文档中心

SSL证书管理 USSL

产品文档

优刻得科技股份有限公司 版权所有

目录

Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

概览

Copyright © 2012-2021 UCloud 优刻得

    - DV类型申请
    - OV/EV类型申请
- 操作指南
    - 购买证书
    - 补全信息
    - 验证身份
    - 吊销证书
    - 证书退费
    - 个人中心
    - 证书托管
- 产品价格
- 证书部署
    - Nginx部署
    - Tomcat8.5/Tomcat9的证书部署
    - Apache2.x证书部署
    - JBoss证书部署
    - IIS服务器证书部署
- FAQ
    - Trustasia免费/DV证书验证常见问题
    - 续费证书的申请流程和部署
    - 免费证书验证匹配，但一直未颁发
    - 证书订单被拒绝
    - 证书吊销流程和注意点
    - 证书申请失败原因排查
    - 证书格式转换
    - 证书申请中文域名
    - 证书申请时的验证限制
    - 如何验证域名所有权

Copyright © 2012-2021 UCloud 优刻得

- 证书的颁发时间说明
- 证书退费说明
- SSL证书重颁发声明
- https字样并非呈现绿色
- DV证书自主检测工具手册
- SSL证书过期了怎么办?
- 证书正常安装后提示不安全
- 证书格式的区别
- 为App部署SSL证书应对苹果ATS限制
- 苹果公司宣布Safari浏览器对SSL证书有效期的要求说明
- 多年期证书说明
- 免费证书配额说明

Copyright © 2012-2021 UCloud 优刻得

产品概述

UCloud新上线的“SSL证书服务”与亚洲诚信、上海CA等多家权威证书机构合作，为云上用户提供SSL证书购买、认证、颁布、部署、管理等一站式服务。

SSL技术原理

SSL是指安全套接层协议（以及传输层协议TLS），位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持，是目前使用最广泛的安全协议。它为互联网或内部网络连接，进行操作的两台机器之间提供安全信息通道，即HTTPS。

SSL证书的重要性

在互联网发展之初http协议被发明并被广泛应用，但创始人Ted Nelson并未考虑到信息传输安全性的问题，这就给以后的互联网信息安全埋了个“雷”。http协议通过明文传输，无法保障数据传输过程中的安全性，导致数据泄露，数据篡改，流量劫持，钓鱼攻击等安全问题频频发生，为解决这一安全问题，https协议产生，通过数据加密传输及身份验证双重保障让数据在传输过程中不被泄露，篡改。因此，云服务中SSL证书是保障信息传输安全的必备产品。

安装SSL证书后，用户访问网站期间通过识别证书所有者身份信息，确认网站的真实性，从而确保站点识别钓鱼网站。而数据传输期间可以建立起安全的信息传输加密通道，保证信息传输的机密性。保护用户账户安全，避免信息泄露及防止信息篡改。有效的解决中间人劫持的困扰，杜绝搜索结果页被篡改及强行插入弹窗或嵌入式广告等问题的发生，防止推广流量流失，大大降低了推广成本。

Copyright © 2012-2021 UCloud 优刻得

免费和收费证书的区别

一、什么是免费证书

免费证书即为免费型DV SSL证书，最多保护一个完整的域名（如: buy.example.com，或next.buy.example.com, 各个明细子域名都算一个完整的域名），不支持通配符。免费SSL证书只验证域名信息，签发速度非常快。

二、什么是付费证书

付费SSL证书主要分为企业型 OV-SSL 证书和增强型 EV-SSL 证书两大类，这些证书对申请者都需要做严格的身份审核验证，需要提供可信身份证明。签发时间一般在3至15个工作日。

三、两者的共同点

1、全球信任，支持各类浏览器和移动设备；

2、支持SHA256签名算法；

四、两者的区别

Copyright © 2012-2021 UCloud 优刻得

1、严格的身份审核验证：免费的SSL证书不需要提供可信的身份证明，付费的SSL证书需要严格的身份审核验证过程。

身份验证的作用是用户可对网站的真实进行验证，可帮助用户辨明网站的真实身份，免受中间的攻击或误入钓鱼网站，建立用户对网站真实性的信任。

2、安全保险：免费SSL证书无安全保险；收费SSL证书可最高享受175万美元的安全保险；

3、设备兼容性：免费SSL证书的设备兼容性一般；收费SSL证书的设备兼容性较好。

五、适用范围

免费SSL证书：适合微小企业/个人网站/API服务，能满足网站部分基本的加密要求；

付费SSL证书：适合企业官网/金融平台/政府机关；

付费SSL证书不仅具备高强度信息加密传输功能，而且所有浏览器均支持。能在证书信息中显示企业真实身份信息，向网站用户展示网站品牌形象，提升网站转化率，企业部署SSL证书目的就在于保护网站安全，涉及到用户信息、数据资料、在线交易、证券、金融等领域的网站最好一律使用付费证书。

Copyright © 2012-2021 UCloud 优刻得

证书品牌和证书类型

SSL证书品牌主要提供四种，TrustAsia证书、UniTrust 证书、GeoTrust证书以及Digcert（原Symantec，已更名）证书。

1. Digicert公司是全球领先的数字证书认证机构，部署赛门铁克证书可激活互联网最受信任的诺顿安全签章。

2. GeoTrust公司是全球知名的数字证书颁发机构，是Digcert旗下性价比品牌。

3. 亚洲诚信公司是一家专业为各行业提供国际证书和自主产权证书的公司。

4. CFCA即中国金融认证中心，是由中国人民银行于1998年牵头组建，经国家信息安全管理机构批准成立的权威电子认证机构。

5. UniTrust隶属于上海市数字证书认证中心有限公司(简称上海 CA，SHECA)是中央密码工作领导小组批准的唯一试点，国内第一家专业的第三方电子认证服务机构。

Copyright © 2012-2021 UCloud 优刻得

选择证书类型

证书颁发机构（CA）提供三种不同的服务器验证方式，对应三种信任级别的SSL证书：域名型DV SSL证书、企业型OV SSL证书和增强型EV SSL证书。其中只有OV SSL证书和EV SSL证书才能真正帮助企业实现安全与可信，这也是PCI安全标准委员会推荐这两类证书的主要原因。

1 DV SSL证书，域名型SSL证书，能起到基本的信息传输加密功能，验证基本的域名管理权。CA只审核域名的所有权，申请过程系统自动完成，所以DV证书往往价格很低，甚至免费。

2 OV SSL证书，即组织型或机构型证书。OV型证书显然适用于企业、政府等机构。OV证书不仅具备加密传输和身份验证的完整功能，价格也比较便宜，而且签发便捷。

3 EV SSL证书，即增强型SSL证书，企业型证书的升级版。在原有加密性和验证身份的基础上，加强了防假冒网站功能，在功能和效果上更强大。

Copyright © 2012-2021 UCloud 优刻得

Digicert（原Symantec）证书对比

Symantec.	增强型EV-SSL证书 专业版	增强型EV-SSL证书	企业型SSL证书 专业版	企业型SSL证书	企业型通配符SSL证书
信任等级	4	4	3	3	3
安全性等级	4	3	4	2	2
绿色地址栏	✓	✓			
扩展审核	✓	✓			
安全签章	Norton SECURED powered by Symantec	Norton SECURED powered by Symantec	Norton SECURED powered by Symantec	Norton SECURED powered by Symantec	Norton SECURED powered by Symantec
企业身份审核	✓	✓	✓	✓	✓
漏洞评估服务	✓	✓	✓		
网站恶意软件扫描	✓	✓	✓	✓	✓
Seal-in-Search	✓	✓	✓	✓	✓

Copyright © 2012-2021 UCloud 优刻得

颁发周期	7-15个工作日	7-15个工作日	7-15个工作日	7-15个工作日	7-15个工作日
加密强度	支持高达256位	支持高达256位	支持高达256位	支持高达256位	支持高达256位
算法支持	ECC/RSA	RSA	ECC/RSA	RSA	RSA
公钥长度	ECC(256位以上)	RSA(2048位以上)	ECC(256位以上)	RSA(2048位以上)	RSA(2048位以上)
赔付保障	175万美元	175万美元	175万美元	150万美元	150万美元
主流浏览器支持	✔	✔	✔	✔	✔
移动设备支持	✔	✔	✔	✔	✔
客户服务支持	✔	✔	✔	✔	✔
SAN (UC) 支持	✔	✔	✔	✔	
通配符支持					✔
IDN支持	✔	✔	✔	✔	✔
TrustAsia安装检查	✔	✔	✔	✔	✔

Copyright © 2012-2021 UCloud 优刻得

TrustAsia状态监测	✔	✔	✔	✔	✔

Copyright © 2012-2021 UCloud 优刻得

GeoTrust证书对比

GeoTrust	增强型EV SSL证书	企业型SSL证书
信任等级		
安全性等级		
绿色地址栏	✓	
扩展审核	✓	
安全签章		
企业身份审核	✓	✓
颁发周期	7-15个工作日	3-5个工作日
加密强度	支持高达256位	支持高达256位
公钥长度	RSA(2048位以上)	RSA(2048位以上)
赔付保障	150万美元	125万美元

Copyright © 2012-2021 UCloud 优刻得

赔付保障	150万美元	125万美元
主流浏览器支持	✔	✔
移动设备支持	✔	✔
客户服务支持	✔	✔
SAN (UC) 支持	✔	✔
IDN支持	✔	✔
TrustAsia安装检查	✔	✔
TrustAsia状态监测	✔	✔
免费重新颁发	✔	✔
OCSP	✔	✔

Copyright © 2012-2021 UCloud 优刻得

TrustAsia证书对比

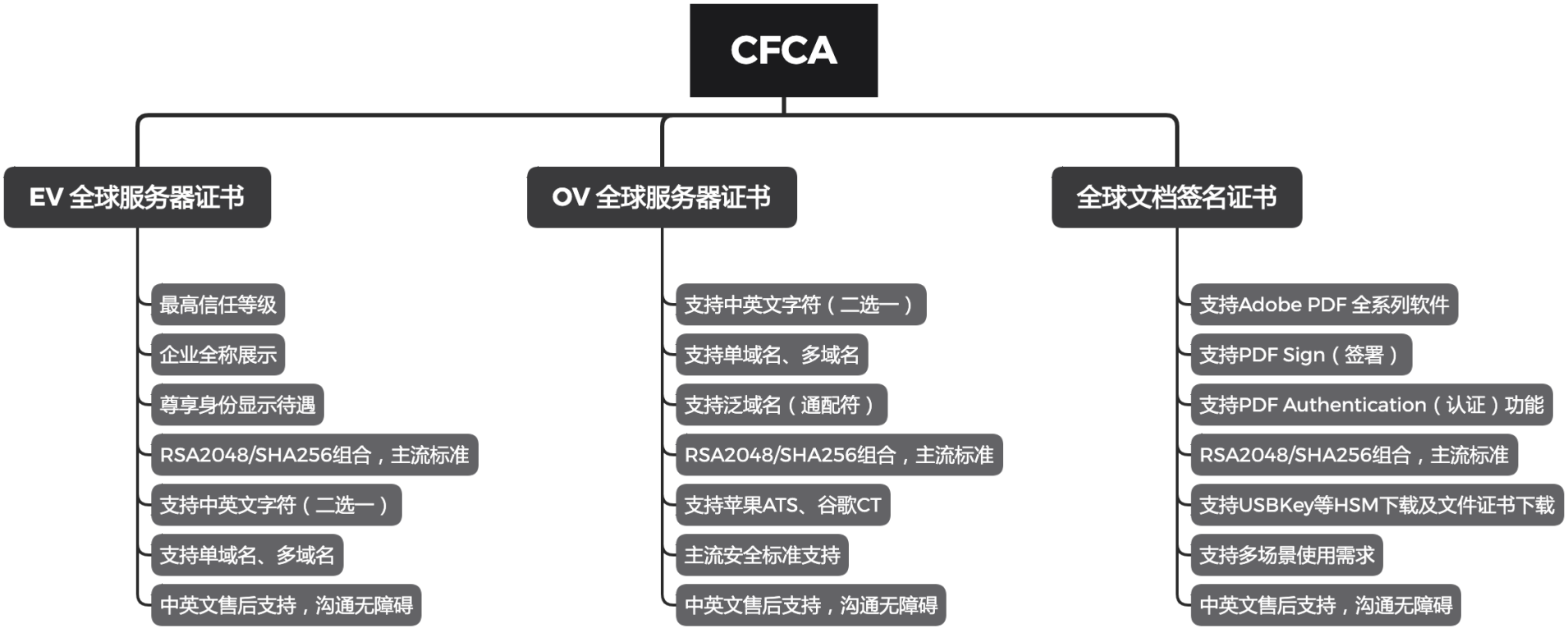
	TrustAsia DV 单域名证书	TrustAsia DV 多域名证书	TrustAsia DV 通配符证书
信任等级	域名级	域名级	域名级
审核内容	验证域名所有权	验证域名所有权	验证域名所有权
颁发时间	10～15分钟	10～15分钟	10～15分钟
浏览器呈现	绿色小锁＋https https://www.	绿色小锁＋https https://www.	绿色小锁＋https https://www.
加密强度	128位到256位自适应	128位到256位自适应	128位到256位自适应
浏览器兼容性	支持99.9% 桌面和移动浏览器	支持99.9% 桌面和移动浏览器	支持99.9% 桌面和移动浏览器
浏览器兼容性列表 - 浏览器与应用	Google Chrome	Google Chrome	Google Chrome
	Microsoft IE 5.01+	Microsoft IE 5.01+	Microsoft IE 5.01+
	Mozilla Firefox 1.0+	Mozilla Firefox 1.0+	Mozilla Firefox 1.0+
	AOL 5+	AOL 5+	AOL 5+
	Apple Safari 1.0+	Apple Safari 1.0+	Apple Safari 1.0+
	Netscape 7.1+	Netscape 7.1+	Netscape 7.1+
	Java 1.4.2+	Java 1.4.2+	Java 1.4.2+
浏览器兼容性列表 - 系统与设备	Android 2.3+	Android 2.3+	Android 2.3+
	Apple iOS 3.0+	Apple iOS 3.0+	Apple iOS 3.0+
	Windows Phone 7+	Windows Phone 7+	Windows Phone 7+
	Blackberry 5+	Blackberry 5+	Blackberry 5+
	Windows 2000+	Windows 2000+	Windows 2000+
	Apple OS X 10.5+	Apple OS X 10.5+	Apple OS X 10.5+

Copyright © 2012-2021 UCloud 优刻得

浏览器兼容性 Demo:https://www.v2ex.com			
根证书Symantec G5	Symantec 根证书认证颁发	Symantec 根证书认证颁发	Symantec 根证书认证颁发
重颁发	免费	免费	免费
免服务器授权	无授权限制	无授权限制	无授权限制
客户服务支持	邮件，电话，在线客服	邮件，电话，在线客服	邮件，电话，在线客服
IDN（中文域名）支持	支持	支持	支持
TrustAsia安装检查	支持	支持	支持
TrustAsia状态检测	支持	支持	支持

Copyright © 2012-2021 UCloud 优刻得

CFCA证书对比



Copyright © 2012-2021 UCloud 优刻得

Digicert增强型EV-SSL证书专业版

包括：扩展验证、绿色地址栏，从最低 128 位到 256 位的加密、价值 1,750,000 美元的保障以及漏洞评估服务。

绿色地址栏

EVSSL证书可以让客户更加确信：他们在与信任的网站进行交易，网站的信息都是安全的。EV SSL 证书可以触发高级别安全网络浏览器在绿色地址栏中显示贵公司的名称，以及颁发该证书的证书颁发机构的名称。证书颁发机构采用经过审核的严格身份验证方法，加上浏览器对显示的内容加以控制，因此使网页仿冒者和造假者难以劫持您的品牌和客户。

