

安全电子邮件技术白皮书

Version 1.1



华翔腾数码 华翔腾数码科技有限公司

地址：长沙麓谷高新区麓龙路 199 号标志麓谷坐标 15 楼

邮编：410205

电话：(86) 731-88239608

传真：(86) 731-88239600

网址：WWW.WallGreat.com

目 录

1 安全电子邮件概述.....	2
1.1 定义.....	2
1.2 应用环境和应用领域.....	3
1.3 国内外发展概况.....	3
1.4 与其它系统的比较.....	4
2 安全电子邮件系统组成.....	7
2.1 PCI密码卡	8
2.2 智能密码钥匙.....	9
2.3 密钥管理中心（证书认证中心）	10
2.3.1 密钥管理中心结构.....	10
2.3.2 密钥管理系统功能.....	11
2.4 用户端应用系统.....	12
2.4.1 用户端应用系统组成.....	12
2.4.2 用户端应用系统功能.....	13
3 系统工作原理和过程.....	16
3.1 智能密码钥匙的发放.....	16
3.2 安全电子邮件发送与接收.....	17
3.3 用户证书的更新.....	17
4 支持环境.....	17
4.1 系统运行环境.....	17
4.2 系统基本配置.....	18
5 特点.....	20
6. 典型应用解决方案.....	21
6.1 区域性应用——基层政府部门间的公文交换	21
6.2 企业应用——企业间的商业文件交换	23
6.3 行业性应用——教育主管部门与各学校间的文件交换	24

1 安全电子邮件概述

1.1 定义

电子邮件是目前政府部门、教育系统、企业和个人之间传递数据的主要手段，许多重要敏感信息都可能通过电子邮件进行传输，但目前大部分人员对电子邮件的安全性重视不够，许多邮件都可能在未经授权的情况下被别人非法窃取或阅读。

湖南华翔腾数码科技有限公司与教育部教育管理信息中心校园卡标准化研究所联合开发的 SQY29 安全电子邮件系统，是一套以 PKI 技术为基础的，针对不同应用环境提供的安全有效而又经济易行的套件产品。该系统综合采用了国家密码管理局批准的安全密码算法与产品，保证了文件基于公用网络进行交换的机密性、完整性、可认证性和不可抵赖性。

SQY29 安全电子邮件系统，解决了部门之间、用户之间通过电子邮件方式进行重要文件传输与处理的安全性问题。它为系统提供电子邮件数据加密、数字信封、数字签名功能，弥补了普通电子邮件的安全性不足。SQY29 安全电子邮件系统不是邮件服务系统，而是对用户已有邮件系统的安全性补充。它适用于 SMTP/POP3 方式和 WEB 方式的电子邮件服务系统。

1.2 应用环境和应用领域

在信息化飞速发展的同时，计算机网络已渗透到社会的方方面面，但在我国现阶段，政府各部门之间，尤其是县、乡、镇的文件交换与传递，还依托传真、电话、邮件方式，没有充分利用计算机网络资源进行信息文件交换。这种方式效率低且对将要交换的机密文件是极不安全的，而且增加了办公成本。因此，为提高办公效率，提供快捷方便的文件交换机制，加强文件交换的安全性、可靠性和本地文件存储的安全性，我们向国家密码管理局申请立项，研制开发“SQY29安全电子邮件系统”。该系统采用国家密码管理局批准的安全密码算法与产品，对电子邮件以及传递的文件实现安全传输与系统保护，确保电子邮件传输的机密性、完整性、可认证性和不可抵赖性，以及本地文件存储的安全性，用在县乡安全文件交换以及企事业单位安全传递电子文件的单位。

1.3 国内外发展概况

目前，安全电子邮件在国外发展比较迅速，但是均是多数是采用与微软软件捆绑机制，如采用 IE + SSL128 方式收发安全 webmail、采用 Outlook 加上签名加密机制实现安全邮件、采用 PGP 安全邮件系统收发安全邮件等等，而且它们都是采用美国国家认可的密码算法，不符合我国国情，所以，与国外的类似产品相比，没有很多的可比性。

国内的同类产品目前比较多，如广东虹天的安全电子邮件系统、

深圳卫斯通的安全电子邮件等，多数都是采用类似的机制来实现文件的加密解密和签名验签方法，并且在应用中，也大同小异，主要应用与县乡传真升级改造。但是，与所有这些同类产品相比较，华翔腾数码科技公司的 SQY29 具有很多自己的特点，在“安全、方便、实用”方面突出了自己的特色。

1.4 与其它系统的比较

在下面的文字中，我们分几个方面比较几家公司的产品，但是基本需要完成的功能就不一一赘述。

(说明：由于我们没有能完全看到别的公司的软件系统，比较只能比较部分功能，并且不能保证他们的软件更新是否修改或者增加功能。)

