如何保证数据在传输中的安全？

深圳市沃通电子商务服务有限公司
www.wosign.com

议　题

- 数字证书在信息安全领域的重要作用
- 数字证书简介(3大类)
- SSL证书在国外和国内的部署情况
- SSL证书如何保证数据的传输安全
- 部署SSL证书应该注意哪些重要问题
- 数字证书的其他应用
- WoSign品牌产品简介

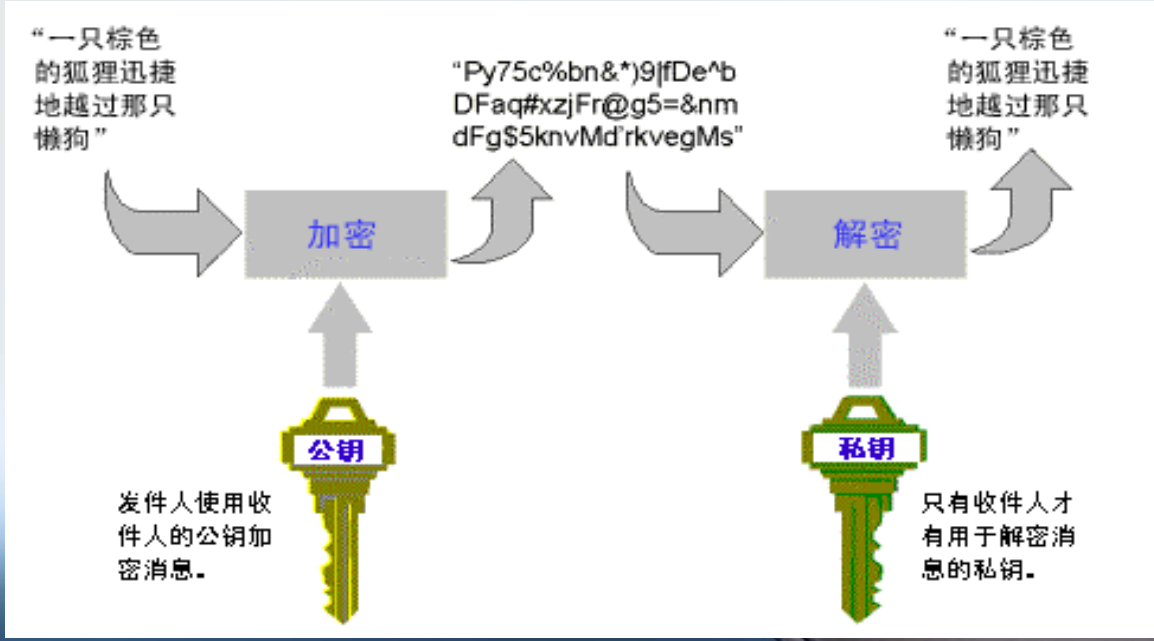
数字证书在信息安全领域的重要作用

- 数字证书主要作用：加密和身份认证
- 信息安全领域的最重要部分也是加密和身份认证
- 加密：确保机密信息在网络传输过程中不会被非法窃取和非法篡改；
- 身份认证：确保所声称的身份的真实性，确保真实的身份有权访问应该能访问的资源。

数字证书如何发挥其重要作用？ **Next**

数字证书简介

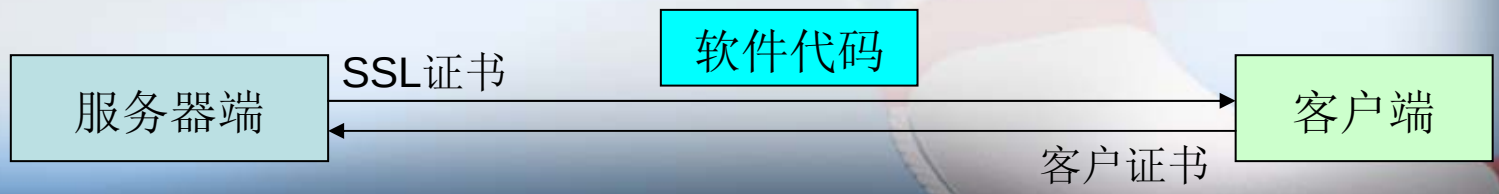
- PKI (Public Key Infrastructure，公钥基础设施)
  参考：http://www.wosign.com/Basic/aboutPKI.htm
- 数字证书(公钥和私钥，加密算法和摘要算法)、证书颁发机构(CA)、证书链(受信任的根证书颁发机构 - 中级根证书颁发机构 - 用户证书)、证书管理(颁发、吊销、重新颁发、续期)
- 数字证书主要用途：加密与解密、身份验证与数字签名



数字证书简介

主要有三大类：

- **SSL证书**(服务器端): (1) 确保从用户浏览器到服务器之间传输的信息自动加密，防止非法篡改和非法窃取; (2) 确保服务器的真实身份。
- **代码签名证书**：(1) 确保软件代码在通过互联网或移动互联网发布时不会被非法篡改; (2) 让用户确信此代码的真实来源。
- **客户端证书**：(1) 电子邮件的数字签名与加密，确保电子邮件信息的自动加密，防止非法篡改和非法窃取; (2) 确保客户端的真实身份，用于强身份认证和数字签名。(3) PDF文件的数字签名与加密