ECC算法

ECC 具有更好的安全性，性能更佳：相比目前采用的加密方法，它可以提供更好的保护，而所用密钥长度更短（例如，256 位的 ECC 密钥即可提供与 3,072 位 RSA 密钥相同的安全水平）。结果怎么样呢?更好的安全性，能够满足移动设备和平板电脑连接爆炸式增长的需求。

漏洞评估功能

Digicert漏洞扫描功能旨在检测最常见的攻击最常使用的入口点。漏洞报告则根据漏洞的类型和危险性对其加以分类，并提出相应的纠正措施。该组合有助于企业快速识别关键的漏洞并加以补救，从而更轻松地保护网站。

恶意代码扫描

恶意代码隐藏在您网站的源代码中，如果不逐行进行分析，很难被检测到，有些恶意软件通过页面显示的方式激活。您使用Symantec SSL证书保护网站时，我们免费包含了针对公共网页的每日恶意软件扫描服务。如果检测到恶意软件，它就会将您定向到受感染页面的列表，并就导致该问题的代码向您发送通知。

诺顿签章功能

诺顿安全认证签章是互联网上受信任的标记，每天在 170 个国家或地区的网站上显示 5 亿多次。Digicert Seal-in-Search 在启用了免费插件的浏览器和合作伙伴购物网站上以及产品评测页面上您链接的旁边显示诺顿安全认证签章。

Seal-in-Search

Copyright © 2012-2021 UCloud 优刻得

客户在线浏览时，他们通常会发现长长的网站列表，各网站为争取业务而相互竞争。Digicert Seal-in-Search 是 Digicert SSL 证书 的一项功能，可将诺顿安全认证签章放置在搜索结果中您链接的旁边，证明您的网站为Digicert所信任。

WebTrust国际安全审计认证

WebTrust是由全球两大著名注册会计师协会AICPA（美国注册会计师协会）和CICA（加拿大注册会计师协会）共同制定的安全审计标准，主要对互联网服务商的系统及业务运作逻辑安全性、保密性等共计七项内容进行近乎严苛的审查和鉴证。

中文语言支持

身份审核可以直接使用中文企业营业执照，而且证书可以支持中文名称显示，在网站安全签章中也可以显示出企业的中文信息，方便客户识别网站的真实性和安全性。

多域名支持

主题备用名称（SAN）证书使用单个 SSL 证书保护多个域名，SAN 证书常用于统一通信 (UC)，可以保护 Microsoft Exchange 2007 Server、Office Communications Server 2007 或 Mobile Device Manager 以及服务器名、Intranet 和本地名。SAN 也可用于：Intranet 中的服务器名（例如，“server.local”或“faxtool”）主机名（例如，mailserver）。

Copyright © 2012-2021 UCloud 优刻得

Digicert增强型EV-SSL证书

吸引更多客户访问您的网站，并给予他们完成交易的信心。

包括：扩展验证、绿色地址栏、最高 256 位加密、价值 1,750,000 美元的保障以及漏洞评估服务。

绿色地址栏

EVSSL证书可以让客户更加确信：他们在与信任的网站进行交易，网站的信息都是安全的。EV SSL 证书可以触发高级别安全网络浏览器在绿色地址栏中显示贵公司的名称，以及颁发该证书的证书颁发机构的名称。证书颁发机构采用经过审核的严格身份验证方法，加上浏览器对显示的内容加以控制，因此使网页仿冒者和造假者难以劫持您的品牌和客户。

漏洞评估功能

Digicert漏洞扫描功能旨在检测常见的攻击最常使用的入口点。漏洞报告则根据漏洞的类型和危险性对其加以分类，并提出相应的纠正措施。该组合有助于企业快速识别关键的漏洞并加以补救，从而更轻松地保护网站。

恶意代码扫描

恶意代码隐藏在您网站的源代码中，如果不逐行进行分析，很难被检测到，有些恶意软件通过页面显示的方式激活。您使用Digicert SSL证书保护网站时，我们免费包含了针对公共网页的每日恶意软件扫描服务。如果检测到恶意软件，它就会将您定向到受感染页面的列表，并就导致该问题的代码向您发送通知。

诺顿签章功能

诺顿安全认证签章是互联网上受信任的标记，每天在 170 个国家或地区的网站上显示 5 亿多次。Digicert Seal-in-Search 在启用了免费插件的浏览器和合作伙伴购物网站上以及产品评测页面上您链接的旁边显示诺顿安全认证签章。

Seal-in-Search

客户在线浏览时，他们通常会发现长长的网站列表，各网站为争取业务而相互竞争。Digicert Seal-in-Search 是 Digicert SSL 证书 的一项功能，可将诺顿安全认证签章放置在搜索结果中您链接的旁边，证明您的网站为Symantec所信任。

Copyright © 2012-2021 UCloud 优刻得

WebTrust国际安全审计认证

WebTrust是由全球两大著名注册会计师协会AICPA（美国注册会计师协会）和CICA（加拿大注册会计师协会）共同制定的安全审计标准，主要对互联网服务商的系统及业务运作逻辑安全性、保密性等共计七项内容进行近乎严苛的审查和鉴证。

中文语言支持

身份审核可以直接使用中文企业营业执照，而且证书可以支持中文名称显示，在网站安全签章中也可以显示出企业的中文信息，方便客户识别网站的真实性和安全性。

多域名支持

主题备用名称（SAN）证书使用单个 SSL 证书保护多个域名，SAN 证书常用于统一通信 (UC)，可以保护 Microsoft Exchange 2007 Server、Office Communications Server 2007 或 Mobile Device Manager 以及服务器名、Intranet 和本地名。SAN 也可用于：Intranet 中的服务器名（例如，“server.local”或“faxtool”）主机名（例如，mailserver）。

主要特点

- 全面的企业身份验证和域名所有权验证
- 最高支持256位加密强度可为在线数据传输提供安全保障
- 激活浏览器绿色地址栏，显示网站经营者的真实企业身份用以阻止钓鱼网站
- 支持所有浏览器和移动设备
- 价值175万美元赔付保障
- Digicert是早期通过WebTrust认证的服务商之一
- Digicert诺顿安全认证签章，网站恶意软件扫描向客户证明您致力于保障他们的安全
- Digicert漏洞评估服务可防止您的站点遭受黑客攻击
- 支持“数字证书.com”和“数字证书.中国”等类型多语言域名
- 证书有效期内免费提供证书补发服务
- TrustAsia提供完善的本土化电话和电子邮件技术支持
- TrustAsia SSL证书运行状态监控服务
- 一次购买多年可享受优惠折扣

Copyright © 2012-2021 UCloud 优刻得

Digicert企业型通配符SSL证书

Digicert企业型通配符SSL证书(Digicert Secure Site Wildcard SSL Certificates) 提供40位至256位加密来保障您网站数据传输的安全,完整的企业真实身份和域名所有权审核，互联网上受认可的信任标记 Norton Secured Seal(诺顿安全认证签章)以及恶意软件扫描，确保网站身份真实可靠。

恶意代码扫描

恶意代码隐藏在您网站的源代码中,如果不逐行进行分析,很难被检测到,有些恶意软件通过页面显示的方式激活。您使用Digicert SSL证书保护网站时,我们免费包含了针对公共网页的每日恶意软件扫描服务。如果检测到恶意软件,它就会将您定向到受感染页面的列表,并就导致该问题的代码向您发送通知。

诺顿签章功能

诺顿安全认证签章是互联网上受信任的标记,每天在 170 个国家或地区的网站上显示 5 亿多次。Digicert Seal-in-Search 在启用了免费插件的浏览器和合作伙伴购物网站上以及产品评测页面上您链接的旁边显示诺顿安全认证签章。

Seal-in-Search

客户在线浏览时,他们通常会发现长长的网站列表,各网站为争取业务而相互竞争。Digicert Seal-in-Search 是 Digicert SSL 证书 的一项功能,可将诺顿安全认证签章放置在搜索结果中您链接的旁边,证明您的网站为Digcert所信任。

WebTrust国际安全审计认证

WebTrust是由全球两大著名注册会计师协会AICPA(美国注册会计师协会)和CICA(加拿大注册会计师协会)共同制定的安全审计标准,主要对互联网服务商的系统及业务运作逻辑安全性、保密性等共计七项内容进行近乎严苛的审查和鉴证。

中文语言支持

身份审核可以直接使用中文企业营业执照,而且证书可以支持中文名称显示,在网站安全签章中也可以显示出企业的中文信息,方便客户识别网站的真实性和安全性。

Copyright © 2012-2021 UCloud 优刻得

Digicert企业型SSL证书专业版

Digicert企业型SSL证书专业版(Digicert Secure Site Pro SSL Certificates) 提供了真正128位至256位加密来保障您网站数据传输的安全,完整的企业真实身份和域名所有权审核,互联网上受认可的信任标记 Norton Secured Seal(诺顿安全认证签章),漏洞评估服务以及网站恶意软件扫描,可以帮您采取措施防御关键的网站漏洞。

ECC算法

ECC 具有更好的安全性,性能更佳:相比目前采用的加密方法,它可以提供更好的保护,而所用密钥长度更短(例如,256 位的 ECC 密钥即可提供与 3,072 位 RSA 密钥相同的安全水平)。结果怎么样呢?更好的安全性,能够满足移动设备和平板电脑连接爆炸式增长的需求。

漏洞评估功能

漏洞报告则根据漏洞的类型和危险性对其加以分类,并提出相应的纠正措施。该组合有助于企业快速识别关键的漏洞并加以补救,从而更轻松地保护网站。

恶意代码扫描

恶意代码隐藏在您网站的源代码中,如果不逐行进行分析,很难被检测到,有些恶意软件通过页面显示的方式激活。您使用Digicert SSL证书保护网站时,我们免费包含了针对公共网页的每日恶意软件扫描服务。如果检测到恶意软件,它就会将您定向到受感染页面的列表,并就导致该问题的代码向您发送通知。

诺顿签章功能

诺顿安全认证签章是互联网上受信任的标记,每天在 170 个国家或地区的网站上显示 5 亿多次。Digicert Seal-in-Search 在启用了免费插件的浏览器和合作伙伴购物网站上以及产品评测页面上您链接的旁边显示诺顿安全认证签章。

Seal-in-Search

客户在线浏览时,他们通常会发现长长的网站列表,各网站为争取业务而相互竞争。Digicert Seal-in-Search 是 Digcert SSL 证书 的一项功能,可将诺顿安全认证签章放置在搜索结果中您链接的旁边,证明您的网站为Digicert所信任。

WebTrust国际安全审计认证

Copyright © 2012-2021 UCloud 优刻得

WebTrust是由全球两大著名注册会计师协会AICPA（美国注册会计师协会）和CICA（加拿大注册会计师协会）共同制定的安全审计标准，主要对互联网服务商的系统及业务运作逻辑安全性、保密性等共计七项内容进行近乎严苛的审查和鉴证。

中文语言支持

身份审核可以直接使用中文企业营业执照，而且证书可以支持中文名称显示，在网站安全签章中也可以显示出企业的中文信息，方便客户识别网站的真实性和安全性。

Copyright © 2012-2021 UCloud 优刻得

Digicert企业型SSL证书

Digicert企业型SSL证书(Digicert Secure Site SSL Certificates) 提供40位至256位加密来保障您网站数据传输的安全,完整的企业真实身份和域名所有权审核,信任标记 Norton Secured Seal(诺顿安全认证签章)以及恶意软件扫描,确保网站身份真实可靠。

恶意代码扫描

恶意代码隐藏在您网站的源代码中,如果不逐行进行分析,很难被检测到,有些恶意软件通过页面显示的方式激活。您使用Digicert SSL证书保护网站时,我们免费包含了针对公共网页的每日恶意软件扫描服务。如果检测到恶意软件,它就会将您定向到受感染页面的列表,并就导致该问题的代码向您发送通知。

诺顿签章功能

诺顿安全认证签章是互联网上受信任的标记,每天在 170 个国家或地区的网站上显示 5 亿多次。Digicert Seal-in-Search 在启用了免费插件的浏览器和合作伙伴购物网站上以及产品评测页面上您链接的旁边显示诺顿安全认证签章。

Seal-in-Search

客户在线浏览时,他们通常会发现长长的网站列表,各网站为争取业务而相互竞争。Digicert Seal-in-Search 是 Digicert SSL 证书 的一项功能,可将诺顿安全认证签章放置在搜索结果中您链接的旁边,证明您的网站为Digicert所信任。

中文语言支持

身份审核可以直接使用中文企业营业执照,而且证书可以支持中文名称显示,在网站安全签章中也可以显示出企业的中文信息,方便客户识别网站的真实性和安全性。

多域名支持

主题备用名称(SAN)证书使用单个 SSL 证书保护多个域名,SAN 证书常用于统一通信 (UC),可以保护 Microsoft Exchange 2007 Server、Office Communications Server 2007 或 Mobile Device Manager 以及服务器名、Intranet 和本地名。SAN 也可用于:Intranet 中的服务器名(例如,“server.local”或“faxtool”)主机名(例如,mailserver)。

Copyright © 2012-2021 UCloud 优刻得

GeoTrust增强型EV-SSL证书

增强型EV-SSL证书 吸引更多客户访问您的网站，并给予他们完成交易的信心。包括：扩展验证、绿色地址栏、价值 1,500,00 美元的保障以及安全签章。

绿色地址栏

EVSSL证书可以让客户更加确信：他们在与信任的网站进行交易，网站的信息都是安全的。EV SSL 证书可以触发高级别安全网络浏览器在绿色地址栏中显示贵公司的名称，以及颁发该证书的证书颁发机构的名称。证书颁发机构采用经过审核的严格身份验证方法，加上浏览器对显示的内容加以控制，因此使网页仿冒者和造假者难以劫持您的品牌和客户。

安全网站签章

拥有 GeoTrust域名型SSL证书的同时，您还可同时拥有了一个网站安全签章。将该标志放在网站上，可以时刻提醒在线用户，所有在线提交的数据信息正在受到高强度的加密传输保护。更为重要的是，GeoTrust安全网站签章的技术可以确保该标志不会被假冒或钓鱼网站非法使用。

WebTrust国际安全审计认证

WebTrust是由全球两大著名注册会计师协会AICPA（美国注册会计师协会）和CICA（加拿大注册会计师协会）共同制定的安全审计标准，主要对互联网服务商的系统及业务运作逻辑安全性、保密性等共计七项内容进行近乎严苛的审查和鉴证。

中文语言支持

身份审核可以直接使用中文企业营业执照，而且证书可以支持中文名称显示，在网站安全签章中也可以显示出企业的中文信息，方便客户识别网站的真实性和安全性。

Copyright © 2012-2021 UCloud 优刻得

GeoTrust企业型通配符SSL证书

使用一张通配符证书即可保护您所有的下级子级域名，并且没有数量限制，可随时根据需要添加下级子级域名，节省您的时间与管理成本。

安全网站签章

拥有 GeoTrust域名型SSL证书的同时，您还可同时拥有了一个网站安全签章。将该标志放在网站上，可以时刻提醒在线用户，所有在线提交的数据信息正在受到高强度的加密传输保护。更为重要的是，GeoTrust安全网站签章的技术可以确保该标志不会被假冒或钓鱼网站非法使用。

WebTrust国际安全审计认证

WebTrust是由全球两大著名注册会计师协会AICPA（美国注册会计师协会）和CICA（加拿大注册会计师协会）共同制定的安全审计标准，主要对互联网服务商的系统及业务运作逻辑安全性、保密性等共计七项内容进行近乎严苛的审查和鉴证。

中文语言支持

身份审核可以直接使用中文企业营业执照，而且证书可以支持中文名称显示，在网站安全签章中也可以显示出企业的中文信息，方便客户识别网站的真实性和安全性。

主要特色

- 企业身份验证和域名所有权验证
- 支持256位加密强度，可为在线数据传输提供安全保障
- 支持所有主流浏览器和移动设备
- 价值125万美元赔付保障
- 一张证书同时保护多个子域名
- GeoTrust安全网站动态签章，向客户证明您致力于保障他们的安全
- 证书有效期内免费提供证书补发服务