PKI 机制应用

华翔腾	全面应用
虹天	部分应用
卫斯通	全面应用

采用 UKey 硬件密码算法

华翔腾	应用
虹天	可以采用 DES 等软件算法
卫斯通	采用的国密局批准的软算法

加密解密速度

华翔腾	正常
虹天	采用软件算法时速度很快
卫斯通	速度很快

采用 PCI 密码卡

华翔腾	采用
虹天	采用
卫斯通	采用

采用虚拟磁盘机制

华翔腾	未采用，采用自己定义的文件保护机制，文件夹容量没有限制，而且解密的风险最小，同时有效防止其它进程访问解密数据
虹天	采用，有虚拟磁盘机制造成安全漏洞 - 不能防止其它进程访问解密数据
卫斯通	采用，有虚拟磁盘机制造成安全漏洞 - 不能防止其它进程访问解密数据

提供粉碎机功能

华翔腾	提供
-----	----

虹天	提供
卫斯通	提供

UKey 遗失 CA 处理机制

华翔腾	补发一个用户 UKey 就解决
虹天	全部换发
卫斯通	补发一个用户 UKey 就解决

提供防火墙功能

华翔腾	提供
虹天	提供
卫斯通	未提供

提供程序自动在线升级功能

华翔腾	提供
虹天	未提供
卫斯通	未提供

提供 UKey 锁屏功能

华翔腾	提供
虹天	提供

卫斯通	未提供
-----	-----

提供一体化的自动扫描功能

华翔腾	提供
虹天	未提供
卫斯通	未提供

2 安全电子邮件系统组成

系统基本组成包括：硬件和软件。

硬件密码设备为 PCI 密码卡、Ukey 智能密码钥匙。

软件包括密钥管理中心和客户端应用系统。

系统拓扑结构见图 2-1。

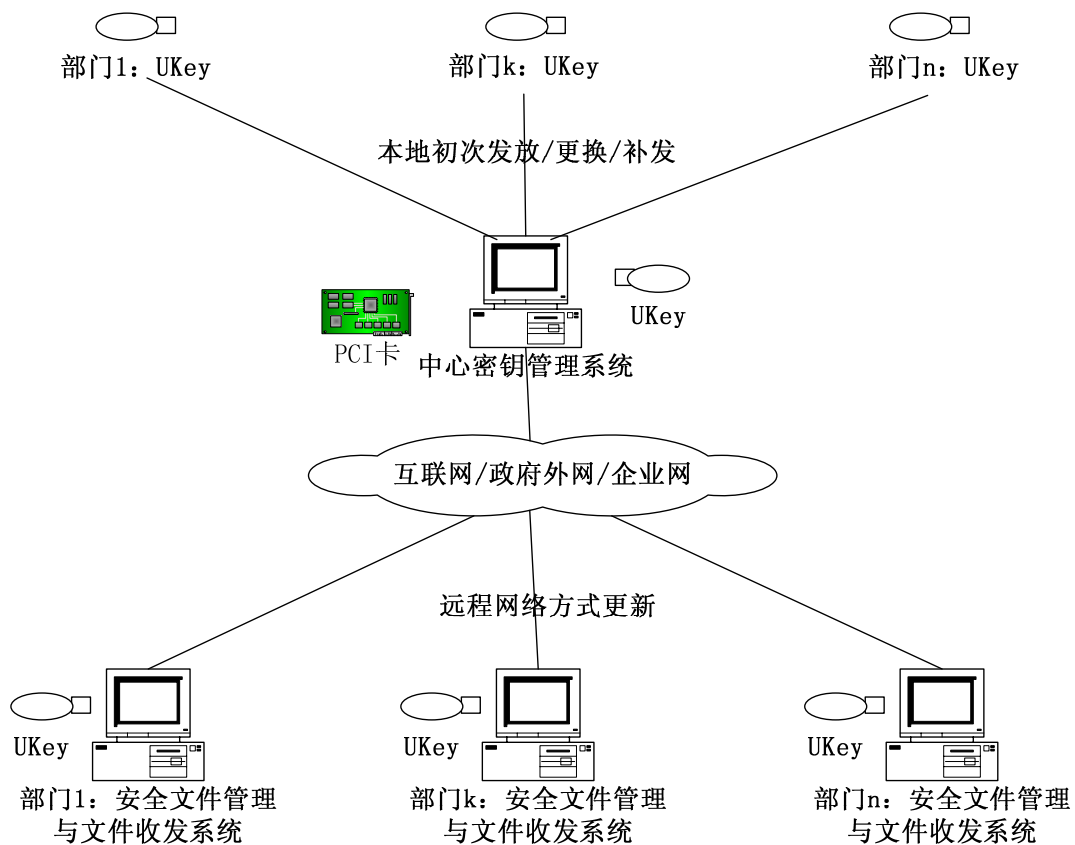


图 2-1 系统拓扑结构

2.1 PCI 密码卡



图 2-2 PCI 密码卡

本系统采用的 PCI 密码卡为华正天网密码卡 SJW16-B(简称为 PCI 密码卡, 如图 2-2)。该卡通过国密办安全审查与鉴定, 是专门为密码处理和计算而精心设计与优化的硬件设备, 支持 PCI 接口, 具有处

