零信浏览器“何德何能”担当首发产品

浏览器大家都不陌生了，市场上已经有 N 多浏览器，而且个个都是大厂出品。为何零信技术即将上线的第一个产品是浏览器？笔者作为公司 CEO，本文为读者解读其中原因和奥秘。

浏览器是上网入口，但是目前的浏览器仍然有许多用户不满意或者没有满足用户需求的地方，主要有以下八点：

(1) 虽然 SM2/SM3/SM4 密码算法已经成为 ISO 国际标准，但是国外厂家的浏览器仍然都不支持国密 SSL 证书，无法满足《密码法》合规要求。而部分国产浏览器支持国密 SSL 证书，但又是收费的，这不符合浏览器普遍免费使用的用户认知。

(2) 浏览器作为上网入口，就变成了广告的入口，用户很是讨厌有些浏览器的无孔不入的广告。

(3) 浏览器作为上网入口，用户的上网行为变成了所谓的“大数据”，某些浏览器会出售用户的上网行为数据，或者利用这些数据向用户发送有针对性的定向广告。

(4) 在 https 普及时代，有些浏览器居然不显示 https 加密安全锁标识，不提醒用户正在访问的 http 明文传输的网站是不安全的，这是对用户上网安全的不负责任。

(5) 各个大厂浏览器居然都把展示部署最严格身份认证的 EV SSL 证书的网站为绿色地址栏的功能给砍了，这大大降低了浏览器用户上网的可视化安全！

(6) 由于各个大厂浏览器只强调 https 加密的重要，而忽视了网站身份认证的重要性，使得假冒银行网站像正宗银行网站一样展示安全锁，这是一个巨大的上网安全问题，特别是现在的免费 SSL 证书随手可得，使得假冒银行网站和假冒政府网站几乎是零成本和零门槛！

(7) 各种网站安全事件如 SQL 注入、网页篡改、网站挂马等频繁发生，根据国家互联网应急中心发布的数据，2020 年我国境内被篡改的网站数量高达 10 万多。这些事件虽然与浏览器厂商无关，但是浏览器作为入口是否有义务提醒用户注意这方面的安全？

(8) 浏览器的第二个主要应用是 Web 方式查收电子邮件，浏览器是否可以在保护电子邮件的安全方面做出一些努力？

笔者还可以列出更多问题和更多可以改进的地方，相信读者也一定对某些问题深恶痛绝，一定会想“怎么就没有一个浏览器能解决这些问题呢”，笔者作为一个老网民也是深有同感。

同时，笔者作为一个深耕密码技术 18 年之久的老兵，重新创业时必须为这个产业做出点贡献。所以，零信技术就是结合本人在 CA 领域和网络安全领域的丰富经验而定位为一个基于密码技术的零信任安全提供商，不仅仅是要解决上述用户痛点，更重要的是要从产业发展的高度来引领和融合这两个领域产业的未来。

零信浏览器的核心创新主要有以下五点：

第一：让绿色地址栏回归，因为用户仍然需要对网站的身份有一个可视化的快速了解。

免费 SSL 证书的随手可得，使得假冒银行网站和假冒政府网站几乎是零成本和零门槛！这些假冒网站同正宗网站一样有安全锁标识，如何让用户明确识别网站部署的 SSL 证书类型和网站真实身份已经成为一个急需解决的问题。零信浏览器的解决方案是采用 4 个不同的标识(T1/T2/T3/T4)直接在地址栏展示网站部署的 SSL 证书的身份认证级别和展示已验证的身份信息，同时显示已经部署了最严格验证网站身份的 EV SSL 证书的网站为绿色地址栏，让已经消失的绿色地址栏重新回到用户的视线。

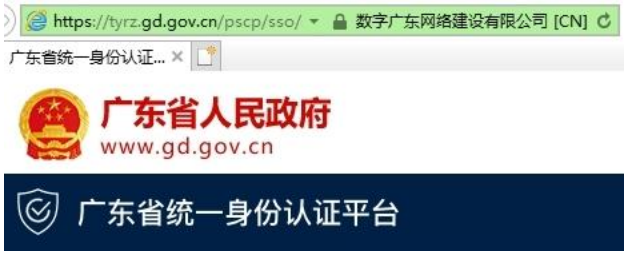
绿色地址栏的回归不仅能帮助用户简单快速识别网站身份，而且能助力 CA 产业的健康发展。因为自从各大浏览器取消了对 EV SSL 证书的绿色地址栏显示，使得 EV SSL 证书的市场份额从最高点时的 25%跌到了现在的 0.087%，大家一定能想象到这对 CA 公司的营收有多大的影响。

