[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 9/14 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810035274.9

[43] 公开日 2008 年 8 月 20 日

[11] 公开号 CN 101247232A

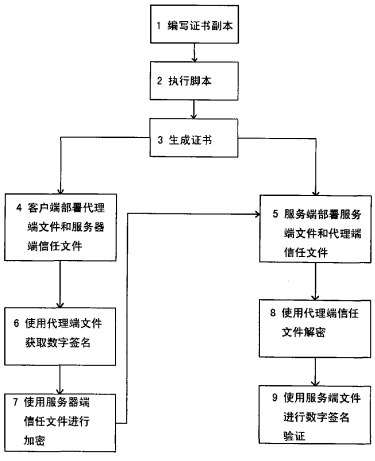
[22] 申请日 2008.3.27
[21] 申请号 200810035274.9
[71] 申请人 上海金鑫计算机系统工程有限公司
地址 200040 上海市静安区南京西路 1486 号 3 号楼 7 层
[72] 发明人 计岩平 陈 铭 袁文聪 童 茵 陈 任 张 彬 李晓丹
[74] 专利代理机构 北京英特普罗知识产权代理有限公司
代理人 童素珠
权利要求书 6 页 说明书 19 页 附图 5 页

[54] 发明名称

数据交换传输中基于数字签名的加密技术方法

[57] 摘要

一种涉及信息技术领域的电子产品服务方法，尤旨在异构系统之间数据交换传输过程中基于数字签名的加密技术的实现，主要应用于网络服务中的数据交换传输中基于数字签名的加密技术方法。 该方法通过网络服务使用简单物件存取协定 SOAP 进行网络服务过滤和数据交换，获得端到端的消息级安全；通过数据加密、数字证书和数据共享交换过程中安全网络服务，对可扩展标记语言 XML 进行数字签名与加密工作，实现数据的安全性；主要解决如何确保信息传递过程中机密性、完整性以及一致性等有关技术问题。 本发明的积极效果是：采取基于数字签名的加密技术，可以确保信息传递过程中机密性、完整性以及一致性；具有方便了用户，提升了服务质量等优点。



1、一种数据交换传输中基于数字签名的加密技术方法，其特征在于：该方法运行于异构系统之间数据交换传输过程，通过网络服务使用简单物件存取协定 SOAP 进行网络服务过滤和数据交换，获得端到端的消息级安全；通过数据加密、数字证书和数据共享交换过程中安全网络服务，对可扩展标记语言 XML 进行数字签名与加密工作，实现数据的安全性；采用 Verisign 公司传输协议 HTTP 的信任服务集成工具箱，支持完成简单物件存取协定 SOAP 包的数字签名、验证、加密与解密工作；该数据共享交换过程中安全网络服务的工作流程，具体包括以下步骤：

步骤 1：编写证书脚本（1）

用 Verisign 公司的信任服务集成工具箱的使用标准，编写数据证书生成脚本，为编写证书脚本（1）模块；

步骤 2：执行脚本（2）

执行完编写证书脚本（1）模块后，编写证书脚本（1）模块的输出信号传递到执行脚本（2）模块；

步骤 3：生成证书（3）

执行完执行脚本（2）模块后，执行脚本（2）模块的输出信号传递到生成证书（3）模块；通过数字证书脚本生成四个文件：服务器端文件：bms.keystore；代理端文件：bmc.keystore；服务器信任

文件：bms.truststore 和代理端信任文件：bmc.truststore；

步骤 4：客户端部署代理端文件和服务器端信任文件（4）

执行完生成证书（3）模块后，生成证书（3）模块的输出信号分为两路，一路传递到客户端部署代理端文件和服务器端信任文件（4）模块，为网络客户端部署代理端文件 bmc.keystore 与服务器信任文件 bms.truststore 两个文件；

步骤 5：服务端部署服务端文件和代理端信任文件（5）

执行完生成证书（3）模块后，生成证书（3）模块的输出信号的另一路传递到服务端部署服务端文件和代理端信任文件（5）模块，为服务端部署服务器端文件 bms.keystore 与代理端信任文件 bmc.truststore 两个文件；

步骤 6：使用代理端文件获取数字签名（6）

执行完客户端部署代理端文件和服务器端信任文件(4)模块后，则进入使用代理端文件获取数字签名（6）模块，客户端调用接口时用代理端文件 bmc.keystore 的私钥数字签名；

步骤 7：使用服务器端信任文件进行加密（7）

执行完使用代理端文件获取数字签名（6）模块后，则进入使用服务器端信任文件进行加密（7）模块，使用服务器端信任文件进行加密（7）模块的输出信号传递到服务端部署服务端文件和代理端信任文件（5）模块；用服务器信任文件bms.truststore的公钥对简单物件存取协定 SOAP 包做加密；

步骤 8：使用代理端信任文件解密（8）

执行完服务端部署服务端文件和代理端信任文件（5）模块后，

则进入使用代理端信任文件解密（8）模块，处理响应时用代理端文件bmc.keystore的私钥对简单物件存取协定 SOAP 包做解密；

步骤 9：使用服务端文件进行数字签名验证（9）

执行完使用代理端信任文件解密（8）模块后，则进入使用服务端文件进行数字签名验证（9）模块，用服务器信任文件bms.truststore的公钥验证数字签名。

2、根据权利要求 1 所述的数据交换传输中基于数字签名的加密技术方法，其特征在于：所述的数字签名与加密工作为基于阿帕奇扩展网际系统 AXIS，通过客户端（21）和服务端 A（22）之间的发送和接收完成，客户端（21）和服务端 A（22）之间为加密 SOAP 包（23）模块和传输协议 HTTP（24）的电连接，其中：

客户端（21）包括：对 SOAP 消息使用数字证书进行签名（25）模块、对 SOAP 消息进行加密（26）模块和加密函数（27）模块，对 SOAP 消息使用数字证书进行签名(25)模块的输出信号传递到对 SOAP 消息进行加密（26）模块的输入端；加密函数（27）模块的输出信号传递到对 SOAP 消息进行加密（26）模块的输入端；

