教育网域名安全证书服务方案 (CFCA证书)

赛尔网络有限公司

工程研究中心

2020年6月



	录
	-

目

一、CFCA 全球信任 SSL 证书介绍	1
1.1 什么是 SSL 证书?	1
1.2 什么是 CFCA 全球信任 SSL 证书?	1
1.3 CFCA 全球信任 SSL 证书有哪些优势?	2
1.4 CFCA 全球信任 SSL 证书有哪些产品?	2
1.4.1 CFCA EV SSL 证书	2
1.4.2 CFCA EV 多域名 SSL 证书	4
1.4.3 CFCA OV SSL 证书	5
1.4.4 CFCA OV 多域名 SSL 证书	5
1.4.5 CFCA OV 通配符 SSL 证书	6
1.5 CFCA 全球信任 SSL 证书教育行业用户案例	7
二、CFCA EV/OV 证书办理说明	7
2.1 申请材料说明	7
2.2 审核说明	10
2.3 证书签发	10
2.4 证书更新、延期、吊销	10
三、CFCA 全球信任 SSL 证书制作	10
3.1 证书制作说明	10
3.2 密钥和证书请求文件 CSR	11
3.3 证书文件格式	11
3.4 证书制作	12
3.4.1 简易便捷的在线制作方式(优先推荐使用)	12
3.4.2 使用 Keytool 工具制作证书	12
3.4.3 使用 OpenSSL 工具制作证书	15
3.4.4 使用 iKeyman 工具制作证书	17
3.5 证书格式转换	22
3.5.1 工具转换(优先推荐)	22
3.5.2 JKS 转换为 PFX	22
3.5.3 PFX 转换为 JKS	22
3.5.4 KEY&CRT 转换为 PFX	23
3.5.5 PFX 转换为 KEY&CRT	23
3.5.6 KDB 转换为 PFX	23
3.5.7 PFX 转换为 KDB	24
3.5.8 KYR 格式证书制作	29
3.6 证书部署方法	31
3.6.1 Apache 证书配置	31
3.6.2 Tomcat 证书配置	32
3.6.3 Nginx 证书配置	34
3.6.4 Weblogic 证书配置	37
3.6.5 IBM Http Server 证书配置	40



	3.6.6 JBoss 业书配置	
	3.6.7 IIS 证书配置	41
	3.6.8 Websphere 证书配置	47
	3.6.9 IHS+WAS 证书配置	55
	3.6.10 F5 设备证书配置	56
	3.6.11 SAP 证书配置	
	3.6.12 阿里云通用证书配置	
	3.6.13 阿里云 LSB 证书配置	65
	3.6.14 腾讯云证书配置	
附录一、	CFCA 全球信任证书(SSL 证书)申请表	
附录二、	CFCA 域名验证方式	
附录三、	CFCA 全球信任根证书获取方式	
附录四、	CFCA 全球信任证书链	
附录五、	SHA 摘要算法介绍	
附录六、	常见问题	
附录七、	销售服务渠道和联系人	
×	HAN HANN	

一、CFCA 全球信任 SSL 证书介绍

1.1 什么是 SSL 证书?

随着信息技术的发展,互联网站以及基于互联网的应用系统面临越来越严重 的安全威胁。其中,网站面临的两个最基本的问题是:

1、网站身份的真实性

用户访问网站时需要确认网站的真实性。由于互联网的开放和共享,互联网上存在很多虚假的网站。如何让用户信任自己访问的网站是真实的?

2、信息传输的保密性

大量的网上应用需要用户向网站应用系统提交一些隐私或者机密信息,同时 网站应用系统也可能向用户返回一些隐私或者机密信息。如何确保信息传输过程 中的安全?

SSL证书,是由权威的、可信的第三方数字证书认证机构(CA)签发,用来标记网站身份的数字证书。因其通常部署在网站服务器上,也称为网站证书或者服务器证书。SSL证书通过在客户端浏览器和网站服务器之间建立一条 SSL 安全通道(Secure Socket Layer),对传输的数据进行加密,确保数据在传输过程中不被窃听、篡改和伪造。有效地解决了网站身份的真实性和信息传输的保密性问题。

赛尔网络与国内权威 CA 机构 CFCA 合作为教育网用户提供国产 SSL 证书服务,证书类型丰富,操作流程简单方便,为高校用户提供一站式 HTTPS 安全解决方案。提供 SSL 证书的申请、管理、部署等服务,轻松实现网站与 Web 应用的HTTPS 加密部署。

1.2 什么是 CFCA 全球信任 SSL 证书?

中国金融认证中心(China Financial Certification Authority,简称 CFCA)是经中国人民银行和国家信息安全管理机构批准成立的国家级权威安全认证机构,是国家重要的金融信息安全基础设施之一。在《中华人民共和国电子签名法》颁布后,CFCA 成为首批获得电子认证服务许可的电子认证服务机构。

中国金融认证中心全球信任证书(Global Trust Certificate)是发放给全球范围的数字证书,通过微软根证书项目认证、Mozilla 根证书认证,谷歌(安卓)根证书认证和苹果根证书认证,其根证书已经预埋在微软系统、设备,Mozilla 相关

产品,谷歌(安卓操作系统)相关产品以及苹果相关产品中。

CFCA 全球服务器证书(SSL 证书)由 CFCA 自主研发。CFCA 作为国内第一家 与国外 SSL 服务器证书厂商媲美的电子认证服务机构,严格按照国际标准提供电 子认证服务,并结合我国国情,在密码算法、安全技术服务等方面兼容国际和国 产算法。目前已通过第三方审计公司按照国内、国际双重标准进行的审计。

CFCA 全球服务器证书(SSL 证书)相当于 Web 站点的网络身份证,可为 Web 站点提供身份鉴定,并为 Web 站点提供高强度安全加密传输,保证信息在传输 过程中的安全,能够有效地防止信息传输过程中的网络钓鱼、窃听、篡改等安全 问题。

1.3 CFCA 全球信任 SSL 证书有哪些优势?

CFCA 全球信任 SSL 证书的优势:

- ✓ 由中国权威数字证书认证机构 CFCA 签发;
- ✓ CFCA 是国际 CA 浏览器联盟组织(CA/Browser Forum)成员,是国际 证书标准的参与者;
- ✓ CFCA 通过国际 WebTrust 认证,遵循全球统一鉴证标准;
- ✔ 根系统、吊销列表、证书管理、鉴证资料、服务支持本地化;
- ✓ 金融级的安全保障服务;
- ✔ 完善的风险承保计划,确保理赔的可行性和便捷性;
- ✓ 中文版 CPS (全球信任体系电子认证业务规则)便于用户理解双方权 利和义务。

1.4 CFCA 全球信任 SSL 证书有哪些产品?

- CFCA 全球信任 SSL 证书包括:
- CFCA EV SSL 证书
- CFCA EV 多域名 SSL 证书
- CFCA OV SSL 证书
- CFCA OV 多域名 SSL 证书
- CFCA OV 通配符 SSL 证书

1.4.1 CFCA EV SSL 证书

CFCA EV SSL 服务器证书相当于网站的身份证,可为网站提供身份鉴定和高强度安全加密服务。CFCA EV SSL 证书遵循全球统一认证标准中最严格的 Webtrust EV 标准。部署 CFCA EV SSL 证书的网站,浏览器地址栏自动变成绿色,循环显示公司名称(支持中文)和 CFCA 认证机构标识。访客浏览器和网站服务器之间建立起 SSL 安全加密通道(Secure Sockets Layer),有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。主流浏览器效果参见下图:

	e	https://www.cfca.com.cn	单位名称 [CN]	с×
	Interr	net Explorer		
9	Chro	单位名称 [CN] www.cfca.com.cn me		\$
٩	Firefo	● 单位名称 [CN] www.cfca.com.cn	\$	⊽ C ⁱ
١	Safar	单位名称 [CN] www.cfca.com.cn i	ĊR	eader
		Trusted www.cfca.com.cn		*
Ū	✓ ✓ ✓	有效期1至2年; 2至5个工作日快速签发; 有效期内免费重新签发; 证书到期前自动提醒;		
	√	提供安全站占然音.		
	$\overline{\mathbf{A}}$	支持 RSA 算法,2048 位密钥强度,SHA256 摘要算	法;	
X	\checkmark	Windows 平台浏览器 100%支持,包括但不限于:	Internet Exp	lorer、
17	$\boldsymbol{\zeta}$	Google Chrome、Mozilla Firefox(版本 38 及更新版	(本)、Oper	ra,以
		及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产	^立 浏览器;	
	✓	Windows Phone 平台浏览器 100%支持;		
	✓	Android (Android 6.0 Marshmallow 及更新版本)平	白浏览器 1	00%支
		持;		
	✓	Linux 平台浏览器 100%支持;		

✓ Mac OS(10.12.1 及更新版本)平台浏览器 100%支持,包括但不限于:

Safari、Google Chrome、Mozilla Firefox 等;

- ✓ IOS (10.1 及更新版本)平台浏览器 100%支持;
- ✓ 支持苹果 ATS;
- ✓ 支持 128 位至 256 位加密强度;
- ✔ 最高人民币 50 万元赔付保障。

1.4.2 CFCA EV 多域名 SSL 证书

CFCA EV 多域名 SSL 证书,将有限多个域名写入一个证书文件中,可以同时保护多个域名的 EV SSL 证书。部署 CFCA EV 多域名 SSL 证书的多个网站,浏览器地址栏自动变成绿色,循环显示公司名称(支持中文)和 CFCA 认证机构标识。访客浏览器和网站服务器之间建立起 SSL 安全加密通道(Secure Sockets Layer), 有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。

- ✓ 有效期1至2年;
- ✓ 2至5个工作日快速签发;
- ✔ 有效期内免费重新签发;
- ✔ 证书到期前自动提醒;
- ✔ 提供安全站点签章;
- ✓ 支持 RSA 算法, 2048 位密钥强度, SHA256 摘要算法;
- ✓ Windows 平台浏览器 100%支持,包括但不限于: Internet Explorer、 Google Chrome、Mozilla Firefox(版本 38 及更新版本)、Opera,以 及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器;
- / Windows Phone 平台浏览器 100%支持;
- Android (Android 6.0 Marshmallow 及更新版本) 平台浏览器 100%支持;
- ✓ Linux 平台浏览器 100%支持;
- ✓ Mac OS(10.12.1 及更新版本)平台浏览器 100%支持,包括但不限于:
 Safari、Google Chrome、Mozilla Firefox 等;
- ✓ IOS (10.1 及更新版本)平台浏览器 100%支持;
- ✓ 支持苹果 ATS;
- ✓ 支持 128 位至 256 位加密强度;

✔ 最高人民币 50 万元赔付保障。

1.4.3 CFCA OV SSL 证书

CFCA OV SSL 服务器证书相当于网站的身份证,可为网站提供身份鉴定和高强度安全加密服务。部署 CFCA 标准 SSL 证书的网站,浏览器地址栏有锁的标志,可以查看证书颁发机构名称,增加客户信赖度。访客浏览器和网站服务器之间建立起 SSL 安全加密通道(Secure Sockets Layer),有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。

- ✓ 有效期1至2年;
- ✓ 2至5个工作日快速签发;
- ✔ 有效期内免费重新签发;
- ✔ 证书到期前自动提醒;
- ✔ 提供安全站点签章;
- ✓ 支持 RSA 算法, 2048 位密钥强度, SHA256 摘要算法;
- ✓ Windows 平台浏览器 100%支持,包括但不限于: Internet Explorer、 Google Chrome、Mozilla Firefox(版本 38 及更新版本)、Opera,以 及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器;
- ✓ Windows Phone 平台浏览器 100%支持;
- ✓ Android (Android 6.0 Marshmallow 及更新版本)平台浏览器 100%支持;
 持; Linux 平台浏览器 100%支持;
- ✓ Mac OS(10.12.1 及更新版本)平台浏览器 100%支持,包括但不限于:
 Safari、Google Chrome、Mozilla Firefox 等;
- ✓ IOS (10.1 及更新版本)平台浏览器 100%支持;
- ✓ 支持苹果 ATS;
- ✓ 支持 128 位至 256 位加密强度;
- ✔ 最高人民币 50 万元赔付保障。

1.4.4 CFCA OV 多域名 SSL 证书

CFCA OV 多域名 SSL 证书,将有限多个域名写入一个证书文件中,可以同时保护多个域名的 SSL 证书。部署 CFCA 标准多域名 SSL 证书的多个网站,浏览器地址栏有锁的标志,可以查看证书颁发机构名称,增加客户信赖度。访客浏览器

