

产品名称 Product name	密级 Confidentiality level
mToken GM3000	
产品版本 Product version	
V1.1	

## mToken GM3000 CAPI 证书应用指南

Prepared by 拟制		Date 日期	
Reviewed by 评审人		Date 日期	
Approved by 批准		Date 日期	



**北京世纪龙脉科技有限公司**  
Beijing Century Longmai Technology Co., Ltd.

All rights reserved

版权所有侵权必究

## Revision Record 修改记录

Date 日期	Revision Version 修订 版本	Sec No. 修改 章节	Change Description 修改描述	Author 作者
2013/4/22	V1.0		初始版本	

# 目录

<b>第一章</b>	<b>GM3000 CAPI 应用说明 .....</b>	<b>4</b>
1.1	配置证书颁发机构 .....	4
1.2	GM3000 的 CAPI 进行证书申请 .....	7
1.3	GM3000 的 CAPI 访问 SSL 加密站点 .....	9
<b>第二章</b>	<b>GM3000 的 CAPI 安全电子邮件应用 .....</b>	<b>11</b>
2.1	获取数字标识 .....	11
2.2	OUTLOOK 2010 中安全设置 .....	14
2.3	发送和阅读安全电子邮件 .....	17
<b>联系我们 .....</b>		<b>20</b>
公司总部 .....		20
杭州办事处 .....		20
广州办事处 .....		20
申请试用 .....		20
购买产品 .....		21
技术支持 .....		21

## 第一章 GM3000 CAPI 应用说明

GM3000的主要功能是与现有的PKI体系应用无缝的集成。PKI应用开发商无需对GM3000进行任何形式的编程开发就能通过配置相关服务而开始将GM3000集成于PKI应用当中。

目前支持PKI的应用有些使用PKCS#11接口，有些使用Crypto API（简称CAPI）接口，后者是微软的Windows平台下的应用，而前者在任何平台下都有。

以下主要讲述如何将GM3000的CAPI接口集成到现有的PKI体系中，主要包括IE申请证书，访问SSL加密站点，Outlook发送加密、签名邮件等。

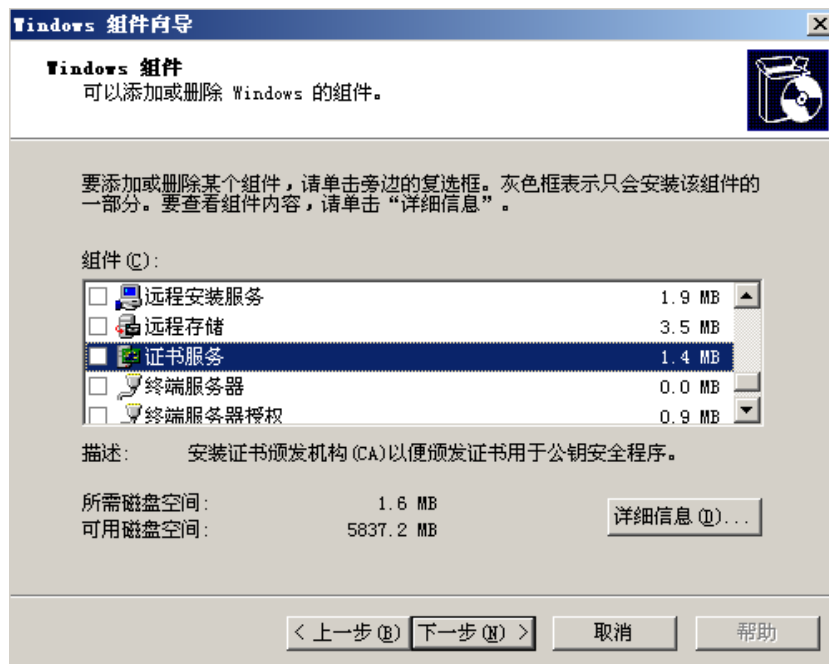
### 1.1 配置证书颁发机构

证书颁发机构即通常所说的CA中心，是PKI应用的核心。任何PKI应用都需要CA中心的支持。支持PKI技术的CA有很多，如BJCA（<http://www.bjca.org.cn/>）、VeriSign(<http://www.verisign.com/cn/>)等等，下面讲解如何在Windows Server 2003上安装和配置证书服务器。

注意：如果用户没有安装IIS，请先安装IIS。

在Windows Server 2003计算机上安装证书颁发机构(CA)，请按照下列的步骤进行操作：

1. 打开“开始”菜单→“设置”→“控制面板”选项，启动Windows 2003控制面板。
2. 选择“添加或删除程序”，启动添加或删除程序，再选择“添加/删除Windows组件”选项，如下图：



3. 请在Windows组件向导的“组件”列表里，选择“证书服务”的选项，以便在Windows Server 2003计算机上安装证书服务。当勾选“证书服务”的选项后，请接着

按“下一步”按钮。接下来，系统会出现证书授权类型的设置过程。只需要按照需要，选择要安装的证书颁发机构(CA)的类型即可。用户可以选择设置的各种证书颁发机构的类型以及用途，如图所示：



**企业根CA(Enterprise Root CA)：**如果所设置的证书颁发机构要将证书发行到企业Active Directory域内所有的个体上，用户就必须选择此选项。请注意，此部证书颁发机构将会登记在Active Directory域内。如果企业的硬件资源足够时，建议只将企业根CA(Root CA)使用在发行授权(证书)给企业从属CA(Subordinate CA)之用，因为这样可以确保较好的安全性。如果企业域内部目前并没有任何的证书颁发机构，也必须选择安装企业根CA(Root CA)。

**企业从属CA(Enterprise Subordinate CA)：**如果设置的证书颁发机构要将证书发行到企业Active Directory域内的每一个个体上，而且企业域上已经有一台企业根CA，就可以选择此选项。请注意，此部证书颁发机构将会登记在Active Directory域内。

**独立根CA(Stand-alone root CA)：**如果所安装的这部证书颁发机构将要发行证书给企业域外部的个体使用时，就必须选择这种证书颁发机构方式。选择了这种方式的证书颁发机构，将会成为一个证书颁发机构层次架构的独立根证书颁发机构。