数字证书简介—SSL证书

- 什么是 SSL 证书？

  SSL 证书就是遵守 SSL 安全套接层协议的服务器数字证书。SSL 安全协议最初是由美国网景(NetScape)公司设计开发的，全称为：安全套接层协议 (Secure Sockets Layer)， 它指定了在应用程序协议 (如 HTTP 、 Telnet 、 FTP) 和 TCP/IP 之间提供数据安全性分层的机制，它是在传输通信协议 (TCP/IP) 上实现的一种安全协议，采用公钥技术，它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。由于此协议很好地解决了互联网明文传输的不安全问题，很快得到了业界的支持，并已经成为国际标准。
- SSL 证书由浏览器中“受信任的根证书颁发机构”在验证服务器身份后颁发，具有网站身份认证和信息加密传输的双重功能。
- 所有流行的浏览器和服务器软件都支持SSL证书的信息加密传输功能，用户无需编程，也无需修改现有网页和系统，只需把http://访问改为https://访问即可，非常简单！

数字证书简介—SSL证书主要用途

(1) 确保用户输入的登录密码能从用户电脑自动加密传输到服务器，从而大大降低了用户密码被盗的可能性。有关统计表明：在用户登录页面部署SSL证书后，可以降低80%的由于用户密码问题的带来的客户服务工作量，这将为服务提供商大大降低客服成本；

(2) 确保用户安全登录后在线提交个人机密信息以及公司机密信息和浏览其机密信息时能从用户电脑到网站服务器之间能自动加密传输，防止非法窃取和非法篡改；

(3) 让在线用户能在线查询网站服务器的真实身份，防止被假冒网站所欺诈。如假冒银行网站，用户只要查看SSL证书中的主题信息的O字段就能了解此网站并不是真正的银行网站；而被列入黑名单的欺诈网站，IE7浏览器能实时帮助用户识别；

(4) 让在线用户放心，这点对于电子商务网站非常重要，因为部署了SSL证书，一方面表明服务提供商是采取了可靠的技术措施来保证用户的机密信息安全，另一方面，也就是更重要的是，可以让用户了解到此网站的真实身份已经通过权威的第三方认证，网站身份是真实的，是现实世界合法存在的企业，只有这样，才能让用户放心；

(5) 法律法规遵从：部署SSL证书就等于该网站已经按照有关法律法规要求而采取了可靠的技术措施，这对于企业的健康发展非常重要。

SSL证书在国外和国内的部署情况

- 国外部署情况

SSL证书从诞生到现在已经有15年的历史，由于SSL证书能高效地加密网上机密信息，所以自推出以来就在欧美获得了大量部署，因为欧美各国早就有相应的个人隐私保护法律法规(当然包括网上信息隐私保护)，这就不难理解为何**几乎100%**美国政府网站、电子商务网站和著名的免费电子邮件服务提供商等等，凡是有需要用户登录的地方，**都**部署了 SSL证书，从而保护了用户在线输入个人机密信息和在线管理个人机密信息的安全，确保从用户浏览器到服务器之间的所有信息是高强度加密传输的。之所以都有 SSL 证书，就是美国相关法律所要求的。从技术上讲， **只有**系统部署了 SSL 证书才能保证机密信息的安全，这是**唯一的、非常成熟的**解决方案。