和网站服务器之间建立起 SSL 安全加密通道(Secure Sockets Layer),有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。

- ✓ 有效期1至2年;
- ✓ 2至5个工作日快速签发;
- ✔ 有效期内免费重新签发;
- ✔ 证书到期前自动提醒;
- ✔ 提供安全站点签章;
- ✓ 支持 RSA 算法, 2048 位密钥强度, SHA256 摘要算法;
- ✓ Windows 平台浏览器 100%支持,包括但不限于: Internet Explorer、 Google Chrome、Mozilla Firefox(版本 38 及更新版本)、Opera,以 及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器;
- ✓ Windows Phone 平台浏览器 100%支持;
- ✓ Android (Android 6.0 Marshmallow 及更新版本)平台浏览器 100%支持;
 挂; Linux 平台浏览器 100%支持;
- ✓ Mac OS(10.12.1 及更新版本)平台浏览器 100%支持,包括但不限于:
 Safari、Google Chrome、Mozilla Firefox 等;
- ✓ IOS (10.1 及更新版本)平台浏览器 100%支持;
- ✓ 支持苹果 ATS;
- ✓ 支持 128 位至 256 位加密强度;
- ✔ 最高人民币 50 万元赔付保障。

1.4.5 CFCA OV 通配符 SSL 证书

CFCA OV 通配符 SSL 证书适用于网站主域名(domain.com)以及子域名 (*.domain.com),不限制子域名数量。部署 CFCA 标准通配符 SSL 证书的多个 网站,浏览器地址栏有锁的标志,可以查看证书颁发机构名称,增加客户信赖度。 访客浏览器和网站服务器之间建立起 SSL 安全加密通道(Secure Sockets Layer), 有效地防止信息传输过程中的网络窃听、伪造、篡改等安全问题。

- ✓ 有效期1至2年;
- ✓ 2至5个工作日快速签发;
- ✔ 有效期内免费重新签发;

- ✔ 证书到期前自动提醒;
- ✔ 提供安全站点签章;
- ✓ 支持 RSA 算法, 2048 位密钥强度, SHA256 摘要算法;
- ✓ Windows 平台浏览器 100%支持,包括但不限于: Internet Explorer、 Google Chrome、Mozilla Firefox(版本 38 及更新版本)、Opera,以 及 360、搜狗、遨游、QQ、UC、猎豹、百度等国产浏览器;
- ✓ Windows Phone 平台浏览器 100%支持;
- ✓ Android (Android 6.0 Marshmallow 及更新版本)平台浏览器 100%支持;
 持; Linux 平台浏览器 100%支持;
- ✓ Mac OS(10.12.1 及更新版本)平台浏览器 100%支持,包括但不限于:
 Safari、Google Chrome、Mozilla Firefox 等;
- ✓ IOS (10.1 及更新版本)平台浏览器 100%支持;
- ✓ 支持苹果 ATS;
- ✓ 支持 128 位至 256 位加密强度;
- ✔ 最高人民币 50 万元赔付保障。

1.5 CFCA 全球信任 SSL 证书教育行业用户案例

中国人民解放军国防科技大学、中国劳动关系学院、首都体育学院、北京经济管理职业学院、内蒙古财经大学、上海市建筑工程学校、北京市第二十中学、江苏省教育考试院、内蒙古自治区教育招生考试中心、湖南省中小学教师发展中心

二、CFCA EV/OV 证书办理说明

CFCA 全球信任 SSL 证书办理过程,申请机构必须提供真实的材料,以证明 机构的真实身份、申请人的真实身份、机构对域名的所有权等。CFCA 将对机构 提供的材料进行严格审查。

2.1 申请材料说明

申请机构需要向 CFCA 提供如下材料:

1、全球信任服务器证书申请表,需加盖公章(单位公章或带单位名称的部 门章即可);文件参考<u>附录一</u>



2、证书请求文件 CSR(生成方式请访问 <u>https://ssl.cfca.com.cn/Web/tool</u>, 详细说明请参考 3.4.1 章节)。

3、域名所属机构的身份证件复印件(如事业单位法人证书,无需盖章);

4、经办人身份证件复印件(如身份证,无需盖章);

5、根据自身情况选择域名验证方式以完成域名验证。CFCA 域名验证支持邮件验证、DNS 验证、文件验证及域名证书(盖章)四种方式。详细区别及操作方法参考以下文档或<u>附录二</u>

PDF 域名验证指南-V1. 2.pdf

6、公网 IP 的证明(一般为网络运营商出具,用于证明 IP 所有权,仅申请 IP 形式的 OV SSL 证书时需要提供);

IP 使用权证明示例如下:

公网 IP 证明函

	中金金融认证中	心有限公司	:				
	运营商:	(运营商名称	()			
	证明以下公网 IF	>地址:			Х		
	IP1:				, H	1	
	IP2:				- D)	
	IP3:		<i>V</i>	X			
	为我司分配给			(证书申	请单位	(名称)	使
用!			K				
		FR					
<u> </u>		运营商:				(公置	<u> </u>
救	\rightarrow		I	时间:	年	月	日

所盖公章为单位公章,可使用部门章,公章(部门章)的名称要与单位名称 一致。

申请机构需要将上述所有材料的电子版提供给赛尔网络,申请机构必须保证

所提供材料的真实性,赛尔网络将协助申请机构办理证书。

2.2 审核说明

赛尔网络业务部门将对申请机构提供的材料进行审查,主要内容包括:

1、检查证书申请表中机构信息与提供的机构身份证件是否相符。

2、检查证书申请表中申请人信息与提供的申请人身份证件是否相符。

3、检查证书申请表中域名与提供的域名证明是否相符。如域名非申请机构 所有,则需要申请机构提供该域名所有者出具的唯一使用该域名的授权证明材料。 如使用公网 IP,需提供网络运营商出具的 IP 使用权证明。

4、CSR 文件, DN 规则要求符合如下规范:

(1) DN 中各项顺序依次为: CN、OU、O、L、ST、C;

(2) CN 项是域名或者 IP, 与证书申请表中域名一致;

(3)O项必须是真实的、完整的机构名称,与证书申请表中机构名称一致;

