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

mToken GM3000 Firefox 及 Thunderbird 证书应用

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

© 北京世纪龙脉科技有限公司，2013

第一章 GM3000 的 FireFox 应用

GM3000 提供了符合业界规范的Microsoft CryptoAPI 和PKCS#11 接口，并支持多个证书和密钥对的存放，任何兼容这种接口的应用程序都可以立即集成 GM3000 进行使用。

本章主要讲述 GM3000 的 FireFox 应用，本手册还讲述了在 linux 平台下使用 GM3000 进行申请数字证书、访问 SSL 加密站点和收发签名、加密邮件。

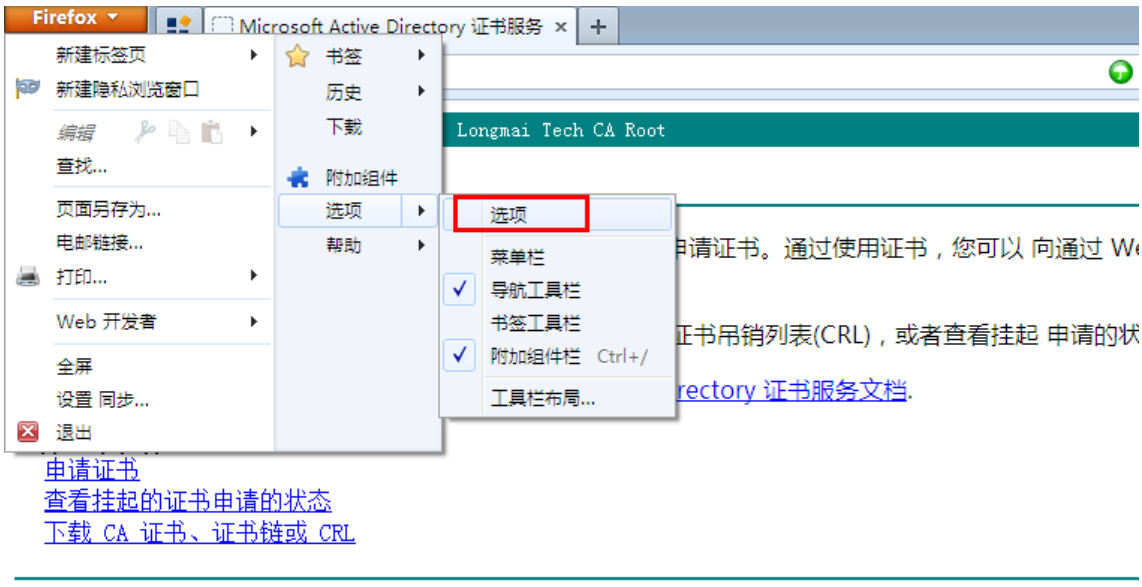
Linux 平台下注意事项：

1. GM3000 PKCS11 在 Linux 内核 2.6.32 编译，并在 UBUNTU X86,X64 下测试通过
2. 在使用 GM3000 PKCS11 模块之前请确认 sg3_utils 成功安装到系统中，可通过 sg_map -i 来检查是否正确安装 sg3_utils 网站： http://sg.danny.cz/sg/sg3_utils.html
3. 如果您使用的是其它版本 LINUX,请与龙脉科技联系是否适用

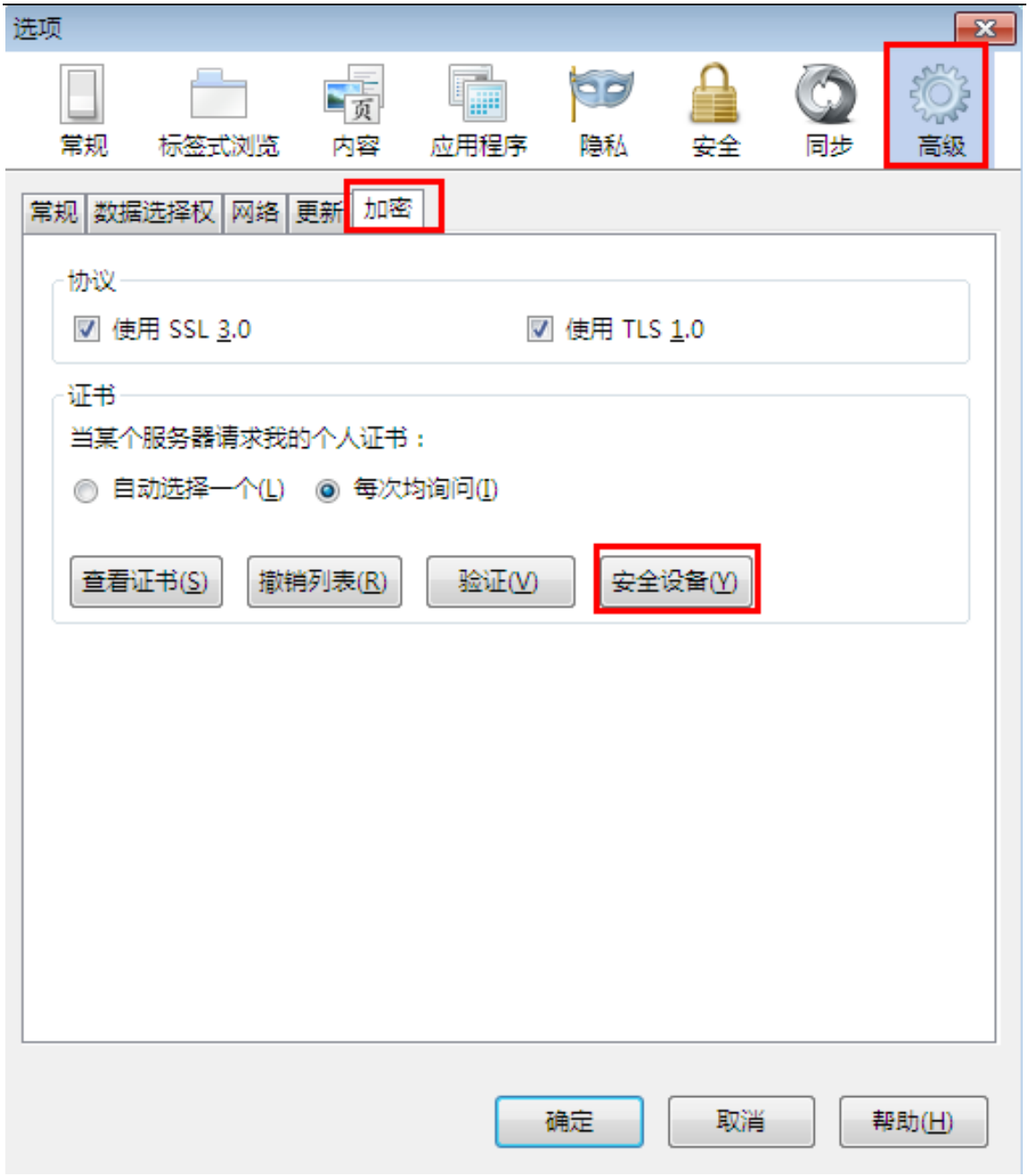
1.1 Linux 平台下的 FireFox 与 GM3000 的应用

在 Linux 下为了能够使 FireFox 能够对 GM3000 进行操作，必须是 FireFox 集成 GM3000。在打开 FireFox 后，具体的操作步骤如下：