服务端 A（22）包括：对数字证书进行验证（28）模块，对 SOAP 消息进行解密（29）模块和解密函数（30）模块，对数字证书进行验证（28）模块的输出信号传递到对 SOAP 消息进行解密（29）模块的输入端；解密函数（30）模块的输出信号传递到对 SOAP 消息进行解密（29）模块的输入端；该数字签名与加密工作包括以下步骤：

步骤 1：客户端（21）

在客户端（21）通过签名函数对简单物件存取协定 SOAP 信息进行加密；

步骤 2：加密过程

加密时，首先获得私有钥匙和相关证书，然后对简单物件存取协定SOAP 消息进行签名，最后将签名后的文件通过传输协议HTTP（24）协议发送到服务端；

步骤 3：服务端 A（22）

服务端A（22）通过数据验证函数验证已经签名的简单物件存取协定SOAP 消息；

步骤 4：解密过程

验证后根据私有key和相关证书对文档进行解密。

3、根据权利要求 1 所述的数据交换传输中基于数字签名的加密技术方法，其特征在于：所述的网络服务过滤包括：代理端（31）和服务端 B（32），代理端（31）和服务端 B（32）之间通过请求（33）和响应（34）信号的电连接完成，其中：

代理端（31）包括：数字证书认证（35）、数字证书授权（36）、内容加密（37）和日志记录（38）模块，各模块之间为平行的电连接；

服务端 B（32）包括：数字证书验证（39）、内容解密（40）和网络服务缓存（41）模块，各模块之间为平行的电连接；该网络服务过滤工作包括以下步骤：

a)、 对客户端进行认证、授权；

b)、把用户的访问写入系统日志；

c)、对请求的简单物件存取协定SOAP 消息进行加密，解密；

d)、为网络服务对象做缓存。

4、一种数据交换传输中基于数字签名的加密技术的装置，该装置有业务系统、中心数据库和业务数据库，其特征在于还包括：业务系统A（11）、数据中心（15）和业务系统B（18）；业务系统A（11）中的共享文件夹A（12）与业务系统B（18）中的共享文件夹B（19）之间相互电连接；业务系统A（11）中的数据代理A（14）与数据中心（15）中的数据交换中心（17）之间相互电连接；数据中心（15）中的数据交换中心（17）与业务系统B（18）中的数据代理B（20）之间相互电连接；其中：

业务系统A（11）中依次顺序连接有共享文件夹A（12）、数据代理A（14）和业务数据库A（13）；共享文件夹A（12）、数据代理A（14）和业务数据库A（13）之间为相互电连接，共享文件夹A（12）与共享文件夹B（19）之间相互电连接；

数据中心（15）中依次顺序连接有中心数据库（16）和数据交换中心（17）；中心数据库（16）和数据交换中心（17）之间相互电连接；

业务系统B（18）中依次顺序连接有共享文件夹B（19）、数据代

理 B（20）和业务数据库 B（10）；共享文件夹 B（19）、数据代理 B（20）和业务数据库 B（10）之间为相互电连接，数据代理 B（20）与数据交换中心（17）之间相互电连接。

数据交换传输中基于数字签名的加密技术方法

技术领域

本发明涉及一种信息技术领域的电子产品服务方法。尤旨在异构系统之间数据交换传输过程中基于数字签名的加密技术的实现，主要应用于网络服务中，使用简单物件存取协定 SOAP（SIMPLE OBJECT ACCESS PROTOCOL）来进行数据交换时，可扩展标记语言 XML（EXTENSIBLE MARKUP LANGUAGE）在默认情况下是明文编码，这样使信息在传输过程中保密性受到威胁，因此采取基于数字签名的加密技术，可以确保信息传递过程中机密性、完整性以及一致性。

背景技术

安全的网络服务是网络服务成功的必要保证。但众所周知的是，网络服务使用简单物件存取协定SOAP(SIMPLE OBJECT ACCESS PROTOCOL)，基于可扩展标记语言XML(EXTENSIBLE MARKUP LANGUAGE)来进行数据交换，而XML在默认情况下是明文编码的；同时，大部分网络服务使用传输协议 HTTP(HYPERTEXT TRANSPORT PROTOCOL）协议

作为传输协议，同样，传输协议 HTTP 也是使用明文方式来传输数据的。这样使信息传输的保密性受到威胁，不能满足安全性基本要求：

- 机密性，确保数据的保密性。通常是使用加密实现的，使用加密算法将明文转换为密文，并使用相应的解密算法将密文转换回明文。
- 数据完整性，确保数据免受意外或者故意（恶意）的篡改。完整性通常是由消息身份验证代码或哈希值提供的。
- 身份验证，确定数据的来源。数字证书用于提供身份验证。数字签名通常应用于哈希值，因为这些值比它们所代表的源数据小得多。

2002年12月份IBM、Microsoft和Verisign联合发布了一个关于网络服务安全性网络服务 （WS-Security）的规范，该规范描述如何向简单物件存取协定 SOAP(SIMPLE OBJECT ACCESS PROTOCOL) 消息附加签名和加密报头，提供了一套网络服务开发者保护简单物件存取协定SOAP 消息交换的机制。

目前有两类不同的加密技术：

一类是对称加密，双方具有共享的密钥,只有在双方都知道密钥的情况下才能使用，通常应用于孤立的环境之中，如果用户数目多，这种机制并不可靠。常用的算法：数据加密标准DES(DATA ENCRYPTION STANDARD)、TripleDES(三重DES)、Rijndael、RC2等。

另一类是非对称加密，也称为公开密钥加密PKI(Public Key Infrastructure)，密钥是由公开密钥/私有密钥组成的密钥对，用私

有密钥进行加密，利用公开密钥可以进行解密，但是由于公开密钥无法推算出私有密钥，所以公开的密钥并不会损害私有密钥的安全，公开密钥无须保密，可以公开传播，而私有密钥必须保密。常用算法：数字签名算法DSA(Digital Signature Algorithm)、RSA等。

数字签名是一种新兴的用来保证信息完整性的安全技术，它保证信息的安全不受侵犯，可以解决否认、伪造、篡改及冒充等问题。它实际使用了信息发送者的私有密钥变换所需传输的信息。常用算法：哈希Hash、DSS、RSA等。