- 国内部署情况

几乎100%都没有部署！

SSL证书在国外和国内的部署情况

- 国外部署情况

  几乎**100%**部署

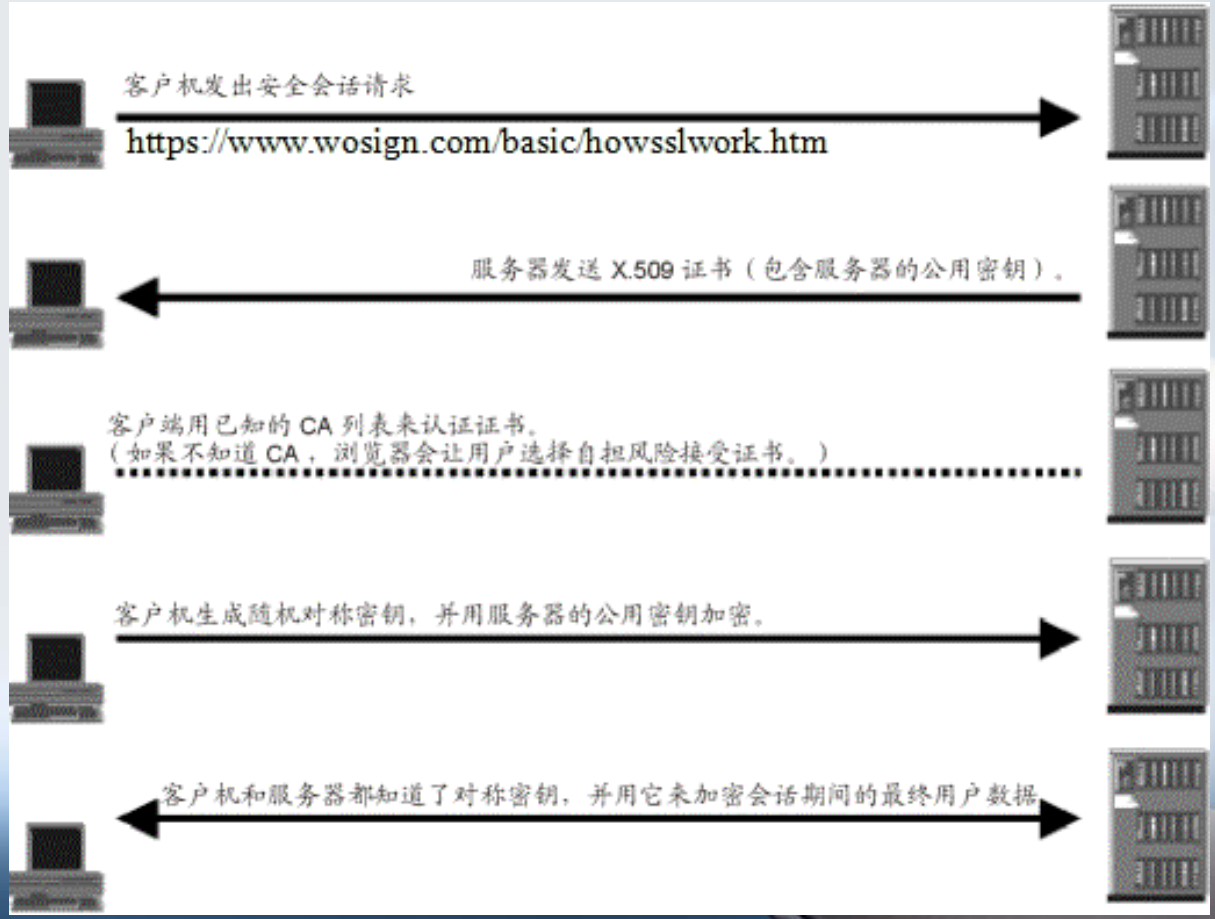
- 国内部署情况

反观我国，SSL证书的应用情况却糟糕得多，我国各种电子政务网站和电子商务网站，**几乎100%** 都没有部署SSL证书，也就是说，网站根本没有采取有效的技术手段来加密用户机密信息安全，如个人手机号码、家庭地址等，其中重要的原因之一是中国相关法律的严重缺失。因此，希望中国的有关部门能尽快立法来保护广大网民的网络隐私权。

特别值得关注的是：国内许多在美国上市的公司的网站和系统也没有部署 SSL 证书，这已经触犯了美国有关法律，可能随时会遭到检控，希望这些公司的CIO/CSO们能尽快部署 SSL 证书，以免因小小失误而影响了公司的美好发展前程。

SSL证书如何保证数据的传输安全

- 互联网是明文传输的，要保证机密信息的传输安全，必须部署SSL证书来加密传输机密信息。参考：https://www.wosign.com/Basic/howsslwork.htm



SSL证书如何保证数据的传输安全

- **SSL证书解决了哪两个信息安全问题？**

  (1) 互联网的匿名问题：互联网的匿名性对于网上购物和电子商务来讲是危险的，因为您不能也不应该相信所访问的网站就是所称的某某公司(某某品牌)就是您心目中现实世界的某某公司(某某品牌)；

  (2) 互联网的明文传输问题：互联网所使用的 IP 技术就是明文传输所有信息，这样，就使得您在网站上提交的所有机密信息如果不采用任何加密措施的话，就很有可能其他任何人都能看到，因为从您的电脑到网站服务器要经过许多路由，有许多人都能接触到传输路由，都有可能非法截获甚至篡改您的机密交易信息(特别是银行卡信息)。

  以上两个安全问题就需要SSL证书来解决，具体体现在浏览器的地址栏上就是使用https://来访问，而不是常用的http://访问。https 就是安全的 http 连接， s 就是 secure ，也就是说：如果您正在浏览的页面的浏览器地址栏的网址前面是 https:// 的话，就表明您在此网站上输入的任何信息都是从你的电脑上自动加密传输到网站服务器的。只要这样，才能保证您在网站上提交的机密信息不会被非法截获或非法篡改。否则，为了您的机密信息安全，千万不要提交机密信息。

