支付网关系统的保护神－数字证书的设计

the protector of payment gateway system—design of digital certificate

易永丰 （华夏银行信息技术部 100032）

摘要：安全性是银行支付网关系统能否得到推广应用的关键因素之一。本文主要讨论在支付网关系统中如何利用 CFCA 的数字证书的安全机制进行系统设计。

关键词：支付网关 数字证书 CFCA CC CS

1 概述

1.1 证书使用简介

支付网关系统涉及的实体对象

(1) 按交易实体分有：持卡人、商家、银行

(2) 按系统结构分有：客户浏览器、商家网站、银行支付网关

银行与商家之间要互相认证，消费者与银行之间要相互认证，这就需要一个可信的第三方的认证机构给各方颁发证书并进行认证，中国金融认证中心(CFCA)正好就是这样一个机构。因此，银行与消费者之间的认证，采用银行安装 WEB 服务器证书，个人消费者使用个人普通证书的认证方式；而商家与银行之间的认证，则采用每个商家都申请 CFCA 企业高级证书，银行支付网关也申请 CFCA 高级证书来进行商户与银行之间的认证、加解密和数字签名。第一种应用情况的设计实现比较简单，本文主要阐述第二种应用情况的设计。

1.2 系统功能描述

为了使在网络上传输数据的安全性得到切实的保证，支付网关系统中对于从商家客户端 ilink 向银行服务器 PCS 发送的数据，全程使用 CFCA 的证书 API 进行加密保护。

数据加密保护过程如图 1 所示：

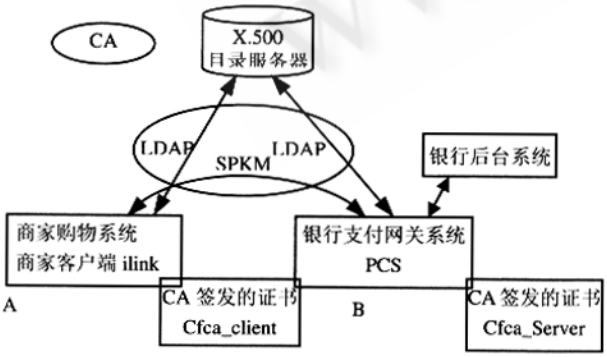

图 1 数据加密保护过程

1.3 系统组成介绍

证书系统由服务器端和客户端组成。服务端以 UNIX 平台为例，客户端以 windows 平台为例。

2 支付网关系统认证总体架构

说明：

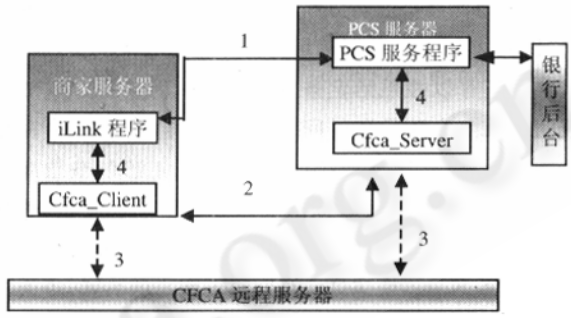

图 2 系统认证总体结构图

Cfca_Client 认证客户端程序，封装了 EntrustToolKit 的 API，负责建立和维护通信的安全通道，对 iLink 请求信息进行加密和解密。以下简称为 CC。与之相对应的是 Cfca_Server 认证服务端程序。以下简称为 CS。

实线连接 1 表示完成定单信息传输。这些数据需要使用 CFCA 的证书加密以后传输。

实线连接 2 表示商家服务器 Cfca_client 与 PCS 服务器 Cfca_server 之间建立安全通道。分别保留安全通道句柄。

虚线连接 3 表示从 CFCA 得到证书的 CRL，验证证书。获得证书句柄。

实线连接 4 表示：

(1) iLink 程序与 CC。iLink 把需要加密或解密的信息送给 CC 进行处理，并从 CC 处得处理结果。在 NT 操作系统平台下，采用内存映射文件作为 iLink 和 CC 进行数据交换的通道。(2) PCS 服务程序与 CS。PCS 服务程序把需要加密或解密的信息送给 Cfca_Server 进行处理，并从

