

# 面向电子政务网络的手机短信安全接入方法

吴 森, 邹 翔, 倪力舜

(公安部第三研究所 信息网络安全公安部重点实验室, 上海 201204)

**摘 要:** 针对电子政务网络的特点和使用中存在的问题, 设计了一种面向电子政务网络、采用手机短信方式的安全接入方法。给出了手机短信安全接入技术的安全要求和整体架构, 设计了安全短信接入平台, 提出了一种 SIM 卡端和短信网关之间的密钥协商协议, 对方法涉及的技术进行了深入的阐述。最后分别对方法的性能和安全性进行了实验和分析。实验结果表明, 该方法在接入电子政务网络时, 能确保电子政务网络中重要信息的安全和保密, 同时在性能上也能达到预期。

**关键词:** 安全短信; 移动安全接入; 电子政务网络

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2011)03-0161-04

## E-Government Network Secure Access Approach by Using Cell Phone Short Message Service

WU Miao, ZOU Xiang, NI Li-shun

(Key Laboratory of Information and Network Security, 3rd Research Institute, Ministry of Public Security, Shanghai 201204, China)

**Abstract:** According to the specialty of the e-government network and the problem in using e-government network, a secure access technology using cell phone short message is designed. Give the security requests of the technology and architecture of deployment. The secure short message platform and key agreement protocol between SIM card and short message gateway are designed. The key technology is discussed. The results are analyzed. The results demonstrate that the approach can keep the information in e-government safe and has good performance.

**Key words:** secure short message service; mobile secure access; e-government network

### 0 引 言

随着我国电子政务网络的建设和不断完善, 各级政府、机关单位对电子政务信息系统的依赖性也与日俱增, 重要关键信息数据量也日趋庞大。电子政务信息涉及国家安全、经济利益和公民隐私<sup>[1-3]</sup>。

在某些特殊领域, 为了安全保密需要, 所有的网络应用系统都是部署在电子政务网络内部的, 这种部署方式完全确保了特殊关键信息的安全和保密。但是在使用过程中也逐渐发现了一些使用上的问题。通常要接入电子政务网络获取信息就必须使用装有特殊软件的专用计算机客户端进行接入操作, 这种方式对于办公室人员来说没有任何问题, 但是对于一线人员, 他们就无法及时地接入电子政务网络, 无法及时获取相关的重要信息, 对工作开展带来一些麻烦。例如工作在一线的交警无法在现场及时有效地获取违法车辆的详

细信息等等, 同时现有的方案<sup>[4-7]</sup>无法很好地满足文中的需求。

针对上述情况, 设计了一种面向电子政务网络的手机短信安全接入方法, 有效解决这一问题。

文中主要工作如下:

(1) 改造 SIM 卡<sup>[8]</sup>, 加入 PKI 体系、商密算法和自定义功能菜单。

(2) 设计安全短信接入平台。

(3) 提出了一种基于 SIM 卡端和短信网关之间的共享密钥协商协议。

(4) 根据特定的业务需求, 开发服务代理程序, 根据短信指令从电子政务网络中获取相关信息。

### 1 电子政务网络手机接入安全要求

手机短信是在公网上传输的, 任何在公网上传输的数据都可能被黑客监听和截获, 所以为了保证电子政务网络中重要关键信息的安全和保密, 提出了以下几点安全要求:

(1) 共享过程密钥安全: A 端和 B 端之间的每一

收稿日期: 2010-07-20; 修回日期: 2010-10-17

基金项目: 国家 863 计划项目 (2008AA01Z412)

作者简介: 吴 森 (1982-), 男, 研究实习员, 硕士, 研究方向为网络信息安全。

次密钥协商都应该生成唯一的共享过程密钥  $KS$ 。确保过程密钥在传输时的安全。能定时主动更新过程密钥。

(2) 密钥攻破假冒: 假定实体 A 的长期私钥被公开, 显然知道该私钥的攻击者能假冒 A, 因为私钥唯一标识一个实体。然而, 理想的情况是即使密钥被公开, 其它实体仍不能冒充实体 A。

