前，还包括：所述第二电子签名令牌将所述私钥备份响应中的第一电子签名令牌的标识与本地存储的第二电子签名令牌对应的主电子签名令牌的标识进行比较；如果第一电子签名令牌的标识与所述第二电子签名令牌对应的主电子签名令牌的标识相同，则执行对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密的操作。

[0007] 其中，第一电子签名令牌执行获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息的操作，包括：所述第一电子签名令牌执行发送标识查询请求数据包的操作；CA 服务器在接收到所述标识查询请求数据包后，获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息，并利用 CA 服务器私钥对所述标识信息进行签名，再执行通过标识查询响应数据包将签名处理后的标识信息发送给所述第一电子签名令牌的操作；所述第一电子签名令牌对所述签名处理后的标识信息进行验证；如果验证通过，获取所述标识信息。

[0008] 其中，所述标识查询请求数据包包括所述第一电子签名令牌的第二签名；所述 CA 服务器在接收到所述标识查询请求数据包之后，获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息之前，还包括：所述 CA 服务器对所述第一电子签名令牌的第二签名进行验证；如果验证通过，则所述 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

[0009] 其中，所述第一电子签名令牌执行发送标识查询请求数据包的操作，包括：所述第一电子签名令牌对标识查询请求数据包进行签名，并发送签名后的标识查询请求数据包所述 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息之前，还包括：在接收到所述签名后的标识查询请求数据包后，所述 CA 服务器对签名后的标识查询请求数据包进行验证；如果验证通过，则 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

[0010] 其中，所述第二电子签名令牌执行发送私钥备份请求数据包的操作，包括：所述第二电子签名令牌对私钥备份请求数据包进行签名，并发送签名处理后的私钥备份请求数据包；所述第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证之前，还包括：在接收到所述签名处理后的私钥备份请求数据包后，所述第一电子签名令牌对所述签名处理后的私钥备份请求数据包进行验证，如果验证通过，则第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证。

[0011] 其中，所述第一电子签名令牌执行发送私钥备份响应数据包的操作，包括：所述第一电子签名令牌对私钥备份响应数据包进行签名，并发送签名处理后的私钥备份响应数据包；所述第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证之前，还包括：在接收到所述签名处理后的私钥备份响应数据包后，所述第二电子签名令牌对签名处理后的私钥备份响应数据包进行验证，如果验证通过，则执行所述第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证的操作。

[0012] 其中，所述第一电子签名令牌对所述主电子签名令牌的私钥进行加密得到加密后的主电子签名令牌的私钥，包括：第一电子签名令牌和第二电子签名令牌获取匹配码；第一电子签名令牌与第二电子签名令牌利用所述匹配码协商两者通信所使用的加密策略以及该加密策略对应的解密策略；第一电子签名令牌利用所述加密策略对所述主电子签名令牌的私钥加密，得到加密后的主电子签名令牌的私钥；所述第二电子签名令牌对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥，包括：所述第二电子签名令牌利用所述解密策略对所述加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

[0013] 其中，第一电子签名令牌与第二电子签名令牌利用所述匹配码协商两者通信所使

用的加密策略以及该加密策略对应的解密策略，包括：将第二电子签名令牌获取到的匹配码作为待验证码，第二电子签名令牌执行发送该待验证码给第一电子签名令牌的操作；第一电子签名令牌在获取到该待验证码后，判断所述待验证码与本地获取到的匹配码进行比较；如果比较结果一致，则第一电子签名令牌生成两者通信所使用的加密策略以及该加密策略对应的解密策略；第一电子签名令牌至少将解密策略发送给第二电子签名令牌。

[0014] 其中，第一电子签名令牌与第二电子签名令牌利用所述匹配码协商两者通信所使用的加密策略以及该加密策略对应的解密策略，包括：第一电子签名令牌和第二电子签名令牌获取匹配码、加密策略和解密策略的对应关系；第一电子签名令牌和第二电子签名令牌在所述对应关系中查找所述匹配码对应的加密策略和解密策略；如果查找到，则将查找到的加密策略和解密策略作为两者通信所使用的加密策略以及该加密策略对应的解密策略。

[0015] 其中，所述第一电子签名令牌对主电子签名令牌的私钥进行加密包括：所述第一电子签名令牌获取密钥，该密钥与第一签名中存储的密钥相同，并利用密钥加密所述主电子签名令牌的私钥，得到加密后的主电子签名令牌的私钥；所述第二电子签名令牌对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥，包括：第一电子签名令牌从本地获取所述密钥，并利用所述密钥对加密后主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

[0016] 一种备份电子签名令牌中信息的系统，包括：第一电子签名令牌中的第一获取模块，用于当第一电子签名令牌从主电子签名令牌备份得到主电子签名令牌的私钥后，执行获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息的操作；第二电子签名令牌中的第一发送模块，用于执行发送私钥备份请求数据包的操作，其中所述私钥备份请求数据包包括由 CA 服务器为所述第二电子签名令牌颁发的第一签名；所述第二电子签名令牌中的第一验证模块，用于在接收到私钥备份请求数据包后，对私钥备份请求数据包中的所述第一签名进行验证；所述第一电子签名令牌中的判断模块，用于如果验证通过，判断所述第二电子签名令牌的标识是否在获取的标识信息中；所述第一电子签名令牌中的加密模块，用于如果所述第二电子签名令牌的标识在所述标识信息中，则对所述主电子签名令牌的私钥进行加密，得到加密后的主电子签名令牌的私钥；所述第一电子签名令牌中的第二发送模块，用于执行发送私钥备份响应数据包的操作，其中所述私钥备份响应数据包包括由 CA 服务器为所述第一电子签名令牌颁发的第二签名以及加密后的主电子签名令牌的私钥；

