浅谈 https\ssl\数字证书

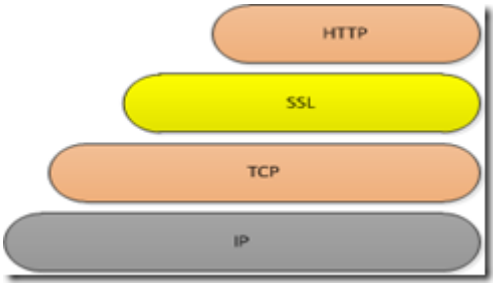
在互联网安全通信方式上，目前用的最多的就是 https 配合 ssl 和数字证书来保证传输和认证安全了。本文追本溯源围绕这个模式谈一谈。

名词解释

首先解释一下上面的几个名词：

https：在 http(超文本传输协议)基础上提出的一种安全的 http 协议，因此可以称为安全的超文本传输协议。http 协议直接放置在 TCP 协议之上，而 https 提出在 http 和 TCP 中间加上一层加密层。从发送端看，这一层负责把 http 的内容加密后送到下层的 TCP，从接收方看，这一层负责将 TCP 送来的数据解密还原成 http 的内容。

SSL(Secure Socket Layer)：是 Netscape 公司设计的主要用于 WEB 的安全传输协议。从名字就可以看出它在 https 协议栈中负责实现上面提到的加密层。因此，一个 https 协议栈大致是这样的：



数字证书：一种文件的名称，好比一个机构或人的签名，能够证明这个机构或人的真实性。其中包含的信息，用于实现上述功能。

加密和认证：加密是指通信双方为了防止铭感信息在信道上被第三方窃听而泄漏，将明文通过加密变成密文，如果第三方无法解密的话，就算他获得密文也无能为力；认证是指通信双方为了确认对方是值得信任的消息发送或接受方，而不是使用假身份的骗子，采取的确认身份的方式。只有同时进行了加密和认真才能保证通信的安全，因此在 SSL 通信协议中这两者都被应。

因此，这三者的关系已经十分清楚了：https 依赖一种实现方式，目前通用的是 SSL，数字证书是支持这种安全通信的文件。另外有 SSL 衍生出 TLS 和 WTLS，前者是 IEFT 将 SSL 标准化之后产生的（TSL1.0），与 SSL 差别很小，后者是用于无线环境下的 TSL。

如何加密

SSL 的加密过程

需要注意的是非对称加解密算法的效率要比对称加解密要低的多。所以 SSL 在握手过程中使用非对称密码算法来协商密钥，实际使用对称加解密的方法对 http 内容加密传输。

下面是对这一过程的形象的比喻：

假设 A 与 B 通信，A 是 SSL 客户端，B 是 SSL 服务器端，加密后的消息放在方括号[]里，以突出明文消息的区别。双方的处理动作的说明用圆括号（）括起。

A：我想和你安全的通话，我这里的对称加密算法有 DES,RC5,密钥交换算法有 RSA 和 DH，摘要算法有 MD5 和 SHA。

B：我们用 DES－RSA－SHA 这对组合好了。

这是我的证书，里面有我的名字和公钥，你拿去验证一下我的身份（把证书发给 A）。

A：（查看证书上 B 的名字是否无误，并通过手头早已有的数字的证书验证了 B 的证书的真实性，如果其中一项有误，发出警告并断开连接，这一步保证了 B 的公钥的真实性）

（产生一份秘密消息，这份秘密消息处理后将用作对称加密密钥，加密初始化向量和 hmac 的密钥。将这份秘密消息-协议中称为 per_master_secret-用 B 的公钥加密，封装成称作 ClientKeyExchange 的消息。由于用了 B 的公钥，保证了第三方无法窃听）

我生成了一份秘密消息，并用你的公钥加密了，给你（把 ClientKeyExchange 发给 B）

注意，下面我就要用加密的办法给你发消息了！

（将秘密消息进行处理，生成加密密钥，加密初始化向量和 hmac 的密钥）

[我说完了]

B：（用自己的私钥将 ClientKeyExchange 中的秘密消息解密出来，然后将秘密消息进行处理，生成加密密钥，加密初始化向量和 hmac 的密钥，这时双方已经安全的协商出一套加密办法了）

注意，我也要开始用加密的办法给你发消息了！

[我说完了]

A: [我的秘密是...]