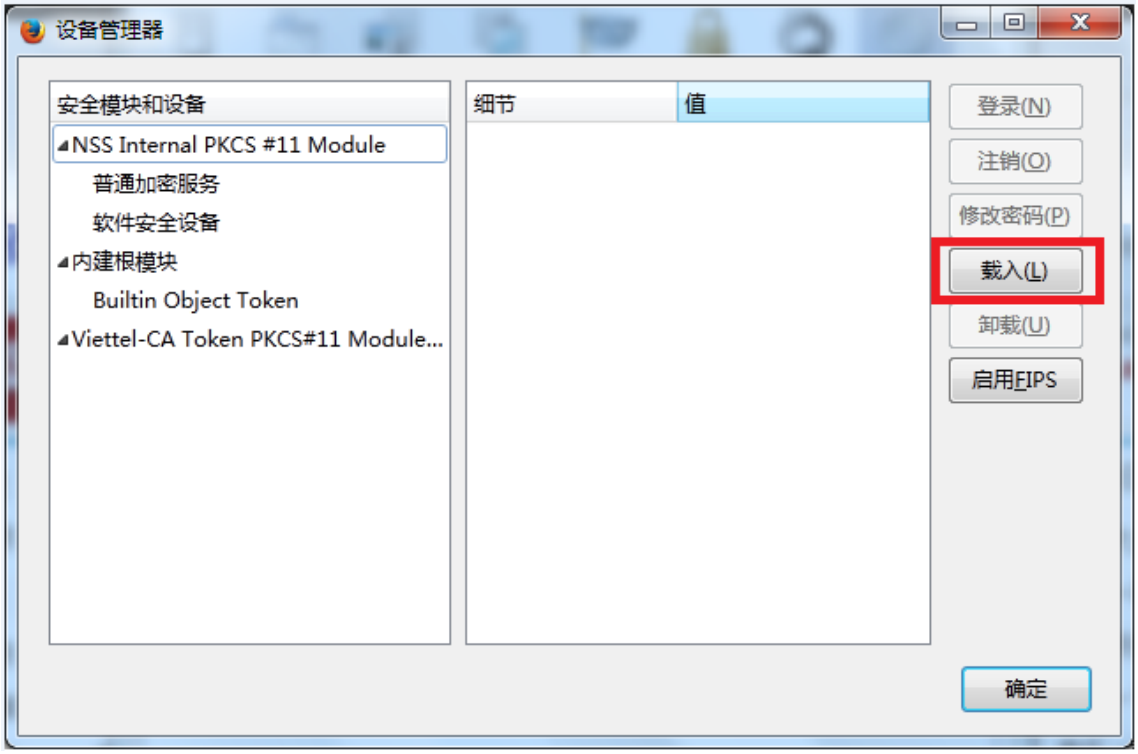
1. 启动 FireFox 后，“选项”菜单单击，如下图所示：



2. Firefox 将弹出“选项”弹框，选择“高级→加密”选项，然后点击“安全设备”按钮，如下图所示：



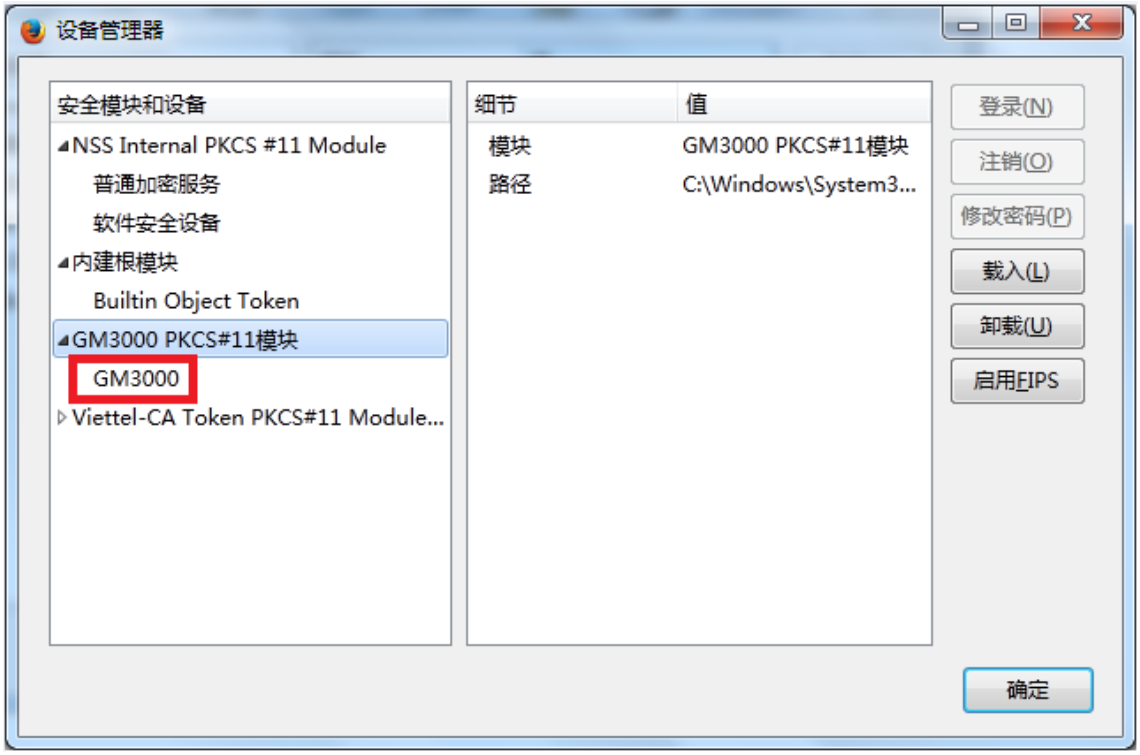
3. 点击了安全设备按钮，FireFox 将弹出“设备管理器”弹框，然后点击“载入”按钮，如下图所示：



4. 点击“下载”按钮后，会弹出如下弹框，请您输入或选择安全模块的名称和路径，路径为：C:\Windows\System32\GM3000_pkcs11.dll(C 盘为系统所在的盘符)，如下图所示：

5. 点击“确定”后，会在设备管理器左侧出现 GM3000 模块的信息，其中“GM3000 PKCS#11 模块”显示“GM3000”插入了计算机，如下图所示：

© 北京世纪龙脉科技有限公司，2013



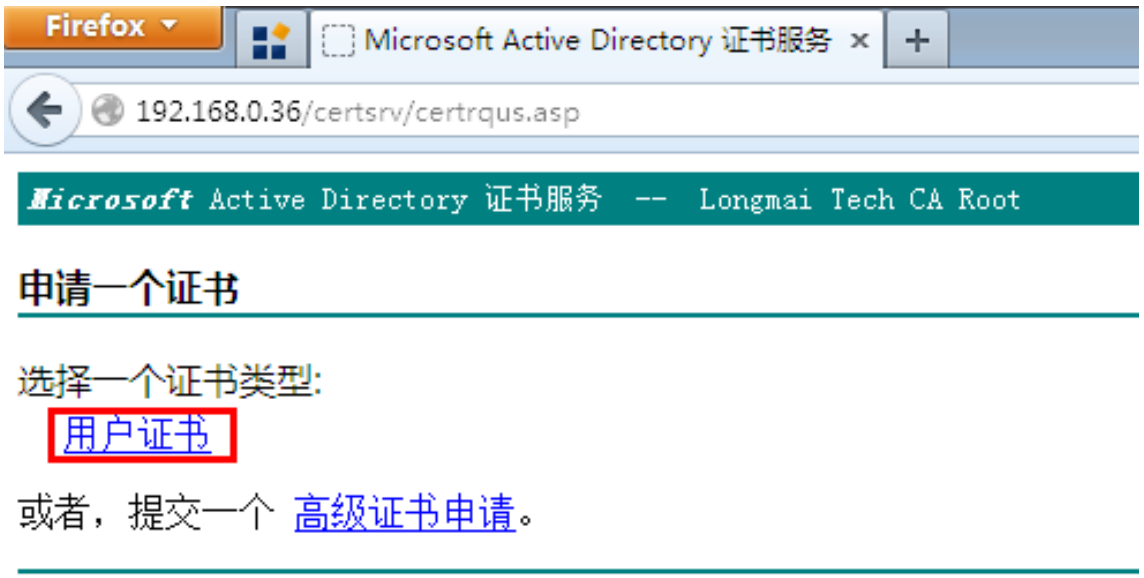
此时，您已经成功将 GM3000 与 FireFox 集成了，您可以对该 GM3000 进行登录和登出操作。

