



广东省数字证书认证中心

GDCA 信鉴易® TrustAUTH®证书常见问题解答

2015/11/23

## GDCA 信鉴易® TrustAUTH®证书常见问题解答

### 目录

产品信息部分常见问题.....	3
一、 什么是 GDCA 信鉴易 TrustAUTH®证书 .....	3
二、 信鉴易®TrustAUTH®证书系列包含哪些产品 .....	3
三、 【恒信】、【睿信】、【速信】这三个不同系列的产品有什么区别呢? .....	3
四、 什么是 SSL 证书? .....	3
五、 SSL 证书有什么作用? .....	4
六、 我如何知道网站部署了 SSL 证书? .....	4
七、 SSL 证书有哪几种? 如何区分? .....	5
八、 网站部署更高级别的 EV SSL 证书有什么好处? .....	5
九、 EV SSL 证书的证书主题中会显示哪些信息? .....	5
十、 SSL 证书支持多域名吗? .....	6
十一、 浏览器是如何检查 SSL 证书正常工作的? .....	6
十二、 为什么说部署自签 SSL 证书非常不安全? .....	6
十三、 为什么要选择 GDCA 的 SSL 证书? .....	6
十四、 我的服务器更换、重装或者丢失了 SSL 证书怎么办? .....	7
十五、 购买了 SSL 证书我可以无条件退款吗? .....	7
十六、 如何查验 SSL 证书是否支持 SGC 强制 128 位加密技术? .....	7
十七、 服务器上装上 SSL 证书会不会影响到速度和流量? .....	7
十八、 代码签名证书有哪几种? .....	8
十九、 为什么需要代码签名证书? .....	8
二十、 我在申请代码签名证书时单位名称应该填中文还是英文? .....	8
二十一、 如果改变了硬件、软件 (web server) 证书需要重新申请吗? .....	9
二十二、 物理服务器出现故障对 SSL 证书使用会有什么影响? .....	9
二十三、 我申请的 GDCA 的 SSL 证书需要多久才能签发? .....	9
二十四、 GDCA 的 SSL 证书与国外品牌 SSL 证书有什么区别? .....	9



## 产品信息部分常见问题

### 一、 什么是 GDCA 信鉴易 TrustAUTH®证书

TrustAUTH®证书是 GDCA 自有的专利品牌，GDCA 是国内领先的权威第三方电子认证机构，自主研发的信鉴易® TrustAUTH® 证书系列通过了全球最高标准的 WEBTRUST 国际认证体系的认证，真正实现一证通行，全球信任！

### 二、 信鉴易®TrustAUTH®证书系列包含哪些产品

GDCA 现有的 TrustAUTH®证书主要包含服务器证书（SSL 证书）和代码签名证书，分别按不同品牌等级分为【恒信】、【睿信】、【速信】三大产品系列，如下图所示：

品牌	企业 EV	企业 OV	个人及个人代码
信鉴易® TrustAUTH® 证书	恒信 企业 EV SSL 证书	睿信 (OV) SSL 证书	速信 个人代 码签名证书
	恒信 企业 EV 代码签名证书		

### 三、 【恒信】、【睿信】、【速信】这三个不同系列的产品有什么区别呢？

这三个系列的产品主要从安全级别和信任级别、安全保险赔付金额、证书申请和审核流程验证等几个方面不同来进行区分的。

### 四、 什么是 SSL 证书？

SSL 证书也称为服务器证书，是遵守全球统一的严格身份认证的 SSL 协议的一种数字证书，由全球信任的证书颁发机构 (CA) 验证服务器身份后颁



发。将 SSL 证书安装在网站服务器上，可实现网站身份验证和数据加密传输双重功能。

## 五、 SSL 证书有什么作用？

部署了 GDCA 的 SSL 证书产品，可以实现两个重要功能：一是**实现加密传输**，二是**认证服务器真实身份**

用户通过 http 协议访问网站时，浏览器和服务器之间是明文传输，这就意味着用户填写的密码、帐号、交易记录等机密信息都是明文，随时可能被泄露、窃取、篡改，被黑客加以利用。安装 SSL 证书后，使用 Https 协议加密访问网站，可激活客户端浏览器到网站服务器之间的“SSL 加密通道”（SSL 协议），实现高强度双向加密传输，防止传输数据被泄露或篡改钓鱼欺诈网站泛滥。

同时，网站部署全球信任的 SSL 证书后，浏览器内置安全机制，实时查验证书状态，通过浏览器向用户展示网站认证信息，让用户轻松识别网站真实身份，防止钓鱼网站仿冒。

## 六、 我如何知道网站部署了 SSL 证书？

网站安全非常重要，因为涉及到用户的机密信息，甚至涉及到银行卡信息等，已部署 SSL 证书的网站可以让访问的用户方便地知道该网站是否已经使用了 SSL 证书，主要有以下标志：

