(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 109257347 A
(43)申请公布日 2019.01.22

(21)申请号 201811049838.4

(22)申请日 2018.09.10

(71)申请人 中国建设银行股份有限公司
地址 100032 北京市西城区金融大街25号

(72)发明人 叶苏诺 陈大平 程明远 王振生 樊广源 肖琳

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/30(2006.01)
H04L 9/32(2006.01)
H04L 9/06(2006.01)

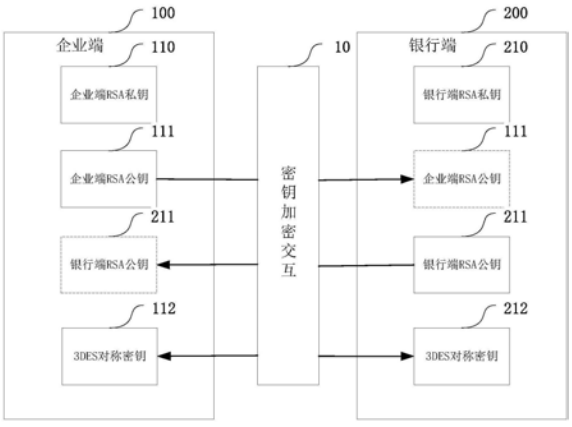
权利要求书2页 说明书9页 附图5页

(54)发明名称

适于银企间数据交互的通信方法和相关装置、存储介质

(57)摘要

本发明提供了一种适于银企间数据交互的通信方法和相关装置、存储介质。其中，所述通信方法包括：银行端和企业端通过专线网络联通，所述银行端和企业端中发送数据的一方作为发送方，接收数据的一方作为接收方；发送方生成一对RSA密钥对，所述RSA密钥对包括RSA公钥和RSA私钥；发送方将RSA公钥进行加密后发送给接收方；接收方接收并解密经发送方加密的RSA公钥；发送方使用密钥对待发送的报文数据进行加密和数字签名，并发送给接收方；接收方使用对应密钥对数据进行解密和验签。实施本发明，能够提高银企系统网间交互的数据传输安全性。



CN 109257347 A

1.一种适于银企间数据交互的通信方法,其特征在于,银行端和企业端通过专线网络联通,所述银行端和企业端中发送数据的一方作为发送方,接收数据的一方作为接收方;

其中,所述通信方法包括:

发送方生成一对RSA密钥对,所述RSA密钥对包括RSA公钥和RSA私钥;

发送方将RSA公钥进行加密后发送给接收方;

发送方使用3DES对称密钥对待发送的报文数据进行加密,并使用所述RSA私钥对原始数据进行数字签名得到签名数据;

发送方将加密后的报文数据和签名数据发送给接收方。

2.如权利要求1所述的通信方法,其特征在于,所述通信方法还包括:

接收方接收所述发送方经加密发送的RSA公钥,并解密得到所述RSA公钥;

接收方接收所述发送方发送的加密后的报文数据和签名数据;

接收方使用3DES对称密钥对报文数据进行解密,使用所述RSA公钥对签名数据进行验签。

3.如权利要求1所述的通信方法,其特征在于,所述通信方法还包括:

发送方和接收方中的一方生成3DES对称密钥,并将生成的3DES对称密钥加密发送给发送方和接收方中的另一方。

4.如权利要求3所述的通信方法,其特征在于,所述通信方法还包括:

所述另一方生接收所述经加密的3DES对称密钥,然后解密得到3DES对称密钥。

5.如权利要求1所述的通信方法,其特征在于,所述待发送报文包括请求内容或响应内容。

6.一种适于银企间数据交互的通信装置,其特征在于,所述通信装置包括:

第一密钥生成模块,用于生成一对RSA密钥对,所述RSA密钥对包括RSA公钥和RSA私钥;

第一密钥发送模块,用于将RSA公钥进行加密后发送给对端;

报文加密模块,使用3DES对称密钥对待发送的报文数据进行加密;

数字签名模块,使用所述RSA私钥对原始数据进行数字签名得到签名数据;

报文发送模块,将加密后的报文数据和签名数据发送给对端。

7.如权利要求6所述的通信装置,其特征在于,所述通信装置还包括:

第一密钥接收模块,用于接收所述对端经加密发送的RSA公钥,并解密得到对端的RSA公钥;

报文接收模块,用于接收对端发送的加密后的报文数据和签名数据;

报文解密模块,使用3DES对称密钥对收到的报文数据进行解密;以及

签名验证模块,使用对端的RSA公钥对收到的签名数据进行验签。

8.如权利要求6所述的通信装置,其特征在于,所述通信装置还包括:

第二密钥生成模块,用于生成3DES对称密钥;

第二密钥发送模块,用于将所述3DES对称密钥加密发送给对端。

9.如权利要求6所述的通信装置,其特征在于,所述通信装置还包括:

第二密钥接收模块,用于接收对端经加密发送的3DES对称密钥,并解密得到所述3DES对称密钥。

10.如权利要求6所述的通信装置,其特征在于,所述待发送报文包括请求内容或响应

内容。

11.一种计算机存储介质，其特征在于，所述计算机存储介质上存储有计算机可读指令，该所述计算机可读指令被处理器执行时所述处理器进行权利要求1-5任意一项所述的方法所述的操作。

12.一种通信设备，其特征在于，所述通信设备包括：

存储器，存储有计算机可读指令；

处理器，执行所述计算机可读指令以进行权利要求1-5任意一项所述的方法所述的操作。

适于银企间数据交互的通信方法和相关装置、存储介质

技术领域

[0001] 本发明涉及通信领域，更为具体而言，涉及一种适于银企间数据交互的通信方法和相关装置、存储介质。

背景技术

[0002] 传统的，当企业客户ERP(企业资源计划)系统与银行系统交互时，往往需要借助安全硬件来完成数据加解密，数字签名等操作。客户对数字信息进行签名一般都在客户端USB KEY内执行：将摘要信息用客户USB KEY内的私钥加密，与信息原文一起传送给服务端。服务端使用客户的公钥解密被加密的摘要信息，然后用哈希函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。然而使用硬件USB KEY进行数字签名往往成为系统交互的效率瓶颈，无法灵活进行密钥变更，以及硬件设备使用寿命等局限性。

[0003] 随着互联网的快速发展，原始的银企(非直联)合作方式，例如使用银行的网银系统B/S模式(浏览器/服务器模式)或通过银行网点进行企业账务处理后，再与企业财务系统进行人工落地对接处理的业务流程，将导致企业业务处理不连贯，工作效率低，并且在保证银行系统与企业财务系统账务一致性问题上存在风险。