Copyright © 2012-2021 UCloud 优刻得

- TrustAsia提供完善的本土化电话和电子邮件技术支持
- TrustAsia SSL证书运行状态监控服务
- 一次购买多年可享受优惠折扣

Copyright © 2012-2021 UCloud 优刻得

GeoTrust企业型SSL证书

True BusinessID是集SSL加密技术和身份认证于一体的SSL证书服务包，意味着为您和您的客户提供了更高等级的安全保护，这样会大大提高您网站的可信度，从而增加您的商业效益和收入。

安全网站签章

拥有 GeoTrust域名型SSL证书的同时，您还可同时拥有了一个网站安全签章。将该标志放在网站上，可以时刻提醒在线用户，所有在线提交的数据信息正在受到高强度的加密传输保护。更为重要的是，GeoTrust安全网站签章的技术可以确保该标志不会被假冒或钓鱼网站非法使用。

WebTrust国际安全审计认证

WebTrust是由全球两大著名注册会计师协会AICPA（美国注册会计师协会）和CICA（加拿大注册会计师协会）共同制定的安全审计标准，主要对互联网服务商的系统及业务运作逻辑安全性、保密性等共计七项内容进行近乎严苛的审查和鉴证。

中文语言支持

身份审核可以直接使用中文企业营业执照，而且证书可以支持中文名称显示，在网站安全签章中也可以显示出企业的中文信息，方便客户识别网站的真实性和安全性。

主要特点

- 企业身份验证和域名所有权验证
- 支持256位加密强度可为在线数据传输提供安全保障
- 支持所有主流浏览器和移动设备
- 价值125万美元赔付保障
- 可同时保护您的www和非www网站
- 支持SAN（UC）多域名（可选服务）

Copyright © 2012-2021 UCloud 优刻得

- GeoTrust安全网站动态签章,向客户证明您致力于保障他们的安全
- GeoTrust是WebTrust认证的服务商之一
- 证书有效期内免费提供证书补发服务
- TrustAsia提供完善的本土化电话和电子邮件技术支持
- TrustAsia SSL证书运行状态监控服务
- 一次购买多年可享受优惠折扣

Copyright © 2012-2021 UCloud 优刻得

TrustAsia 域名型证书

TrustAsia域名型单域名证书

TrustAsia提供的服务器SSL证书能使您的客户与您的网站之间进行安全数据传输，确保交易的安全性和完整性。TrustAsia域名型SSL证书支持128/256位加密，有着非常高的性价比。

主要特点

- 10分钟快速颁发
- 灵活的验证方式文件、DNS
- 全球可信，兼容所有客户端
- 支持HASH256算法
- 完善的技术支持服务
- Symantec根证书
- 免费重新颁发

TrustAsia域名型多域名证书

TrustAsia提供的服务器SSL证书能使您的客户与您的网站之间进行安全数据传输，确保交易的安全性和完整性。TrustAsia域名型SSL证书支持128/256位加密，有着非常高的性价比。

- 10分钟快速颁发
- 灵活的验证方式文件、DNS
- 全球可信，几乎兼容所有客户端
- 支持全新的HASH256算法
- 提供技术支持服务

Copyright © 2012-2021 UCloud 优刻得

- Symantec根证书
- 免费重新颁发
- 最高支持100个域名
- 可以支持不同主域
- 不支持通配符，必须是单域名

TrustAsia域名型通配符证书

功能和特点与单域一致，区别在于允许添加域名通配符。

- 10分钟快速颁发
- 灵活的验证方式文件、DNS
- 全球可信，几乎兼容所有客户端
- 支持全新的HASH256算法
- 提供技术支持服务
- 免费重新颁发
- 可保护同域下同级所有子域名
- Symantec根证书
- 免费支持上级主域

Copyright © 2012-2021 UCloud 优刻得

TrustAsia国密证书

国密算法SSL证书是基于国家根颁发的可信服务器证书，遵循国密规范标准，使用国密的签名证书及加密证书和国密套件进行HTTPS SSL加密通信，可颁发单域名、多域名及通配符类型。国密算法通过加密和签名其兼容性等性能如下所示：

Copyright © 2012-2021 UCloud 优刻得

	国密算法 SSL 证书
证书功能解耦	加密证书+签名证书
算法	SM2/SM3
公钥长度	256
密钥保护	签名私钥硬件内保存（满足国家标准）
应用环境	支持国密算法的浏览器
发证速度	1-3个工作日
支持版本	单域名、多域名和通配符

主要特点

1、加密传输：

Copyright © 2012-2021 UCloud 优刻得

支持 SM2 国产密码算法和国密安全协议，实现高强度双向加密传输，防止传输数据被泄露或者篡改。

2、安全身份认证：

支持 SM2 国产密码算法和国密安全协议，实现高强度双向加密传输，防止传输数据被泄露或者篡改。

3、地址栏安全锁：

地址栏头部的“锁”型图标使您的访客放心浏览网页，提高用户信任度。

4、浏览器支持：

360 浏览器、密信浏览器和红莲花等国密浏览器可支持国密标准（SM2）证书，可使用 “双证书部署” 和 “自适应浏览器兼容” 方案来解决主流浏览器兼容的问题。

5、中文语言支持：

身份审核可以直接使用中文企业营业执照，而且证书可以支持中文名称显示，在网站安全签章中也可以显示出企业的中文信息，最大方便客户识别网站的真实性和安全性。

Copyright © 2012-2021 UCloud 优刻得

CFCA 证书

数字证书认证系统基于 PKI 关键技术，实现数字证书的申请、审核、签发、查询、发布，证书吊销列表的签发、查询、发布等全生命周期管理功能。CA 系统作为 CFCA 的主打服务，在第三方金融 CA 领域占据 90% 以上的市场份额，在 CA 领域广受赞誉。

证书产品特点

标准符合性：CFCA 数字证书认证系统完全基于 PKI 关键技术，遵照国密系列和 X509 系列标准。敏感数据的存储、传输和验证采用加密信息语法标准，使用密码设备的接口标准连接加密设备。

高稳定性：自 CFCA CA 系统上线五年以来 故障率为零。

易用性：系统提供简单清晰的 WEB 页面进行系统初始化和系统管理。系统只需简单配置就可以使用，同时系统提供完备的手册进行专业的指导。

可扩展性： 采用模块化设计，支持高并发、多级 CA 及交叉认证、用户自定义证书扩展、系统负载均衡。

平台独立性使用标准接口的不同厂家、不同型号的加密机、智能卡；支持 Oracle、SQL Server、DB2 等大型数据库产品；支持复合 LDAPv3 标准协议的目录服务器；系统采用纯 JAVA 开发，不受运行操作系统平台限制。

Copyright © 2012-2021 UCloud 优刻得

UniTrust 证书

万维信UniTrust隶属于上海市数字证书认证中心有限公司(简称上海 CA,SHECA)是中央密码工作领导小组批准的唯一试点,国内第一家专业的第三方电子认证服务机构。是首家将SM2根证书内置入360安全浏览器和统信UOS操作系统信创根证书库中的数字信任服务厂商。

获得工信部电子认证服务资质、国密局电子认证服务使用密码许可证、国密局电子政务电子认证服务资质,通过国家卫健委测试和复审,通过国际 WebTrust 认证、实现主流浏览器直接信任的机构,通过CMMI3认证、ISO9001认证、ISO27001认证。

Copyright © 2012-2021 UCloud 优刻得

证书快速申请指南

一、快速购买指导：

1、DV类型证书申请流程：

验证方式：只需dns/文件解析认证即可

签发时间：验证通过后最快20分钟（验证检测：控制台工具/手动解析/亚数工具），一般不超过24小时，，dv证书为系统自动签发，存在不签发的，如超过24小时建议购买OV/EV证书。

2、OV/EV证书申请流程：

验证方式： 第一步：企业认证（需上传PDF格式公司盖章确认函）

第二步：dns/文件解析认证（参考）

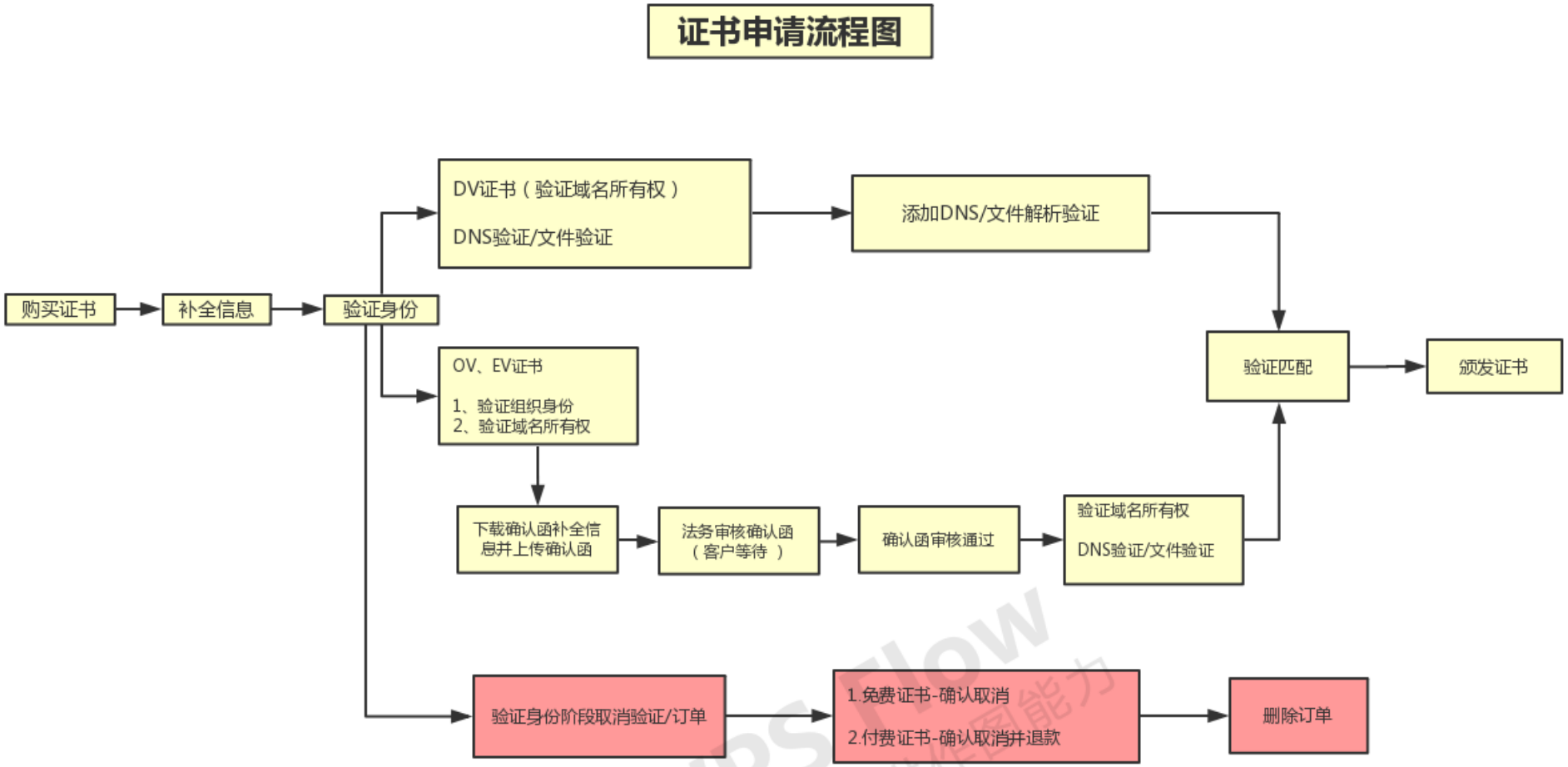
签发时间：3-7天签发，如需加急请联系产品负责人

3、证书注销流程

证书注销流程同购买流程，都需要二次验证，参考购买流程

Copyright © 2012-2021 UCloud 优刻得

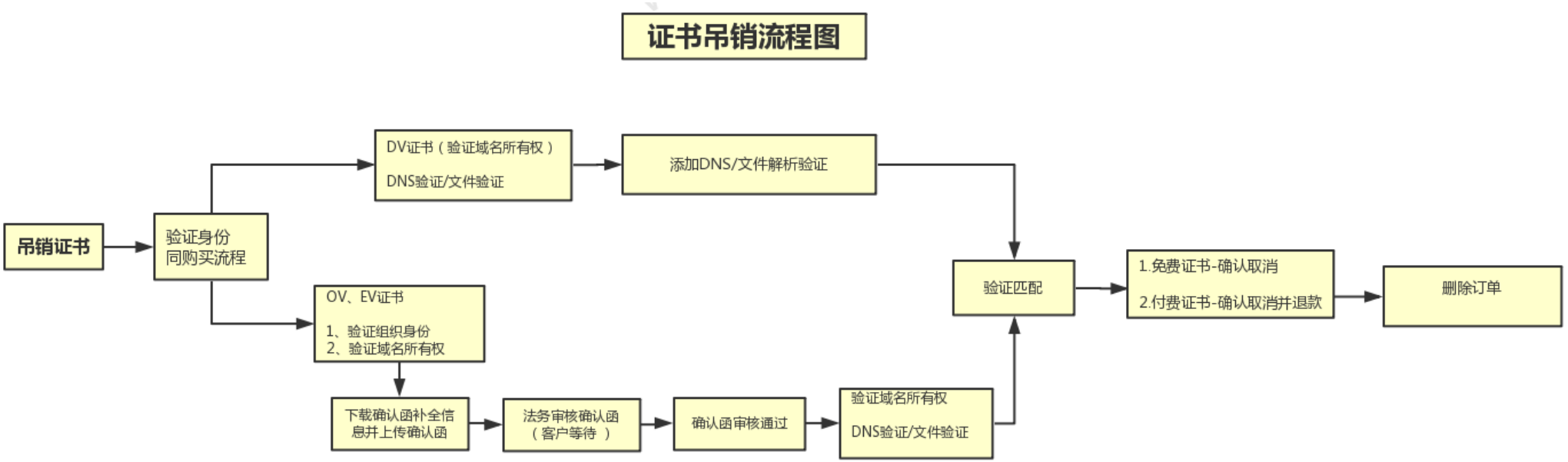
二、证书申请流程



三、证书注销流程

备注:针对已颁发证书,吊销流程同购买流程,都需要验证

Copyright © 2012-2021 UCloud 优刻得



Copyright © 2012-2021 UCloud 优刻得

域名型(DV)证书购买签发流程

流程总结：新购证书->补全信息->域名验证(DNS/文件验证)->验证通过->签发/等待签发证书

特别说明:验证检测通过后(建议手动检测),只需等待证书签发即可,dv证书为系统检测自行签发,存在不签发的情况;如24小时未签发,请购买ov/ev证书。

Step1：新购证书

ucloud首页->控制台->全部->证书管理 USSL>购买证书

Copyright © 2012-2021 UCloud 优刻得

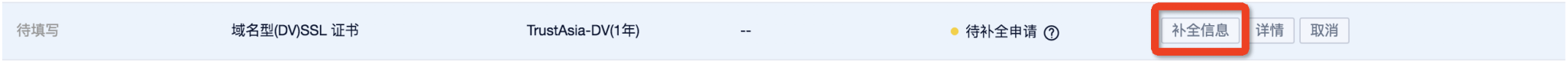
Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