(3) 存储的安全性: 包括私钥、公钥和过程密钥的存储安全, 私钥不能随便导出等。

(4) 短信传输的安全性<sup>[9]</sup>: 短信的传输需通过公网连接到移动运营商, 所以要求在传输过程保证短信的安全和保密, 即使被黑客截获也无法得到真实的内容。

## 2 电子政务网络手机安全接入方法设计

### 2.1 总体拓扑结构

电子政务网络手机安全接入方法的总体拓扑结构如图 1 所示。

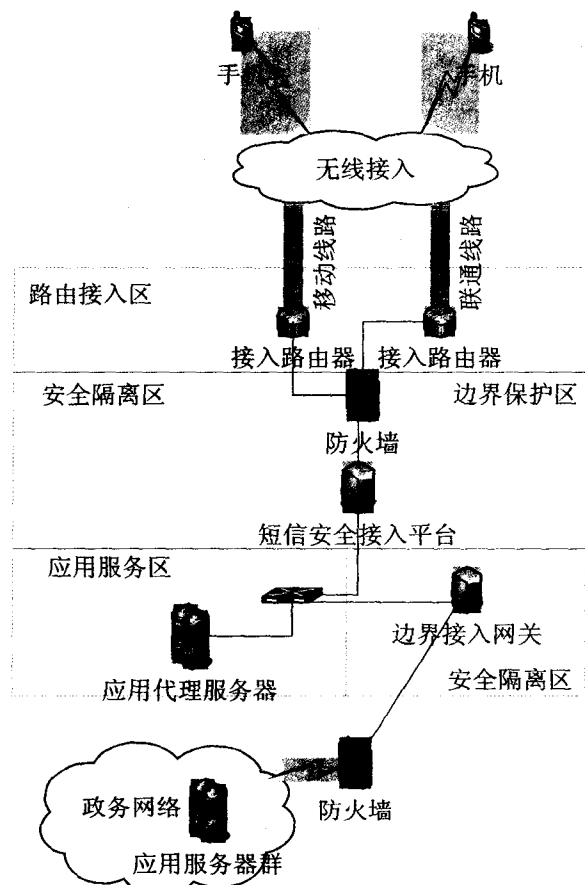


图 1 总体拓扑结构

要进行安全接入, 需要使用安全 SIM 卡, 并且需要定制手机的服务功能菜单。无线接入区就是移动/联通/电信运营商网络。用户使用手机通过无线接入网络连接到短信安全接入平台, 短信安全接入平台负

责上/下行短信的加密/解密、短信的解析和发送。短信安全接入平台解析短信请求之后, 调用应用代理服务器中的代理程序获取电子政务网络中的信息。应用代理服务器是短信安全接入平台和业务应用之间的桥梁, 用于穿透边界接入网关。边界接入网关的作用是使得公网通过身份认证能直接访问电子政务网络。按照图 1 中的拓扑结构部署, 完成短信安全接入。

### 2.2 SIM 卡安全初始化

安全 SIM 卡是在普通的 SIM 卡上增加了 PKI 体系、商密专用算法和自定义功能。文中所有对 SIM 卡的读取和写入操作都是使用特定的 SIM 卡写卡器来完成的。

安全 SIM 卡安全初始化过程实际就是 SIM 卡端生成卡端 RSA 密钥对(部分算法参考了文献[10]), 同时和安全短信网关程序之间互相交换 RSA 公钥的过程, 如图 2 所示。

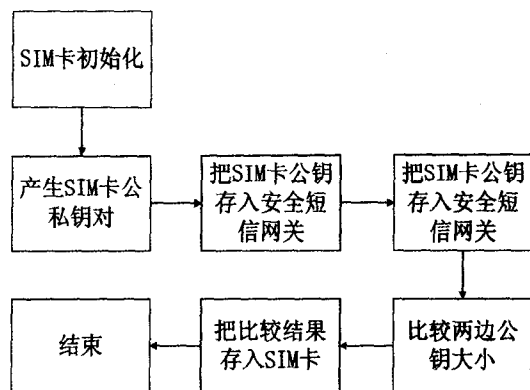


图 2 SIM 卡安全初始化过程

其中“把比较结果写入 SIM 卡”这一环节, 是由于 SIM 卡本身没有比较两端公钥大小的功能, 所以在开卡过程中需要预先写入大小的比较结果。在文中后面的过程中, 需要完成两次 RSA 操作, 一次是使用 SIM 卡的公钥加密共享过程密钥和验证因子, 第二次是使用短信网关的私钥完成签名。RSA 操作的先后次序和公钥的大小有关, 在下面的章节中有说明, 所以此结果非常重要。