B: [其它人不会听到的...]

从上面的过程可以看到，SSL 协议是如何用非对称密码算法来协商密钥，并使用密钥加密明文并传输的。还有以下几点补充：

1.B 使用数字证书把自己的公钥和其他信息包装起来发送 A，A 验证 B 的身份，下面会谈到 A 是如何验证的。

2.A 生成了了加密密钥、加密初始化向量和 hmac 密钥是双方用来将明文摘要和加密的。加密初始化向量和 hmac 密钥首先被用来对明文摘要（防止明文被篡改），然后这个摘要和明文放在一起用加密密钥加密后传输。

3.由于只有 B 有私钥，所以只有 B 可以解密 ClientKeyExchange 消息，并获得之后的通信密钥。

4.事实上，上述过程 B 没有验证 A 的身份，如果需要的话，SSL 也是支持的，此时 A 也需要提供自己的证书，这里就不展开了。在设置 IIS 的 SSL Require 的时候，通常默认都是 igore client certification 的。

数字证书

由上面的讨论可以知道，数字证书在 ssl 传输过程中扮演身份认证和密钥分发的功能。究竟什么是数字证书呢？

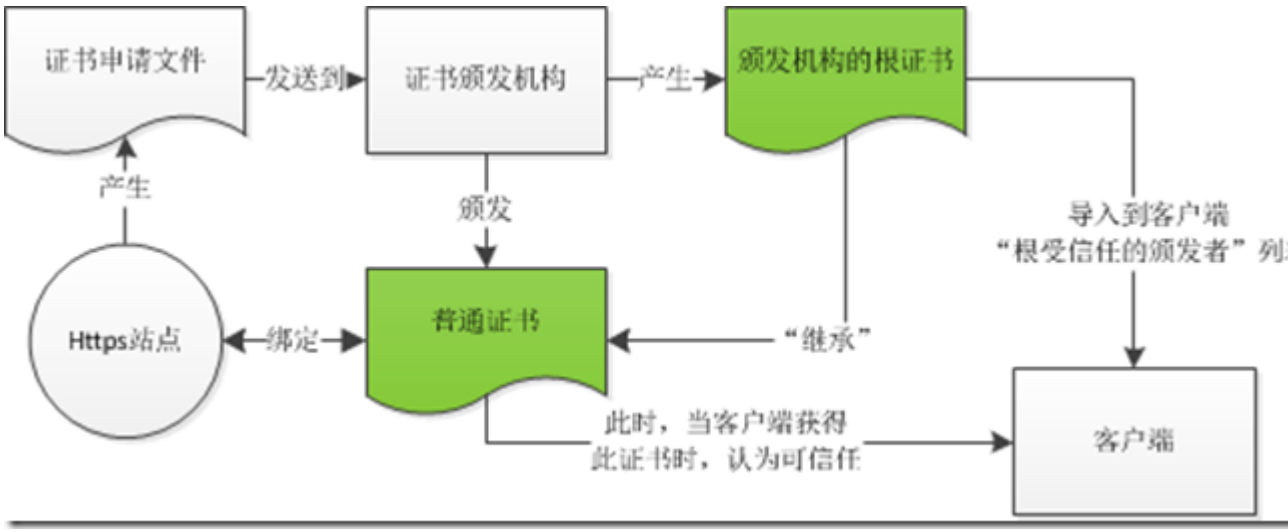
简而言之数字证书是一种网络上证明持有者身份的文件，同时还包含有公钥。一方面，既然是文件那么就有可能“伪造”，因此，证书的真伪就需要一个验证方式；另一方面，验证方需要认同这种验证方式。