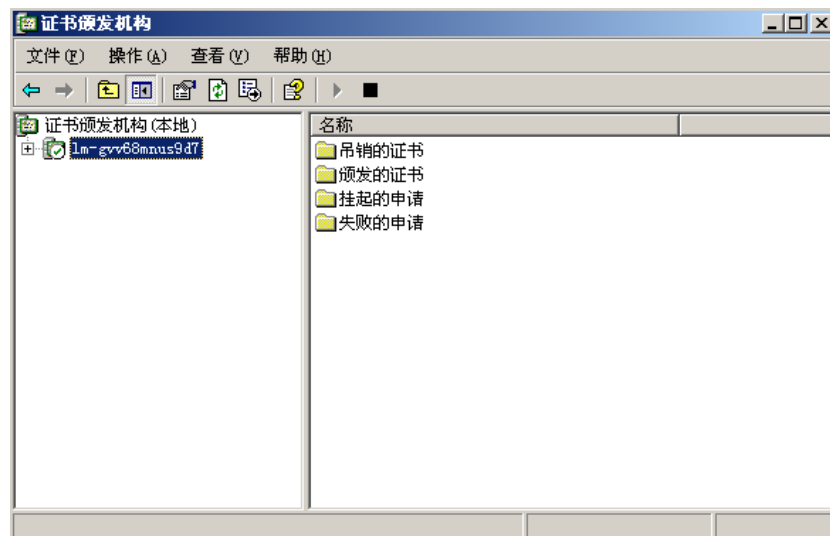
**独立从属CA (Stand-alone subordinate CA)：**如果要将此部证书颁发机构设置为一个已经设置好的证书层次架构里的一员，就应该选择此选项。证书层次架构组织可以是用户之前所安装的独立证书系统，也可以是存在于企业外部的一个商用性证书颁发机构。

4. 选择“独立根CA”，下一步，向导会出现“CA识别信息”的设置窗口。用户在此窗口里设置此证书颁发机构的标识信息，下一步，向导会出现“证书数据库设置”窗口：



在这个过程中，系统会提示先停止IIS的运行，以便顺利安装证书服务器，选择是继续，最后给出完成提示。

5. 查看证书颁发机构是否安装成功，“开始”菜单→“所有程序”→“管理工具”→“证书颁发机构”选项，启动证书颁发机构系统管理工具来管理证书服务器了，如图：

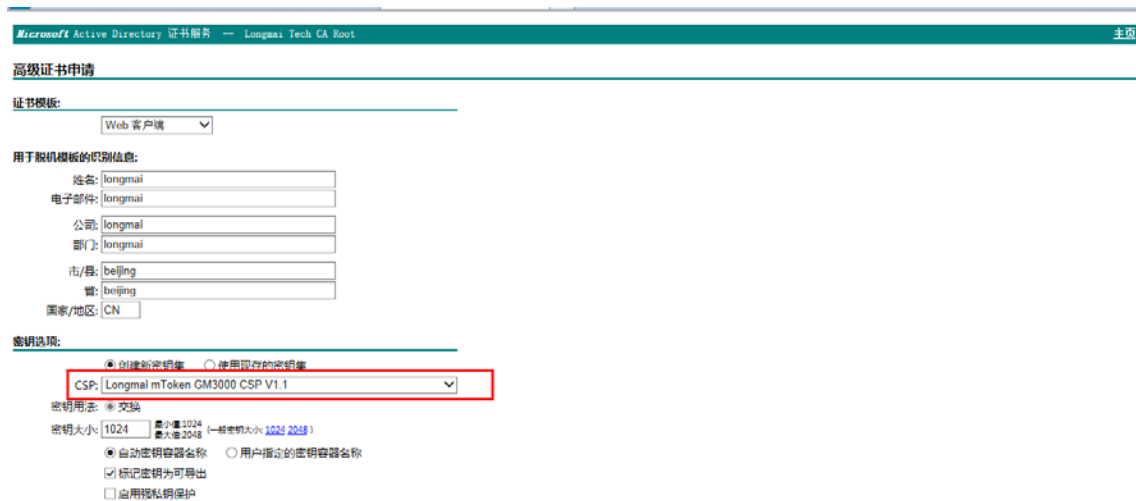


## 1.2 GM3000 的 CAPI 进行证书申请

1. 插入一只未装证书的 GM3000。然后通过 IE 打开证书颁发机构的网页，如图



2. 选择“申请证书”，再选择更多选项。在“CSP”（加密服务提供程序）选项中选择“LongMai mToken GM3000 CSP V1.1”，如果您所选择的是 GM3000 PCSC 型号，请选择“LongMai mToken GM3000 CSP（PCSC） V1.1”如图所示：



3. 完成上述设置后，单击“提交”按钮，系统弹出提示输入用户 PIN 码的对话框，如图所示：

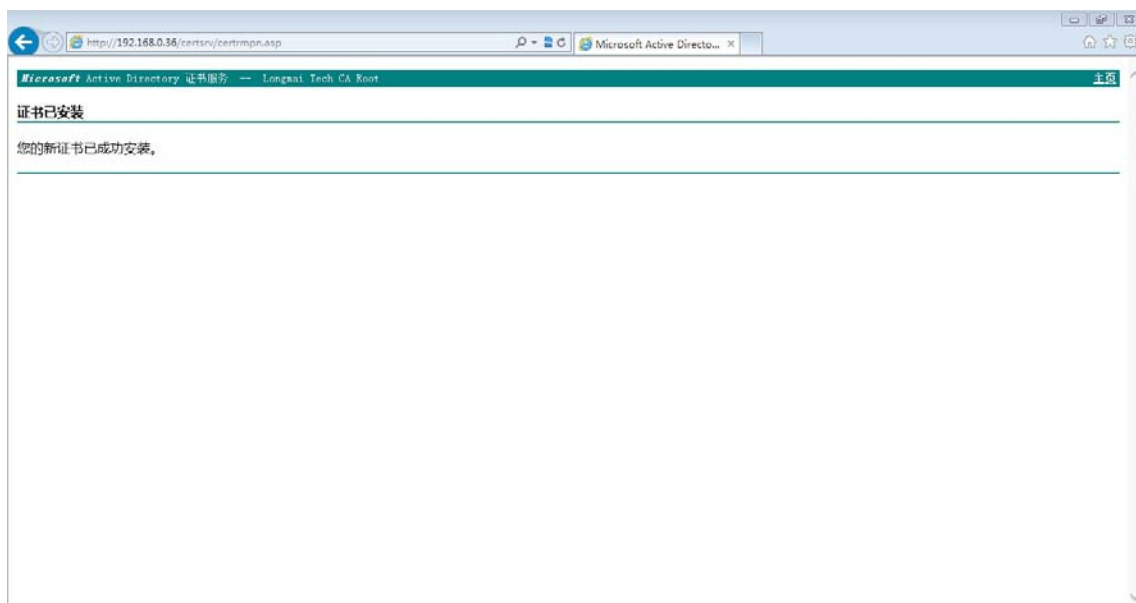
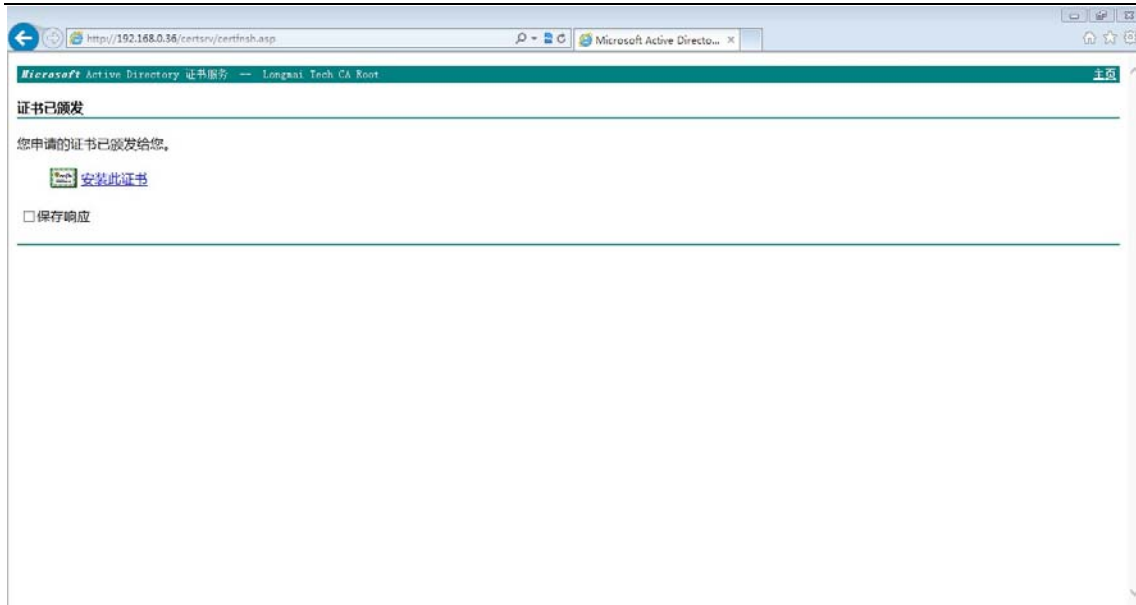