- 1、能用 https 方式访问的站点；
- 2、打开浏览器显示访问的网址有安全锁标志；只要有这两个标志，就说明此网站是使用了 SSL 证书来确保用户的机密信息安全的；
- 3、访问用户可以通过查看 SSL 证书上已经验证的信息来辨别网站真实性；



## 七、 SSL 证书有哪几种？如何区分？

目前 GDCA 信鉴易 TrustAUTH®证书系列主要是按身份验证方式的不同分为两种：Extended Validation SSL(扩展验证型 SSL 证书，简称为 EV SSL) 和 Organization Validation SSL(机构验证型 SSL 证书，简称为：OV SSL)

1、【Extended Validation SSL(EV SSL)】证书是全球统一最高标准的严格身份验证的 SSL 证书，要求所有证书颁发机构严格遵守此标准来颁发 EV SSL 证书。GDCA 恒信 (EV) SSL 证书除了要验证域名所有权外，验证过程还包括验证联系人是否得到申请单位的授权来申请证书，验证申请单位是否为政府合法注册的单位，营业执照是否已经年审，同时还验证申请单位是否有合法的办公场所等。为了体现与其他 SSL 证书的不同，主流安全浏览器如 IE7 就会在用户访问部署了 EV SSL 证书的网站时把地址栏变成绿色，让用户对此网站的真实身份放心。

2、【Organization Validation SSL(OV SSL)】：GDCA 睿信 (OV) SSL 证书不仅验证域名所有权，同时要求用户提供营业执照和第三方证明文件等，证书中会显示申请单位的单位名称，支持中文单位名称的显示，方便在线用户查看 SSL 证书信息。用户查看 SSL 证书上的已经验证的信息就可以辨别网站真实性。

## 八、 网站部署更高级别的 EV SSL 证书有什么好处？

由于在线欺诈网站和钓鱼网站的猖獗，使得用户非常担心会身份被盗和被欺诈。在输入敏感机密信息（如用户名 / 密码、银行卡信息等）时，用户需要确信此网站是否可信、是否是所声称的单位的网站和是否加密传输其机密信息。如果不能得到明确的确认，用户会放弃使用网站服务。而 EV SSL 证书以绿色显示来明显地告诉用户此网站的身份已经通过严格验证，同时部署了 SSL 证书来加密机密信息，这样才能增强用户信心。

## 九、 EV SSL 证书的证书主题中会显示哪些信息？

EV SSL 证书的证书主题中会显示已经验证的所有信息，如机构名称、网站



域名、营业执照或组织机构代码证号、运营和注册地址等。

## 十、 SSL 证书支持多域名吗？

GDCA 恒信企业 EV(SSL)证书和睿信(OV) SSL 证书均支持多个域名；多域名证书不限域名类型。您只需购买一个多域名 SSL 证书就可满足多个域名使用。

## 十一、 浏览器是如何检查 SSL 证书正常工作的？

浏览器通过检查 SSL 是否由受信任的认证机构颁发，SSL 证书是否和域名匹配，SSL 证书是否过期或还未生效等方面来检测 SSL 证书是否正常工作。

## 十二、 为什么说部署自签 SSL 证书非常不安全？

自签证书即自建 PKI 系统做的 SSL 证书，是不受浏览器信任的，没有经过可靠验证机制的 SSL 证书，存在着许多的安全隐患。GDCA 自主研发的信鉴易® TrustAUTH® 系列 SSL 证书通过了全球最高标准的 WEBTRUST 认证体系，真正实现一证通行，全球信任！

## 十三、 为什么要选择 GDCA 的 SSL 证书？

GDCA 为国内首批获得工信部颁发《电子认证服务许可证》、并通过 webtrust 国际认证的权威第三方电子认证机构，自主研发的信鉴易® TrustAUTH® 系列 SSL 证书具有以下优点：

