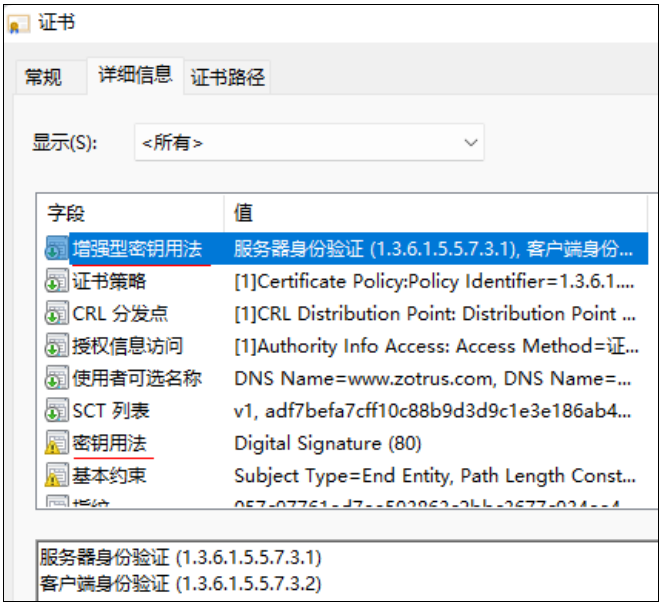
重新认识 SSL 证书

根据最新的谷歌证书透明日志数据，仅验证域名所有权的 DV SSL 证书已占 SSL 证书的 83.43%，也就是说网民访问的 100 个已经部署了 SSL 证书的网站中，有 83 个网站部署的是没有验证网站主身份的 SSL 证书，DV SSL 证书已经成为了主流 SSL 证书。这使得我们不得不重新认识 SSL 证书，什么是 SSL 证书？该如何面对 SSL 证书已经变成了 DV SSL 证书的天下的现实。

点击 https 网站的安全锁标识，查看证书，如下左图所示，证书信息显示“这个证书的目的如下：向远程计算机证明你的身份，保证远程计算机的身份”，这是英文“Ensure the identity of a remote computer, Proves your identity to a remote computer”的直译，笔者认为 Windows 的中文翻译是有问题的，两句话刚好翻译反了。第一句话的准确翻译应该是：确保远程计算机的身份，这个“远程计算机”指服务器，意思是 SSL 证书能证明 Web 服务器的身份；第二句话的准确翻译应该是：向远程计算机证明你的身份，这个“远程计算机”是指用户电脑，用户使用浏览器访问网站时，网站的身份由 SSL 证书来证明网站的真实身份。两句话的核心意思是 Web 服务器的可信身份由 SSL 证书来证明。



读者如果还有些困惑的话，可以再点击证书“详细信息”，如上右图所示，证书的“增强型密钥用法”为“服务器身份验证、客户端身份验证”和“密钥用法”为“Digital Signature”(数字签名)，可以看出：SSL 证书的主要用法是身份认证，用数字签名来证明其可信身份，保证服

务器身份可信。https 加密只是一个副功能，在验证了 Web 服务器身份后才用服务器的公钥加密同 Web 服务器交换的数据。

而现在被广泛使用的 DV SSL 证书在签发时并没有验证网站的真实身份，所以 DV SSL 证书的使用者信息只有网站域名，并没有网站主身份信息。DV SSL 证书仅用于交换公钥和用于 https 加密而不再验证服务器的真实身份，由“副”转“正”是否已远离了发明 SSL 证书的初衷呢？由机器验证域名控制权后自动化签发的 SSL 证书让欺诈假冒网站也都有了 SSL 证书，使得假冒银行的网站同正宗的银行官网显示的安全锁标识一模一样，假冒政府网站同正宗的政府官网显示的安全锁标识一模一样，这是我们需要的“安全”吗？难怪美国联邦调查局(FBI)官网向消费者发出警告-不要再信任浏览器的 https 或安全锁标识。全球网民所依赖的安全标识不再安全，怎么办？

零信技术对此现状的解决方案就是发布零信浏览器，明显区分显示网站部署了已验证身份的 OV SSL 证书和 EV SSL 证书，地址栏分别为白色和绿色，并直接在地址栏显示 OV SSL 证书和 EV SSL 证书中的网站主单位名称，让网站访问者能非常容易地知道此网站的真实身份信息，而不是某些政府网站一样自己做一个声明，假冒网站也可以做这样的声明。对于部署了 DV SSL 证书的网站，则不仅地址栏变成了灰色，而且直接在地址栏显示“身份未认证”，让网站访问者明辨网站身份并做出明智的安全决策。

而为了解决大量部署了 DV SSL 证书的网站的身份可信问题，零信技术推出了网站可信认证服务，以弥补 DV SSL 证书在网站身份方面的缺失，仍然按照 OV SSL 证书和 EV SSL 证书的国际标准完成网站身份认证，并在零信浏览器像部署了 OV SSL 证书和 EV SSL 证书一样的展示网站的真实身份，DV SSL 证书仅用于 https 加密，其身份认证功能则由零信网站可信认证服务和零信浏览器来承担，以弥补目前的 DV SSL 证书没有验证网站真实身份和无法展示网站真实身份的不足，从而有效保障了广大网民访问互联网的安全。

SSL 证书从 1994 年诞生到现在已经 28 个年头了，GeoTrust 于 2002 年发明了仅验证域名的 DV SSL 证书，DV SSL 证书对普及 https 加密立下了汗马功劳，但是，这是一个“阉割”了 SSL 证书的身份认证功能的“缺陷”产品，可是我们今天又已经离不开这个产品了，因为 DV SSL 证书可以免费或者低价得到。也就是说，是时候重新认识 SSL 证书了，我们必须接受 85% 的 SSL 证书都没有了网站身份信息的现实，只能把 SSL 证书作为一种加密产品来看待，展示并验证网站身份的工作就只能由浏览器来完成了，这个工作已经由零信浏览器作为一个公共服务产品来提供给全球用户，将为保障全球互联网安全可信做出应有的贡献。

零信网站安全云服务是一个集 https 加密、WAF 防护和网站可信认证于一体的网站安全解决方案，能完美地弥补网站部署 DV SSL 证书仅实现 https 加密的不足，因为用户需要的是一

个安全的可信的网站，而不仅仅是一个仅加密的网站，加密并不等于安全。

王高华

2022 年 6 月 6 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。