[0004] 银企直联可以彻底解决以上弊端，同时银企直联系统利用成熟的商密技术，实现客户系统与银行系统间的身份认证、安全加密、数字签名等各方面的安全需求，向客户提供不间断的银行服务，实现了企业ERP或财务系统业务操作的7*24连续性，针对有特殊要求的客户也可量身定制个性化的应用服务。为满足各类型客户的银企直联需求，银行系统需提供功能全面、接口规范统一、接入方式灵活方便的银企直连服务系统给企业客户使用。

[0005] 然而银企直连双方，无论是银行端服务系统和客户ERP系统都面临着相同的安全问题，如何快速、安全识别对端身份，保证银企系统间数据传输的机密和完整已经成为企业管理者面临的核心问题之一。

发明内容

[0006] 为解决上述技术问题，本发明提供了一种适于银企间数据交互的通信方法和相关装置、存储介质，通过专线网络联通银企双系统，银企双方各自生成的RSA密钥对，其中RSA公钥加密互换，并且3DES对称密钥加密传输，在交换数据时发送方和接收方分别利用3DES对称密钥进行加密和解密，签名时利用各自生成的RSA私钥进行签名，以及通过解密收到的对端RSA公钥进行验签，从而实现了一种不依赖于硬件密码芯片，而是基于专线与网络访问权限控制，结合软加密以及数字签名的多层次、全方位的银企交互安全保障策略。

[0007] 根据本发明实施方式的第一面，提供了一种适于银企间数据交互的通信方法，包括：银行端和企业端通过专线网络联通，所述银行端和企业端中发送数据的一方作为发送方，接收数据的一方作为接收方；其中，所述通信方法包括：发送方生成一对RSA密钥对，所述RSA密钥对包括RSA公钥和RSA私钥；发送方将RSA公钥进行加密后发送给接收方；发送方使用3DES对称密钥对待发送的报文数据进行加密，并使用所述RSA私钥对原始数据进行数

字签名得到签名数据;发送方将加密后的报文数据和签名数据发送给接收方。

[0008] 在本发明的一些实施方式中,所述通信方法还包括:接收方接收所述发送方经加密发送的RSA公钥,并解密得到所述RSA公钥;接收方接收所述发送方发送的加密后的报文数据和签名数据;接收方使用3DES对称密钥对报文数据进行解密,使用所述RSA公钥对签名数据进行验签。

[0009] 在本发明的一些实施方式中,所述通信方法还包括:发送方和接收方中的一方生成3DES对称密钥,并将生成的3DES对称密钥加密发送给发送方和接收方中的另一方。

[0010] 在本发明的一些实施方式中,所述通信方法还包括:所述另一方接收所述经加密的3DES对称密钥,然后解密得到3DES对称密钥。

[0011] 在本发明的一些实施方式中,所述待发送报文包括请求内容或响应内容。

[0012] 根据本发明实施方式的第二方面,提供了一种适于银企间数据交互的通信装置,所述通信装置包括:第一密钥生成模块,用于生成一对RSA密钥对,所述RSA密钥对包括RSA公钥和RSA私钥;第一密钥发送模块,用于将RSA公钥进行加密后发送给对端;报文加密模块,使用3DES对称密钥对待发送的报文数据进行加密;数字签名模块,使用所述RSA私钥对原始数据进行数字签名得到签名数据;报文发送模块,将加密后的报文数据和签名数据发送给对端。

[0013] 在本发明的一些实施方式中,所述通信装置还包括:第一密钥接收模块,用于接收所述对端经加密发送的RSA公钥,并解密得到对端的RSA公钥;报文接收模块,用于接收对端发送的加密后的报文数据和签名数据;报文解密模块,使用3DES对称密钥对收到的报文数据进行解密;以及签名验证模块,使用所述对端的RSA公钥对收到的签名数据进行验签。

[0014] 在本发明的一些实施方式中,所述通信装置还包括:第二密钥生成模块,用于生成3DES对称密钥;第二密钥发送模块,用于将所述3DES对称密钥加密发送给对端。

[0015] 在本发明的一些实施方式中,所述通信装置还包括:第二密钥接收模块,用于接收对端经加密发送的3DES对称密钥,并解密得到所述3DES对称密钥。

[0016] 在本发明的一些实施方式中,所述待发送报文包括请求内容或响应内容。

[0017] 根据本发明实施例的第三方面,提供一种计算机可读存储介质,所述计算机存储介质上存储有计算机可读指令,其中,所述计算机可读指令被处理器执行时,使得计算机执行如下操作:所述操作包括如上中任意一项所述银企间数据交互的通信方法所包含的步骤。

[0018] 根据本发明实施例的第四方面,提供一种适于银企间数据交互的通信装置,所述通信装置包括:存储器,存储有计算机可读指令;处理器,执行所述计算机可读指令以执行如上所述银企间数据交互的通信方法所包含的步骤。

[0019] 本发明实施方式提供的适于银企间数据交互的通信方法、相关装置和存储介质,通过采用安全密码算法、数字证书、数字签名、访问控制等技术,实现了银企系统交互身份认证安全、数据传输安全、数据存储安全、数据加密安全、密钥调用安全等关键技术功能,构建了银企系统网间交互的可信安全服务体系。

附图说明

[0020] 图1是根据本发明实施方式所适用的场景示意图;

[0021] 图2是根据本发明一种实施方式中实现银企双方密钥交互的示意图；

[0022] 图3是根据本发明一种实施方式中实现银企双方密钥交互中的密钥加密交互方法的流程示意图；

[0023] 图4是根据本发明一种实施方式的用于企业端向银行端发送请求报文以及银行端向企业端返回响应报文的通信方法的示意图；

[0024] 图5是根据本发明一种实施方式的用于银行端向企业端发送请求报文以及企业端向银行端返回响应报文的通信方法的示意图；

[0025] 图6是根据本发明一种实施方式的用于银企间数据交互的通信装置的结构示意图。

具体实施方式

[0026] 以下结合附图和具体实施方式对本发明的各个方面进行详细阐述。其中，众所周知的模块、单元及其相互之间的连接、链接、通信或操作没有示出或未作详细说明。并且，所描述的特征、架构或功能可在一个或一个以上实施方式中以任何方式组合。本领域技术人员应当理解，下述的各种实施方式只用于举例说明，而非用于限制本发明的保护范围。还可以容易理解，本文所述和附图所示的各实施方式中的模块或单元或处理方式可以按各种不同配置进行组合和设计。

