SSL 证书发展历程

SSL 协议是 NetScape 公司于 1994 年提出的一个关注互联网信息安全的信息加密传输协议，其目的是为客户端(浏览器) 到服务器端之间的信息传输构建一个加密通道，此协议是与操作系统和 Web 服务器无关。同时，NetScape 在 SSL 协议中采用了主流的加密算法(如： DES、AES 等) 和采用了通用的 PKI 加密技术。目前，SSL 已经发展到 V3.0 版本，已经成为一个国际标准，并得到了所有浏览器和服务器软件的支持。

1、部署了 SSL 证书的作用

起初，SSL 证书 的主要角色就是为网站的机密数据提供加密传输功能，从而确保机密信息的机密性、完整性和不可否认性。但是，对于电子商务来讲，用户在向网站提交机密信息之前如果不能信任此网站 ,那再高强度的加密也是没有用的，因为加密只是一种技术保护措施。所以，SSL 证书标准也在不断完善，使得 SSL 证书不仅起到加密作用，而且成为了网站的电子身份证或称“数字营业执照”，因为 SSL 证书中将包含经过证书颁发机构验证的单位名称和所在地区等信息，这样，就大大方便了在线用户能实时查验此网站是否是用一个现实世界的实体所拥有和是否就是网站上所声称的单位，从而让用户放心地从事在线交易。

2、不严格的身份验证就颁发 SSL 证书给在线交易带来了信任危机

数字证书颁发机构在维护在线身份的真实性上起到关键的作用 ,因为其颁发的证书就代表申请单位在网络世界的数字身份 ,数字证书颁发机构一定要严格验证申请单位的真实身份，并把通过其验证的信息包含在数字证书中。

但不幸的是，由于后来的数字证书颁发机构为了占领市场或为了降低成本，就推出了只验证域名所有权的 SSL 证书(超快 SSL)，而不要求提供营业执照并验证，这种 SSL 证书只能起到加密作用，而不能起到最关键的真实身份认证的作用。而更糟糕的是：这种 SSL 证书(超快 SSL)在浏览器中同恒信 SSL 证书一样显示一样的安全锁标志，只要仔细查看证书主题才能发现：超快 SSL 不显示单位名称(只显示域名)，而恒信 SSL 则显示单位名称。但一般用户是不会查验证书详细信息的，只是在浏览器中看到有安全锁就以为安全了。

如果两个网站： www.ABCcompany.com 和 www.ABC-company.com 都申请了 SSL 证书，如何判断哪个网站确实是 ABC company 的网站呢？这就是需要第三方的验证资料，这体现在 SSL 证书上，需要仔细查看证书的主题信息，因为都会显示一个“安全锁”标志，因为假冒网站是非常容易获得只验证域名所有权的 SSL 证书的，但这就给在线欺诈分子一个可乘之机，因为一般网上消费者根本就不能识别此 SSL 证书是否已经验证真实身份。

3、EV 证书的推出就是为了解决 SSL 证书的信任危机

正是由于以上 SSL 证书中存在的问题，就诞生了 EV SSL 证书。

当网站部署了 EV SSL 证书后，让用户使用 IE7 或其他新版浏览器访问此网站时，其地址栏是绿色的，而地址栏右边的安全状态栏会循环显示此网站所属的单位名称和颁发此证书的证书颁发机构，如下图所示，绿色表示此网站的身份是经过严格的身份验证的，而其他 SSL 证书则仍然显示一般的白色：

SSL 证书在网站信息安全上是至关重要的，它保护了信息的机密性、完整性和身份认证。而电子商务不仅需要加密，更重要的是需要增强在线消费者信心，让消费者相信电子商务网站的真实身份，所以严格身份验证的 SSL 证书对于电子商务来讲是至关重要的。相信 EV SSL 证书的推出，一定会为电子商务提供更好的安全保证和身份保证。这样，电子商务才能继续快速而健康地发展，为人们提供安全可信的在线购物和其他在线服务。