

Outlook 2010 电子邮件签名加密指南



沃通电子认证服务有限公司

WoTrus CA Limited

目 录

一、	安装电子邮件签名加密证书的环境	3
1.1	电子邮件签名加密证书安装环境简介	3
1.2	网络环境要求	3
二、	电子邮件签名加密证书的安装	3
2.1	获取电子邮件签名加密证书	3
2.2	安装电子邮件签名加密证书	5
2.3	配置 Outlook 邮件客户端	5
2.3.1	配置 Outlook 帐号使用数字证书	5
2.4	发送数字签名的邮件	6
2.5	发送加密的电子邮件	7
三、	电子邮件签名加密证书的备份	9
四、	电子邮件签名加密证书的恢复	9

技术支持联系方式

技术支持邮箱: support@wotrus.com

技术支持热线电话: 0755-26027828

技术支持网页: <https://bbs.wosign.com>

公司官网地址: <https://www.wosign.com>

一、安装电子邮件签名加密证书的环境

1.1 电子邮件签名加密证书安装环境简介

Windows pc 机一台

安装 office outlook2010 软件

电子邮件签名加密证书一张（备注：本指南使用 supp2@wosign.com 电子邮件签名加密证书进行操作,通用其它版本证书）

1.2 网络环境要求

请确保您的电脑可以正常收发邮件。

二、电子邮件签名加密证书的安装

2.1 获取电子邮件签名加密证书

最终沃通数字证书系统将会给您颁发证书文件（.zip）压缩格式，当中有包含三种证书格式如：for Apache、for Nginx、for Other Server；IIS 应用服务器上需要 for Nginx 里面的 crt 证书文件，然后用工具合成 pfx 格式：

 for Apache.zip	2019/1/21 14:15	ZIP 文件	6 KB
 for Nginx.zip	2019/1/21 14:15	ZIP 文件	6 KB
 for Other Server.zip	2019/1/21 14:15	ZIP 文件	7 KB

打开 for Nginx 文件可以看到公钥，如图 2

 test.wosign.com_bundle.crt	2017/11/27 15:27	安全证书	6 KB
--	------------------	------	------

图 2

私钥 key 文件，需要找到生成 CSR 一起生成出的两个文件，如图 3，其中一个是.key 文件。



图 3

合成工具下载地址：<https://download.wosign.com/wosign/wosigncode.exe>

合成方式：先把 key 文件放到 for nginx 里，再双击下载的工具，选择证书项，操作选项，选择证书格式转换，源格式选择 PEM，目标格式选择 PFX。

证书文件：点击后面的选择按钮，找到 for nginx 目录，选择 yourdomain.com_bundle.crt，点击确定。

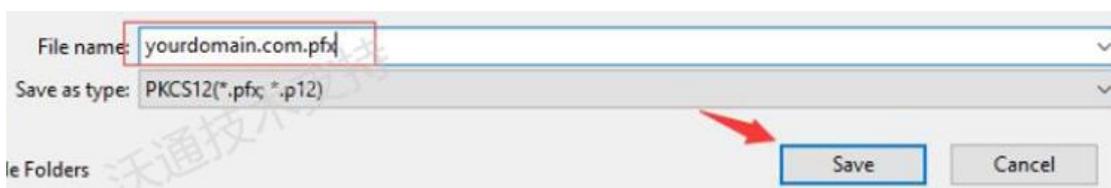
私钥文件：点击后面的选择按钮，找到 for nginx 目录，选择 yourdomain.com.key，点击确定。

私钥密码：为空，不用填写（因为生成私钥的时候没有填写，如果之前有填写过私钥密码，这里也填写相同的私钥密码）

PFX 密码：任意填写一个密码（合成 PFX 格式证书后的密码，之后在 IIS 上安装证书的时候需要使用到）



填写完毕后，点击转换，选择保存证书文件的位置，填写证书名称，推荐使用 yourdomain.com.pfx，点击保存。



最后，得到 pfx 格式证书。

 yourdomain.com.key	12/5/2017 12:02 PM	KEY File	2 KB
 yourdomain.com.pfx	3/6/2018 10:15 AM	Personal Informati...	6 KB
 yourdomain.com_bundle.crt	12/5/2017 12:02 PM	Security Certificate	6 KB