[0027] 下面对本文中使用的术语进行简要说明。

[0028] ERP,Enterprise Resource Planning企业资源计划

[0029] USB,Universal Serial Bus通用串行总线

[0030] QoS,Quality of Service服务质量

[0031] IP,Internet Protocol网络之间互连的协议

[0032] 3DES,TDEA,Triple Data Encryption Algorithm三重数据加密算法。

[0033] RSA,公钥加密算法。

[0034] MD5WithRSA,结合MD5与RSA的签名算法。

[0035] 图1是根据本发明实施方式所适用的场景示意图。

[0036] 其中，银行端和企业端通过专线网络联通。网络专线就是为某个机构拉一条独立的网线，也就是一个独立的局域网，让用户的数据传输变得可靠可信，专线的优点就是安全性好，QoS可以得到保证。通过网络访问权限控制，限制发起方的IP地址，规定访问端口，只有在合法范围内的访问才能接入系统。从而在访问权限控制方面，在基础网络层面保障银企系统网间交互的数据传输的安全和对客户身份的严格把关。

[0037] 其中，企业端100包括业务模块101和传输模块102，银行端200包括银行内部业务逻辑201和接入接出模块202。其中，传输模块都包括：密钥加密交互模块10、签名验签模块11、加密解密模块12以及通讯模块。银企双方通过各自的传输模块将业务模块中的各种请求以及响应做交互，实现银企间的通信。

[0038] 图2是根据本发明一种实施方式中实现银企双方密钥交互的示意图。

[0039] 其中，企业端100和企业端200各自生成一对RSA密钥对，企业端RSA密钥对包括企业端RSA私钥110和企业端RSA公钥111，银行端RSA密钥对包括银行端RSA私钥210和银行端RSA公钥211，企业端和银行端将各自生成的RSA公钥通过密钥加密交互模块10发送给对端，

此外，企业端和银行端还包括3DES对称密钥，所述3DES对称密钥可以由企业端或者银行端生成，并且，企业端和银行端其中一端生成3DES对称密钥后将该对称密钥通过密钥加密交互10发送给另一端。

[0040] 在本发明的实施方式中，图2中密钥加密交互模块10即图1中企业端和银行端传输模块中的密钥加密交互模块10。

[0041] 图3是根据本发明一种实施方式中实现银企双方密钥交互中的密钥加密交互方法的流程示意图。

[0042] 在本发明的实施方式中，图2中密钥加密交互模块10的具体操作方法即图3所示实现银企双方密钥交互中密钥加密交互的方法。

[0043] 如图3所示，本发明的一种实施方式中用于实现银企双方密钥交互中的密钥加密交互方法可包括：处理S31和处理S32，下面对上述的处理进行具体的描述。

[0044] 在处理S31中，使用双方约定的特定规则的密钥，使用DES加密算法做加密后传输。其中，双方约定的特定规则的密钥可以使用国际通用密钥，从而降低系统双方的开发难度，并且支持线上实时变更密钥，简化了密钥变更的流程，降低了密钥泄露的风险。

[0045] 在处理S32中，使用双方约定的特定规则的密钥，使用DES解密算法进行解密。其中，双方约定的特定规则的密钥可以使用国际通用密钥，从而降低系统双方的开发难度，并且支持线上实时变更密钥，简化了密钥变更的流程，降低了密钥泄露的风险。

[0046] 在本发明的实施方式中，企业端RSA公钥、银行端RSA公钥和3DES对称密钥的加密发送即通过图3所述的方法做密钥交互。

[0047] 图4是根据本发明一种实施方式的用于企业端向银行端发送请求报文以及银行端向企业端返回响应报文的示意图。

[0048] 如图4所示，本发明一种实施方式的用于企业端向银行端发送请求报文以及银行端向企业端返回响应报文的通信方法可包括：处理S11、处理S12、处理S13、处理S14、处理S15、处理S16、处理S17、处理S18、处理S19、处理S20、处理S21、处理S22和处理S23，下面对上述的处理进行具体描述。

[0049] 如图4所示，企业端100为处理业务模块101中的业务，首先使用企业端RSA私钥110对请求报文做请求报文数字签名处理S11，得到签名数据，其次企业端100做发送签名数据处理S12，将签名数据发送给银行端200，随后企业端使用由银行端生成并加密发送，由企业端解密得到的3DES对称密钥(或由企业端生成的3DES对称密钥)对企业端将要发送的请求报文做请求报文加密处理S13，得到加密报文，企业端100做发送加密报文处理S14，将加密报文发送给银行端200。

[0050] 在本发明的实施方式中，请求报文数字签名处理S11包括：企业端通过使用企业端生成的企业端RSA私钥110对待发送的请求报文用MD5WithRSA签名算法做数字签名，得到签名数据。

[0051] 在本发明的实施方式中，请求报文的报文加密处理S13包括：企业端将待发送的报文数据使用企业端解密得到的银行端生成的3DES对称密钥(或企业端生成的3DES对称密钥)并应用3DES算法进行报文加密，得到加密报文。

[0052] 在本发明的可选实施方式中，处理S11、S12和处理S13、S14的顺序可以改变。即企业端可以先做处理S13和S14，后做处理S11和S12，也可以在做处理S11和S12的同时做处理

S13和S14。

[0053] 在处理S15中，银行端200接收加密报文并解密，其方法可以为：银行端200使用银行端生成的3DES对称密钥212(或解密得到的企业端生成的3DES对称密钥112)并应用3DES算法对加密报文进行解密。

[0054] 在处理S16中，银行端200接收签名数据并验签，其方法可以为：银行端200使用解密得到的企业端RSA公钥111对接收到的数字签名数据使用MD5WithRSA算法进行验签。此时，银行端200得到企业端100发送的请求报文。

[0055] 在处理S17中，银行端200根据企业端100发送的请求报文产生响应报文。

[0056] 在处理S18中，银行端200对响应报文做数字签名，其方法可以为：银行端200通过使用银行端生成的银行端私钥210对待返回企业端的响应报文用MD5WithRSA签名算法做数字签名，得到签名数据。

[0057] 在处理S19中，银行端200将签名数据发送给企业端100。

[0058] 在处理S20中，银行端200对响应报文做报文加密，其方法可以为：银行端200使用银行端生成的3DES对称密钥212(或解密得到的企业端生成的3DES对称密钥112)并使用3DES算法对银行端将要返回企业端的响应报文做报文加密，得到加密报文。

[0059] 在处理S21中，银行端200将加密报文发送给企业端100。

[0060] 在本发明的可选实施方式中，处理S18、S19和处理S20、S21的顺序可以改变。即企业端可以先做处理S18和S19，后做处理S20和S21，也可以在做处理S18和S19的同时做处理S20和S21。

[0061] 在处理S22中，企业端100接收银行端200发送的加密报文并解密，其方法可以为：企业端100使用解密得到的银行端生成的3DES对称密钥212(或企业端生成的3DES对称密钥112)并应用3DES算法对加密报文进行解密。

[0062] 在处理S23中，企业端100接收银行端200发送的签名数据并验签，其方法可以为：企业端100使用解密得到的银行端RSA公钥211对接收到的数字签名数据使用MD5WithRSA算法进行验签。此时，企业端根据解密及验签结果得到了银行端对企业端发送的请求的响应内容。