(4)L项、ST项、C项是必须是机构注册地,与机构身份证件中的注册地区 一致。

2.3 证书签发

CFCA 最终审核通过后,将由赛尔网络证书管理员签发证书。证书公钥及证书链将发送到证书申请表中的申请人邮箱。

2.4 证书更新、延期、吊销

使用证书过程中,如果出现证书遗失、损坏、密钥泄露等问题,需要重新签 发证书,机构应按照 1.1 章节重新提供材料办理证书。证书有效期内 CFCA 免费 进行证书操作。

证书到期前三个月内,赛尔网络会主动提醒机构申请联系人办理证书延期。 机构应按照 2.1 章节重新提供材料办理证书延期。

机构如果不再使用证书,可以联系赛尔网络办理证书吊销,并将该证书从网 站服务器上移除。

三、CFCA 全球信任 SSL 证书制作

3.1 证书制作说明

CFCA 全球信任 SSL 证书需要部署在网站 Web 服务上,制作证书之前请先了 解网站 Web 服务所使用的软件或者硬件。

1、如果网站使用网关、负载均衡等硬件设备提供 Web 服务,请咨询相应的 硬件厂商制作和部署 SSL 证书的方法。

2、如果网站使用 IBM Http Server (IHS)、Internet Information Services (IIS)、 Oracle Weblogic 等商业软件提供 Web 服务,请优先咨询软件厂商制作和部署 SSL 证书的方法。本章节也提供了部分商业软件制作 SSL 证书方法,仅供参考。

3、如果网站使用 Nginx、Apache、Tomcat 等开源软件,请优先通过开源软件的技术文档了解制作和部署 SSL 证书的方法。本章节也提供了部分开源软件制作 SSL 证书方法,仅供参考。

4、部署 SSL 证书时,必须部署相应的证书链。办理 CFCA EV SSL 证书,需要 部署根证书 CFCA EV Root 和中级证书 CFCA EV OCA;办理 CFCA OV SSL 证书,需 要部署根证书 CFCA EV Root 和中级证书 CFCA OV OCA。证书链文件会与证书文件 一起发送到证书申请表中的申请人邮箱。关于证书链的详细信息可参考"<u>附录四、</u> CFCA 全球信任证书链"。

3.2 密钥和证书请求文件 CSR

SSL证书中含有一套非对称密钥,用于客户端浏览器和网站服务器之间的数据加密。证书申请机构应当在安全的服务器或者设备上生成密钥和证书请求文件 CSR(Cerificate Signing Request)。其中,CSR 提交给 CFCA 用于签发证书(详见 1.1 章节),密钥由证书申请机构保管。

特别提醒,任何机构或者个人如果拥有该密钥,即可通过技术手段解密客户 端浏览器和网站服务器之间的加密数据,给网站和网站用户造成极大的安全威胁。 因此,证书申请机构务必妥善保管密钥!一旦密钥泄露,请证书申请机构重新生 成密钥和 CSR,并立即联系赛尔网络进行证书更新(参考 1.4 章节)。赛尔网络 将使用新提供的 CSR 申请并签发证书,并将原证书吊销。

3.3 证书文件格式

一般来说, 主流的 Web 服务软件, 通常都基于两种基础密码库: OpenSSL 和 Java。

Tomcat、Weblogic、JBoss 等,使用 Java 提供的密码库。通过 Java 的 Keytool

11

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。

3.4 章节提供了部分主流的 Web 服务软件生成密钥、CSR、证书文件的方法,

3.5 章节提供了常用证书文件格式相互转换的方法,仅供参考。

3.4 证书制作

3.4.1 简易便捷的在线制作方式(优先推荐使用)

CFCA 提供的证书制作网站地址是: <u>https://ssl.cfca.com.cn</u>,可以通过此网站 生成证书请求文件 CSR 和密钥 key 文件。证书申请机构将证书请求文件 CSR 连同 相关材料(详见 1.1)提供给赛尔网络,并妥善保管密钥文件(key.txt)。赛尔网 络审核资料后,将公钥证书和证书链反馈给证书申请机构。证书申请机构在通过 此网站合成需要使用格式的证书文件。网站具体使用方法详见相关手册。

3.4.2 使用 Keytool 工具制作证书

Keytool 是 JDK 中自带的密钥管理工具,可以制作 Keystore (jks) 格式的证书 文件。下载并安装 JDK 后,可以通过相关命令制作服务器证书。

以下地址可以下载 JDK:

https://www.oracle.com/java/technologies/

以下以 Windows 平台为例,介绍制作证书的方法。

1、进入 Keytool 目录;

cd C:\Program Files\java\jdk1.6.0_39\bin

2、生成证书文件 Keystore,文件后缀名可以是 jks、keystore,证书文件中包含密钥;

keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore D:\server.jks

其中, keyalg 是密钥类型, 必须为 RSA; keysize 是密钥长度, 必须是 2048,

alias 是证书别名,可自定义; keystore 是证书文件保存的路径。

而后,输入证书文件的密码:

输入 keystore 密码:

再次输入新密码:

而后,输入名称(CN),即证书申请表中的域名;

您的名字与姓氏是什么?

[Unknown]: www.cfca.com.cn

而后,输入组织单位(OU),即证书申请表中申请人的部门名称;

您的组织单位名称是什么?

[Unknown]: 技术支持部

而后,输入组织(O),即机构身份证件中机构名称全称;

您的组织名称是什么?

[Unknown]: 中金金融认证中心有限公司

而后,输入城市(L),即机构身份证件中机构所在市级地区;

您所在的城市或区域名称是什么?

[Unknown]: 北京

而后,输入省份(ST),即机构身份证件中机构所在省级地区;

您所在的州或省份名称是什么?

[Unknown]: 北京

而后,输入机构身份证件中机构所在的国家或者行政区(C),限定两位字

母,如中国输入 CN,美国输入 US 等;

该单位的两字母国家代码是什么?

[Unknown]: CN

输入完成后,确认输入内容是否正确;

CN=www.cfca.com.cn, OU=技术支持部, O=中金金融认证中心有限公司, L=北京, ST=北京, C=CN

正确吗?