1.2 使用 GM3000 的 pkcs#11 申请数字证书

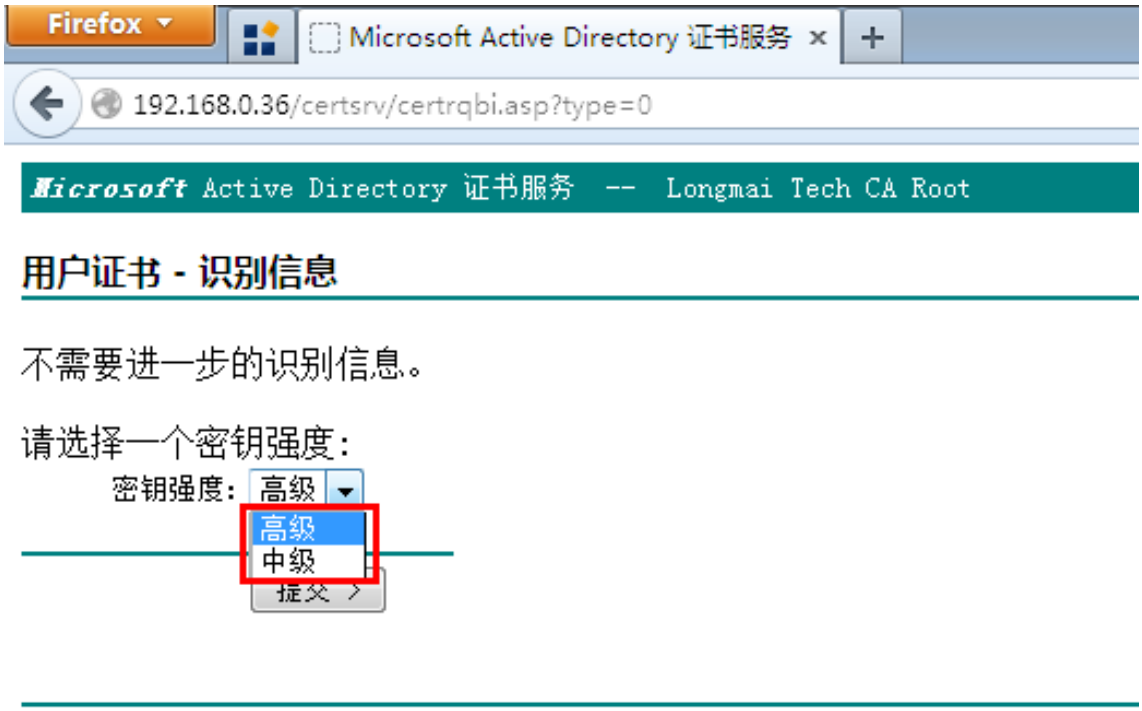
我们以在 Linux 平台下的 FireFox 为例来说明使用 pkcs#11 的证书申请过程。

1. 插入一只未装证书的 GM3000，然后通过 FireFox 打开证书颁发机构的网页，如下图所示：

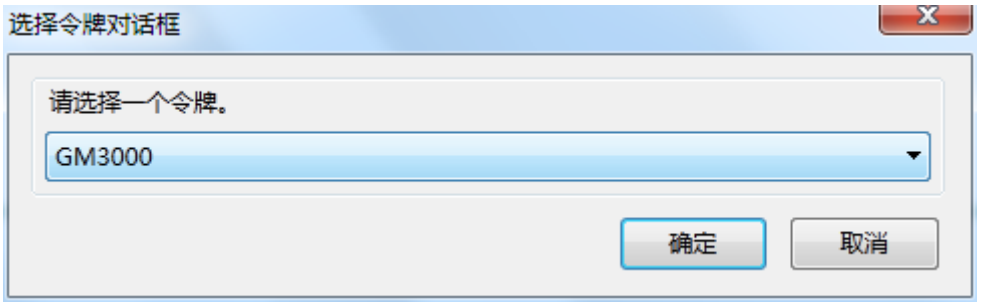
2. 选择“申请证书”后，进入“选择申请类型”界面，选择“用户证书”单击按钮，如下图所示：