SSL证书如何保证数据的传输安全

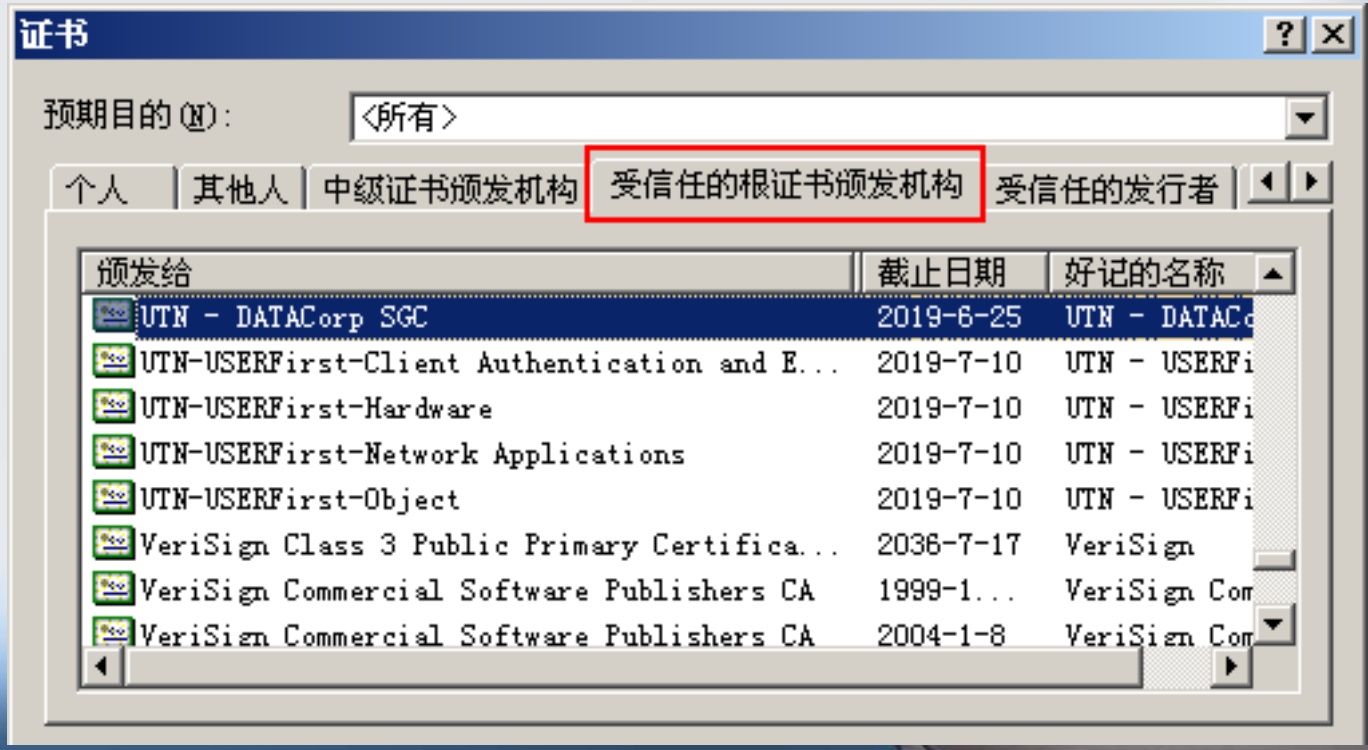
- **SSL证书是什么样的？**

  为了方便互联网用户能醒目地识别出网站是否部署了SSL证书 (用户往往不留意是使用 http:// 还是使用 https://)，所有浏览器就做了一个明显的安全锁标志，以 IE 浏览器为例，左图为 IE 6 版本浏览器的安全锁标志，是显示在状态栏的右下角，鼠标放在安全锁上面会显示目前采用的加密强度(如图为128 位加密长度)；而右图为 IE 7 版本浏览器的安全锁标志，是显示在地址栏的右边，将大大方便用户查看。

SSL证书如何保证数据的传输安全

- 如何识别不同类型的SSL证书？

正常显示安全锁标志的前提是此SSL证书必须是浏览器中“受信任的根证书颁发机构” 所颁发，您可以在IE浏览器的“工具”-“Internet选项”-“内容”-“证书”，就能看到“受信任的根证书颁发机构”：