[0017] 所述第一电子签名令牌中的第二验证模块，用于在接收到私钥备份响应数据包后，对私钥备份响应数据包中的第二签名进行验证；

[0018] 所述第二电子签字令牌中的解密模块，用于如果验证通过，则对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥。

[0019] 其中，所述私钥备份响应数据包还包括所述第一电子签名令牌的标识；所述第二电子签名令牌还包括：比较模块，用于将所述私钥备份响应中的第一电子签名令牌的标识与本地存储的第二电子签名令牌对应的主电子签名令牌的标识进行比较；如果第一电子签名令牌的标识与所述第二电子签名令牌对应的主电子签名令牌的标识相同，则执行对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密的操作。

[0020] 其中，所述第一获取模块，用于执行发送标识查询请求数据包的操作；所述系统还包括 CA 服务器，其中所述 CA 服务器包括：第二获取模块，用于在接收到所述标识查询请求数据包后，获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息；签名模块，用于利用 CA 服务器私钥对所述标识信息进行签名；第三发送模块，用于执行通过标识查询响应数据包将签名处理后的标识信息发送给所述第一电子签名令牌的操作；其中，所述第一获取模块还用于对所述签名处理后的标识信息进行验证；如果验证通过，获取所述标识信息。

[0021] 其中，所述标识查询请求数据包包括所述第一电子签名令牌的第二签名；所述 CA 服务器还包括：第三验证模块，用于对所述第一电子签名令牌的第二签名进行验证，如果验证通过，则所述 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

[0022] 其中，所述第一获取模块，用于对标识查询请求数据包进行签名，并发送签名后的标识查询请求数据包；所述 CA 服务器还包括：第四验证模块，用于在接收到所述签名后的标识查询请求数据包后，所述 CA 服务器对签名后的标识查询请求数据包进行验证；如果验证通过，则 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

[0023] 其中，所述第一发送模块，用于对私钥备份请求数据包进行签名，并发送签名处理后的私钥备份请求数据包；所述第一电子签名令牌还包括：第五验证模块，用于在接收到所述签名处理后的私钥备份请求数据包后，对所述签名处理后的私钥备份请求数据包进行验证，如果验证通过，则第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证。

[0024] 其中，所述第二发送模块，用于对私钥备份响应数据包进行签名，并发送签名处理后的私钥备份响应数据包；所述第二电子签名令牌还包括：

[0025] 第六验证模块，用于在接收到所述签名处理后的私钥备份响应数据包后，对签名处理后的私钥备份响应数据包进行验证，如果验证通过，则执行所述第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证的操作。

[0026] 其中，第一电子签名令牌和第二电子签名令牌均包括：协商模块，用于获取匹配码，并利用所述匹配码协商两者通信所使用的加密策略以及该加密策略对应的解密策略；其中，所述加密模块利用所述加密策略对所述主电子签名令牌的私钥加密，得到加密后的主电子签名令牌的私钥；其中，所述解密模块利用所述解密策略对所述加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

[0027] 其中，第一电子签名令牌与第二电子签名令牌中的协商模块通过如下方式得到两者通信所使用的加密策略以及该加密策略对应的解密策略，包括：将第二电子签名令牌获取到的匹配码作为待验证码，第二电子签名令牌执行发送该待验证码给第一电子签名令牌的操作；第一电子签名令牌在获取到该待验证码后，判断所述待验证码与本地获取到的匹配码进行比较；如果比较结果一致，则第一电子签名令牌生成两者通信所使用的加密策略以及该加密策略对应的解密策略；第一电子签名令牌至少将解密策略发送给第二电子签名令牌。

[0028] 其中，第一电子签名令牌与第二电子签名令牌中的协商模块通过如下方式得到两者通信所使用的加密策略以及该加密策略对应的解密策略，包括：第一电子签名令牌和第

二电子签名令牌获取匹配码、加密策略和解密策略的对应关系；第一电子签名令牌和第二电子签名令牌在所述对应关系中查找所述匹配码对应的加密策略和解密策略；如果查找到，则将查找到的加密策略和解密策略作为两者通信所使用的加密策略以及该加密策略对应的解密策略。

[0029] 其中，所述加密模块，用于获取密钥，该密钥与第一签名中存储的密钥相同，并利用密钥加密所述主电子签名令牌的私钥，得到加密后的主电子签名令牌的私钥；其中，所述解密模块，用于从本地获取所述密钥，并利用所述密钥对加密后主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