理速度快、安全性高、通用性好、即插即用等诸多优点。其主要技术指标如下：

- 支持国密办认可的对称密钥密码算法；
- 支持模长为 1024 比特的 RSA 非对称密钥密码算法，可实现数字签名、验证签名，以及加解密处理；
- 支持国密办认可的数字摘要算法；
- 支持加密密钥、非对称密钥密码算法的私有密钥存储于 PCI 卡中，并且加解密运算也在卡中执行；
- 支持密钥的安全备份和安全导入导出。

2.2 智能密码钥匙

本系统采用的明华 SZD12 智能密码钥匙 (Ukey) 是一种设计精巧、便于随身携带，集智能芯片和读写控制于一体的 USB 接口产品，是通过国密办安全审查的微型密码设备。

UKey 具有网络环境下的数字签名、身份认证、信息和数据的安全加密、存放数字证书、存放用户私有密钥等功能。其主要技术指标如下：

- 采用标准的 USB 接口，即插即用，无需其它支持；
- 内置 CPU 智能芯片，具有智能卡操作系统的所有功能；
- 密钥存储于芯片中，运算操作由智能芯片完成，外部无法跟踪；

- 支持非对称模长为 1024 比特的 RSA 算法,能够实现数字签名、验证签名,以及加解密运算;
- 支持国密办认可的对称密钥密码算法,内置硬件随机数发生器;
- 支持 SHA1 Hash 摘要算法;
- 符合 PC/SC 规范;
- 可运行于 Windows98/2000/XP 环境下

2.3 密钥管理中心（证书认证中心）

2.3.1 密钥管理中心结构

密钥管理中心结构图如图 2-3。

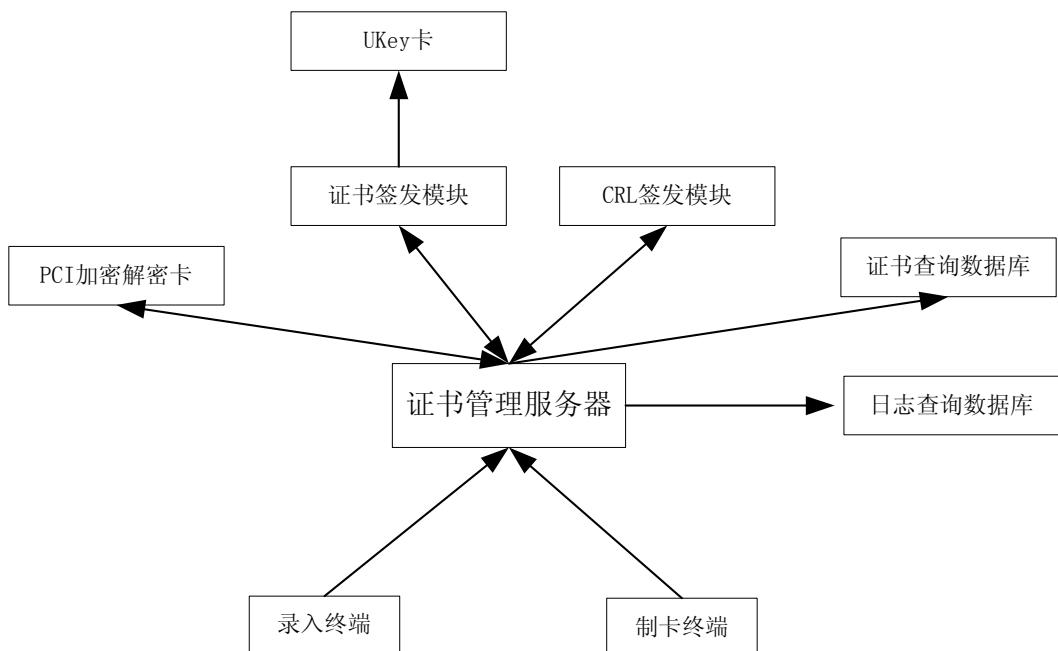


图 2-3 密钥管理中心结构图

- CRL 签名模块负责接收 CRL 制作请求并制作 CRL，保存操作日志。
- 证书签发模块负责接收证书制作请求并制作证书，保存操作日志。
- 证书查询数据库接收数据更新信息，并更新数据；接收并处理客户端发送的证书作废状态查询请求。
- 证书管理服务器负责接收业务请求并作相应的处理，是 CA 管理中心与用户的唯一接口。同时是全系统的用户资料的备份。
- 日志查询数据库负责处理用户提出的日志查询请求
- PCI 加密卡负责硬件加密方式实现 CA 管理功能
- 录入终端用于操作员录入用户资料，具备操作员控制功能。
- 制卡终端用于操作员制作 UKey 证书卡，具备操作员控制功能。

