(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114036490 B
(45)授权公告日 2024.07.02

(21)申请号 202111346185.8
(22)申请日 2021.11.15
(65)同一申请的已公布的文献号
申请公布号 CN 114036490 A
(43)申请公布日 2022.02.11
(73)专利权人 公安部交通管理科学研究所
地址 214151 江苏省无锡市滨湖区钱荣路88号
(72)发明人 方万胜 黄金 王军华 金涛 蒋虎 林万华 许超
(74)专利代理机构 无锡市大为专利商标事务所(普通合伙) 32104
专利代理师 陈丽丽 曹祖良
(51)Int.Cl.
G06F 21/44(2013.01)
G06F 21/34(2013.01)
G06F 21/64(2013.01)
(56)对比文件
CN 108243166 A,2018.07.03
CN 109728909 A,2019.05.07
审查员 张力

权利要求书3页 说明书11页 附图4页

(54)发明名称

外挂软件接口调用安全认证方法、USBKey驱动装置及认证系统

(57)摘要

本发明涉及信息安全技术领域,具体公开了一种外挂软件接口调用安全认证方法,其中,包括:获取CA系统签发的USBKey硬件数字证书,USBKey硬件数字证书中存储外挂软件接口的授权信息;根据USBKey硬件数字证书和外挂软件数字证书实现USBKey硬件与外挂软件之间的身份相互认证;根据USBKey硬件数字证书和后台服务系统数字证书实现USBKey硬件与后台服务系统之间的身份相互认证;接收外挂软件的业务请求参数,在确定存在有效的会话密钥时实现外挂软件与后台服务系统之间的数据通信。本发明还公开了一种USBKey驱动装置及安全认证系统。本发明提供的外挂软件接口调用安全认证方法能够防范数据篡改,有效识别外挂软件身份。

CN 114036490 B

1.一种外挂软件接口调用安全认证方法,其特征在于,包括:

获取CA系统签发的USBKey硬件数字证书,其中所述CA系统用于根据后台服务系统、外挂软件和USBKey硬件的数字证书请求文件进行审批并签发生成对应的后台服务系统数字证书、外挂软件数字证书和USBKey硬件数字证书,所述USBKey硬件数字证书中存储外挂软件接口的授权信息;

根据所述USBKey硬件数字证书和所述外挂软件数字证书实现所述USBKey硬件与所述外挂软件之间的身份相互认证;

根据所述USBKey硬件数字证书和所述后台服务系统数字证书实现所述USBKey硬件与所述后台服务系统之间的身份相互认证;

接收所述外挂软件的业务请求参数,在确定存在有效的会话密钥时实现所述外挂软件与所述后台服务系统之间的数据通信;

其中,所述根据所述USBKey硬件数字证书和所述外挂软件数字证书实现所述USBKey硬件与所述外挂软件之间的身份相互认证,包括:

根据所述USBKey硬件数字证书、所述外挂软件生成的第一随机数以及非对称加密算法,实现所述外挂软件对所述USBKey硬件的身份认证;

根据所述外挂软件数字证书、非对称加密算法以及所述USBKey硬件生成的第二随机数,实现所述USBKey硬件对所述外挂软件的身份认证;

其中,所述根据所述USBKey硬件数字证书和所述后台服务系统数字证书实现所述USBKey硬件与所述后台服务系统之间的身份相互认证,包括:

根据所述USBKey硬件数字证书、非对称加密算法以及所述USBKey硬件生成的第三随机数,实现所述后台服务器对所述USBKey硬件的身份认证;

根据所述后台服务系统数字证书、后台服务系统生成的会话密钥以及非对称加密算法,实现所述USBKey硬件对所述后台服务系统的身份认证;

其中,所述接收所述外挂软件的业务请求参数,在确定存在有效的会话密钥时实现所述外挂软件与所述后台服务系统之间的数据通信,包括:

获取所述外挂软件的业务请求参数;

根据所述业务请求参数判断当前是否存在有效的会话密钥;

若存在有效的会话密钥,则计算当前调用路径的哈希值,并根据对称加密算法通过所述会话密钥对所述业务请求参数、当前调用路径的哈希值和当前时间戳进行加密,并得到密文数据;

当所述后台服务系统根据所述对称加密算法以及所述密文数据确定所述会话密钥合法时,接收所述后台服务系统返回的密文业务数据;

根据所述对称加密算法对所述密文业务数据进行解密得到业务数据明文,并将所述业务数据明文发送至所述外挂软件。

2.根据权利要求1所述的外挂软件接口调用安全认证方法,其特征在于,所述根据所述USBKey硬件数字证书、所述外挂软件生成的第一随机数以及非对称加密算法,实现所述外挂软件对所述USBKey硬件的身份认证,包括:

接收所述外挂软件生成的第一随机数;

根据所述对称加密算法对所述第一随机数进行加密得到第一认证值;

计算当前外挂接口的第一调用路径的哈希值,并将所述第一随机数、所述第一认证值以及所述第一调用路径的哈希值均发送至所述USBKey硬件,其中所述USBKey硬件能够根据所述对称加密算法对所述第一随机数进行加密得到第二认证值,若所述第二认证值与所述第一认证值一致,则完成所述USBKey硬件对USBKey驱动装置的认证;所述USBKey硬件完成对USBKey驱动的认证后能够生成第二随机数,将所述第一随机数和第二随机数进行异或后得到的异或数根据非对称加密算法进行签名,得到异或数的签名值;

接收所述USBKey硬件发送的所述第二随机数、异或数的签名值以及所述USBKey硬件数字证书,并将所述第二随机数、异或数的签名值以及所述USBKey硬件数字证书发送至所述外挂软件;

当所述外挂软件对所述异或数的签名值的验证通过后,完成所述外挂软件对所述USBKey硬件的身份认证;

其中所述外挂软件能够根据所述对称加密算法验证所述USBKey硬件数字证书的合法性,以及在所述USBKey硬件数字证书的合法性验证通过后,根据所述USBKey硬件数字证书验证所述异或数的签名值。

3.根据权利要求2所述的外挂软件接口调用安全认证方法,其特征在于,所述根据所述外挂软件数字证书、非对称加密算法以及所述USBKey硬件生成的第二随机数,实现所述USBKey硬件对所述外挂软件的认证,包括:

接收所述外挂软件发送的外挂软件数字证书和第二随机数的签名值,其中所述外挂软件能够根据非对称加密算法对所述第二随机数进行签名,得到第二随机数的签名值;

计算当前外挂接口的第二调用路径的哈希值,并将所述第二随机数的签名值、外挂软件数字证书和第二调用路径的哈希值均发送至所述USBKey硬件,其中所述USBKey硬件能够在确定所述第一调用路径的哈希值和所述第二路径的哈希值一致时,根据非对称加密算法验证所述外挂软件数字证书的合法性,以及在所述外挂软件数字证书的合法性验证通过后,能够根据所述非对称加密算法通过所述外挂软件数字证书验证所述第二随机数的签名值;

当所述第二随机数的签名值验证通过后,完成所述USBKey硬件对所述外挂软件的身份认证。

4.根据权利要求1所述的外挂软件接口调用安全认证方法,其特征在于,所述根据所述USBKey硬件数字证书、非对称加密算法以及所述USBKey硬件生成的第三随机数,实现所述后台服务器对所述USBKey硬件的身份认证,包括:

接收所述USBKey硬件发送的所述第三随机数、第三随机数的签名值以及所述USBKey硬件数字证书,其中所述USBKey硬件能够生成第三随机数,并根据非对称加密算法对所述第三随机数进行签名得到第三随机数的签名值;

将所述第三随机数、第三随机数的签名值以及所述USBKey硬件数字证书发送至所述后台服务系统;

当所述后台服务系统对所述第三随机数的签名值验证通过后,完成所述后台服务系统对所述USBKey硬件的身份认证;

其中所述后台服务系统能够根据所述非对称加密算法验证所述USBKey硬件数字证书的合法性,以及在所述USBKey硬件数字证书的合法性验证通过后,根据所述USBKey硬件数