[0030] 与现有技术相比，第一电子签名令牌获取与自身存储在备份关系的电子签名令牌的标识信息，并在接收到第二电子签名令牌发送的私钥备份请求数据包时，第二电子签名令牌对第一签名进行验证，以确定第二电子签名令牌是否是合法设备，再通过判断第二电子签名令牌是否在标识信息中，以确定第一电子签名令牌和第二电子签名令牌之间是否存在主备关系，在上述两个条件都满足时，第一电子签名令牌再将主电子签名令牌的私钥加密，再将加密后主电子签名令牌的私钥通过私钥备份响应数据包发送出去，在第二电子签名令牌接收到私钥备份响应数据包后，第二电子签名令牌对第二签名进行验证，以确定第一电子签名令牌是否是合法设备，在确定合法户，第二电子签名令牌再将加密后的第二电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥，完成私钥的备份。通过第二电子签名令牌和第一电子签名令牌分别验证对方的合法性，以及第一电子签名令牌验证主备关系，在确定对方安全的前提下，再进行私钥的传输，实现了安全备份私钥。

附图说明

[0031] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述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，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他附图。

[0032] 图 1 为本发明实施例提供的备份电子签名令牌中信息的方法实施例的流程示意图；

[0033] 图 2 为本发明实施例提供的备份电子签名令牌中信息的系统实施例的结构示意图。

具体实施方式

[0034] 下面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，显然，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，都属于本发明的保护范围。

[0035] 在本发明的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发

明的限制。此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或数量或位置。

[0036] 在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。

[0037] 下面将结合附图对本发明实施例作进一步地详细描述。

[0038] 图 1 为本发明提供的备份电子签名令牌中信息的方法实施例的流程示意图。图 1 所示方法实施例包括：

[0039] 步骤 101、当第一电子签名令牌从主电子签名令牌备份得到主电子签名令牌的私钥后，第一电子签名令牌执行获取第二电子签名令牌的标识信息的操作；

[0040] 步骤 102、第二电子签名令牌执行发送私钥备份请求数据包的操作，其中所述私钥备份请求数据包包括由 CA（Certificate Authority，证书授证）服务器为所述第二电子签名令牌颁发的第一签名；

[0041] 步骤 103、第一电子签名令牌在接收到私钥备份请求数据包后，对私钥备份请求数据包中的所述第一签名进行验证；

[0042] 步骤 104、如果验证通过，判断所述第二电子签名令牌的标识是否在获取的标识信息中；如果所述第二电子签名令牌的标识在所述标识信息中；

[0043] 步骤 105、如果第二电子签名令牌的标识在标识信息中，则所述第一电子签名令牌对所述主电子签名令牌的私钥进行加密得到加密后的主电子签名令牌的私钥；

[0044] 步骤 106、所述第一电子签名令牌执行发送私钥备份响应数据包的操作，其中所述私钥备份响应数据包包括由 CA 服务器为所述第一电子签名令牌颁发的第二签名以及加密后的主电子签名令牌的私钥；

[0045] 步骤 107、所述第一电子签名令牌在接收到私钥备份响应数据包后，对私钥备份响应数据包中的第二签名进行验证；

[0046] 步骤 108、如果验证通过，则对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥。

[0047] 与现有技术相比，第一电子签名令牌获取与自身存储在备份关系的电子签名令牌的标识信息，并在接收到第二电子签名令牌发送的私钥备份请求数据包时，第二电子签名令牌对第一签名进行验证，以确定第二电子签名令牌是否是合法设备，再通过判断第二电子签名令牌是否在标识信息中，以确定第一电子签名令牌和第二电子签名令牌之间是否存在主备关系，在上述两个条件都满足时，第一电子签名令牌再将主电子签名令牌的私钥加密，再将加密后主电子签名令牌的私钥通过私钥备份响应数据包发送出去，在第二电子签名令牌接收到私钥备份响应数据包后，第二电子签名令牌对第二签名进行验证，以确定第一电子签名令牌是否是合法设备，在确定合法户，第二电子签名令牌再将加密后的第二电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥，完成私钥的备份。通过第二电子签名令牌和第一电子签名令牌分别验证对方的合法性，以及第一电子签名令牌验证主备关系，在确定对方安全的前提下，再进行私钥的传输，实现了安全备份私钥。

[0048] 下面对本发明提供的方法实施例作进一步的说明：

[0049] 可选的，所述私钥备份响应数据包还包括所述第一电子签名令牌的标识；

[0050] 所述第二电子签名令牌对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密之前，还包括：

[0051] 所述第二电子签名令牌将所述私钥备份响应中的第一电子签名令牌的标识与本地存储的第二电子签名令牌对应的主电子签名令牌的标识进行比较；

[0052] 如果第一电子签名令牌的标识与所述第二电子签名令牌对应的主电子签名令牌的标识相同，则执行对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密的操作。

[0053] 由上可以看出，第二电子签名令牌通过判断第一电子签名令牌的标识与自身的主电子签名令牌的标识进行比较，可以确定第一电子签名令牌和第二电子签名令牌之间是否存在主备关系，保证自身的私钥备份安全。

[0054] 其中，第一电子签名令牌执行向 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息的操作，包括：

[0055] 所述第一电子签名令牌执行发送标识查询请求数据包的操作；

[0056] CA 服务器在接收到所述标识查询请求数据包后，获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息，并利用 CA 服务器私钥对所述标识信息进行签名，再通过标识查询响应数据包将签名处理后的标识信息发送给所述第一电子签名令牌；