通常公钥信息、用户信息都是保存在数字证书中。数字证书是一段包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。身份验证机构的数字签名可以确保证书信息的真实性，用户公钥信息可以保证数字信息传输的完整性，用户的数字签名可以保证数字信息的不可否认性。X.509 V3标准在编排公共密钥密码格式方面已被广为接受并应用于许多网络安全。

由于近年来我国信息技术的蓬勃发展，异构子系统之间数据集成要求越来越高，因此在数据交换共享时如何保障数据内容的机密性、完整性、安全性以及一致性，就成为必须要思考的问题。

发明内容

为了克服上述不足之处，本发明的主要目的旨在提供一种可以根据国际网络服务安全性的规范在数据交换过程中实现基于数字签名

的加密技术；通过网络服务使用简单物件存取协定 SOAP 进行网络服务过滤和数据交换,通过数据加密、数字证书和数据共享交换过程中安全网络服务，采用 Verisign 公司传输协议 HTTP 的信任服务集成工具箱，支持完成简单物件存取协定 SOAP 包的数字签名、验证、加密与解密工作的数据交换传输中基于数字签名的加密技术方法。

本发明另一目的旨在使用数据加密和数字证书满足数据共享交换时网络安全性服务要求；当使用数字证书方法时，网络服务请求者必须有一个由可信认证中心签署的数字证书；请求者使用这个证书来表明它们的身份，并对简单物件存取协定SOAP（SIMPLE OBJECT ACCESS PROTOCOL）消息进行数字签名；对方系统接收到消息后，就可对消息做时间戳记并进行日志记录，验证。验证过程将确保消息来自发送方，并且还要验证消息内容在传输过程中没有被篡改。

信息被签名后再加密，然后把加密后的信息网络上传播，这样，即使第三方获得加密后的传输信息，也不能解密。

本发明要解决的技术问题是：主要解决在异构系统之间数据交换传输过程中，如何确保信息传递过程中机密性、完整性以及一致性问题；要解决如何通过网络服务获得端到端的消息级安全问题；要解决如何完成简单物件存取协定 SOAP 包的数字签名、验证、加密与解密工作等有关技术问题。

本发明解决其技术问题所采用的技术方案是：该方法运行于异构系统之间数据交换传输过程，通过网络服务使用简单物件存取协定

SOAP进行网络服务过滤和数据交换，获得端到端的消息级安全；通过数据加密、数字证书和数据共享交换过程中安全网络服务，对可扩展标记语言XML进行数字签名与加密工作，实现数据的安全性；采用Verisign公司传输协议HTTP 的信任服务集成工具箱，支持完成简单物件存取协定SOAP 包的数字签名、验证、加密与解密工作；该数据共享交换过程中安全网络服务的工作流程，具体包括以下步骤：

步骤 1：编写证书脚本

用 Verisign 公司的信任服务集成工具箱的使用标准，编写数据证书生成脚本，为编写证书脚本模块；

步骤 2：执行脚本

执行完编写证书脚本模块后，编写证书脚本模块的输出信号传递到执行脚本模块；

步骤 3：生成证书

执行完执行脚本模块后，执行脚本模块的输出信号传递到生成证书模块；通过数字证书脚本生成四个文件：服务器端文件：bms.keystore；代理端文件：bmc.keystore；服务器信任文件：bms.truststore 和代理端信任文件：bmc.truststore；

步骤 4：客户端部署代理端文件和服务器端信任文件

执行完生成证书模块后，生成证书模块的输出信号分为两路，一路传递到客户端部署代理端文件和服务器端信任文件模块，为网络客户端部署代理端文件 bmc.keystore 与服务器信任文件 bms.truststore 两个文件；

步骤 5：服务端部署服务端文件和代理端信任文件

执行完生成证书模块后，生成证书模块的输出信号的另一路传递到服务端部署服务端文件和代理端信任文件模块，为服务端部署服务器端文件bms.keystore与代理端信任文件bmc.truststore两个文件；

步骤6：使用代理端文件获取数字签名

执行完客户端部署代理端文件和服务器端信任文件模块后，则进入使用代理端文件获取数字签名模块，客户端调用接口时用代理端文件bmc.keystore的私钥数字签名；

步骤7：使用服务器端信任文件进行加密

执行完使用代理端文件获取数字签名模块后，则进入使用服务器端信任文件进行加密模块，使用服务器端信任文件进行加密模块的输出信号传递到服务端部署服务端文件和代理端信任文件模块；用服务器信任文件bms.truststore的公钥对简单物件存取协定 SOAP 包做加密；

步骤 8：使用代理端信任文件解密

执行完服务端部署服务端文件和代理端信任文件模块后，则进入使用代理端信任文件解密模块，处理响应时用代理端文件bmc.keystore的私钥对简单物件存取协定 SOAP 包做解密；

步骤 9：使用服务端文件进行数字签名验证

执行完使用代理端信任文件解密模块后，则进入使用服务端文件进行数字签名验证模块，用服务器信任文件bms.truststore的公钥验证数字签名。

所述的数据交换传输中基于数字签名的加密技术方法的数字签

名与加密工作为基于阿帕奇扩展网际系统 AXIS，通过客户端和服务端 A 之间的发送和接收完成，客户端和服务端 A 之间为加密 SOAP 包模块和传输协议 HTTP 的电连接，其中：

客户端包括：对 SOAP 消息使用数字证书进行签名模块、对 SOAP 消息进行加密模块和加密函数模块，对 SOAP 消息使用数字证书进行签名模块的输出信号传递到对 SOAP 消息进行加密模块的输入端；加密函数模块的输出信号传递到对 SOAP 消息进行加密模块的输入端；

服务端 A 包括：对数字证书进行验证模块，对 SOAP 消息进行解密模块和解密函数模块，对数字证书进行验证模块的输出信号传递到对 SOAP 消息进行解密模块的输入端；解密函数模块的输出信号传递到对 SOAP 消息进行解密模块的输入端；该数字签名与加密工作包括以下步骤：

