邮件证书简介

GDCA 的电子邮件加密证书已发布，可用于加密电子邮件内容和电子邮件的数字签名，可给互联网电子邮件系统带来真正的安全和便利。

一、应用特点

此免费邮件证书不仅可以用于电子邮件的数字签名和加密，而且还可以用于强身份认证，这将大大降低邮件使用客户的强身份认证技术的成本，从而快速推动基于邮件证书的强身份认证技术在邮件信息系统中的普及应用，这必将提升整个中国企业的管理信息系统的安全水平，从而增强中国企业的核心竞争力，这是 GDCA 作为一个此领域的技术领先者和市场领先者应尽的社会责任和义务。

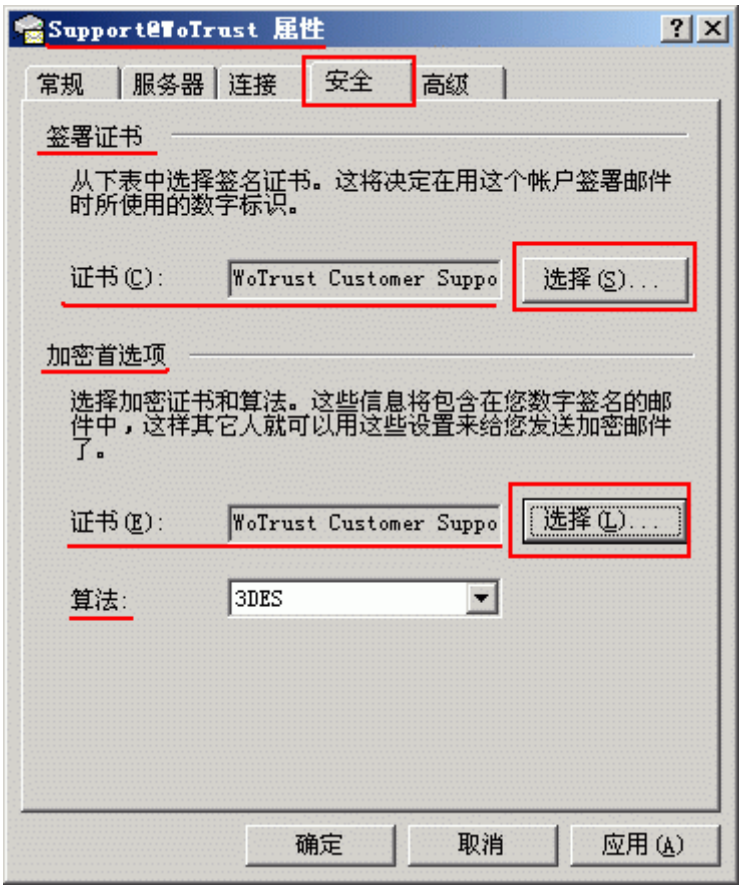
我们将免费提供基于邮件证书的强身份认证技术部署的技术咨询和技术支持，并免费提供有关 ASP 源代码，从而确保企业能快速地取消不安全的用户名/密码方式的身份认证方式，而平稳无缝地升级到更加安全的基于邮件证书的强身份认证方式。