详细内容参见购买证书介绍。

Step2：补全信息

购买后会看到生成了一条没有任何信息的待补全信息的证书，点击【补全信息】填写内容提交。



详细内容参见补全信息介绍。

Step3：域名所有权验证

验证按钮工具只是辅助客户验证的工具，不是最终证书签发的依据

客户解析配置是否正确可以借助手动解析来确认；如可获取到解析值，则等待签发即可；超过24小时未签发，请购买付费证书

域名验证方式一：DNS解析验证

1、点击验证按钮

2、获取验证信息

Copyright © 2012-2021 UCloud 优刻得

请验证以下信息

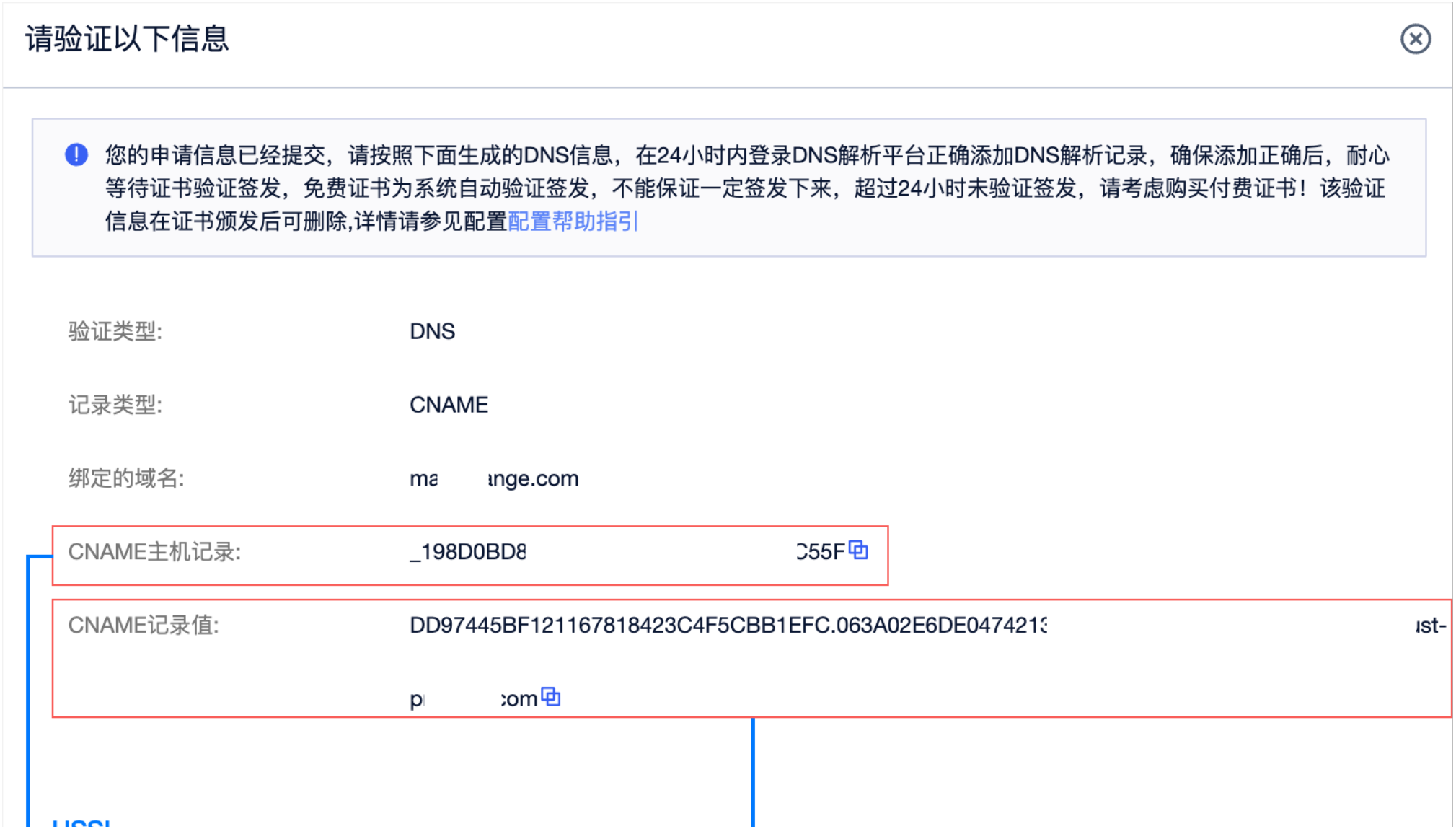
您的申请信息已经提交，请按照下面生成的DNS信息，在24小时内登录DNS解析平台正确添加DNS解析记录，确保添加正确后，耐心等待证书验证签发，免费证书为系统自动验证签发，不能保证一定签发下来，超过24小时未验证签发，请考虑购买付费证书！该验证信息在证书颁发后可删除,详情请参见配置配置帮助指引

验证类型:	DNS
记录类型:	CNAME
绑定的域名:	malachange.com
CNAME主机记录:	_198D0BD839D43701A2277CCDF94BC55F
CNAME记录值:	DD97445BF121167818423C4F5CBB1EFC.063A02E6DE0474213423FC03A862777A.TTD1Gmun28.trust-provider.com

Copyright © 2012-2021 UCloud 优刻得

3、填写验证信息

在DNS服务商(如DNSPOD)新增域名解析,样例如下:



4、解析验证

手动解析

通过本地客户端shell命令验证确认添加的解析是否正确，nslookup -q=CNAME 文件记录.主域名

```
user@FVFF877ZQ6LR ~ % nslookup -q=CNAME _6BFC7DAD6075C35BF0982D3B6C400AC6.uhasadmin.com
Server:         192.168.215.102
Address:        192.168.215.102#53

Non-authoritative answer:
_6BFC7DAD6075C35BF0982D3B6C400AC6.uhasadmin.com canonical name = b02d18da4b89e9d896561e9cc9621cb0.b06d42
c813c54d08c91c3577b4f5ca31.ttdtwpc52y.trust-provider.com.

Authoritative answers can be found from:

user@FVFF877ZQ6LR ~ %
```

获取到记录值

证书吊销使用txt验证的订单，命令使用nslookup -q=TXT 主机记录.主域名

域名验证方式二：文件验证（与服务器本身安全配置相关，容易出现验证不匹配的情况）

Copyright © 2012-2021 UCloud 优刻得

1、根据验证路径创建文本文件文件名称，并输入文件内容，文件内容结尾不能有回车或换行符

2、保证文件名称路径与验证一致，缺少可自行补齐

3、纪录值验证，浏览器访问https://domain+/.well-known/pki-validation/+文件名称 或者http://domain+/.well-known/pki-validation/+文件名称；并获取到对应的txt值，则表示文件解析添加成功

举例：

domain为 www.ucloud.cn; 访问：https://www.ucloud.cn/.well-known/pki-validation/文件名称获取到文件内容则为验证成功

Step4：证书签发

等待大概10分钟的时间，然后刷新控制台，看到状态变为“已颁发”，操作中出现【下载】按钮后，即可下载证书使用。

DV证书验证中出现问题，可以通过工具自查原因。

Copyright © 2012-2021 UCloud 优刻得

Step5：下载证书&部署

在控制台中下载证书后就可以在自己的服务器中部署证书了，部署证书可参考帮助文档。

Copyright © 2012-2021 UCloud 优刻得

企业型(OV)/增强型(EV)证书购买签发流程

总结:购买证书->补全信息->上传公司盖章确认函->后台公司信息审核->域名验证(DNS/文件验证)->签发证书

Step1：新购证书

ucloud首页-\>控制台-\>全部-\>证书管理 USSL\>购买证书

Copyright © 2012-2021 UCloud 优刻得

物联网边缘网关 UIoT Edge
AI训练服务 UAI Train
DDoS攻击防护 UDDoS
智能接入盒子 AccessBox
AI算法平台 UAI Algorithm
主机入侵检测 UHIDS
WEB漏洞扫描 UWS
无间盾反欺诈系统 UIW

安全合规

云安全中心 USC
堡垒机 UAuditHost
等保咨询 UDBCP
数据库审计 UDAS
密钥管理服务 UKMS
云日志审计 ULogAudit

企业应用

域名服务 UDNR
SSL证书管理 USSL
RMQ消息队列 URocketMQ
API网关 UAPIGateway
备案 ICP

云通信

短信服务 USMS
智能短信 ISMS

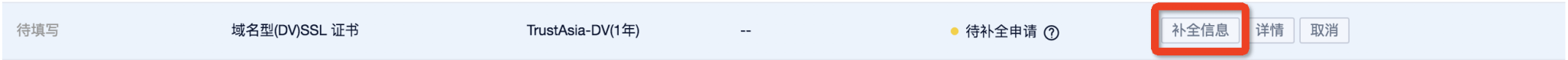
Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

详细内容参见购买证书介绍。

Step2：补全信息

购买后会看到生成了一条没有任何信息的待补全信息的证书，点击【补全信息】填写内容提交。



详细内容参见补全信息介绍。

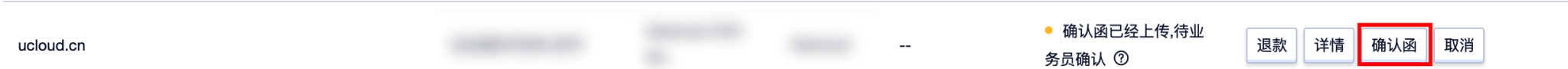
Step3：上传公司盖章确认函

附件信息（OV、EV证书）

OV、EV证书完成基础信息填写后，需完善附件信息上传，该步骤主要验证您的组织（企业）信息，根据不同CA中心，需提供附件分为以下两类（提交一类附件信息即可）

确认函

下载确认函附件表，填写相关信息后上传即可。



Copyright © 2012-2021 UCloud 优刻得

申请资料

需依次证书申请表、服务协议表、营业执照复印件、身份证正反面等信息

Copyright © 2012-2021 UCloud 优刻得

补充证明材料

您需要先下载申请表和服务协议，填写完整后请加盖公章,提交完整的星标必需上传的材料,等待审核。请上传jpg,png,gif,pdf,rar,zip,docx等格式文件

深圳CA机构SSL证书申请表 下载机构SSL证书申请表模版

深圳CA数字证书服务协议 下载数字证书服务协议模版

上传机构SSL证书申请表 * 请选择文件 请选择符合规则的文件

上传数字证书服务协议 * 请选择文件 请选择符合规则的文件

上传营业执照复印件 * 请选择文件 请选择符合规则的文件

上传经办人身份证正反面复印件 * 请选择文件 请选择符合规则的文件

上传公证处出具的授权委托书 请选择文件 请选择符合规则的文件

上传域名所有权证明或证书使用范围声明 请选择文件 请选择符合规则的文件

Copyright © 2012-2021 UCloud 优刻得

立即提交

Step4：公司信息人工审核（后台，客户无需操作，只需等待）

申请提交后CA中心将在3至7个工作日内完成审核，不同CA中心审核周期会有所区别。审核期间我们将电话、邮件联系申请人，请届时配合我们的审核。审核通过后我们会短信、邮件通知申请人。

CA中心审核

订单状态为待CA人工审核后，系统会自动发送域名确认邮件至相关联系人邮箱，请及时登录域名所有权邮箱或管理员邮箱进行邮件批准。

域名确认邮件批准后，订单联系人电话保持畅通，接听审核部电话。

注意，此处需要确认邮件，请注意查收邮箱中的邮件，有时候可能会在垃圾邮件中。

审核通过

我们将邮件、短信通知申请人，接到通知后可上控制台下载证书开始使用。

审核不通过

我们将邮件、短信通知申请人，控制台上证书状态变为审核失败，需要重新补全信息、重新上传确认函。

Step5：域名所有权验证

Copyright © 2012-2021 UCloud 优刻得

域名验证方式一：DNS解析验证

1、点击验证按钮

2、获取验证信息

3、填写验证信息

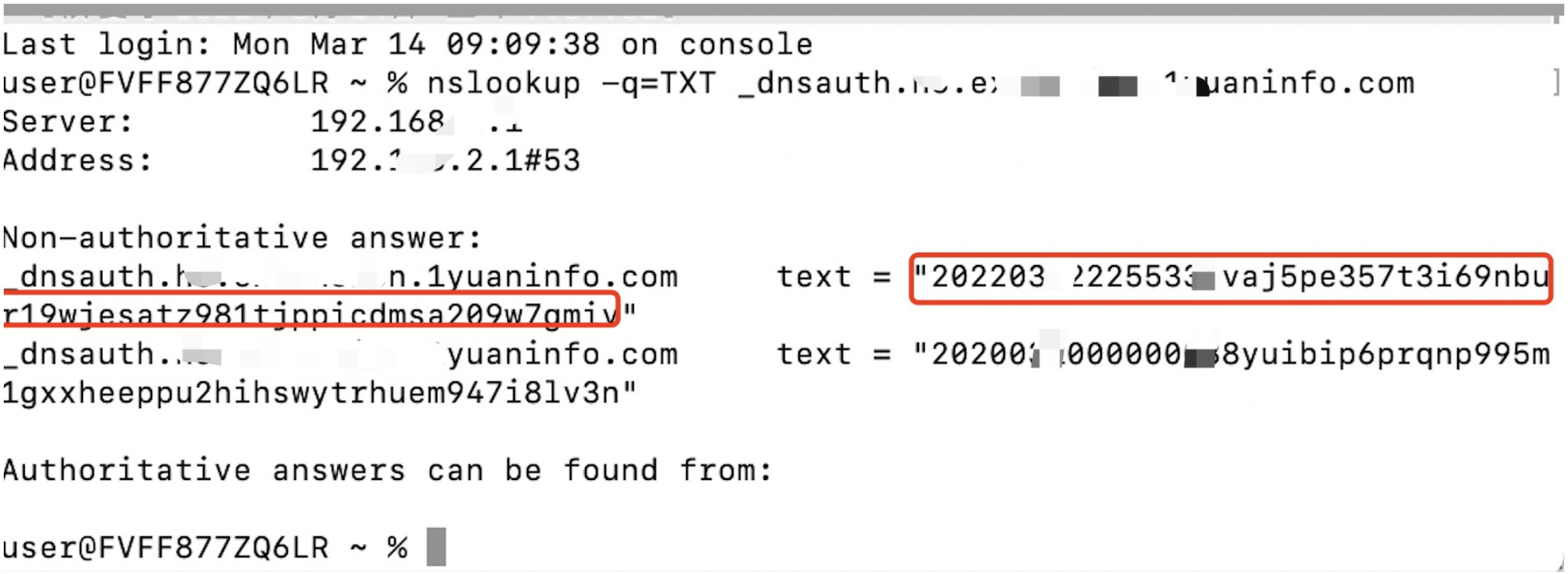
在域名解析平台或DNS服务商(如DNSPOD)新增域名解析，样例如下：

Copyright © 2012-2021 UCloud 优刻得


请验证以下信息
您的申请信息已经提交，请在24小时内修改DNS解析记录，该验证信息在证书颁发后可删除,请参见配置配置帮助指引
验证类型: DNS
记录类型: TXT
主机记录: _dnsauth
绑定的域名: www.ceshi.cn
TXT记录类型: ceshi.cn
TXT主机记录值: 202203221352403g2bl78v6jectx67vg1d9wb7wbdian9zs1xfa61die6pbgl7l
主机记录
记录类型
线路类型
记录值
权重
MX
TTL
最后操作时间
操作
TXT
默认
600
2022-03-23 13:48
确认
取消

4）、解析验证

本地客户端shell命令验证，nslookup -q=TXT __dnsauth.域名



域名验证方式二：文件验证（与服务器本身安全配置相关，容易出现验证不匹配的情况）

1、根据验证路径创建文本文件fileauth.txt，并输入txt值，文件内容结尾不能有回车或换行符

2、保证文件fileauth.txt路径与验证一致，可自行补齐

3、纪录值验证，浏览器访问https://domain+/.well-known/pki-validation/+fileauth.txt 或者http://domain+/.well-known/pki-validation/+fileauth.txt；并获取到对应的txt值，则表示文件解析添加成功

Copyright © 2012-2021 UCloud 优刻得

举例：

domain为 www.ucloud.cn; authKey为fileauth.txt，访问：https://www.ucloud.cn/.well-known/pki-validation/fileauth.txt

获取到文件内容（authValue）201704181133503c8morpl4g9gk5naytt4dmfwpw50pokoie4d4vjoy259gmbfai则为验证成功