2.3.2 密钥管理系统功能

本系统建立的密钥管理中心，是在局部范围内负责通讯用户数字证书的生成、分发、更新、注销、恢复等处理，并负责用户密钥的生成与管理的基础系统。它支持本地将用户证书及密钥信息写入用户 UKey 中，同时支持远程密钥分发功能，实现远程终端方式下，对用户 Ukey 的密钥更新。

该中心主要具有如下功能：

- 能够完成用户证书及相关密钥的生成并注入 Ukey、分发；
- 具有简单证书与密钥的管理能力，可完成用户证书、用户信

息、用户密钥等的更新、恢复、撤销;

- 采用标准的 X.509v3 数字证书, 支持直接采用符合国密办要求的地区公用 CA 证书;
- 支持离线操作, 支持系统自动为用户端下传与更新证书列表;
- 采用国密办安全审查通过的 PCI 密码卡、Ukey 硬件以及国密办批准的密码算法, 提高系统的应用安全性。

2.4 用户端应用系统

2.4.1 用户端应用系统组成

系统功能结构如图 2-4 所示:



图 2-4

2.4.2 用户端应用系统功能

用户端功能：

- 加密安全文件、邮件。依照 CMF 格式加密文件。
- 解密安全邮件、文件。此模块实现解密收到的安全邮件、本地保存的加密文件。
- 创建邮件/加密文件与显示、编辑安全文件。
- 显示接收到的安全邮件保存的安全文件。
- 发送安全扫描文件。此模块实现调用“扫描文件”模块，并支持多页连扫。
- 发送安全邮件功能。

- 扫描文件。此模块实现对于不同扫描仪支持，将纸张扫描为指定文件名称的图片。
- 短信模块。在安全邮件发送成功后，将发送的邮件信息作为短信写入数据库。此模块启动后，定时将数据库中待发的短信发送到指定的手机。
- 接收安全邮件。
- 打开安全邮件。
- 注入私钥。此模块实现自动更新用户 Ukey 的私钥。当用户收到的安全邮件标志为私钥时，验证 CA 的签名，并解密私钥数据，比较私钥是否 Ukey 中的私钥，不同就将私钥注入到 Ukey 中，同时将此私钥加密保存到用户私钥历史库中。
- 证书入库。此模块实现自动将用户证书列表更新（包含证书的吊销、增加、修改等），当 CA 有任何证书修改后，将发送私钥给最近改动用户，同时发送证书库给所有已经注册用户。用户收到 CA 发送的安全邮件，如果标志为证书库，在验证签名后，将自动更新证书库。
- 安全文件夹管理。支持增加、删除、更名文件夹；支持多级文件夹。用户的安全文件、保存的安全邮件放置在安全文件夹中；支持显示所有文件列表；支持预览文件标题与附件名称；支持打开安全文件（注意是否自己签名安全文件打开界面不一样）功能；支持不同文件夹中移动安全文件；支持安全文件、文件夹属性查看；支持调用地址簿显示；支持显示关于与帮助列表；支持设置属性等。
- 安全文件查询、统计。此模块实现在整个安全文件夹子或者指定的目录下，依照发送人地址、接收人地址、创建时间、标题、是否为接收的邮件（是不是自己签名）等查找安全文件，并统计、显示出来。
- 安全审计功能。此模块实现对于所有操作的日志显示。包含收发邮件、发送短信成功失败、创建加密文件、保存位置、等等操作的记录。
- 传真预览打印。此模块实现将指定文件解析成原来的页数，并依照原来次序显示，并可以设置打印机、打印预览、打印。
- 安全删除文件、文件夹。此模块实现对于任何非加密文件的粉碎。
- 防火墙。此模块实现对于任何网络断开或者连接，需要支持自己定义的消息

通断网络。

- 地址簿。此模块显示用户当前所有证书库中用户信息。支持查询、导出、打印功能；支持修改用户手机信息。
- 系统完整性检查。此模块实现对系统自身完整性检查（包含执行文件的完整性、数据库各表完整性），发现任何问题，提示用户错误信息（文件改变大小、变化时间等），帮助用户修复数据库（通过备份的数据库）。
- 浮动窗口。此模块实现显示一个类似 **FlashGet** 一样的浮动窗口，支持用户拖动一个或者多个文件加密，并弹出创建安全文件夹界面窗口；支持用户右键菜单；支持有名内存文件与安全文件夹创建安全文件界面通讯；此模块显示与否可以在安全平台服务器中设置。
- 安全平台服务器。此模块常启动（无论有无 **Ukey**），并可以设置一些属性；支持右键菜单启动系统其它模块；显示浮动窗口；此模块不能正常退出；检测 **Ukey** 的拔出动作；支持快捷屏幕保护。
- 属性设置。此模块为设置一些系统属性。被服务器、安全文件夹调用。此模块的所有信息来源是注册表，确定后将设置的信息写回注册表。包含防火墙设置、**Ukey** 动作相应等。
- 快捷键支持。
- 关于与帮助。关于模块显示系统关于信息。不同应用程序采用一样的风格，调用时采用传入本进程名称、版本号等信息；帮助模块为不同进程实现 **F1** 时出现系统帮助文件显示，帮助主题文件为 **help.chm**。