4. 输入正确的用户 PIN 码点击“登录”按钮后，稍候会看到证书挂起页面，需要等待颁发机构验证身份并颁发证书，如图所示：



5. 回到第 1 步，选择“查看挂起的证书申请的状态”，收到证书颁发机构的通知后，用户就可以去领取证书了，在安装证书时，系统同样会让用户输入正确的用户 PIN 码，点击“安装此证书”，根据提示判断证书是否安装成功：

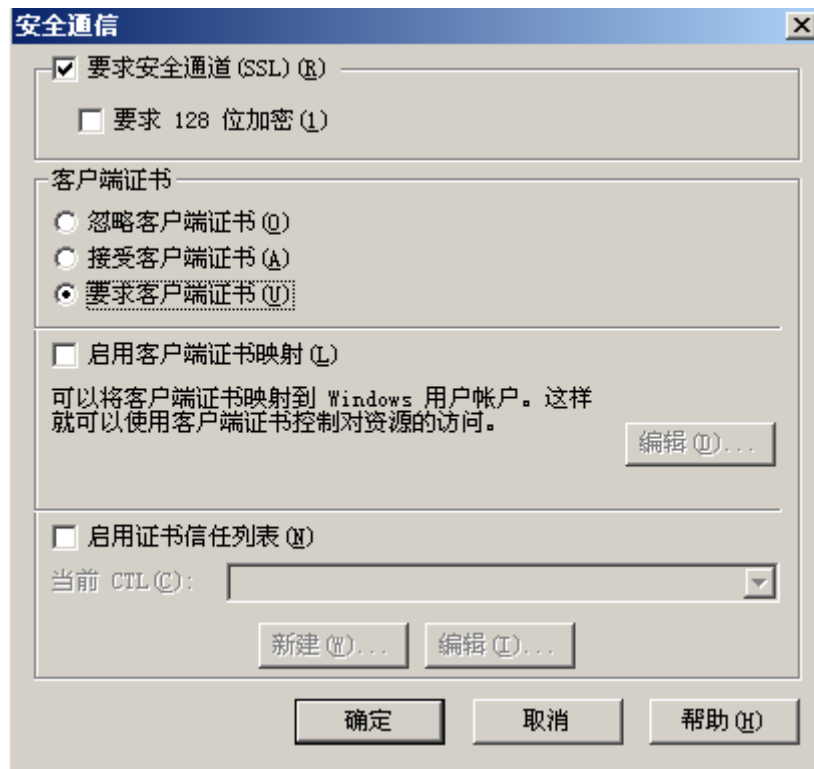




### 1.3 GM3000 的 CAPI 访问 SSL 加密站点

安全套接字层 (SSL) 是一套提供身份验证、保密性和数据完整性的加密技术。SSL 最常用在 Web 浏览器和 Web 服务器之间建立安全通信通道。它也可以在客户端应用程序和 Web 服务之间使用。为支持 SSL 通信，必须为 Web 服务器配置 SSL 证书。本章介绍如何获取 SSL 证书，以及如何配置 Microsoft® Internet 信息服务 (IIS)，以便支持 Web 浏览器和其他客户端应用程序之间使用 SSL 安全地进行通信。

1. 右键单击某个虚拟目录，然后单击“属性”，单击“目录安全性”选项卡，单击“安全通信”下的“编辑”。如下设置：



2. 登录 SSL 加密站点，用 IE 浏览器通过 https 连接到要访问的 Web 站点：



3. 选中证书，单击“确定”按钮。系统弹出 PIN 码输入框，用户输入正确 PIN 码进行登录之后就能够看到这个安全 Web 站点的内容了：

## 第二章 GM3000 的 CAPI 安全电子邮件应用

越来越多的人通过电子邮件进行重要的商务活动和发送机密信息，因此保证邮件的真实性（即不被他人伪造）和不被其他人截取和偷阅也变得日趋重要。安全电子邮件因此应运而生。依托 PKI 技术的实现，以下讲解如何在 Outlook Express 中配置和收发安全电子邮件。

