文章编号：2096-1472(2016)-08-45-03

一种基于虚拟专用网及数据加密技术的企业财务会计记录直报系统的实现方案

康保军
（浙江长征职业技术学院计算机与信息技术系，浙江 杭州 310023）

摘　要：随着计算机与通信技术的发展和应用的推广，一些地区的财政部门为提高本辖区内的企业数据上报的及时性和便利性，积极升级改造企业财务会计记录的上报方法，其中有些地方利用了互联网的便利性，推出了企业财务会计记录直报系统。但是，由于目前日益严重的信息安全问题困扰着很多地方的企业及其主管部门，如何在信息安全和工作效率之间找到一个平衡点，是很多系统建设者要考虑的重要问题。本文针对了从企业财务会计记录采集、发送到接收、入库中可能存在的安全问题，提出使用虚拟专用网技术以及数据加密、数字信封、哈希函数和数字签名等技术，从而避免在这个过程中的安全隐患，提高了整个系统的信息安全保障。

关键词：财务会计记录；虚拟专用网；数据加密；数字签名
中图分类号：TP311.1　　**文献标识码**：A

An ImplementationScheme of Direct Reporting System of Enterprise Financial Accounting Based on Virtual Private Network and Data Encryption Technology

KANG Baojun
(*Zhejiang Changzheng Vocational and Technical College*,*Department of Computer and Information Technology*,*Hangzhou* 310023,*China*)

Abstract: With the promotion of the development and application of computer and communications technology,some areas of the financial sector for improve the timeliness and convenience within the jurisdiction of the enterprise data reported that actively upgrading transformation of the enterprise financial accounting records of the reporting method,which in some places using the convenience of internet,launched the enterprise financial accounting records of the reporting system.But due to the increasingly serious problem of information security plagued many local enterprises and departments,how to find a balance point between of the information security and the work efficiency is a lot of system builders to consider important issues.This paper also discusses from the enterprise financial accounting records collected and sent to the receiver,thetreasury may exist safety problem,it proposes using virtual private network technology and digital encryption,digital envelope,hash function and digital signature etc.,thus avoiding security hidden danger in the process,improve the information security of the whole system.

Keywords:financial accounting records;virtual private net;data encryption;digital signature

1 引言(Introduction)

随着计算机与通信技术的发展和应用的推广，当前社会进入了信息社会，同时信息的安全问题也成为了人们关注的焦点，为了解决信息安全中存在的一些问题，很多人致力于发现新的安全技术以及新的算法的应用。在人们解决信息安全的过程中，普遍认为加密技术是信息安全的核心。因此，数据加密技术也随着信息社会的到来而蓬勃发展。为了提高信息的安全性，人们将多种加密技术综合起来，充分发挥各种技术的特点，共同提高信息的安全性；比如利用数据加密、数字信封、哈希函数和数字签名等技术来实现数据的机密性、完整性、认证性和不可否认性[1-3]。

目前，一些地区的财政部门为提高本辖区内的企业数据上报的及时性和便利性，积极升级改造企业财务会计记录的上报方法，其中有些地方利用了互联网的便利性，推出了企业财务会计记录直报系统。通过这种方式，提高了企业财务会计记录数据上报系统的性能，提高了工作效率，但是由于这些数据可能包含每个企业的商业机密，因此，不论是在企业财务会计记录的生成、传输还是上报过程中，都会存在数据信息的安全性问题，可能造成信息的泄露、篡改，就会使企业蒙受损失，影响系统的正常运行以及企业的信誉、生产和经营。

因此，一个功能完善的企业财务会计记录直报系统，除

了需要具备之前系统的数据导入、数据查询、数据统计、权限控制等功能外，企业财务会计记录数据从生成到入库的安全性尤其重要。企业财务会计记录直报系统不仅需要保证数据信息的准确性和及时性，更要保证的机密性、完整性、认证性和不可否认性。而本研究方案所使用的虚拟专用网[4]及多种数据加密技术，很好地满足了企业财务会计记录直报系统的要求，为企业财务会计记录直报提供了一个较好的解决方案。

通过对企业财务会计记录直报系统使用环境的研究，并针对从企业财务会计记录采集、发送到企业财务会计记录接收、入库过程中可能存在的安全问题，提出了一套完整的解决方案：通过虚拟专用网技术在互联网上建立数据传输安全通道，实现各企业与本地财政系统的随时联网，提高了系统的可伸缩性，降低系统运行成本；再利用数据加密、数字信封、哈希函数和数字签名[5]来实现数据的机密性、完整性、可鉴别和不可否认性，为企业财务会计记录直报系统的正常运行，提供了安全保障。