字证书验证所述第三随机数的签名值。

5.根据权利要求1所述的外挂软件接口调用安全认证方法,其特征在于,所述根据所述后台服务系统数字证书、后台服务系统生成的会话密钥以及非对称加密算法,实现所述USBKey硬件对所述后台服务系统的身份认证,包括:

接收所述后台服务系统发送的会话密钥密文、会话密钥密文的签名值和后台服务系统数字证书,其中所述后台服务系统能够随机生成会话密钥,并能够根据非对称加密算法对所述会话密钥加密得到会话密钥密文,以及能够对所述会话密钥密文进行签名,得到会话密钥密文的签名值;

将所述会话密钥密文、会话密钥密文的签名值和后台服务系统数字证书发送至所述USBKey硬件,其中所述USBKey硬件能够根据所述非对称加密算法通过所述后台服务系统数字证书验证所述会话密钥密文的签名值;

当所述会话密钥密文的签名值验证通过后,完成所述USBKey硬件对所述后台服务系统的身份认证,其中所述USBKey硬件还能够在完成对所述后台服务系统的身份认证后,根据所述非对称加密算法解密所述会话密钥密文得到所述会话密钥;

接收所述USBKey硬件解密得到的所述会话密钥,并通知所述后台服务系统身份认证完成,其中所述后台服务系统能够根据身份认证完成的通知更新会话密钥备案表,记录外挂接口序列号、会话密钥与生成时间戳三者之间的对应关系。

6.一种USBKey驱动装置,用于实现权利要求1至5中任意一项所述的外挂软件接口调用安全认证方法,其特征在于,包括:

获取模块,用于获取CA系统签发的USBKey硬件数字证书,其中所述CA系统用于根据后台服务系统、外挂软件和USBKey硬件的数字证书请求文件进行审批并签发生成对应的后台服务系统数字证书、外挂软件数字证书和USBKey硬件数字证书,所述USBKey硬件数字证书中存储外挂软件接口的授权信息;

第一身份相互认证模块,用于根据所述USBKey硬件数字证书和所述外挂软件数字证书实现所述USBKey硬件与所述外挂软件之间的身份相互认证;

第二身份相互认证模块,用于根据所述USBKey硬件数字证书和所述后台服务系统数字证书实现所述USBKey硬件与所述后台服务系统之间的身份相互认证;

调用模块,用于接收所述外挂软件的业务请求参数,在确定存在有效的会话密钥时实现所述外挂软件与所述后台服务系统之间的数据通信。

7.一种安全认证系统,其特征在于,包括:后台服务系统、外挂软件、USBKey硬件和权利要求6所述的USBKey驱动装置,所述USBKey硬件与所述USBKey驱动装置通信连接,所述外挂软件通过所述USBKey驱动装置与所述后台服务系统通信连接;

所述后台服务系统能够提供业务数据;

所述外挂软件能够通过所述USBKey驱动向所述后台服务系统请求所述业务数据;

所述USBKey驱动装置能够被所述外挂软件调用,以及能够实现所述外挂软件与所述USBKey硬件之间的身份认证、以及实现所述后台服务系统与所述USBKey硬件之间的身份认证;

所述USBKey硬件能够被所述USBKey驱动装置调用,并能够向所述USBKey驱动装置提供数字签名、验签和密码服务。

外挂软件接口调用安全认证方法、USBKey驱动装置及认证系统

技术领域

[0001] 本发明涉及信息安全技术领域,尤其涉及一种外挂软件接口调用安全认证方法、USBKey驱动装置及安全认证系统。

背景技术

[0002] 随着“互联网+政务服务”模式的兴起,行业主管部门为更好的发挥基础数据的作用,满足人民群众日益增长的个性化、多样化数据需求,政务平台向各类外挂软件提供了丰富的请求服务接口,实现政务数据开放共享,打造新型数字政府。

[0003] 目前,各类外挂软件数量众多,但在外挂软件接口申请、授权、使用等方面仍存在不少突出问题。主要包括:一,外挂软件接口访问认证机制存在缺陷,外挂身份难以识别。后台服务系统通常采用接口授权码、IP 地址、有效期止进行验证,只要掌握了在有效期内的接口授权码,任何一个外挂软件都可以通过部署在指定 IP 服务器上,从而“合法”地访问接口,各地挪用接口授权、多个外挂共用接口授权等情况时有发生;二,外挂接口授权信息存在篡改的风险。外挂软件访问接口时,后台服务系统会对接口授权信息和校验码做一致性验证,如果关键信息被篡改,会报校验码错误。但是,对于多层级部署的系统来说,一致性验证算法存放在各地数据库存储过程中,容易被反编译和篡改;三,外挂版本难以管控。送检的外挂软件版本与实际部署的外挂软件版本不一致,在完成安全检测后,实际部署外挂存在屏蔽安全机制、增加违规功能等情况,甚至违规增加接口二次封装功能,难以及时发现。

[0004] 因此,如何能够解决外挂软件调用过程中存在的授权信息篡改、外挂软件身份难以识别、外挂软件版本难以管控等问题成为本领域技术人员亟待解决的技术问题。

发明内容

[0005] 本发明提供了一种外挂软件接口调用安全认证方法、USBKey驱动装置及安全认证系统,解决相关技术中存在的外挂软件调用过程中存在的授权信息篡改、外挂软件身份难以识别、外挂软件版本难以管控的问题。

[0006] 作为本发明的第一个方面,提供一种外挂软件接口调用安全认证方法,其中,包括:

[0007] 获取CA系统签发的USBKey硬件数字证书,其中所述CA系统用于根据后台服务系统、外挂软件和USBKey硬件的数字证书请求文件进行审批并签发生成对应的后台服务系统数字证书、外挂软件数字证书和USBKey硬件数字证书,所述USBKey硬件数字证书中存储外挂软件接口的授权信息;

[0008] 根据所述USBKey硬件数字证书和所述外挂软件数字证书实现所述USBKey硬件与所述外挂软件之间的身份相互认证;

[0009] 根据所述USBKey硬件数字证书和所述后台服务系统数字证书实现所述USBKey硬

件与所述后台服务系统之间的身份相互认证；

[0010] 接收所述外挂软件的业务请求参数，在确定存在有效的会话密钥时实现所述外挂软件与所述后台服务系统之间的数据通信。

[0011] 进一步地，所述根据所述USBKey硬件数字证书和所述外挂软件数字证书实现所述USBKey硬件与所述外挂软件之间的身份相互认证，包括：

[0012] 根据所述USBKey硬件数字证书、所述外挂软件生成的第一随机数以及非对称加密算法，实现所述外挂软件对所述USBKey硬件的身份认证；

[0013] 根据所述外挂软件数字证书、非对称加密算法以及所述USBKey硬件生成的第二随机数，实现所述USBKey硬件对所述外挂软件的身份认证。

[0014] 进一步地，所述根据所述USBKey硬件数字证书、所述外挂软件生成的第一随机数以及非对称加密算法，实现所述外挂软件对所述USBKey硬件的身份认证，包括：

[0015] 接收所述外挂软件生成的第一随机数；

[0016] 根据所述对称加密算法对所述第一随机数进行加密得到第一认证值；

[0017] 计算当前外挂接口的第一调用路径的哈希值，并将所述第一随机数、所述第一认证值以及所述第一调用路径的哈希值均发送至所述USBKey硬件，其中所述USBKey硬件能够根据所述对称加密算法对所述第一随机数进行加密得到第二认证值，若所述第二认证值与所述第一认证值一致，则完成所述USBKey硬件对USBKey驱动装置的认证；所述USBKey硬件完成对USBKey驱动的认证后能够生成第二随机数，将所述第一随机数和第二随机数进行异或后得到的异或数根据非对称加密算法进行签名，得到异或数的签名值；

[0018] 接收所述USBKey硬件发送的所述第二随机数、异或数的签名值以及所述USBKey硬件数字证书，并将所述第二随机数、异或数的签名值以及所述USBKey硬件数字证书发送至所述外挂软件；