步骤 1：客户端

在客户端通过签名函数对简单物件存取协定 SOAP 信息进行加密；

步骤 2：加密过程

加密时，首先获得私有钥匙和相关证书，然后对简单物件存取协定SOAP 消息进行签名，最后将签名后的文件通过传输协议HTTP协议发送到服务端；

步骤 3：服务端 A

服务端A通过数据验证函数验证已经签名的简单物件存取协定

SOAP 消息；

步骤 4：解密过程

验证后根据私有key和相关证书对文档进行解密。

所述的数据交换传输中基于数字签名的加密技术方法的网络服务过滤包括：代理端和服务端 B，代理端和服务端 B 之间通过请求和响应信号的电连接完成，其中：

代理端包括：数字证书认证、数字证书授权、内容加密和日志记录模块，各模块之间为平行的电连接；

服务端 B 包括：数字证书验证、内容解密和网络服务缓存模块，各模块之间为平行的电连接；该网络服务过滤工作包括以下步骤：

a)、 对客户端进行认证、授权；

b)、把用户的访问写入系统日志；

c)、对请求的简单物件存取协定SOAP 消息进行加密，解密；

d)、为网络服务对象做缓存。

一种数据交换传输中基于数字签名的加密技术的装置，该装置有业务系统、中心数据库和业务数据库，还包括：业务系统 A、数据中心和业务系统 B；业务系统 A 中的共享文件夹 A 与业务系统 B 中的共享文件夹 B 之间相互电连接；业务系统 A 中的数据代理 A 与数据中心中的数据交换中心之间相互电连接；数据中心中的数据交换中心与业务系统 B 中的数据代理 B 之间相互电连接；其中：

业务系统 A 中依次顺序连接有共享文件夹 A、数据代理 A 和业务

数据库 A；共享文件夹 A、数据代理 A 和业务数据库 A 之间为相互电连接，共享文件夹 A 与共享文件夹 B 之间相互电连接；

数据中心中依次顺序连接有中心数据库和数据交换中心；中心数据库和数据交换中心之间相互电连接；

业务系统 B 中依次顺序连接有共享文件夹 B、数据代理 B 和业务数据库 B；共享文件夹 B、数据代理 B 和业务数据库 B 之间为相互电连接，数据代理 B 与数据交换中心之间相互电连接。

本发明的有益效果是：该方法提供了一种在数据共享交换的过程中安全网络服务实现，使应用程序能够构建安全的简单物件存取协定 SOAP 消息交换、获得端到端的消息级安全；可扩展标记语言 XML 签名用于认证发送者的身份、确保简单物件存取协定 SOAP 消息的完整性，并对可扩展标记语言 XML 加密提高了数据的安全性；采取基于数字签名的加密技术，可以确保信息传递过程中机密性、完整性以及一致性；具有方便了用户，提升了服务质量等优点。

附图说明

下面结合附图和实施例对本发明进一步说明。

附图 1 为本发明硬件环境结构方框示意图；

附图 2 为本发明数据共享交换过程中安全网络服务的总工作流程示意图；

附图 3 为本发明的数字签名与加密工作流程示意图；

附图 4 为本发明的网络服务过滤流程示意图；

附图 5 为本发明实施例之一的应用系统实现流程示意图；

附图中标号说明：

1—编写证书脚本；

2—执行脚本；

3—生成证书；

4—客户端部署代理端文件和服务器端信任文件；

5—服务端部署服务端文件和代理端信任文件；

6—使用代理端文件获取数字签名；

7—使用服务器端信任文件进行加密；

8—使用代理端信任文件解密；

9—使用服务端文件进行数字签名验证；

10—业务数据库B；

11—业务系统A；

12—共享文件夹A；

13—业务数据库A；

14—数据代理A；

15—数据中心；

16—中心数据库；

17—数据交换中心；

18—业务系统 B；

19—共享文件夹 B；

20—数据代理 B；

21—客户端；

22—服务端 A；

23—加密 SOAP 包；

24—传输协议 HTTP；

25—对 SOAP 消息使用数字证书进行签名；

26—对 SOAP 消息进行加密；

27—加密函数；

28—对数字证书进行验证；

29—对 SOAP 消息进行解密；

30—解密函数；

31—代理端；

32—服务端 B；

33—请求；

34—响应；

35—数字证书认证；

36—数字证书授权；

37—内容加密；

38—日志记录；

39—数字证书验证；

40—内容解密；

41—网络服务缓存；

51—发送方 A 数据打包；

52—数字签名并加密；

53—发送结果到中间库；

54—中间库 C 验证并保存数据；

55—向发送方返回历史记录；

56—接收方 B 从中间库获取 XML；

57—解密 XML，验证数字证书；

58—向中间库数据置位；

59—解析 XML 入库；

60—向接收方返回历史记录。

具体实施方式

请参阅附图 1、2、3、4 所示，该方法运行于异构系统之间数据

交换传输过程，通过网络服务使用简单物件存取协定 SOAP 进行网络服务过滤和数据交换，获得端到端的消息级安全；通过数据加密、数字证书和数据共享交换过程中安全网络服务，对可扩展标记语言 XML 进行数字签名与加密工作，实现数据的安全性；采用 Verisign 公司传输协议 HTTP 的信任服务集成工具箱，支持完成简单物件存取协定 SOAP 包的数字签名、验证、加密与解密工作；该数据共享交换过程中安全网络服务的工作流程，具体包括以下步骤：

步骤 1：编写证书脚本 1

用 Verisign 公司的信任服务集成工具箱的使用标准，编写数据证书生成脚本，为编写证书脚本 1 模块；

步骤 2：执行脚本 2

执行完编写证书脚本 1 模块后，编写证书脚本 1 模块的输出信号传递到执行脚本 2 模块；

步骤 3：生成证书 3

执行完执行脚本 2 模块后，执行脚本 2 模块的输出信号传递到生成证书 3 模块；通过数字证书脚本生成四个文件：服务器端文件：bms.keystore；代理端文件：bmc.keystore；服务器信任文件：bms.truststore 和代理端信任文件：bmc.truststore；

步骤 4：客户端部署代理端文件和服务器端信任文件 4

执行完生成证书 3 模块后，生成证书 3 模块的输出信号分为两路，一路传递到客户端部署代理端文件和服务器端信任文件 4 模块，为网络客户端部署代理端文件 bmc.keystore 与服务器信任文件 bms.truststore 两个文件；