对于第一个需求，目前的解决方案是，证书可以由国际上公认的证书机构颁发，这些机构是公认的信任机构，一些验证证书的客户端应用程序：比如浏览器，邮件客户端等，对于这些机构颁发的证书完全信任。当然想要请这些机构颁发证书可是要付“到了斯”的，通常在 windows 部署系统的时候会让客户端安装我们自己服务器的根证书，这样客户端同样可以信任我们的证书。

对于第二个需求，客户端程序通常通过维护一个“根受信任机构列表”，当收到一个证书时，查看这个证书是否是该列表中的机构颁发的，如果是则这个证书是可信任的，否则就不信任。

证书的信任

因此作为一个 https 的站点需要与一个证书绑定，无论如何，证书总是需要一个机构颁发的，这个机构可以是国际公认的证书机构，也可以是任何一台安装有证书服务的计算机。客户端是否能够信任这个站点的证书，首先取决于客户端程序是否导入了证书颁发者的根证书。下图说明了这个流程：



有时一个证书机构可能授权另一个证书机构颁发证书，这样就出现了证书链。

IE 浏览器在验证证书的时候主要从下面三个方面考察，只要有任何一个不满足都将给出警告

1、证书的颁发者是否在“根受信任的证书颁发机构列表”中

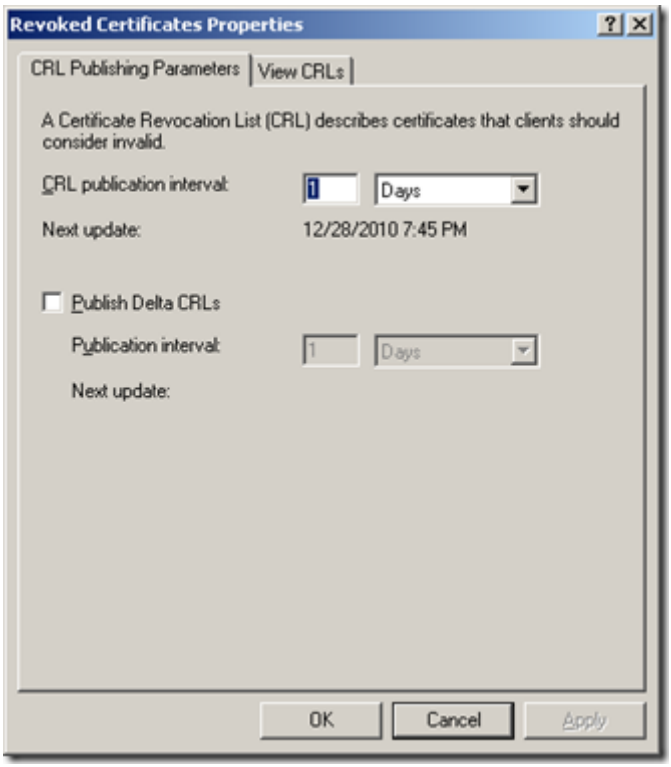
2、证书是否过期

3、证书的持有者是否和访问的网站一致

另外，浏览器还会定期查看证书颁发者公布的“证书吊销列表”，如果某个证书虽然符合上述条件，但是被它的颁发者在“证书吊销列表”中列出，那么也将给出警告。每个证书的 **CRL Distribution Point** 字段显示了查看这个列表的 url。尽管如此，windows 对于这个列表是“不敏感”的，也就是说 windows 的 api 会缓存这个列表，直到设置的缓存过期才会再从

CRL Distribution Point 中下载新的列表。目前，只能通过在证书颁发服务端尽量小的设置这个有效期(最小1天),来尽量使windows的客户端“敏感”些。具体设置方法为(winserver2003)：