[0057] 所述第一电子签名令牌对所述签名处理后的标识信息进行验证；如果验证通过，获取所述标识。

[0058] 与现有技术中通过用户手动输入该标识信息等方式相比，本发明实施例中标识信息是通过 CA 服务器来获取，且利用 CA 服务器私钥对标识信息进行签名，准确性和安全性高。

[0059] 其中，标识查询请求数据包包括所述第一电子签名令牌的第二签名；

[0060] 所述 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息之前，还包括：

[0061] 所述 CA 服务器对所述第一电子签名令牌的第二签名进行验证；

[0062] 如果验证通过，则所述 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

[0063] 由上可以看出，CA 服务器利用 CA 服务器公钥验证第一电子签名令牌的第一签名通过，表示该第一电子签名令牌为合法设备，再获取该标识信息，避免非法电子签名令牌骗取该标识信息，提高信息的安全性。

[0064] 进一步的，为了避免其他电子签名令牌窃取到第一电子签名令牌的第二签名后进而从 CA 服务器骗取标识信息，所述第一电子签名令牌执行发送标识查询请求数据包的操作，包括：

[0065] 所述第一电子签名令牌对标识查询请求数据包进行签名，并发送签名后的标识查询请求数据包；

[0066] 其中，此处签名使用的是第一电子签名令牌与 CA 服务器协商确定的两者通信过程中第一电子签名令牌在签名时所使用的私钥；

[0067] 相应的，所述 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息之前，还包括：

[0068] 所述 CA 服务器对签名后的标识查询请求数据包进行验证；

[0069] 如果验证通过，则 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

[0070] 其中，CA 服务器验证签名所使用的是第一电子签名令牌与 CA 服务器协商确定的两者通信过程中第一电子签名令牌签名时所使用的私钥对应的公钥。

[0071] 为了避免合法的电子签名令牌在获取到第一签名后，冒充真正的第二电子签名令牌骗取主电子签名令牌的私钥，造成私钥泄漏的安全，上述方法流程中：

[0072] 所述第二电子签名令牌执行发送私钥备份请求数据包的操作，包括：

[0073] 所述第二电子签名令牌对私钥备份请求数据包进行签名，并发送签名处理后的私钥备份请求数据包；

[0074] 所述第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证之前，还包括：

[0075] 所述第一电子签名令牌对所述签名处理后的私钥备份请求数据包进行验证，如果验证通过，则第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证。

[0076] 由上可以看出，通过第二电子签名令牌对私钥备份请求数据包进行签名，再由第一电子签名令牌对私钥备份请求数据包进行验证，实现对发起备份请求的第二电子签名令牌的身份认证，使得具有第一签名的电子签名令牌无法骗取到主电子签名令牌的私钥，提高私钥备份的安全性。

[0077] 其中，私钥备份请求数据包的签名所使用的私钥以及第一电子签名令牌验证签名后的私钥备份请求数据包所使用的公钥是预先协商好的，且分别写入到的各自的设备中的。

[0078] 同理，为了避免合法的电子签名令牌在获取到第二签名后，冒充真正的第一电子签名令牌发送错误的私钥给第二电子签名令牌，造成私钥备份失败的问题，上述方法流程中：

[0079] 所述第一电子签名令牌执行发送私钥备份响应数据包的操作，包括：

[0080] 所述第一电子签名令牌对私钥备份响应数据包进行签名，并发送签名处理后的私钥备份响应数据包；

[0081] 所述第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证之前，还包括：

[0082] 所述第二电子签名令牌对签名处理后的私钥备份响应数据包进行验证，如果验证通过，则执行所述第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证的操作。

[0083] 由上可以看出，通过第一电子签名令牌对私钥备份响应数据包进行签名，再由第二电子签名令牌对私钥备份响应数据包进行验证，实现对发起备份响应的第一电子签名令牌的身份认证，使得具有第二签名的合法电子签名令牌无法妨碍第二电子签名令牌获取正确的私钥，保证第二电子签名令牌能够备份得到正确的私钥。

[0084] 其中，私钥备份请求数据包的签名所使用的私钥以及第二电子签名令牌验证签名

后的私钥备份请求数据包所使用的公钥是预先协商好的，且分别写入到的各自的设备中的。

[0085] 其中，第一电子签名令牌对主电子签名令牌的私钥进行加密有如下两种方式，具体包括：

[0086] 方式一：第一电子签名令牌和第二电子签名令牌获取匹配码，第一电子签名令牌与第二电子签名令牌利用所述匹配码协商两者通信所使用的加密策略以及该加密策略对应的解密策略；第一电子签名令牌利用所述加密策略对所述主电子签名令牌的私钥加密，得到加密后的主电子签名令牌的私钥；

[0087] 其中，所述第二电子签名令牌对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥，包括：所述第二电子签名令牌利用所述解密策略对所述加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

[0088] 方式二：第一电子签名令牌获取密钥，该密钥与第二电子签名令牌的数字签名中存储的密钥相同，并利用密钥加密所述主电子签名令牌的私钥，得到加密后的主电子签名令牌的私钥；

[0089] 相应的，所述第二电子签名令牌对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥，包括：第一电子签名令牌对私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥。