Cfca_Server 处得处理结果。在 UNIX 操作系统平台下，采用管道和消息队列作为 PCS 和 CS 进行数据交换的通道。

3 EntrustSession 基本的编程模式

(1) 发起人获得他的证书。为此，她需要先分别调用 ents_set_inifile() 和 ents_set_password() 指定她的 epf 文件和密码，然后她调用 gss_acquire_cred() 访问她的证书，如图 3 所示。

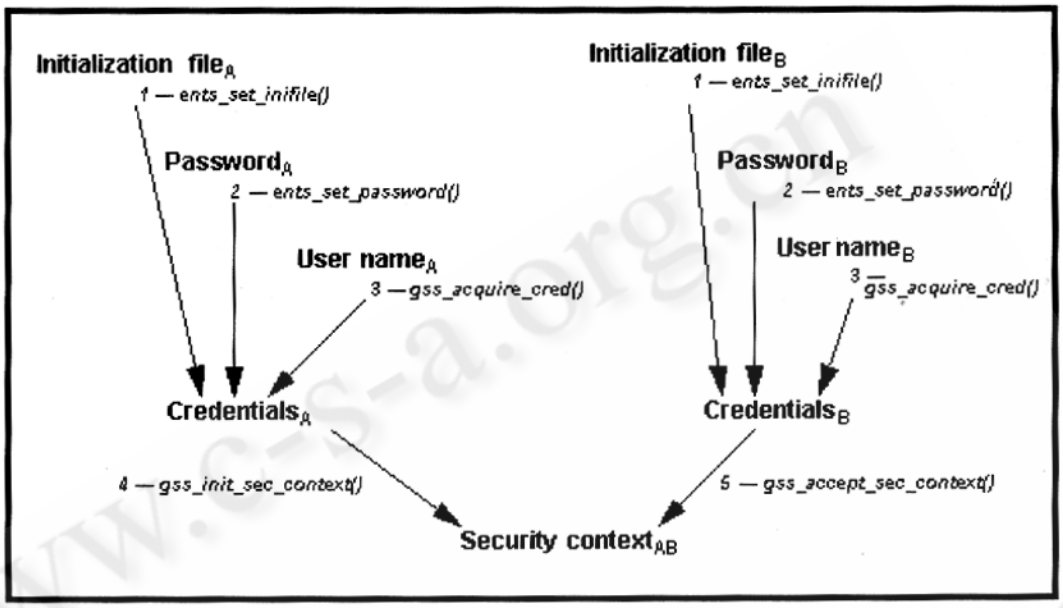

图 3　获得证书并建立安全通道

注意：

另外，证书也可以通过调用 ents_acquire_cred() 得到。该函数合并了 ents_set_password() 和 gss_acquire_cred() 的功能。

(2) 发起人指定她想建立联接并接收安全通道的目标。为此，发起人的应用程序调用 gss_init_sec_context()，该函数返回一个发起人的应用程序发送给目标程序的句柄。

(3) 当目标程序收到从发起人送过来的句柄后，可以通过 gss_accept_sec_context() 调用获得到对方的证书，如果它还没有这样作，gss_accept_sec_context() 函数返回一个输出句柄，目标的应用程序把该句柄发送给发起人，发起人需调用 gss_init_sec_context()。句柄的内容在建立安全通道时进行了交换，这一切是建立在安全的算法和认证模式上的。

(4) 一目标安全通道建立成功，发起人和目标就可以发送受保护的信息了。在这里有一对 GSS－API 函数用来进行对信息的保护。一对是 gss_get_mic() 和 gss_verify_mic()，用在信息和安全句柄分开传输时，这时句柄中包含信息的数字签名或 MAC。另一对 gss_wrap() 和 gss_unwrap()，它们用在信息加密传输或发送者只是简单的把信息的明文和数字签名或 MAC 放入句柄中传输时。

(5) 当对方收到受保护的信息时，如果信息是加密的，那么解密，并且验证数字签名或 MAC。发送方使用的函数是 gss_wrap()，接收方应使用 gss_unwrap()；发送方使用的函数是 gss_get_mic()，接收方应使用 gss_verify_mic()。这一过程如图 4 所示。