Step6：证书颁发

完成以上步骤，恭喜您证书申请成功，您可下载对应证书文件部署到服务器。

Copyright © 2012-2021 UCloud 优刻得

证书部署详细内容参见证书部署介绍。

备注：因为域名型(DV)的验证信息是通过签发系统自动扫描签发的，不能实现100%成功签发，若24小时之内没有签发，为保障使用，请换成升级为OV证书。

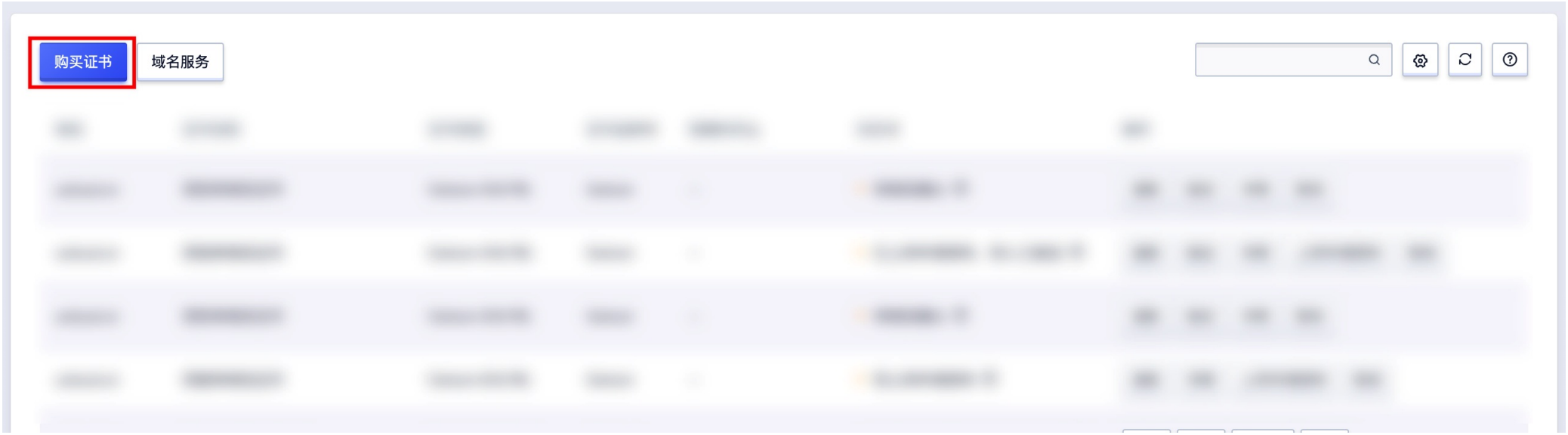
Copyright © 2012-2021 UCloud 优刻得

购买证书

购买入口

ucloud首页->控制台->全部->证书管理 USSL>购买证书

Copyright © 2012-2021 UCloud 优刻得



证书推荐

为便于您快速部署，针对性提供证书快速购买套餐。

Copyright © 2012-2021 UCloud 优刻得

选择证书

您可根据需求自定义购买证书

Copyright © 2012-2021 UCloud 优刻得

1.证书品牌

Symantec：Symantec公司是全球第一的数字证书认证机构，部署赛门铁克证书可激活互联网最受信任的诺顿安全签章。

GeoTrust：GeoTrust公司是全球第二大数字证书颁发机构，是Symantec旗下性价比品牌。

亚洲诚信：亚洲诚信公司是一家专业为各行业提供国际证书和自主产权证书的公司。

上海CA：国内第一家专业的第三方电子认证服务机构。

Copyright © 2012-2021 UCloud 优刻得

2.证书类型

OV:即组织型或机构型证书。OV型证书显然适用于企业、政府等机构。OV证书不仅具备加密传输和身份验证的完整功能,价格也比较便宜,而且签发便捷。

EV:即增强型SSL证书,企业型证书的升级版。在原有加密性和验证身份的基础上,加强了防假冒网站功能,在功能和效果上更强大。

DV:域名型SSL证书,能起到最基本的信息传输加密功能,验证最基本的域名管理权。CA只审核域名的所有权,申请过程系统自动完成,所以DV证书往往价格很低,甚至免费。

3.证书名称

根据所选的证书品牌和证书类型显示不同的证书,主要区别在于区分为普通和专业证书,以及通配符证书,请根据自身情况进行选择。

4.域名个数

除了多域名证书外,都只支持1个域名,购买时注意是普通的证书还是通配符证书。

通配符证书和多域名证书都支持泛域名。

5.证书有效期

按年售卖。可选1年、2年或者3年。根据证书类型不同可选年限不同。

证书为一次性购买,审核通过授予证书30天后将无法进行退款和取消。

Copyright © 2012-2021 UCloud 优刻得

补全信息

购买完成后在列表中找到刚才购买的证书，点击【补全信息】的按钮。

新的弹窗中填写需补全的所有信息。

域名信息

Copyright © 2012-2021 UCloud 优刻得

1. 绑定域名：

1）如果购买的是免费证书，则填写完整的域名，比如www.ucloud.cn;

2）如果购买的是多域名证书，则填写多个完整域名，域名个数根据购买时确定的个数为准，一次性填写完；

3）如果购买的是通配符证书，则填写泛域名，比如*.ucloud.cn

1. CSR信息：

Copyright © 2012-2021 UCloud 优刻得

分为在线生成和粘贴CSR

在线生成:加密算法为RSA,密钥参数对2048.

粘贴CSR:推荐使用网络上的CSR在线生成工具,生成CSR时注意跟补全信息时填写给我们的信息一致。不要使用特殊字符,保存好私钥文件。

要生成CSR文件,你必须为服务器创建密钥key。密钥key和SSL证书是不可分开的,一旦丢失或损坏了公钥、私钥或密码,重新生成密钥key文件后,和原来的SSL证书就不匹配了。这时需要重新生成CSR文件,可以申请免费重新签发SSL证书。

公司信息

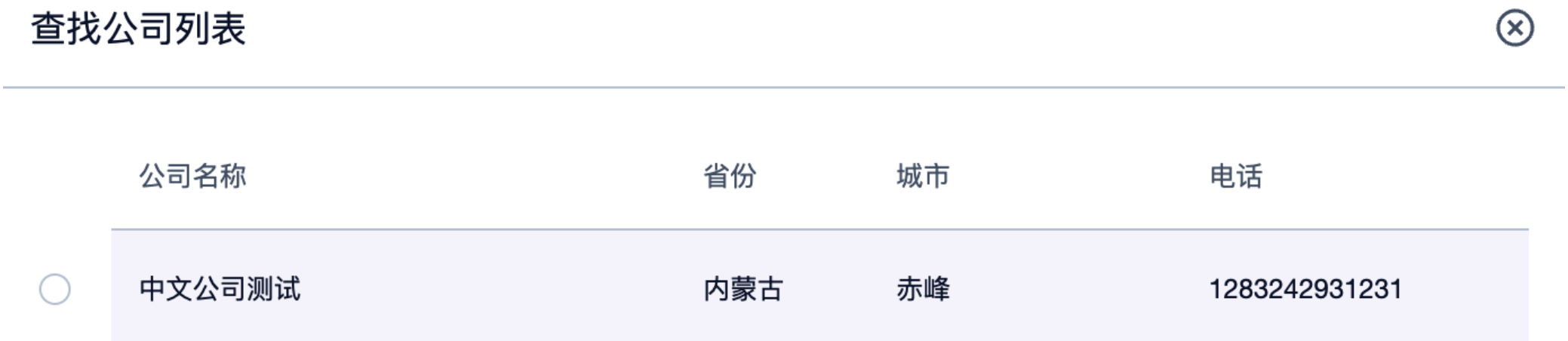
手动填写

填写公司名称、联系地址、电话、部门等基本资料。

Copyright © 2012-2021 UCloud 优刻得

快速填充

可选择公司列表的信息快速填充。公司信息管理参见个人中心。



Copyright © 2012-2021 UCloud 优刻得

○	easdasd	HeBei	QinHuangDao	1231231
○	北京万事达商业信息有限公司	北京	北京	13537837212
○	中文测试不带公司性质	北京	北京	123423123123
○	撒撒撒的公司	北京	北京	13423432342
○	enTest	ShanXi	TaiYuan	13554382912

取消 确定

申请人信息

手动填写

填写申请人姓名、手机号、职位等基本资料。

Copyright © 2012-2021 UCloud 优刻得

快速填充

可选择公司列表的信息快速填充。公司信息管理参见个人中心。

Copyright © 2012-2021 UCloud 优刻得

域名身份验证（仅DV证书需要选择）

可选DNS验证或者文件验证。

DNS验证：需要修改DNS记录。

文件验证：需要上传文件到指定服务器目录，能够访问到这个包含特殊内容的文件则表明验证通过。

Copyright © 2012-2021 UCloud 优刻得

验证身份

购买证书后必须补全信息才能完成证书申请。

注意填写正确的手机号和邮箱，审核人员将会通过手机号和邮箱与您联系。

DV 类型证书

验证方式可以选择DNS验证或者文件上传

DNS验证

Copyright © 2012-2021 UCloud 优刻得

请验证以下信息

您的申请信息已经提交，请按照下面生成的DNS信息，在24小时内登录DNS解析平台正确添加DNS解析记录，确保添加正确后，耐心等待证书验证签发，免费证书为系统自动验证签发，不能保证一定签发下来，超过24小时未验证签发，请考虑购买付费证书！该验证信息在证书颁发后可删除,详情请参见配置配置帮助指引

验证类型:	DNS
记录类型:	CNAME
绑定的域名:	malachange.com
CNAME主机记录:	_198D0BD839D43701A2277CCDF94BC55F
CNAME记录值:	DD97445BF121167818423C4F5CBB1EFC.063A02E6DE0474213423FC03A862777A.TTD1Gmun28.trust-provider.com

Copyright © 2012-2021 UCloud 优刻得

验证类型:DNS

记录类型:CNAME

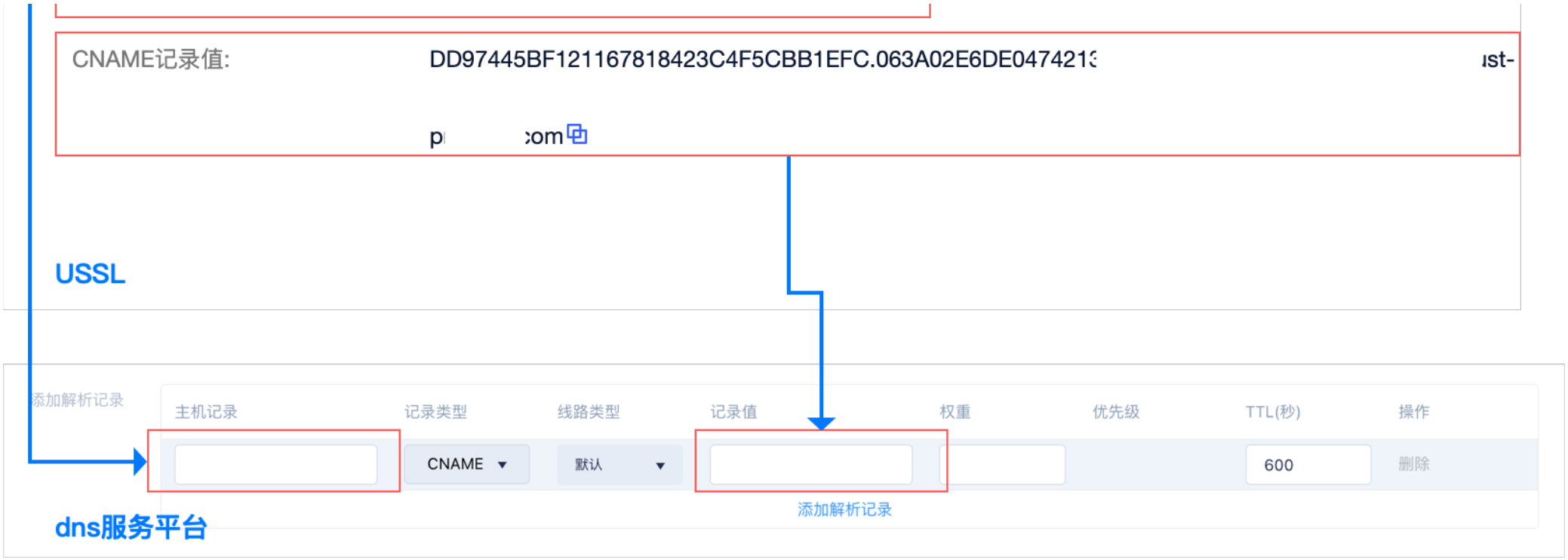
绑定的域名:显示补全信息时填写的域名

CNAME主机记录:根据域名返回的唯一的CNAME主机记录。

CNAME记录值:根据域名返回的唯一的CNAME记录值,请到您的DNS服务商处尽快添加CNAME记录。

请尽快于 24 小时内手动设置 DNS 解析记录,通过后 20 分钟内即可签发证书,超时将导致申请失败。

在DNS服务商比如DNSPOD添加主机记录



文件验证

Copyright © 2012-2021 UCloud 优刻得

3、配置监测
（1）HTTPS配置检验链接：https://domain+/.well-known/pki-validation/468BCEB7AE6AC5146CE45B7DA9161E9A.txt
（2）HTTP配置检测链接：http://domain+/.well-known/pki-validation/468BCEB7AE6AC5146CE45B7DA9161E9A.txt
domain+为您的域名文件，内容结尾不能有回车或换行符。 文件验证不支持任何形式的跳转，需要直接响应200状态码和文件内容。

验证方式:	FILE
绑定的域名:	ma
文件名称:	46 46CE45B7DA9161E9A.txt
文件路径:	/.w dation/
文件内容:	14 :879BDC9317B107A52122DCA60CFEEF2A88DEB1DD120111E7 trust-
	pr Drvvg
验证方式:	FIL
绑定的域名:	wv m
文件名称:	46 46CE45B7DA9161E9A.txt
文件路径:	/.w dation/
文件内容:	14 :879BDC9317B107A52122DCA60CFEEF2A88DEB1DD120111E7 trust-

Copyright © 2012-2021 UCloud 优刻得

1、创建文件： 文件验证方式一般需要您的站点管理人员进行操作，先创建C5704CE6BB76F223420F371E8346A609.txt，并将验证的文件文件内容粘贴在文件中进行保存。

2、创建目录： 在站点的根目录下创建.well-known/pki-validation子目录。注意第一层目录是带点的隐藏目录，Windows下命令为：m".well-known"。将创建的文件放在该子目录中；如果你的站点由于某种原因无法创建隐藏目录，选择其他DNS验证方式。

3、配置监测

(1)HTTPS配置检验链接：https://domain+/.well-known/pki-validation/C5704CE6BB76F223420F371E8346A609.txt

(2)HTTP配置检测链接：http://domain+/.well-known/pki-validation/C5704CE6BB76F223420F371E8346A609.txt

domain+为您的域名文件，内容结尾不能有回车或换行符。文件验证不支持任何形式的跳转，需要直接响应200状态码和文件内容。

解析校验

手动解析：手动解析可以帮助客户确认添加的解析是否正确

本地客户端shell命令验证，nslookup -q=CNAME 文件记录.主域名

Copyright © 2012-2021 UCloud 优刻得

```
user@FVFF877ZQ6LR ~ % nslookup -q=CNAME _6BFC7DAD6075C35BF0982D3B6C400AC6.uhasadmin.com
Server:         192.168.215.102
Address:        192.168.215.102#53

Non-authoritative answer:
_6BFC7DAD6075C35BF0982D3B6C400AC6.uhasadmin.com canonical name = b02d18da4b89e9d896561e9cc9621cb0.b06d42c813c54d08c91c3577b4f5ca31.ttdtwpc52y.trust-provider.com.

Authoritative answers can be found from:

user@FVFF877ZQ6LR ~ %
```