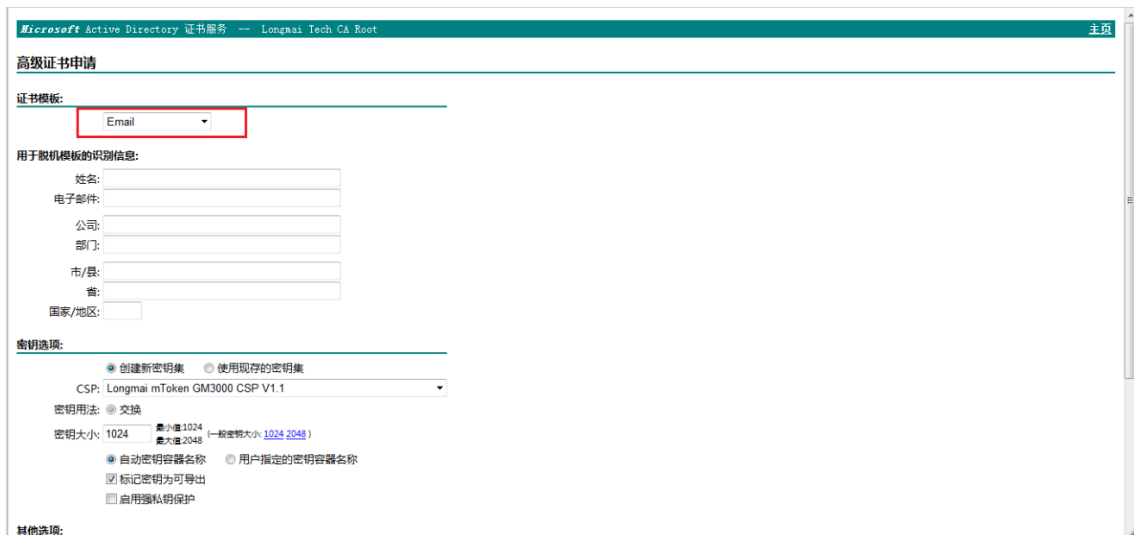
### 2.1 获取数字标识

Outlook Express 收发签名与加密邮件之前，要进行 Outlook Express 的安全设置，必须先获取具有电子邮件安全处理能力的证书（在 Outlook Express 里称为“数字标识”），当获取用户的数字标识后，用户才可以发送具有签名的或者信息加密的电子邮件。

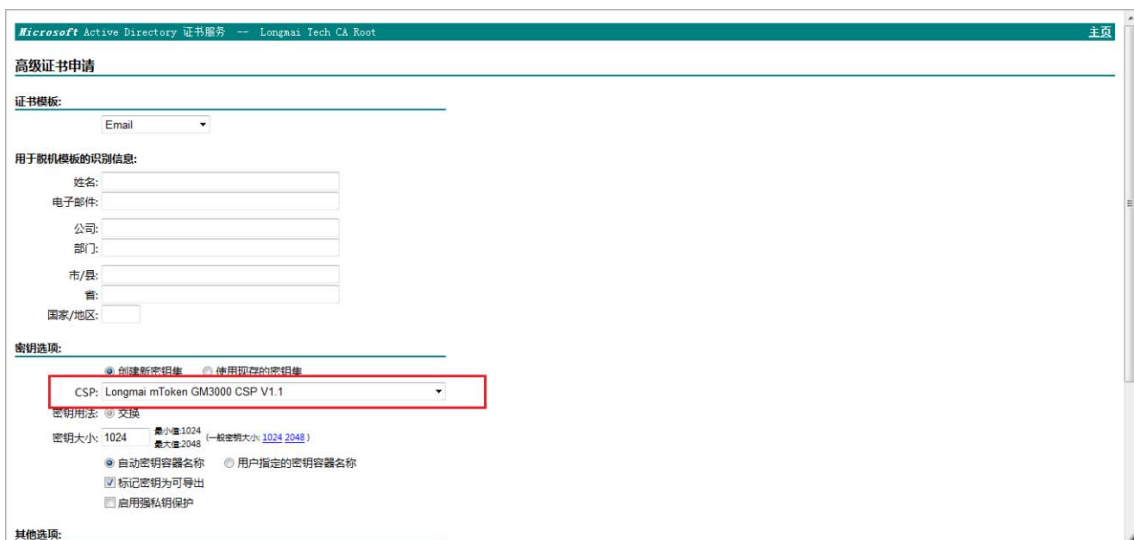
1. 插入一只未装证书的 GM3000，获取用于证明用户身份的数字标识，如下图：



选择“申请证书”，再选择“高级证书申请”中的“创建并向此 CA 提交一个申请”，证书模板选择“Email”，如下图：



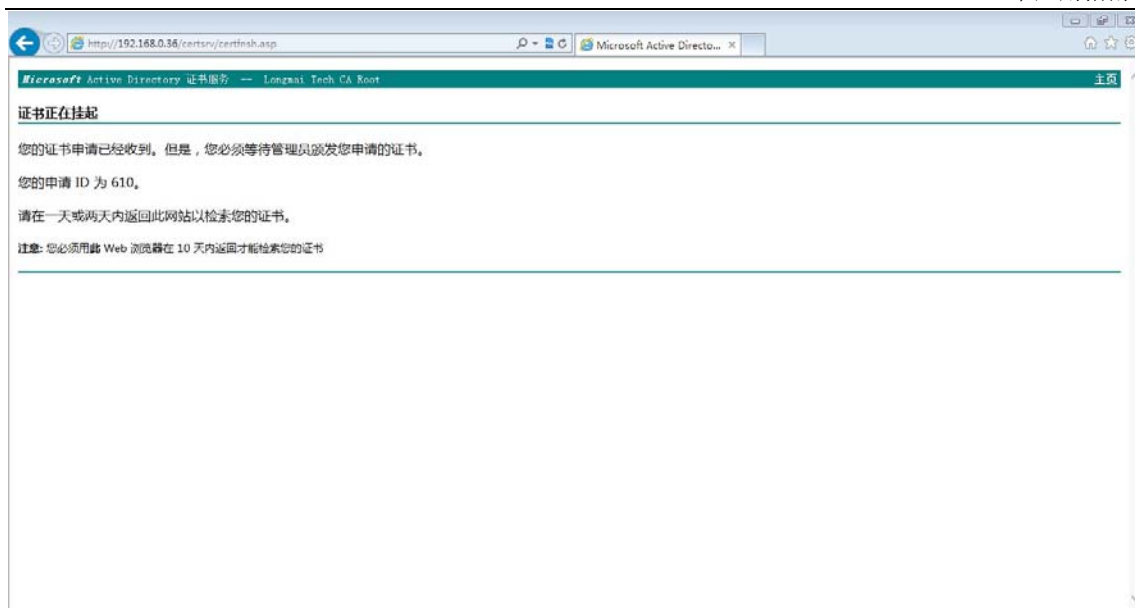
2. 数字证书里的 E-Mail 项必须和该账户 E-Mail 地址一致，在“CSP”（加密服务提供程序)选项中选择“LongMai mToken GM3000 CSP V1.1”，如果您所选择的是 GM3000 PCSC 型号，请选择“LongMai mToken GM3000 CSP (PCSC) V1.1”，如图所示：