[否]: Y

而后,提示输入密钥(Key)密码,可以与证书(Keystore)密码一致;

输入<server>的主密码

(如果和 keystore 密码相同, 按回车):

确认后,即在 keystore 保存的路径下,生成证书文件(server.jks)。

3、通过证书文件, 生成证书请求;

keytool -certreq -sigalg SHA256withRSA -alias server -keystore d:\server.jks -file d:\certreq.csr

其中, sigalg 是摘要算法, 推荐 SHA256withRSA; alias 是别名, 必须与第 2 步 生成证书文件时定义的别名一致; keystore 是证书文件的路径, file 是产生证书 请求(CSR)的路径。

而后,提示输入 keystore 的密码;

输入 keystore 密码:

确认后,即产生证书请求(CSR)文件(certreq.csr)。,,

4、证书申请机构将证书请求文件(certreq.csr)连同相关材料(详见 2.1)提供给赛尔网络,并妥善保管证书文件(server.jks)。

5、赛尔网络审核资料后,将公钥证书和证书链反馈给证书申请机构。

6、证书申请机构将收到的公钥证书和证书链(包括根证书和中级证书)装回到证书文件(server.jks)中。

其中,证书文件一般以申请单位全称命名; EV SSL 证书的根证书是 CFCA_EV_CA.cer; 中级证书是 CFCA_EV_OCA.cer; OV SSL 证书的根证书是 CFCA_OV_CA.cer; 中级证书是 CFCA_OV_OCA.cer(详见附录四)。

7、导入根证书(以 EV SSL 证书为例, OV SSL 证书请导入 OV 的根证书,下同);

keytool -import -alias evca -keystore d:\server.jks -trustcacerts -file d:\CFCA_EV_CA.cer

而后,输入证书文件密码;

输入 keystore 密码:

而后,会显示根证书的属性;

所有者: CN=CFCA EV ROOT, O=China Financial Certification Authority, C=CN

发布者: CN=CFCA EV ROOT, O=China Financial Certification Authority, C=CN

序列号: 184accd6

有效期开始日期: Wed Aug 08 11:07:01 CST 2012,截止日期: Mon Dec 31 11:07:01 CST 2029 证书指纹: MD5: 74:E1:B6:ED:26:7A:7A:44:30:33:94:AB:7B:27:81:30

SHA1: E2:B8:29:4B:55:84:AB:6B:58:C2:90:46:6C:AC:3F:B8:39:8F:84:83

SHA256:

5C:C3:D7:8E:4E:1D:5E:45:54:7A:04:E6:87:3E:64:F9:0C:F9:53:6D:1C:CC:2E:F8:00:F3:55:C4:C5:FD:7 0:FD

签名算法名称: SHA256withRSA

.....

而后,确认信任认证,导入完成。

信任这个认证? [否]: Y

认证已添加至 keystore 中

8、导入中级证书;

keytool -import -alias evoca -keystore d:\server.jks -trustcacerts -file d:\CFCA_EV_OCA.cer

而后,输入证书文件密码;

输入 keystore 密码:

导入完成。

认证已添加至 keystore 中

9、导入服务器证书(证书文件一般以申请单位的全称命名);

keytool -import -alias server -keystore d:\server.jks -trustcacerts -file d:\中金金融认证中心有限 公司.cer

其中,别名(alias)必须是生成证书文件时设置的别名,必须与第2步生成 证书文件时定义的别名一致;

而后,输入证书文件密码;

输入 keystore 密码:

导入完成。

认证已添加至 keystore 中

完成上述操作后,生成完整的证书文件(server.jks),可以部署在 Tomcat、 Weblogic 等 Web 应用中。

3.4.3 使用 OpenSSL 工具制作证书

使用 OpenSSL 工具可以制作 KEY 和 CRT 格式的证书文件, OpenSSL 工具可以

从以下地址下载:

http://www.openssl.org/

以下以 Windows 平台为例,介绍制作证书的方法。

1、进入 OpenSSL 目录;

cd D:\OpenSSL\bin

2、生成证书文件 key 和证书请求文件 csr;

openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr

其中, newkey 必须是 rsa:2048, key 为密钥文件, csr 为证书请求文件, 默认都在 OpenSSL 目录下;

Generating a 2048 bit RSA private key

.....+++

.....+++

writing new private key to 'server.key'

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

而后,输入机构身份证件中机构所在的国家或者行政区(C),限定两位字

母,如中国输入 CN,美国输入 US 等;

Country Name (2 letter code) [AU]:CN

而后,输入省份(ST),即机构身份证件中机构所在省级地区;

State or Province Name (full name) [Some-State]:Beijing

而后,输入城市(L),即机构身份证件中机构所在市级地区;

Locality Name (eg, city) []:Beijing

而后,输入组织(O),即机构身份证件中机构名称全称;

Organization Name (eg, company) [Internet Widgits Pty Ltd]:China Financial
Certification Authority
而后,输入组织单位(OU),即证书申请表中申请人的部门名称;
Organizational Unit Name (eg, section) []:Technology Department
而后,输入名称(CN),即证书申请表中的域名;
Common Name (e.g. server FQDN or YOUR name) []:www.cfca.com.cn
而后,以下几项均可不填写;
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Please enter the following 'extra' attributes

而后,将在 OpenSSL 目录下,产生证书文件 key 和证书请求文件 csr。

3、证书申请机构将证书请求文件(server.csr)连同相关材料(详见 2.1 章节) 提供给赛尔网络,并妥善保管密钥文件(server.key)。

4、赛尔网络审核资料后,将公钥证书和证书链反馈给申请机构。

其中,证书文件一般以申请单位全称命名; EV SSL 证书的根证书是 CFCA_EV_CA.cer; 中级证书是 CFCA_EV_OCA.cer; OV SSL 证书的根证书是 CFCA_OV_CA.cer; 中级证书是 CFCA_OV_OCA.cer。

5、将服务器证书公钥另存为 server.crt。

完成上述操作后, server.key 为密钥文件、server.crt 为服务器证书文件, 和 证书链文件一起, 可以部署在 Apache、Nginx 等 Web 应用中。

