浏览器是如何识别 SSL 证书类型的？

有用户反映，零信浏览器升级到 114 版本后原先 97 版本显示网站身份认证级别为 **T3** 的网站显示为 **T1**，在浅绿色地址栏显示的单位名称也不见了，这是怎么回事？本文就讲一讲这个问题，这个问题与 114 版本无关，这是一个关于国密 SSL 证书类型如何定义和浏览器如何识别的问题，也是一个零信技术参与制定的相关国密标准中的待定的问题，笔者认为有必要好好讲一讲这个问题，以期不仅能解答用户的问题，而且还能给制定国密 SSL 证书标准中的证书类型讨论抛砖引玉，有利于业界达成共识。

如下左图所示，这是零信浏览器在内核升级之前显示北京银行个人网银页面，在浅绿色地址栏上显示绿色加密锁标识、绿色国密加密标识和绿色 T3 标识。右图为这次升级后显示的界面，这与内核版本升级没有任何关系，只是与这次升级改变了 UI 显示规则有关。这个由正常显示网站身份认证级别为“**T3**”的网站变成了显示为**“T1”**，并不是零信浏览器弄错了，而是由于这个网站部署的 SSL 证书没有正确的证书类型 OID 导致的。本文就详细讲一下证书类型 OID。

SSL 证书类型有 4 类：DV SSL、IV SSL、OV SSL 和 EV SSL，这是按照身份认证级别来定义的。其中，DV SSL 证书只需验证域名控制权，IV SSL 证书不仅需要验证域名控制权，而且还需要验证网站的个人身份；OV SSL 证书不仅需要验证域名控制权，而且还需要验证网站的单位身份；EV SSL 证书不仅需要验证域名控制权，而且还需要按照更严格的验证标准来扩展验证网站的单位身份。

零信技术依据这个分类给网站可信身份也一样定义了 4 个级别：T1、T2、T3 和 T4，T 就是英文“Trust”的第一个字母，T1、T2、T3 和 T4 分别对应 DV SSL、IV SSL、OV SSL 和 EV SSL。也就是说，凡是部署了 DV SSL 证书的网站，浏览器地址栏会显示 T1 标识，如此类推，部署了 IV/OV/EV SSL 证书的网站会分别显示 T2/T3/T4 标识。上左图大家看到的北京银行网站的 T3 标识为何升级到 114 版本后就变成了上右图的 T1 标识了呢？这是本文要讲的重点。

为了让浏览器能正常识别网站部署的 SSL 证书的证书类型和身份认证级别，国际标准组织-CA/浏览器论坛为 4 种 SSL 证书类型定义了 4 个 OID，分别是：

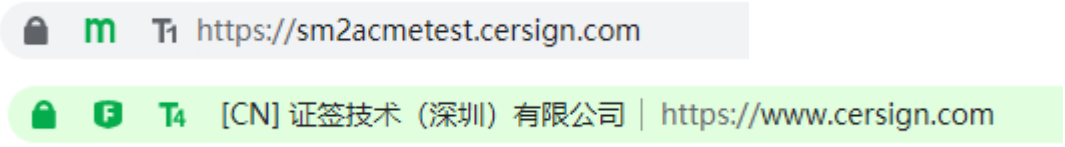
- ✦ DV SSL 证书： CA/B Forum OID：2.23.140.1.2.1
- ✦ IV SSL 证书： CA/B Forum OID：2.23.140.1.2.3
- ✦ OV SSL 证书： CA/B Forum OID：2.23.140.1.2.2
- ✦ EV SSL 证书： CA/B Forum OID：2.23.140.1.1

所有国际 SSL 证书都会在 SSL 证书的“证书策略”字段包含这 4 个 OID 之一来证明这张 SSL 证书是什么类型的 SSL 证书。如下左图所示为零信官网部署的国际 SSL 证书的证书策略“Policy Identifier=2.23.140.1.2.1”，这就表明这张 SSL 证书是 DV SSL 证书，而右图为证签官网部署的国际 SSL 证书的证书策略“Policy Identifier=2.23.140.1.1”，这就表明这张 SSL 证书是 EV SSL 证书。

早期所有浏览器都对部署了 EV SSL 证书的网站显示为绿色地址栏就是依据 EV SSL OID 来判断的，而为了防止 CA 机构错误使用 EV SSL 类型 OID，浏览器一般要求 CA 机构再提供一个 EV SSL 证书专用的从各 CA 自己的 OID 体系分配的 OID，如上右图的第一个 OID 就是 Sectigo 的专用 EV SSL OID，浏览器会另外预置管理一个能签发 EV SSL 证书的根证书列表。下图为 IE 浏览器显示的 EV SSL 证书效果。