也许正是由于这个影响，使得现存的 EV SSL 证书和 OV SSL 证书中绑定的单位名称出现了许多乌龙事件，明明是.gov.cn 域名的网站，证书中绑定的单位名称却是一个公司。反正浏览器地址栏不显示单位名称，谁还在于证书主题中的 O 字段是什么单位呢？强烈推荐大家使用零信浏览器看看各种.gov.cn 域名的网站中绑定的五花八门的公司名称，而不是政府机关名称。

零信浏览器让绿色地址栏强势回归，大家仍然可以坚信“不显示绿色地址栏的银行网站就不是正宗的银行官网”的安全理念了。

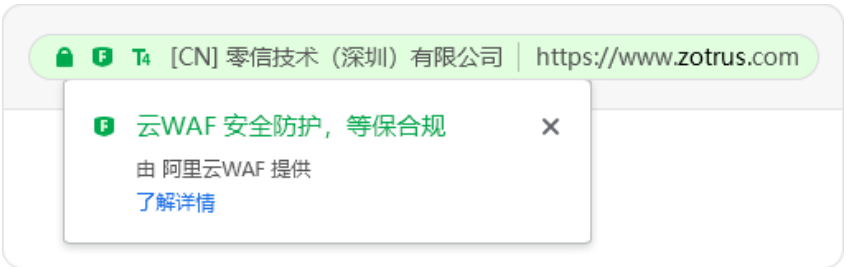
第二：提供网站可信认证服务，发挥绿色地址栏的作用，彻底解决 DV SSL 证书无可信身份难题。

绿色地址栏非常重要，但是申请 EV SSL 证书有国际标准的约束，才导致了目前许多政府网站的 SSL 证书绑定的单位名称是有问题的，因为省人民政府没有营业执照，很难满足 EV SSL 证书的认证要求。同时，为了解决已经部署了市场份额高达 80%的无身份信息的 DV SSL 证书的网站可信身份问题，我们同步启动了零信网站可信认证服务，使得部署了 DV SSL 证书的网站也能展示其可信身份，同时还可以把证书中绑定的错误公司名称更正为正确的单位名称。如下左图为直接读取证书中单位名称显示效果(IE 浏览器或老版本的谷歌浏览器)，可以看出这是有问题的。零信技术通过网站可信认证服务解决了这个问题，零信浏览器会优先显示零信可信网站认证数据库中的单位名称，如下右图所示。



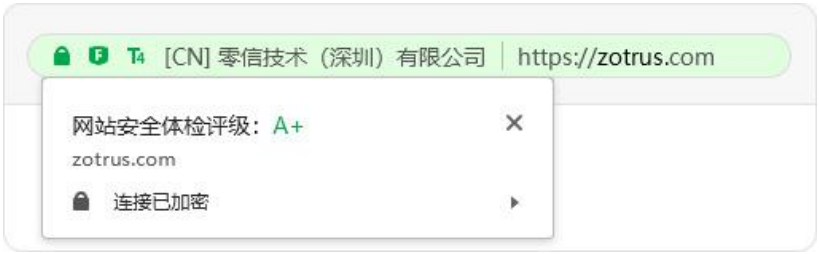
第三：地址栏显示云 WAF 防护标识，增强网站防护意识，普及云 WAF 防护应用，切实保障网站安全。

网站仅部署 SSL 证书并不能保护网站被攻击，所以，零信浏览器不提示 https 为“安全”，仅显示为“已加密”。浏览器作为上网入口，用户对正在浏览的网站是否安全是一无所知的，而目前各种网站攻击已经成为了常态，网站主也并不知晓其网站是否遭遇了攻击，除非是明显的造成了无法访问的攻击。所以，为了提升网站主和网站访问者的安全防护意识，满足《网络安全法》的合规要求，零信浏览器全球独家直接在地址栏显示网站是否有云 WAF 防护，让网站访问者对网站的安全防护状况和是否“等保合规”一目了然，这也是一个技术创新。这个创新一定能推动云 WAF 在网站安全防护的普及应用，从而带动云 WAF 产业的快速健康发展。