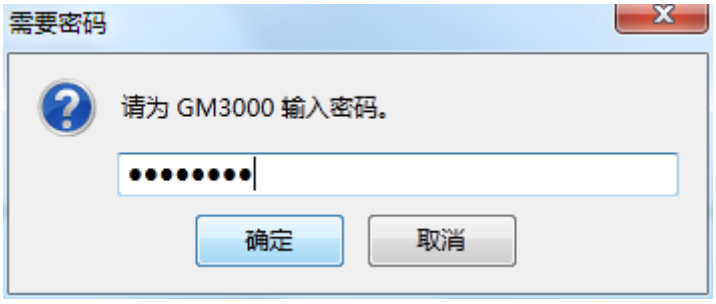
3. 接着，进入选择密钥长度的页面，在下拉框中选择合适的密钥长度，如下图所示：



4. 点击“提交”按钮后，会弹出一个“记号选择对话框”，要求选择所要产生密钥对的安全设备，从中选择 GM3000，然后点击“OK”按钮，如下图所示：

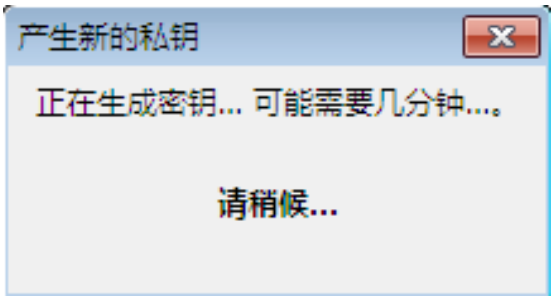


5. 这时，FireFox 弹出对话框要求用户输入 PIN 码，如下图所示：

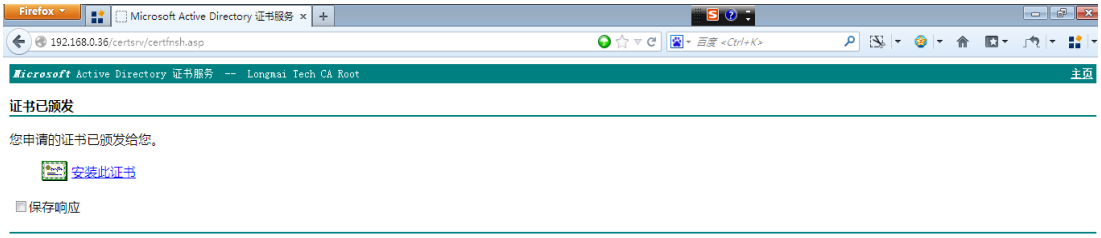


注意：如果在 1.1 的最后一步中已经登录了，那么在此处就不会出现 PIN 码框而直接产生密钥对。

6. 点击“确定”按钮后，FireFox 开始产生密钥对，如下图所示：



7. 密钥对产生完成后，FireFox 将密钥信息以及个人信息发送给证书颁发机构，由证书颁发机构颁发证书，成功后转向如下图所示的界面：



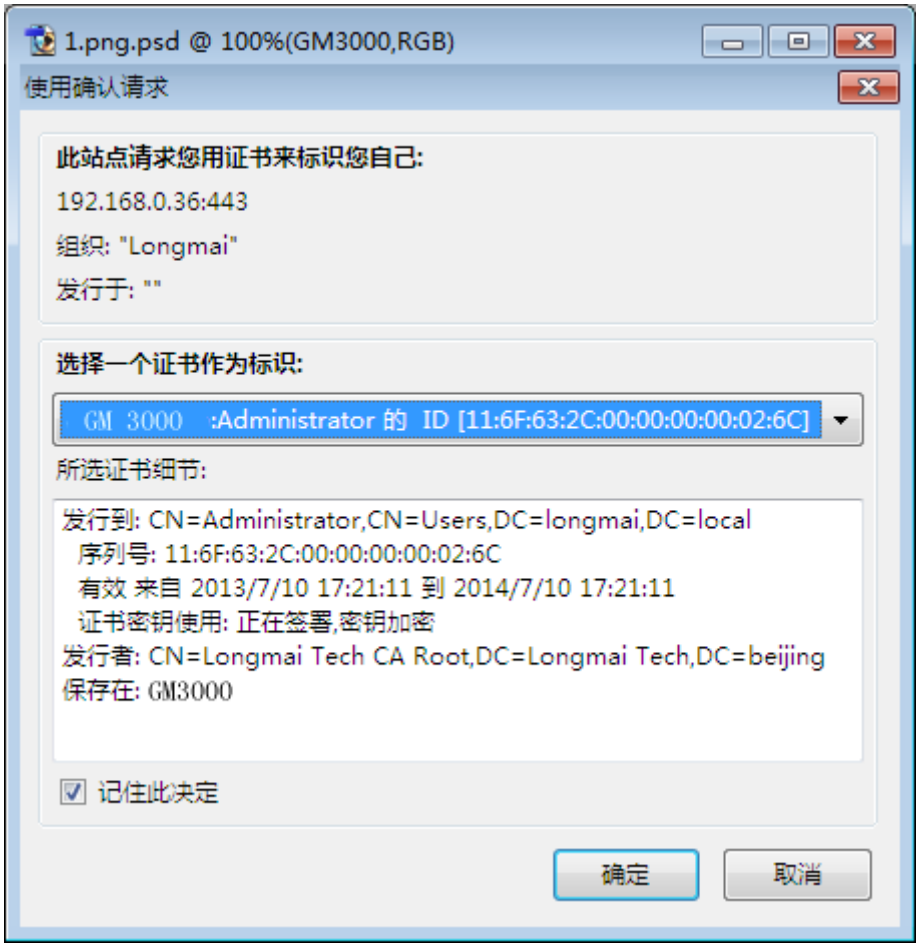
8. 点击所示页面的“安装证书”链接，FireFox 将此证书安装 GM3000 中，至此，整个证书申请流程完成。

1.3 使用 GM3000 的 pkcs#11 访问 SSL 加密站点

1. 确认已经在计算机的 USB 口上插上含有证书的 GM3000。启动 FireFox，用 https 协议访问 SSL 加密站点。
2. 如果一切正常，FireFox 将陆续弹出所有和计算机连接的安全设备的密码框，此处只有 GM3000 和计算机连接，其 PIN 码输入框如下图所示：

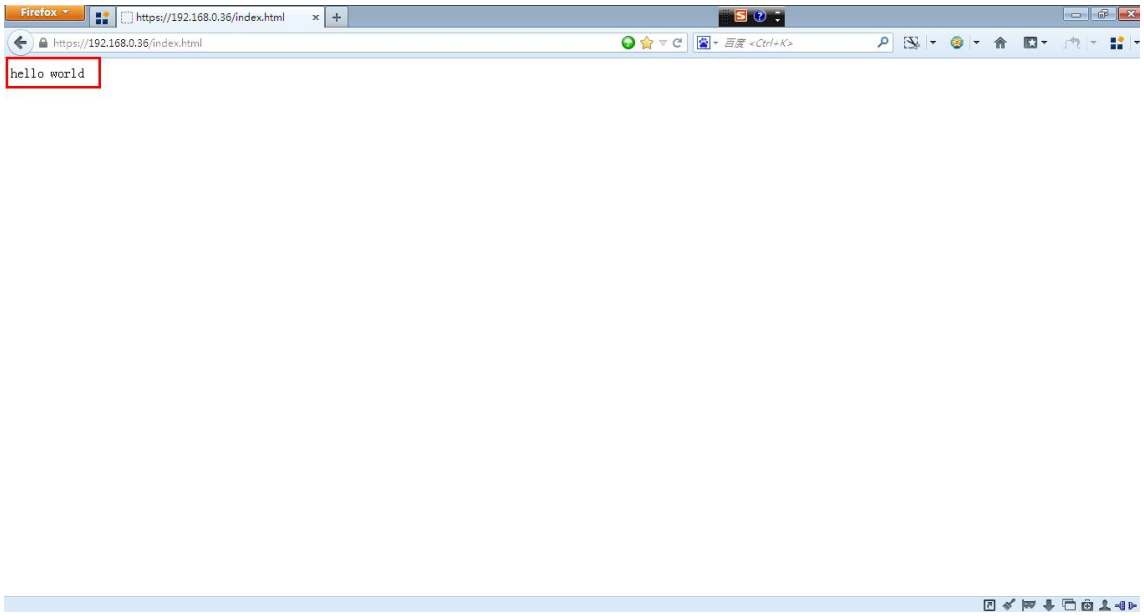
© 北京世纪龙脉科技有限公司，2013

3. 输入 PIN 码并点击“确定”按钮后 FireFox 将访问 GM3000 的 pkcs#11 接口，加载 GM3000 上的密钥和证书信息，然后弹出所有符合要求证书列表，请用户选择其中一个作为用户的身份信息，如图所示：



注意：如果在 1.1 的步骤当中的“选项”弹框中“证书”那一块儿选择了“自动选择一个”单选按钮，FireFox 会自动选择证书，则不会弹出上图所示的选择证书对话框，如果选择“每次均询问”单选按钮，才会弹出上图所示的选择证书对话框。

4. 选择相应的证书后点击“OK”按钮，FireFox 就会和该 SSL 加密站点交换信息，并进行一系列的认证过程。如果一切都符合要求，则所访问的页面就会显示出来（此安全 WEB 站点为示例站点）如下图所示：



1.4 使用 GM3000 的 pkcs#11 收发签名与加密邮件

本小节以 Linux 平台下的 Thunderbird 为例来说明使用 pkcs#11 获取安全邮件证书以及收发签名与加密邮件的过程。

在使用 Thunderbird 之前，首先要保证用户可以使用 Thunderbird 发送普通邮件，即首先需要连接上电子邮件服务器和配置好用户账号信息，在这些操作都完成后，要设置 Thunderbird 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，当获取用户的安全证书后，用户才可以发送具有数字签名或者信息加密的电子邮件。