获取到记录值

证书吊销使用txt验证的订单，命令使用nslookup -q=TXT 主机记录.主域名

OV / EV 类型证书

需要通过填写确认函上传给我们，由人工进行审核派发证书。

1. 下载确认函

2. 填写确认函

3. 确认函打印并盖章，生成扫描件（拍照也可，请确保清晰）后到控制台上传

4. 我们尽快进行审批处理

5. 审批通过后则可以下载证书，我们将短信、邮件通知申请人。

Copyright © 2012-2021 UCloud 优刻得

吊销证书

颁发了证书后，从订单提交时间开始30天内完成吊销可以退款。超过30天仅吊销证书不退款。

可将下列情况指定为吊销证书的理由：泄露密钥、泄露 CA、从属关系改变、被取代、业务终止、证书持有（这是唯一让您能够改变被吊销证书状态的理由码，在证书状态有问题的情况下非常有用）。

由 CA 吊销证书意味着，CA 在证书正常到期之前撤销其允许使用该密钥对的有关声明。在吊销的证书到期之后，CRL 中的有关条目被删除，以缩短 CRL 列表的大小。

Copyright © 2012-2021 UCloud 优刻得

证书退费

只有以下条件下证书允许退费：

1. 刚购买了证书，还未补全信息

2. 补全信息且提交了，还未进行验证（DV为dns验证或文件验证，OV\EV证书为确认函方式验证）

3. 提交了验证还未下发证书

4. 颁发了证书后，从订单提交时间开始30天内完成吊销可以退款

注意：证书订单超过30天则无法退款。

Copyright © 2012-2021 UCloud 优刻得

个人中心

个人中心主要用于管理个人及企业的相关信息，包含模块告警信息、公司信息、联系人信息。

告警设置

查看、管理、筛选对应的告警信息，产生告警事件后信息将通过邮件与短信的方式通知对应管理人员。

Copyright © 2012-2021 UCloud 优刻得

证书状态更新告警说明：未配置证书告警模块及告警通知人，默认不通知客户变更情况，如果告警通知请配置告警功能！

告警设置

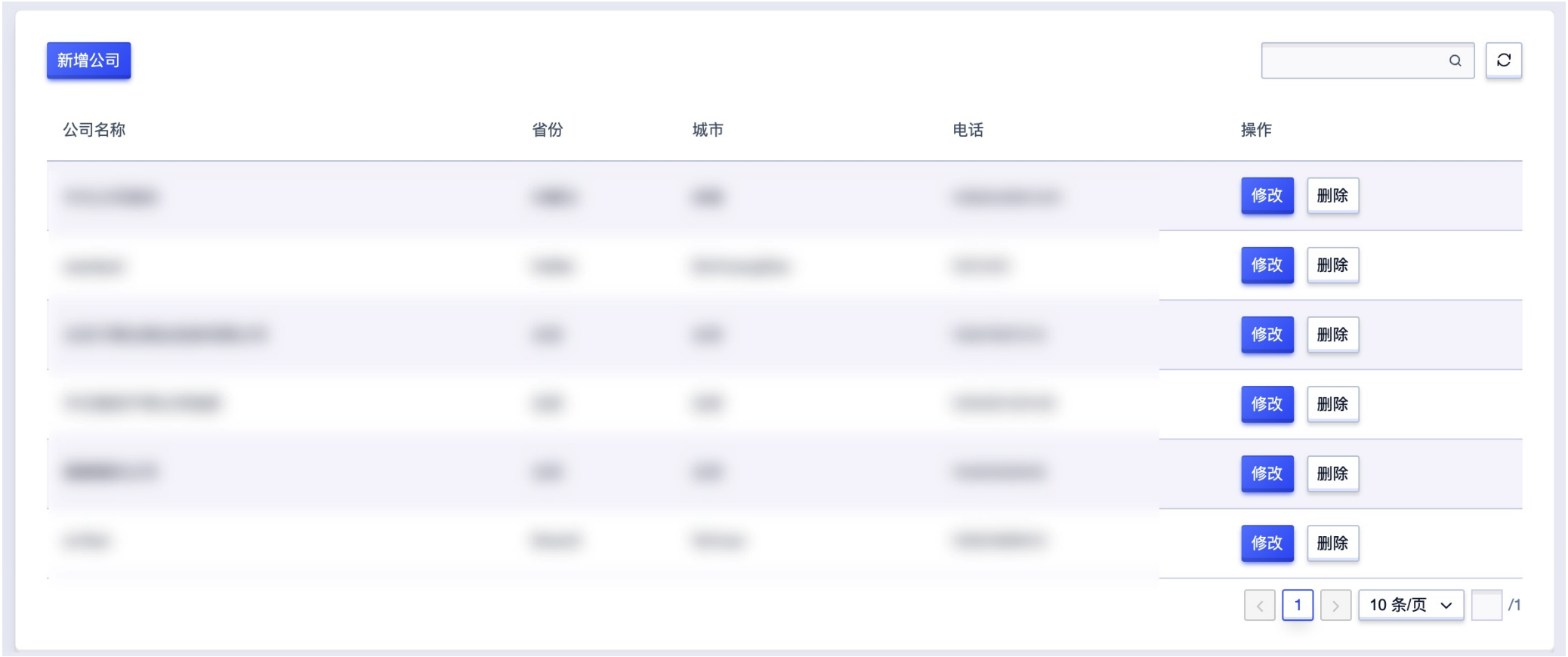
域名	证书类型	证书品牌	到期时间	状态	操作
[redacted]	[redacted]	[redacted]	[redacted]	待续费	删除告警
[redacted]	[redacted]	[redacted]	[redacted]	待续费	删除告警
[redacted]	[redacted]	[redacted]	[redacted]	待续费	删除告警
[redacted]	[redacted]	[redacted]	[redacted]	已续费	删除告警
[redacted]	[redacted]	[redacted]	[redacted]	待续费	删除告警
[redacted]	[redacted]	[redacted]	[redacted]	待续费	删除告警

Copyright © 2012-2021 UCloud 优刻得

公司信息

查看、管理、筛选对应的公司信息，可在信息补充时快速填充到对应信息栏。

Copyright © 2012-2021 UCloud 优刻得



添加/编辑公司信息

公司信息不允许中英文混写,混写可能导致证书审核不通过，请使用纯中文或纯英文填写对应信息

Copyright © 2012-2021 UCloud 优刻得

选择语言 * 中文 英文

公司名称 * 只能填写纯中文

联系地址 * 请填写联系地址

电话 * 请填写电话

国家 * 中国

省份 * 北京

城市 * 北京

公司性质 请选择公司性质

公司证件类型 请选择公司证件类型

公司证件类型对应的证件号码 请填写公司证件类型对应的证件

Copyright © 2012-2021 UCloud 优刻得

部门 *

请填写部门

邮编 *

请填写邮编

取消 确定

联系人信息

查看、管理、筛选对应的联系人信息，可在信息补充时快速填充到对应信息栏。

Copyright © 2012-2021 UCloud 优刻得

添加/编辑联系人信息

联系人信息不允许中英文混写,混写可能导致证书审核不通过，请使用纯中文或纯英文填写对应信息

申请人姓名 *
请填写申请人姓名

职位 *
请填写职位

电话 *
请填写电话

邮箱 *
请填写邮箱

取消 确定

Copyright © 2012-2021 UCloud 优刻得

证书上传

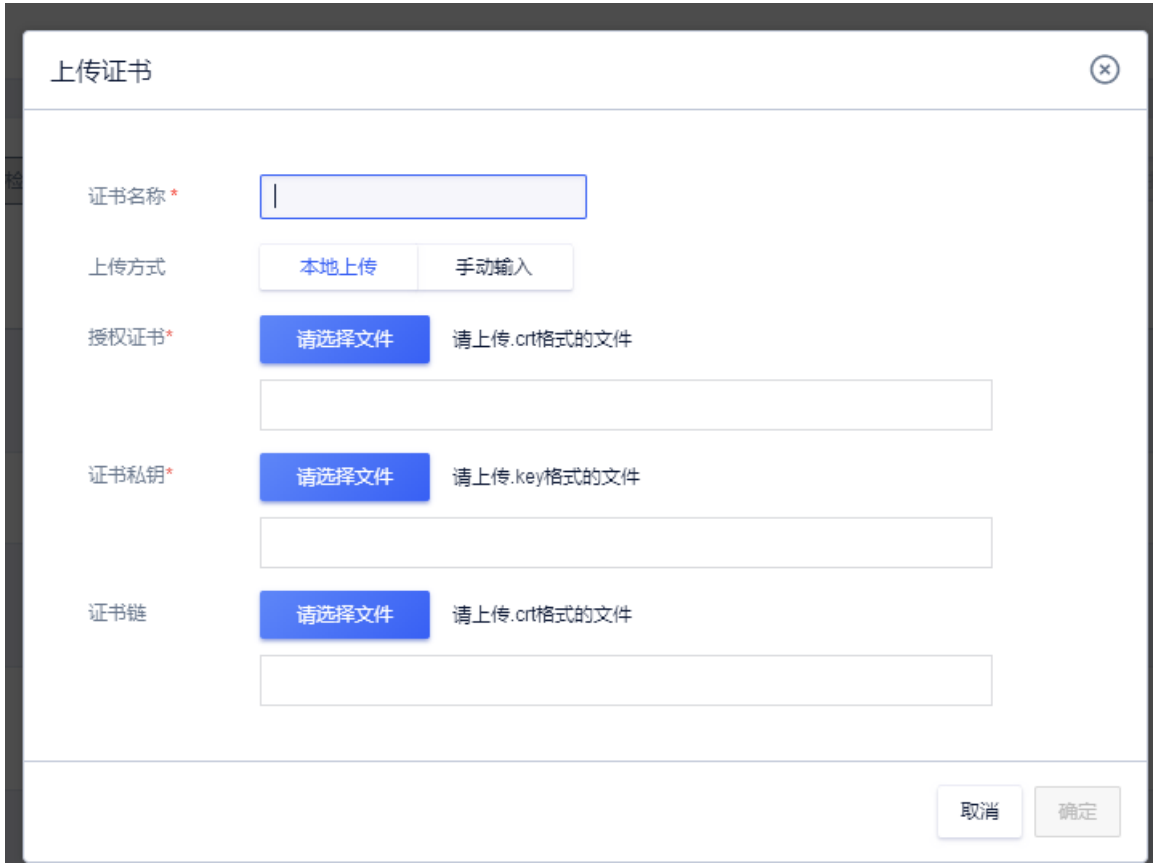
USSL证书管理平台支持其他平台购买证书的一键上传上传和生命周期管理服务

操作如下：

1、进入控制台的证书管理USSL页面

2、点击上传证书按钮 ，自定义证书名称

Copyright © 2012-2021 UCloud 优刻得



3、证书上传

普通格式

证书文件包含：公钥：public.crt、私钥：private.key、ca证书链：CA.crt；请按照下图指引进行上传

Copyright © 2012-2021 UCloud 优刻得

pem格式

证书文件包含:公钥+ca证书链:public.pem、私钥-private.key;请按照下图指引进行上传

Copyright © 2012-2021 UCloud 优刻得

4、上传完成

上传成功的证书，平台将自动获取到证书域名、签发机构、有限时间；从证书类型及状态可判断是否为上传证书，如图所示

Copyright © 2012-2021 UCloud 优刻得

Copyright © 2012-2021 UCloud 优刻得

产品价格

Digcert(原Symantec，已更名)证书价格

产品名称	年限	价格（元）
企业型OV证书	1	4850
企业型OV证书	2	8730
企业型OV证书专业版	1	7650
企业型OV证书专业版	2	13770
企业型OV通配符证书	1	38000
企业型OV通配符证书	2	68400
企业型OV通配符证书专业版	1	68000
企业型OV通配符证书专业版	2	122400
增强型EV证书	1	7950
增强型EV证书	2	14310
增强型EV证书专业版	1	12650
增强型EV证书专业版	2	22770

Copyright © 2012-2021 UCloud 优刻得

GeoTrust证书价格

产品名称	年限	价格（元）
企业型OV证书	1	2578
企业型OV证书	2	4578
企业型OV通配符证书	1	6678
企业型OV通配符证书	2	10778
企业型OV多域名证书	1	5580
企业型OV多域名证书	2	10044
增强型EV证书	1	4850
增强型EV证书	2	8730
增强型EV多域名证书	1	9650
增强型EV多域名证书	2	17370

TrustAsia证书价格

产品名称	年限	价格（元）
域名型DV证书-免费证书	1	0

Copyright © 2012-2021 UCloud 优刻得

域名型DV通配符证书	1	1999
域名型DV多域名证书	1	4900
企业型OV单域名证书	1	4500
企业型OV单域名证书	2	8100
企业型OV单域名额外增加域名	1	2000/个
企业型OV单域名额外增加域名	2	3600/个
企业型OV通配符证书	1	13500
企业型OV通配符证书	2	24300
增强型EV单域名证书	1	9500
增强型EV单域名证书	2	17100
增强型EV单域名额外增加域名	1	3500/个
增强型EV单域名额外增加域名	2	6300/个
国密域名型DV证书	1	1500
国密域名型DV证书	2	2700
国密域名型DV证书	3	3900
国密域名型DV通配符证书	1	3500
国密域名型DV通配符证书	2	6300
国密域名型DV通配符证书	3	9100

Copyright © 2012-2021 UCloud 优刻得

国密域名型DV多域名证书	1	1500/个
国密企业型OV证书	1	4500
国密企业型OV证书	2	8100
国密企业型OV证书	3	11700
国密企业型OV通配符证书	1	13500
国密企业型OV通配符证书	2	24300
国密企业型OV通配符证书	3	35100
国密企业型OV多域名证书	1	4500/个

GlobalSign证书价格

产品名称	年限	价格（元）
企业型OV单域名证书	1	3728
企业型OV单域名证书	2	6710
企业型OV单域名基础上额外增加域名	1	1980
企业型OV单域名基础上额外增加域名	2	3564
企业型OV通配符证书	1	13048
企业型OV通配符证书	2	23486

Copyright © 2012-2021 UCloud 优刻得

增强型EV单域名证书	1	9880
增强型EV单域名证书	2	17784
增强型EV单域名基础上额外增加域名	1	2980/个
增强型EV单域名基础上额外增加域名	2	5364/个

UniTrust证书价格

产品名称	年限	价格（元）
域名型DV单域名证书	1	980
域名型DV单域名证书	2	1764
域名型DV单域名证书	3	2548
域名型DV通配符证书	1	5280
域名型DV通配符证书	2	9504
域名型DV通配符证书	3	13728
企业型OV单域名证书	1	2780
企业型OV单域名证书	2	5004
企业型OV单域名证书	3	7228
企业型OV通配符证书	1	9580

Copyright © 2012-2021 UCloud 优刻得

企业型OV通配符证书	2	17244
企业型OV通配符证书	3	24908
企业型OV多域名证书	1	2980 + 980/个
增强型EV单域名证书	1	4080
增强型EV单域名证书	2	7344
增强型EV单域名证书	3	10608
增强型EV单域名证书	2	17100
增强型EV多域名证书	1	4080 + 1680/个

私有证书价格

产品名称	购买量级	价格（元）
根CA-RSA	1 月	3200
根CA-SM（国密）	1 月	6400
根CA-ECC	1 月	4800
子CA-RSA	1 月	1600
子CA-SM（国密）	1 月	3200

Copyright © 2012-2021 UCloud 优刻得

子CA-ECC	1 月	2400
证书RSA	100-1000张	10
证书RSA	1000-5000张	8
证书RSA	5000张以上	5
证书SM(国密)	100-1000张	30
证书SM(国密)	1000-5000张	18
证书SM(国密)	5000张以上	15
证书ECC	100-1000张	20
证书ECC	1000-5000张	12
证书ECC	5000张以上	10

Copyright © 2012-2021 UCloud 优刻得

Nginx部署

一、 获取pem格式的证书公私钥

首先登录SSL控制台：https://console.ucloud.cn/ussl/ussl。然后下载证书

证书格式：pem for nginx（证书下载完打开Nginx文件夹）

解压后会获得两个文件：pem后缀的是证书公钥+ca证书文件(例如：public.pem)，key后缀的是私钥文件(例如：private.key)

