# 关于中国防火墙（GFW）影响 TrustAsia DV 证书使用说明

**一：事件描述：**因为中国长城防火墙（GFW）在中国时间 2020 年 3 月 6 日约凌晨 1 点---15 点期间策略调整，导致海外的 OCSP 节点无法正常响应。对于只有海外 OCSP 节点的 DV SSL 证书且 DV 证书是应用应用于苹果移动端的用户，会载页面延迟影响。

**二：事件原因：**

1　证书是分为三个安全级别，最低 DV，其次是 OV，最高是 EV

2　TrustAsia 品牌 OV 和 EV 证书的 OCSP 服务器，都是中国+海外双备份节点。所以中国有护网行动的时候，拦截海外 IP 也不影响使用，因为还有中国境内的 OCSP 服务器节点响应。

3　TrustAsia DV 证书因为价格便宜（DV 单域名免费），所以安全级别低，DV 证书是没有海外+中国双 OCSP 节点备份的，只有海外 CA 的 OCSP 节点响应。

4 在 SSL/TLS 握手过程中 客户端需要通过 OCSP 协议校验服务器证书和中级证书的 吊销状态是否正常。客户端会通过每个证书中的 OCSP 地址向 CA 的 OCSP 服务器发送 证书吊销状态查询 并等待 OCSP 服务器的响应。大部分客户端为了加快访问速度 会在握手后异步检测 OCSP 状态，但有些移动客户端（IOS 移动端）会在握手过程中阻塞式强制先检测 OCSP 状态，这种情况下 如果 OCSP 响应慢就会影响 HTTPS 的访问速度。

**三 解决办法：**

1 为杜绝以后有类似的事情发生，客户把自己的证书升级为 OV 证书就可以完全解决这个问题

2 对于不愿意升级 OV 证书的用户，可以把证书替换为支持海外+中国双 OCSP 节点备份的 DV 型号证书，但出于对用户的安全保障考虑，还是建议客户如果是正式生产环境使用，还是使用 OV。

3　对于 UCloud 已经使用了 TrustAsia 品牌 DV 付费证书的用户（续费期外），提供免费升级到同类型 TrustAsia OV 证书/或替换支持海外+中国双节点的 DV 证书

**四 后续优化：**

**1** 增加主动通知机制，在发现中国长城防火墙（GFW）策略调整第一时间通知到 UCloud，以便于提前做好客户响应准备。

2 TrustAsia DV 证书（付费 DV）会增加中国 OCSP 节点。从而杜绝被墙。

3 对应商业用户在正式生产环境使用，**教育和引导客户使用 OV 企业型或者 EV 增强型证书，DV 证书仅适用于个人体验和企业测试；**OV 和 EV 的价格虽然比 DV 高，但是更安全，DV 虽然便宜，但它丧失了 SSL 证书的另一重要功能，即域名所有者组织身份的真实性验证，且不够安全有保障。