二、应用介绍

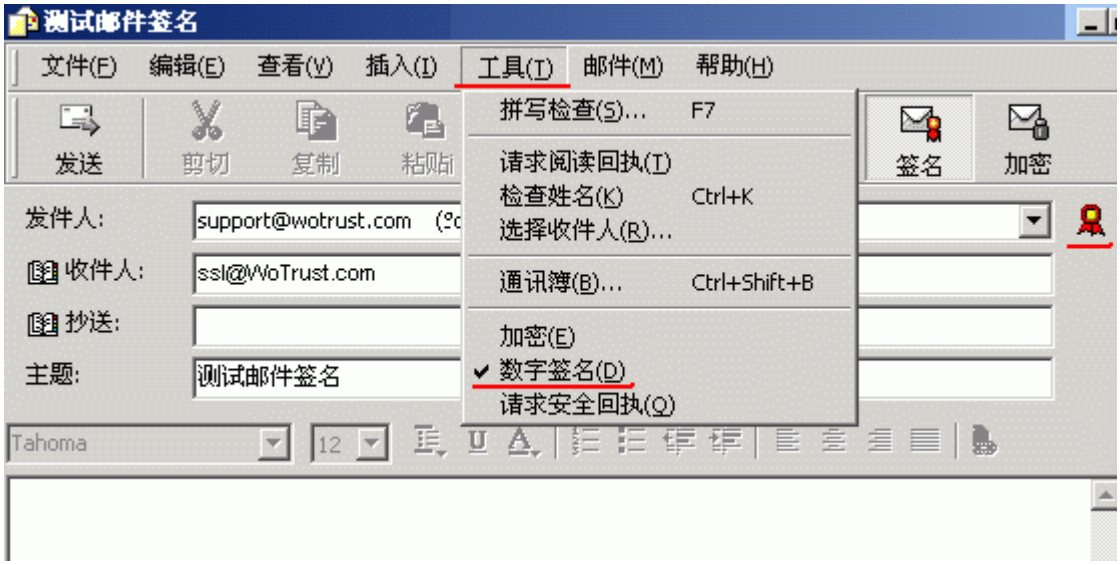
您成功申请 GDCA 邮件证书后，就可以使用该证书签名电子邮件内容和加密电子邮件。请同时参考： 安全电子邮件系统解决方案 。 本指南仅详细介绍了如何使用 Windows 自带的 Outlook Express 进行电子邮件签名和加密，如果您使用其他电子邮件客户端软件，请参考微软网站上有关指南: Outlook 2010 电子邮件数字签名指南、Outlook 2007 电子邮件数字签名指南 。

在 Outlook Express (OE) 的帮助中是这样解释的：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。更详细点讲就是：由于电子邮件发件人是可以伪造的，如果您希望对方确信此邮件确实是您发出的，则一定要使用您的个人证书签名此邮件。

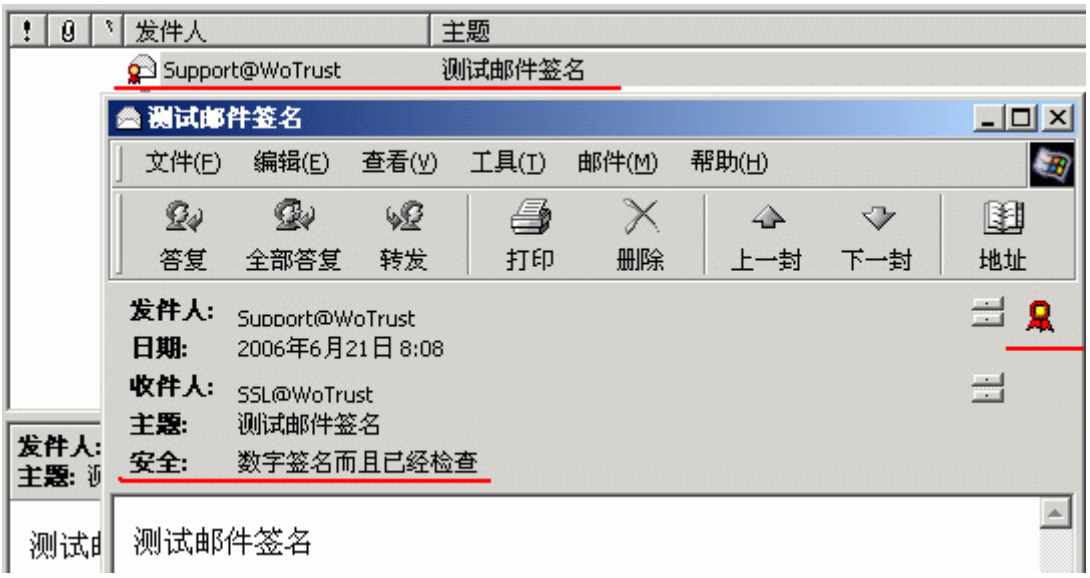
(1) 在 Outllok Express 的“工具” - “帐号”中选中需要签名的电子邮件帐号，点击“属性” - “安全”，如图 1 所示，点击第 1 个“选择”从 Windows 证书存储区选择签名证书，点击第 2 个“选择”从 Windows 证书存储区选择加密证书，可以是同一个证书，也可以是不同的证书，您还可以选择不同的加密算法。