步骤 5：服务端部署服务端文件和代理端信任文件 5

执行完生成证书 3 模块后，生成证书 3 模块的输出信号的另一路传递到服务端部署服务端文件和代理端信任文件 5 模块，为服务端部署服务器端文件 bms.keystore 与代理端信任文件 bmc.truststore 两个文件；

步骤 6：使用代理端文件获取数字签名 6

执行完客户端部署代理端文件和服务器端信任文件 4 模块后，则进入使用代理端文件获取数字签名 6 模块，客户端调用接口时用代理端文件 bmc.keystore 的私钥数字签名；

步骤 7：使用服务器端信任文件进行加密 7

执行完使用代理端文件获取数字签名 6 模块后，则进入使用服务器端信任文件进行加密 7 模块，使用服务器端信任文件进行加密 7 模块的输出信号传递到服务端部署服务端文件和代理端信任文件 5 模块；用服务器信任文件bms.truststore的公钥对简单物件存取协定 SOAP 包做加密；

步骤 8：使用代理端信任文件解密 8

执行完服务端部署服务端文件和代理端信任文件 5 模块后，则进入使用代理端信任文件解密 8 模块，处理响应时用代理端文件bmc.keystore的私钥对简单物件存取协定 SOAP 包做解密；

步骤 9：使用服务端文件进行数字签名验证 9

执行完使用代理端信任文件解密 8 模块后，则进入使用服务端文件进行数字签名验证 9 模块，用服务器信任文件bms.truststore

的公钥验证数字签名。

请参阅附图 3 所示，所述的数据交换传输中基于数字签名的加密技术方法的数字签名与加密工作为基于阿帕奇扩展网际系统AXIS，通过客户端 21 和服务端 A 22 之间的发送和接收完成，客户端 21 和服务端 A 22 之间为加密 SOAP 包 23 模块和传输协议 HTTP 24 的电连接，其中：

客户端 21 包括：对 SOAP 消息使用数字证书进行签名 25 模块、对 SOAP 消息进行加密 26 模块和加密函数 27 模块，对 SOAP 消息使用数字证书进行签名 25 模块的输出信号传递到对 SOAP 消息进行加密 26 模块的输入端；加密函数 27 模块的输出信号传递到对 SOAP 消息进行加密 26 模块的输入端；

服务端 A 22 包括：对数字证书进行验证 28 模块，对 SOAP 消息进行解密 29 模块和解密函数 30 模块，对数字证书进行验证 28 模块的输出信号传递到对 SOAP 消息进行解密 29 模块的输入端；解密函数 30 模块的输出信号传递到对 SOAP 消息进行解密 29 模块的输入端；该数字签名与加密工作包括以下步骤：

步骤 1：客户端 21

在客户端 21通过签名函数对简单物件存取协定 SOAP 信息进行加密；

步骤 2：加密过程

加密时，首先获得私有钥匙和相关证书，然后对简单物件存取

协定SOAP 消息进行签名，最后将签名后的文件通过传输协议HTTP 24 协议发送到服务端；

步骤 3：服务端 A 22

服务端A 22通过数据验证函数验证已经签名的简单物件存取协定SOAP 消息；

步骤 4：解密过程

验证后根据私有key和相关证书对文档进行解密。

本发明数字签名与加密工作的实施方式：

①在客户端通过签名函数对简单物件存取协定SOAP（SIMPLE OBJECT ACCESS PROTOCOL）信息进行加密；

②加密时，首先获得私有钥匙和相关证书，然后对简单物件存取协定SOAP（SIMPLE OBJECT ACCESS PROTOCOL）消息进行签名，最后将签名后的文件通过传输协议HTTP （HYPERTEXT TRANSPORT PROTOCOL）协议发送到服务端；

③服务端通过数据验证函数验证已经签名的简单物件存取协定(SOAP，全写为SIMPLE OBJECT ACCESS PROTOCOL）消息；

④验证后根据私有key和相关证书对文档进行解密。

请参阅附图 4 所示，所述的数据交换传输中基于数字签名的加密技术方法的网络服务过滤包括：代理端 31 和服务端 B 32，代理端 31 和服务端 B 32 之间通过请求 33 和响应 34 信号的电连接完成，其中：

代理端 31 包括：数字证书认证 35、数字证书授权 36、内容加密

37 和日志记录 38 模块，各模块之间为平行的电连接；

服务端 B 32 包括：数字证书验证 39、内容解密 40 和网络服务缓存 41 模块，各模块之间为平行的电连接；该网络服务过滤工作包括以下步骤：

a)、 对客户端进行认证、授权；

b)、把用户的访问写入系统日志；

c)、对请求的简单物件存取协定SOAP 消息进行加密，解密；

d)、为网络服务对象做缓存。

请参阅附图 1 所示，一种数据交换传输中基于数字签名的加密技术的装置，该装置由业务系统、中心数据库和业务数据库等模块，还包括：业务系统 A 11、数据中心 15 和业务系统 B 18；业务系统 A 11 中的共享文件夹 A 12 与业务系统 B 18 中的共享文件夹 B 19 之间相互电连接；业务系统 A 11 中的数据代理 A 14 与数据中心 15 中的数据交换中心 17 之间相互电连接；数据中心 15 中的数据交换中心 17 与业务系统 B 18 中的数据代理 B 20 之间相互电连接；其中：

业务系统 A 11 中依次顺序连接有共享文件夹 A 12、数据代理 A 14 和业务数据库 A 13；共享文件夹 A 12、数据代理 A 14 和业务数据库 A 13 之间为相互电连接，共享文件夹 A 12 与共享文件夹 B 19 之间相互电连接；

数据中心 15 中依次顺序连接有中心数据库 16 和数据交换中心 17；中心数据库 16 和数据交换中心 17 之间相互电连接；

业务系统 B 18 中依次顺序连接有共享文件夹 B 19、数据代理 B 20 和业务数据库 B 10；共享文件夹 B 19、数据代理 B 20 和业务数据库 B 10 之间为相互电连接，数据代理 B 20 与数据交换中心 17 之间相互电连接。