[0019] 当所述外挂软件对所述异或数的签名值的验证通过后，完成所述外挂软件对所述USBKey硬件的身份认证；

[0020] 其中所述外挂软件能够根据所述对称加密算法验证所述USBKey硬件数字证书的合法性，以及在所述USBKey硬件数字证书的合法性验证通过后，根据所述USBKey硬件数字证书验证所述异或数的签名值。

[0021] 进一步地，所述根据所述外挂软件数字证书、非对称加密算法以及所述USBKey硬件生成的第二随机数，实现所述USBKey硬件对所述外挂软件的认证，包括：

[0022] 接收所述外挂软件发送的外挂软件数字证书和第二随机数的签名值，其中所述外挂软件能够根据非对称加密算法对所述第二随机数进行签名，得到第二随机数的签名值；

[0023] 计算当前外挂接口的第二调用路径的哈希值，并将所述第二随机数的签名值、外挂软件数字证书和第二调用路径的哈希值均发送至所述USBKey硬件，其中所述USBKey硬件能够在确定所述第一调用路径的哈希值和所述第二路径的哈希值一致时，根据非对称加密算法验证所述外挂软件数字证书的合法性，以及在所述外挂软件数字证书的合法性验证通过后，能够根据所述非对称加密算法通过所述外挂软件数字证书验证所述第二随机数的签名值；

[0024] 当所述第二随机数的签名值验证通过后，完成所述USBKey硬件对所述外挂软件的身份认证。

[0025] 进一步地,所述根据所述USBKey硬件数字证书和所述后台服务系统数字证书实现所述USBKey硬件与所述后台服务系统之间的身份相互认证,包括:

[0026] 根据所述USBKey硬件数字证书、非对称加密算法以及所述USBKey硬件生成的第三随机数,实现所述后台服务器对所述USBKey硬件的身份认证;

[0027] 根据所述后台服务系统数字证书、后台服务系统生成的会话密钥以及非对称加密算法,实现所述USBKey硬件对所述后台服务系统的身份认证。

[0028] 进一步地,所述根据所述USBKey硬件数字证书、非对称加密算法以及所述USBKey硬件生成的第三随机数,实现所述后台服务器对所述USBKey硬件的身份认证,包括:

[0029] 接收所述USBKey硬件发送的所述第三随机数、第三随机数的签名值以及所述USBKey硬件数字证书,其中所述USBKey硬件能够生成第三随机数,并根据非对称加密算法对所述第三随机数进行签名得到第三随机数的签名值;

[0030] 将所述第三随机数、第三随机数的签名值以及所述USBKey硬件数字证书发送至所述后台服务系统;

[0031] 当所述后台服务系统对所述第三随机数的签名值验证通过后,完成所述后台服务系统对所述USBKey硬件的身份认证;

[0032] 其中所述后台服务系统能够根据所述非对称加密算法验证所述USBKey硬件数字证书的合法性,以及在所述USBKey硬件数字证书的合法性验证通过后,根据所述USBKey硬件数字证书验证所述第三随机数的签名值。

[0033] 进一步地,所述根据所述后台服务系统数字证书、后台服务系统生成的会话密钥以及非对称加密算法,实现所述USBKey硬件对所述后台服务系统的身份认证,包括:

[0034] 接收所述后台服务系统发送的会话密钥密文、会话密钥密文的签名值和后台服务系统数字证书,其中所述后台服务系统能够随机生成会话密钥,并能够根据非对称加密算法对所述会话密钥加密得到会话密钥密文,以及能够对所述会话密钥密文进行签名,得到会话密钥密文的签名值;

[0035] 将所述会话密钥密文、会话密钥密文的签名值和后台服务系统数字证书发送至所述USBKey硬件,其中所述USBKey硬件能够根据所述非对称加密算法通过所述后台服务系统数字证书验证所述会话密钥密文的签名值;

[0036] 当所述会话密钥密文的签名值验证通过后,完成所述USBKey硬件对所述后台服务系统的身份认证,其中所述USBKey硬件还能够在完成对所述后台服务系统的身份认证后,根据所述非对称加密算法解密所述会话密钥密文得到所述会话密钥;

[0037] 接收所述USBKey硬件解密得到的所述会话密钥,并通知所述后台服务系统身份认证完成,其中所述后台服务系统能够根据身份认证完成的通知更新会话密钥备案表,记录外挂接口序列号、会话密钥与生成时间戳三者之间的对应关系。

[0038] 进一步地,所述接收所述外挂软件的业务请求参数,在确定存在有效的会话密钥时实现所述外挂软件与所述后台服务系统之间的数据通信,包括:

[0039] 获取所述外挂软件的业务请求参数;

[0040] 根据所述业务请求参数判断当前是否存在有效的会话密钥;

[0041] 若存在有效的会话密钥,则计算当前调用路径的哈希值,并根据对称加密算法通过所述会话密钥对所述业务请求参数、当前调用路径的哈希值和当前时间戳进行加密,并

得到密文数据;

[0042] 当所述后台服务系统根据所述对称加密算法以及所述密文数据确定所述会话密钥合法时,接收所述后台服务系统返回的密文业务数据;

[0043] 根据所述对称加密算法对所述密文业务数据进行解密得到业务数据明文,并将所述业务数据明文发送至所述外挂软件。

[0044] 作为本发明的另一个方面,提供一种USBKey驱动装置,用于实现前文所述的外挂软件接口调用安全认证方法,其中,包括:

[0045] 获取模块,用于获取CA系统签发的USBKey硬件数字证书,其中所述CA系统用于根据后台服务系统、外挂软件和USBKey硬件的数字证书请求文件进行审批并签发生成对应的后台服务系统数字证书、外挂软件数字证书和USBKey硬件数字证书,所述USBKey硬件数字证书中存储外挂软件接口的授权信息;

[0046] 第一身份相互认证模块,用于根据所述USBKey硬件数字证书和所述外挂软件数字证书实现所述USBKey硬件与所述外挂软件之间的身份相互认证;

[0047] 第二身份相互认证模块,用于根据所述USBKey硬件数字证书和所述后台服务系统数字证书实现所述USBKey硬件与所述后台服务系统之间的身份相互认证;

[0048] 调用模块,用于接收所述外挂软件的业务请求参数,在确定存在有效的会话密钥时实现所述外挂软件与所述后台服务系统之间的数据通信。

[0049] 作为本发明的另一个方面,提供一种安全认证系统,其中,包括:后台服务系统、外挂软件、USBKey硬件和前文所述的USBKey驱动装置,所述USBKey硬件与所述USBKey驱动装置通信连接,所述外挂软件通过所述USBKey驱动装置与所述后台服务系统通信连接;

[0050] 所述后台服务系统能够提供业务数据;

[0051] 所述外挂软件能够通过所述USBKey驱动向所述后台服务系统请求所述业务数据;

[0052] 所述USBKey驱动装置能够被所述外挂软件调用,以及能够实现所述外挂软件与所述USBKey硬件之间的身份认证、以及实现所述后台服务系统与所述USBKey硬件之间的身份认证;

[0053] 所述USBKey硬件能够被所述USBKey驱动装置调用,并能够向所述USBKey驱动装置提供数字签名、验签和密码服务。

[0054] 本发明提供的外挂软件接口调用安全认证方法,通过构建基于USBKey硬件的外挂软件接口调用安全认证体系,依托硬件数字签名与数字证书,建立外挂软件与USBKey硬件、后台服务系统与USBKey硬件的双向身份认证机制,防范数据篡改,有效识别外挂软件身份;运用接口调用路径检测与时间戳比对等策略,规范外挂软件安全使用。通过上述方式,本发明实现了外挂软件接口调用时的安全认证,提升了外挂软件安全设计水平,规范了外挂软件管理工作流程。

附图说明

[0055] 附图是用来提供对本发明的进一步理解,并且构成说明书的一部分,与下面的具体实施方式一起用于解释本发明,但并不构成对本发明的限制。在附图中:

[0056] 图1为本发明提供的安全认证系统的结构框图。

[0057] 图2为本发明提供的外挂软件接口调用安全认证方法的流程图。

[0058] 图3为本发明提供的外挂软件与USBKey硬件之间身份相互认证流程图。

[0059] 图4为本发明提供的后台服务系统与USBKey硬件之间身份相互认证流程图。

[0060] 图5为本发明提供的业务接口调用流程示意图。

具体实施方式

[0061] 需要说明的是,在不冲突的情况下,本发明中的实施例及实施例中的特征可以相互结合。下面将参考附图并结合实施例来详细说明本发明。

[0062] 为了使本领域技术人员更好地理解本发明方案,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,显然,所描述的实施例仅仅是本发明一部分的实施例,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,都应当属于本发明保护的范围。

[0063] 需要说明的是,本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本发明的实施例。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包括,例如,包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0064] 作为本发明的一个实施例,提供一种安全认证系统,如图1所示,包括:后台服务系统、外挂软件、USBKey硬件和USBKey驱动装置,所述USBKey硬件与所述USBKey驱动装置通信连接,所述外挂软件通过所述USBKey驱动装置与所述后台服务系统通信连接;

[0065] 所述后台服务系统能够提供业务数据;

[0066] 所述外挂软件能够通过所述USBKey驱动向所述后台服务系统请求所述业务数据;

[0067] 所述USBKey驱动装置能够被所述外挂软件调用,以及能够实现所述外挂软件与所述USBKey硬件之间的身份认证、以及实现所述后台服务系统与所述USBKey硬件之间的身份认证;

[0068] 所述USBKey硬件能够被所述USBKey驱动装置调用,并能够向所述USBKey驱动装置提供数字签名、验签和密码服务。

[0069] 本发明的这种安全认证系统,采用数字证书与数字签名结合的方式完成外挂软件与USBKey硬件、后台服务系统与USBKey硬件的双向身份认证,能够有效识别外挂软件身份,实现数据防篡改。

[0070] 具体地,在所述安全认证系统中还包括:密码机,所述密码机与所述后台服务系统通信连接,能够向所述后台服务系统提供数字签名、验签、数字加解密等密码服务。

[0071] 具体地,所述安全认证系统还可以包括CA系统,所述CA系统用于提供证书签发服务,用于生成后台服务系统数字证书、外挂软件数字证书和USBKey硬件数字证书。

[0072] 作为本发明的另一个实施例,提供一种USBKey驱动装置,具体可以实现外挂软件接口调用安全认证方法,具体可以包括:

[0073] 获取模块,用于获取CA系统签发的USBKey硬件数字证书,其中所述CA系统用于根据后台服务系统、外挂软件和USBKey硬件的数字证书请求文件进行审批并签发生成对应的后台服务系统数字证书、外挂软件数字证书和USBKey硬件数字证书,所述USBKey硬件数字

证书中存储外挂软件接口的授权信息；

[0074] 第一身份相互认证模块，用于根据所述USBKey硬件数字证书和所述外挂软件数字证书实现所述USBKey硬件与所述外挂软件之间的身份相互认证；

[0075] 第二身份相互认证模块，用于根据所述USBKey硬件数字证书和所述后台服务系统数字证书实现所述USBKey硬件与所述后台服务系统之间的身份相互认证；

[0076] 调用模块，用于接收所述外挂软件的业务请求参数，在确定存在有效的会话密钥时实现所述外挂软件与所述后台服务系统之间的数据通信。

[0077] 本发明实施例提供的USBKey驱动装置，与USBKey硬件结合，能够有效解决外挂软件调用过程中的授权信息篡改、外挂软件身份难以识别以及外挂软件版本难以管控的问题，为外挂软件接口调用提供更可靠的安全支撑及监管保障。

[0078] 作为本发明的另一实施例，提供一种外挂软件接口调用安全认证方法，在本实施例中以所述USBKey驱动装置作为执行主体描述外挂软件接口调用安全认证方法的具体实现过程。如图2所示是根据本发明实施例提供的外挂软件接口调用安全认证方法的流程图，如图2所示，包括：

[0079] S110、获取CA系统签发的USBKey硬件数字证书，其中所述CA系统用于根据后台服务系统、外挂软件和USBKey硬件的数字证书请求文件进行审批并签发生成对应的后台服务系统数字证书、外挂软件数字证书和USBKey硬件数字证书，所述USBKey硬件数字证书中存储外挂软件接口的授权信息。

[0080] 在本发明实施例中，关于CA系统生成后台服务系统数字证书、外挂软件数字证书和USBKey硬件数字证书的具体过程，包括：

[0081] (1)后台服务系统在密码机中随机生成一对公私钥，生成数字证书请求文件并提交给CA系统；CA系统完成审批后，签发生成后台服务系统数字证书，发送给后台服务系统；后台服务系统接收后，安全保存在密码机中；

[0082] (2)外挂软件随机生成一对公私钥，生成数字证书请求文件并提交给CA系统；CA系统完成审批后，签发生成外挂软件数字证书，发送给外挂软件；外挂软件接收后，安全保存；

[0083] (3)USBKey硬件在内部随机生成一对公私钥，生成数字证书请求文件并提交给CA系统；CA系统完成审批后，签发生成USBKey硬件数字证书，发送给USBKey硬件；USBKey硬件接收后，在硬件内部安全保存，其中USBKey硬件数字证书中还存储外挂软件接口授权信息。

[0084] 在一些实施方式中，外挂软件需要实现接口备案，具体可以包括：

[0085] (1)外挂软件在部署之前需进行检测，检测过程采集外挂认证过程中的所有路径和业务接口调用过程中的所有路径信息，提交至后台服务系统；

[0086] (2)后台服务系统维护外挂接口备案表，备案记录包括外挂接口序列号、外挂接口授权信息、外挂接口所有调用路径信息等。

[0087] S120、根据所述USBKey硬件数字证书和所述外挂软件数字证书实现所述USBKey硬件与所述外挂软件之间的身份相互认证。

[0088] 在本发明实施例中，具体可以包括：

[0089] 根据所述USBKey硬件数字证书、所述外挂软件生成的第一随机数以及非对称加密算法，实现所述外挂软件对所述USBKey硬件的身份认证；

[0090] 根据所述外挂软件数字证书、非对称加密算法以及所述USBKey硬件生成的第二随

机数,实现所述USBKey硬件对所述外挂软件的身份认证。

[0091] 作为一种具体地实施方式,所述根据所述USBKey硬件数字证书、所述外挂软件生成的第一随机数以及非对称加密算法,实现所述外挂软件对所述USBKey硬件的身份认证,包括:

[0092] 接收所述外挂软件生成的第一随机数;

[0093] 根据所述对称加密算法对所述第一随机数进行加密得到第一认证值;

[0094] 计算当前外挂接口的第一调用路径的哈希值,并将所述第一随机数、所述第一认证值以及所述第一调用路径的哈希值均发送至所述USBKey硬件,其中所述USBKey硬件能够根据所述对称加密算法对所述第一随机数进行加密得到第二认证值,若所述第二认证值与所述第一认证值一致,则完成所述USBKey硬件对USBKey驱动装置的认证;所述USBKey硬件完成对USBKey驱动的认证后能够生成第二随机数,将所述第一随机数和第二随机数进行异或后得到的异或数根据非对称加密算法进行签名,得到异或数的签名值;

[0095] 接收所述USBKey硬件发送的所述第二随机数、异或数的签名值以及所述USBKey硬件数字证书,并将所述第二随机数、异或数的签名值以及所述USBKey硬件数字证书发送至所述外挂软件;

[0096] 当所述外挂软件对所述异或数的签名值的验证通过后,完成所述外挂软件对所述USBKey硬件的身份认证;

[0097] 其中所述外挂软件能够根据所述对称加密算法验证所述USBKey硬件数字证书的合法性,以及在所述USBKey硬件数字证书的合法性验证通过后,根据所述USBKey硬件数字证书验证所述异或数的签名值。

[0098] 在该实施方式中,实现的是所述外挂软件对所述USBKey硬件的身份认证。

[0099] 作为优选地实施方式,如图3所示,所述外挂软件认证USBKey硬件具体可以包括:

[0100] (1)外挂软件生成32字节第一随机数R1,将第一随机数R1发送到USBKey驱动;

