Analysis on Security Strategy of Double-factor Authentication in Unified Logistics Information System

LIN Xing-zhi

Guangxi Economic Management Cadre College，Nanning，Guangxi，530007，China

lxz4562509@139.com

Abstract: According to the safety technical requirements of modern logistics information system and the characteristics of unified information communication technology, through the analysis of unified logistics information system and authentication technology with RSA double factors, this paper puts forward the authentication security strategy and interactive double-factor solutions for unified logistics information system, combining the objective and task achieved by RSA double- factor authentication technology in unified logistics information system. Double-factor authentication in unified logistics information system is an innovative security authentication technology system, constructed by computer technology and Internet technology integrated telecommunications with the integration of RSA double factors. In the omnipresent logistics information service environment, the author designs the hardware token authentication, the mobile token authentication, the mobile phone text messages token authentication, etc. implementing the core verification and signature of double-factor authentication by J2EE technology. Testing through JAVA, its results show that the double-factor authentication of unified logistics information system is feasible in realization model and strategy.

Keywords: Logistics；Unified information system；Double-factor authentication ；Security strategy

物流统一信息系统双因素认证安全策略分析

林兴志

广西经济管理干部学院，广西南宁，中国，530007

Lxz4562509@139.com

【摘要】通过对物流统一信息系统与 RSA 双因素认证技术的分析，根据现代物流信息系统的安全技术要求与统一信息通信技术的特点，结合 RSA 双因素认证技术在物流统一信息系统中实现的目标和任务，提出了物流统一信息系统交互式双因素认证安全策略与解决方案。物流统一信息系统双因素认证是运用计算机电信集成技术与互联网技术融合 RSA 双因素认证技术构建的创新安全体系，在无所不在的物流信息服务环境中设计了硬件令牌认证、移动令牌认证、手机短信令牌认证等便捷的认证方式与方法，采用 J2EE 等技术实现了双因素认证的核心验证与签名。通过 JAVA 等测试结果输出表明，物流统一信息系统双因素认证在实现模式与策略上可行。

【关键词】物流；统一信息系统；双因素认证；安全策略

1 引言

物流统一信息系统(Unified Messaging System，UMS) 存在于无所不在的物流服务领域中，具有推动经济与社会发展的战略意义，是计算机电信集成(Computer Telecommunication Integration，CTI)、Internet 和管理思维的有机融合应用[1-2]。系统以一种开放式的服务架构形式存在，在应用上将固定电话、手机、PDA、掌上电脑和 Internet 提供的各种信息服务融合起来构成分布式的物流服务体系，在给用户与企业带来便利的同时，又给系统带来了储多方面的信息与系统安全隐患。强大的 “双因素认证”技术引入，给物流统一信息系统带来了安全领域中革命性的变革[3]。双因素认证在单一口令记忆因素前提上，增加第二个物理认证因素，以使

基金资助：广西经济管理干部学院基金项目《广西北部湾经济区物流统一信息系统研究》（10KYC008）;广西教育厅科研项目《基于区域经济的制造企业协同物流系统建模与优化》（200911LX541）。

978-1-935068-09-9

认证的确定性和安全性几何级递增。物流统一信息系统双因素认证机制，采用软硬口令结合的方式，将有效卡和静态 PIN 密码结合使用，提供了足够的安全级别，以支持用户对物流统一信息系统服务及业务流程的安全访问[4]。

2 物流统一信息系统双因素认证概述

物流统一信息系统采用 B/S 模式，硬件和接口程序有 NGN（Next Generation Network，下一代网络）、CTI 服务器、ISMG（Internet Short Message Gateway，短信网关）和 GSMmodem（GSM 调制解调器）等，可基于 API(Application Programming Interface，应用程序编程接口)接口开发各种包括交互式语音呼叫、视频、信息在内的特色物流统一信息增值服务[5-6]。多硬件与软件开放性接口的融合应用，给系统带来了多方面的安全隐患，但系统与接口的开放性恰给 RSA 双因素认证技术很好的支持平台，使安全认证技术的应用具有便捷性和可用性[7]。双因素身份验证系统主要由三个模块组成:动态口令产生模块、客户端代理模块和验证服务器模块。

RSA 双因素认证是指，用已知的“PIN 码”加上计算出来的“令牌码”这两个要素组合到一起确认合法的身份，要求使用者在第一次使用令牌登录系统时即设定一个静态 PIN 码，用户每次登录系统时要输入“PIN 码+令牌码”，即构成一个完整的双因素口令[8]。RSA 双因素认证技术集成到一个认证令牌上，依据后台服务器的预定时钟，此令牌将和后台服务器同步产生一个新的且一次性令牌码，在物流统一信息系统中用户只需输入用户 ID 或 PIN，加上令牌产生的一次性令牌码，就可以完成认证过程。