3.4.4 使用 iKeyman 工具制作证书

IBM HTTP Server 含有,可以制作证书。

1、执行 IHS7 安装目录下, "bin"目录下的"ikeyman"命令,进入 iKeyman
 界面。

IBM 密钥管理	×			
密钥数据库文件(F) 创建(C) 查看(V) 帮助(H)				
密钥数据库信息				
数据库类型:				
文件名(F):				
令牌标签(T):				
密钥数据库内容				
个人证书	▼ 接收(!)			
	1110年(D)			
	查看/编辑(<u>W</u>)			
	导入(P)			
	重新创建请求(A)			
	重命名(M)			
	新建自签名(<u>G</u>)			
	抽取证书(])			
要启动,请选择"密钥数据库文件"禁单以使用密钥数据库				

2、选择"密钥数据库文件——新建",弹出以下对话框。

	新建	×
密钥数据库类型(<u>K</u>)	CMS 👻	
文件名(<u>F</u>):	key.kdb	浏览(<u>B</u>)
位置(L):	D:\]
	确定(<u>O)</u> 取消(<u>C</u>)	

3、在密钥数据库类型中选择"CMS"。点击"浏览"选择密钥数据库文件所 在路径,默认情况下应该在执行 ikeyman 的 bin 目录下。点击确定进入如下界面:

	密码提示		
XK)	密砖(P): ••••••		
181	确认密码(<u>N</u>): ••••••		
	 ☑ 到期时间(E) 60 ● 孫密時存储到文件中(S) 		
	确定(<u>O</u>) 重新设置(<u>R</u>) 取消(<u>C</u>)		

4、输入密钥数据库的密码,选择"将密码存储到文件中"点击"确定"进入如下界面,同时生成密码存储文件"key.sth"。该密码存储文件必须和密码数

据库文件放在同一目录下。

0		IBM 密钥管理 - [D:\key.kdb]		- 🗆 🗙
密钥数据库文件(E) (刘建(<u>C)</u> 查看(V) 帮助(H)			
	2 🚯 📃			
		密钥数据库信息		
数据库类型:	CMS			
文件名(F):	D:\key.kdb			
令牌标签(T):				
		密钥数据库内容		
个人证书请求			-	新建(<u>W</u>)
				删除(D)
				查看(l)
				抽取(<u>X</u>)
请求的操作已成功完成	<u>۶</u> !			

5、切换到"个人证书请求",选择界面上方的"创建——新建证书请求" 进入如下界面。其中:

密钥大小必须为 2048;

公用名(CN),即证书申请表中的域名;

组织(O),即机构身份证件中机构名称全称;

组织单元(OU),即证书申请表中申请人的部门名称;

市、县、区(L),即机构身份证件中机构所在市级地区;

省、直辖市(ST),即机构身份证件中机构所在省级地区;

国家或地区(C),输入机构身份证件中机构所在的国家或者行政区,限定 两位字母,如中国输入 CN,美国输入 US 等。

6、点击确定后,即在该路径下生成证书请求文件 certreq.arm。证书申请机 构将证书请求文件提供给 CFCA,并妥善保管证书文件(key.kdb)和证书密码文 件(key.sth)。

7、赛尔网络审核资料后,将公钥证书和证书链反馈给申请机构。

8、证书申请机构将收到的公钥证书和证书链装回到证书文件(key.kdb)中。 其中,证书文件一般以申请单位全称命名; EV SSL 证书的根证书是 CFCA_EV_CA.cer; 中级证书是 CFCA_EV_OCA.cer; OV SSL 证书的根证书是 CFCA_OV_CA.cer; 中级证书是 CFCA_OV_OCA.cer。

9、选择"签署者证书",进入如下界面。

密钥数据库文件(F) 创3	∉(C) 查看(V) 帮助(H)			
🗅 🚄 层 🔮	· 😰 🔤			
	密钥数据库信息			
数据库类型: (CMS			
文件名(F): [D:lkey.kdb			
令牌标签(T):				
	密钥数据库内容			
签署者证书		添加(<u>A</u>)		
		删除(D)		
		查看/编辑(<u>W</u>)		
		抽取(<u>X</u>)		
		填充(P)		
		重命名(Ⅲ)		
请求的操作已成功完成!				