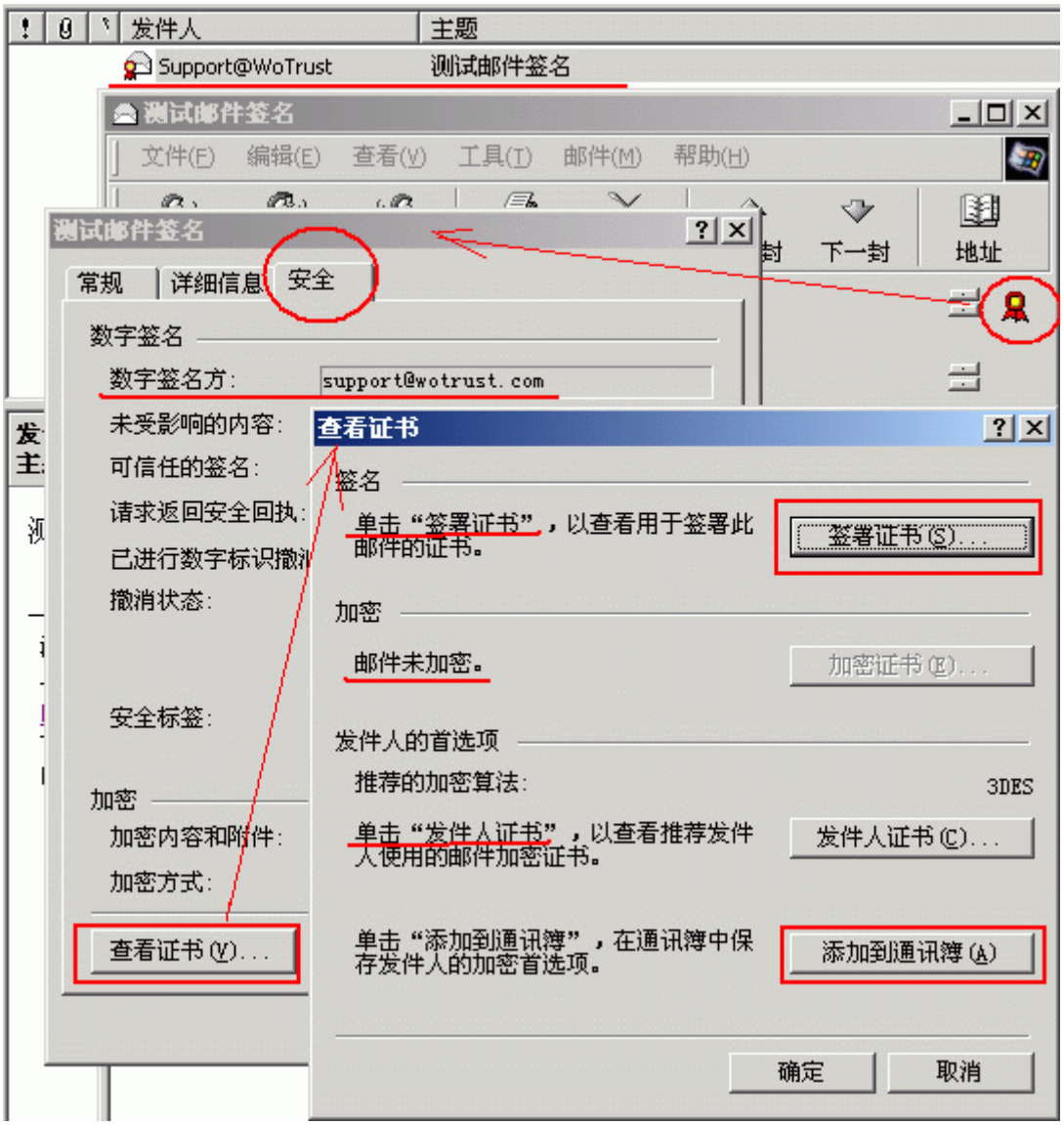
(2) 个人证书设置成功后，就可以签名电子邮件了。如下图 2 所示，测试邮件签名是从 support 帐号发签名邮件给 ssl ，创建邮件后，只要在“工具”中点击“数字签名”即可，会显示一个勾号。如果您已经把签名功能按钮设置到功能按钮栏，则直接点击“签名”按钮即可。在发件人的后面会显示一个红色的证书图标，点击“发送”即可：