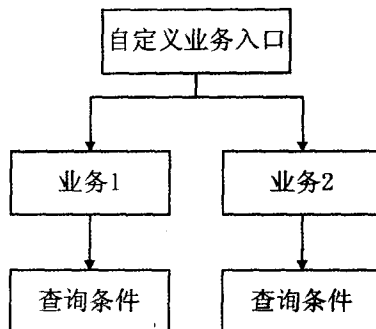


图 3 安全 SIM 卡自定义菜单结构

同时为了通过使用手机短信调用特定的业务程

序,必须在 SIM 卡中加入自定义的菜单。使用特定的程序和 SIM 卡写卡器把菜单文件烧入 SIM 卡中。自定义菜单的格式如图 3 所示。根结点代表手机菜单的入口,点击手机中的“自定义业务入口”,进入有两个业务组成的二级菜单,每个二级菜单分别对应一个短信命令字。点击二级菜单“业务 1”进入,输入查询条件即可完成特定信息查询。

### 2.3 安全短信接入平台设计

安全短信接入平台模块结构如图 4 所示,安全短信平台建立在分布式的多模块结构基础上。通讯网关与业务应用完全分离,整个系统的模块间通讯使用消息队列 MSMQ 来完成。

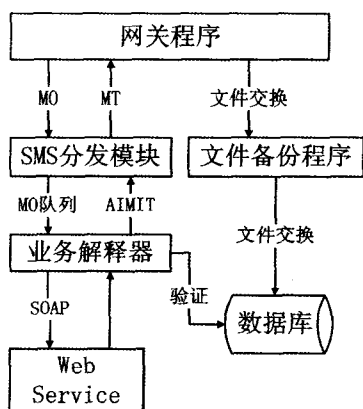


图4 安全短信网关平台模块结构

网关程序借助移动的 CMPP 协议<sup>[11]</sup>和联通的 SGIP 协议<sup>[12]</sup>与移动/联通网关连接,将下行消息提交到移动/联通网关,接收来自用户的上行消息,同时写回 MO 队列,并完成备份上下行和状态报告的数据信息。

SMS 分发模块为消息路由模块,完成短消息的上下行分发工作。提供业务特征配置、路由分发的功能,可通过配置对用户上行消息进行分发到各业务解释器,最后由解释器对用户上行指令进行解析处理,完成跟用户的交互工作。而对于下行消息,程序可实现路由分发功能,把消息分布到用户所属地区的网关进行发送。

业务解释器负责业务流程解释和控制。通过短消息跟用户进行交互。

Web Service 模块就是部署在应用代理服务器中的一系列应用接口,负责查询电子政务网络中特定的数据,将数据返回给业务解释器。

### 2.4 短信共享密钥协商协议设计

短信密钥协商协议设计方案是通过安全初始化后的安全 SIM 卡和网关程序互相配合完成基于公钥体制的共享密钥的协商,使用协商得到的共享密钥加密和解密短消息。所有的密钥协商请求和应答都是基于