(6) 当安全通道不再使用时，通信双方都应调用 gss_delete_sec_context() 去删除本地的安全通道拷贝。

(7) 当建立安全通道时不再需要证书时，通信双方都应调用释放 gss_release_cred() 她或他的证书。

(8) 最后调用 ents_release_inifile() 释放初始化时调用 ents_set_inifile() 所占用的内存。

4 支付网关系统认证工作流程图(见图 5)

5 证书设计说明

(1) CC 是一个守护进程，负责维护与 CS 的安全通道、对客户端证书的认证、iLink 业务信息的加密和解密，它运行在后台。在 NT 操作系统上，可以作为一 NT 服务出现。iLink 把需要加密或解密的信息送给 CC 进行处理，并从 CC 处得处理结果。在 NT 操作系统平台下，采用内存映射文件作为 iLink 和 CC 进行数据交换的通道。

(2) CS 是一个守护进程，运行在后台。负责对服务端证书的认证、保存安全通道、PCS 业务信息的加密和解密。

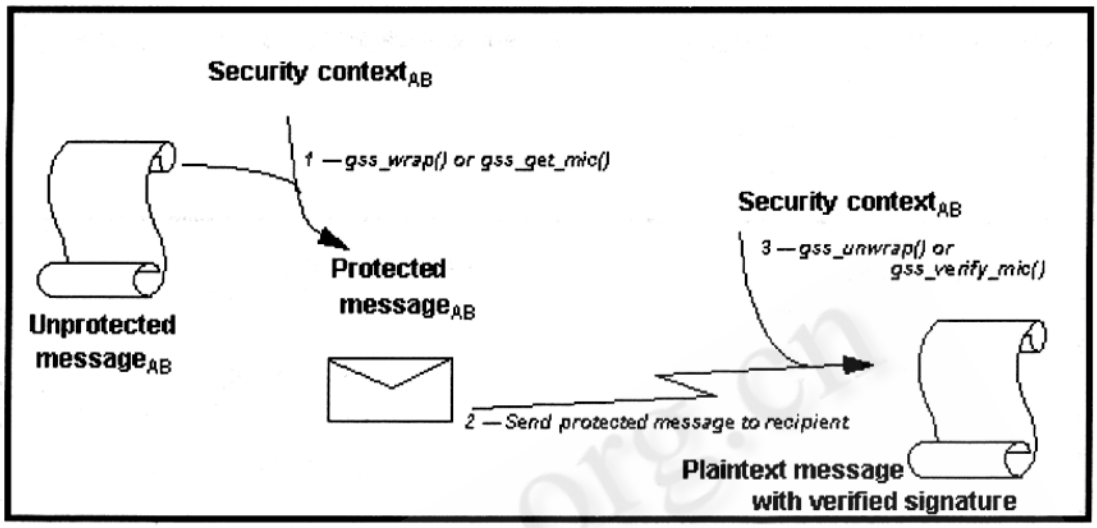

图 4　交换受保护的数据

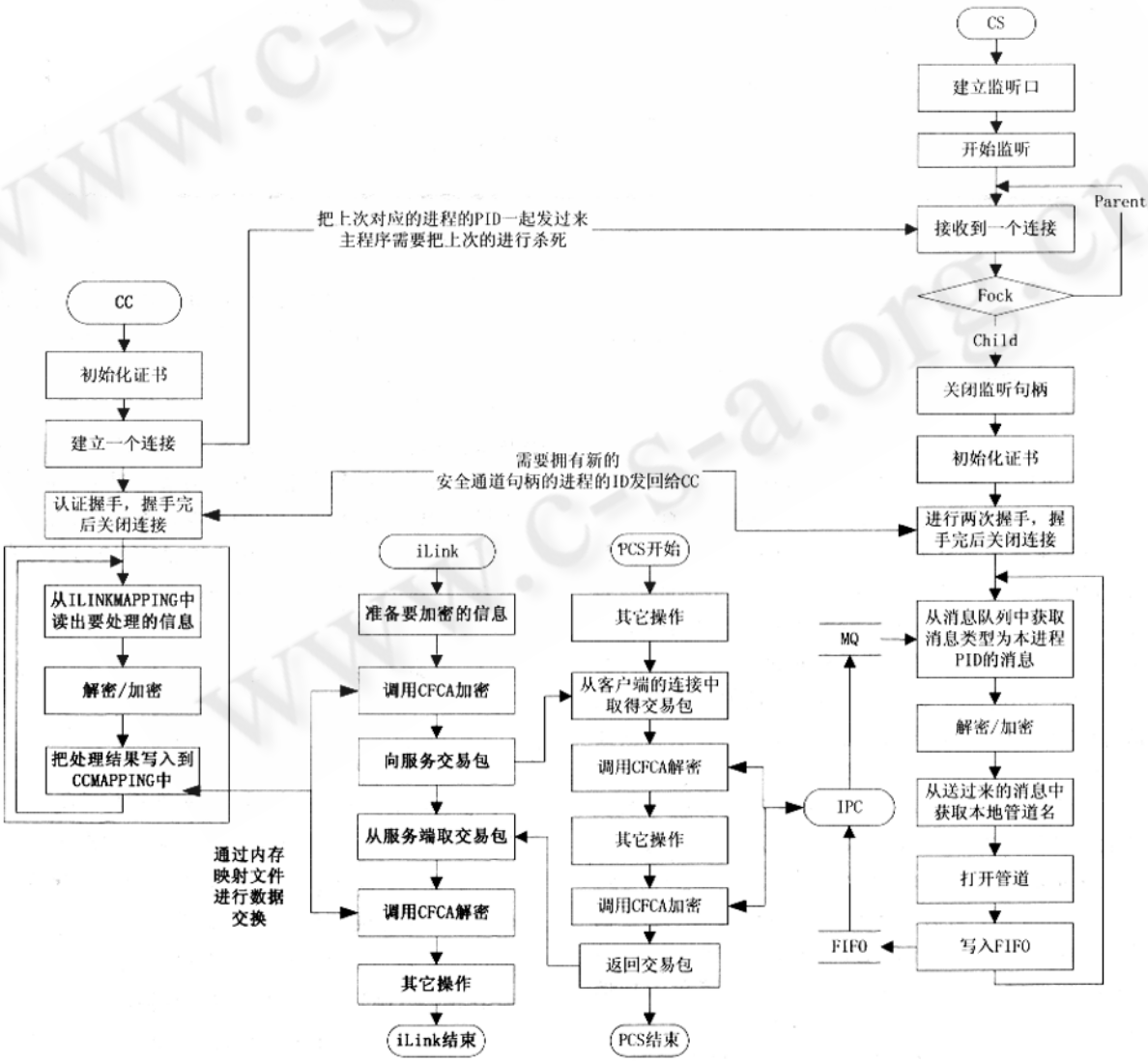

图 5　支付网关系统工作流程图

（下转第 56 页）

(上接第 52 页)