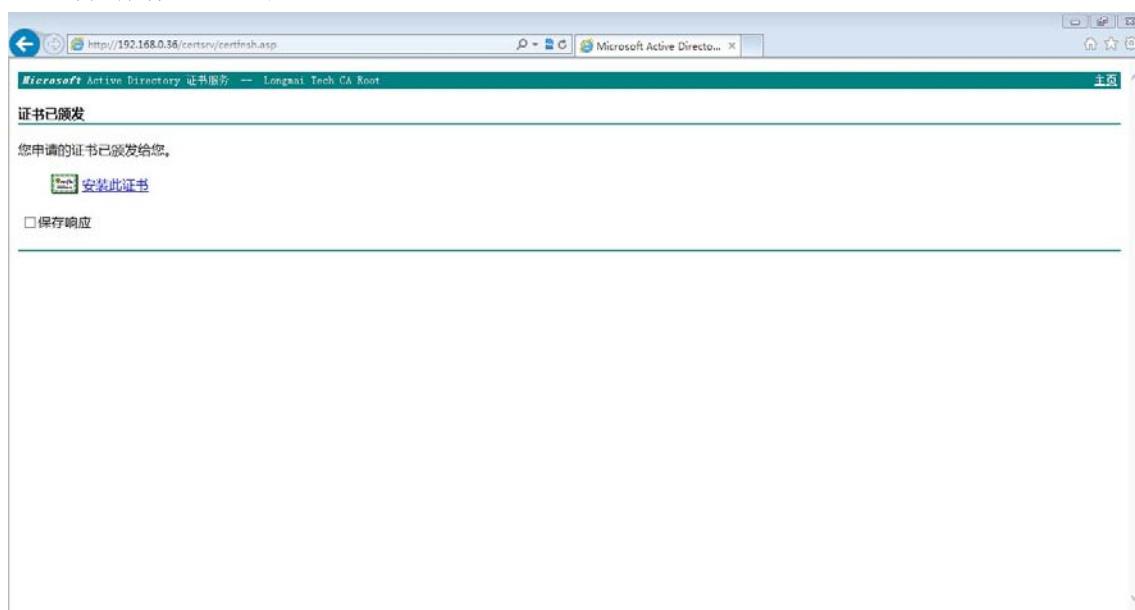
填写完整的识别信息，点击“提交”，会弹出 GM3000 的登录窗口，如下图：

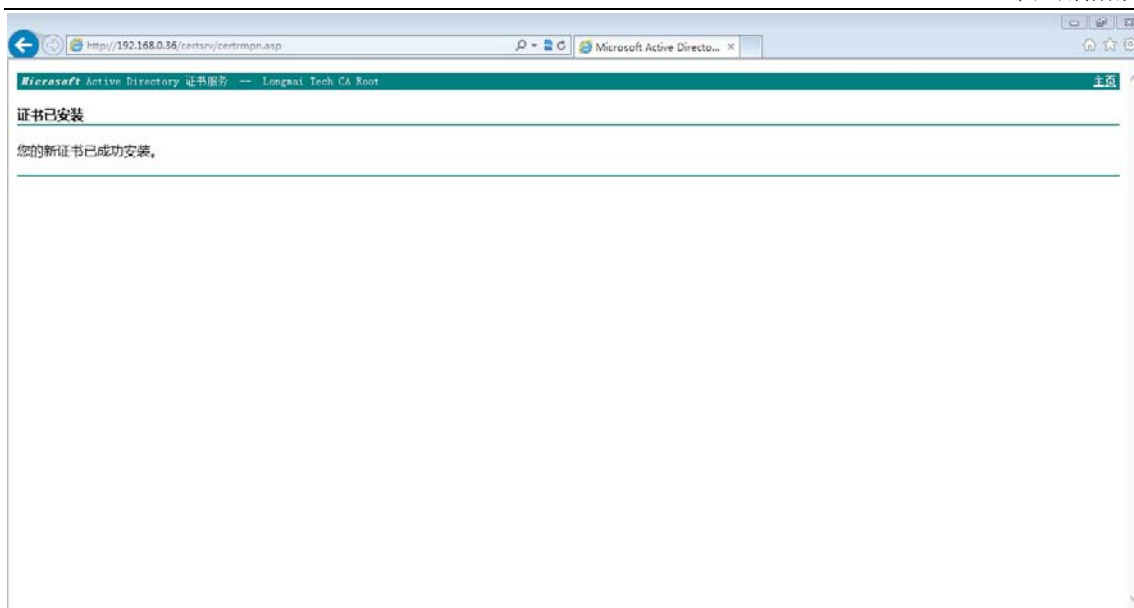


输入正确的用户 PIN 码，给出下图信息，说明证书申请提交成功，等待管理员颁发证书：



3. 如果管理员已颁发证书，回到第 1 步，选择“查看挂起的证书请求的状态”，收到证书颁发机构的通知后，用户就可以去领取证书了，在安装证书时，系统同样会让用户输入正确的用户 PIN 码：