短信的形式。

文中使用 RSA 算法进行数字签名和共享密钥协商,密钥长度为 1024 bit。共享密钥协商协议如图 5 所示。

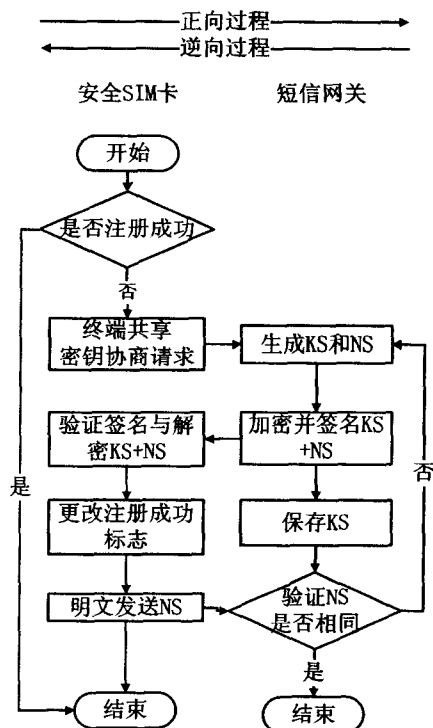


图5 共享密钥协商协议

在用户使用安全 SIM 卡的情况下,安全 SIM 卡会检测用户是否已经注册,若没有注册则自动以短信的方式向安全短信网关发送“终端共享密钥协商请求”,安全短信网关在收到短信请求后,随机生成共享密钥 KS 和一个验证因子 NS,安全短信网关使用用户安全 SIM 卡的公钥加密 KS 和 NS,并且使用自己的私钥签名 KS 和 NS,以短信的方式发回安全 SIM 卡。安全 SIM 卡在收到安全短信网关发来的短信后,使用自己的私钥解密 KS 和 NS,用安全短信网关的公钥验证 KS 和 NS 的签名,在数据库中把该手机对应的用户信息修改成已注册,同时用明文短信的方式向安全短信网关发送验证因子 NS,安全短信网关收到安全 SIM 卡发来的验证因子 NS,和自身保留的验证因子进行比较,若一致的话,协商过程成功结束,反之则要重新生成 KS 和 NS,重新进行密钥协商过程。

协商完毕之后,就可以使用安全手机接入电子政务网络。所有的短信接入都使用协商得到的共享密钥 KS,采用 3DES 密钥算法加密和解密短信内容。SIM 卡使用共享密钥 KS 加密短信,通过公网发送到移动运营商,移动运营商再把短信发送到安全短信平台,短信网关程序接收之后,解密短信,通过分发模块发送到业务解释器,业务解释器根据短信的业务要求调用不

同的 web service 接口从电子政务网络中获取特定的信息,获取的信息以同样的安全短信方式返回到用户的安全手机中,从而完成了电子政务网络的短信安全接入。

加密和签名过程需要注意以下情况。

正向过程:如果短信网关公钥小,先以 PKCS#1 填充方式用短信网关公钥加密,然后再以无填充方式用 SIM 卡私钥签名;如果 SIM 卡公钥小,先以 PKCS#1 填充方式用 SIM 卡私钥签名,然后再以无填充方式用短信网关公钥加密。

逆向过程:如果短信网关公钥小,先以无填充方式用 SIM 卡公钥验证,然后再以 PKCS#1 填充方式用短信网关私钥解密;如果 SIM 卡公钥小,先以无填充方式用短信网关私钥解密,然后再以 PKCS#1 填充方式用 SIM 卡公钥验证。由于篇幅限制,具体算法在此不做详细阐述。

### 2.5 Web Service 代理程序开发

Web Service 模块就是部署在应用代理服务器中的一系列应用代理接口,负责查询电子政务网络中特定的数据,将数据返回给业务解释器。使用 Visual Studio 2008 平台 C#语言开发 Web Service 代理程序。在开发 Web Service 应用代理接口时,遵循以下规则。

[ WebMethod ]

```
public string[] run(string[] QueryString) {}
```

Web 方法的参数是一个 string 类型的数组。string[0]代表短信命令字,string[1]代表查询的关键词。返回值也是 string 类型的数组。string[0]存放出错信息,从 string[1...n]存放查询到的结果。

短信的格式为(短信命令字,关键词 1,关键词 2...),由安全短信接入平台中的业务解释器解析之后传送给 Web Service 接口。

## 3 实验结果与安全性分析

测试环境如下:

(1)安全短信接入平台:CPU:Intel(R) Core(TM) 2 Quad CPU Q9550 @ 2.83GHz 2.83GHz,内存:4.00 GB。

(2)软件环境:Windows 2003 Server 操作系统,SQL Server 2005 数据库。

(3)手机:多普达 Windows Mobile 智能手机。

### 3.1 性能分析

测试的前提是网络环境通畅,和运营商的连接正常。在 SIM 卡正常安全初始化后,通过自定义菜单连续发送接入查询,到收到结果为止,分别在硬加密和软加密方式下进行了测试。