2.2 安装电子邮件签名加密证书

开始 -> 运行 -> MMC，启动控制台程序 -> 选择菜单“文件 -> 添加/删除管理单元” -> “添加” -> “可用的独立管理单元”列表中选择“证书” -> 选择“当前用户”。在控制台的左侧显示证书树形列表，选择“个人” - “证书”，右键单击，选择“所有任务-> 导入”，根据“证书导入向导”的提示，将.pfx 格式文件导入“**根据证书内容自动选择存储区**”。（注意导入过程中勾选该选项，并且需要输入密码）导入成功后，可以看到如图 2 所示的证书信息；也可以双击 pfx 证书，根据提示下一步安装证书。

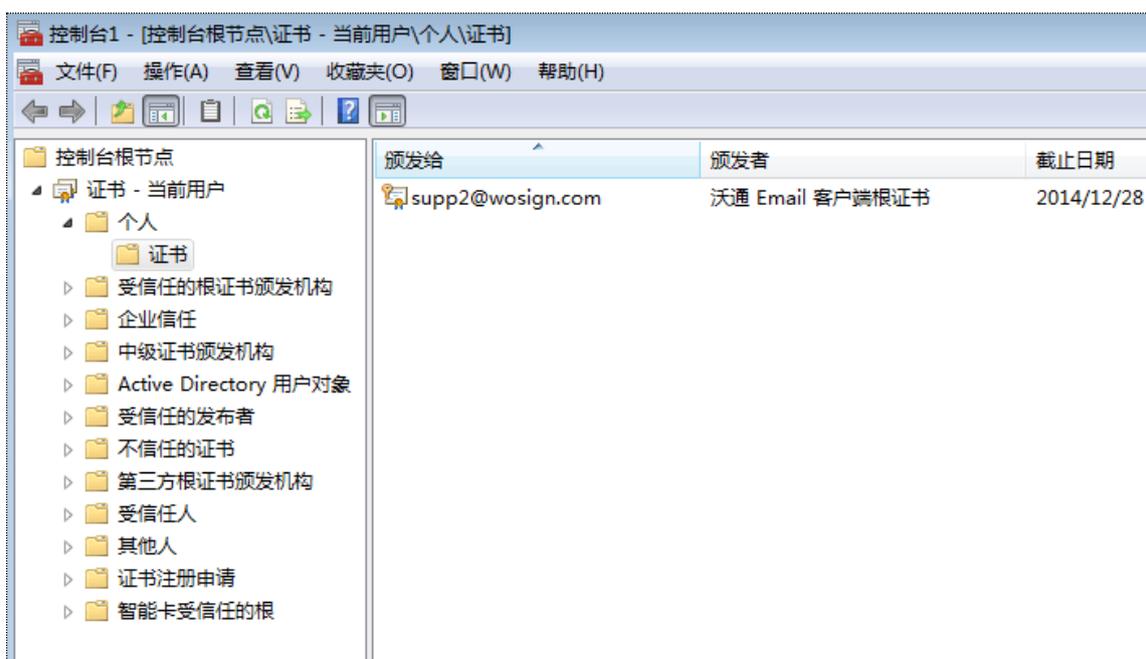


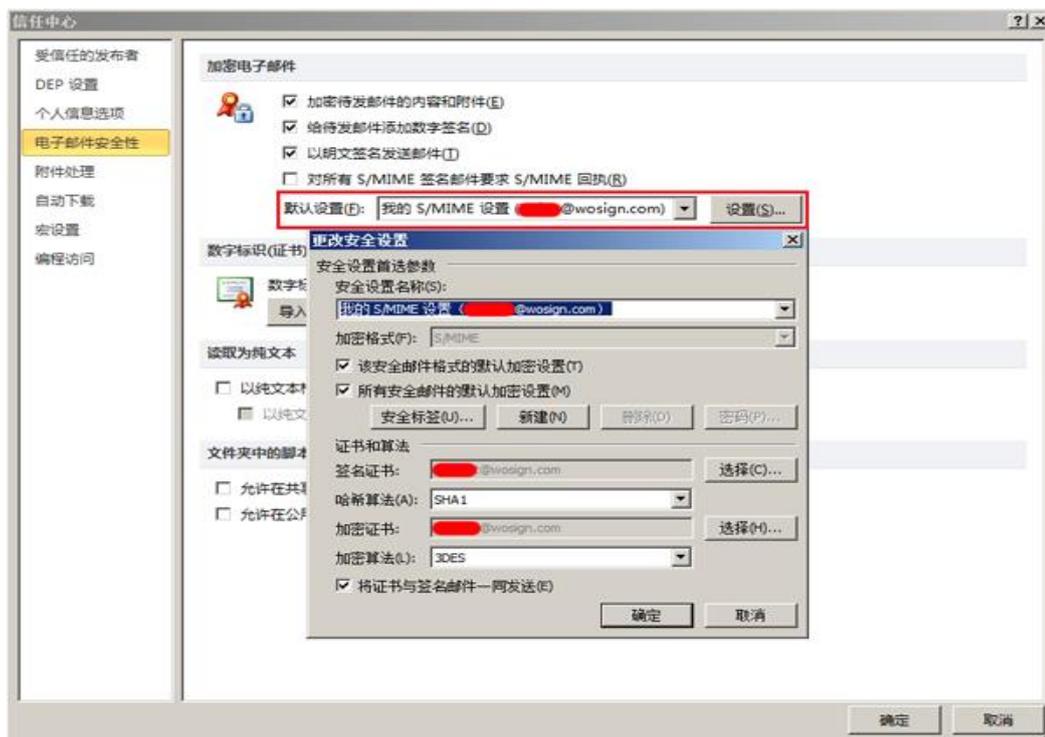
图 2

2.3 配置 Outlook 邮件客户端

在配置收发签名加密邮件之前，请确保您的 outlook 可以正常收发邮件；

2.3.1 配置 Outlook 帐号使用数字证书

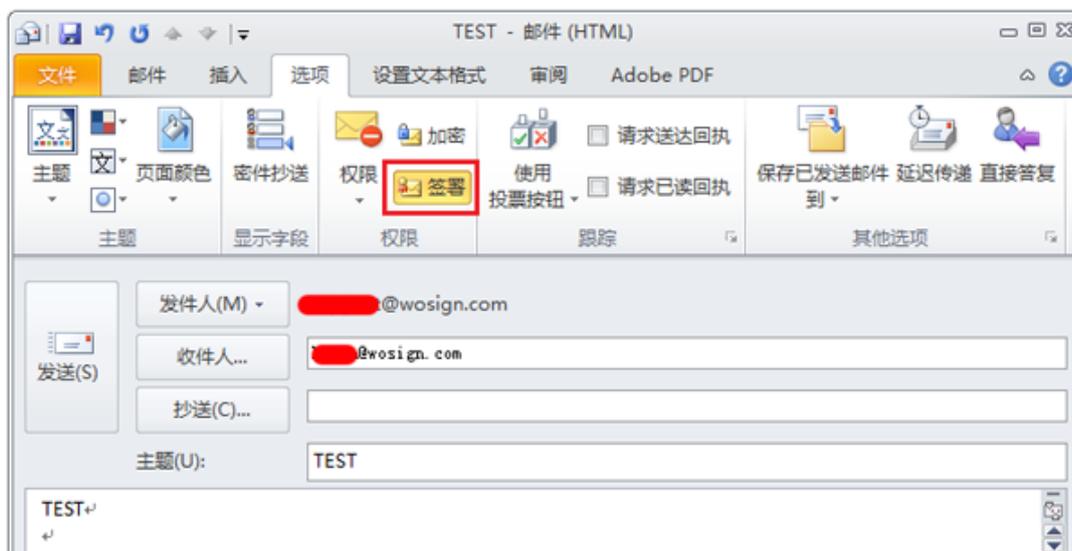
- 打开 Outlook 2010，点击“文件—选项—信任中心—信任中心设置—电子邮件安全性”
- 在加密电子邮件下面，点“设置”，出现“更改安全设置”对话框。单击“确定”接受默认值。如图下所示。