第四：实时网站安全体检，提升 SSL 证书的正确部署水平，提升网站安全整体水平。

网站未部署 SSL 证书是不安全的，所有浏览器都会提示“不安全”，但是部署了 SSL 证书，浏览器提示为“安全”，这也是有问题的。因为一个不正确的 SSL 证书部署仍然是不安全的，甚至为网站增加了更多的安全漏洞。所以，零信浏览器把提示“安全”改成了显示网站安全体检评级级别，让网站访问者和网站业主能及时了解此网站的安全状况。网站安全体检服务从 SSL 证书部署、云 WAF 防护和网站可信认证等三个方面对网站的安全防护情况做了一个全面的体检和评分评级。



零信浏览器在使用 HTTPS 协议同服务器握手过程中就已经全部了解了 SSL 证书的安全部署情况，了解了网站是否有可信的云 WAF 防护，了解了网站身份是否已经通过认证，这样，零信浏览器就可以依据零信网站安全体检评级指南自动计算出体检得分和安全级别，在正常显示安全锁标识的同时显示网站安全体检评级级别，这是零信浏览器的全球独家率先创新实现，有利提升网站安全的整体水平。

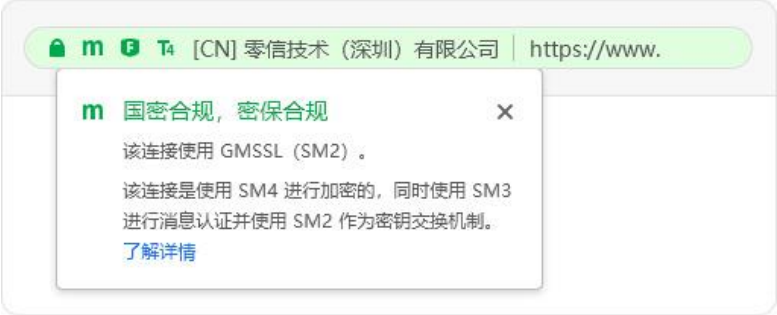
第五：优先使用国密算法实现 https 加密，地址栏直接展示国密合规和密保合规标识。

这是零信浏览器的最主要特色，全面支持国密算法和国密 SSL 证书，这是实现网站安全的核心技术的国密合规创新技术之一。随着《密码法》的不断深入贯彻实施，各个政府机构也已经越来越需要实现政务网站安全的国密合规，并逐渐开始部署国密 SSL 证书实现国密 https 加密。

如何简单明了地让网站访问者了解一个网站是否部署了国密 SSL 证书和是否“密保合规”，零信浏览器的创新就是在安全锁后面增加了一个“m”标识来突显此网站已经部署了零信浏览器信任的国密 SSL 证书，实现了国密算法 https 加密。点击“m”标识，则显示“国密合规，密保合规”，让用户一眼就知道这个网站是否是采用国密算法保护的和密保合规的，也让网站主办单位无需出具什么合规证明，直接让监督检查单位用零信浏览器访问试试就知道是否已经合规，这是一个创新，大大降低了《密码法》合规的检查和监督成本。

推荐我国所有网站(特别是政府网站)都部署 RSA/SM2 双 SSL 证书，零信浏览器的优先采用国密算法实现 https 加密，不仅能提升我国网站安全的自主可控能力，推动国密 SSL 证书的

普及应用，而且能快速提升我国 CA 的 SSL 证书市场占有率，从而带动我国 CA 产业的快速健康发展。



其实，零信浏览器还有很多创新点和亮点，比如：没有烦人的广告，是一个干净的纯粹的浏览器，也是一个完全免费的国密浏览器。笔者就不在这里一一列举，剩余的亮点就留给用户自己去发现吧。这是零信技术发布的第一个产品，作为公司的零信任安全首发产品是否已经解决了用户的部分痛点呢?当然是用户说了算。欢迎广大用户免费 下载 检验，体验和享受不一样的零信任安全上网浏览器！虽然是免费的，但笔者始终坚信：只要我们专注于用户，其他一切都会随之而来。

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。