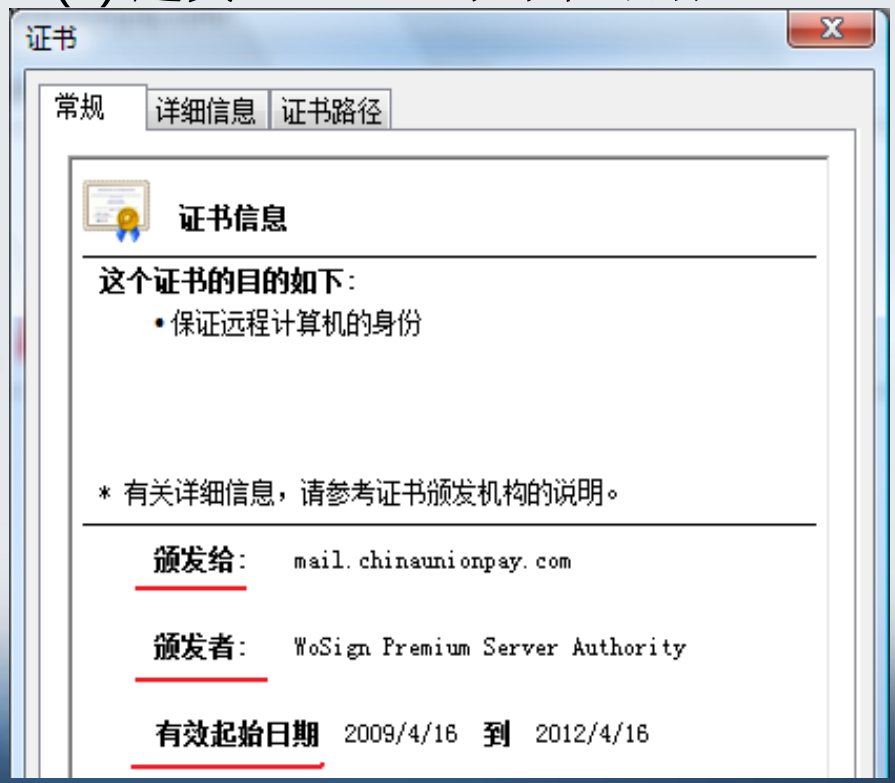


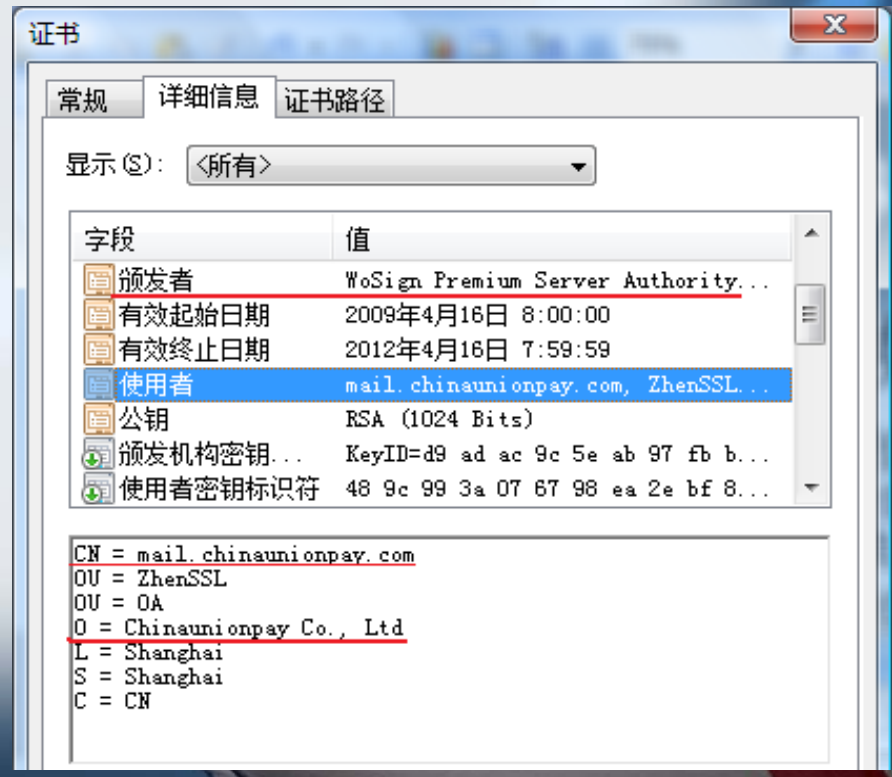
SSL证书如何保证数据的传输安全

- 如何识别不同类型的SSL证书？

  虽然由浏览器中“受信任的根证书颁发机构”所颁发的SSL证书都会显示安全锁标志，但不同类型的SSL证书的作用和性能是不一样，主要分4种：

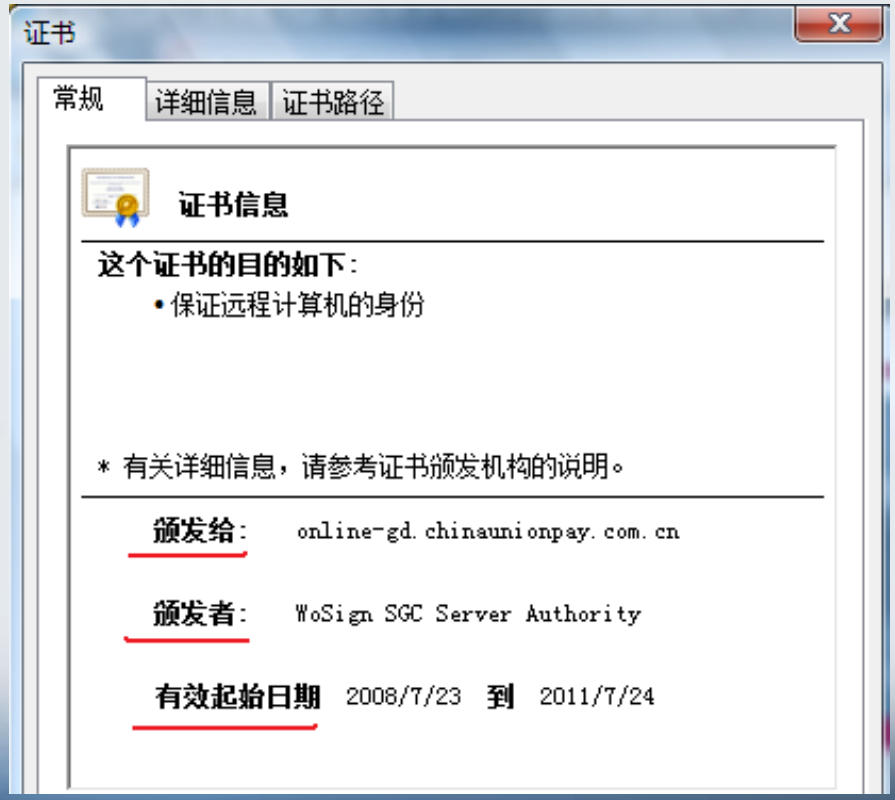
  (1) 超真SSL：显示单位名称，40/56/128/256位自适应加密强度；