按照相同的方法为另外一个 B 帐号配置 Outlook 2010 以使用数字证书。

2.4 发送数字签名邮件

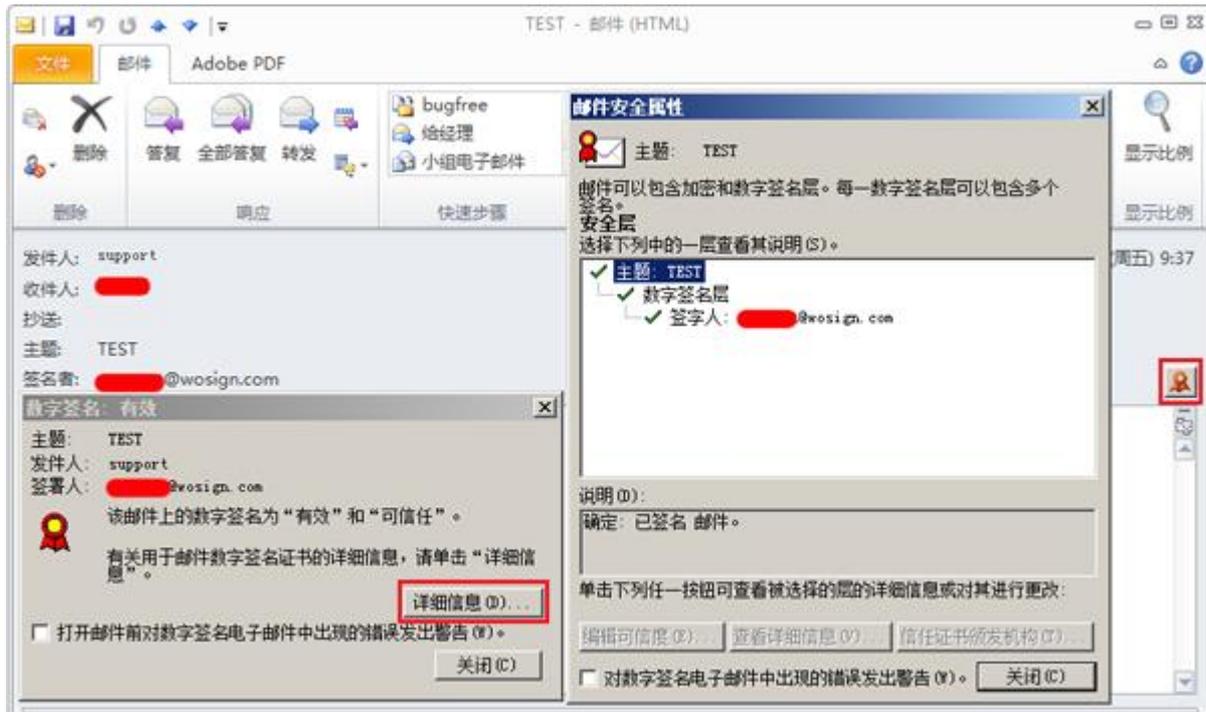
- 点“开始—新建电子邮件”，填写好收件人（B 帐号）和邮件主题，
- 点击“选项”上面的“签署”按钮，如图所示。