PCS 服务程序把需要加密或解密的信息送给 Cfca_Server 进行处理,并从 Cfca_Server 得到处理结果。在 UNIX 操作系统平台下,采用管道和消息队列作为 PCS 和 CS 进行数据交换的通道。

(3) iLink 与 PCS 服务器之间的通信信息都是经过发送方的加密签名和接收方的解密验证签名的,也就是说实在安全通道之内。

(4) CC 和 CS 在初始化证书时完成环境参数的初始化,包括初始化证书文件的配置文件信息、到 CA 验证证书。

(5) CC 负责定时(按参数配置)重建安全通道,每个安全通道都有唯一的安全句柄,CS 负责保存与客户端的安全句柄,并为每一个安全句柄产生一个子进程处理服务端的加密和解密。

参考文献

1 金融系统电子商务研究小组,电子商务安全认证与网上支付,人民出版社,1999.9。

2 杨波,网络安全理论及应用,电子工业出版社 2001.10。

3 Entrust Entrust Session Tookit。

4 卢开澄《计算机密码学:计算机网络中的数据保密与安全(第 3 版)》,清华大学出版社,2004.01。

5 段钢编《加密与解密(第二版)》,电子工业出版社,2003.06。

6 Charles P. Pfleeger Shari Lawrence Pfleeger《security Computer》,机械工业出版社,2004.01。