[0101] (2)USBKey驱动装置接收到第一随机数R1后,具体的对称加密算法可以采用白盒SM4算法,对第一随机数R1加密得到32字节第一认证值Auth,计算当前外挂接口第一调用路径Path1的哈希(Hash)值,将第一随机数R1、第一认证值Auth、第一调用路径Path1的Hash值发送到USBKey硬件;

[0102] (3)USBKey硬件接收到数据后,采用SM4算法,使用内置的认证密钥对第一随机数R1加密得到第二认证值Auth',比较第一认证值Auth与第二认证值Auth'的一致性,若一致,则完成USBKey硬件对USBKey驱动的认证,进入步骤(4);若不一致,则返回错误到USBKey驱动,认证结束;

[0103] (4)USBKey硬件生成32字节第二随机数R2,将第一随机数R1和第二随机数R2异或得到32字节异或数R12,采用非对称加密算法,如SM2算法,使用USBKey硬件私钥对异或数R12签名,得到64字节异或数签名值SignR12,将第二随机数R2、异或数签名值SignR12、USBKey硬件数字证书发送到USBKey驱动;

[0104] (5)USBKey驱动接收到数据后,将第二随机数R2、异或数签名值SignR12、USBKey硬件数字证书转发到外挂软件;

[0105] (6)外挂软件接收到数据后,采用SM2算法,使用CA根证书公钥验证USBKey硬件数字证书的合法性,若验证通过,进入步骤(7);若验证不通过,认证结束;

[0106] (7)外挂软件使用USBKey硬件数字证书公钥验证SignR12,若验证通过,则完成外挂软件对USBKey硬件的认证,进入USBKey硬件认证外挂软件的过程;若验证不通过,认证结束。

[0107] 作为另一种具体地实施方式,所述根据所述外挂软件数字证书、非对称加密算法以及所述USBKey硬件生成的第二随机数,实现所述USBKey硬件对所述外挂软件的认证,包括:

[0108] 接收所述外挂软件发送的外挂软件数字证书和第二随机数的签名值,其中所述外挂软件能够根据非对称加密算法对所述第二随机数进行签名,得到第二随机数的签名值;

[0109] 计算当前外挂接口的第二调用路径的哈希值,并将所述第二随机数的签名值、外挂软件数字证书和第二调用路径的哈希值均发送至所述USBKey硬件,其中所述USBKey硬件能够在确定所述第一调用路径的哈希值和所述第二路径的哈希值一致时,根据非对称加密算法验证所述外挂软件数字证书的合法性,以及在所述外挂软件数字证书的合法性验证通过后,能够根据所述非对称加密算法通过所述外挂软件数字证书验证所述第二随机数的签名值;

[0110] 当所述第二随机数的签名值验证通过后,完成所述USBKey硬件对所述外挂软件的身份认证。

[0111] 在该实施方式中,实现的是所述USBKey硬件对所述外挂软件的身份认证。

[0112] 作为优选地实施方式,如图3所示,所述USBKey硬件对所述外挂软件的身份认证具体可以包括:

[0113] (1)外挂软件采用非对称加密算法,如SM2算法,使用外挂软件私钥对第二随机数R2签名,得到64字节第二随机数签名值SignR2,将第二随机数签名值SignR2、外挂软件数字证书发给USBKey驱动;

[0114] (2)USBKey驱动接收到数据后,计算当前外挂接口第二调用路径Path2的Hash值,将第二随机数签名值SignR2、外挂软件数字证书、第二调用路径Path2的Hash值发送到USBKey硬件;

[0115] (3)USBKey硬件接收到数据后,首先比较第一调用路径Path1的Hash值和第二调用路径Path2的Hash值,若一致,则进入步骤(4);若不一致,则返回错误到USBKey驱动,认证结束;

[0116] (4)USBKey硬件采用SM2算法,使用CA根证书公钥验证外挂软件数字证书的合法性,若验证通过,则进入步骤(5);若验证不通过,则返回错误到USBKey驱动,认证结束;

[0117] (5)USBKey硬件采用SM2算法,使用外挂软件数字证书公钥验证SignR2,若验证通过,则完成USBKey硬件对外挂软件的认证,进入后台服务系统认证USBKey硬件的过程;若验证不通过,返回错误到USBKey驱动,认证结束。

[0118] S130、根据所述USBKey硬件数字证书和所述后台服务系统数字证书实现所述USBKey硬件与所述后台服务系统之间的身份相互认证。

[0119] 在本发明实施例中,具体可以包括:

[0120] 根据所述USBKey硬件数字证书、非对称加密算法以及所述USBKey硬件生成的第三随机数,实现所述后台服务器对所述USBKey硬件的身份认证;

[0121] 根据所述后台服务系统数字证书、后台服务系统生成的会话密钥以及非对称加密

算法,实现所述USBKey硬件对所述后台服务系统的身份认证。

[0122] 作为一种具体地实施方式,所述根据所述USBKey硬件数字证书、非对称加密算法以及所述USBKey硬件生成的第三随机数,实现所述后台服务器对所述USBKey硬件的身份认证,包括:

[0123] 接收所述USBKey硬件发送的所述第三随机数、第三随机数的签名值以及所述USBKey硬件数字证书,其中所述USBKey硬件能够生成第三随机数,并根据非对称加密算法对所述第三随机数进行签名得到第三随机数的签名值;

[0124] 将所述第三随机数、第三随机数的签名值以及所述USBKey硬件数字证书发送至所述后台服务系统;

[0125] 当所述后台服务系统对所述第三随机数的签名值验证通过后,完成所述后台服务系统对所述USBKey硬件的身份认证;

[0126] 其中所述后台服务系统能够根据所述非对称加密算法验证所述USBKey硬件数字证书的合法性,以及在所述USBKey硬件数字证书的合法性验证通过后,根据所述USBKey硬件数字证书验证所述第三随机数的签名值。

[0127] 在该实施方式中,实现的是所述后台服务系统对USBKey硬件的身份认证。

[0128] 作为优选地实施方式,如图4所示,所述后台服务系统认证USBKey硬件具体可以包括:

[0129] (1)USBKey硬件生成32字节第三随机数R3,采用非对称加密算法,如SM2算法,使用USBKey硬件私钥对第三随机数R3签名得到64字节第三随机数签名值SignR3,将第三随机数R3、第三随机数签名值SignR3、USBKey硬件数字证书、第一调用路径Path1(或第二调用路径Path2)的Hash值发给USBKey驱动;

[0130] (2)USBKey驱动接收到数据后,将第三随机数R3、第三随机数签名值SignR3、USBKey硬件数字证书、第一调用路径Path1(或第二调用路径Path2)的Hash值转发给后台服务系统;

[0131] (3)后台服务系统接收到数据后,采用SM2算法,调用密码机使用CA根证书公钥验证USBKey硬件数字证书的合法性,若验证通过,则进入步骤(4);若验证不通过,认证结束;

[0132] (4)后台服务系统采用SM2算法,调用密码机使用USBKey硬件数字证书公钥验证SignR3,若验证通过,则完成后台服务系统对USBKey硬件的认证,进入步骤(5);若验证不通过,认证结束;

[0133] (5)后台服务系统解析USBKey硬件数字证书中的外挂接口授权信息,根据外挂接口序列号查询外挂接口备案表中是否存在Path1(或Path2)的Hash值,若存在,表明当前认证调用路径合法,进入USBKey硬件认证后台服务系统的过程;若不存在,认证结束。

[0134] 作为另一种具体地实施方式,所述根据所述后台服务系统数字证书、后台服务系统生成的会话密钥以及非对称加密算法,实现所述USBKey硬件对所述后台服务系统的身份认证,包括:

[0135] 接收所述后台服务系统发送的会话密钥密文、会话密钥密文的签名值和后台服务系统数字证书,其中所述后台服务系统能够随机生成会话密钥,并能够根据非对称加密算法对所述会话密钥加密得到会话密钥密文,以及能够对所述会话密钥密文进行签名,得到会话密钥密文的签名值;