[0063] 在本发明的实施方式中，每当企业端需要执行业务模块中的各项业务时，只需重复上述S11至S23的步骤即可。

[0064] 图5是根据本发明一种实施方式的用于银行端向企业端发送请求报文以及企业端向银行端返回响应报文的通信方法的示意图。

[0065] 如图5所示，本发明一种实施方式的用于企业端向银行端发送请求报文以及银行端向企业端返回响应报文的通信方法可包括：处理S31、处理S32、处理S33、处理S34、处理S35、处理S36、处理S37、处理S38、处理S39、处理S40、处理S41、处理S42和处理S43，下面对上述的处理进行具体描述。

[0066] 在处理S31中，银行端200对请求报文做数字签名，其方法可以为：银行端200通过使用银行端生成的银行端私钥210对待发送给企业端的请求报文用MD5WithRSA签名算法做数字签名，得到签名数据。

[0067] 在处理S32中，银行端200将签名数据发送给企业端100。

[0068] 在处理S33中，银行端200对请求报文做报文加密，其方法可以为：银行端200使用

银行端生成的3DES对称密钥212(或解密得到的企业端生成的3DES对称密钥112)并使用3DES算法对银行端将要发送给企业端的请求报文做报文加密,得到加密报文。

[0069] 在处理S34中,银行端200将加密报文发送给企业端100。

[0070] 在本发明的可选实施方式中,处理S31、S32和处理S33、S34的顺序可以改变。即企业端可以先做处理S31和S32,后做处理S33和S34,也可以在做处理S31和S32的同时做处理S33和S34。

[0071] 在处理S35中,企业端100接收加密报文并解密,其方法可以为:企业端100使用解密得到的银行端生成的3DES对称密钥212(或企业端生成的3DES对称密钥112)并应用3DES算法对加密报文进行解密。

[0072] 在处理S36中,企业端100接收签名数据并验签,其方法可以为:企业端100使用解密得到的银行端RSA公钥211对接收到的数字签名数据使用MD5WithRSA算法进行验签。此时,企业端100得到银行端200发送的请求报文。

[0073] 在处理S37中,企业端100根据银行端200发送的请求报文产生响应报文。

[0074] 在处理S38中,企业端100对响应报文做数字签名,其方法可以为:企业端100通过使用企业端生成的企业端私钥110对待返回企业端的响应报文用MD5WithRSA签名算法做数字签名,得到签名数据。

[0075] 在处理S39中,企业端100将签名数据发送给银行端200。

[0076] 在处理S40中,企业端100对响应报文做报文加密,其方法可以为:企业端100使用解密得到的银行端生成的3DES对称密钥212(或企业端生成的3DES对称密钥112)并使用3DES算法对企业端将要返回银行端的响应报文做报文加密,得到加密报文。

[0077] 在处理S41中,企业端100将加密报文发送给银行端200。

[0078] 在本发明的可选实施方式中,处理S38、S39和处理S40、S41的顺序可以改变。即企业端可以先做处理S38和S39,后做处理S40和S41,也可以在做处理S38和S39的同时做处理S40和S41。

[0079] 在处理S42中,银行端接收企业端100发送的加密报文并解密,其方法可以为:银行端200使用银行端生成的3DES对称密钥212(或解密得到的企业端生成的3DES对称密钥112)并应用3DES算法对加密报文进行解密。

[0080] 在处理S43中,银行端200接收企业端100发送的签名数据并验签,其方法可以为:银行端200使用解密得到的企业端RSA公钥111对接收到的数字签名数据使用MD5WithRSA算法进行验签。此时,银行端根据解密及验签结果得到了企业端对银行端发送的请求的响应内容。

[0081] 在本发明的实施方式中,每当银行端需要执行业务模块中的各项业务时,只需重复上述S31至S43的步骤即可。

[0082] 根据本发明的通信方法,银行端和企业端通过专线网络联通,银企间数据传输时利用多种软加密算法和数字签名算法的组合,并通过对密钥互换的过程中使用加密传输的方法,使得攻击者无法对传输数据进行篡改或伪装,保证了银企系统网间交互的核心安全问题,同时,减少了客户使用硬件介质的繁琐问题,提高了系统效率。

[0083] 图6是根据本发明一种实施方式的用于银企间数据交互的通信装置的结构示意图。所述通信装置布置在银行端和企业端。

[0084] 参见图6,所述通信装置可包括:

[0085] 第一密钥生成模块301,用于生成一对RSA密钥对,所述RSA密钥对包括RSA公钥和RSA私钥;

[0086] 第一密钥发送模块302,用于将生成的RSA公钥加密发送给对端系统;

[0087] 第二密钥生成模块303,用于生成3DES对称密钥;

[0088] 第二密钥发送模块304,用于将生成的3DES对称密钥加密发送给对端系统;

[0089] 第一密钥接收模块305,用于接收对端经加密发送的RSA公钥,并解密得到对端RSA公钥;

[0090] 第二密钥接收模块306,用于接收对端经加密发送的3DES对称密钥,并解密得到所述3DES对称密钥;

[0091] 数字签名模块307,用由第一密钥生成模块301生成的所述RSA私钥对原始数据进行数字签名得到签名数据;

[0092] 报文加密模块308,使用由第二密钥生成模块303生成的3DES对称密钥对待发送的报文数据进行加密得到加密报文;

[0093] 报文发送模块309,将数字签名模块和报文加密模块得到的签名数据和加密报文发送给对端系统;

[0094] 报文接收模块310,用于接收对端报文发送模块发送的签名数据和加密报文;

[0095] 报文解密模块311,使用3DES对称密钥对收到的报文数据进行解密;

[0096] 签名认证模块312,使用所述对端RSA公钥对接收的签名数据进行验签。

[0097] 在本发明的一种实施方式中,对照图1中的各模块,图6中的第一密钥发送模块302、第二密钥发送模块304、第一密钥接收模块305和第二密钥接收模块306可对应分布于图1中的密钥加密交互模块10;图6中的数字签名模块307和签名验证模块312可对应分布于图1中的签名验签模块11;图6中的报文加密模块308和报文解密模块311可对应分布于图1中的加密解密模块12。

[0098] 在本发明的实施方式中,第一密钥发送模块303和第二密钥发送模块304中加密发送的方法可以为:使用银企双方约定的特定规则的密钥,使用DES加密算法做加密后传输。其中,双方约定的特定规则的密钥可以使用国际通用密钥,从而降低系统双方的开发难度,并且支持线上实时变更密钥,简化了密钥变更的流程,降低了密钥泄露的风险。

[0099] 在本发明的实施方式中,第一密钥接收模块305和第二密钥接收模块306中解密的方法可以为:使用双方约定的特定规则的密钥,使用DES解密算法进行解密。其中,双方约定的特定规则的密钥可以使用国际通用密钥,从而降低系统双方的开发难度,并且支持线上实时变更密钥,简化了密钥变更的流程,降低了密钥泄露的风险。