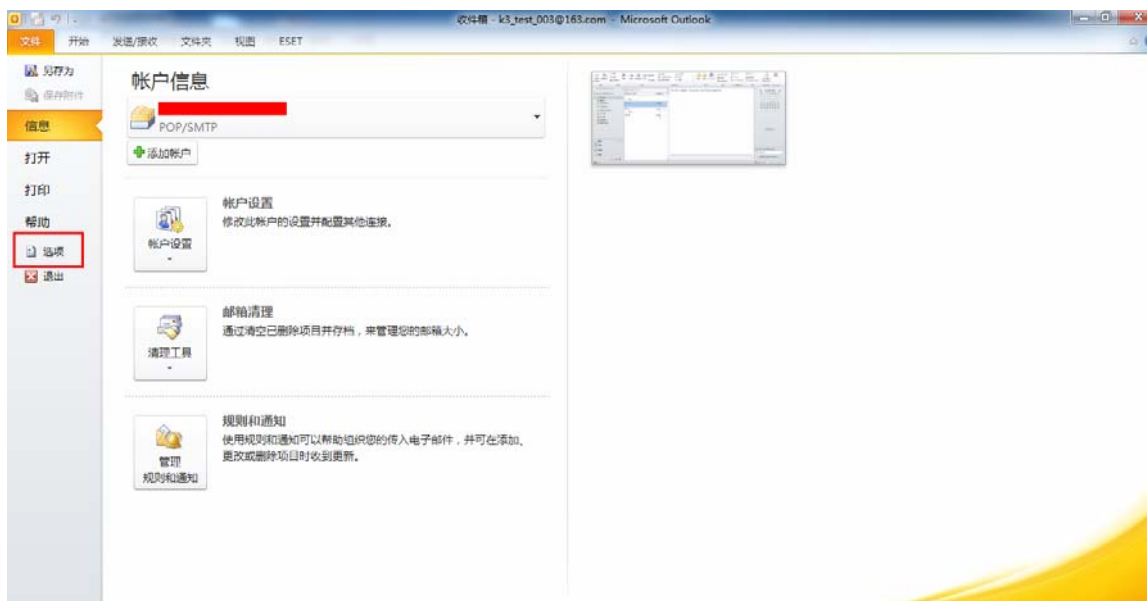




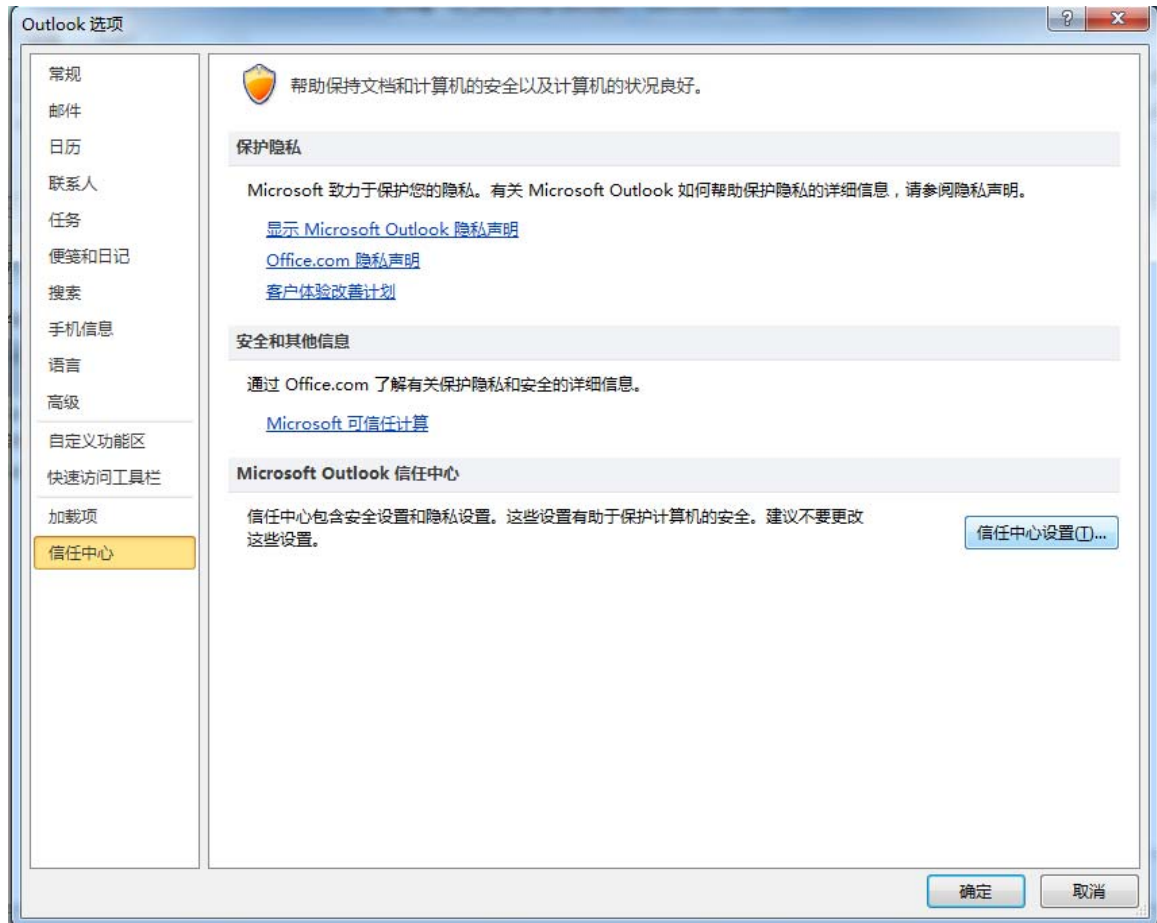
## 2.2 Outlook 2010 中安全设置

设置 Outlook 2010 的 Email 帐号中的安全性功能，按照下列的操作步骤顺序进行操作：

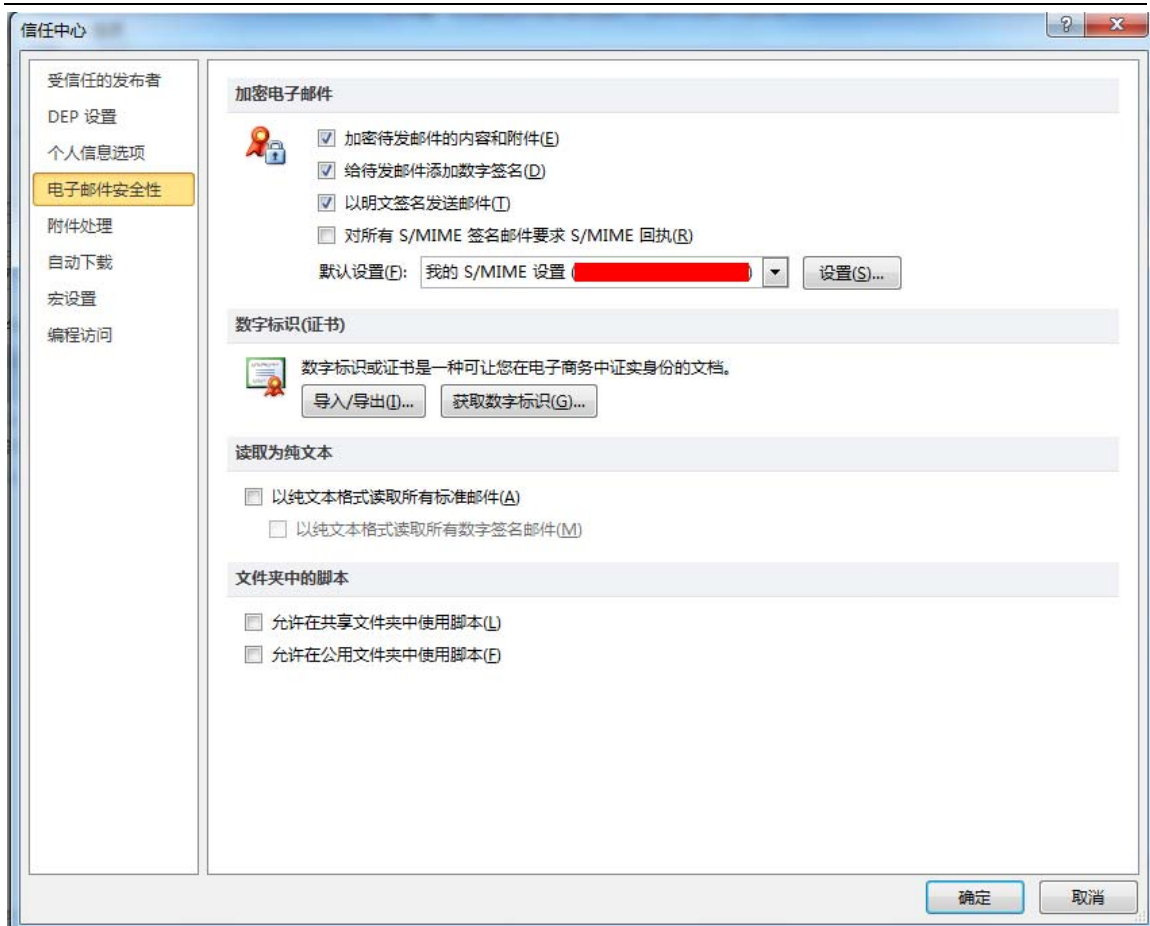
1. Outlook 2010 上方的菜单中选择“文件”→“选项”，如图：



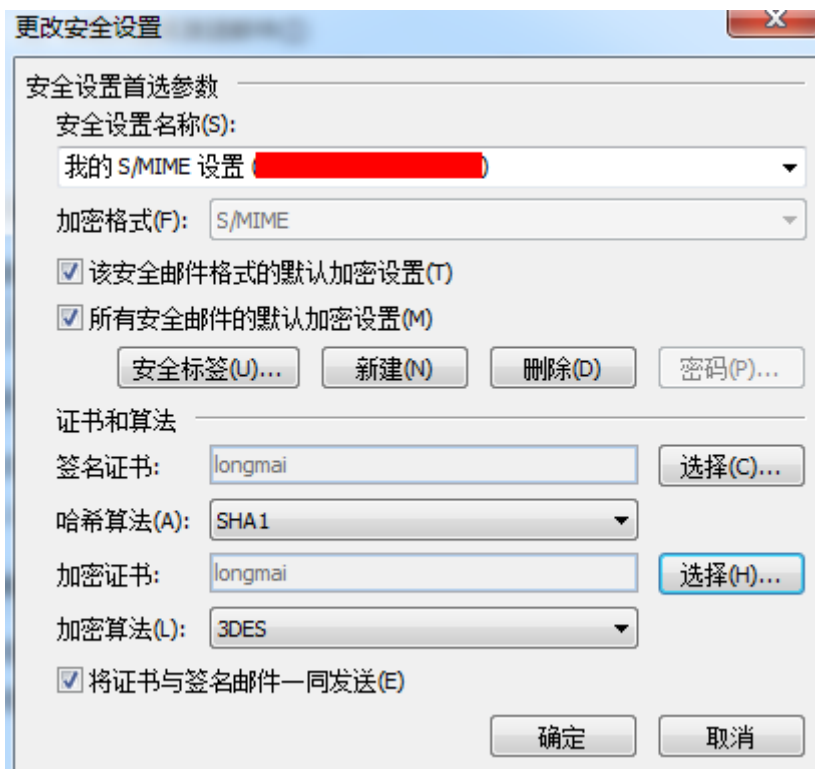