测试结果如表 1 所示。

表 1 性能分析表

连续接入次数	硬加密(秒)	软加密(秒)
50	223	331
100	509	712
200	1121	1500

从表 1 中可以看出在效率上硬加密的方式明显优于软加密的方式,采用硬加密方式的安全短信接入速度符合预期目标,用户在使用过程中不会感觉有明显的等待感。

### 3.2 安全性分析

(1)共享过程密钥的安全性。要使用手机短信接入政务网络,必须使用安全初始化之后并且成功注册的安全 SIM 卡。安全 SIM 卡在注册时会和安全短信网关程序进行协商,获得唯一的共享密钥 KS,共享密钥在 SIM 卡端和安全短信网关之间的传输都经过加密和签名,完全保护了共享密钥的安全和完整。

(2)密钥存储安全性。SIM 卡端的 RSA 密钥对和共享过程密钥存储在 SIM 卡中,安全短信网关的 RSA 密钥对存储在硬件加密卡中,用户无法导出私钥,所有的 RSA 密钥对都不在本地硬盘上驻留。安全短信网关拥有的共享过程密钥加密之后存储在数据库中。同时 SIM 卡端和安全短信网关之间能定时更新共享过程密钥。这些措施都能最大程度保证密钥的安全。

(3)密钥攻破假冒。虽然 SIM 卡中的私钥是无法导出的,但是一旦某块经过安全初始化后的安全 SIM 卡丢失,恶意用户可以使用该 SIM 卡接入电子政务网,相当于密钥被攻破了。本方法也提供了 SIM 卡遥毁功能,管理员通过管理平台向处于开机状态的 SIM 卡发出遥毁指令,SIM 卡接到指令后,就无法再接入电子政务网络。

(4)短信内容的安全性。短信内容传输都会经过公网,SIM 卡端和短信网关之间的密钥协商,发送短信操作都是基于短信的形式。在密钥协商阶段,所有的协商请求和应答,包括共享过程密钥的传输都是使用 RSA 算法加密和签名的。在用户使用阶段,所有的短信内容使用协商得到的共享过程密钥加密/解密的,在公网一段传输的短信都是密文。所以能有效保证以短信为载体的信息安全和保密。

## 4 结束语

文中设计了一种面向电子政务网络的手机安全接入方法。实验表明该方法有效解决了使用手机短信的方式安全接入电子政务网络的问题,具有很高的安全性和实用性,能完全保证电子政务网络中重要关键信

(下转第 169 页)

明显;但是随着恶意节点的比例不断增加,在文中的信任机制下从评价标准、异常评价概率、交易时间以及交易金额等对信任度的计算更加科学,使得用户能够选择信任较高的节点交易。

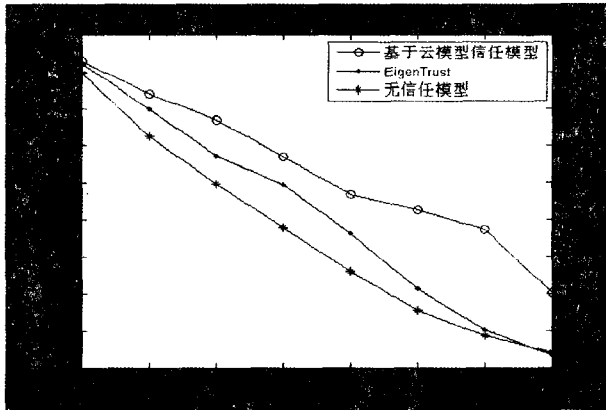


图1 恶意节点比例不同时不同模型之间的对比

## 6 结束语

文中提出了一种电子商务信任机制,该机制充分考虑了每个人的评价尺度,将每个人心中的价值映射到同一可比较的坐标中。考虑了时间对信任的影响程度,可以有效预防恶意节点通过小额交易获得高信任度,同时可有效防止战略性恶意行为。在文中机制下,用户可以较为准确地对善意和恶意节点进行区分判断,正确选择高信任度节点进行交易,从而降低恶意交易行为发生的概率,提高了电子商务交易的安全性。