[0136] 将所述会话密钥密文、会话密钥密文的签名值和后台服务系统数字证书发送至所述USBKey硬件,其中所述USBKey硬件能够根据所述非对称加密算法通过所述后台服务系统数字证书验证所述会话密钥密文的签名值;

[0137] 当所述会话密钥密文的签名值验证通过后,完成所述USBKey硬件对所述后台服务系统的身份认证,其中所述USBKey硬件还能够在完成对所述后台服务系统的身份认证后,根据所述非对称加密算法解密所述会话密钥密文得到所述会话密钥;

[0138] 接收所述USBKey硬件解密得到的所述会话密钥,并通知所述后台服务系统身份认证完成,其中所述后台服务系统能够根据身份认证完成的通知更新会话密钥备案表,记录外挂接口序列号、会话密钥与生成时间戳三者之间的对应关系。

[0139] 在该实施方式中,实现的是USBKey硬件对后台服务系统的身份认证。

[0140] 作为优选地实施方式,如图4所示,所述USBKey硬件认证后台服务系统具体可以包括:

[0141] (1)后台服务系统调用密码机生成随机的16字节会话密钥SessionKey,采用非对称加密算法,如SM2算法,调用密码机使用USBKey硬件数字证书公钥对会话密钥SessionKey加密得到112字节会话密钥SessionKey密文,调用密码机使用后台服务系统私钥对会话密钥SessionKey密文进行签名,得到64字节会话密钥签名值SignSessionKey密文,将会话密钥SessionKey密文、会话密钥签名值SignSessionKey密文、后台服务系统数字证书发送到USBKey驱动;

[0142] (2)USBKey驱动接收到数据后,将会话密钥SessionKey密文、会话密钥签名值SignSessionKey密文、后台服务系统数字证书转发到USBKey硬件;

[0143] (3)USBKey硬件接收到数据后,采用SM2算法,使用CA根证书公钥验证后台服务系统数字证书的合法性,若验证通过,则进入步骤(4);若验证不通过,返回错误到USBKey驱动,认证结束;

[0144] (4)USBKey硬件采用SM2算法,使用后台服务系统数字证书公钥验证会话密钥签名值SignSessionKey密文,若验证通过,则完成USBKey硬件对后台服务系统的认证,进入步骤(5);若验证不通过,返回错误到USBKey驱动,认证结束;

[0145] (5)USBKey硬件采用SM2算法,使用USBKey硬件私钥解密会话密钥SessionKey密文得到会话密钥SessionKey,将会话密钥SessionKey发送给USBKey驱动;

[0146] (6)USBKey驱动接收到数据后,通知后台服务系统认证完成;

[0147] (7)后台服务系统更新会话密钥SessionKey备案表,记录外挂接口序列号、SessionKey及生成时间戳的对应关系,整个认证过程结束。

[0148] S140、接收所述外挂软件的业务请求参数,在确定存在有效的会话密钥时实现所述外挂软件与所述后台服务系统之间的数据通信。

[0149] 具体地,可以包括:

[0150] 获取所述外挂软件的业务请求参数;

[0151] 根据所述业务请求参数判断当前是否存在有效的会话密钥;

[0152] 若存在有效的会话密钥,则计算当前调用路径的哈希值,并根据对称加密算法通过所述会话密钥对所述业务请求参数、当前调用路径的哈希值和当前时间戳进行加密,并得到密文数据;

[0153] 当所述后台服务系统根据所述对称加密算法以及所述密文数据确定所述会话密钥合法时,接收所述后台服务系统返回的密文业务数据;

[0154] 根据所述对称加密算法对所述密文业务数据进行解密得到业务数据明文,并将所述业务数据明文发送至所述外挂软件。

[0155] 作为优选地实施方式,如图5所示,业务接口调用的具体过程包括:

[0156] 首先,实现外挂软件调用USBKey驱动,具体包括:

[0157] 外挂软件准备好业务请求参数(包含外挂接口序列号等),将业务请求参数发送到USBKey驱动。

[0158] 其次,实现USBKey驱动调用业务接口,具体包括:

[0159] (1)USBKey驱动接收到数据后,先判断当前是否存在会话密钥SessionKey且有效,若会话密钥SessionKey存在且有效,进入步骤(2);若不存在或无效,返回执行外挂软件认证USBKey的步骤;

[0160] (2)USBKey驱动计算当前调用路径Path的Hash值,采用对称加密算法,如SM4算法,使用会话密钥SessionKey对业务请求参数(除外挂接口序列号外)、当前调用路径Path的Hash值和当前时间戳进行加密,得到密文数据ReqEnc,将外挂接口序列号、密文数据ReqEnc发送到后台服务系统;

[0161] (3)后台服务系统接收到数据后,根据外挂接口序列号查询会话密钥SessionKey备案表,找到对应的会话密钥SessionKey及时间戳信息;

[0162] (4)后台服务系统采用SM4算法,调用密码机使用对应的会话密钥SessionKey解密密文数据ReqEnc得到明文业务请求参数、当前调用路径Path的Hash值和当前时间戳,先判断时间戳有效性,若有效,进入步骤(5);若失效,返回执行外挂软件认证USBKey的步骤;

[0163] (5)后台服务系统查询外挂接口备案表,查找当前调用路径Path的Hash值是否存在,若存在,进入步骤(6);若不存在,表明会话密钥SessionKey非法或调用路径不合法,调用结束;

[0164] (6)后台服务系统准备好要返回的业务数据,调用密码机使用对应的会话密钥SessionKey加密要返回的业务数据,得到业务数据密文WorkEnc,将业务数据密文发给USBKey驱动;

[0165] (7)USBKey驱动接收到数据后,采用SM4算法,使用会话密钥SessionKey解密业务数据密文WorkEnc得到业务数据明文,将业务数据明文发送到外挂软件;

[0166] (8)外挂软件接收到数据后,调用完成。

[0167] 综上,本发明实施例提供的外挂软件接口调用安全认证方法,通过构建基于USBKey硬件的外挂软件接口调用安全认证体系,依托硬件数字签名与数字证书,建立外挂软件与USBKey硬件、后台服务系统与USBKey硬件的双向身份认证机制,防范数据篡改,有效识别外挂软件身份;运用接口调用路径检测与时间戳比对等策略,规范外挂软件安全使用。通过上述方式,本发明实现了外挂软件接口调用时的安全认证,提升了外挂软件安全设计水平,规范了外挂软件管理工作流程。

[0168] 可以理解的是,以上实施方式仅仅是为了说明本发明的原理而采用的示例性实施方式,然而本发明并不局限于此。对于本领域内的普通技术人员而言,在不脱离本发明的精神和实质的情况下,可以做出各种变型和改进,这些变型和改进也视为本发明的保护范围。