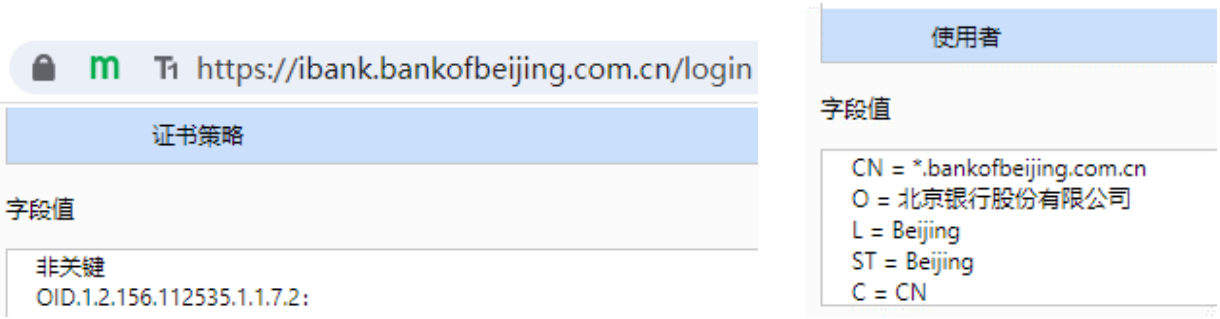
虽然其他浏览器现在都已经放弃了 EV SSL 证书的绿色地址栏，但是零信浏览器认为 EV 绿色地址栏仍然是很有价值的，能让用户一眼就能识别出这个网站是一个高度可信的网站，因为其真实身份已经通过第三方可信 CA 机构的严格认证。所以，零信浏览器继续维持 EV SSL 证书的绿色地址栏，继续为证书中含有国际标准 EV SSL 证书 OID 的网站显示绿色地址栏。而其他类型的 SSL 证书也一样依据国际标准的证书类型 OID 来识别网站部署的 SSL 证书的类型，从而显示不同的 UI，对于部署了 DV SSL 证书的网站，地址栏显示 T1 标识，而对于部署

了 EV SSL 证书的网站地址栏显示为 T4 标识。



谷歌浏览器虽然放弃了 EV 绿色地址栏，但是仍然保留了对部署了 EV SSL 证书的网站在“证书有效”标识下显示这张 SSL 证书绑定的单位名称（证书主题 O 字段）。

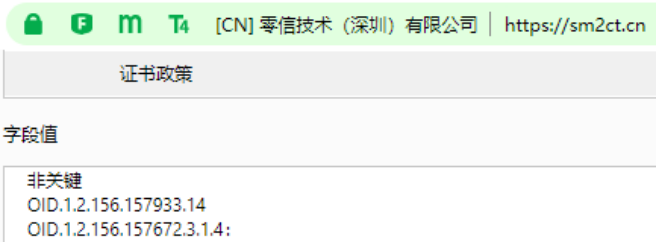
回到用户的问题，北京银行部署的国密 SSL 证书中“证书策略”中并没有上面所展示的 4 个 OID 之一，如下左图所示，所以，零信浏览器由于无法识别证书类型而只能显示为“T1”标志，因为这张 SSL 证书之所以能签发，一定是已经完成了域名控制权验证，一定满足显示 T1 标识的要求。用户一定会问：既然没有所要求的 OID，那为何 97 版本能显示为“T3”标识呢？请看下右图，这张 SSL 证书的主题信息中有 O 字段，97 版本就是依据这张 SSL 证书有 O 字段就在地址栏显示 T3 标识和显示 O 字段的单位名称，这是 97 版本当时在发现几乎所有国密 SSL 证书都没有证书类型 OID 后做出的妥协方案，而这次升级到 114 版本后，零信浏览器调整了 UI 方案，严格依据国际标准来展示网站部署的 SSL 证书类型，所以，新版本浏览器就因为找不到证书类型 OID 而显示为“T1”标识。



也许专业用户或者签发 CA 会反问：为何我们签发的国密 SSL 证书类型必须有国际 SSL 证书类型 OID 呢？我们就是喜欢用自己的 OID，浏览器是否可以依据我们自己的 OID 来识别出正确的证书类型呢？这些都是好问题。零信浏览器在发布可信根证书认证计划时就已经明确告知各 CA，零信浏览器已经免费为国密 SSL 证书类型定义了 4 个 OID，所有 CA 机构都可以免费使用这 4 个 OID 来定义自己签发的国密 SSL 证书类型。

- DV SSL 证书：1.2.156.157933.11，对应 CA/B Forum OID：2.23.140.1.2.1
- IV SSL 证书： 1.2.156.157933.12，对应 CA/B Forum OID：2.23.140.1.2.3
- OV SSL 证书：1.2.156.157933.13，对应 CA/B Forum OID：2.23.140.1.2.2
- EV SSL 证书：1.2.156.157933.14，对应 CA/B Forum OID：2.23.140.1.1