3 系统工作原理和过程

3.1 智能密码钥匙的发放

生成用户证书流程如图 3-1。

系统要为每个用户发放数字证书，并存于 Ukey 中。

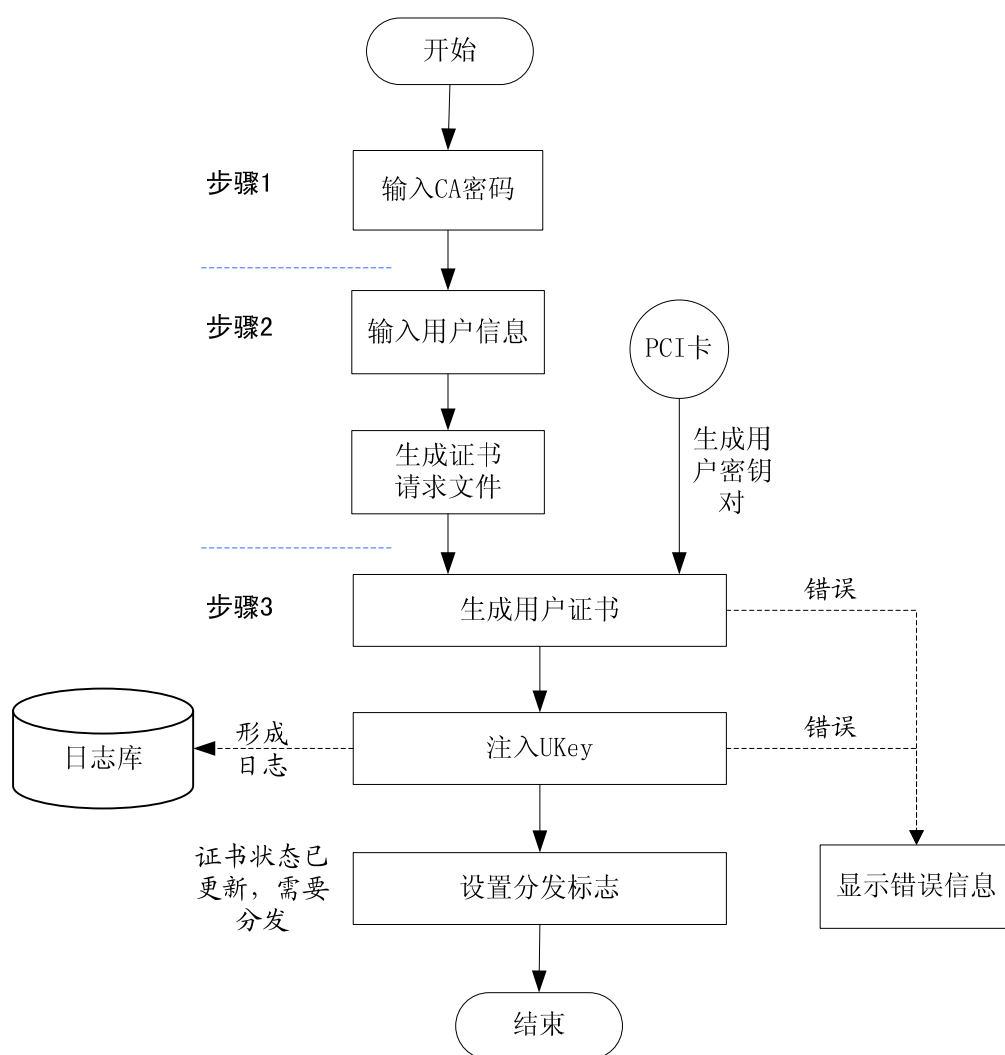


图 3-1 生成用户证书流程

3.2 安全电子邮件发送与接收

安全邮件是普通邮件加密之后的密文数据，收发均采用标准的 SMTP 协议和 POP3 协议实现。

在收到之后，系统自动验证签名并解密数据。

3.3 用户证书的更新

更新用户证书分三种情况：

- 更新用户的手机号码

此时只需更新证书库中对应用户的手机号码即可，而无需改变已有证书和密钥。

- 更新用户的 Email 地址和用户名称

要生成新的交换密钥和交换证书，需形成相应的 CMF 文件并发送。

- 更新用户的其他信息

交换密钥不需更改，但要生成新的交换证书，需形成相应的 CMF 文件并发送。

4 支持环境

4.1 系统运行环境

硬件配置：

- ◇ CPU: P41.8G (推荐)
- ◇ 内存: 256MB (推荐)
- ◇ 硬盘: 20G (推荐)
- ◇ Ukey (必备)
- ◇ 至少有一个 USB 接口 (必备)
- ◇ 扫描传真一体机 (传真必备)
- ◇ 短信发送器 (可选)

软件配置:

- ◇ Windows 2000 + Sp4 (推荐)
- ◇ 华安安全加密文件交换系统

4.2 系统基本配置

(1) 中心管理端配置

编号	设备/系统名称	产品型号	备注
一	基本配置		
1.1	硬件加密卡	PCI 数据加密卡	华翔腾提供
1.2	密钥中心管理系统软件	华安基本组件	华翔腾提供
1.3	管理员 USB-Key	腾盾 USB 接口智	华翔腾提供

		能安全钥匙	
1.4	密钥管理中心服务器	通用 PC 服务器	可用原有设备
1.5	管理端终端	通用 PC 终端	可用原有设备
1.6	安全电子邮件系统	SQY29 安全电子 邮件	华翔腾提供
二	可选的扩展配置		
2.1	短信服务系统	SMSSvr	华翔腾提供
三	其它扩展可选的设备		
3.1	打印、扫描、复印一体 机或复印机	通用设备	支持文件扫描与 发送

(2) 普通用户端设备配置

编号	设备/系统名称	产品型号	备注
一	基本配置		
1.1	USB-Key	腾盾 USB 接口智 能安全钥匙	华翔腾提供
1.2	计算机	通用 PC	可用原有设备
1.3	安全电子邮件系统	华安安全电子邮 件	华翔腾提供
二	其它扩展可选的设备		
2.1	打印、扫描、复印一体 机或复印机	通用设备	支持文件扫描与 发送

5 特点

系统特点是“安全、方便、实用”，具体描述如下：

- 支持 Windows 操作系统以及常用的邮件收发系统，如：Outlook、FoxMail；
- 基于 UKey 进行身份认证、数字签名与数据加密；
- 支持一体化文件发送与接收处理，实现文件从扫描、打包、加密、存储到发送和文件接收、存储、解密等的流程跟踪控制；
- 文件发送系统可与短信通知系统连结，实现文件发送后的短信及时通知；
- 收发文件夹与安全文件夹绑定，实现文件发送与接收的自动加/解密处理；
- 自动定义用户地址簿，直接选择安全文件接收用户，而无需输入接收方邮件帐号。
- 采用通过国密办认可的密码设备，有效完成数据密码处理，且操作简单；
- 支持常用邮件客户端软件如：Outlook、Foxmail 等；
- 系统启动时会安全自检，并给出异常提示；
- 用户安全智能钥匙（Ukey）拔出来后，立即锁定计算机屏幕；
- 数据备份与灾难恢复支持；

- 彻底删除用户不需要的敏感数据;
- 加密数据只能在本系统内进行有效操作(读取、访问等),且必须在完成身份验证以后方可进行;任何其它进程均不能访问,也不可能被非法网络共享;
- 密钥存储在密码设备中,保证系统安全;
- 有效防止黑客暴力破解密钥、用户 PIN;
- 加密文件夹打开后,存在的风险最小:不会解密所有文件,打开哪个文件才解密哪个文件,并在关闭后立即自动清除临时文件;
- 内置网络防火墙可以在有密文数据时,自动断开网络。

6. 典型应用解决方案

6.1 区域性应用——基层政府部门间的公文交换

通过安全电子邮件系统,可为政府部门的上、下级之间,尤其为信息网络条件不发达的基层政府部门,建立了一套安全、方便、经济实用的公文传递与交换系统。

其系统结构图 6-1 如下:

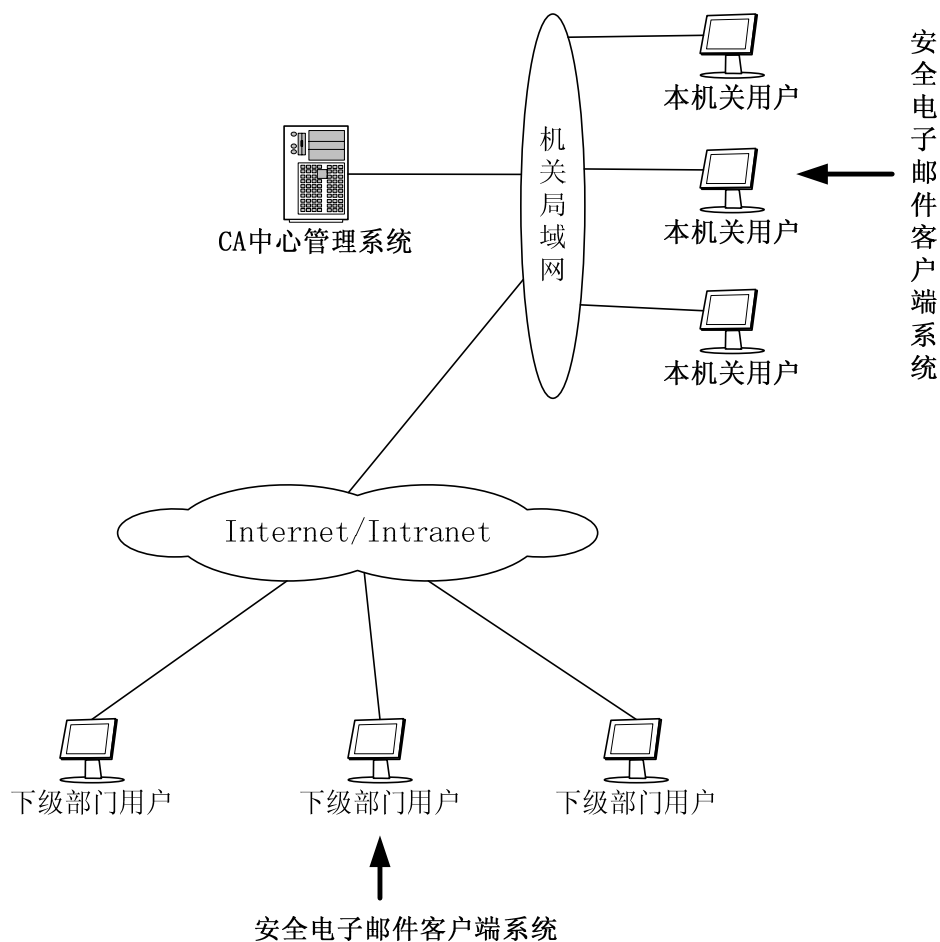


图 6 - 1

在上级部门建立 CA 中心管理系统，主要包括：证书认证与密钥管理系统、相关套件产品。通过中心管理系统，实现了：各部门用户数字证书生成与维护、用户密钥注册与发放、证书更新、密钥更新等功能。

系统的安全性依赖于系统产生的数字证书，并以硬件密码钥匙为载体，对信息进行加密、签名，保证网络传递的文件都经过数字签名与加密，并不能被篡改、抵赖、伪造、仿冒或者产生泄密。

在用户端，只要安装安全电子邮件客户端系统，用户持系统注册

的 UKey，就可实现下级用户向上级提交请示报告，上级领导对文件进行批示并反馈给请示人员，以及上级发放文件、通知、通告、消息等文件传递与交换功能。

6.2 企业应用—企业间的商业文件交换

通过配置安全电子邮件系统，为企业内部以及企业合作伙伴之间建立了一套高效、安全、方便、经济实用的商业文件（包括：合同、订单、协议、公司文件等）传递系统。

系统结构图如图 6-2:

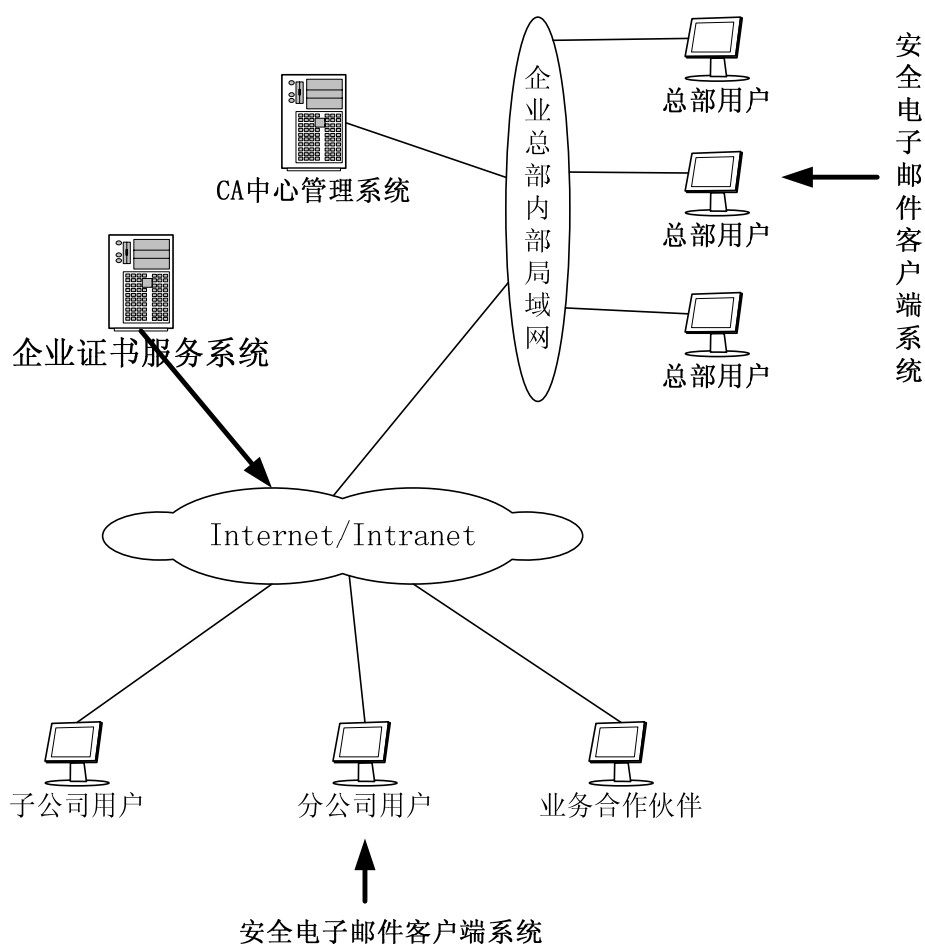


图 6-2

与政府部门的应用不同，为节省投资，企业可以选择采用商业级证书认证系统（如华翔腾公司在 Internet 上建立的翔全商业认证服务系统）来产生、维护、更新用户的密钥与数字证书，并发放商业级密码钥匙。因此，企业不用担心自身没有专业计算机人员来建设、管理与维护中心系统，可以轻松委托专业认证服务机构来解决后顾之忧。其证书的安全性由商业认证服务系统负责。当然，有条件的企业，也可以选择自己建立内部的证书认证与密钥管理中心。