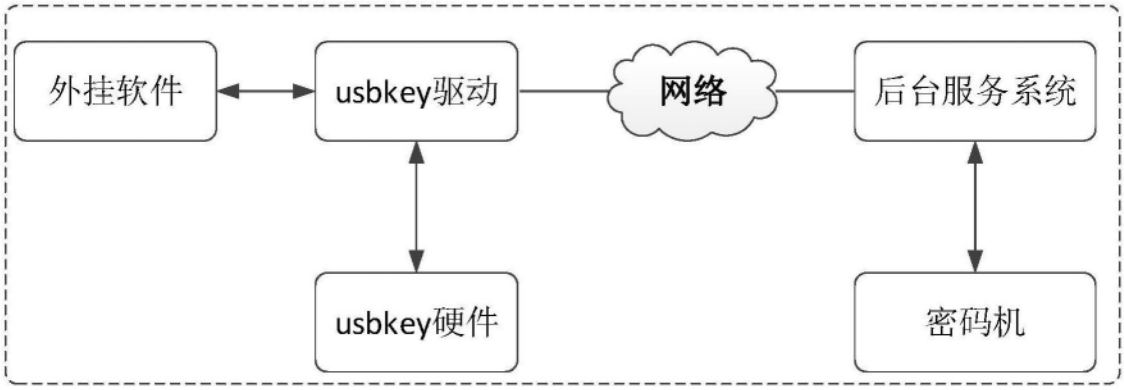
外挂软件
usbkey驱动
网络
后台服务系统
usbkey硬件
密码机

图1

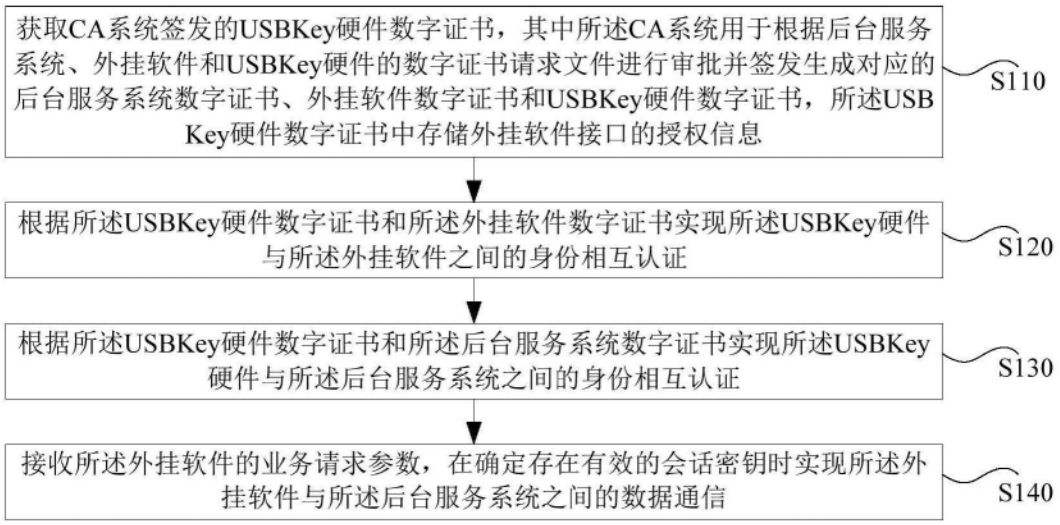
获取CA系统签发的USBKey硬件数字证书，其中所述CA系统用于根据后台服务系统、外挂软件和USBKey硬件的数字证书请求文件进行审批并签发生成对应的后台服务系统数字证书、外挂软件数字证书和USBKey硬件数字证书，所述USB Key硬件数字证书中存储外挂软件接口的授权信息
S110
根据所述USBKey硬件数字证书和所述外挂软件数字证书实现所述USBKey硬件与所述外挂软件之间的身份相互认证
S120
根据所述USBKey硬件数字证书和所述后台服务系统数字证书实现所述USBKey硬件与所述后台服务系统之间的身份相互认证
S130
接收所述外挂软件的业务请求参数，在确定存在有效的会话密钥时实现所述外挂软件与所述后台服务系统之间的数据通信
S140

图2

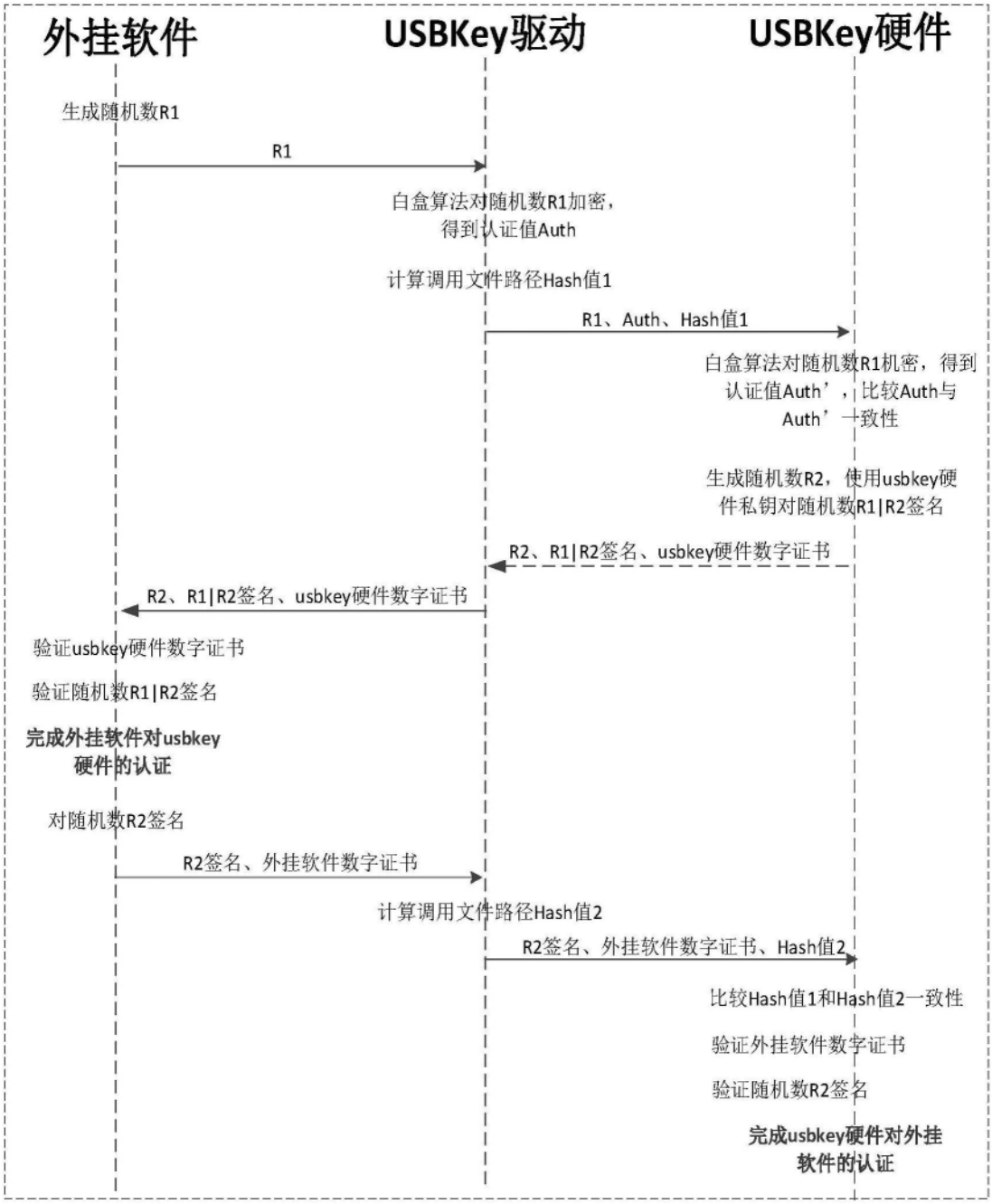
外挂软件
USBKey驱动
USBKey硬件
生成随机数R1
R1
白盒算法对随机数R1加密，
得到认证值Auth
计算调用文件路径Hash值1
R1、Auth、Hash值1
白盒算法对随机数R1机密，得到
认证值Auth'，比较Auth与
Auth'一致性
生成随机数R2，使用usbkey硬
件私钥对随机数R1|R2签名
R2、R1|R2签名、usbkey硬件数字证书
R2、R1|R2签名、usbkey硬件数字证书
验证usbkey硬件数字证书
验证随机数R1|R2签名
完成外挂软件对usbkey
硬件的认证
对随机数R2签名
R2签名、外挂软件数字证书
计算调用文件路径Hash值2
R2签名、外挂软件数字证书、Hash值2
比较Hash值1和Hash值2一致性
验证外挂软件数字证书
验证随机数R2签名
完成usbkey硬件对外挂
软件的认证

