

展示网站身份是浏览器的义务

请读者使用 **IE 浏览器** 访问广东省人民政府网站，点击“个人中心”，IE 浏览器会显示绿色地址栏和地址栏的安全锁后面显示“数字广东网络建设有限公司”，如下图所示。这个网站是广东省人民政府官网，怎么会显示为一个公司的名称？难道是“古老”的 IE 浏览器显示错了？



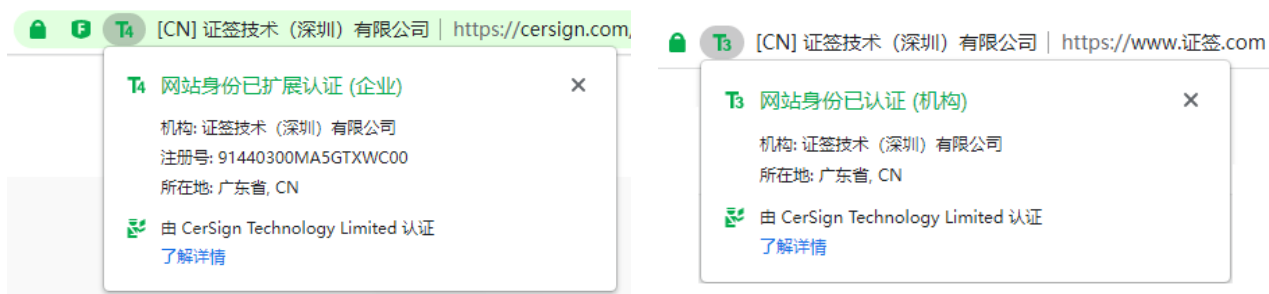
IE 浏览器并没有显示错！因为这是一张 EV SSL 证书，按照 EV SSL 证书的展示规则，浏览器会显示为绿色地址栏和在地址栏显示 EV SSL 证书主题信息中的 O 字段信息，如下左图所示，这张证书的 O 字段就是“数字广东网络建设有限公司”。如下右图所示为谷歌浏览器的展示情况，虽然谷歌浏览器现在不再对 EV SSL 证书显示为绿色地址栏，但是还是会展示证书中的单位名称。



也许大家会有疑问，这是否是 CA 机构签发了错误证书？应该不是，这是全球著名 CA-DigiCert 签发的 EV SSL 证书。只有一种可能，那就是这张证书的确是数字广东网络建设有限公司申请的，并且提交的身份证明文件也是该公司的文件，因为该公司是广东省政务系统的建设单位。但建设单位等同于房屋的建筑公司，不能说所有房子的房主都是建筑公司吧！造成这个问题的根本原因是现在的浏览器都不在地址栏显示 EV SSL 证书的单位名称而造成的，但用

户仍然习惯地为重要网站申请最严格验证的身份的 EV SSL 证书，这个“锅”还得由不展示证书中绑定的单位名称的浏览器来“背”！

笔者在博文《[全球网民熟悉的绿色地址栏强势回归](#)》中写道：谷歌浏览器和火狐浏览器不再显示 EV SSL 证书的绿色地址栏这事遭遇了多家国际 CA 巨头和多个著名 CA 专家的反对。笔者作为一个从事 CA 业务 18 年之久的专业人士，也是反对这种改变的。现在，零信浏览器的发布不仅仅是表明了我的反对的态度，更是一个实实在在的行动，不仅让 EV SSL 证书的绿色地址栏强势回归，而且还创新地展示了部署 OV SSL 和 IV SSL 证书网站的身份信息。因为笔者认为：展示网站身份是浏览器的责任和义务，浏览器是用户上网入口，必须非常直观地提供网站的身份信息供用户做出正确的安全决策，而不应该不从业界的意见而做出不适当的改变，毕竟浏览器不是一个普通的产品，是一个公益性的上网必备公共产品。



而对于上述广东省人民政府官网的证书展示问题，零信浏览器通过网站可信认证服务来纠正，对于没有认证网站，则直接展示 SSL 证书中的 O 字段单位名称，而对于已经通过网站可信认证的网站则优先显示通过我们认证的单位身份信息，所以，使用零信浏览器访问该网站会显示为如下展示效果：



再请大家看看北京市人民政府网站的类似情况，如果零信浏览器只是在地址栏展示 SSL 证书中的 O 字段单位名称，那就是如下左图的展示效果，因为这是一张 OV SSL 证书，如下右图所示的 O 字段信息。按照零信浏览器对 OV SSL 证书的展示规则就是白色地址栏和显示单位名称和 T3 认证标识。



这张 SSL 证书中绑定的单位名称是一个英文单位名称，让用户看起来就更加不伦不类了，估计这个单位也是北京市政务系统的建设单位，并用自己单位的身份证明文件申请了 OV SSL 证书。同广东省政府网站的 SSL 证书错误一样，这些“张冠李戴”网站身份错误绑定问题，也是由于现在的浏览器都不再重视展示 SSL 证书中绑定的身份信息而造成的，可以说一种技术倒退，这也是大家都只部署便宜的 DV SSL 证书的必然结果，反正浏览器展示各种认证级别的 SSL 证书都是一样的只显示安全锁标识。

当然，针对这种身份乌龙问题，零信浏览器对这个网站采用了优先显示网站可信认证的单位名称，准确展示了网站身份如下左图显示。请注意，安全锁后面多了一个云 WAF 防护标识，说明此网站有云 WAF 防护。如下右图所示，这个网站也有 O 字段错误，已经修正为正确的身份信息。请注意，这个网站的安全锁后面有一个 m 标志，说明此网站部署了零信浏览器信任的国密 SSL 证书，采用国密算法 SM2 实现了加密保护，是一个国密合规的网站。后面的云 WAF 标识说明此网站也有云 WAF 防护。



读者从以上展示案例应该能体会到零信浏览器在展示网站身份方面的独具匠心，创新地准确的展示网站的身份，方便网站访问者正确识别网站展示身份，从而做出正确的安全决策。为了方便大家理解我们的创新方案，笔者给大家推荐一篇反对谷歌浏览器和火狐浏览器不再展示 EV SSL 证书的博文《[Why Are You Removing Website Identity, Google and Mozilla?](#)》(为什么要移除网站身份，谷歌和 Mozilla?)，作者是国际 CA 巨头 Sectigo 的首席合规官 Tim Callan，于 2019 年 8 月 27 日发表在 PKI Consortium (国际 PKI 联盟)官网。笔者把 Tim 的博文的最后一段“建议”摘编翻译出来供读者朋友们参考，因为这些话也是我想写的。

“我们是制定 EV SSL 证书国际标准的团队之一。当时，我们设想 EV SSL 证书标准将是

一个持续的、不断发展的标准，CA 和浏览器社区将继续改进。听到关于 EV SSL 不够完美的反对意见，人们不禁想到“完美是好的敌人”的格言。EV 很好，是真的很好，统计数据表明它有助于使互联网变得更好。让我们集中精力让它变得更好。

PKI 联盟认为：行业应该继续完善 EV SSL 证书标识，而不是移除它们。为了打击网络钓鱼和提升网站身份的地位，我们认为浏览器公司应该同 CA 机构合作开发适合于电脑和手机的通用安全指标，并与 CA 合作进行用户培训，以帮助用户根据直观可用的网站身份信息做出正确的安全决策。这里有很大的创新和协作机会，这将使全球互联网用户和整个行业受益。”

王高华

2022 年 6 月 1 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。