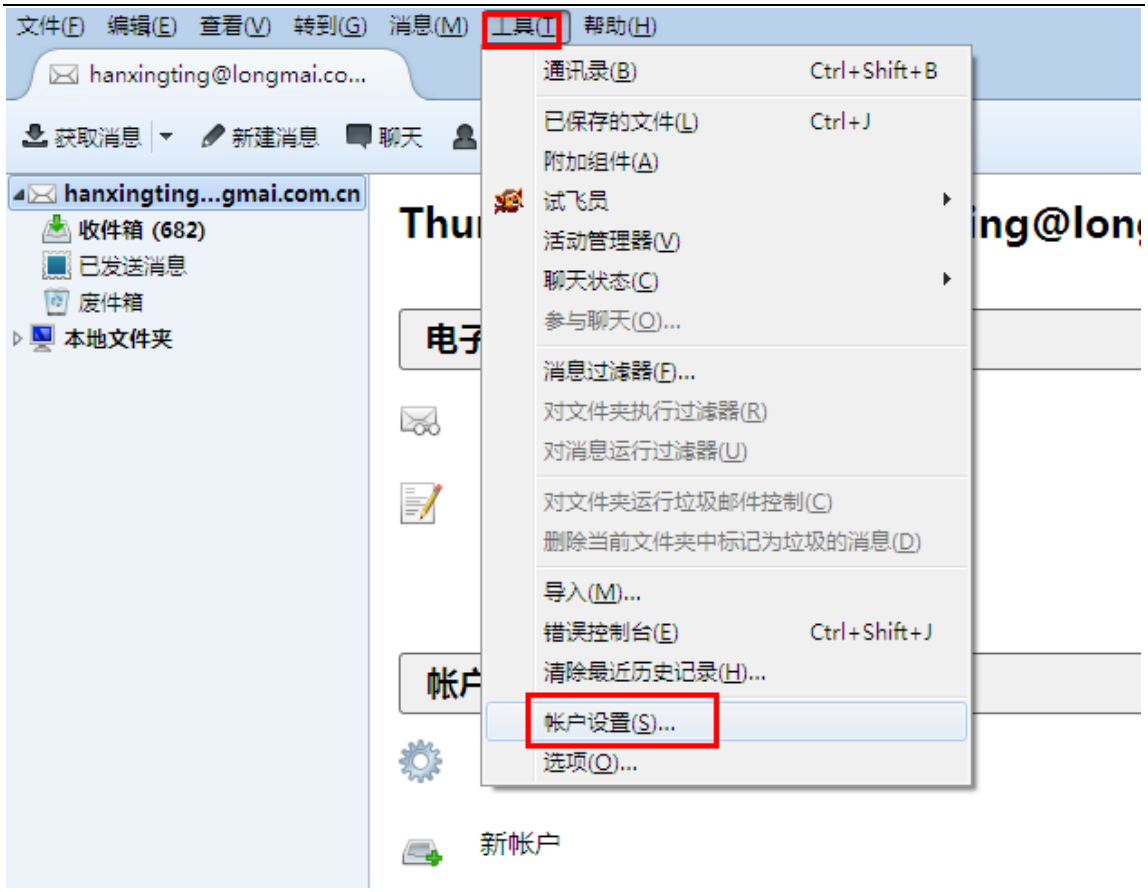
1.4.1 获取得到安全电子邮件数字证书

获取安全邮件数字证书的方法大致流程和 1.2 小节中的申请流程大致相同，具体申请方法和 CA 服务器的设置和选项相关，申请的证书必须是具有邮件属性的证书。在获取数字证书后，用户就可以开始设置 Thunderbird 中的 Email 账号，让 Email 账号具有安全处理邮件的能力。

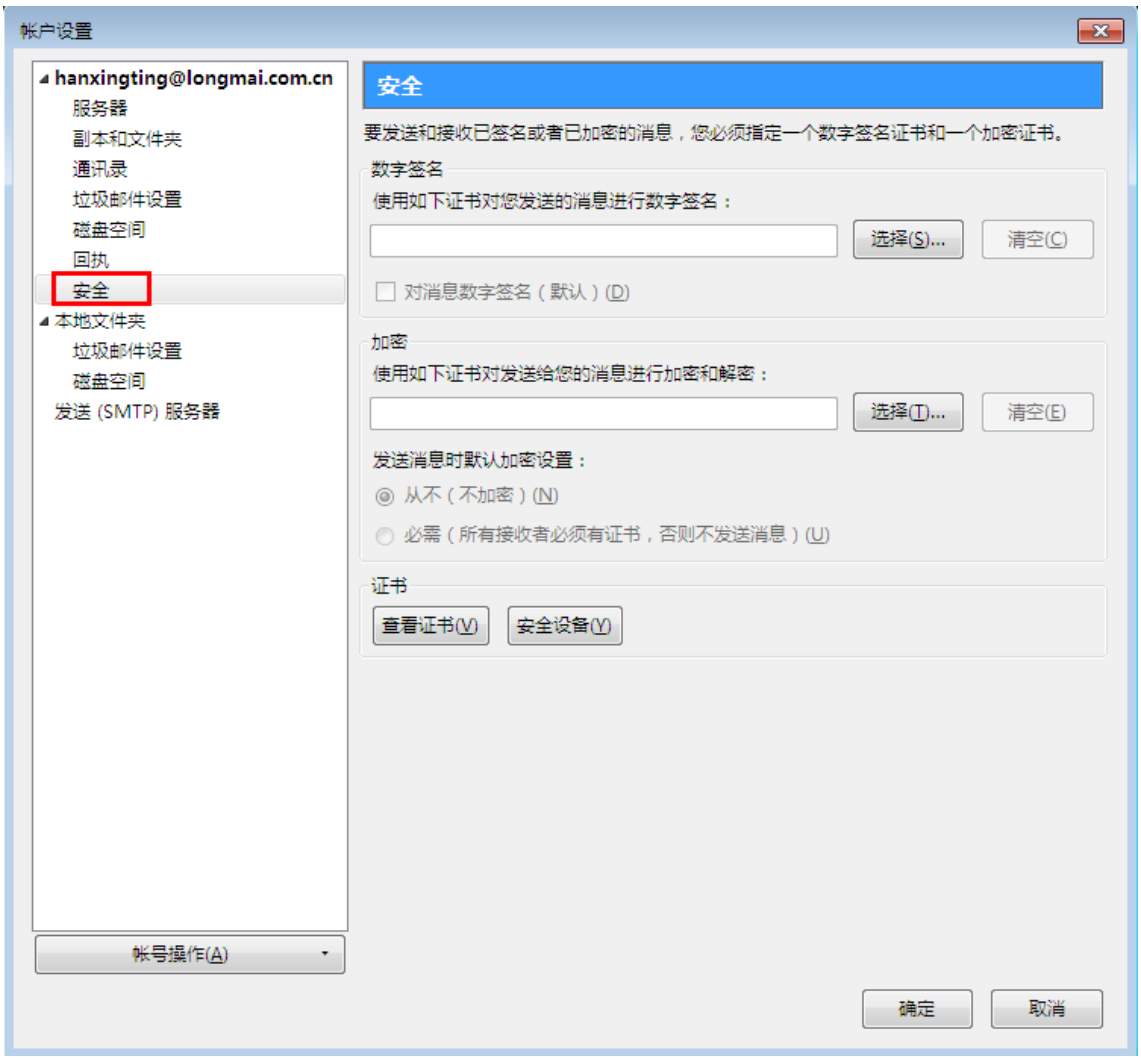
1.4.2 设置 Email 账号的安全性

设置 Email 账号的安全性，请按照以下步骤操作顺序来操作：

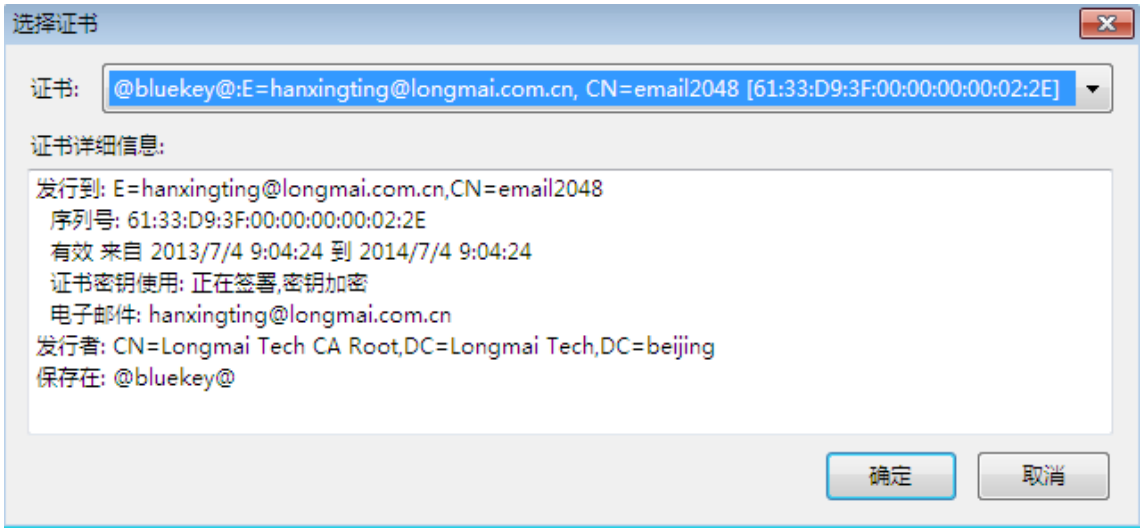
1. 启动 Thunderbird，用户需要在 Thunderbird 设置了安全性邮件的数字证书，选择菜单“工具→账号设置”，如下图所示：