[0100] 在本发明的实施方式中,数字签名模块307中签名方法可以为:过使用第一密钥生成模块301生成的RSA私钥对原始数据使用MD5WithRSA签名算法做数字签名,得到签名数据。

[0101] 在本发明的实施方式中,报文加密模块308中报文加密方法可以为:将待发送的报文数据使用第二密钥生成模块303生成的3DES对称密钥(或第二密钥接收模块解密得到的3DES对称密钥)并应用3DES算法进行加密,得到加密报文。

[0102] 在本发明的实施方式中,报文解密模块311中解密方法可以为:使用第二密钥生成

模块303生成的3DES对称密钥(或第二密钥接收模块解密得到的3DES对称密钥)并应用3DES算法对加密报文进行解密。

[0103] 在本发明的实施方式中,签名认证模块312中验签方法可以为:使用第一密钥接收模块305得到的对端RSA公钥对接收到的加密后的数字签名数据使用MD5WithRSA算法进行验签。

[0104] 在本发明的实施方式中,当实现的是企业端向银行端发送请求以及银行端向企业端发送响应的过程时,首先银企双方的第一密钥生成模块生成各自的RSA密钥对;其中,各自生成的RSA公钥通过第一密钥发送模块发送给对端;对端通过第一密钥接收模块得到解密后的对端RSA公钥;银行端通过第二密钥生成模块生成3DES对称密钥(或企业端通过第二密钥生成模块生成3DES对称密钥);银行端通过第二密钥发送模块将加密后的3DES对称密钥发送给企业端(或企业端通过第二密钥发送模块将加密后的3DES对称密钥发送给银行端);企业端通过第二密钥接收模块得到解密后的3DES对称密钥(或银行端通过第二密钥接收模块得到解密后的3DES对称密钥);企业端通过报文加密模块对所以发送的请求进行报文加密得到加密报文;企业端通过数字签名模块对请求进行签名得到签名数据;企业端通过报文发送模块将加密报文和签名数据发送给银行端;银行端通过报文接收模块接收企业端发送的加密报文和签名数据;银行端通过报文解密模块对企业端发送的加密报文进行解密;银行端通过签名认证模块对企业端发送的签名数据进行解密验签;银行端经过验签后将结果作为响应内容,通过银行端的报文加密模块将响应内容进行加密得到加密报文;银行端通过数字签名模块对响应内容进行数字签名得到签名数据;银行端通过报文发送模块将加密报文和签名数据发送给企业端;企业端通过报文接收模块,接收银行端发送的加密报文及签名数据;企业端通过报文解密模块对收到的加密报文进行解密;企业端通过签名认证模块对收到的签名数据进行验签,得到银行端的响应内容。

[0105] 本发明的另一种实施方式中实现的是银行端向企业端发送请求以及企业端向银行端发送响应的过程。该过程包括:首先银企双方的第一密钥生成模块生成各自的RSA密钥对;其中,各自生成的RSA公钥通过第一密钥发送模块发送给对端;对端通过第一密钥接收模块得到解密后的对端RSA公钥;银行端通过第二密钥生成模块生成3DES对称密钥(或企业端通过第二密钥生成模块生成3DES对称密钥);银行端通过第二密钥发送模块将加密后的3DES对称密钥发送给企业端(或企业端通过第二密钥发送模块将加密后的3DES对称密钥发送给银行端);企业端通过第二密钥接收模块得到解密后的3DES对称密钥(或银行端通过第二密钥接收模块得到解密后的3DES对称密钥);银行端通过报文加密模块对所以发送的请求进行报文加密得到加密报文;银行端通过数字签名模块对请求进行签名得到签名数据;银行端通过报文发送模块将加密报文和签名数据发送给企业端;企业端通过报文接收模块接收银行端发送的加密报文和签名数据;企业端通过报文解密模块对银行端发送的加密报文进行解密;企业端通过签名认证模块对银行端发送的签名数据进行解密验签;企业端经过验签后将结果作为响应内容,通过企业端的报文加密模块将响应内容进行加密得到加密报文;企业端通过数字签名模块对响应内容进行数字签名得到签名数据;企业端通过报文发送模块将加密报文和签名数据发送给银行端;银行端通过报文接收模块,接收企业端发送的加密报文及签名数据;银行端通过报文解密模块对收到的加密报文进行解密;银行端通过签名认证模块对收到的签名数据进行验签,得到企业端的响应内容。

[0106] 通过上述实施例中的方法，可以保证银企系统双方身份认证，以及数据传输的安全性。

[0107] 另外，本发明还提供一种计算机可读存储介质，所述计算机存储介质上存储有计算机可读指令，其中，所述计算机可读指令被处理器执行时，使得计算机执行如下操作：所述操作包括如上中任意一项所述银企间数据交互的通信方法所包含的步骤，在此不再赘述。其中，所述存储介质可以包括：例如，光盘、硬盘、软盘、闪存、磁带等。

[0108] 另外，本发明还提供一种适于银企间数据交互的通信装置，所述通信装置包括：存储器，存储有计算机可读指令；处理器，执行所述计算机可读指令以执行如上所述银企间数据交互的通信方法所包含的步骤。所述通信装置可以是，例如，服务器、台式计算机、笔记本计算机、平板电脑等。

[0109] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件结合硬件平台的方式来实现。基于这样的理解，本发明的技术方案对背景技术做出贡献的全部或者部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例或者实施例的某些部分所述的方法。

[0110] 本发明说明书中使用的术语和措辞仅仅为了举例说明，并不意味构成限定。本领域技术人员应当理解，在不脱离所公开的实施方式的基本原理的前提下，对上述实施方式中的各细节可进行各种变化。因此，本发明的范围只由权利要求确定，在权利要求中，除非另有说明，所有的术语应按最宽泛合理的意思进行理解。