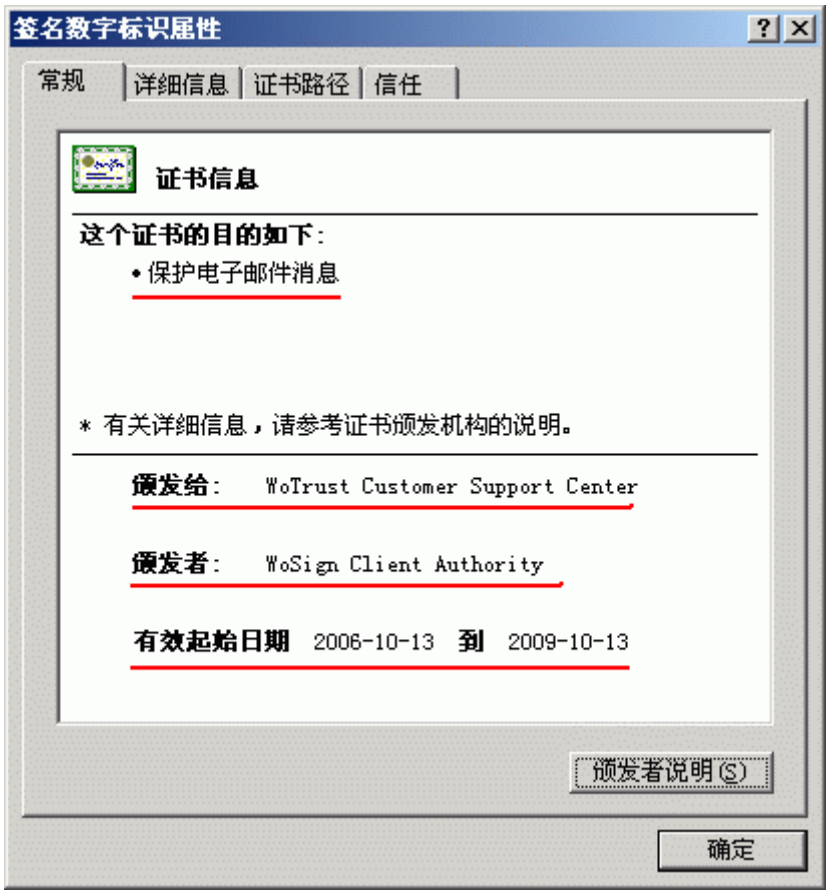
(3) 如下图 3 所示，收件人 (SSL) 收到签名邮件后， Outlook Express 会提示您已经收到一个一个签名邮件， OE 会自动验证签名是否有问题、签名证书是否有效和是否由 Windows 中受信任的根证书颁发机构颁发、邮件是否被篡改等，如果没有问题，就会显示此邮件已经“数字签名并且已经通过检查”，表明没有任何问题：