2. 当打开“Outlook 选项”窗口后，请点选“信任中心”页面中的“信任中心设置”，如图：



3. 点击“电子邮件安全性”。我们假设用户已经设置好电子邮件信箱了，请选择想设置安全性的电子邮件帐号，接着点击设置按钮，如图：



4. 选择证书，并单击确定按钮，如图：





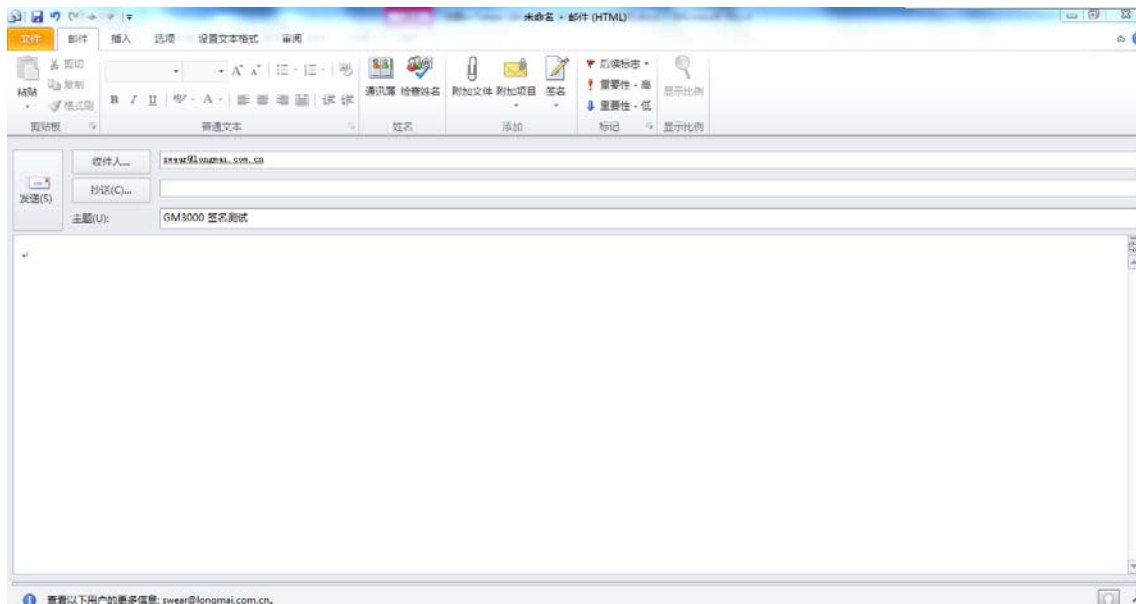
经过以上设置，完成了证书配置。

## 2.3 发送和阅读安全电子邮件

带数字签名的电子邮件允许电子邮件的收件人验证您的身份，加密电子邮件则可以防止其他人在邮件传递过程中偷阅邮件。发送邮件时，可以只对邮件进行签名，或者只对邮件进行加密，也可以对邮件同时进行签名和加密。