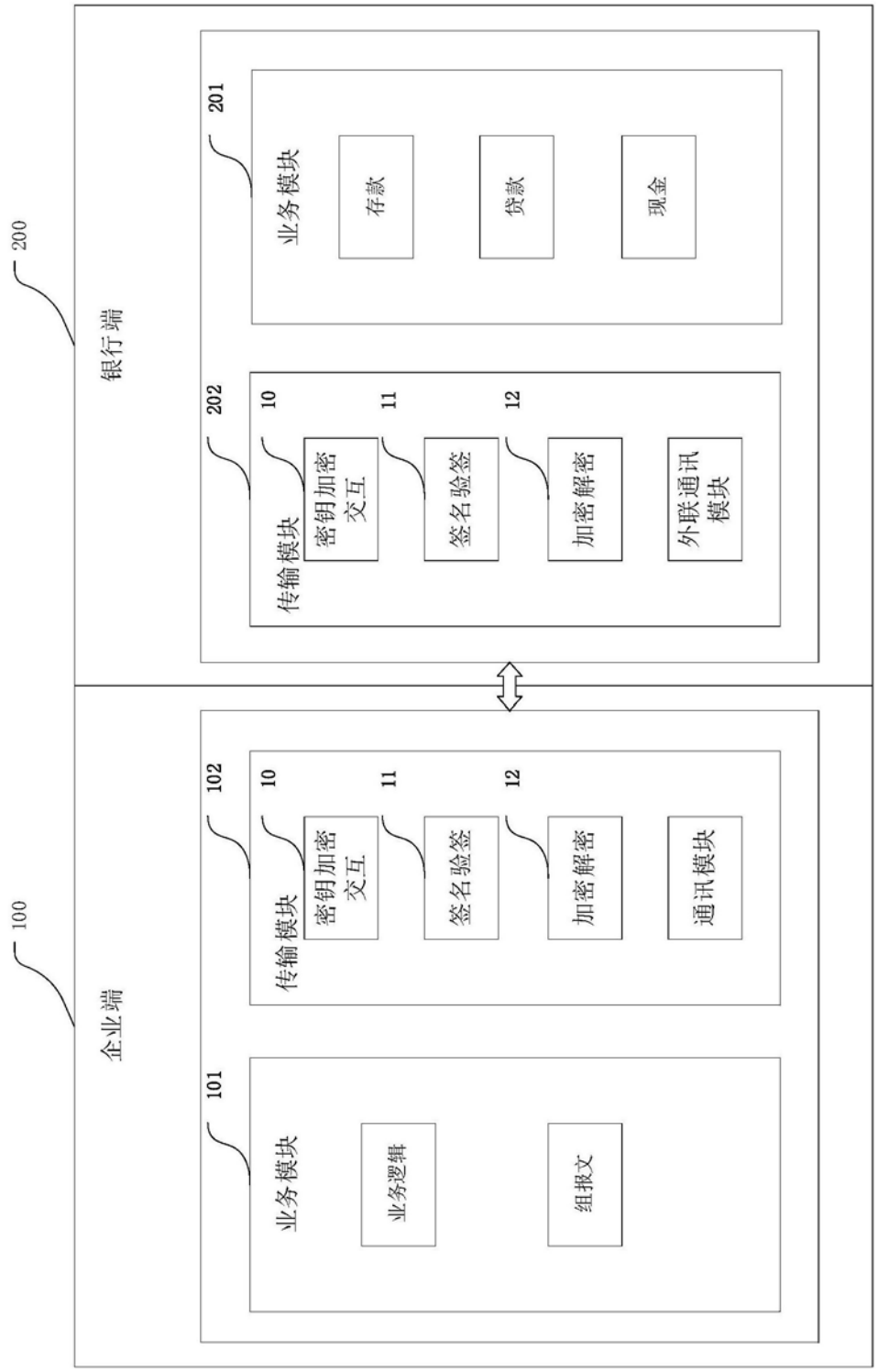

200
银行端
201
业务模块
存款
贷款
现金
202
传输模块
10
密钥加密交互
11
签名验签
12
加密解密
外联通讯模块
100
企业端
102
传输模块
10
密钥加密交互
11
签名验签
12
加密解密
通讯模块
101
业务模块
业务逻辑
组报文

图1

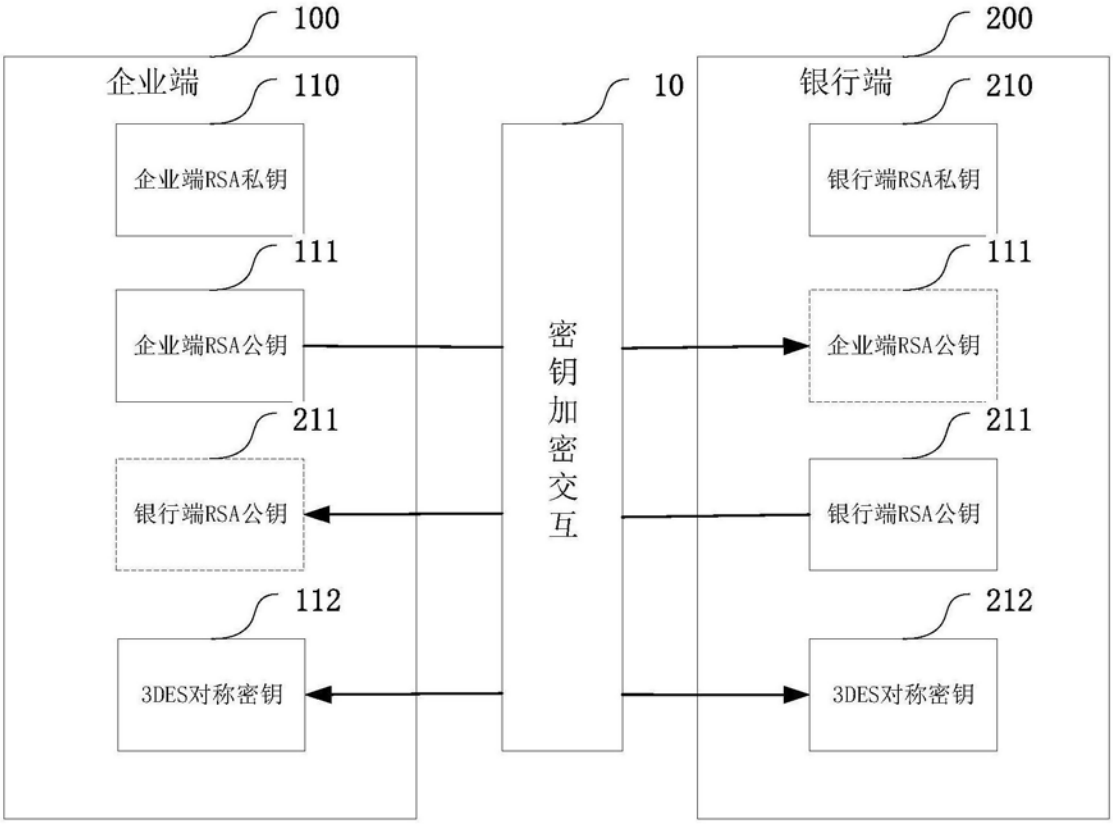

100
企业端
110
企业端RSA私钥
111
企业端RSA公钥
211
银行端RSA公钥
112
3DES对称密钥
10
密钥加密交互
200
银行端
210
银行端RSA私钥
111
企业端RSA公钥
211
银行端RSA公钥
212
3DES对称密钥