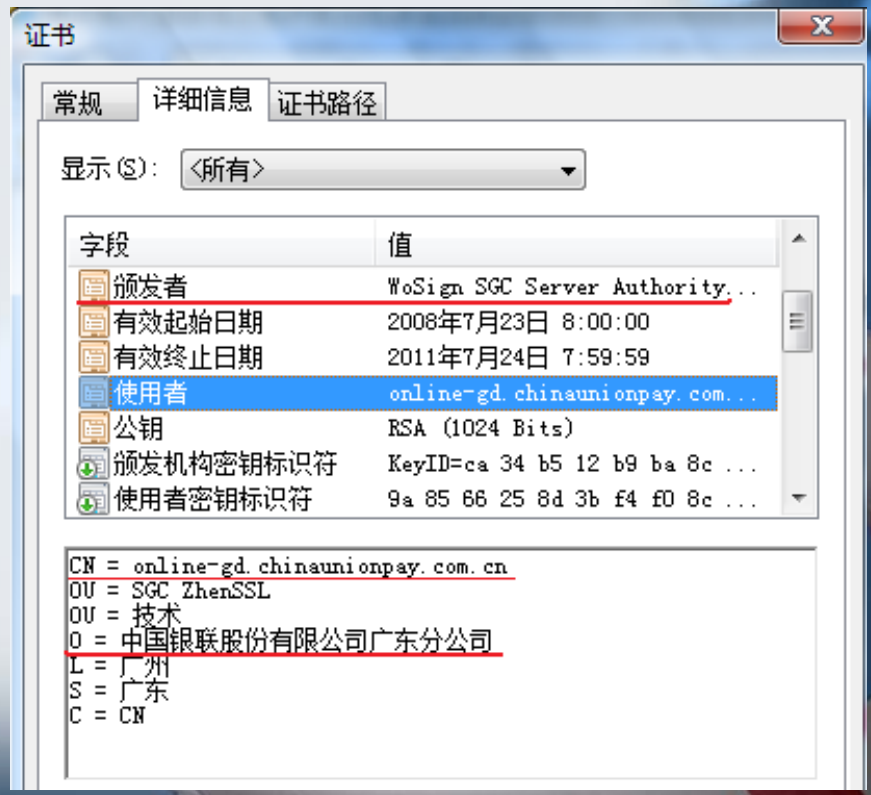




SSL证书如何保证数据的传输安全

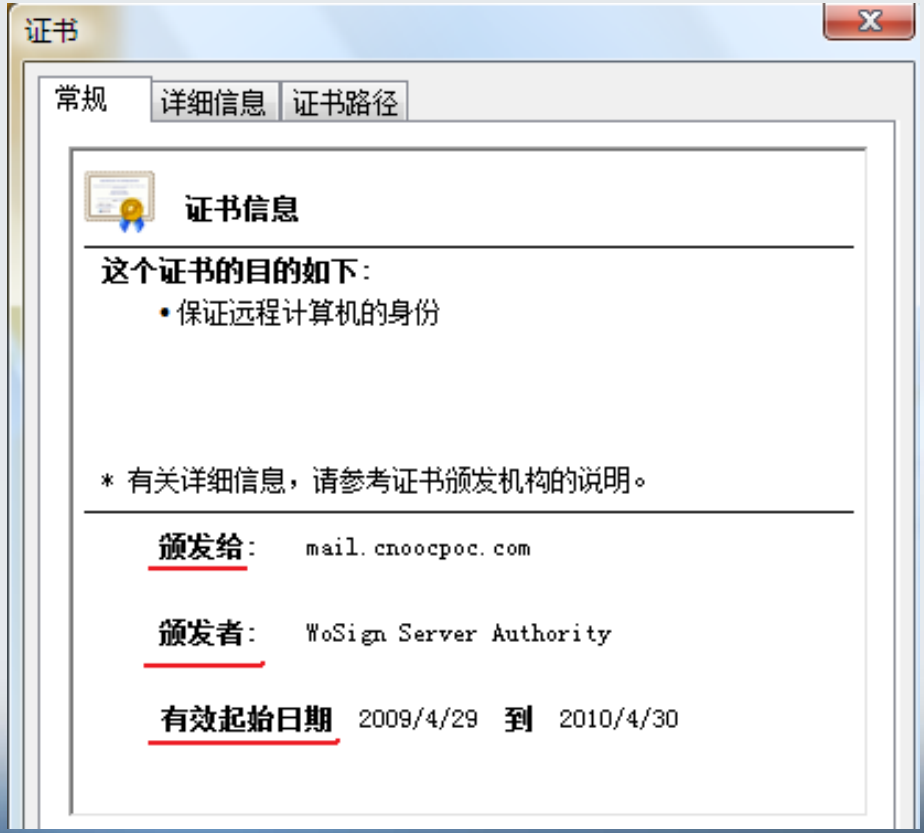
- 如何识别不同类型的**SSL**证书？
  (2) **SGC超真SSL**：显示单位名称，强制128位加密强度(128/256位)，确保不同版本浏览器都能强制实现128位加密。

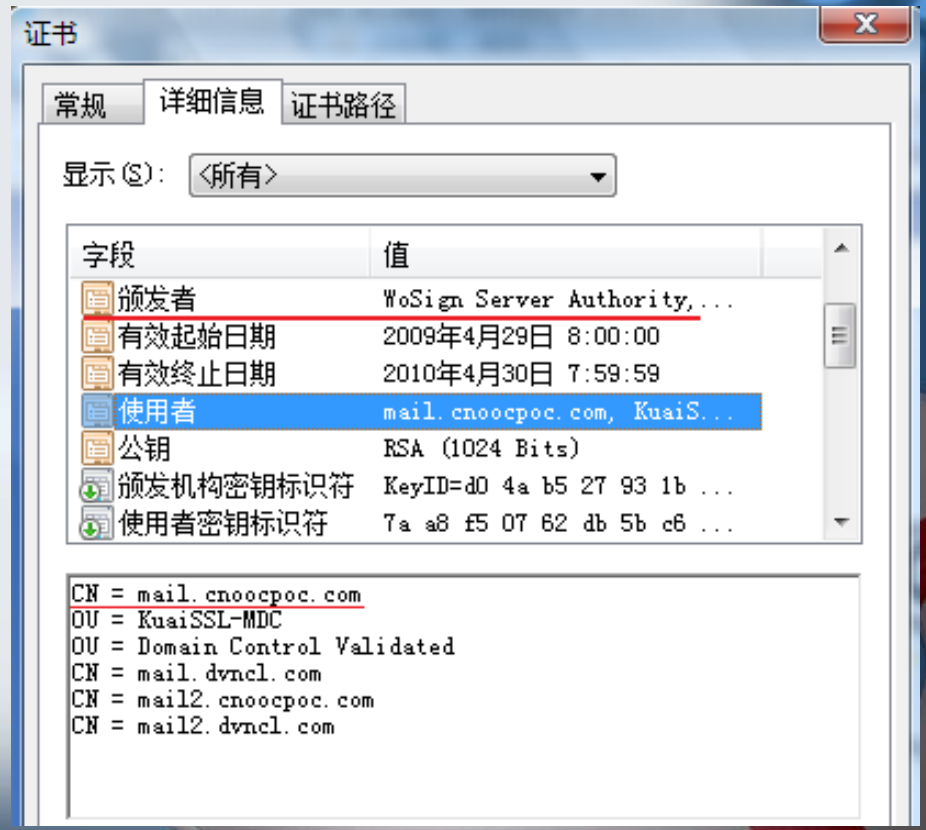




SSL证书如何保证数据的传输安全

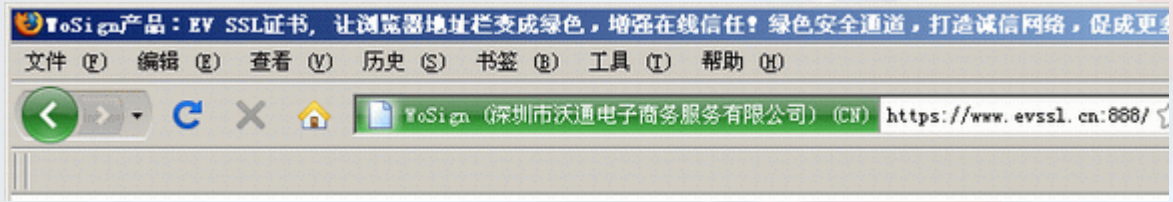
- 如何识别不同类型的**SSL**证书？
  (3) 超快**SSL**：不显示单位名称，只验证域名所有权，自适应加密强度；