[0090] 下面要对方式一作进一步说明：

[0091] 第二电子签名令牌可以根据本地预先存储的匹配码生成策略生成匹配码，该匹配码可以包括文字、数字和字符中的至少一个，并输出该匹配码；当然，第一电子签名令牌获取该匹配码，其中获取的方式有很多种，如通过无线或有线传输方式，也可以通过用户手动输入方式。当然，也可以由银行后台服务器向第二电子签名令牌和第一电子签名令牌发送该匹配码等方式实现第二电子签名令牌和第一电子签名令牌得到匹配码。

[0092] 相比较而言，由第二电子签名令牌生成匹配码，再由第一电子签名令牌获取的方式，较银行后台服务器发送的方式相比，无需银行后台服务器的参与，交互流程简单。

[0093] 其中，利用匹配码协商加解密策略有如下两种，包括：

[0094] A1：将第一电子签名令牌获取到的匹配码作为待验证码，第一电子签名令牌执行发送该待验证码给第二电子签名令牌的操作；第二电子签名令牌在获取到该待验证码后，判断待验证码与本地获取到的匹配码是否相同；如果待验证码与匹配码相同，，则第二电子签名令牌生成两者通信所使用的加密策略以及该加密策略对应的解密策略；第二电子签名令牌执行发送解密策略给第一电子签名令牌的操作。

[0095] 由上可以看出，方式一提供的方式中，第二电子签名令牌通过将待验证码与本地获取到的匹配码进行比较，确定发起与第二电子签名令牌协商加解密策略的设备是否为第一电子签名令牌，来验证第一电子签名令牌的身份，在确定该设备为第一电子签名令牌，再将解密算法发送给第一电子签名令牌，保证了私钥的传输安全。

[0096] 在 A1 中，为了避免其他电子签名令牌窃取该私钥的加密策略，第一电子签名令牌执行发送该待验证码给第二电子签名令牌的操作，包括：

[0097] 第一电子签名令牌对该待验证码进行签名，发签名处理后的待验证码给第二电子签名令牌；

[0098] 相应的，第二电子签名令牌判断待验证码与本地获取到的匹配码是否相同之前，还包括：

[0099] 第二电子签名令牌对签名处理后的待验证码给第二电子签名令牌进行验证，如果验证通过，再判断待验证码与本地获取到的匹配码是否相同。

[0100] 其中，第一电子签名令牌对待验证码进行签名所使用的私钥可以与第一电子签名令牌对私钥备份请求数据包签名时所使用的私钥相同，同理，第二电子签名令牌对签名后的待验证码验证时所使用的公钥与对签名后的私钥备份请求数据包时所使用的公钥相同。

[0101] 为了避免其他电子签名令牌冒充第二电子签名令牌发送错误的解密算法给第一电子签名令牌，第二电子签名令牌执行发送解密策略给第一电子签名令牌的操作，包括：

[0102] 第二电子签名令牌对解密策略进行签名，发签名处理后的解密策略给第一电子签名令牌；

[0103] 相应的，第一电子签名令牌获取解密策略之前还包括：

[0104] 第一电子签名令牌对签名处理后的解密策略进行验证，如果验证通过，则获取解密策略。

[0105] 其中，第二电子签名令牌对解密策略进行签名所使用的私钥可以与第二电子签名令牌对私钥备份响应数据包签名时所使用的私钥相同，同理，第一电子签名令牌对签名后的解密策略验证时所使用的公钥与对签名后的私钥备份响应数据包时所使用的公钥相同。

[0106] A2：第二电子签名令牌和第一电子签名令牌获取匹配码、加密策略和解密策略的对应关系；第二电子签名令牌和第一电子签名令牌在对应关系中查找匹配码对应的加密策略和解密策略；如果查找到，则将查找到的加密策略和解密策略作为两者通信所使用的加密策略以及该加密策略对应的解密策略。

[0107] 在 A2 中，第二电子签名令牌和第一电子签名令牌通过查询本地获取到的对应关系，确定两者通信所使用的加解密策略，实现简单，且无需第二电子签名令牌和第一电子签名令牌之间信息交互，降低了信息被窃取的可能。

[0108] 上述两种方式通过匹配码可以实现随机选择加解密策略的目的，提高了加密方式的随机性，保证了通信安全。

[0109] 综上，本发明中的第一电子签名令牌预先存储有与第二电子签名令牌通信时对内容进行签名的私钥、对第二电子签名令牌发送的经签名后的内容进行验签时所使用的第二电子签名令牌用于通信的公钥，以及自身加解密内容的一对密钥；而第二电子签名令牌预先存储有与第一电子签名令牌通信时对内容进行签名的私钥、对第一电子签名令牌发送的经签名后的内容进行验签时所使用的第一电子签名令牌用于通信的公钥以及第一电子签名令牌请求备份的私钥；除此之外，第一电子签名令牌还存储有与 CA 服务器进行通信时对内容进行签名的私钥，相应的，CA 服务器存储有与第一电子签名令牌通信时对签名内容进行验证所使用的公钥。

[0110] 图 2 为本发明提供的备份电子签名令牌中信息的系统实施例的结构示意图。图 2 所示系统实施例包括：

[0111] 第一电子签名令牌中的第一获取模块 201，用于当第一电子签名令牌从主电子签

名令牌备份得到主电子签名令牌的私钥后，执行获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息的操作；

[0112] 第二电子签名令牌中的第一发送模块202，用于执行发送私钥备份请求数据包的操作，其中所述私钥备份请求数据包包括由CA服务器为所述第二电子签名令牌颁发的第一签名；