图2

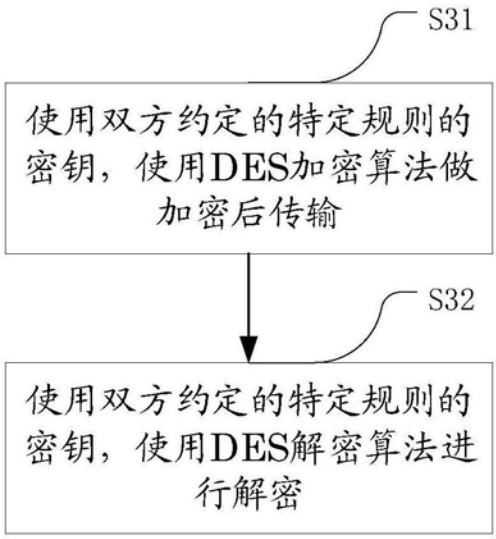

S31
使用双方约定的特定规则的密钥，使用DES加密算法做加密后传输
S32
使用双方约定的特定规则的密钥，使用DES解密算法进行解密

图3

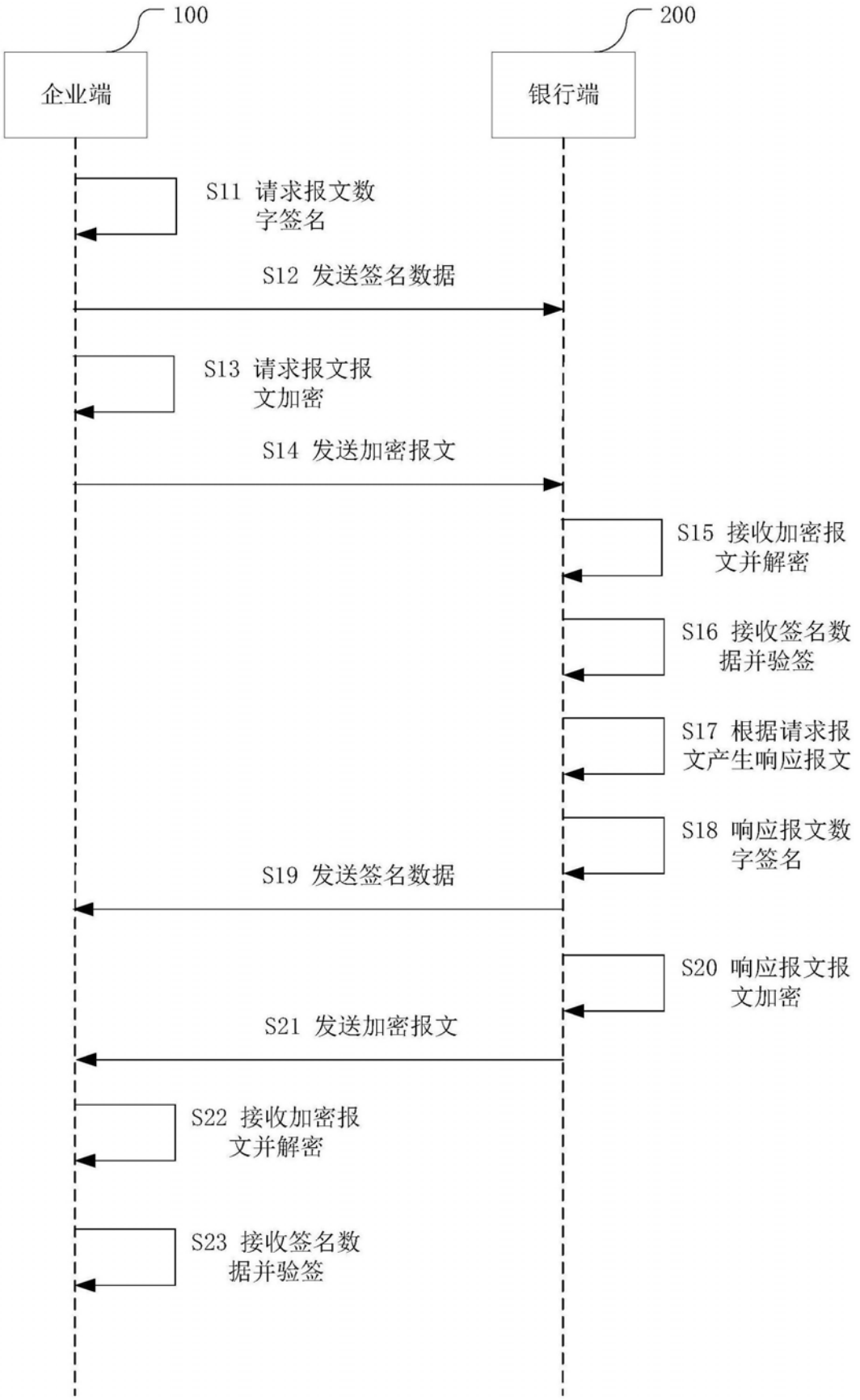

100
200
企业端
银行端
S11 请求报文数字签名
S12 发送签名数据
S13 请求报文报文加密
S14 发送加密报文
S15 接收加密报文并解密
S16 接收签名数据并验签
S17 根据请求报文产生响应报文
S18 响应报文数字签名
S19 发送签名数据
S20 响应报文报文加密
S21 发送加密报文
S22 接收加密报文并解密
S23 接收签名数据并验签