RSA 双因素认证系统中，RSA SeucrID 由认证服务器（RSA Authentication Manager，AM）、代理软件（RSA Authentication/Agent）、认证设备以及认证应用编程接口（API）组成。RSA SecurID 认证令牌可以以硬件、软件和智能卡等多种形式向用户提供，使用唯一的 128 位种子将其初始化，每分钟都会使用一种算法，组合该种子与当前时间，生成一个随机的一次性口令。认证令牌选择有软件、硬件令牌，智能卡令牌、手机短信令牌、USB 令牌、移动设备令牌，且能运行在普通 PC、Palm、WinCE 操作平台上，以及存储种子的智能卡中。

RSA 双因素认证工作流程架构如“Figure 1”（图 1）所示：

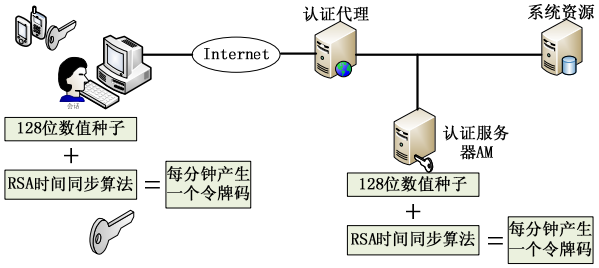

Figure 1. Dual authentication framework. Factors

图 1. 双因素认证架构

当用户试图访问受保护的物流统一信息系统时，连接设备中内置的专用代理软件（RSA ACE/Agent）将启动一个 RSA ACE/Server 认证会话，用户需要输入用户名及由 RSA SecurID 认证设备生成的用来代替密码的令牌代码，外加一个 PIN 号码，由代理软件传输给 RSA ACE/Server，如果信息有效，RSA ACE/Server 将允许用户访问。用户将被授予与其通行证等级相对应的访问权限，这一权限被 RSA ACE/Server 记录在日志文件中。

3 统一信息系统双因素认证安全策略构建

3.1 软硬件与移动双因素认证

RSA 双因素认证需要多个身份认证因素并采用先进技术的系统，通过密钥和加密验证用户的身份，为物流统一信息系统的用户提供证据确凿的用户身份认证。物流统一信息系统双因素认证解决方案根据统一信息系统移动性与分布性的特点，根据不同用户要求采用硬件令牌、手机短信令牌、移动令牌等生成一次性密码，结合用户的 PIN 码来确保安全性。认证流程如“Figure 2”（图 2）所示：

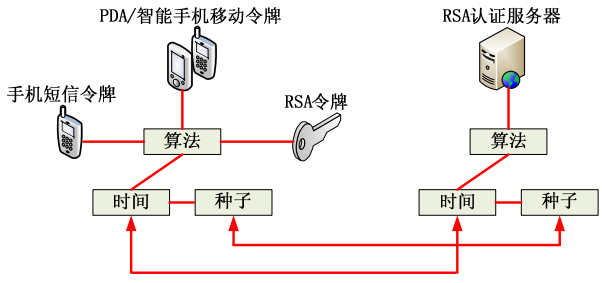

Figure 2. Dual authentication process factors

图 2. 双因素认证流程

硬件令牌认证：主要令牌设备有 RSA 硬件令牌、智能卡令牌、USB 令牌等，硬件令牌认证使用相对简单，只需按动令牌上的按钮或把令牌插入电脑的 USB 接口中，把即时产生的令牌码与 PIN 码组合便能实现系统的双因素认证和安全地访问物流统一信息系统。

移动令牌认证：移动令牌认证是一个软件令牌，主要运行在 Windows 操作系统或 PDA、智能手机上，由于它可用于用户的移动设备，刚好适应了物流统一信息系统的移动性与分布性的特点。这是一种基于软件的认证解决方案，可以在多种流行的移动电话平台上生成一次性密码，这些平台包括 Palm、BlackBerry、Windows Mobile 和具有 J2ME 功能的设备，软件产品有 MobilePass®等系列。两种认证方式：一是基于移动设备的直接访问物流统一信息系统，在设备访问物流统一信息系统的 WEB 界面时同时启动软件令牌程序，点击确认后实现系统登录，在使用方法上与 USB 令牌相类似；二是在其他电脑操作系统上登录物流统一信息系统时，启动移动设备中的软件，以一键确认的方式产生一次性令牌码。