(上接第164页)

息的安全。该技术不但能应用于公安网,还能应用在军网、海关等其它政务网络。该技术目前还存在一些局限,只支持文字短信,下一步的工作就是研究如何支持多媒体短信。

## 参考文献:

- [1] 吕欣. 信息通信新技术环境下电子政务安全保障[J]. 信息网络安全, 2010(2): 19-20.
- [2] 王昊, 赵文静, 边根庆. 基于三方通信构架电子政务安全系统的研究[J]. 计算机技术与发展, 2007, 17(10): 242-244.
- [3] Zhou Zhitian, Hu Congyang. Study on the E-government Security Risk Management[J]. IJCSNS International Journal of Computer Science and Network Security, 2008, 8(5): 208-213.
- [4] 孙亮, 张来顺. 基于J2ME的无线安全研究与应用[J]. 网络安全技术与应用, 2008(11): 70-72.
- [5] 任中岗, 武锦峰, 赵国磊. 移动警务安全短消息通信系统

## 参考文献:

- [1] 张宇, 陈华钧, 姜晓红, 等. 电子商务系统信任管理研究综述[J]. 电子学报, 2008(10): 2011-2020.
- [2] 姜守旭, 李建中. 一种P2P电子商务系统中基于声誉的信任机制[J]. 软件学报, 2007, 18(10): 2551-2563.
- [3] Marsh S P. Formalising Trust as a Computational Concept[D]. Scotland: University of Stirling, 1994.
- [4] Kamvar S D, Schlosser M T, Molina H G. The eigenTrust algorithm for reputation management in P2P networks[C]//In: Proc. of the Twelfth International World Wide Web Conference. New York: ACM Press, 2003: 640-651.
- [5] 李德毅, 刘常昱. 论正态云模型的普适性[J]. 中国工程科学, 2004, 6(8): 28-34.
- [6] 石志国, 刘冀伟, 王志良. 基于时间窗反馈机制的动态P2P信任模型[J]. 通信学报, 2010, 31(2): 120-129.
- [7] Li Xiong, Ling Liu. A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities[C]. the IEEE International Conference on E-Commerce(CEC'03). [s.l.]: [s.n.], 2003.
- [8] 李德毅. 不确定性人工智能[M]. 北京: 国防工业出版社, 2005.
- [9] 李德毅. 知识表示中的不确定性[J]. 中国工程科学, 2000, 2(10): 73-79.
- [10] 吕辉军, 王晔, 李德毅, 等. 逆向云在定性评价中的应用[J]. 计算机学报, 2003, 26(8): 1009-1014.
- [11] 孟祥怡, 张光卫, 刘常昱, 等. 基于云模型的主观信任管理模型研究[J]. 系统仿真学报, 2007, 19(14): 3310-3317.
- [12] 彭冬生, 林闯, 刘卫东. 一种直接评价节点诚信度的分布式信任机制[J]. 软件学报, 2008, 19(4): 946-955.

设计[J]. 计算机技术与发展, 2006, 16(3): 173-175.

- [6] Katankar V K, Thakare V M. Short Message Service using SMS Gateway[J]. (IJCSSE) International Journal on Computer Science and Engineering, 2010, 2(4): 1487-1491.
- [7] Ahmeda S, Edwila A A M. Secure Protocol for short Message Service[J]. World Academy of Science, Engineering and Technoogy, 2009, 49: 864-868.
- [8] 杨振华. IC卡技术及其应用[M]. 北京: 科学出版社, 2006.
- [9] 邹翔. 电子政务网络移动安全接入体系及关键技术研究[J]. 信息网络安全, 2007(2): 52-54.
- [10] 姚国祥, 林良超. RSA密钥对高效生成算法[J]. 计算机工程, 2007, 33(20): 148-149.
- [11] 中国移动通信集团公司. QB-GF-028-2003 中国移动通信互联网短信网关接口协议[S]. 2003.
- [12] 中国联合通信公司. 中国联合通信公司短消息网关系统接口协议[S]. 2003.