SSL证书如何保证数据的传输安全

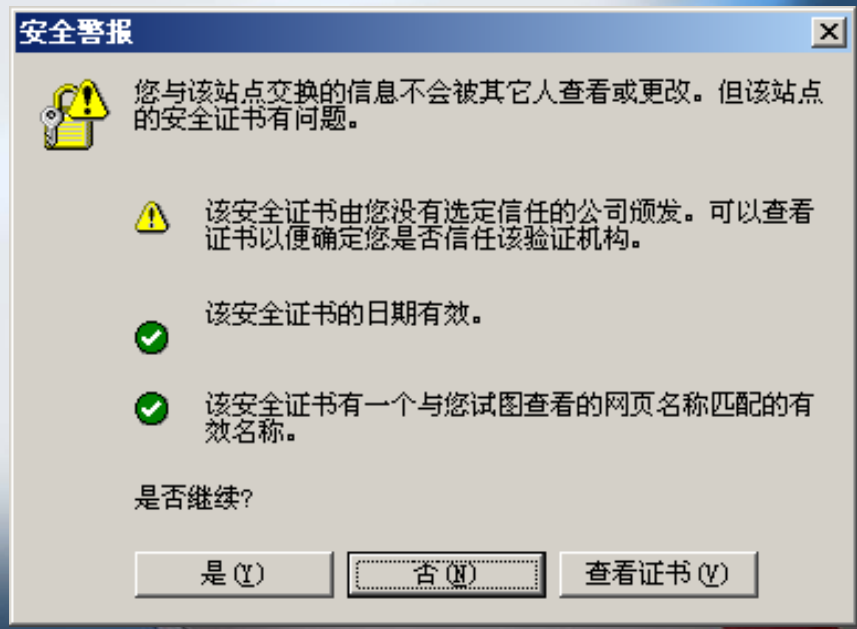
- 如何识别不同类型的SSL证书？
  (4) EV SSL：全球统一的严格身份验证标准的，地址栏显示为绿色的SSL证书，还可以分为是否支持SGC强制128位加密技术两类。不仅地址栏为绿色，而且地址栏右边安全锁旁直接显示此网站的公司名称。



SSL证书如何保证数据的传输安全

- 浏览器如何识别SSL证书是否工作正常？

第一，检查SSL 证书是否是由浏览器中“受信任的根证书颁发机构”颁发？如果不是，则浏览器会有安全警告，为 IE7 浏览器的警告信息为“此网站出具的安全证书不是受信任的证书颁发机构颁发的，安全证书问题可能显示试图欺骗您或截获您向服务器发送的数据，建议关闭此网页，并且不要继续浏览该网站。”IE6浏览器会提示 “该安全证书由您没有选定信任的公司颁发”。



SSL证书如何保证数据的传输安全

- 浏览器如何识别SSL证书是否工作正常？

第二，检查SSL证书中的证书吊销列表，检查证书是否被证书颁发机构吊销？如果已经被吊销，则会显示警告信息：“此组织的证书已被吊销。安全证书问题可能显示试图欺骗您或截获您向服务器发送的数据。建议关闭此网页，并且不要继续浏览该网站。”

SSL证书如何保证数据的传输安全

- 浏览器如何识别SSL证书是否工作正常？

第三，检查此SSL证书是否过期？如果证书已经过了有效期，则会显示警告信息：“此网站出具的安全证书已过期或还未生效。安全证书问题可能显示试图欺骗您或截获您向服务器发送的数据。建议关闭此网页，并且不要继续浏览该网站。”

SSL证书如何保证数据的传输安全

- 浏览器如何识别SSL证书是否工作正常？

第四，检查部署此SSL证书的网站的域名是否与证书中的域名一致？如果不一致，则浏览器也会显示警告信息：“此网站出具的安全证书是为其他网站地址颁发的。安全证书问题可能显示试图欺骗您或截获您向服务器发送的数据。建议关闭此网页，并且不要继续浏览该网站。”

SSL证书如何保证数据的传输安全

- 浏览器如何识别SSL证书是否工作正常？

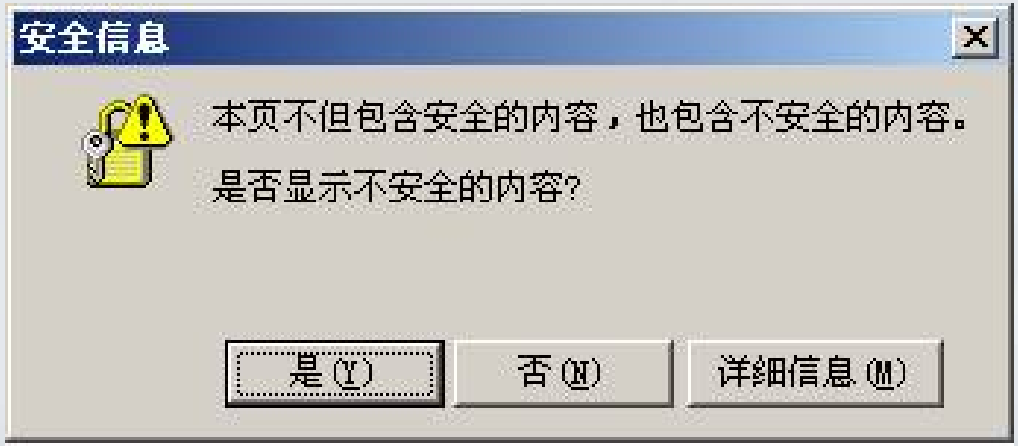
第五，IE7浏览器会到欺诈网站数据库查询此网站是否已经被列入欺诈网站黑名单？如果是，则会显示：“IE已发现一个已报告的仿冒网站。仿冒网站假冒其他网站并试图欺骗您泄漏个人信息或财务信息。建议关闭此网页，并且不要继续浏览该网站。”