进入管理员工具->证书机构->右击某个证书服务下的“吊销的证书”目录->属性：



按图中的设置，将 CRL 发布周期改为 1 天。

IIS 中部署基于数字证书的 https 网站

在 IIS6 中构建一个 https 网站需要如下几个关键步骤：

安装 CA 认证服务：此步骤不是必要的。如果网络中还没有那台主机安装过 CA 认证服务，或者确实需要建个新的 CA 认证服务，那么就需要在某台主机上安装 CA 认证服务。这是 windows 自带的功能，默认不安装。如果装了，就意味这这台主机具有颁发证书的能力，只要安装有这台主机的根证书的客户端会信任这台主机颁发的证书。在 windows server 2003 中的安装步骤，详见 http://jeffyyko.blog.51cto.com/28563/140518

向 CA 认证服务提交证书申请，并将获得的证书跟网站绑定：详见 http://jeffyyko.blog.51cto.com/28563/141322

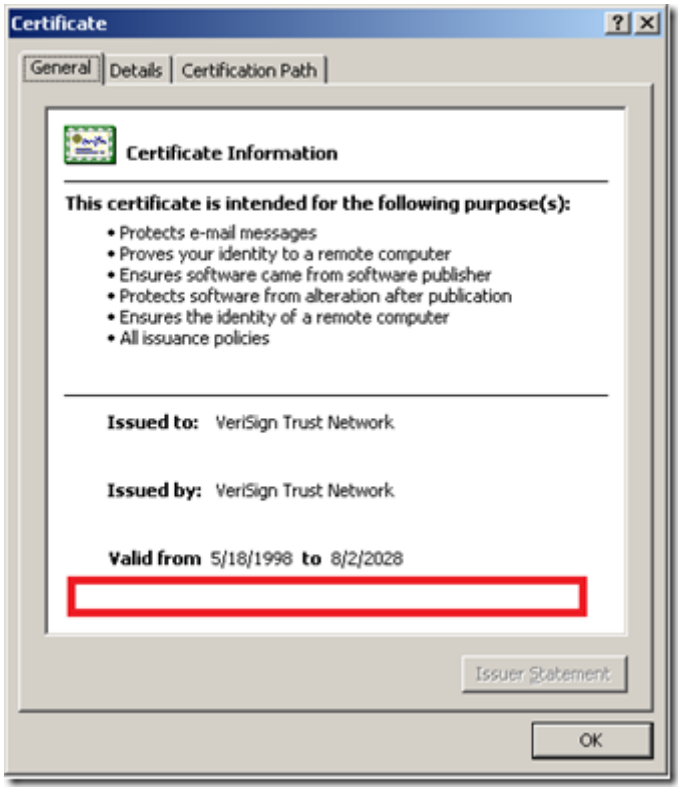
要求客户端导入根证书，以使客户端信任该证书：详见 http://jeffyyko.blog.51cto.com/28563/142280

证书与密钥

在 **ssl 的加密过程**一节中，我们知道要实现 ssl 加密通信，必须要双方协商密钥，ssl 采用的是非对称加密来实现密钥交换。在这个过程中，服务端向客户端发送的公钥就包含在证书中。客户端将自己生成的密钥用公钥加密，服务端用于公钥匹配的私钥解密。因此，可以想到的是，服务端保存了一个私钥，并且也与 https 的站点绑定了。