[0113] 所述第二电子签名令牌中的第一验证模块203，用于在接收到私钥备份请求数据包后，对私钥备份请求数据包中的所述第一签名进行验证；

[0114] 所述第一电子签名令牌中的判断模块204，用于如果验证通过，判断所述第二电子签名令牌的标识是否在获取的标识信息中；

[0115] 所述第一电子签名令牌中的加密模块205，用于如果所述第二电子签名令牌的标识在所述标识信息中，则对所述主电子签名令牌的私钥进行加密，得到加密后的主电子签名令牌的私钥；

[0116] 所述第一电子签名令牌中的第二发送模块206，用于执行发送私钥备份响应数据包的操作，其中所述私钥备份响应数据包包括由CA服务器为所述第一电子签名令牌颁发的第二签名以及加密后的主电子签名令牌的私钥；

[0117] 所述第一电子签名令牌中的第二验证模块207，用于在接收到私钥备份响应数据包后，对私钥备份响应数据包中的第二签名进行验证；

[0118] 所述第二电子签字令牌中的解密模块208，用于如果验证通过，则对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥。

[0119] 其中，所述私钥备份响应数据包还包括所述第一电子签名令牌的标识；

[0120] 所述第二电子签名令牌还包括：

[0121] 比较模块，用于将所述私钥备份响应中的第一电子签名令牌的标识与本地存储的第二电子签名令牌对应的主电子签名令牌的标识进行比较；如果第一电子签名令牌的标识与所述第二电子签名令牌对应的主电子签名令牌的标识相同，则执行对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密的操作。

[0122] 其中，所述第一获取模块，用于执行发送标识查询请求数据包的操作；

[0123] 所述系统还包括CA服务器，其中所述CA服务器包括：

[0124] 第二获取模块，用于在接收到所述标识查询请求数据包后，获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息；

[0125] 签名模块，用于利用CA服务器私钥对所述标识信息进行签名；

[0126] 第三发送模块，用于执行通过标识查询响应数据包将签名处理后的标识信息发送给所述第一电子签名令牌的操作；

[0127] 其中，所述第一获取模块还用于对所述签名处理后的标识信息进行验证；如果验证通过，获取所述标识信息。

[0128] 其中，所述标识查询请求数据包包括所述第一电子签名令牌的第二签名；

[0129] 所述CA服务器还包括：

[0130] 第三验证模块，用于对所述第一电子签名令牌的第二签名进行验证，如果验证通过，则所述CA服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

[0131] 其中，所述第一获取模块，用于对标识查询请求数据包进行签名，并发送签名后的标识查询请求数据包；

[0132] 所述 CA 服务器还包括：

[0133] 第四验证模块，用于在接收到所述签名后的标识查询请求数据包后，所述 CA 服务器对签名后的标识查询请求数据包进行验证；如果验证通过，则 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

[0134] 其中，所述第一获取模块，用于对标识查询请求数据包进行签名，并发送签名后的标识查询请求数据包；

[0135] 所述 CA 服务器还包括：

[0136] 第四验证模块，用于在接收到所述签名后的标识查询请求数据包后，所述 CA 服务器对签名后的标识查询请求数据包进行验证；如果验证通过，则 CA 服务器获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息。

[0137] 其中，所述第一发送模块，用于对私钥备份请求数据包进行签名，并发送签名处理后的私钥备份请求数据包；

[0138] 所述第一电子签名令牌还包括：

[0139] 第五验证模块，用于在接收到所述签名处理后的私钥备份请求数据包后，对所述签名处理后的私钥备份请求数据包进行验证，如果验证通过，则第一电子签名令牌对私钥备份请求数据包中的第一签名进行验证。

[0140] 其中，所述第二发送模块，用于对私钥备份响应数据包进行签名，并发送签名处理后的私钥备份响应数据包；

[0141] 所述第二电子签名令牌还包括：

[0142] 第六验证模块，用于在接收到所述签名处理后的私钥备份响应数据包后，对签名处理后的私钥备份响应数据包进行验证，如果验证通过，则执行所述第二电子签名令牌对私钥备份响应数据包中的第二签名进行验证的操作。

[0143] 其中，第一电子签名令牌和第二电子签名令牌均包括：协商模块，用于获取匹配码，并利用所述匹配码协商两者通信所使用的加密策略以及该加密策略对应的解密策略；

[0144] 其中，所述加密模块利用所述加密策略对所述主电子签名令牌的私钥加密，得到加密后的主电子签名令牌的私钥；所述解密模块利用所述解密策略对所述加密后的主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

[0145] 其中，第一电子签名令牌与第二电子签名令牌中的协商模块通过如下方式得到两者通信所使用的加密策略以及该加密策略对应的解密策略，包括：

[0146] 将第二电子签名令牌获取到的匹配码作为待验证码，第二电子签名令牌执行发送该待验证码给第一电子签名令牌的操作；第一电子签名令牌在获取到该待验证码后，判断所述待验证码与本地获取到的匹配码进行比较；如果比较结果一致，则第一电子签名令牌生成两者通信所使用的加密策略以及该加密策略对应的解密策略；第一电子签名令牌至少将解密策略发送给第二电子签名令牌。

