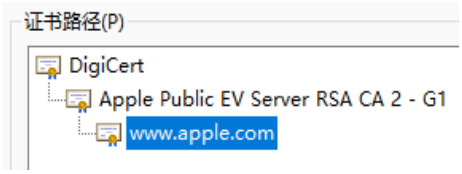
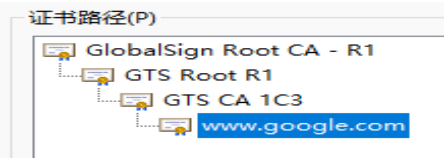
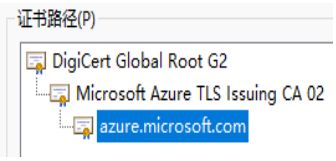
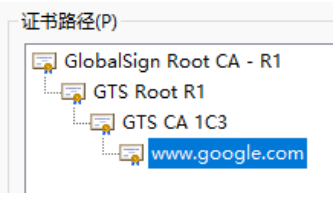
定制 SSL 中级根证书，夯实零信任安全底座

网站部署 SSL 证书，已经成为共识和得到了普及应用。SSL 证书由全球信任的 CA 从自己的中级根证书为用户签发 SSL 证书，互联网公司当然是各个 CA 的大客户，但是细心的读者一定访问过各大互联网巨头的官网或云服务提供商网站，也许会发现这些网站部署的 SSL 证书的证书链同自己网站部署的有点不一样。哪里不一样，还是先看看下面的 SSL 证书链截图吧，分别是微软云官网、苹果公司官网、亚马逊云官网和谷歌搜索官网。



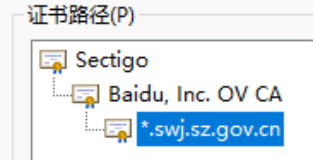


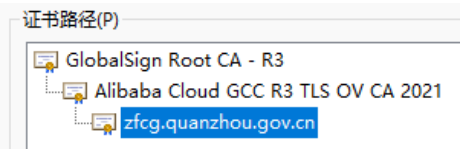


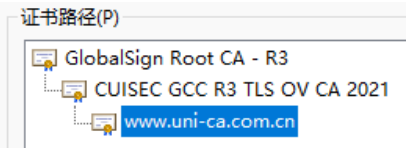


这 4 张 SSL 证书的不同之处是中级根证书名称是各自公司的名称。从第 1 张截图可以看出，微软云自用 SSL 证书是从 DigiCert 根证书定制的中级根证书 Microsoft Azure TLS Issuing CA 签发，Issuing CA 意思是签发 CA 根证书，是用于签发用户 SSL 证书的中级根证书。第 2 张截图是苹果公司官网自用 SSL 证书，从 DigiCert 根证书定制的中级根证书 Apple Public EV Server RSA CA 签发。第 3 张截图是亚马逊云服务网站自用 SSL 证书，由自己的根证书签发，也就是说，亚马逊成立了自己的 CA 公司-Amazon Trust Services。第 4 张截图是谷歌官网自用 SSL 证书，也是由自己的根证书签发，其根证书由 GlobalSign 根证书交叉签名。

我们再看看下面的 3 张 SSL 证书截图，分别是百度云给用户签发的 SSL 证书、阿里云给用户签发的 SSL 证书和联通 CA 官网用 SSL 证书。







从第 1 张截图可以看出，百度云已经定制了 SSL 中级根证书用于签发用户 SSL 证书，这是从 Sectigo 根证书定制的中级根证书 Baidu, Inc. OV CA。从第 2 张截图可以看出，阿里云也

定制了 SSL 中级根证书用于签发用户 SSL 证书，这是从 GlobalSign 根证书定制的中级根证书 Alibaba Cloud GCC R3 TLS OV CA。前两家既是互联网巨头，也是领先的云服务提供商，其中百度中级根证书是 2020 年 4 月定制的，已经以 BaiduTrust 品牌为百度云用户签发 SSL 证书，而阿里云中级根证书则是 2021 年 6 月定制的，也已经为用户签发 SSL 证书。第 3 张截图是联通 CA 签发给自己官网的 SSL 证书，这是从 GlobalSign 根证书定制的中级根证书 CUISEC GCC R3 TLS OV CA 签发的。这是中国联通的子公司联通 CA 计划进军 SSL 证书市场的行动，2021 年 4 月定制了 3 个 SSL 中级根证书。

相信读者一定会想，为何这些国内外的互联网巨头们都定制了 SSL 中级根证书呢？笔者给大家总结出以下三点理由供大家参考、借鉴和学习。

第一，这是对其他 SSL 中级根证书的零信任，**只信任**自己的中级根证书签发的 SSL 证书。

这一点对于各个重要的云服务系统和业务系统非常重要，为每一台云服务器都配置 SSL 证书，每一张 SSL 证书不仅用于 https 加密，更重要的是用于身份认证，用于云中众多服务器之间加密通信的身份认证，只信任自己的中级根证书签发的 SSL 证书，能有效和高效地杜绝 SSL 中间人攻击和假冒服务器身份连接，以确保核心业务系统和云服务系统的基础通信安全和设备安全。

第二，用于设置官网域名的 CAA 记录。

CAA 记录是 DNS 系统新增加的一种资源记录，一种互联网安全策略机制，允许域名持有者指定可以为其域名签发 SSL 证书的证书颁发机构(CA)。CAA 资源记录允许域名持有者实施额外的安全控制，以降低意外证书错误颁发的风险。据 Qualys SSL 实验室对 Alexa 流量排名前 15 万个网站的监测统计数据，截止到 2 月 8 日，有 12.2%的网站设置了 CAA 记录。以上 7 家互联网公司的官网域名只有谷歌设置了 CAA，设置的参数表明谷歌只允许自己的 CA 为 google.com 域名签发 SSL 证书。

这也是对非 CAA 记录允许的其他 CA 的零信任。这一点从系统安全防范策略来看，同第一点的作用类似，从不同的角度实现对 SSL 证书签发行为的零信任，从而高效地保障了 TLS 加密通信的安全。

第三，为用户提供自己品牌的 SSL 证书，不仅能带来新的业务收入，更重要的是为其他云服务产品增强了竞争力。

用户需要一站式解决方案，这对于云服务提供商非常重要，因为用户选购您的云主机，还要去向其他 CA 申请 SSL 证书，再在您的云主机上自己安装和管理证书，这不仅是对用户的漠不关心，而且是白白失去了一个增加业务收入的好机会，用户一定会选择能为其提供全自动配置 SSL 证书的云主机提供商，谁都想省事，对吧？！当然，有些云服务提供商已经对接了第三方 CA 提供的 SSL 证书，但由于是第三方产品，一定不能很好地对接自己的云服务产品，仍然没有彻底解决用户的痛点！

相信读者一定能通过本文了解和理解了为何各大互联网巨头都在定制 SSL 中级根证书。为了提升互联网公司的自身系统安全和提升用户服务能力，赶紧行动起来吧，笔者愿意奉献 17 年的国际 CA 运营经验和国际 CA 资源帮助大家快速拥有属于自己品牌的 SSL 中级根证书，筑牢零信任安全底座，有效保障重要系统的基础通信安全。

王高华

2022 年 2 月 9 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。