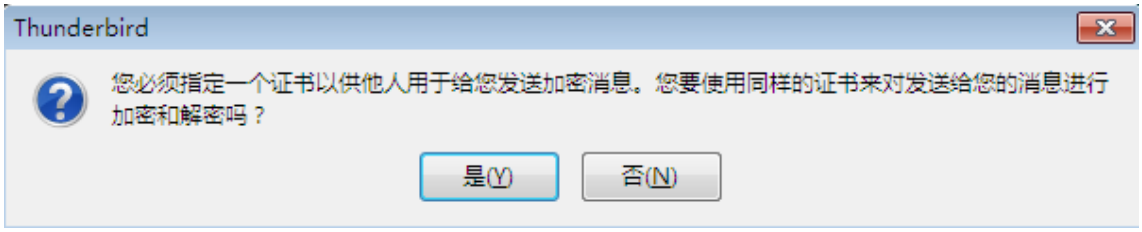
2. 在点击了“账号设置”之后，弹出“账户设置”的弹框，选择左侧菜单的“安全”选项，如下图所示：



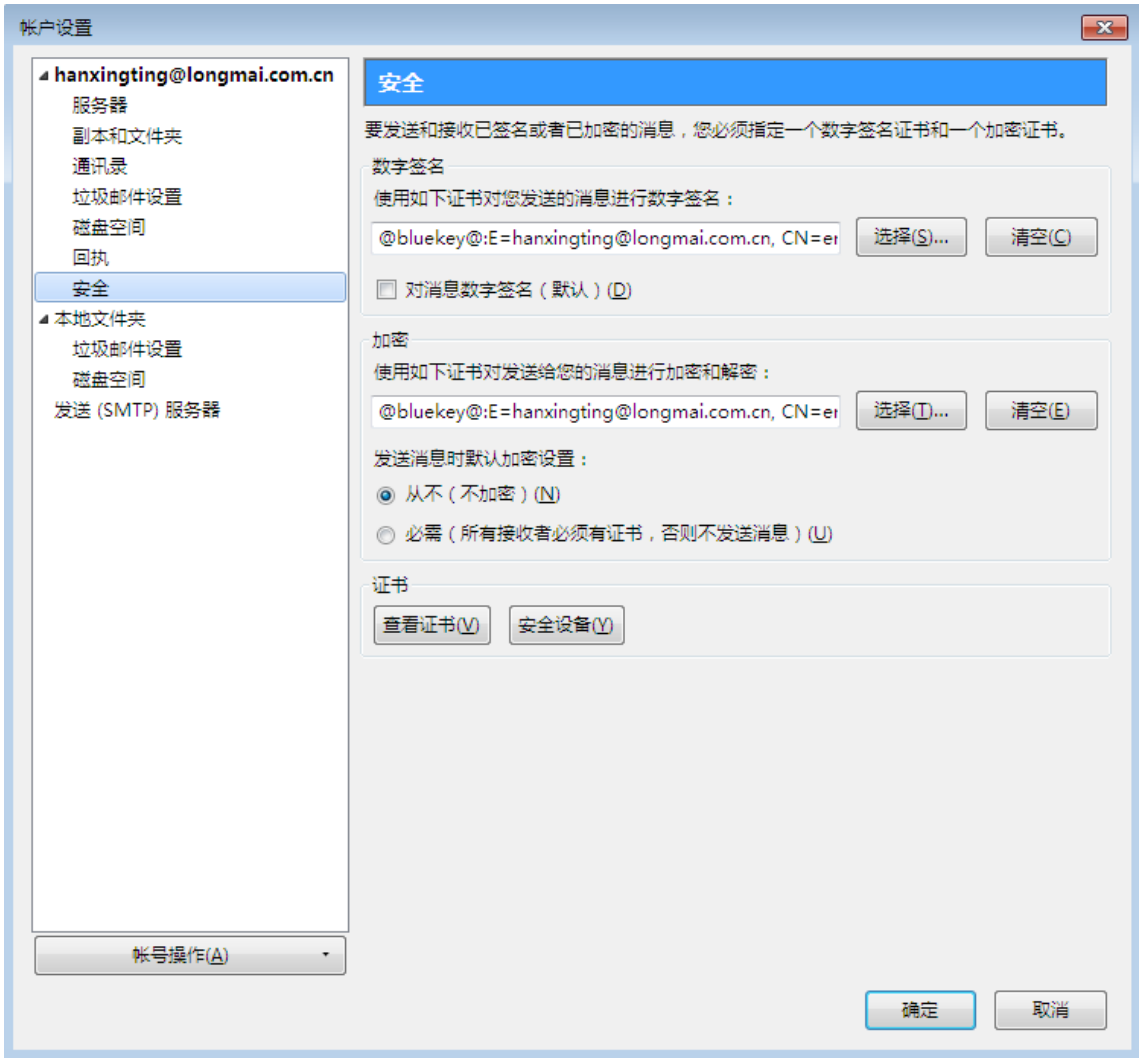
3. 选择右侧的“选择”按钮，Thunderbird 就能将 hanxingting@longmai.com.cn 账号的签名证书列出，供用户选择，输入锁密码之后，出现如下图所示：



4. 选择具有邮件属性的数字证书，选择之后，证书会出现在空白栏内，点击“OK”之后，Thunderbird 又会弹出对话框提示用户指定一个加密证书由其他人给 hanxingting@longmai.com.cn 发送加密邮件时使用，如下图所示：



5. 点击“是”按钮后，Thunderbird 自动将指定的签名证书作为加密证书，如下图所示：



在上图中，可以勾选“对消息数字签名”的选项来指定在缺省情况下对发出去的邮件进行签名，同时也可以勾选“必需（所有接收者必须有证书，否则不发送消息）”来指定在需要情况下对发出去的邮件进行加密。您也可以采用