本发明硬件环境的实施方式：

①数据中心包括数据项管理、网络服务以及简单物件存取协定 SOAP（SIMPLE OBJECT ACCESS PROTOCOL）信息的加密、解密功能；网络服务处理来自数据代理端的接口调用。

②数据代理主要完成数据提供和数据接收两部分功能。每个数据库运行一个数据代理端，也可多个数据库运行一个代理端，代理段也提供网络服务以及简单物件存取协定 SOAP（SIMPLE OBJECT ACCESS PROTOCOL）信息的加密、解密功能。

请参阅附图5所示，为本发明实施例之一的应用系统实现流程图，具体包括以下步骤：

步骤 1. 发送方 A 数据打包（51）

设业务系统 A 11 为发送方 A，即数据提供方 A，准备发送方 A 数据打包（51）工作；

步骤 2. 数字签名并加密（52）

执行完发送方 A 数据打包（51）模块后，则进入数字签名并加密（52）模块；

步骤 3. 发送结果到中间库（53）

执行完数字签名并加密（52）模块后，则进入发送结果到中间库（53）模块；

步骤 4. 中间库 C 验证并保存数据（54）

执行完发送结果到中间库（53）模块后，则进入中间库 C 验证并保存数据（54）模块，中间库 C 验证并保存数据（54）的输出信号分为三路，第一路传递到向发送方返回历史记录（55）模块，第二路传递到接收方 B 从中间库获取 XML（56）模块，第三路传递到向接收方返回历史记录（60）模块；

步骤 5. 解密 XML，验证数字证书（57）

执行完接收方 B 从中间库获取 XML（56）模块后，则进入解密 XML，验证数字证书（57）；

步骤 6. 向中间库数据置位（58）

执行完解密 XML，验证数字证书（57）模块后，则进入向中间库数据置位（58）；

步骤 7. 解析 XML 入库（59）

执行完向中间库数据置位（58）模块后，则进入解析 XML 入库（59）模块。

本发明实施例之一的应用系统实施方式：

现业务系统 A 11 为发送方即数据提供方 A，业务系统 B 12 为获取方即数据获取方 B，数据中心即中间库为 C，A 通过 C 共享数据给 B：

①由 A 定义要共享的关系型数据表描述，提交给 C 及 B；各代理

端在自己系统中建立相应的提供项，根据 A 提供的描述形成自己的导入项；

②C 根据 A 提供的数据表描述，在系统中建立相应的共享数据目录、定义共享时的数据格式可扩展标记语言 XML（ EXTENSIBLE MARKUP LANGUAGE） Schema（保存于网络服务器）。B 也可在本系统内建立数据接收项及可扩展标记语言 XML（ EXTENSIBLE MARKUP LANGUAGE） Element/字段对应关系，便于 B 接收数据。B 方相应的数据库表结构自行定义，但要与数据接收项目的相关元素吻合；

③A 定时启动数据提供进程，把上一次没有共享（新增的或修改过）的记录根据规则打成可扩展标记语言 XML（ EXTENSIBLE MARKUP LANGUAGE）包，此 XML 文件必须遵循上面定义的 XML（ EXTENSIBLE MARKUP LANGUAGE） Schema。经过安全处理后通过 C 提供的接口保存至中心数据库，如果 C 确认接收则修改相应记录的标志位标识已经发送。如果数据要求的优先级较高，要求通知 B；

④B 定时启动数据接收进程。通过 C 提供的查询接口知晓是否有向自己共享的数据，有则从中心数据库获取可扩展标记语言 XML（ EXTENSIBLE MARKUP LANGUAGE）数据，收到数据后，经过 XML（ EXTENSIBLE MARKUP LANGUAGE）-to-Table 转换到数据库中，并修改 C 中的接收标志；A 构建的可扩展标记语言 XML（ EXTENSIBLE MARKUP LANGUAGE）包中包括附件信息，则 B 在解析时将提取相应的 FTP 地址或传输协议 HTTP （HYPERTEXT TRANSPORT PROTOCOL）地址，加入到附件获取列表，从 A 的共享文件夹中下载到 B 的共享文件夹中。