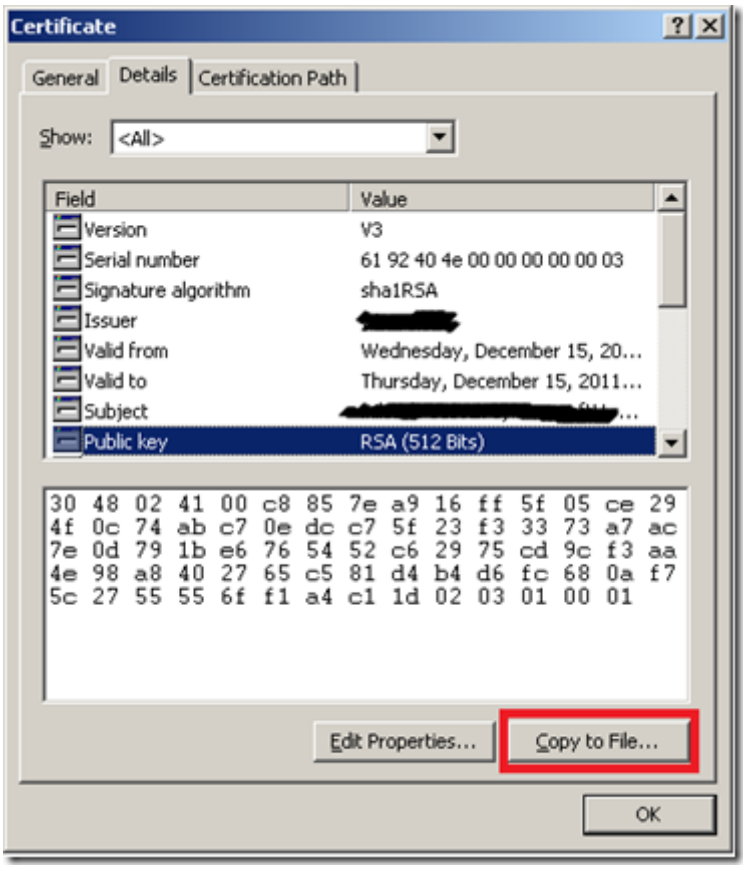
绑定私钥和不绑定私钥的证书

从证书持有者是否拥有证书的私钥，可以把证书分为两种：如下图，**当我们的本机拥有证书的私钥时如左图，否则如右图：**



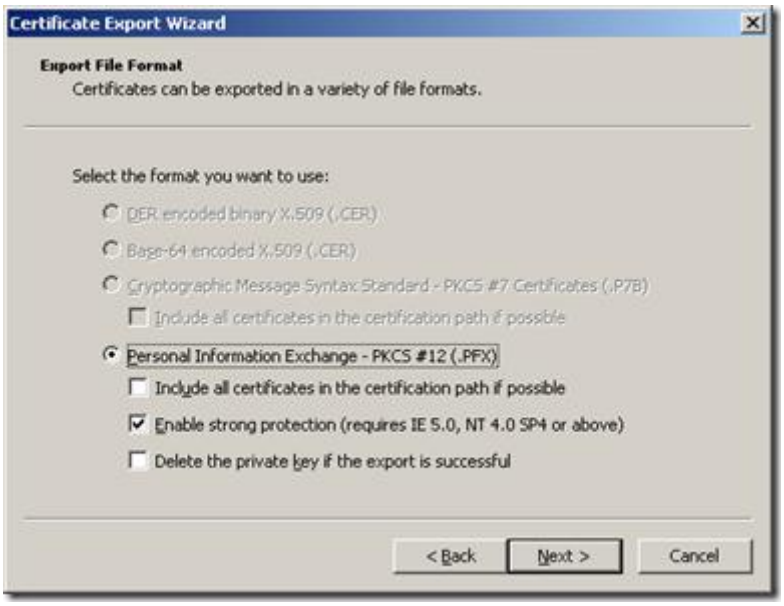
可以看到，左图标识了“你拥有与该证书相匹配的私钥”，而右图没有。对于需要与 https 站点绑定的证书必须是左图的形式，分发给客户端安装的应该是右图的形式，而不该是左图的形式。