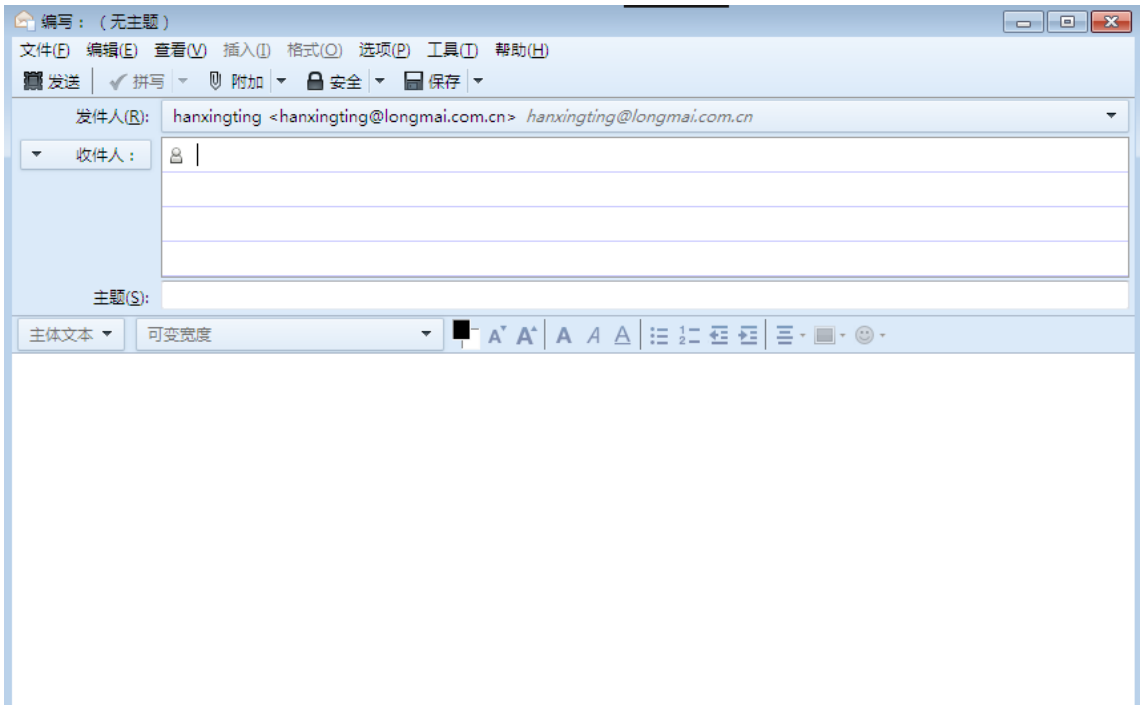
下面的方法来对发出去的邮件进行签名或加密。

至此，已经将 hanxingting@longmai.com.cn 账号的签名证书和加密证书设置完成，可以发送签名和加密邮件了。

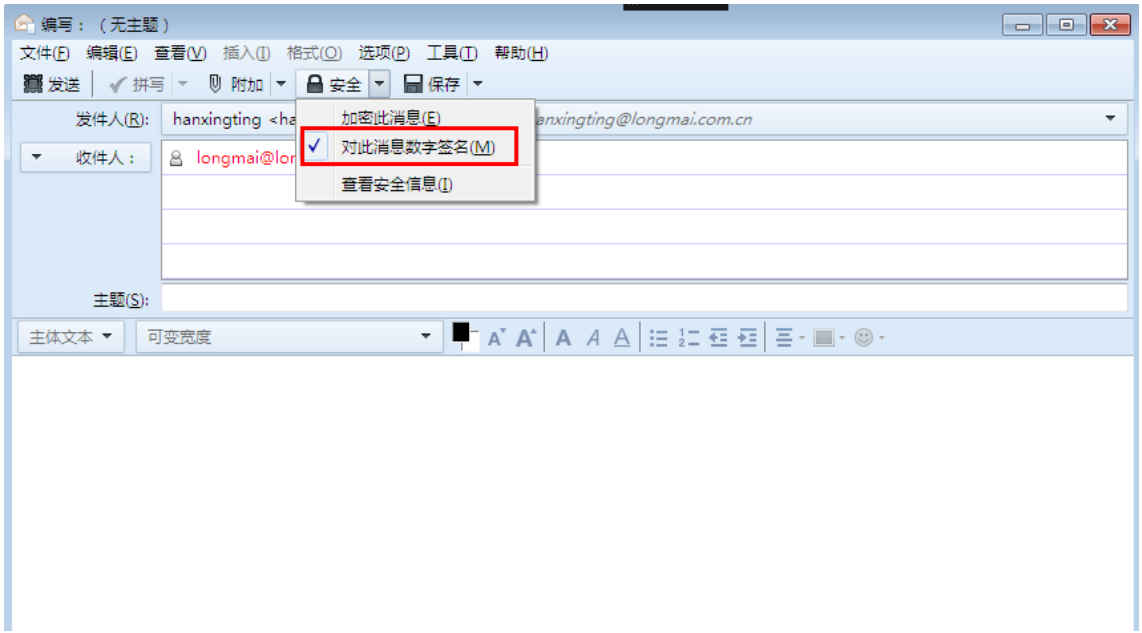
1.4.3 使用 Thunderbird 发送附加数字签名的证书

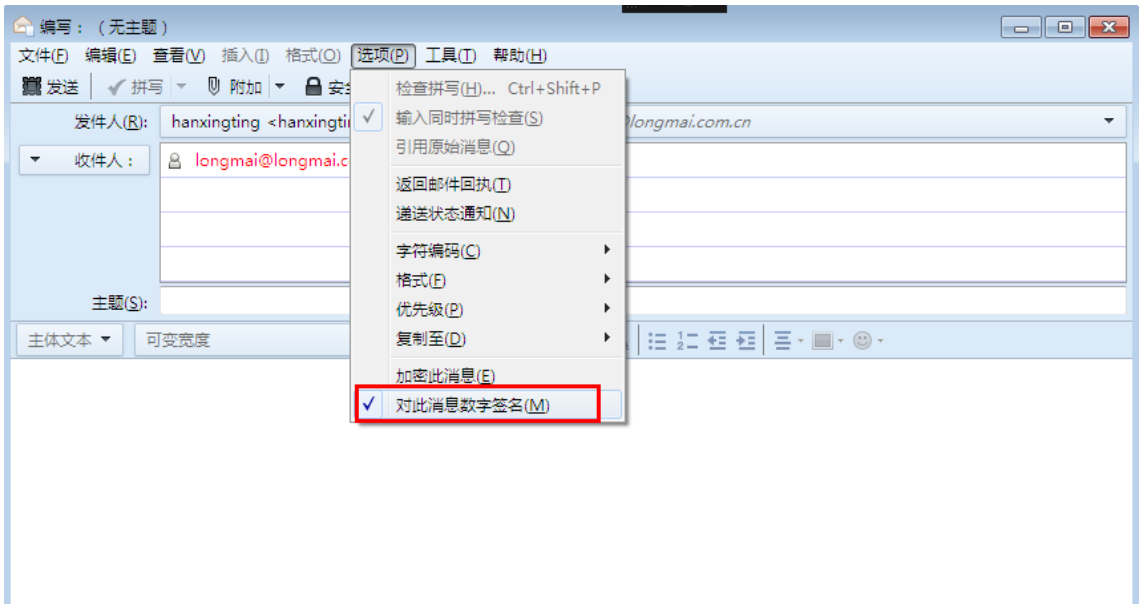
当设置好 Thunderbird 里的安全设置选项后，用户就可以开始发送具有安全性质的电子邮件，现在，我们就列出如何在发送出去的邮件中附加数字签名的操作步骤，步骤如下：

1. 启动 Thunderbird，点击工具栏上的“新建消息”按钮，打开书写邮件的编辑器，如下图所示：



2. 所有内容书写完毕后，点击工具栏上的“安全”按钮，在弹出的菜单上选择“对此消息数字签名”，或者选择 Thunderbird 的菜单“选项→对此消息数字签名”（如下图所示），将该邮件签名。





3. 然后点击工具栏上的“发送”按钮，发出邮件。如果之前没有输入过 GM3000 的 PIN 码，则 ThunderBird 会弹出 PIN 码输入框，请求输入 PIN 码，用户输入正确的 PIN 码后即可将邮件发送出去。

1.4.4 获取收件人的公钥和证书

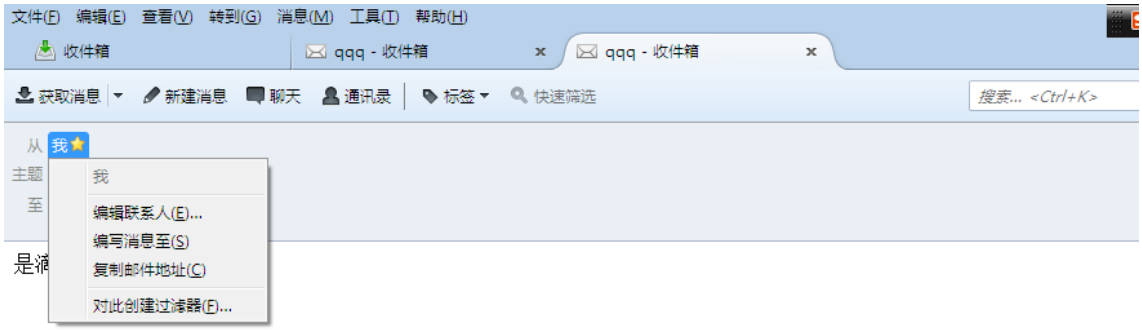
若要发送加密的电子邮件，用户必须先获取对方的公钥或者证书，再利用对方的公钥对用户信息进行加密处理(也就是使用收件人的公钥来进行加密)，这时候，只有此公钥映射的私钥（此私钥只有收件人持有）才能够对此加密过的信件进行解密的处理，因此，只有持有该私钥的人，才能够阅读该信件。

用户要获取对方的公钥或者证书，必须要求对方发送一封带有数字签名的信件，用户将此带有数字签名信息的邮件中的证书存储下来，这时候用户就拥有了对方的证书以及公钥的信息。

若要存储证书或公钥，请按照下列的步骤进行操作：

1. 先要求对方给您发送一份带有数字签名的电子邮件。
2. 启动 ThunderBird 接受并打开对方发送过来的带有数字签名的电子邮件，点击该邮件右侧的信封模样的图标，ThunderBird 弹出一窗口显示发送者的信息及签名证书，以供用户检查该数字签名的正确性。