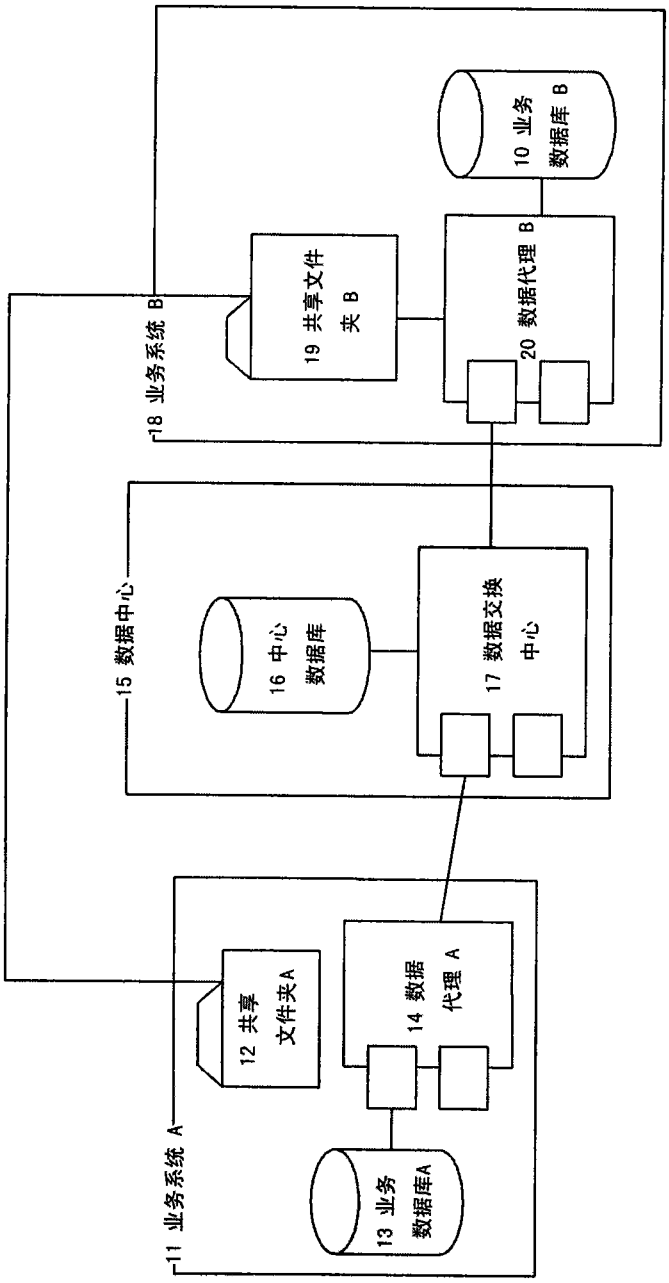

10 业务数据库 B
18 业务系统 B
19 共享文件夹 B
20 数据代理 B
15 数据中心
16 中心数据库
17 数据交换中心
11 业务系统 A
12 共享文件夹A
14 数据代理 A
13 业务数据库A

图 1

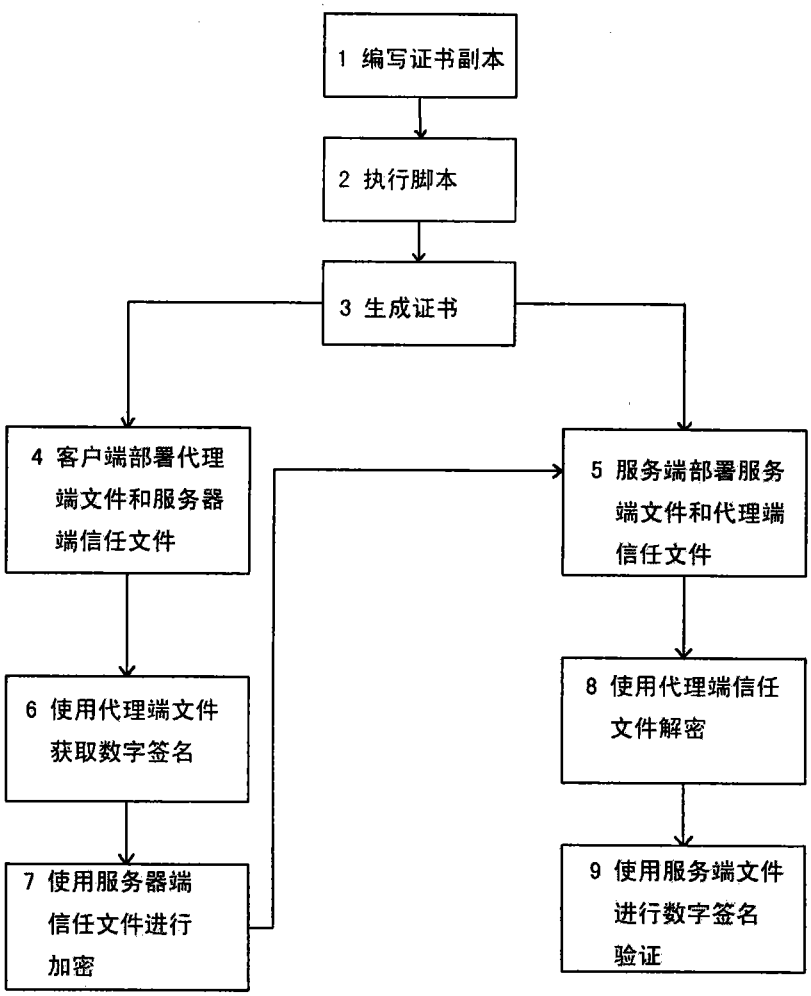

1 编写证书副本
2 执行脚本
3 生成证书
4 客户端部署代理端文件和服务器端信任文件
5 服务端部署服务端文件和代理端信任文件
6 使用代理端文件获取数字签名
7 使用服务器端信任文件进行加密
8 使用代理端信任文件解密
9 使用服务端文件进行数字签名验证

图 2

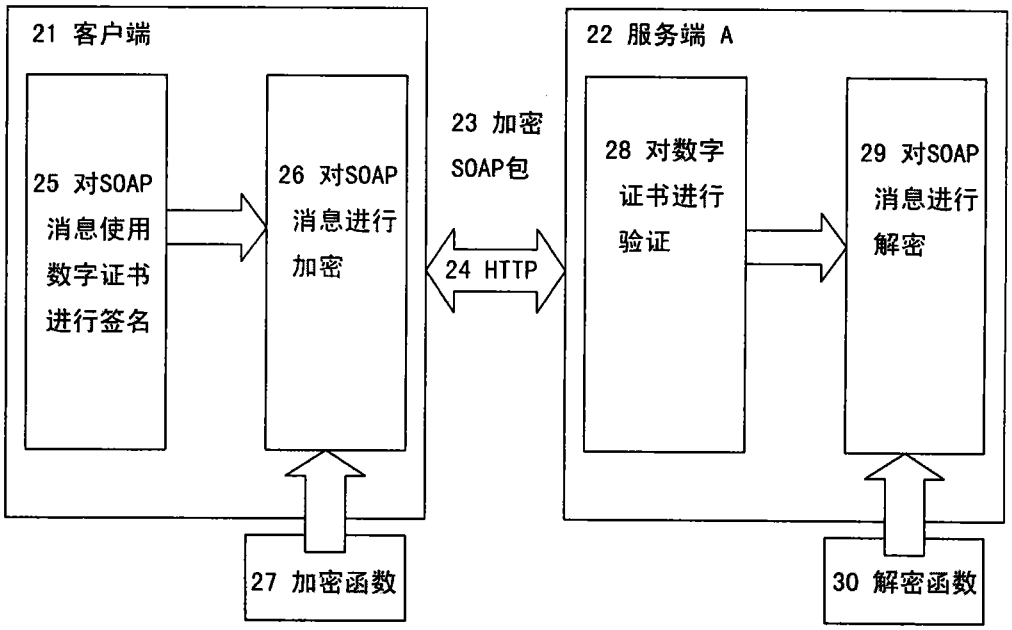

21 客户端
25 对SOAP消息使用数字证书进行签名
26 对SOAP消息进行加密
27 加密函数
23 加密SOAP包
24 HTTP
22 服务端 A
28 对数字证书进行验证
29 对SOAP消息进行解密
30 解密函数