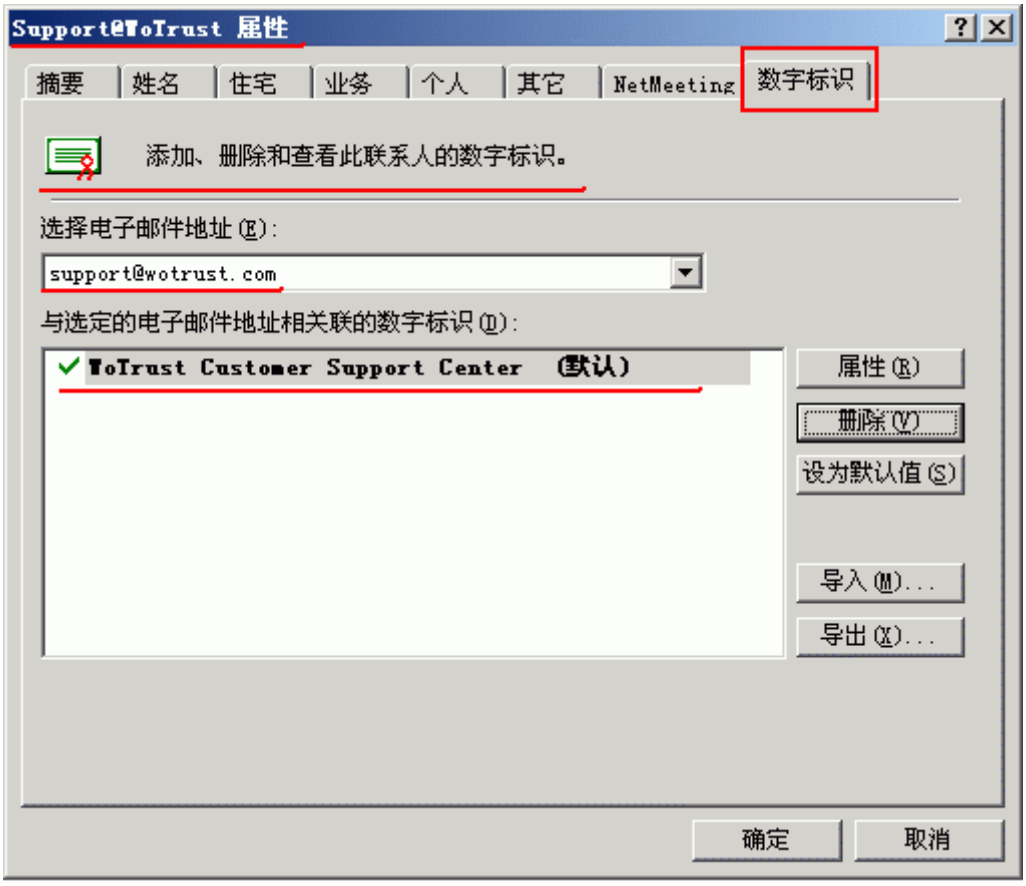
(4) 如下图 4 所示，在发件人的后面会显示一个红色的证书图标，点击证书图标后，就会显示详细的证书信息，包括数字签名方邮件帐号，邮件内容是否被篡改，该证书是否被吊销(撤消)等：



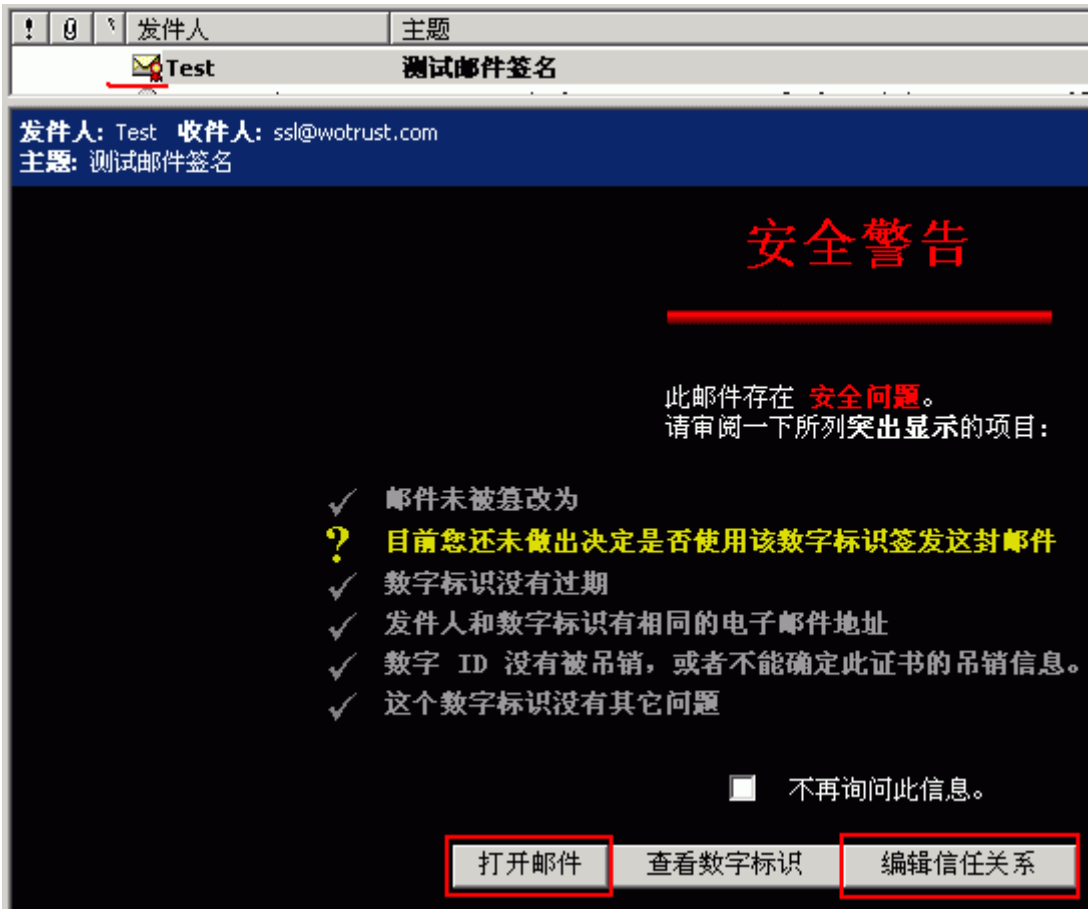
(5) 点击“查看证书”，再点击“签署证书”就可以查看证书的详细信息，如下图 5 所示为 WoTrust 单位证书：