手机短信令牌认证：手机短信令牌是一个便利性操作令牌，用户以 WEB 等方式登录物流统一信息系统时，系统以事件触发的方式触发手机短信令牌管理模块，管理模块按用户预先认证的手机号码启动令牌算法计算机出一次性令牌码，通过 GSMmodem 或短信网关把令牌码以短信方式发送给用户已认证的手机，并设定一定的访问限制时间，超过限制时间后令牌码自动失效。工作流程如“Figure 3”（图 3）所示：

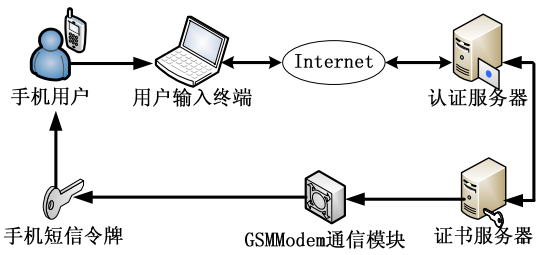

Figure 3. SMS authentication process token

图 3. 手机短信令牌认证流程

3.2 双因素认证核心验证实现

物流统一信息系统采用 J2EE 平台作为核心组件技术[9]，在系统访问的 RSA 双因素认证中使用会话实体来实现身份认证过程中的业务逻辑处理：第一步，映射数据库和认证实体，根据用户名取得证书映射名；第二步，实现认证会话和密钥库通信，通过证书名取得对应证书的公钥；第三步，用户验证，根据公钥认证后决定用户对物流统一信息系统相应模块的访问权限。部分代码如下：

```
SIGN-UKEY(signbytes , tosignbytes , PrivateKeyfilename , PrivateKeypassword , Certificatename)  //密钥地址（PrivateKeyfilename），证书名（Certificatename）等
FileInputStream fIn=
  new FileInputStream(PrivateKeyfilename.trim());
PrivateKey ks_UKEY=PrivateKey.getInstance("UMS");
ks_UKEY.load(fIn，passwd.toCharArray());  //密钥库密码（passwd）
cert_UKEY=ks_UKEY.getCertificate(certname.trim());
fIn.close();
Signature sig_UKEY Signature.
  getInstance("MD5withRSA"，"SunRsaSign" );
sig_UKEY.initUKEY(cert_UKEY.getPublicKey());
sig_UKEY.update(signbyte.getBytes());
Boolean flag=sig_UKEY.UKEY(sigBytes);
reture flag;
```

3.3 双因素认证签名实现

物流统一信息系统利用 RSA 硬件令牌、手机短信令牌、智能 PDA 与手机移动令牌等和信息系统签名服务器进行交互式认证通信，根据令牌时间戳进行签名，签名算法采用 RSA 双因素认证密码算法。实现步骤：第一步，初始化硬件或软件；第二步，找出所有认证端的证书；第三步，以时间、软硬件、用户名等为因素启动 RSA 算法；第四步，启动 MD5 签名引擎；第五步，私钥初始化引擎，更新认证数据，最后实现签名。在私钥初始化引擎后主要通过以下代码实现签名：

```
Sig.initSign(Keystore);  //初始化 Key 引擎
Sig.update(signbyte.getBytes());  //更新数据
byte[]  signBytes=sig.sign();  //签名
return signBytes;
```

4 系统测试数据结果输出

测试环境：红帽 linux、MYSQL、8 通道

978-1-935068-09-9 © 2010 SciRes.

GSMModem、物流统一信息系统、RSA 认证服务器等，测试终端有 RSA 令牌、PDA、智能手机、普通手机。运用 JAVA 建立测试系统分硬件令牌（USBkey、RSA 令牌）、移动令牌（PDA、智能手机）、手机短信令牌对双因素认证密钥的 256bit、512bit、1024bit、2048bit 长度在物流统一信息系统认证时的令牌码初始化响应速度、计算签名摘要速度、服务器验证签名响应速度、回放时间是否同步等方面进行测试。在测试中摘要值使用 MD5 摘要函数，签名使用 RSA 签名函数，每种测试均采用 100 次平均值比较进行验证。在认证算法中，随着密钥长度的增加，安全性以几何倍数增加，且服务器对各种认证软硬件的响应时间均不超过 0.5 秒，回放的时间不同步，系统安全性能提高。测试结果输出如 Table 1（表 1）所示：