### 1. 一证通行，全球信任

通过严格的 WebTrust、WebTrust EV 国际双认证，全球公信；

### 2. 根植国内，安全自主

国内审核验证签批，完美替代国外产品，品质保证安全可控；

### 3. 主流适用，支持中文

根证书预置微软操作系统，支持 IE 或 IE 内核的浏览器，支持中文显示；

### 4. 本地服务，保障无忧



本地化，多维度服务更懂您的需求，百万保险保障无忧！

#### 十四、 我的服务器更换、重装或者丢失了 SSL 证书怎么办？

如果您更换服务器，或服务器重装，可以把备份的 SSL 证书导入到新的服务器中即可。如果您找不到您的备份或其他原因，请联系我们为原域名重新颁发 SSL 证书。

#### 十五、 购买了 SSL 证书我可以无条件退款吗？

EV SSL 证书使用 30 天内可以无条件全额退款、全部 SSL 证书有效期内免费无限次重新颁发。

#### 十六、 如何查验 SSL 证书是否支持 SGC 强制 128 位加密技术？

SGC 技术(Server Gated Cryptography)是在现有的 SSL 证书标准基础上增加的一种增强密钥用法(EKU)，用户可以通过查看证书详细信息-增强型密钥算法来辨别 SSL 证书是否支持 SGC 或者通过证书部署后设置服务器强制要求 128 位加密来访问站点辨别。

#### 十七、 服务器上装上 SSL 证书会不会影响到速度和流量？

安装 SSL 证书因为要为每一个 SSL 连接实现加密和解密，会增加服务器 CPU 的处理负担，但一般不会影响太大。同时建议注意以下几点以减轻服务器的负担：

- (1) 仅为需要加密的页面使用 SSL，如 <https://www.domaincom/login.asp>，不要把所有页面都使用 <https://>，特别是访问量最大的首页；
- (2) 尽量不要在使用了 SSL 的页面上设计大块的图片文件和其他大文件，尽量使用简洁的文字页面。

如果网站的访问量非常大，则建议另外购买 SSL 加速卡来专门负责 SSL 加解密工作，可以完全不增加服务器任何负担，当然也可以另外增加服务器。



## 十八、 代码签名证书有哪几种？

GDCA 信鉴易 TrustAUTH® 证书系更主要有以下两种代码签名证书：

1、恒信（EV）代码签名证书：企业（EV）代码签名证书能使软件开发商对其软件代码进行数字签名，能确保用户通过互联网下载软件时，确信此代码没有被非法篡改和来源可信，从而保护了代码的完整性、保护了用户不会被病毒、恶意代码和间谍软件所侵害，同时也就保护了软件开发商的利益，使得软件开发商能安全快速地通过网络发布软件。

2、速信个人代码签名证书：个人代码签名证书可让软件开发者能对其开发的软件代码进行数字签名，能确保用户通过互联网下载时能确信此代码没有被非法篡改和来源可信，从而保护了代码的完整性、保护了用户不会被病毒、恶意代码和间谍软件所侵害；同时也保护了软件开发者的利益，使得软件开发者能安全快速地通过网络发布软件。

## 十九、 为什么需要代码签名证书？

代码签名证书可以确保软件发布后没有被非法篡改和非法加壳等，还可以验证发行商身份，确保软件来自确定的源，同时，代码签名证书可以让您的用户放心确信此代码确实是您开发的和是没有被非法修改和破坏的。

安装代码签名证书后，用户在下载之前可以查看到软件开发商的详细信息，同时可以看到此代码签名证书是通过权威的第三方（如：GDCA）认证的，是 Windows 可信任的根证书颁发的，是可信的，这样，您的用户就可以放心下载了。

## 二十、 我在申请代码签名证书时单位名称应该填中文还是英文？

中文名称和英文名称的唯一区别就在于显示发行商时是中文单位名称还是英文单位名称，根据您的单位面向的用户群体来决定。



## 二十一、 如果改变了硬件、软件（web server）证书需要重新申请吗？

服务器证书与硬件无关，系统和 web server 版本如果相同也不会有任何影响。如果改变了服务器软件，证书就要重新申请，服务器证书不可以更换平台使用。

## 二十二、 物理服务器出现故障对 SSL 证书使用会有什么影响？

在您申请服务器证书后，请及时备份您的证书(私钥, 公钥)如果物理服务器出现故障只需要将备份的证书配置到新的服务器上就可以了，不会对证书的使用造成影响。

## 二十三、 我申请的 GDCA 的 SSL 证书需要多久才能签发？

只要您按要求提交了完整准确的申请资料并完成审核签发前的全部申请流程；根据您申请的证书品种一般会在 1-7 个工作日内完成签发，审核工作需要准确无误并为您和用户负责，我们会努力加快进度。

## 二十四、 GDCA 的 SSL 证书与国外品牌 SSL 证书有什么区别？

GDCA 的信鉴易® TrustAUTH® 系列 SSL 证书通过了全球最高标准的 WEBTRUST 认证体系，品质保证可完全实现进口替代，国内自主签批，安全更有保障，证书支持中文显示；本地化服务响应更及时服务更到位，当然价格更实在，你懂得！