本文主要介绍本系统所使用的虚拟专用网、数据加密、数字信封、哈希函数和数字签名等技术及系统的设计和实现原理。

2 系统主要技术(Main technology of system)

本研究方案主要涉及的技术包括虚拟专用网、数据加密、数字信封、哈希函数和数字签名等技术，现这些技术简单介绍。

2.1 虚拟专用网技术

虚拟专用网(Virtual Private Net，即VPN)，通常是在公用网络(Internet)上建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。它的功能是在公用网络上建立专用网络，进行加密通讯，虚拟专用网网关通过对数据包的加密和数据包目标地址的转换实现远程访问，在企业网络中有广泛应用。虚拟专用网能提供如下功能：

(1)数据加密：以保证通过公网传输的信息即使被人截获也不会泄露。

(2)信息认证和身份认证：保证信息的完整性、合法性，并能鉴别用户身份。

(3)提供访问控制：不同用户有不同的访问权限。

目前，除了一些专业的公司如思科(Cisco)、华为等有虚拟专用网产品外，常用的操作系统如Windows、Unix，甚至Android、iOS都带有虚拟专用网功能。

2.2 RSA公钥加密算法

RSA[6]是目前很有影响力的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被ISO推荐为公钥数据加密标准。RSA公钥加密算法是1977年由罗纳德·李维斯特(Ron Rivest)、阿迪·萨莫尔(Adi Shamir)和伦纳德·阿德曼(Leonard Adleman)一起提出的。1987年首次公布，当时他们三人都在麻省理工学院工作。RSA就是他们三人姓氏开头字母拼在一起组成的。在本系统中，使用的密钥长度为1024比特。

2.3 数据加密标准

数据加密标准(Data Encryption Standard，DES)[7]，是一种使用对称密钥加密的算法。1977年被美国联邦政府的国家标准局确定为联邦资料处理标准(FIPS)，并授权在非密级政府通信中使用，随后该算法在国际上广泛流传开来。

DES设计中使用了分组密码设计的两个原则：混淆(Confusion)和扩散(Diffusion)，其目的是抗击敌手对密码系统的统计分析。混淆是使密文的统计特性与密钥的取值之间的关系尽可能复杂化，以使密钥和明文以及密文之间的依赖性对密码分析者来说是无法利用的。扩散的作用就是将每一位明文的影响尽可能迅速地作用到较多的输出密文位中，以便在大量的密文中消除明文的统计结构，并且使每一位密钥的影响尽可能迅速地扩展到较多的密文位中，以防对密钥进行逐段破译。为了提高DES的加密强度，也可以使用双重DES和三重DES。在本系统中，使用的密钥长度为2048比特。

2.4 信息—摘要算法5

信息—摘要算法5(Message-Digest Algorithm 5，MD5)[8,9]，为计算机安全领域广泛使用的一种哈希函数，用以提供消息的完整性保护，该算法的文件号为RFC 1321，用于确保信息传输完整一致，是计算机广泛使用的杂凑算法(也称摘要算法、哈希算法)之一。

3 系统设计及实现(System design and realization)

本系统的拓扑结构如图1所示。

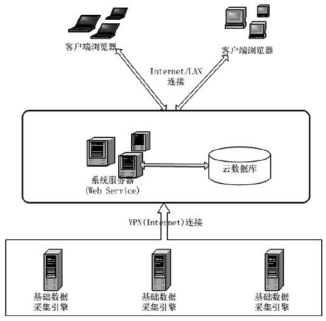

图1 系统拓扑图

Fig.1 System topology diagram

在本系统中，财政部门的信息中心安装有本系统的服务

器(Web Service)和数据库服务器，而该财政部门其所管辖的每个企业都有系统客户端，在这些系统客户端中安装有“基础数据采集引擎”(负责财务会计记录的采集)，这些系统客户端在需要时可以通过虚拟专用网与服务器相连，不需要时则断开连接。虽然，把很多企业的客户端通过VPN的方式连入信息中心的服务器后，如同组建了一个局域网，为各企业上报数据带来了方便性、快捷性；但也会引起本“局域网”的安全问题，如果某个企业可以通过把自己系统客户端或本企业的其他计算机的网卡设置成混杂模式，就可以监听本网络中其他计算机的通信，为了解决本系统可能存在的安全问题，系统服务器和每个系统客户端都采用了通过第三方CA认证的RSA密钥管理机制，上报的数据文件必须进过加密处理。系统客户端上报数据文件的步骤如下：

