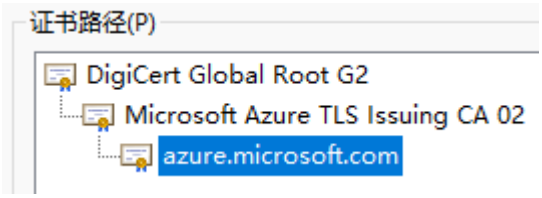
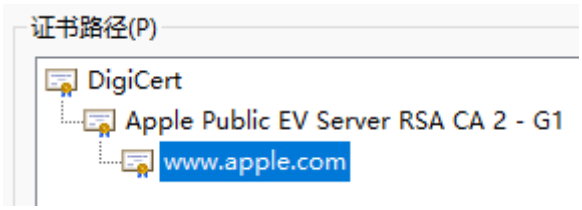
定制 SSL 中级根证书已成为互联网公司的必选项

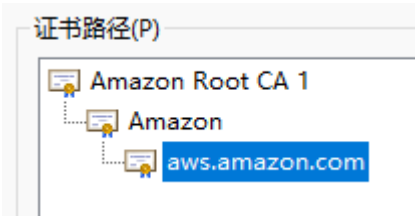
网站必须部署 SSL 证书，这个已经不是可选项了，而是必选项，浏览器会显示没有部署 SSL 证书网站为“**不安全**”，这是因为没有采用 https 加密，所有机密信息从浏览器或移动 App 到服务器端的数据交换都是明文传输的，是非常容易被非法窃取和非法篡改的。

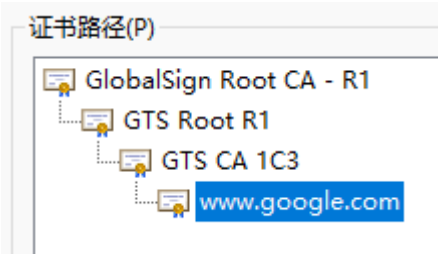
而对于互联网公司或云服务提供商来讲，不仅大量对外提供服务的云服务器都需要 SSL 证书，同时云服务提供商的用户网站和系统也需要 SSL 证书。这就有了大量的 SSL 证书需求，如何保障 SSL 证书供应自给自如，如何降低 SSL 证书的采购成本，如何充分利用 SSL 证书来保障自身系统和云服务系统的安全，这些都是互联网公司和云服务提供商必须马上采取行动事情。

我们还是先看看下面这 4 张 SSL 证书的截图：



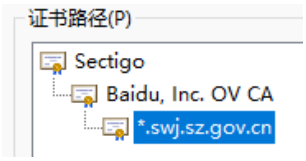


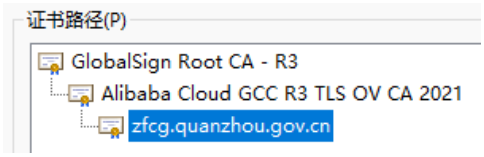


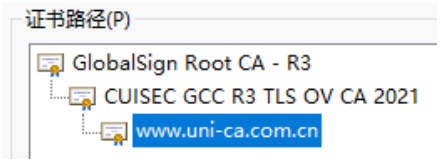


从第 1 张截图可以看出，微软云自用 SSL 证书是从 DigiCert 根证书定制的中级根证书 Microsoft Azure TLS Issuing CA 签发，Issuing CA 就是签发根证书，是用于签发用户 SSL 证书的中级根证书。第 2 张截图是苹果公司官网自用 SSL 证书，从 DigiCert 根证书定制的中级根证书 Apple Public EV Server RSA CA 签发。第 3 张截图是亚马逊云服务网站自用 SSL 证书，由自己的根证书签发，也就是说亚马逊成立了自己的 CA 公司 Amazon Trust Services。第 4 张截图是谷歌官网自用 SSL 证书，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：







第 1 张截图是百度云签发给用户的 SSL 证书，这是从 Sectigo 根证书定制的中级根证书 Baidu, Inc. OV CA 签发的用户证书。第 2 张截图是阿里云签发给用户的 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 签发的用户证书。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今年 6 月份定制的，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 签发的用户证书。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，今年 4 月份定制了 3 个 SSL 中级根证书，还没有对外签发 SSL 证书，估计还在内测中。

看了国内外这么多定制中级根证书的案例，笔者总结一下有以下三点是值得我国其他互联网公司、云服务提供商和电信运营商学习的。

第一，定制中级根可以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，大大方便了用户使用和选购相应的云服务产品。因为用户需要一站式解决方案，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！

第二，对于自己就有大量 SSL 证书部署需求的互联网公司、云服务提供商和电信运营商，定制自己专用的 SSL 中级根证书的好处有三：

(1) 自主管理和签发业务系统所需的 SSL 证书，更能快速满足自己业务系统部署 SSL 证书的需要，因为 SSL 证书是所有系统上线的必须品，自己签发当然非常可控。

(2) 这一点非常重要，为了确保重要的业务系统的安全，应该制定一个仅信任自己的中级根证书签发的 SSL 证书的零信任安全策略，这是防范重要业务系统遭遇 SSL 中间人攻击的有力有效手段，能简单高效地保护核心信息系统的基础通信安全。

(3) 能降低 SSL 证书的总采购费用，这对于降低电信服务、云服务和互联网服务的运营成本也非常重要。

第三，必须设置互联网公司、云服务提供商的官网域名的 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 11 月 14 日，只有 9.3%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。

这一点从系统安全防范策略来看，同第二点的第(2)条有点类似，从不同的角度来保证 SSL 证书和 TLS 加密通信的安全。

总之，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，并指导助力成功启动和开拓广阔的 SSL 证书市场。

王高华

2021 年 12 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。