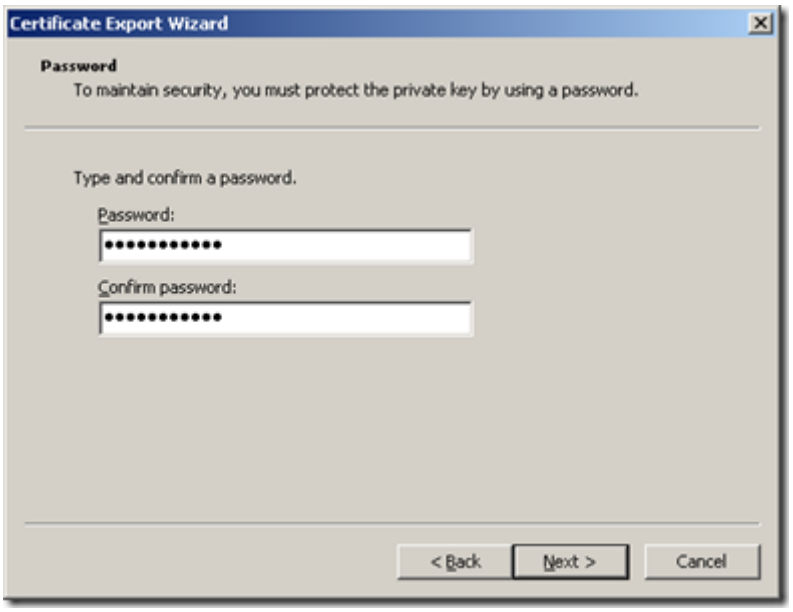
对于左图的证书可以将还有导出含有私钥的.pfx 格式，**用于备份证书或者分发**，步骤如下：



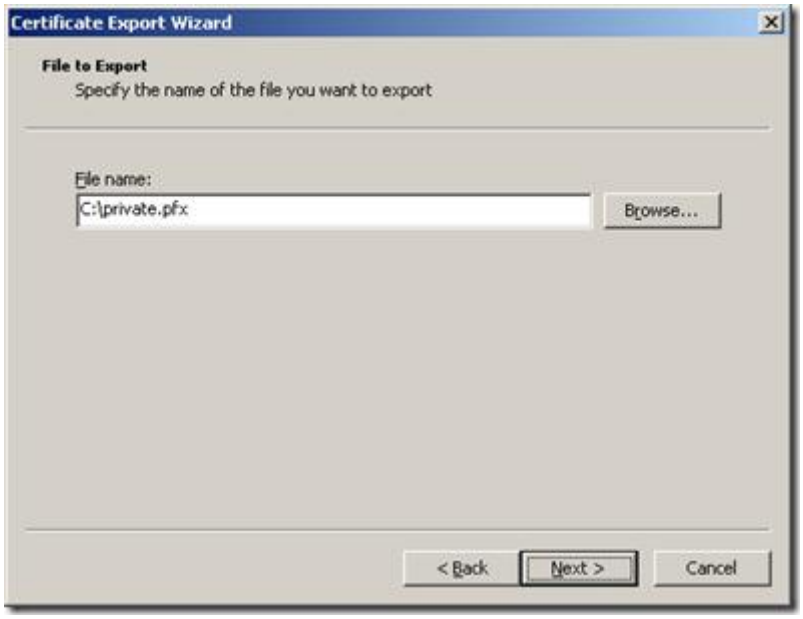

Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
< Back
Next >
Cancel

选择同时导出私钥


Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
Delete the private key if the export is successful
< Back
Next >
Cancel



这里输入的密码在重新安装的时候要输入，所以要 comfirm 一下。



选择一个文件存放，后缀自动为.pfx

对于普通的证书，不能导出含有私钥的.pfx 形式，只能导出下面三种格式：

总结

本文总结了 https/ssl/数字证书的相关基本概念，阐述了 ssl 协议的实现原理，阐述了数字证书在其中扮演的角色。

劳动果实，转载请注明出处：

http://www.cnblogs.com/P_Chou/archive/2010/12/27/https-ssl-certification.html