10、选择"添加",弹出选择证书对话框,选择根证书,点击确定,导入完成。同样,将中级证书也导入到 key.kdb 中。

11、在密钥数据库中选择"个人证书",进入下面的界面。

Control (1) Control (1) Control (1) Control (1) <th>IBM 密钥管理 - [D:\key.kdb]</th> <th>_ 🗆 🗙</th>	IBM 密钥管理 - [D:\key.kdb]	_ 🗆 🗙
States as States as <t< td=""><td>密钥数据库文件(E) 创建(C) 查看(V) 帮助(E)</td><td></td></t<>	密钥数据库文件(E) 创建(C) 查看(V) 帮助(E)	
●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●		
SAMF 2029: 048 100 100 100 100 100 100 100 100 100 10		
	数据库类型: CMS	
中国会社 EVHICULE FOR CO # 2000 ● 2000 # 2000 ● 2000 ● 2000 ● 20000 ● 20000 ● 20000 ● 20000 ● 20000 ● 200000 ● 200000 ● 2000000 ● 2000000000000000000000000000000000000	文件名(F): D:\key.kdb	
	令牌标签(T):	
#X## ■ ##00 ###00 ###00 ###00 ####00 ####00 ######00 ######00 ######00 ######00 ######00 ######00 ######00 ######00 #######00 ######00 #######00 ######00 #######00 #######00 #######00 ####### ####################################	密钥数据库内容	
● ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	个人证书	▼ 接收(!)
		冊降(D)
		查看/编辑(<u>W</u>)
		导入(P)
▲ ##0018#PEL#R05/26.#! ▲ ##018#PEL#R05/26.#! ● #102 ● #		重新创建传动(Δ)
###1264/06 ###1264/06		<u>車</u> 箭名(<u>M</u>)
▲新的時時已成功完成! ▲新的時時已成功完成! 14、点击"接收",弹出如下对话框。 打开 文件名(F): 中国金融认证中心全球服务器证书。cel 御定(D) 取消(C) 15、选择服务器证书公钥文件,点击"确定",导入完成。 医医医尿病无关性PD 00月%CD 家商心 60月0日 > > ************************************		
▲本語的器件已成功完成! 14、点击"接收",弹出如下对话框。 打开 文件名(): 中国金融认证中心全球服务器证书.cer 位置(): DA 小原定() 取消() 15、选择服务器证书公钥文件,点击"确定",导入完成。 ***#88/##*.2**** ***#88/##*.2**** ***#88/##*.2**** ***#88/##*.2**** ***#88/##*.2**** ***#88/##*.2**** ***#88/##*.2**** ***#88/##* ***#88/#******* ***#88/##******************************		
######□ #####0 #####0 #####0 #####0 #####0 #####0 #####0 #####0 #####0 #####0 #####0 #####0 #####0 ######0 ####################################		新建自签名(G)
###BB/##E##0#2# 14、点击"接收",弹出如下对话框。 打开 文件名(E): 中国金融认证中心全球服务器证书.cef ////////////////////////////////////		抽取证书(1)
14、点击"接收",弹出如下对话框。 打开 × 文件名(D): 中国金融认证中心全球服务器证书.cel 浏览(D) 位置(L): D1 國定(O) 取消(C) 15、选择服务器证书公钥文件,点击"确定",导入完成。 201 215、选择服务器证书公钥文件,点击"确定",导入完成。	诸求的操作已成功完成!	
14、点击"接收",弹曲如下对话框。 打开 × 文件名(f): 中国金融认证中心全球服务器证书.ced 浏览(9) 储置(0) 取消(C) 15、选择服务器证书公钥文件,点击"确定",导入完成。 15、选择服务器证书公钥文件,点击"确定",导入完成。 15、选择服务器证书公钥文件,点击"确定",导入完成。 15、选择服务器证书公钥文件,点击"确定",导入完成。 15、选择服务器证书公钥文件,点击"确定",导入完成。 16M 登街登畫 (0		
打开 × 文件名(F): 中国金融认证中心全球服务器证书.ced 浏览(B) 位置(L): D: 「動定(D) 取消(C) 15、选择服务器证书公钥文件,点击"确定",导入完成。 第 100 至3000 至4000 至44000 至4400 至44000 至4400 至4400 至4400 至440	14、点击"接收",弹出如下对话框。	
文件名(日: 中国金融认证中心全球服务器证书.cel 浏览(日) 位置(L): D1 順定(0) 取消(C) 15、选择服务器证书公钥文件,点击"确定",导入完成。 2010 2010 2010 2010 2010 2010 2010 2010 <th< td=""><td>打开</td><td>×</td></th<>	打开	×
位置():	文件名(E) : 中国金融认证中心全球服务器证书.cer	浏览(B)
唐定① 取消① □ □ □ □ □ □ □	位罢(1):	
确定() 取消() 15、选择服务器证书公钥文件,点击"确定",导入完成。 ● ●		
15、选择服务器证书公钥文件,点击"确定",导入完成。	确定(<u>O</u>) 取消(<u>C</u>)	
BM 密钥管理 - [D:\key.kdb] C	15、选择服务器证书公钥文件,点击"确定",导	入完成。
密钥数据库文件(E) 台操(C) 查看(M) 帮助(E) □ ご 記 梁 梁 正 数据库类型: CMS 文件名(F): D:key.kdb 全線标签(T):	IBM 密钥管理 - [D:\key.kdb]	_ 🗆 🗙
○ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	密钥数据库文件(E) 创建(C) 查看(V) 帮助(E)	
密钥数据库信息 数据库类型: CMS 文件名(F): D:key,kdb 全牌标签(T): 密钥数据库内容		
文件名(F): D:key.kdb 全牌标签(T): 密钥数据库内容 个人证书 文 * Server 第erver * Server 第時位() * Server 算出(与入(2)) 重新始建请求(A) 重新台建请求(A) 重新台建请求(A) 重新台建请求(A) ● 新建目签名(G) ● 新建目签名(G)	密钥数据库信息 数据库类型: CMS	
★P#标金(I): 密钥数据库内容 接收() * Server ● ● ● ● ●	文件名(F): D:\key.kdb	
小人证书 「 接收() * Server ● 删除(D) * Server ● 置看/条器(W) * Server ● 当看/条器(W) ● 当日/条器(W) ■新命港連请求(A) 重新命港連请求(A) 重命名(M) 新建自签名(G) 新建自签名(G) 抽取证书(D) 新建自签名(G)	令禪你並(1): 灾知数据库侦察	
* server * server * server 章君،翁禄(W) 导出,导入(X) 董新创建请求(A) 董命名(M) 新建自签名(G) 抽取证书(D	个人证书	▼ 接收()
* Server	* server	删除(D)
导出/导入(X) 重新创建请求(<u>A</u>) 重命名(<u>M</u>)	" server	查看/编辑(<u>W)</u>
重新创建请求(A) 重命名(M) 新建自签名(G) 抽取证书(I)		导出/导入(X)
重命名(M) 新建自签名(G) 抽取证书(D		重新创建请求(A)
新建自签名(G) 抽取证书([]		重命名(<u>M</u>)
新建自签名(G) 抽取证书(D		
<u></u> 抽取证书(<u>]</u> …		新建自签名(G)
		抽取证书(I)
请求的操作已成功完成!	请求的操作已成功完成!	

3.5 证书格式转换

Tomcat、Weblogic、JBoss 等,使用 Java Keystore(JKS)格式的证书文件; Apache、Nginx 等,使用 KEY、CRT 格式的证书文件; IBM Websphere、IBM Http Server 等,使用 KDB 格式的证书文件; IIS 等,使用 PFX (P12)格式的证书文件;

JKS、KEY&CRT、KDB、PFX 等格式的证书文件可以相互转换。如下图所示:



3.5.1 工具转换(优先推荐)

CFCA 提供在线及离线工具两种便捷的证书格式转换工具,可满足大部分需求场景,优先推荐在线方式,如无法转换,可参考下述离线工具转换方式。

在线转换:

https://ssl.cfca.com.cn/Web/tool



3.5.2 JKS 转换为 PFX

可以使用 Keytool 工具,将 JKS 格式转换为 PFX 格式。

keytool -importkeystore -srckeystore D:\server.jks -destkeystore D:\server.pfx -

srcstoretype JKS -deststoretype PKCS12

3.5.3 PFX 转换为 JKS

可以使用 Keytool 工具,将 PFX 格式转换为 JKS 格式。

keytool -importkeystore -srckeystore D:\server.pfx -destkeystore D:\server.jks srcstoretype PKCS12 -deststoretype JKS