图3

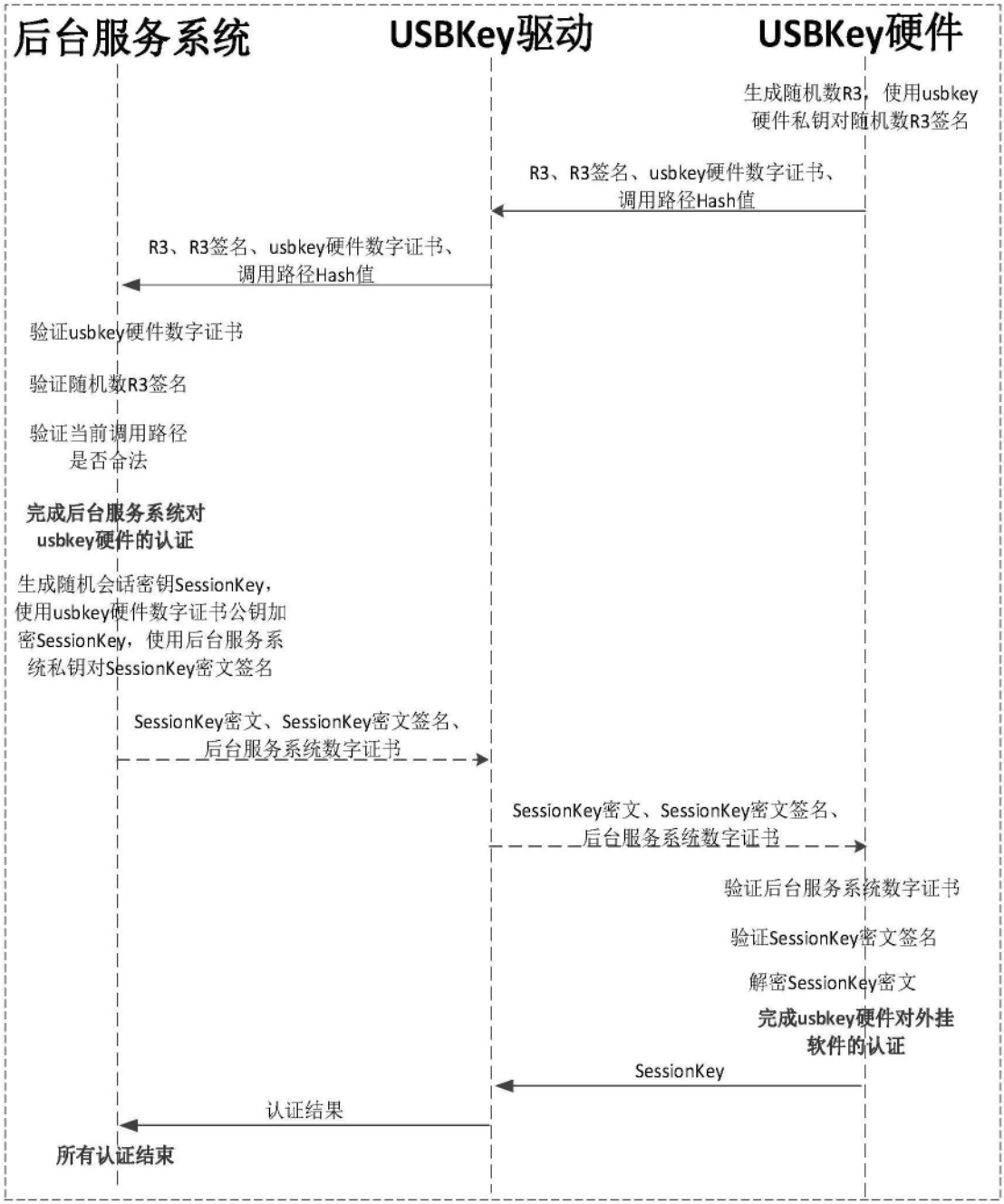
后台服务系统
USBKey驱动
USBKey硬件
生成随机数R3，使用usbkey硬件私钥对随机数R3签名
R3、R3签名、usbkey硬件数字证书、调用路径Hash值
R3、R3签名、usbkey硬件数字证书、调用路径Hash值
验证usbkey硬件数字证书
验证随机数R3签名
验证当前调用路径是否合法
完成后台服务系统对usbkey硬件的认证
生成随机会话密钥SessionKey，使用usbkey硬件数字证书公钥加密SessionKey，使用后台服务系统私钥对SessionKey密文签名
SessionKey密文、SessionKey密文签名、后台服务系统数字证书
SessionKey密文、SessionKey密文签名、后台服务系统数字证书
验证后台服务系统数字证书
验证SessionKey密文签名
解密SessionKey密文
完成usbkey硬件对外挂软件的认证
SessionKey
认证结果
所有认证结束

图4

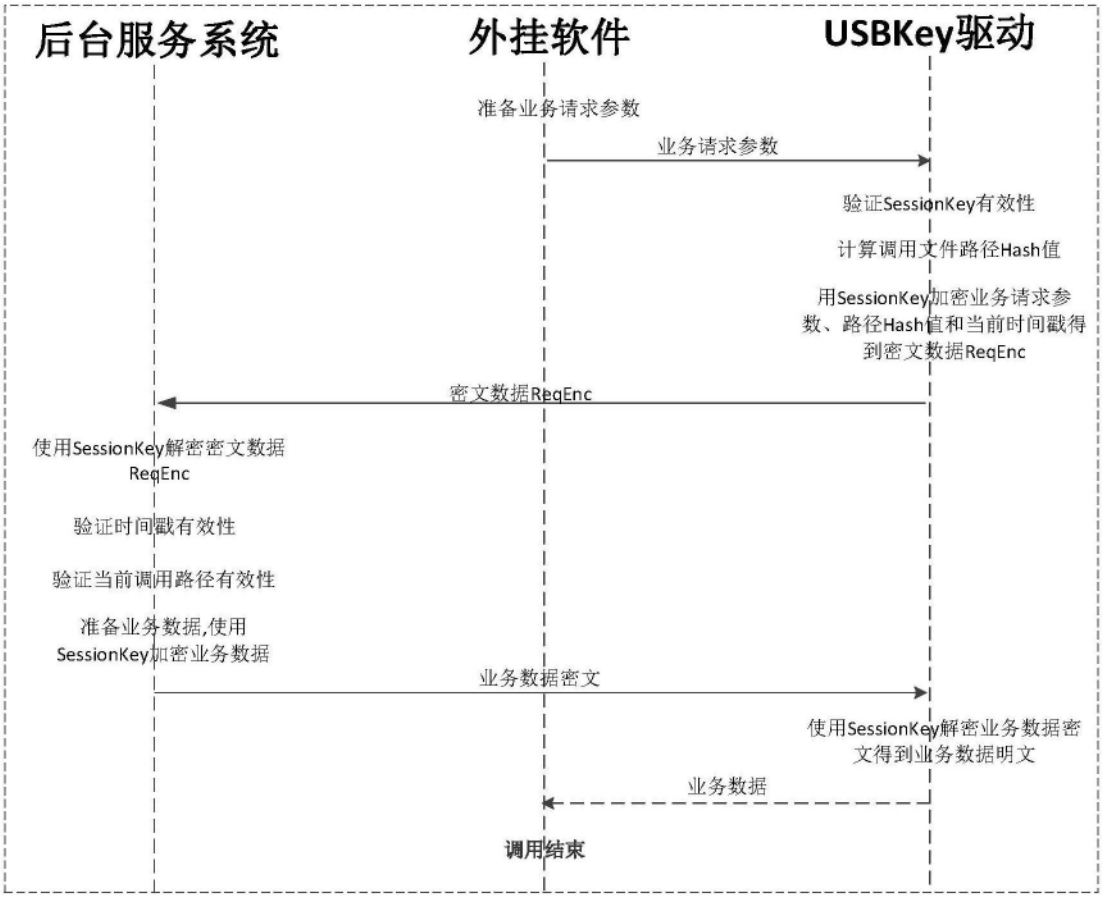
后台服务系统
外挂软件
USBKey驱动
准备业务请求参数
业务请求参数
验证SessionKey有效性
计算调用文件路径Hash值
用SessionKey加密业务请求参数、路径Hash值和当前时间戳得到密文数据ReqEnc
密文数据ReqEnc
使用SessionKey解密密文数据ReqEnc
验证时间戳有效性
验证当前调用路径有效性
准备业务数据,使用SessionKey加密业务数据
业务数据密文
使用SessionKey解密业务数据密文得到业务数据明文
业务数据
调用结束

图5