第一步：系统客户端采集企业财务会计记录。一般而言，在每个周期内，系统客户端根据需要完成企业财务会计记录的采集，生成上报数据文件，如M_0。

第二步：系统客户端对上报数据签名。客户端利用MD5生成上报数据M_0的信息摘要h_0，并用自己的RSA私钥K_1对该信息摘要进行数字签名h_1。然后将上报数据文件M_0和数字签名h_1合并为M_1。

第三步：系统客户端加密上报数据。客户端随机产生一个DES密钥K_{DES}，用DES密钥加密M_1，生成密文C_1；再用服务器的公钥加密DES密钥K_{DES}生成数字信封C_2。

第四步：系统客户端向系统服务器发送数据。客户端通过VPN方式请求连接服务器，通过服务器验证后，客户端将向系统服务器发送上报数据及数字签名的密文C_1和数字信封C_2。

系统服务端处理上报的数据文件有两个步骤如下：

第一步：系统服务器验证上报数据。服务器收到客户端发送的C_1和C_2后，使用自己的私钥打开数字信封C_2，得到客户端的DES密钥K_{DES}；并用此密钥KDES去解密C_1，得到数据M_1，再从M_1中分离出M_0和h_1。然后求出上报数据M0的信息摘要hS，再对该客户端的数字签名进行身份验证，即使用该客户端的RSA公钥解密h_1，得到收到的该客户端发送的消息摘要h_C，比较h_S和h_C，如果$h_S=h_C$，则说明M_0确是该客户端发送的上报数据，如果$h_S \neq h_C$，则收到的上报数据是不可信的。

第二步：企业财务会计记录的入库。系统服务器在收到客户端发送的上报数据并完成验证后，认为该企业财务会计记录确是某个企业所发，于是将企业财务会计记录入库。完成后通知客户端断开VPN连接。

如果在服务器完成企业财务会计记录入库后，发现企业财务会计记录存在错误，系统客户端可以重新发送企业财务会计记录，服务器收到重新入库的请求后，先删除之前的错误企业财务会计记录，再把通过验证的新收到的企业财务会计记录入库，避免了错误信息的存在。

4 结论(Conclusion)

本系统将虚拟专用网技术和数据加密、数字信封、哈希函数和数字签名等结合在一起，实现了系统在安全方面的功能，满足了当前条件下信息的安全性。而且在试运行过程中，该系统可以实现企业财务会计记录的直报要求，并达到快速及时、安全性的要求。但该系统还存在部分不足，主要存在一下几个问题，一是有时候网速比较慢，可能是由于虚拟专用网的配置引起的；二是目前使用的DES和RSA算法的密钥长度可能成为安全隐患。对于以上问题，将在以后的版本中进一步改进和完善。

参考文献(References)

[1] Liu Jinhui,et al.DigitalSignature Protocol Based on Error-correcting Codes[J].Huazhong Univ. of Sci.&Tech.(Natural Science Edition),2014,42(11):97-101.

[2] Wang Mingwei,HuYupu.Forward and Backward Secure Signature Scheme[J].JournalofXidian University,2014,41(2):71-78.

[3] Wang Ding,Wang Ping,Lei Ming.Cryptanalysis and Improvement of Gateway-oriented Password Authenticated Key Exchange Protocol Based on RSA[J].Acta Electronica Sinica,2015,41(1):176-184.

[4] 百度百科[EB/OL].http://baike.baidu.com/view/480950.htm

[5] 何明星,等.高效的可证明安全的无证书数字签名方案[J].电子科技大学学报,2015,44(6):887-891.

[6] 陈财森,等.针对RSA算法的踪迹驱动数据Cache计时攻击研究[J].计算机学报,2014,37(5):1039-1051.

[7] 程磊.基于AES和RSA的网络数据加密方案[J].现代电子技术,2015,38(09):87-89.

[8] 吴志军,赵婷,雷缙.基于改进的Diameter/EAP-MD5的SWIM认证方法[J].通信学报,2014,35(8):1-7.

[9] 百度百科[EB/OL].http://baike.baidu.com/view/7636.htm.

作者简介：

康保军(1970-)，男，硕士，系统分析师.研究领域：软件工程，数据库应用.