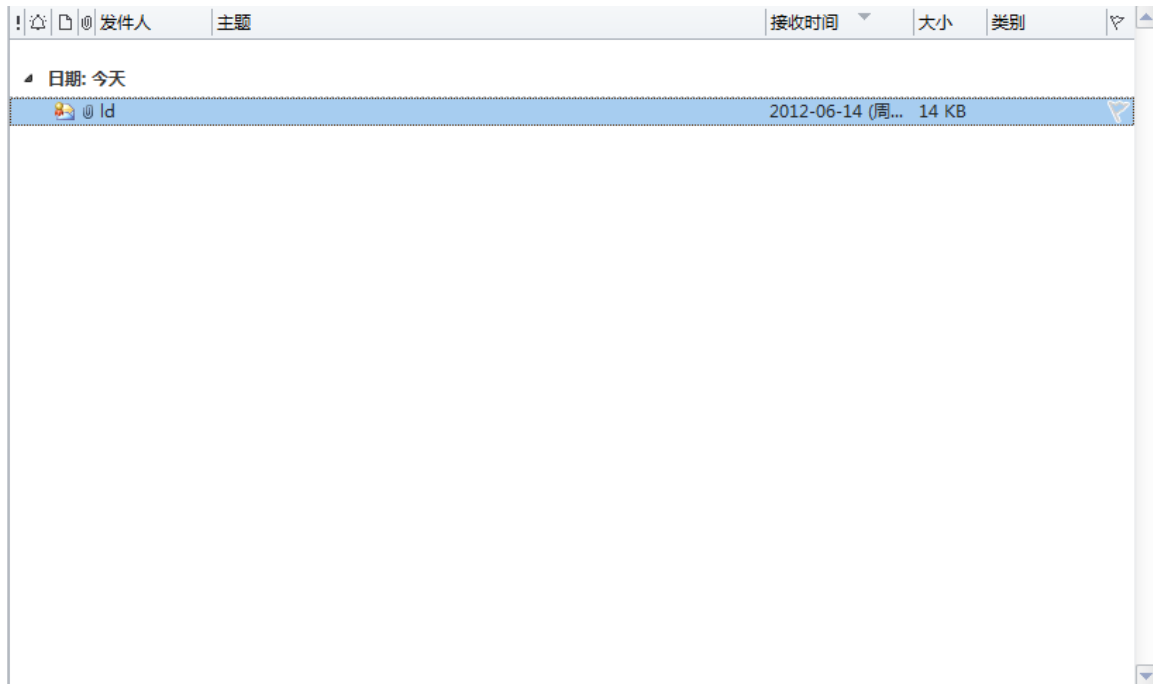
发送签名邮件时签名证书会随邮件内容一起发送，接收者可以根据证书验证邮件的签名，发送加密邮件即使用接收方的证书加密邮件，发送加密邮件时通讯簿中必须包含收件人的证书，该证书可以从 LADP 上查询获得，也可以让他发送一个签名邮件把证书一起发送过来。

1. 发送一份签名的电子邮件，选中签名，点击发送，会弹出验证窗口如下图：

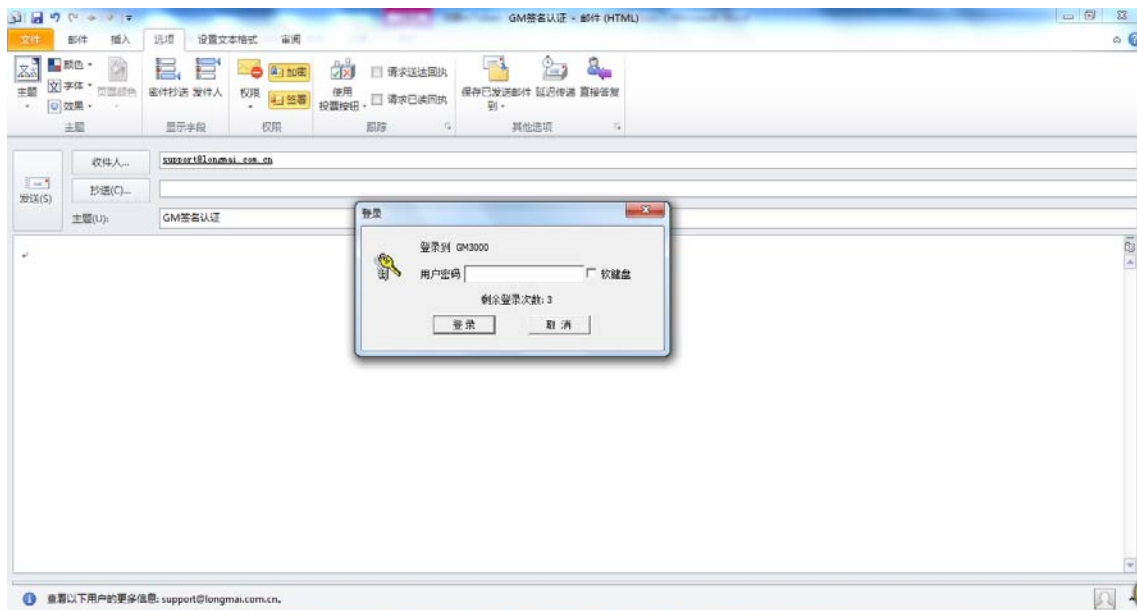


当对方收到邮件后，会将证书自动保存下来，以便下次发送加密电子邮件。

2. 接收一份带签名的邮件，如下图，接收到带证书的邮件会保存下来：



3. 发送一份带加密的邮件，通讯簿中必须包含收件人的证书，上面的操作，已保存收件人的数据标识。如下图选中“加密”，点击发送：



4. 接收一份带加密的邮件，需要进行验证口令，如下图：



用户 PIN 输入正确才能阅读此邮件。

## 联系我们

### 公司总部

地址：北京市海淀区王庄路甲1号工控办公楼三层

电话：010-62323636

传真：010-62313636

热线：400-666-0811（7\*24免费热线）

邮箱：longmai@longmai.com.cn

网站：<http://www.longmai.com.cn>

商城：<http://smart2000.taobao.com/>

邮编：100083

### 杭州办事处

地址：浙江省杭州市西湖区文三西路499号西溪风尚5幢420

电话：0571-86908895

邮箱：hangzhou@longmai.com.cn

邮编：310012

### 广州办事处

地址：广东省广州市天河区黄埔大道中路262号恒安大厦恒福轩14D

电话：020-85272610

邮箱：guangzhou@longmai.com.cn

邮编：510630

### 申请试用

如果您对产品感兴趣，可先申请试用，测试通过后再进行购买。申请试用，请到龙脉官方网站填写试用单或直接打电话与我们联系：

试用：<http://www.longmai.com.cn/apply/index.htm>

邮箱：sales@longmai.com.cn

## 购买产品

如果您希望咨询产品价格或正式购买产品，可以通过如下方式与销售人员联系：

电话：010-62323636

邮箱：sales@longmai.com.cn

QQ：2577880101

## 技术支持

我们提供了多种方式的技术支持服务，您可通过如下方式向技术人员咨询：

电话：010-62323636-661

邮箱：support@longmai.com.cn

Q Q：1586313196