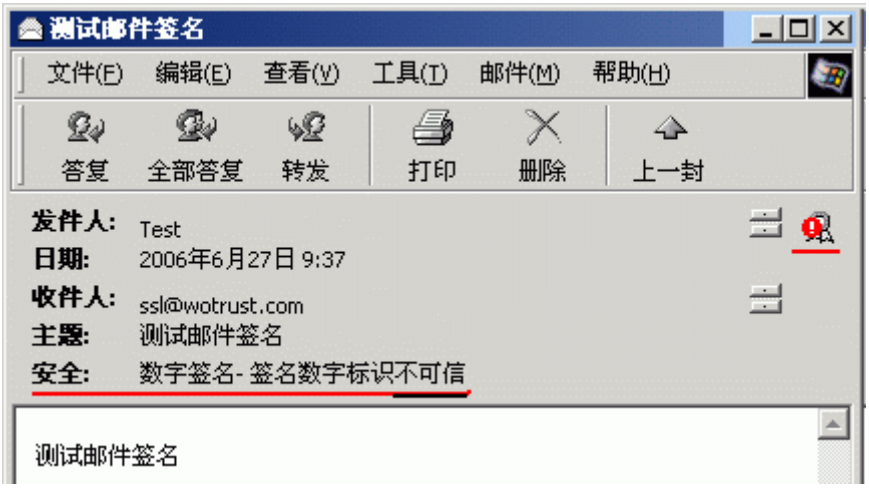
(6) 点击“添加到通讯簿”，就可以把此发件人添加到 Outlook Express 的通讯簿中，如下图 6 所示，您可以编辑姓名等信息，其中“数字标识”就是发件人的单位数字证书，只有把发件人和其对应的个人证书添加到通讯簿才可以回复发件人签名邮件和加密邮件。



(7) 最后，请用户注意：一定要使用全球通用的客户端数字证书来实现电子邮件的数字签名和加密，也就是说：颁发个人证书的根证书一定要是 Windows 受信任的根证书颁发机构中已经列出的证书颁发机构，如果不是，如下图 7 所示， Outlook Express 会提示“此邮件存在 安全问题 ”，主要颁发证书的根证书不是 Windows 所信任的根证书，当然，您可以点击“编辑信任关系”而信任该证书，信任后就不会出现此警告信息：



(8) 如下图 8 所示，如果点击“打开邮件”，则会显示“数字签名标识不可信”，同时在发件人的右边的证书图标是灰色的带一红色感叹号：



请注意：电子邮件数字签名后如果邮件没有在发送过程中被篡改，则显示此邮件已经“数字签名并且已经通过检查”，但如果邮件被篡改，则会提示“邮件

已被篡改”，如下图 9 所示。可能是在发送邮路上被无意篡改或有意篡改。由此可见，电子邮件的数字签名是多么重要，而没有签名的邮件即使被非法篡改，您也是不会直到，因为没有数字签名的邮件没有是否被篡改的验证机制。