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。

| 😪 Suppor t@ToT | 'rust 雇性 | ? × |
|------------------------|----------------------------------|--------------------|
| 常规 服务器 | 连接 安全 高级 | |
| 签署证书 — | | |
| 从下表中选排 时所使用的数 | 释签名证书。这将决定在用这个 数字标识。 | ▶●帐户签署邮件 |
| 证书(C): | WoTrust Customer Suppo | 选择(5) |
| 加密首选项 - | | |
| 选择加密证书 件中,这样却 了。 | 的和算法。这些信息将包含在悠 其它人就可以用这些设置来给悠 | 密数字签名的邮 密发送加密邮件 |
| 证书(图): | WoTrust Customer Suppo | [选择①] |
| 算法: | 3DES 💌 | |
| | | |
| | | |
| | | |
| | | 应用(A) |







(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:

| 💼 测试邮件 | ' 签名 | | | | | | | | | |
|---------|-----------------|------------|------------|-----------|------------|-----------------------|--------------|-------|----|---|
| 」 文件(E) | 编辑(E) | 查看(⊻) | 插入(I) | 工具 | (I). | 邮件(M) | 帮助(H) | | | |
| | X | P | 2 | 拼 | 写检 | 查(<u>5</u>) | F7 | | | |
| 发送 | 剪切 | 复制 | 粘贴 | 请 | 求阅 | 读回执(<u>T</u>) | | 签名 | 加密 | |
| 发件人: | supp | ort@wotru: | st.com (?c | 检选 | ·查姓: 择收 | 名(<u>K)</u> 件人(R) | Ctrl+K | | - | 8 |
| 1 收件人 | : ssl@ | WoTrust.co | om | 通 | (讯簿) | (<u>B</u>) | Ctrl+Shift+B | | | |
| 11 抄送: | | | | 加 | 密(E) | | | | | |
| 主题: | 测试 | 邮件签名 | | <u>✓数</u> | 字签 | 名(D) | | | | |
| Tahoma | | 12 | • E, | | | 王叫玖(Q) E E E E | | . ⊴ ■ | 6 | |
| | | | | | | | | | | |
| | | | | | | | | | | |

(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:





| ! 0 | * 发件人 | | É | É题 | | | | |
|-------|-------------|-----------------------|---------------------|----------|----------------|----------------|-----|----------------|
| | 👷 Suppor | rt@WoTrust | 钡 | 则试邮件签 | 名 | | | |
| | 🙈 测试邮 | 件签名 | | | | | | |
| | 」 文件(E) | 编辑(<u>E</u>) | 查看(⊻) | 工具(I) | 邮件(<u>M</u>) | 帮助(<u>H</u>) | | 3 |
| | 24 | <u>G</u> v | 42 | | X | 4 | <₽ | |
| | 答复 | 全部答复 | 转发 | 打印 | 删除 | 上一封 | 下一封 | 地址 |
| | 发件人: 日期: | Support@W 2006年6月: | /oTrust 21日 8:08 | | | | | ≓ & |
| 发件人: | 收件人: 主题: | SSL@WoTru 测试邮件釜 | ust ž名 | <u>.</u> | | | | ÷. |
| 主题: 1 | <u>安全</u> : | 数字签名向 | 1 且已经检 | <u>查</u> | | | | |
| 测试的 | 测试邮 | 件签名 | | | | | | |

(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:





| ! 0 \ 发件人 | | |
|----------------|------------------------------|---------------|
| 👷 Support@WoTr | rust 测试邮件签名 | |
| ▲ 测试邮件签名 | | - 🗆 × |
| 」 文件(E) 编辑(E | E) 查看(V) 工具(I) 邮件(M) 帮助(H) | <u></u> |
| 测试邮件签名 | | |
| 常规 详细信息 安 | | |
| 数字签名 | | |
| 数字签名方: | support@wotrust.com | = |
| 发 未受影响的内容: | 查看证书 | <u>? ×</u> |
| 主: 可信任的签名: | A#2 | |
| 请求返回安全回执: | :/「单击"签署证书",以查看用于签署此 | TTTC: |
| 已进行数字标识撤; | ,邮件的证书。 | <u>近节夏)</u>] |
| 撤消状态: / | 加密 | |
| 1 | 邮件未加密。 | 正书(2) |
| ! 安全标签: | 发件人的首选项 | |
| 1 tus: | 推荐的加密算法: | 3DES . |
| 加密内容和附件: | 单击"发性人证书",以查看推荐发件 发件人 | 证书(C) |
| 加密方式: | 人使用的邮件加密证书。 ———— | |
| 查看证书(火) | 单击"添加到通讯簿",在通讯簿中保存发件人的加密首选项。 | 到通讯簿(A) |
| | | 取消 |

(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:





| 签名数字标识属性 | <u>? ×</u> |
|-------------------------------------------------|------------|
| 常规 详细信息 证书路径 信任 | |
| □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ | |
| 这个证书的目的如下 : 保护电子邮件消息 | |
| * 有关详细信息,诸参考证书颁发机构的说明。 | _ |
| 褒发者 : WoSign Client Authority | |
| 有效起始日期 2006-10-13 到 2009-10-13 | |
| | |
| | ŧ |

(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。





| Support@ToTrust 雇性?× |
|-----------------------------------------------|
| 摘要 姓名 住宅 业务 个人 其它 NetMeeting 数字标识 |
| □ 添加、删除和查看此联系人的数字标识。 |
| 选择电子邮件地址 (2): |
| support@wotrust.com |
| 与选定的电子邮件地址相关联的数字标识(2): |
| ✓ ToTrust Customer Support Center (武认) 屈性 (E) |
| |
| |
| |
| |
| |
| 导出 (红) |
| |
| |
| |
| |
| |

(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:





| ! 0 \ 发件人 | 主题 | | |
|--------------------------------------------------------------|---------------------------------------|-------------------------------|-------------------------------------------|
| Test | 测试邮件签名 | | |
| 发件人: Test 收件人: ssl@wotrus 主题: 测试邮件签名 | t.com | | |
| | | 安全 | 警告 |
| | | 此邮件存在 安 请审阅一下所列 | 全 <mark>问题</mark> 。 突出显示 的项目: |
| ? | 邮件未被篡改为 目前您还未做出决定 教字标识没有过期 | 是否使用该数字体 | 际识签发这 封邮件 |
| | 发件人和数字标识有 数字 ID 没有被吊销 这个数字标识没有其 | 相同的电子邮件」 新,或者不能确定 它问题 | 电址 此证书的吊销信息。 |
| | | ■ 不再 | 询问此信息。 |
| | 打开邮件 | 查看数字标识 | 编辑信任关系 |

(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:

| 🚔 测试邮 | 件签名 | | | | | |
|-----------------------------------|--------------------------------------------------|----------------------------------|---------------------|-------|---------|-------------------|
|] 文件(E) | 编辑(E) | 查看(⊻) | 工具(I) | 邮件(Ϻ) | 帮助(出) | |
| 公司 公司 | 2 2) 全部答复 | ₩2 转发 | 日 一 打印 | × | 上→封 | |
| 发件人: 日期: 收件人: 主题: 安全: | Test 2006年6月: ssl@wotrus 测试邮件鉴 数字签名- | 27日 9:37 t.com 逐名 签名数字标 | 示识不可信 | | | 11 <u>8</u> 11 |
| 测试邮件 | ·签名 | | | | | |

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。