也就是说，零信浏览器会依据 4 个国际标准证书类型 OID 和 4 个零信浏览器证书类型 OID 来判断 SSL 证书的类型，如果 SSL 证书的证书策略含有 OID: 1.2.156.157933.14 或者 2.23.140.1.1，则零信浏览器就知道这张 SSL 证书是 EV SSL 证书，就会显示 T4 标识，如下左图所示，这张国密 SSL 证书中“证书策略”有“Policy ID: 2.23.140.1.1”，零信浏览器就会显示 T4 标识。如下右图所示，这张国密 SSL 证书中“证书策略”有“Policy ID: 1.2.156.157933.14”，零信浏览器也会显示 T4 标识。

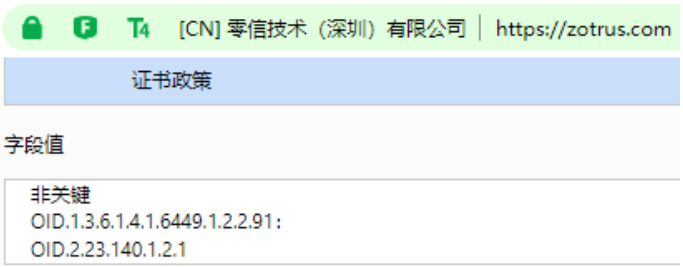


零信云 SSL 服务系统签发的国密 SSL 证书都只包含零信浏览器定义的 4 个国密 SSL 证书类型 OID，不会包含国际 SSL 证书类型 OID，这是因为 CA/浏览器论坛官网发布国际 OID 页面明确指出了这些国际 OID 的适用范围，如 EV SSL 证书 OID 的定义：extended-validation(1) — **2.23.140.1.1** (Certificate issued in compliance with the Extended Validation Guidelines) (适用于遵循扩展验证指南标准签发的 SSL 证书)。而所有国密 SSL 证书只是参考了国际标准，并没有完全遵循 EV 国际标准，密码算法就不符合 EV 国际标准，所以，按照以上定义是不能使用这些国际 OID 来定义国密 EV SSL 证书。这就是零信技术在讨论制定国密 SSL 证书标准时提出“必须制定国密 SSL 证书的证书类型 OID”提议的依据。而在国密 SSL

证书类型没有国密标准 OID 之前，零信技术免费提供了 4 个国密 SSL 证书类型 OID 供各个国密 CA 机构免费使用。

零信浏览器目前采用的政策是兼容国际证书类型 OID，无论国密 SSL 证书中含有国际 SSL 证书类型 OID 还是零信浏览器制定的国密 SSL 证书类型 OID，零信浏览器都能正确显示国密 SSL 证书类型，其他非这两类 OID 都不被正确识别而导致证书类型显示为 T1 标识。零信浏览器无法识别每个 CA 自定义的证书类型 OID。

细心的读者可能还会问：零信官网部署的国际 SSL 证书的证书策略“Policy Identifier = 2.23.140.1.2.1”，是 DV SSL 证书，为何零信浏览器会显示 T4 标识？同样，为何中国政府官网部署的是 OV SSL 证书，为何零信浏览器会显示 T4 标识？



这也是零信浏览器的创新之一—**网站可信认证服务**。鉴于全球 83%的网站部署的是未验证网站身份的 DV SSL 证书，为了解决这些网站的可信身份缺失问题，零信技术推出了网站可信认证服务，由零信技术来完成网站的可信身份认证，通过 EV 认证的网站无论网站部署的 SSL 证书是没有身份信息的 DV SSL 证书还是通过单位认证的 OV SSL 证书，零信浏览器都会显示“T4”标识和绿色地址栏，显示效果等同于网站部署了 EV SSL 证书。上图显示“T4”标识的网站已经通过零信技术的 EV 认证，所以会显示“T4”标识。

相信通过上面的讲解，大家应该能理解为何升级后的零信浏览器会把原先显示为“T3”标识的网站显示为“T1”标识。笔者在这里提醒各个零信浏览器信任的国密 CA 机构尽快升级 CA

系统，在签发的国密 SSL 证书中增加零信浏览器定义的 4 个 SSL 证书类型 OID，或者添加国际 SSL 证书类型 OID，以便零信浏览器能正确识别各家 CA 签发的国密 SSL 证书类型，正确显示网站可信认证标识。

欢迎用户申请零信网站可信认证服务，网站仍然可以部署免费的或便宜的 DV SSL 证书，通过零信网站可信认证后，零信浏览器会显示“T4”标识、绿色地址栏和单位名称。网站安全同时需要 https 加密和可信身份，能有效提升网站访问者信心，从而促成更多的在线交易。

王高华

2023 年 8 月 7 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。