[0147] 其中，第一电子签名令牌与第二电子签名令牌中的协商模块通过如下方式得到两者通信所使用的加密策略以及该加密策略对应的解密策略，包括：

[0148] 第一电子签名令牌和第二电子签名令牌获取匹配码、加密策略和解密策略的对应

关系；第一电子签名令牌和第二电子签名令牌在所述对应关系中查找所述匹配码对应的加密策略和解密策略；如果查找到，则将查找到的加密策略和解密策略作为两者通信所使用的加密策略以及该加密策略对应的解密策略。

[0149] 其中，所述加密模块，用于获取密钥，该密钥与第一签名中存储的密钥相同，并利用密钥加密所述主电子签名令牌的私钥，得到加密后的主电子签名令牌的私钥；

[0150] 其中，所述解密模块，用于从本地获取所述密钥，并利用所述密钥对加密后主电子签名令牌的私钥进行解密，得到所述主电子签名令牌的私钥。

[0151] 与现有技术相比，第一电子签名令牌获取与自身存储在备份关系的电子签名令牌的标识信息，并在接收到第二电子签名令牌发送的私钥备份请求数据包时，第二电子签名令牌对第一签名进行验证，以确定第二电子签名令牌是否是合法设备，再通过判断第二电子签名令牌是否在标识信息中，以确定第一电子签名令牌和第二电子签名令牌之间是否存在主备关系，在上述两个条件都满足时，第一电子签名令牌再将主电子签名令牌的私钥加密，再将加密后主电子签名令牌的私钥通过私钥备份响应数据包发送出去，在第二电子签名令牌接收到私钥备份响应数据包后，第二电子签名令牌对第二签名进行验证，以确定第一电子签名令牌是否是合法设备，在确定合法户，第二电子签名令牌再将加密后的第二电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥，完成私钥的备份。通过第二电子签名令牌和第一电子签名令牌分别验证对方的合法性，以及第一电子签名令牌验证主备关系，在确定对方安全的前提下，再进行私钥的传输，实现了安全备份私钥。

[0152] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0153] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0154] 本技术领域的普通技术人员可以理解实现上述实施例方法携带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种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0155] 此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。

[0156] 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0157] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示

例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0158] 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在不脱离本发明的原理和宗旨的情况下在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。本发明的范围由所附权利要求及其等同限定。