图 3

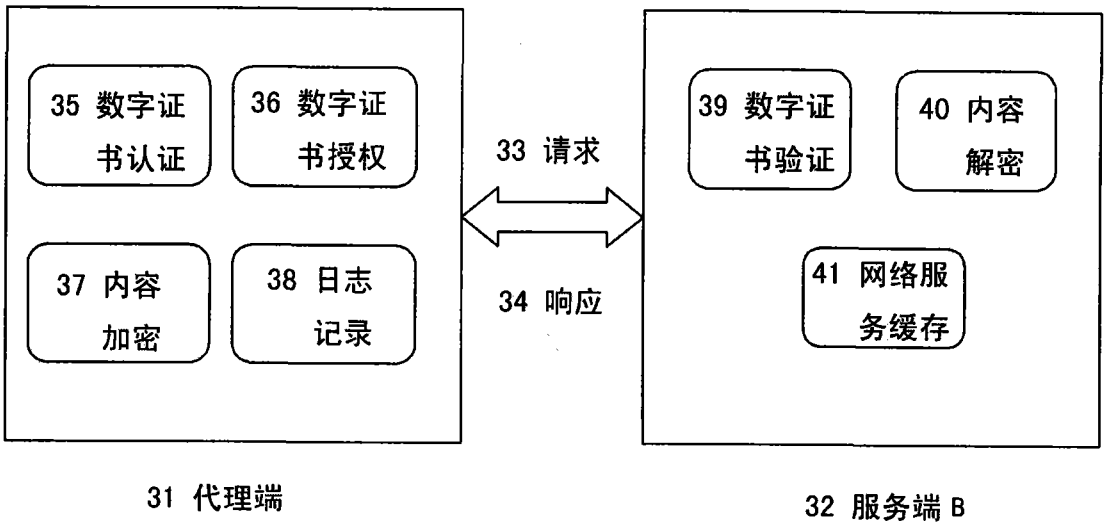

35 数字证书认证
36 数字证书授权
37 内容加密
38 日志记录
33 请求
34 响应
39 数字证书验证
40 内容解密
41 网络服务缓存
31 代理端
32 服务端 B

图 4

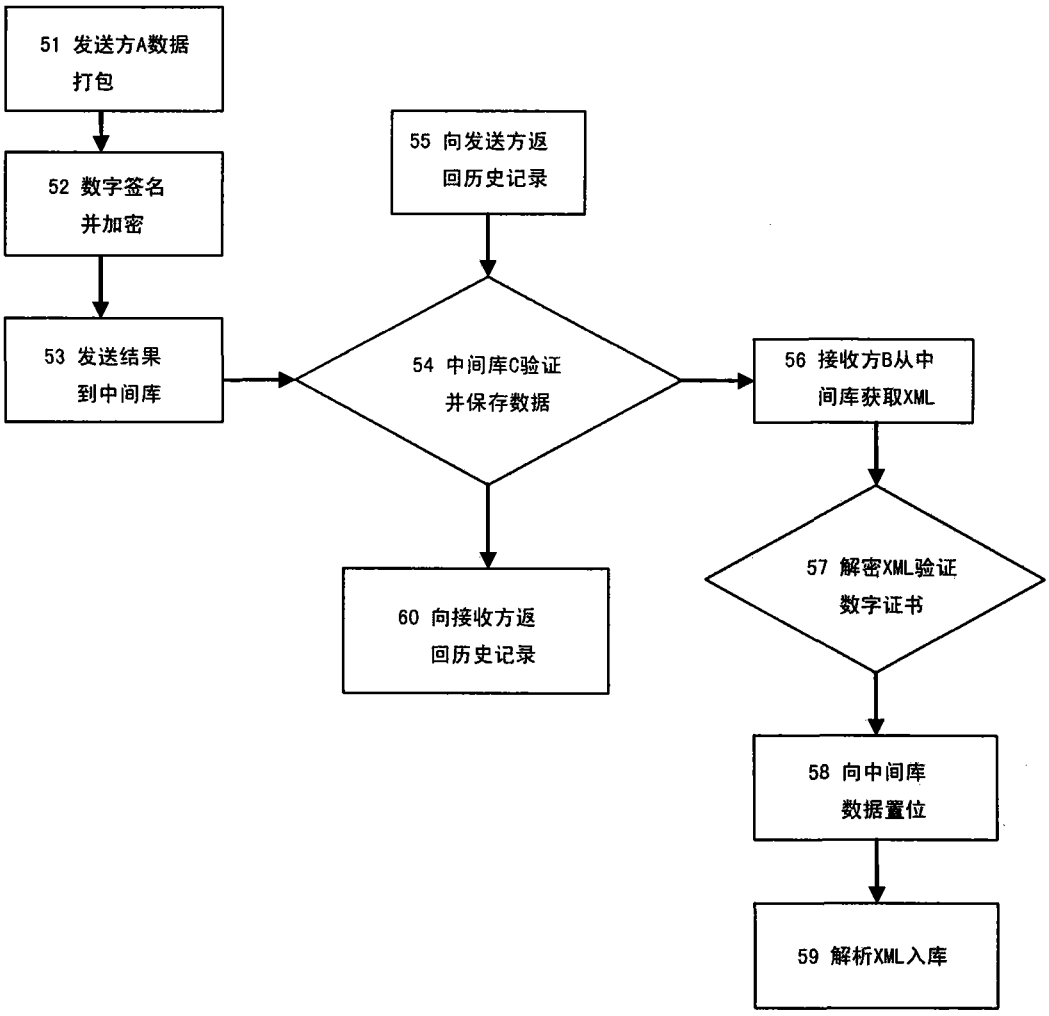

51 发送方A数据打包
52 数字签名并加密
53 发送结果到中间库
54 中间库C验证并保存数据
55 向发送方返回历史记录
56 接收方B从中间库获取XML
57 解密XML验证数字证书
58 向中间库数据置位
59 解析XML入库
60 向接收方返回历史记录

图 5