图4

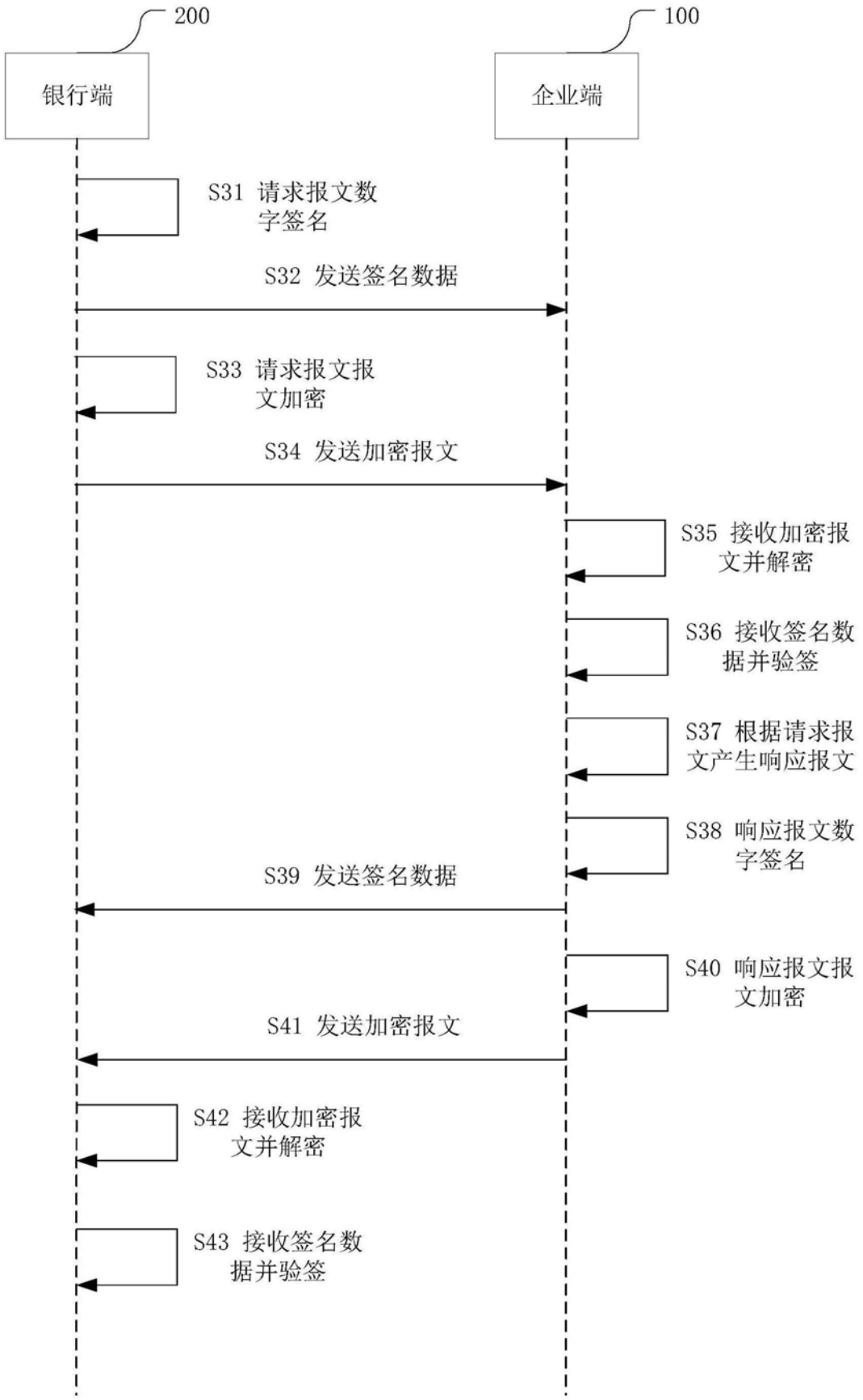

200
100
银行端
企业端
S31 请求报文数字签名
S32 发送签名数据
S33 请求报文报文加密
S34 发送加密报文
S35 接收加密报文并解密
S36 接收签名数据并验签
S37 根据请求报文产生响应报文
S38 响应报文数字签名
S39 发送签名数据
S40 响应报文报文加密
S41 发送加密报文
S42 接收加密报文并解密
S43 接收签名数据并验签

图5

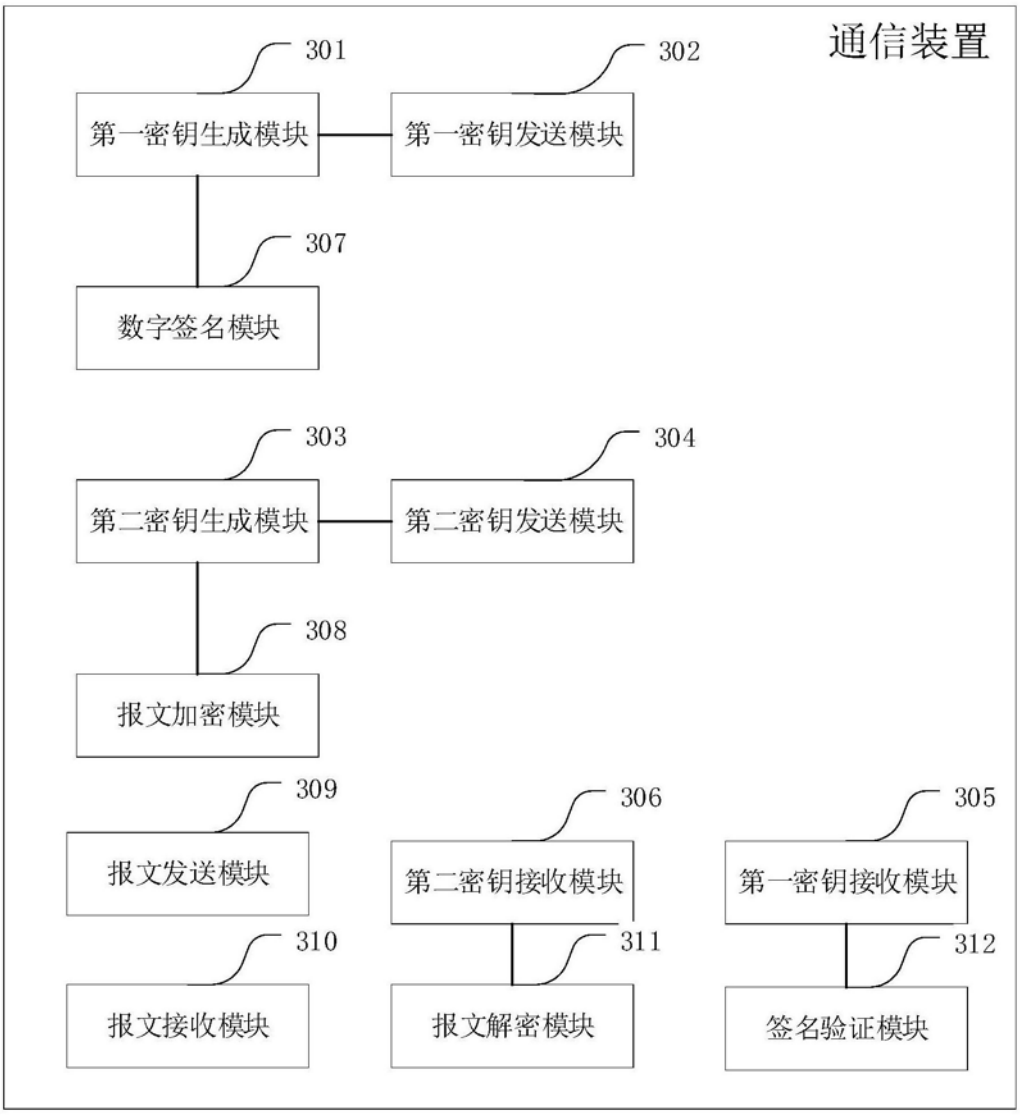

通信装置
301
第一密钥生成模块
302
第一密钥发送模块
307
数字签名模块
303
第二密钥生成模块
304
第二密钥发送模块
308
报文加密模块
309
报文发送模块
306
第二密钥接收模块
305
第一密钥接收模块
310
报文接收模块
311
报文解密模块
312
签名验证模块

图6