Table 1. Test results
表 1.测试结果输出

密钥长度	令牌	初始化	计算签名	服务器响应	回放同步
256 bit	硬件令牌	3659	71	428	N
	移动令牌	3781	72	431	N
	短信令牌	3856	75	447	N
512 bit	硬件令牌	4003	79	451	N
	移动令牌	4051	81	469	N
	短信令牌	4101	84	486	N
1024 bit	硬件令牌	4201	86	501	N
	移动令牌	4462	89	528	N
	短信令牌	4656	92	542	N
2048 bit	硬件令牌	4735	93	561	N
	移动令牌	4866	97	593	N
	短信令牌	4972	103	617	N

单位：ms

5 结论

物流统一信息系统双因素认证提供了整套的用户身份认证和安全管理解决方案，帮助物流企业和用户有效地管理和控制系统访问的安全性，有效地保护了业务数据和信息资源。同时，在物流统一信息系统中定义了不同的安全策略和实施方法，在移动业务处理设备、服务器、数据库系统、无线网络等各种应用中实现了安全的无所不在的统一信息服务功能。系统采用 RSA 双因素认证，保障了用户权益，较好地体现了信息技术在物流业务处理中的易用性与安全性，规避了系统在业务处理中大部分安全隐患。全球办公日趋步入移动状态，物流统一信息系统部署双因素认证，既保护系统移动用户登录身份的安全性与确定性，又推动了物流业务处理信息技术与物流信息系统的可持续发展。

致　谢

本文为广西经济管理干部学院科研项目《广西北部湾经济区物流统一信息系统研究》（10KYC008）、广西教育厅科研项目《基于区域经济的制造企业协同物流系统建模与优化》（200911LX541）的研究成果，在撰写与研究时得到了项目组成员的大力支持与帮助，在此深表感谢。

References (参考文献)

[1] LIN Xing-zhi1,WEI Ying,LUO Hai-peng.Research and Implementation of Unified Message Interactive Platform[J].Journal of Guangxi Academy of Sciences. 2010,26(1):23-26,31.
林兴志,魏鹰,罗海鹏.统一信息互动平台的研究与实现[J].广西科学院学报.2010,26(1):23-26,31.

[2] WEI Ying,LIN Xing-zhi,XIE Ming.Demand Analysis to Unified Logistic Information System in Guangxi Beibu Bay Economic Zone.[J].Enterprise Science and Technology & Development. 2010, (10):10-13.
魏鹰,林兴志,谢铭.广西北部湾经济区物流统一信息系统需求分析.2010,(10):10-13.

[3] LI Lan-yan,MAO Xue-shi.Dynamic Password Two-factor Authentication and Its Application[J].Computer Era. 2010,(04):11-13.
李兰燕,毛雪石.动态口令双因素认证及其应用[J].计算机时代.2010,(04):11-13.

[4] LI Xiu-ying.Scheme of Role-Based Access Control Based on Dual-factor Authentication[J].Microcomputer Information. 2010, (12):100-101,124.
李秀滢,彭静.基于双因素认证机制的角色访问控制方案[J].微计算机信息.2010,(12):100-101,124.

[5] LIN Xing-zhi1,WEI Ying1,LUO Hai-peng.Unified Messaging Service of Information System in Next Generation Network Environment[J].Journal of Guangxi Academy of Sciences. 2010, 26(2):167-170.
林兴志,魏鹰,罗海鹏.下一代网络环境下信息系统的统一信息服务构建[J].广西科学院学报.2010,26(2):167-170.

[6] LIN Xing-zhi.Integration Application of NGN and Universities and Colleges Unified Messaging System.[J]Journal of Guangxi Economic Management Cadre College.2010,(2):99-104,109.
林兴志. NGN 与高校统一信息系统融合应用[J].广西经济管理干部学院学报.2010,(2):99-104,109.

[7] Feng Xiaoling et al.Research on Two-factor Authentication based on RSA[J].Computer Development & Applications. 2009, (08):7-9.
冯小玲,张永奎.基于 RSA 的双因素身份认证应用研究[J].电脑开发与应用.2009,(08):7-9.

[8] HE Rong-yu.Dual-factor authentication scheme based on

WPKI[J].Computer Engineering and Design. 2009, (01):35-37, 135.
鹤荣育.基于 WPKI 的双因素认证方案[J].计算机工程与设计.2009,(01):35-37,135.
[9] JIA Ying-tao,ZHENG Jian-de.Study of Dual Factor Authentication System Based on J2EE Platform[J]. Journal of Xiamen University(Natural Science).2007,(01):43-46.
贾英涛,郑建德.J2EE 平台双因素认证的设计与实现[J].厦门大学学报(自然科学版).2007,(01):43-46.

978-1-935068-09-9 © 2010 SciRes.