- 点击发送。

3. 使用 Outlook 2010 查看经过数字签名的邮件

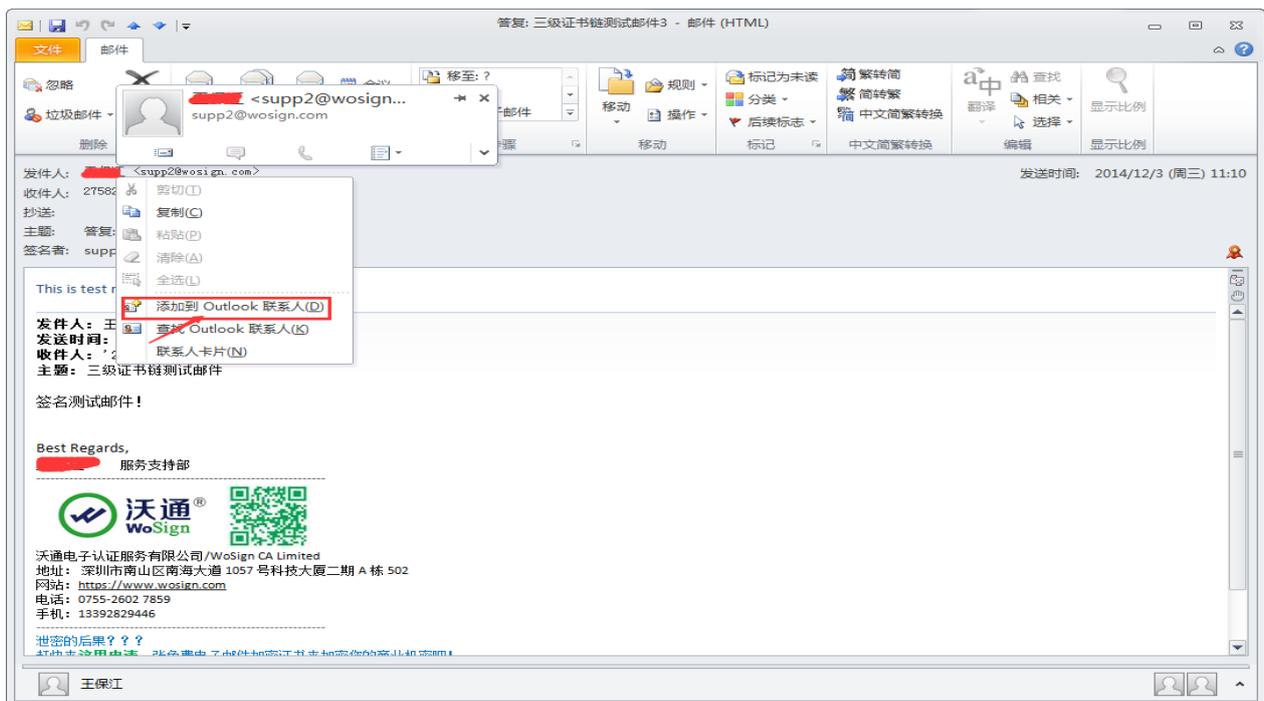
- 在 B 帐号收件箱中找到该邮件，双击该邮件，点击“验证签名”按钮，
- 单击“验证签名”右边的按钮，将显示“数字签名”对话框，指明该数字签名是有效的。如图所示。