SSL证书如何保证数据的传输安全

- 浏览器如何识别SSL证书是否工作正常？

第六，通过以上5个方面的检查都正常后，浏览器才检查所访问的网页中是否有不安全因素(如：Flash, Java Script, 链接到没有SSL证书的网站等)，如果有，则会有警告信息，只有点击“否”才会显示安全锁标志，否则不会显示。

只有通过以上6个步骤的检查后才会正常显示安全锁标志。



部署SSL证书应该注意哪些重要问题

(1) 一定要部署支持所有浏览器的SSL证书，绝对不能为了省钱而使用自签证书！也就是说：不需要在您的电脑上安装任何根证书就能让您的浏览器能识别出网站已经部署了SSL证书，这点是部署SSL证书的最低要求，因为您不可能要求您的所有用户都安装某个特定根证书，而用户在访问时IE7浏览器会直接拦截不支持浏览器的SSL证书，达不到部署SSL证书的目的；

(2) 要根据自己的业务需要选择合适的SSL证书(前提是支持浏览器的SSL证书)，因为目前市场上有多个品牌可以选择，当然首选支持浏览器的国内品牌(如：WoSign)，不仅性能价格比高，而且证书全面支持中文和本地的技术支持和售后服务。

(3) 从产品功能上来讲，则首选支持SGC强制128位加密的SSL证书(如：WoSign品牌的SGC超真SSL)，只有这样，才能保证用户使用各种版本浏览器都能实现128位高强度加密，因为40位和56位的加密都已经不安全了；其次，如果用户都是使用支持128位加密的浏览器的话，则您可以选购验证实体身份和证书中显示单位名称的SSL证书(如：WoSign品牌的超真SSL)，价格会便宜些。最后，如果网站对价格非常敏感，则可以考虑部署只验证域名所有权的SSL证书(如：WoSign品牌的超快SSL)，此证书中不显示单位名称。

(4) 对于电子商务(网上购物)网站则推荐EV SSL证书，此证书可以让IE7、火狐3等新版浏览器的地址栏变成绿色，明确地告诉网站访问者，此网站的身份是经过全球统一标准严格验证的，是可信的，绿色地址栏意味着绿色安全通道，可以增强客户信任和促成更多的在线销售。

数字证书的其他应用

- 代码签名证书

代码签名证书为软件开发商提供了一个理想的软件代码安全解决方案，使得软件开发商能对其软件代码进行数字签名，以便用户可以在互联网上安全下载和安全下载到各种终端上，使用户能确信此代码开发者的真实身份，并且确信此代码在传输过程中没有被非法篡改和被破坏。所有代码签名证书都是强制要求，以确保系统安全。

共有10种代码签名证书：

(1)微软代码签名证书：用于数字签名基于微软Windows平台的各种代码 (ActiveX控件);

(2) Symbian代码签名证书：用于数字签名Symbian平台代码，并用于 Symbian认证；

(3) Java代码签名证书：用于数字签名PC的Java代码和手机的Java代码；

(4) 微软徽标认证证书：用于数字签字Windows Vista内核代码并做徽标认证；

(5) 微软移动代码签名证书：用于数字签名Windows mobile平台代码；

(6) Adobe AIR代码签名证书：用于数字签名Adobe AIR代码；

(7) 微软Office宏签名证书：用于数字签名微软Office宏；

(8) 高通BREW代码签名证书：用于数字签名高通平台的代码；

(9) 火狐浏览器插件签名证书：用于数字签名火狐浏览器的插件；

(10) XML代码签名证书：用于数字签名XML代码。

数字证书的其他应用

- 如何防止用户的网络身份被盗用？

采用数字证书技术实现强身份认证，服务器端有SSL证书，客户端有客户端个人证书，必须使用个人证书实现身份认证才能登录，推荐USB Key+证书方式。

- 如何预防机密信息从企业泄露？

采用数字证书技术使用客户端证书或代码签名证书来数字加密机密文件，调阅机密文件必须用相应的证书才能阅读，这样即使拿走加密文件也没有用，做到无需任何防范，因为绝对是防不甚防的。

此方案是唯一可行和可靠的方案，Adobe Acrobat 有现成的加密PDF文件解决方案，实用方便，无需做任何开发。

WoSign品牌产品简介

WoSign品牌主要有十大特别优势：
(http://www.wosign.com/FAQ/WoSign_Certificate_Advantage.htm)

- 全球通用：支持所有浏览器和服务器
- 价格优势：全球最便宜(由于大大降低了身份验证成本和人工成本)
- 服务优势：款到即刻颁发，本地化技术支持、售前和售后服务
- 技术优势之一：全面彻底支持中文证书和中文域名
- 技术优势之二：支持SGC强制128位加密技术
- 技术优势之三：支持多域名SSL证书
- 技术优势之四：代码签名证书无需升级根证书和免费提供时间戳服务
- 技术优势之五：动态中文显示SSL安全认证签章
- 技术优势之六：支持1-5年、1-10年证书有效期
- 技术优势之七：全球独家推出个性化定制数字证书

WoSign品牌产品客户案例

- SSL证书中国市场占有率50%以上，代码签名证书市场占有率90%以上
- 银行、证券、基金、电信、邮政、各大企业、各大电子商务网站等等纷纷部署

讨论与提问?

谢　谢！

深圳市沃通电子商务服务有限公司
WoSign eCommerce Services Ltd.
服务热线：4006-WOSIGN　　0755-3363 3000
http://www.wosign.com