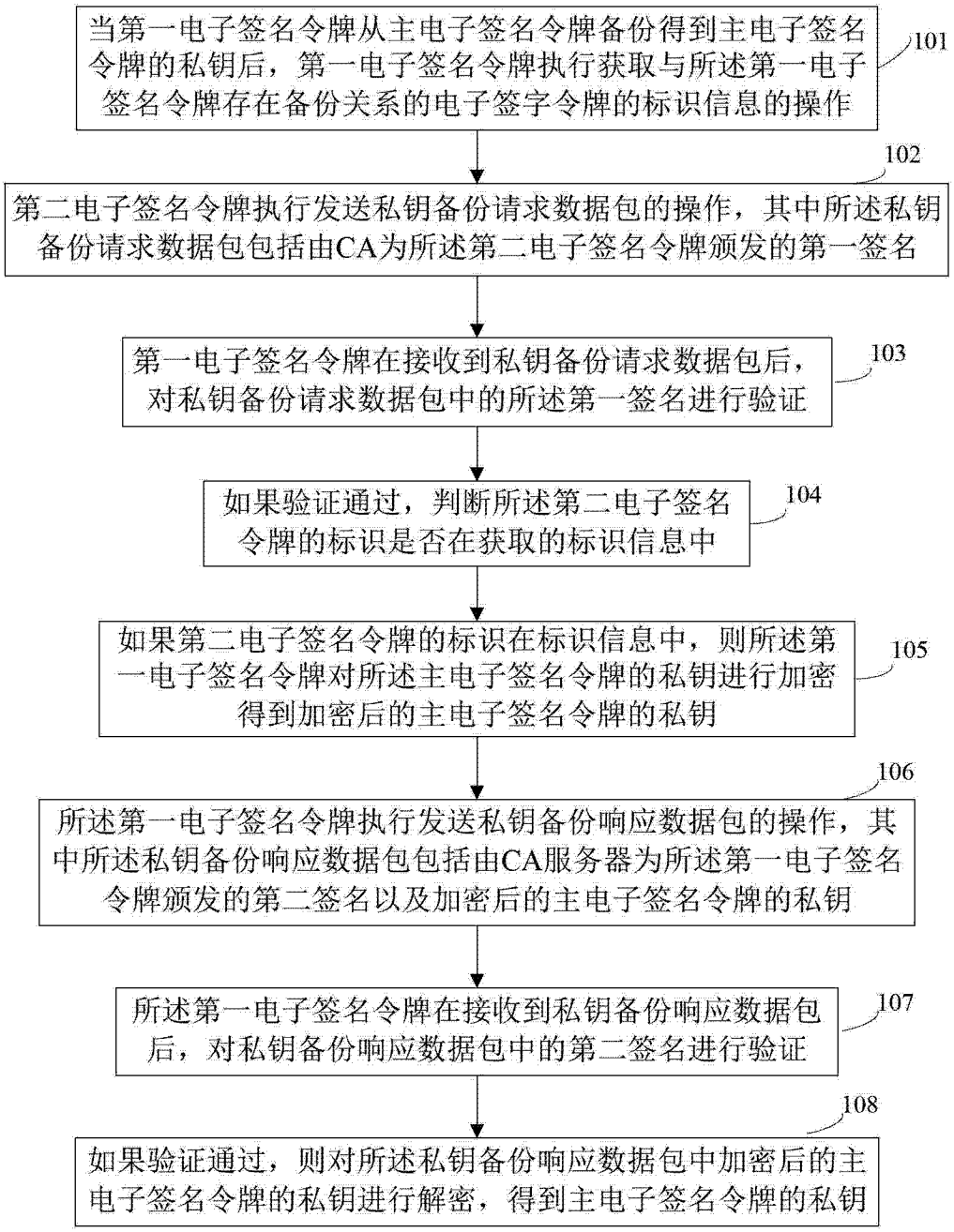

当第一电子签名令牌从主电子签名令牌备份得到主电子签名令牌的私钥后，第一电子签名令牌执行获取与所述第一电子签名令牌存在备份关系的电子签字令牌的标识信息的操作
101
第二电子签名令牌执行发送私钥备份请求数据包的操作，其中所述私钥备份请求数据包包括由CA为所述第二电子签名令牌颁发的第一签名
102
第一电子签名令牌在接收到私钥备份请求数据包后，对私钥备份请求数据包中的所述第一签名进行验证
103
如果验证通过，判断所述第二电子签名令牌的标识是否在获取的标识信息中
104
如果第二电子签名令牌的标识在标识信息中，则所述第一电子签名令牌对所述主电子签名令牌的私钥进行加密得到加密后的主电子签名令牌的私钥
105
所述第一电子签名令牌执行发送私钥备份响应数据包的操作，其中所述私钥备份响应数据包包括由CA服务器为所述第一电子签名令牌颁发的第二签名以及加密后的主电子签名令牌的私钥
106
所述第一电子签名令牌在接收到私钥备份响应数据包后，对私钥备份响应数据包中的第二签名进行验证
107
如果验证通过，则对所述私钥备份响应数据包中加密后的主电子签名令牌的私钥进行解密，得到主电子签名令牌的私钥
108

图 1

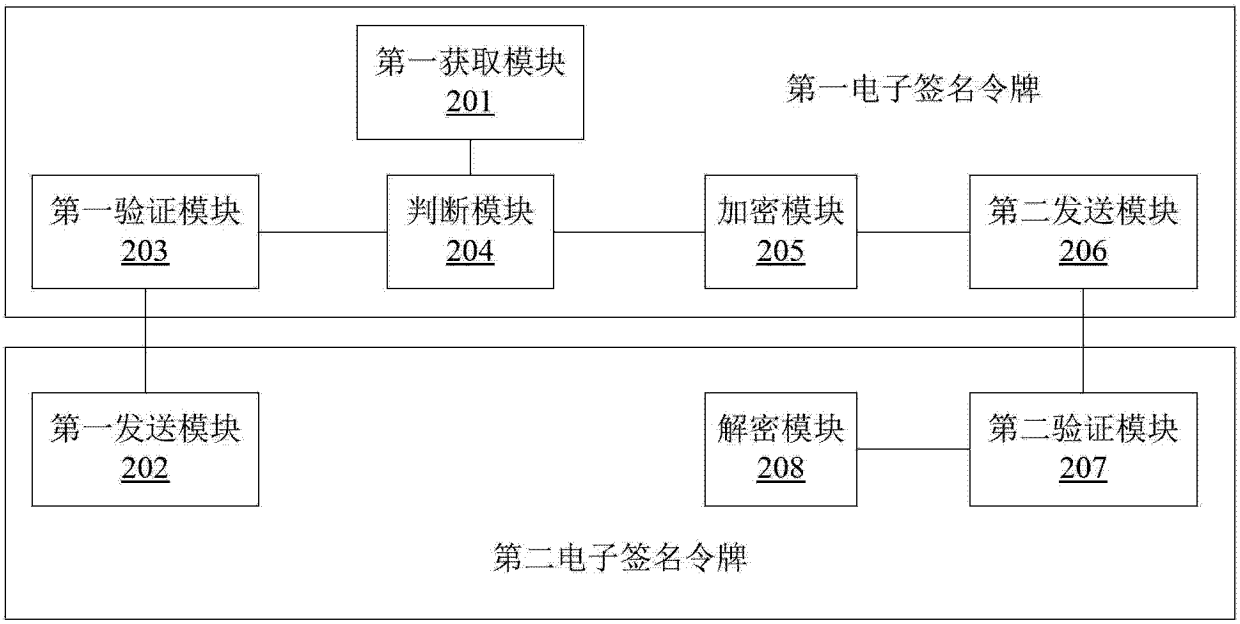

第一获取模块
201
第一电子签名令牌
第一验证模块
203
判断模块
204
加密模块
205
第二发送模块
206
第一发送模块
202
解密模块
208
第二验证模块
207
第二电子签名令牌

图 2