企业总部、子公司、分公司以及企业合作伙伴之间，安装华安客户端安全电子邮件系统，可以实现相互之间商业文件在网络上的安全加密传递。

6.3 行业性应用——教育主管部门与各学校间的文件交换

通过配置安全电子邮件系统，为教育部、教育厅、教育局等教育主管部门与主管学校之间建立了一套安全、方便、经济实用的文件传递与交换系统。

系统结构图如图 6-3:

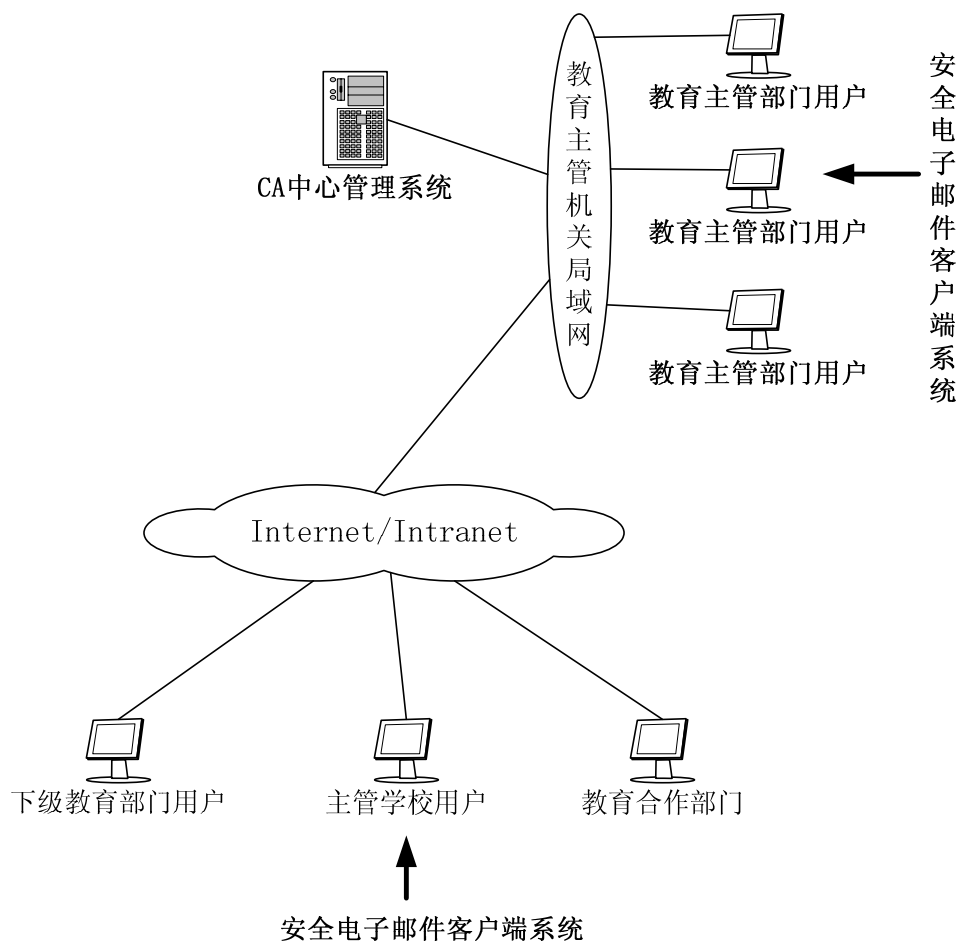


图 6 - 3

与政府应用类似，教育主管部门可以建立一套统一的证书认证与密钥管理系统(也可直接采用教育部建立的全行业性证书认证与管理 系统)，负责对本机关、下级教育部门、下级学校、教育合作部门的 用户产生、维护、更新、注销、管理数字证书，并发放用户注册的密 码钥匙(腾盾 Key)。

依此类推，下级教育部门与其下级学校之间同样可以建立安全文 件交换通道。，但无需重复建设局部密钥管理中心，因为在上级主管 部门建立的证书认证与密钥管理系统，可以直接支持下级的用户数字 证书管理需求。

因此，在教育主管部门、学校、下级部门之间，只要建立统一的密钥管理系统，通过腾盾 Key 的注册分发，各部门用户通过华安安全电子邮件系统系统，就可以实现相互之间的文件安全加密传递。

(完)