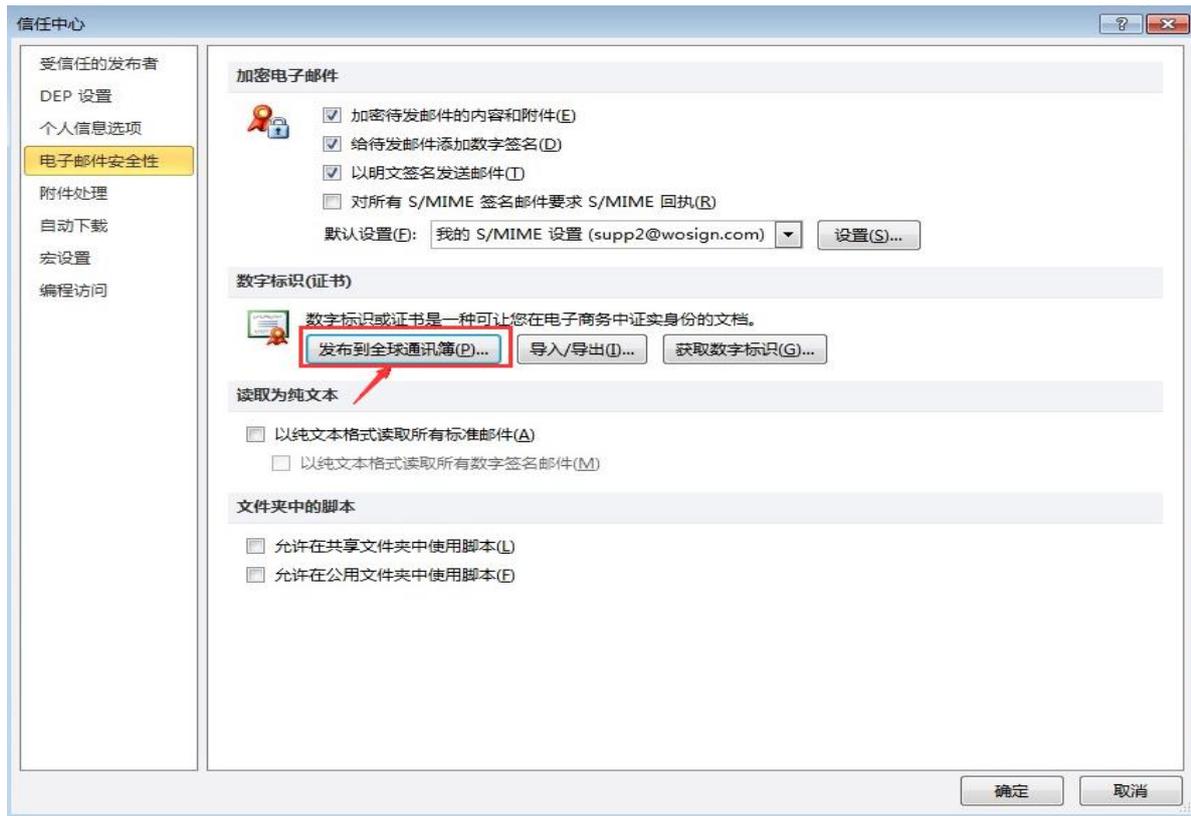


2.5 发送数字加密邮件

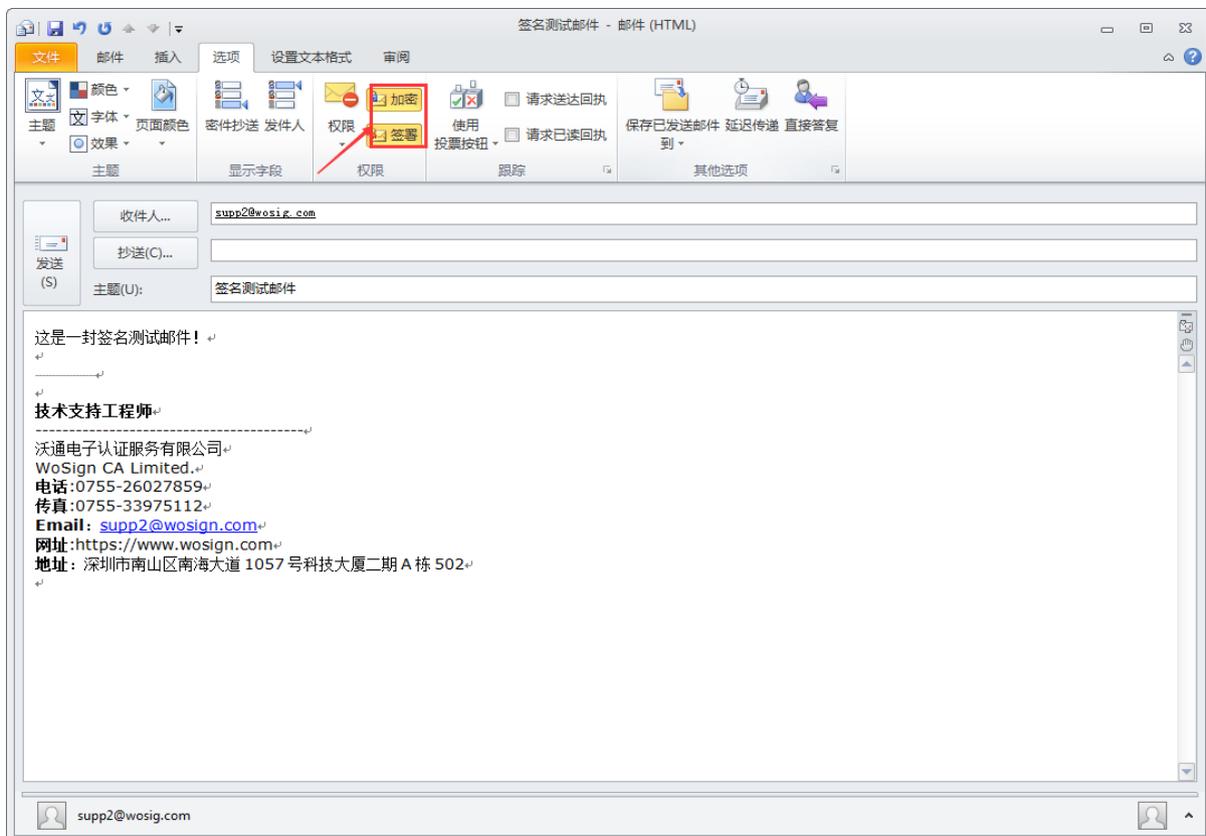
要发送加密邮件，双方邮箱都必须拥有数字证书才可以，A 要向 B 邮箱发送加密邮件必须先要获取 B 邮箱的证书公钥，可以通过以下两种方式获取：