3. 在上图中的左侧的 从 栏后面的邮件地址上鼠标单击，则出现如下图所示菜单：



4. 选择“编辑联系人”，将对方的姓名及地址加入到地址簿中，这样对方的证书已经和其邮件地址关联起来了。

实际上如果收到过对方的签名邮件，那么该邮件地址和其证书已经被自动关联起来并被 ThunderBird 记录下来。以后发送加密邮件时只要在收件人栏中写入该邮件地址，ThunderBir 会自动使用其关联的证书。

© 北京世纪龙脉科技有限公司，2013

1.4.5 使用 ThunderBird 发送加密邮件

若要发送加密的邮件给对方，要确定发件人已经使用上一节的方式获取对方的公钥或者证书等信息（证书包含了公钥的信息）。在这里，假设发件人已经以上一节的方式获取对方的公钥证书并且已经存储在 ThunderBird 的通讯簿列表中了。

要发送一封加密的邮件，按照下列的步骤进行操作：

方法一：直接回复发件人

1. 启动 ThunderBird。
2. 打开对方发过来的邮件，然后选择菜单中的“回复”按钮，则 ThunderBird 打开书写回复邮件的界面窗口。
3. 书写完毕后，选择“安全”按钮下的“加密此消息”，或者选择 ThunderBird 的菜单“选项→加密此消息”。
4. 然后点击工具栏上的“发送”按钮，发出邮件。如果以前没有输入过 GM3000 的 PIN 码，则 ThunderBird 会弹出 PIN 码输入框，请求输入用户 PIN 码，输入正确的 GM3000 的 PIN 码后点击“OK”按钮即可将邮件发出。

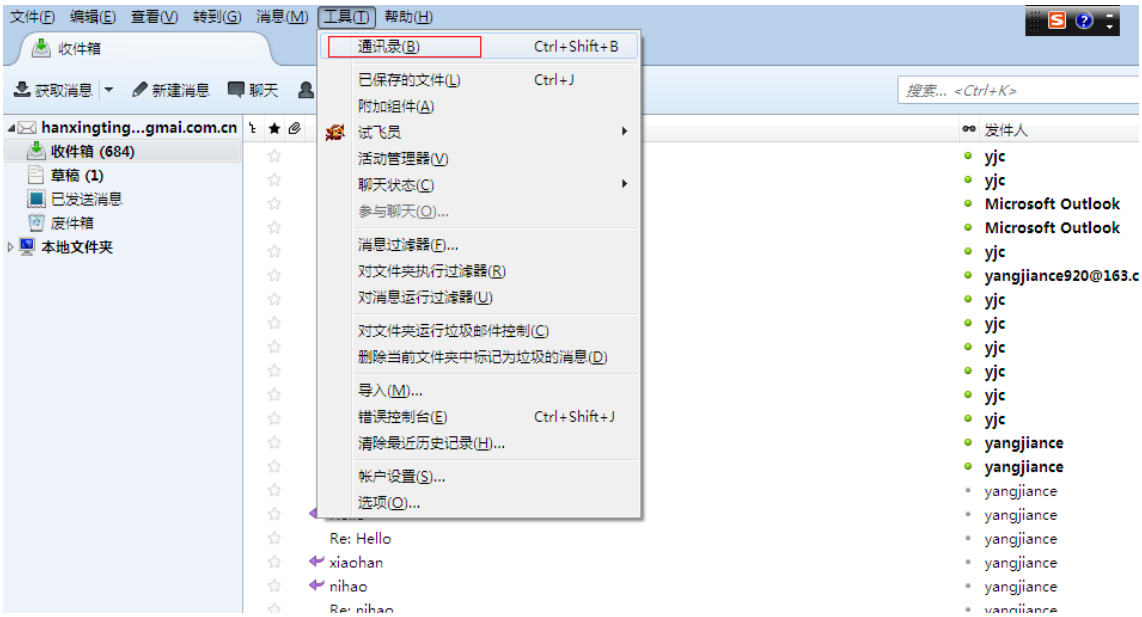
方法二：直接输入收件人邮件地址

1. 启动 ThunderBird。
2. 点击工具栏上的“新建消息”按钮，打开书写新邮件的编辑器。
3. 在邮件的收件人中填入正确的电子邮件地址，则 ThunderBird 自动会使用该电子邮件地址所关联的证书作为加密证书。
4. 书写完毕后，选择“安全”按钮下的“加密此消息”，或者选择 ThunderBird 的菜单“选项→加密此消息”。
5. 然后点击工具栏上的“发送”按钮，发出邮件。如果以前没有输入过 GM3000 的 PIN 码，则 ThunderBird 会弹出 PIN 码输入框，请求输入用户 PIN 码，输入正确的 GM3000 的 PIN 码后点击“OK”按钮即可将邮件发出。

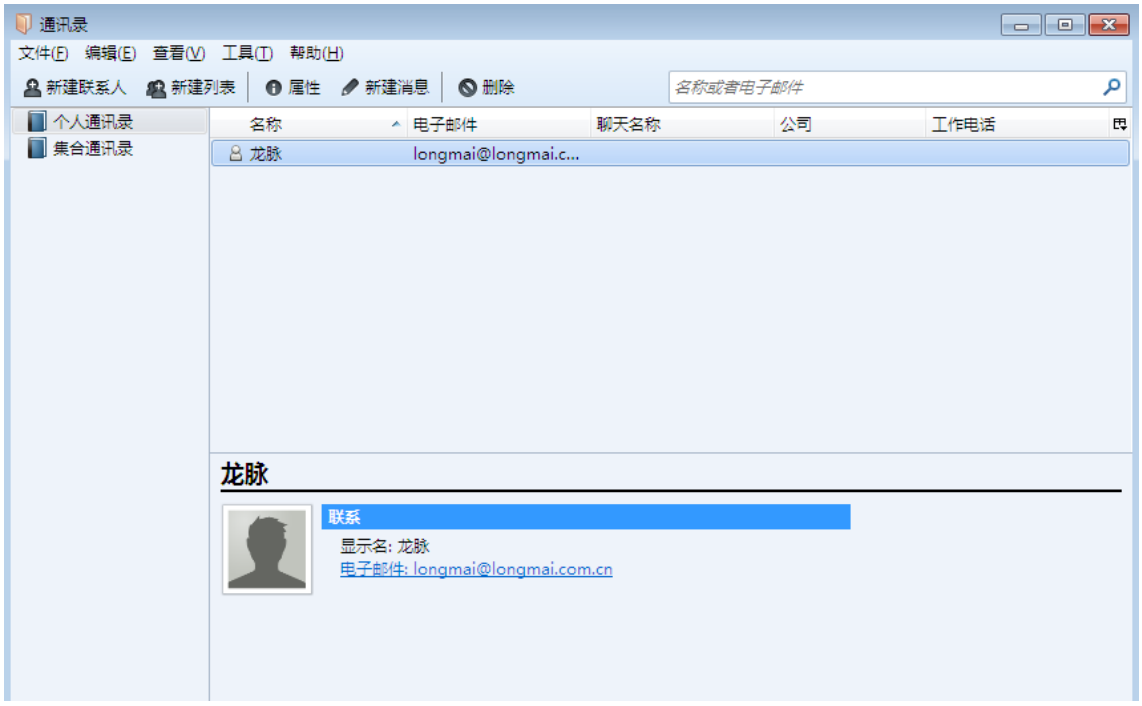
方法三：从地址簿中选择收件人

1. 启动 ThunderBird。
2. 选择菜单中的“工具”下的“通讯录”，如下图所示：

© 北京世纪龙脉科技有限公司，2013



3. 选取“通讯录”菜单后，ThunderBird 将地址薄窗口打开，如下图所示：



4. 选择要发送邮件的地址，然后点击工具栏中的“新建消息”，则 ThunderBird 的书写新邮件的窗口就会打开。打开之后的流程，请参考 1.4.3 的流程。

1.4.6 使用 ThunderBird 发送签名加密邮件

此过程与发送加密或签名邮件的过程相似，在选择安全选项时将“加密此消息”和“对此消息数字签名”同时选中。

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（7x24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

© 北京世纪龙脉科技有限公司，2013

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

© 北京世纪龙脉科技有限公司，2013