二、 在nginx里部署证书及优化配置ssl

到nginx的conf目录，找到nginx.conf文件，修改或者配置这样一段

```
server {
listen 443;(ps:nginx1.15及以上的版本要修改为listen 443 ssl;)
server_name www.trustasia.com #你们的域名，如www.abc.com;
ssl on;
ssl_certificate_pem /xxx/xxx/server.pem; #根据实际的路径和文件名配置
ssl_certificate_key /xxx/xxx/server.key; #根据实际的路径和文件名配置
ssl_session_timeout 5m;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; #按照这个协议配
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;#按照这个套件配
ssl_prefer_server_ciphers on;
location / {
root html; #站点目录
```

Copyright © 2012-2021 UCloud 优刻得

```
index index.html index.htm;
}
}
```

下面为配置文件参数说明： listen 443

SSL访问端口号为443

---

ssl on

启用SSL功能

---

ssl_certificate

证书文件server.pem

---

ssl_certificate_key

私钥文件server.key

---

ssl_protocols

使用的协议

---

ssl_ciphers

配置加密套件，写法遵循openssl标准

配置完成后，先用bin/nginx –t**来测试下配置是否有误，正确无误的话，建议重启**nginx。

三、 使用全站加密，http自动跳转https（可选）

Copyright © 2012-2021 UCloud 优刻得

对于用户，不是不知道https，就是知道https也因为懒，不愿意输入https。这样就有一个需求，让服务器自动把http的请求重定向到https。

在服务器这边的话配置的话，可以在页面里加js脚本，也可以在后端程序里写重定向，当然也可以在web服务器来实现跳转。Nginx是支持rewrite的（只要在编译的时候没有去掉pcre）

在http的server里 增加rewrite ^(.*) https://$host$1 permanent;

这样就可以实现80进来的请求，重定向为https了。

Copyright © 2012-2021 UCloud 优刻得

Tomcat8.5/Tomcat9的证书部署

一、获取jks格式证书

登录：https://console.ucloud.cn/ussl/ussl

查看订单后，操作：证书下载，需要从此处格式转换工具转换为JKS格式的证书

JKS格式证书解压缩后看到如图的文件夹

文件夹内文件的格式为pem，cer后缀的是证书公钥(此文件可以改名为server.pem)，key后缀的是私钥(可以改名为server.key)

二、到tomcat中部署证书

把jks文件存放到conf目录下，然后配置同目录下的server.xml文件，第一次配置的话，有段被注释掉的connector，使用的是NIO来做JSSE引擎的，修改为

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150" SSLEnabled="true">

<SSLHostConfig>

<Certificate certificateKeystoreFile="conf/www.trustasia.com.jks"
```

Copyright © 2012-2021 UCloud 优刻得

```
certificateKeystorePassword="刚才设置的证书密码"

certificateKeyAlias="www.trustasia.com"

type="RSA" />

</SSLHostConfig>

</Connector>
```

注:certificateKeystorePassword和certificateKeyAlias 需要添加进去。

certificateKeystorePassword为jks密码

certificateKeyAlias为jks别名,没有特殊情况的别名就是申请的证书域名,比如申请了_.trustasia.com.jks的通配符证书,别名为*.trustasia.com; www.trustasia.com.jks的别名就是www.trustasia.com

别名查看方式,jdk工具里:keytool –list –keystore jks文件 –storepass jks文件密码。这样就可以显示出条目列表。

Copyright © 2012-2021 UCloud 优刻得

Apache 2.x 证书部署

第一步：获取服务器证书和保存到同一个目录

证书审批通过后可以从控制台直接下载证书，证书文件的内容格式如下，把第一段代码保存成一个crt格式的文件（文本格式）如 domain.crt ，第二段和第三段粘贴到一个文本中保存一个crt格式的文件如 CA.crt。

```
-----BEGIN CERTIFICATE-----
MIIDDTCCAfUCAQAwgZQxCzAJBgNVBAYTAkNOMRIwEAYDVQQIDAnkuIrmtbfluIIx
EjAQBgNVBAcMCeS4iua1t+W4gjEtMCsGA1UECgwk5LiK5rW35Z+f6IGU6L2v5Lu2
5oqA5pyv5pyJ6ZmQ5YWs5Y+4MRIwEAYDVQQLDAnmioDmnK/pg6gxGjAYBgNVBAMT
EXd3dy50cnVzdGFzaWEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAyr8u1KAV2ZZ7UmnFgssNV/iyGoNsBsRCl8ZtDneM8gDM1EoteG0nMitPxuPZ
Vwfar9TTYGmJ8PTP3G80aM+hC1oQQbs3iOVWIus/R/AXCtTNQ8CpMDvXjLLMjV5X
KbZotyVL1KpoEw8nyWwtoiDXPJe3OyFYZ7HHx1qBPWvHogwQgn4UhPH/k3/e1GYc
lErZnWq2h2vVDB6sk01X1GuRTXYWozeB7dXYrCcU++umo4Q+pbGw8aWkhZ4WxuWg
vssYC2bHbrv7HiBzBq/E/v8=
-----END CERTIFICATE-----
```

最后把domain.crt 、CA.crt和domain.key (在申请证书时生成的那个私钥保存成 domain.key)三个文件保存到同一个目录，例如/usr/local/apache/conf目录下。

第二步：更新 httpd.conf 配置文件

1.用文本编辑器打开Apache根目录下 conf/httpd.conf 文件 找到

Copyright © 2012-2021 UCloud 优刻得

```
#LoadModule ssl_module modules/mod_ssl.so
```

和

```
#Include conf/extra/httpd-ssl.conf
```

去掉前面的 # 号 2.用文本编辑器打开Apache根目录下 conf/extra/httpd-ssl.conf 文件修改一下内容：

```
<VirtualHostwww.trustasia.com:443>
DocumentRoot "/var/www/html"
ServerName www.trustasia.com
SSLEngine on
SSLCertificateFile /usr/local/apache/conf/domain.crt
SSLCertificateKeyFile /usr/local/apache/conf/domain.key
SSLCertificateChainFile /usr/local/apache/conf/CA.crt
</VirtualHost>
```

下面为配置文件参数说明：

SSLEngine on

启用SSL功能

SSLCertificateFile

证书文件domain.crt

Copyright © 2012-2021 UCloud 优刻得

SSLCertificateKeyFile

私钥文件domain.key

SSLCertificateChainFile

证书链文件 CA.crt

按照以上的步骤配置完成后，重新启动 Apache 就可以使用https:// ***来访问了。***

如有任何问题或疑问请直接与我们联系，谢谢

Copyright © 2012-2021 UCloud 优刻得

JBoss证书部署

第一步：获取并导入证书

下载Jboss类型证书，您将收到三段证书代码，将“您的SSL证书”下面的代码（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）复制粘贴到文本文档 并保存成 cer格式的文件 如server.cer 。以同样的方法把“XX型SSL中级证书”下面的代码保存成intermediate.cer把“XX型SSL交叉证书”下面的代码保存成 cross.cer 最后把server.cer、intermediate.cer、cross.cer和server.jks(生成CSR时产生的文件)几个文件保存到同一个目录，例如c盘根目录目录下。

导入中级证书：

```
keytool -import -alias intermediate -keystore c:\server.jks -trustcacerts –file c:\intermediate.cer
```

提示“认证已添加至keystore中”则导入成功。

导入交叉证书：

```
keytool -import -alias cross -keystore c:\server.jks -trustcacerts -file c:\cross.cer
```

提示“认证已添加至keystore中” 则导入成功。

导入服务器证书：

进入Java_JRE\bin目录，如 cd C:\PROGRA~1\Java\jre1.6.0_10\bin，运行如下命令：

```
keytool -import -alias mykey -keystore c:\server.jks -trustcacerts -file c:\server.cer
```

输入密码后 提示:“认证回复已安装在 keystore中”说明导入成功。

第二步：更新 server.xml配置文件

将已正确导入认证回复的server.jks文件到Jboss安装目录下

Copyright © 2012-2021 UCloud 优刻得

用文本编辑器打开Jboss安装目录下server/default/deploy/jbossweb.sar目录中的server.xml文件，

并更新以下内容

```
<Connector protocol="HTTP/1.1" SSLEnabled="true"

port="443" address="${jboss.bind.address}"

scheme="https" secure="true" clientAuth="false"

keystoreFile="/usr/local/jboss/server.jks "

keystorePass="123456" sslProtocol = "TLS" />
```

下面为配置文件参数说明：

port="443"

SSL访问端口号为443

keystoreFile

私钥库文件 server.jks

keystorePass

私钥库密码 123456

按照以上的步骤配置完成后，重新启动 Jboss。

Copyright © 2012-2021 UCloud 优刻得

如有任何问题或疑问请直接与我们联系，谢谢！

Copyright © 2012-2021 UCloud 优刻得

IIS 服务器证书部署

环境说明

1. * 建议使用 IIS8(支持 SNI),一个站点一个端口允许同时部署多张证书
2. * 对于 IIS6,IIS7,IIS8,操作具体通用性

证书部署指导文档

IIS 服务器证书部署请参考此文档IIS 服务器证书部署指导

Copyright © 2012-2021 UCloud 优刻得

Trustasia免费/DV证书验证常见问题

Trustasia免费/DV证书购买后需要验证域名所有权，验证方式：DNS验证（建议方式）、文件验证；证书签发后，添加的解析即可删除

DNS验证:域名管理平台添加dns解析

文件验证:服务器固定文件目录添加内容,参考:https://docs.ucloud.cn/ussl/operate/fill**

1、Trustasia免费/DV证书控制台点击【验证】按钮报错/显示不匹配

答:控制台上【验证】按钮工具只是辅助客户验证的工具,不是最终证书签发的依据;客户DNS解析配置是否正确可以借助手动解析来确认

2、如何手动解析验证DNS解析配置是否正确?

答:本地客户端shell命令验证,nslookup -q=CNAME 记录值.主域名,样例如下:

TXT类型解析命令为:nslookup -q=TXT 主机记录.主域名

Copyright © 2012-2021 UCloud 优刻得

```
user@FVFF877ZQ6LR ~ % nslookup -q=CNAME _6BFC7DAD6075C35BF0982D3B6C400AC6.uhasadmin.com
Server:         192.168.215.102
Address:        192.168.215.102#53

Non-authoritative answer:
_6BFC7DAD6075C35BF0982D3B6C400AC6.uhasadmin.com canonical name = b02d18da4b89e9d896561e9cc9621cb0.b06d42
c813c54d08c91c3577b4f5ca31.ttdtwpc52y.trust-provider.com.

Authoritative answers can be found from:

user@FVFF877ZQ6LR ~ %
```

获取到记录值

3、已成功配置DNS解析，但是手动命令解析不到对应值

答:1、对比控制台提示信息与域名解析平台添加值是否一一对应,特别说明:多次发现客户购买的域名和添加的域名解析不对应

错误样例:购买证书域名为:www.demon.com,解析添加域名为:www.demon.cn

2、联系域名解析平台确认添加的解析是否生效

4、手动解析到控制台对应值，为何证书一直不签发?

答:Trustasia免费/DV证书签发时间:解析添加成功且后台服务器验证匹配后最快20分钟签发,一般不超过24小时;

dv证书为系统自动签发,存在不签发的情况,如超过24小时建议购买OV/EV证书。

Copyright © 2012-2021 UCloud 优刻得

特别说明:DV类型不是所有证书都能发的,域名会进行安全审核,自动检测有异常的话,ca就不允许颁发; 目前就不可以申请G5系列的证书了,需要申请其它类型的证书**

5、客户文件验证，但检测报错，可让客户重新购买并选择DNS验证

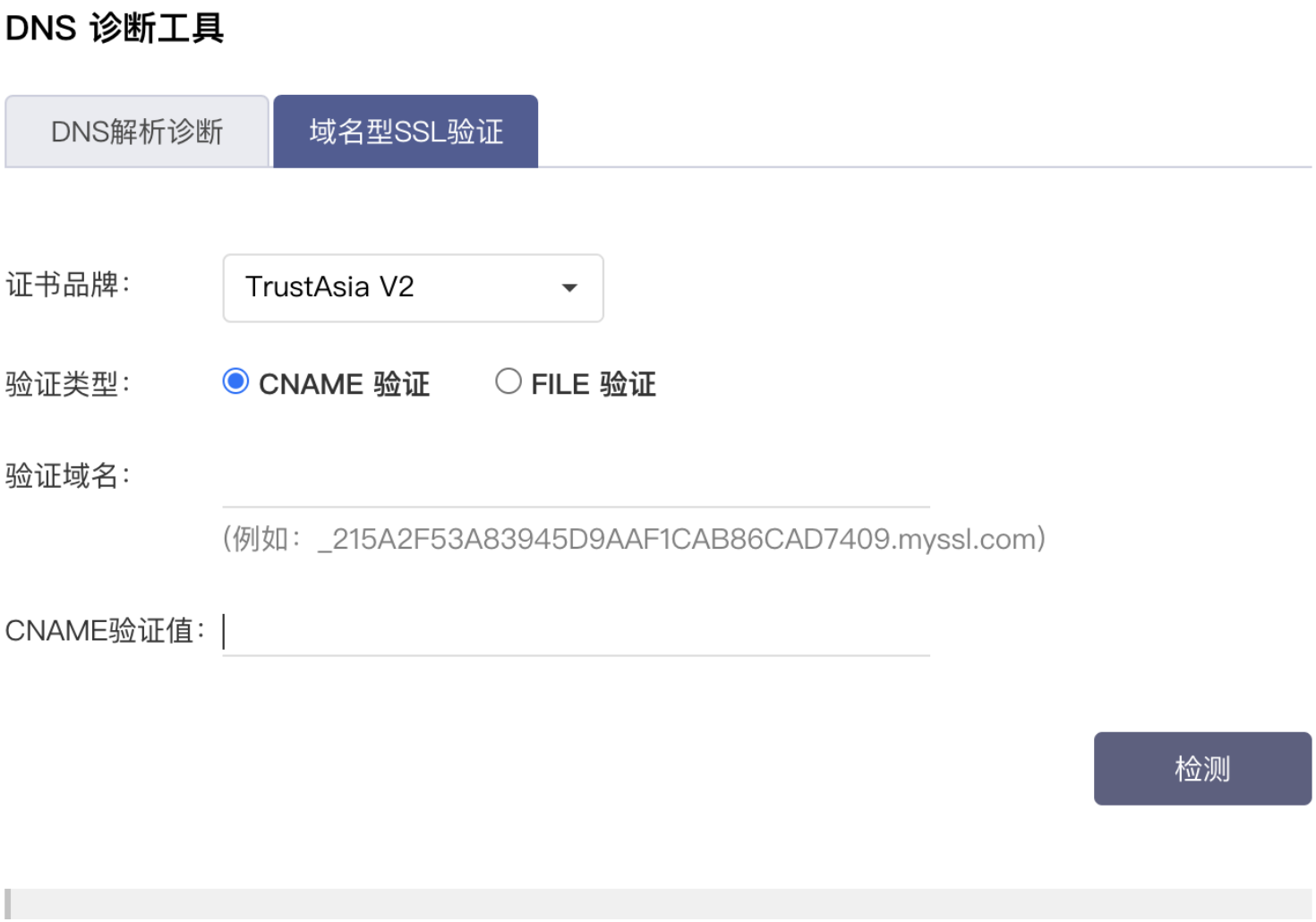
文件验证检测涉及到服务器本身配置问题,建议优先使用DNS验证方式,即重新下单并选择DNS验证方式

6、Trustasia免费/DV证书其他验证方式-亚洲诚信检测工具

检测地址:https://myssl.com/dns_check.html#ssl_verify

示例:三个不同的域名服务器有一个验证匹配,即说明解析添加无误

Copyright © 2012-2021 UCloud 优刻得



如验证不匹配，解决方案：

(1)、是否按照控制台提示的信息，添加dns/文件解析值

Copyright © 2012-2021 UCloud 优刻得

(2)、检查添加的解析值和控制台信息是否一致

(3)、若上述都正确，可在本地shell中手动解析查看情况,获取到对应值则说明解析正常，等待即可

7、亚洲诚信工具解析检测时，只有一个或两个匹配项

检测只有一个或两个匹配项时，说明验证正常，客户只需要等待即可，正常24小时内会颁发证书；如超过24小时还未颁发，请直接购买OV/EV类型的证书。

检测结果

地区	是否匹配
中国	匹配
香港	不匹配 (DNS 错误：查询 CNAME 时间超时)
美国	匹配

8、重颁发验证时TXT验证值和cname冲突

如果DNS验证中txt记录与cname记录冲突导致无法验证成功，可在原主机记录，域名前加一级_dnsauth. 来避免冲突（默认显示值已提示添加）

主机记录值参考https://docs.ucloud.cn/ussl/faq/free

Copyright © 2012-2021 UCloud 优刻得

续费证书的申请流程和部署

1、续费按钮会在老证书过期前的【30天】，显示和生效

2、点击续费后，平台将新生成一张续费新订单，客户点击并确认续费

3、续费证书和新购证书流程一样，都需要进行验证，验证流程同老证书一样

4、续费证书的生效节点为续费证书颁发时间节点，中间无中断，请在老证书过期前进行续费证书的部署

5、续费证书部署：

- 续费证书和老证书可同步部署，续费证书的有效期截止时间为老证书顺延12个月
- 提前续费，续费证书可替换老证书，老证书剩余时间会累加在续费证书上

Copyright © 2012-2021 UCloud 优刻得

免费证书验证匹配，但一直未颁发

- 如果证书检测为匹配,就说明验证正常,检测验证地址:https://myssl.com/dns_check.html\#ssl_verify，或直接点击控制台的验证按钮进行检测
- DV证书为系统检测证书,正常情况下,验证通过后20分钟左右,证书就会颁发,最长不会超过一天
- 不是所有的DV证书都会颁发,DV证书如验证果果24小时仍未颁发,只能购买ov或ev证书

** 备注:DV类型不是所有证书都能发的,域名会进行安全审核,自动检测有异常的话,ca就不允许颁发；目前就不可以申请G5系列的证书了,需要申请其它类型的证书**

Copyright © 2012-2021 UCloud 优刻得

证书订单被拒绝

1、订单被拒绝的原因：DV证书为系统自动检测验证，超过一周未进行验证，系统将自行拒绝此订单

2、如需使用，可选择重新下单，并在7天内进行证书所有权的验证

Copyright © 2012-2021 UCloud 优刻得

证书吊销流程和注意点

1、证书吊销和购买流程一样。都是需要验证的

流程

DV证书：需要DNS/文件验证

ov、ev证书：需要上传确认函并验证域名所有权

2、证书吊销后将立即生效，请谨慎操作

3、购买超过一个月的付费证书，吊销不退费

4、证书吊销前提条件：证书的状态为订单已完成；如果进行续费、重颁发、吊销操作，请取消操作后进行，请联系产品负责人进行后台操作

5、证书在进入倒计时30天有效期内，证书状态将改编成待续费状态，此状态不支持证书的吊销（证书方限制）

Copyright © 2012-2021 UCloud 优刻得

证书申请失败原因排查

DV类型证书

1. 为什么我申请的证书提示“安全审查失败”?

由于DV 证书的验证级别比较低,CA 为了防止有钓鱼嫌疑的域名申请SSL证书进行钓鱼攻击,系统中设置一些列规则 拒绝有嫌疑的域名申请DV证书,具体规则是不公开的,比如域名中包含敏感词如bank,pay金融支付相关的,如Google 这种知名网站相关的,还有其他一些域名黑名单(恶意域名) 白名单(知名域名)等,都有可能被拒绝申请DV证书,这种情况下 就只能去申请收费的 OV 或EV证书。

特定的关键词规则包含: test、live、bank、fund、wallet、pay、lv、nuclear、.pw域名等。

部分全球知名公司注册商标、域名等,如:google、microsoft、apple等。

解决办法

建议首先更换域名中的主机名部分,重新尝试提交订单。如果多次更换主机名,均提示以上错误,则建议选择其他收费证书产品,或选择更换主域名申请证书。

证书格式转换

PEM转JKS

证书格式转换地址:https://myssl.com/cert_convert_wasm.html

Copyright © 2012-2021 UCloud 优刻得

所填项如下：

源格式 pem（选择文件夹all，里面含有一个crt和一个key文件）

目标格式 jks

证书文件 选择下载的crt结尾的文件

私钥文件 选择下载的key结尾的文件

私钥密码 不填（默认控制台下载无密码）

密钥库密码/新文件密码 自己设置一个，不加特殊符号，一会配置文件里用到(如server.xml)

Copyright © 2012-2021 UCloud 优刻得

证书域名含有中文字符

域名中含有中文字符，可先将中文字符域名进行转码，在进行证书申请，域名转码地址：https://myssl.com/punycode.html

Copyright © 2012-2021 UCloud 优刻得

为App部署SSL证书 应对苹果ATS限制

2021年12月1日起，使用文件验证(HTTP)的域名 只能为被验证域名本身签发证书，不支持签发通配符证书和其下级子域名证书

1、目前，行业允许仅对主域名(domain.com)进行域名验证即可，适用于通配符证书(如*.domain.com或*.sub.domain.com等)和其下级所有子域名(如sub.domain.com或sub2.sub1.domain.com等)。

2、DigiCert将在2021年11月15日后，对于使用文件方式验证的域名，只能为被验证域名本身签发证书。如 使用文件验证方式验证域名domain.com，则只能为domain.com签发证书，不能为*.domain.com 或sub.domain.com 签发证书。

3、DNS验证和邮箱验证方式则不受影响，建议优先使用DNS或邮件验证方式。

DigiCert 公告: https://knowledge.digicert.com/alerts/domain-authentication-changes-in-2021.html

GlobalSign公告：https://www.globalsign.com/en/blog/upcoming-changes-publicly-trusted-tls-certificates

Copyright © 2012-2021 UCloud 优刻得

如何验证域名所有权

申请域名型证书时，系统需通过以下方式验证域名的所有权

1.管理员邮箱验证

系统会向你选择的管理员邮箱 发送验证邮件，能够收到验证邮件

并点击邮件中验证链接 即可完成验证。

域名管理员邮箱须符合以下任意规则：

1.域名 whois 管理联系人邮箱

2.域名 whois 技术联系人邮箱

3.默认管理员前缀的邮箱：

```
admin@domain.com
administrator@domain.com
hostmaster@domain.com
webmaster@domain.com
postmaster@domain.com
```

2.DNS验证

通过解析指定的DNS记录验证域名所有权

例如（linux系统下面）dig www.ucloud.cn txt; (windows下面) nslookup www.ucloud.cn txt

Copyright © 2012-2021 UCloud 优刻得

若能检测到 并且与指定的值匹配 则最多等候10分钟可完成域名所有权验证。

如果域名存在CNAME解析 需要特殊处理一下

在主机名前端加_dnsauth

配置 域名 _dnsauth.www.demo.com，TXT记录值为 系统返回的txt记录值

3.文件验证

通过在域名根目录下创建指定的文件验证域名所有权

例如:创建文件 irmvo302.htm 文件内容 NtdutxbskfhWvP3OffXW

系统会定时尝试访问 http://xxx.domain/irmvo302.htm 这个文件,若能访问到 并且内容匹配即可完成域名所有权验证。

Copyright © 2012-2021 UCloud 优刻得

证书的颁发时间说明

1、免费证书为DV证书，为系统签发，验证正确20分钟后自动签发，最长不超过一天，超过一天请更换OV\EV类型证书

2、付费DV证书，如TrustAsia-DV通配符证书，也为系统自动签发证书，验证正确20分钟后自动签发，最长不超过一天，超过一天请更换OV\EV类型证书

3、OV\EV付费证书，需人工审核，审核时间为5-7天左右

备注：DV证书自行检测地址：https://myssl.com/dns_check.html#ssl_verify

Copyright © 2012-2021 UCloud 优刻得

证书退费说明

证书退费说明： 证书颁发的一段时间内，可以视情况吊销证书并申请退款

证书颁发时间：globalsign证书：7天内；securesite、geotrust、trustasia、cfca证书：30天内）

证书吊销、退费流程：

1、点击控制台的吊销按钮，并进行相关验证（吊销验证流程同购买验证流程）

2、吊销成功后，可点击控制台的退费按钮进行退费操作

Copyright © 2012-2021 UCloud 优刻得

SSL证书重颁发声明

关于重颁发说明：

- 基于证书产品自带时间戳的属性，超过有效期的证书均为失效证书不可用，需要做续费操作。
- 续费订单会重新做信息验证,和新订单的验证流程一致。
- DV续费证书－验证域名所有权后签发
- OV,EV续费证书－验证域名所有权和公司信息完成后签发

Copyright © 2012-2021 UCloud 优刻得

https字样并非呈现绿色

请检查部署安装是否正确。修改成https或相对路径方式调用即可。

链接中存在外链，比如：http:等

Copyright © 2012-2021 UCloud 优刻得

DV证书自主检测工具手册

申请Domain Validation（DV）类型的SSL证书时，Certificate Authority（CA）机构只验证域名所有权，不会人工介入审核验证。这一特性使DV证书颁发十分方便快捷，但也导致在系统审核的过程中产生很多验证限制，例如安全审核，DNS验证失败等，影响证书的正常颁发。

为了使用户能够自主定位问题，查询原因，调整配置，提高DV证书的的颁发效率，我司提供《DV证书自主检测工具》（以下简称“工具”）。

通过访问https://myssl.com/dns_check.html#ssl_verify使用此工具。

具体使用方法参见手册：

DV证书自主检测工具手册

Copyright © 2012-2021 UCloud 优刻得

SSL 证书过期了怎么办?

SSL 数字证书过期之后，将无法继续使用，您需要在您的证书到期前办理续费并验证完毕

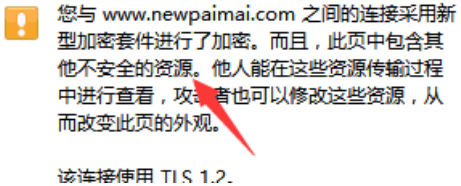
续费完成后，证书服务系统将续期完成将复制当前证书订单的信息到续费订单中，同时自动将续费证书订单提交审核。

审核通过后，您将获得一张新的数字证书，您需要在您的服务器上安装新的数字证书来替换即将过期的证书。

Copyright © 2012-2021 UCloud 优刻得

证书正常安装后提示不安全

正常安全却提示不安全，说明https含有外链导致，HTTPS为加密传输，http是明文传输；修改成HTTPS或相对路径方式引用（chrome浏览器 打开开发者工具 控制台处有提示）



Copyright © 2012-2021 UCloud 优刻得

证书格式的区别

根据web服务软件选择

Tomcat、Weblogic、JBoss等，使用Java提供的密码库。通过Java的Keytool工具，生成Java Keystore（JKS）格式的证书文件。

Apache、Nginx等，使用OpenSSL提供的密码库，生成PEM、KEY、CRT等格式的证书文件。

此外，IBM的产品，如**Websphere、IBM Http Server（IHS）等**，使用IBM产品自带的iKeyman工具，生成KDB格式的证书文件。

微软Windows Server中的**Internet Information Services（IIS），**使用Windows自带的证书库生成PFX格式的证书文件。

根据证书后缀名选择

DER、CER：这样的证书文件是二进制格式，只含有证书信息，不包含私钥。通常只保存公钥。

CRT：二进制格式或者文本格式，适合Apache、Nginx等使用

PEM：一般是文本格式，可以放证书或私钥，或者两者都包含。*.PEM如果只包含私钥，那一般用 *.KEY代替。适合Apache、Nginx等使用

PFX、** P12** 是二进制格式，同时含证书和私钥，一般有密码保护。适用于微软的IIS。

JKS：适用于Tomcat、weblogic、JBoss等

Copyright © 2012-2021 UCloud 优刻得

为App部署SSL证书 应对苹果ATS限制

ATS（App Transport Security）与HTTPS

App Transport Security，简称 ATS，是苹果在 iOS 9 当中推出的一项安全功能。

在开启 ATS 安全特性之后，它会强制App应用及网页通讯自动通过 HTTPS加密传输连接网络服务，通过加密App及网页通讯来保障用户数据安全。即 App后端服务器必须部署SSL证书，启用HTTPS加密协议，否则您的App应用将不能通过苹果商店的审核发布，导致App应用无法正常使用。

ATS功能解读

1. **HTTPS**： App后端服务器必须启用HTTPS加密传输网络服务

2. **TLS1.2**： 服务器所有连接必须支持TLS协议1.2以上版本

3. **哈希算法**： SSL证书是使用SHA256或者更高级的ECC算法

4. **密钥**： SSL证书是使用2048位以上RSA密钥

5. **正向保密：**加密套件配置要求，支持苹果列出的正向保密列表（苹果配置官方文档）

如何便捷通过ATS安全功能要求

Copyright © 2012-2021 UCloud 优刻得

选择合适的服务器SSL证书，启用HTTPS加密连接。截止2016年底，为助力App开发者应对Apple ATS策略，我们提供更优惠的SSL证书申请。国际知名的Symantec SSL证书可满足ATS的各项要求，特别是具有ECC 算法的SSL证书，公钥长度短，延长设备寿命省电并且节省流量 。

便捷免费的ATS检测工具：针对ATS的要求，提供便捷免费的 ATS检测工具,即可一键检测与您App应用交互的服务器是否符合ATS要求。

Copyright © 2012-2021 UCloud 优刻得

《苹果公司宣布Safari浏览器对SSL证书有效期的新要求》说明

近日,苹果公司在第49届CA/浏览器论坛(CA/Browser)会议上宣布：为了提高网络安全性，任何有效期超过了398天的新网站证书都将不会受到Safari浏览器的信任。但是，在截止日期(2020年9月1日)之前颁发的证书不受此规则的影响。

简单来说当SSL证书同时满足以下条件时，将不会被Safari信任：

1、在2020年9月1日之后签发

2、有效期超过398天

在2020年9月1日前签发的证书不受影响。此举目的是通过确保开发者使用最新加密标准的证书来提高网站的安全性,并减少被忽视的旧证书的数量,这些证书有可能被盗窃,并被用于网络钓鱼和驱动器恶意软件攻击。

为保障您的服务可用性,UCloud安全中心建议您:评估受影响程度,合理利用现有证书规则,规划证书申请的有效生命周期。

Ucloud SSL证书优势：

1、UCloud支持可信CA认证机构提供的Symantec、GlobalSign、Geotrust、TrustAsia、CFCA等品牌多类型的一年期、两年期证书

2、支持多平台证书的统一管理

3、支持临过期证书告警,预防证书过期带来的业务风险

4、支持云上证书相关产品一键分发

Copyright © 2012-2021 UCloud 优刻得

多年期证书答疑

1、购买的多年期证书为什么签发的证书有效期只有一年?

由于苹果浏览器对证书的要求,ssl证书有效期最长不超过398天(13个月),多年期每次签发有效期为1年的证书,每年都需验证完成后,证书自动签发,客户需重新下载和部署证书。

验证过程:

第一年:企业身份验证+域名验证

第二年:域名验证(企业身份有效期为398天,第二年只需验证域名所有权)

第三年:企业身份验证+域名验证

2、多年期证书后续验证是否还会二次收费?

多年期证书为一次性收费,后续不会二次收费

3、苹果浏览器对SSL证书的安全要求说明

详情请查看:https://docs.ucloud.cn/ussl/faq/Safari

Copyright © 2012-2021 UCloud 优刻得

免费证书配额说明

1、同一个账户的免费证书配额默认为40个，免费证书有效期三个月

2、同一主域名下证书不超过5个，其他平台购同样占用额度

3、40个指控制台上有效期内免费证书的总数量，手动删除的但处于有效期状态内的证书仍然占用额度

Copyright © 2012-2021 UCloud 优刻得