- 保存 B 邮箱的公钥文件，右键点击发件人（B 帐号），选择添加到 Outlook 联系人；
- B 邮箱将证书发布全球通讯簿；

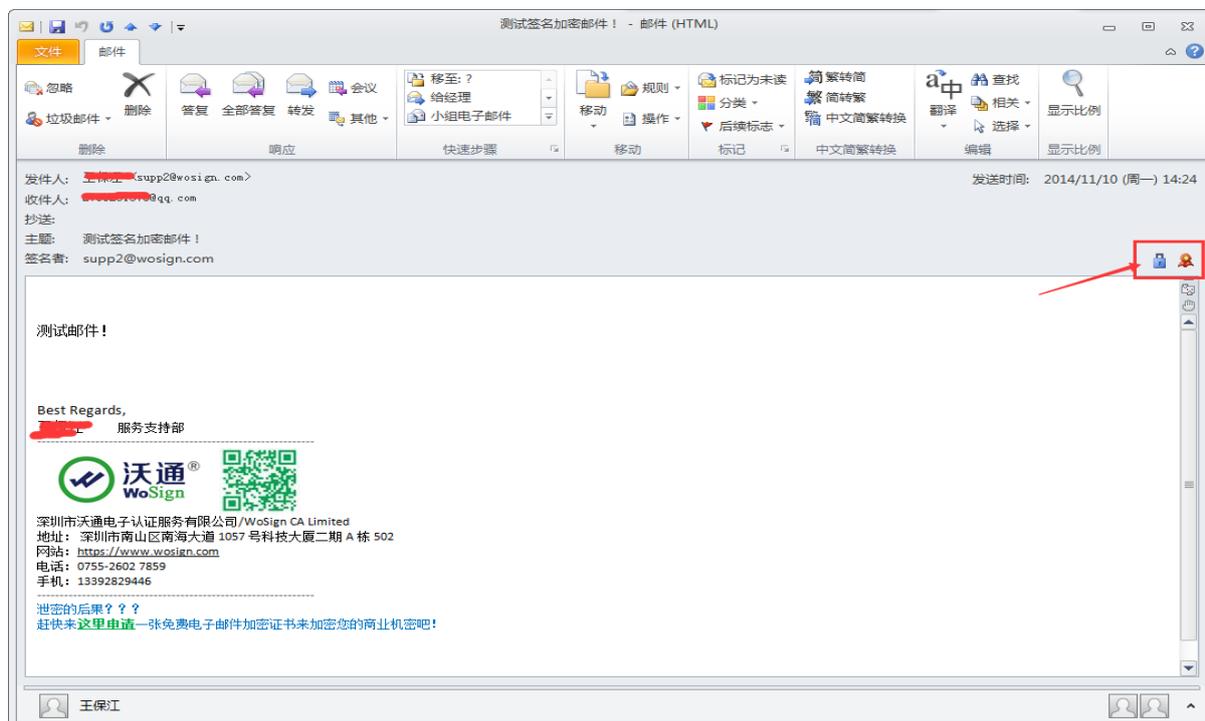




c)在 A 邮箱新建邮件—选项--签署---加密/签署—发送



在 B 帐号收件箱中找到该邮件，双击该邮件，看到签署者的右边有签名和加密的小锁标识；这样发送的邮件就是为加密邮件，只有 B 邮箱安装证书才可以查看发给他的加密邮件；



三、电子邮件签名加密证书的备份

请保存好收到的证书压缩包文件及自己生成 csr 一起的 .key 文件，以防丢失

四、电子邮件签名加密证书的恢复

重复 2.2 操作即可。