3.5.4 KEY&CRT 转换为 PFX

使用 OpenSSL 工具,可以将密钥文件 KEY 和公钥文件 CRT 转化为 PFX 文件。 将密钥文件 KEY 和公钥文件 CRT 放到 OpenSSL 目录下,打开 OpenSSL 执行 以下命令:

openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt

3.5.5 PFX 转换为 KEY&CRT

使用 OpenSSL 工具,可以将 PFX 文件转化为密钥文件 KEY 和公钥文件 CRT。

将 PFX 文件放到 OpenSSL 目录下,打开 OpenSSL 执行以下命令:

openssl pkcs12 -in server.pfx -nodes -out server.pem

openssl rsa -in server.pem -out server.key

openssl x509 -in server.pem -out server.crt

3.5.6 KDB 转换为 PFX

使用 iKeyman 工具,可以将 KDB 文件转化为 PFX 文件。 打开 KDB 文件,点击"导出"按钮。

- ロ - - - - - - - - - - - - -	×
密钥数据库文件(E) 创建(C) 查看(V) 帮助(E)	
密钥数据库信息	
数据库实型: CMS 文件名(F): C:\Users\CFCA\Deskton\kev kdb	
令律标签(T):	
密钥数据库内容	
个人证书	
* server 删除(D)	
查看/编辑(<u>W)</u>	
导出/导入(X)	
重新创建请求(A)	
重命名(M)	
新建自签名(近)	
抽取证书([)	
诸求的操作已成功完成!	
选择"导出密钥",选择 PKCS12 格式。	
选择"导出密钥",选择 PKCS12 格式。	x
选择"导出密钥",选择 PKCS12 格式。 打开 送择操作类型	×
选择"导出密钥",选择 PKCS12 格式。	×
选择"导出密钥",选择 PKCS12 格式。 打开 送择操作类型 ● 导出密钥(E) ○ 导入密钥()	×
选择"导出密钥",选择 PKCS12 格式。	×
选择 "导出密钥",选择 PKCS12 格式。 打开	×
选择 "导出密钥",选择 PKCS12 格式。 打开	×
选择 "导出密钥",选择 PKCS12 格式。 打开	×
选择 "导出密钥",选择 PKCS12 格式。 打开 送择操作类型 ● 导出密钥(E) ● 导入密钥()) 密钥文件类型(K) PKCS12 ▼ 文件名(E): key.pfx	×
选择 "导出密钥",选择 PKCS12 格式。 打开	×
选择 "导出密钥",选择 PKCS12 格式。 打开	×
选择 "导出密钥",选择 PKCS12 格式。 打开	×

即可导出 PFX 文件。

3.5.7 PFX 转换为 KDB

使用 iKeyman 工具,可以将 PFX 文件转化为 KDB 文件。

重新设置(<u>R</u>)

取消(<u>C</u>)

打开 iKeyman,新建一个 KDB 文件。

确定(<u>0</u>)

<u>0</u>		IBM 密钥管理	_ 🗆 ×
密钥数据库文件(F) 创建((〕 查看(⊻) 帮助(H)		
🗅 💕 🖬 🎽	R		
数据库类型:		密钥数据库信息	
文件名(F):			
令牌标签(T):			
		密钥数据库内容	
个人证书		新建	接收(!)
	密钥数据库类型(<u>K</u>)	CMS	删除(D)
	文件名(E):	key.kdb 浏览(B)	查看/编辑(<u>W</u>)
	位置(L):	C:\Users\CFCA\Desktop	导入(巴)
		确定(<u>0</u>) 取消(<u>C</u>)	重新创建请求(A)
			重命名(M)
			新建自签名(<u>G</u>)
			抽取证书(1)
要启动,请选择"密钥数据」	车文件"某单以使用密钥数	次据库	
输入密码,	可将密码有	存储到文件中。	

	密码提示	×
密码(P): 确认密码(<u>N</u>):	•••••	
 □ 到期时间(E ☑ 將密码存储) 60 到文件中(S)	犬(<u>D</u>)
确定(<u>O</u>)	重新设置(<u>R</u>)	取消(<u>C</u>)

选择签署者证书,点击"添加"按钮。

	- 🗆 🗙		
密钥数据库文件(E) 创建(C) 查看(V) 帮助(H)			
密钥数据库信息			
white Free City Service City Service Kdb 文件名印: City Service City Service Kdb			
令牌标签(T):			
密钥数据库内容			
签署者证书	添加(<u>A</u>)		
个人证书 签署者证书	删除(<u>D</u>)		
个人证书请求	查看/编辑(W)		
	抽TFV(X)		
	11-14(2)		
	· 現光(P)		
	重命名(<u>M</u>)		
请求的操作已成功完成!			
依次将根证书和中级证书导入。 选择个人证书,点击"导入"按钮。			
远挥个人证书, 点击 一寻入 按钮。			
匹揮千八և市, 点击 寺八 按钮。 BM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb]	- 🗆 ×		
近律小八և市, 只面 守八 按钮。 IBM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 密钥数据库文件① 创建() 查看() 帮助()	- □ <mark>×</mark>		
匹拌 八 և 中, 只 古 守八 按 山。 IBM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 密钥数据库文件(0) 创建(0) 查看\) 帮助(0)	- • X		
 び、押个、八 ш 市, 只 击 守八 (女 扣。 	- - ×		
	- C X		
近1年小人证书, 点击 守人 1女祖。 ■ IBM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 密钥数据库文件(f) 创速(c) 查看(v) 帮助(t) □ ご ご ご ご (x)			
	- C X		
近1年1・八山田市, 県市 守八 1女祖。 ■ IBM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 密钥数据库文件(f) 创速(c) 查看(v) 帮助(l) □ □ □ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	_ □ ×		
近 1年 小 八 և 亡 寸 , 点 古 守 八 1女 扣。 IBM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 密钥数据库文件④ 创速(2) 查看(M) 帮助(H) ② ② ③ ③ ③ ③ ③ ③ ③ ③ ③ ③ ④ ④ ④ ④ ④ ④ ④ ④	- □ × <u> 接收()</u> 删除(D)		
	- □ × <u> 接收()</u>)))))))))))))		
近1年1°人证十7,	- □ × <u> 接收()</u>		
近1年1・八山二寸, 只古 守八 1女祖。 [BM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 密钥数据库文件(f) 创速(c) 查看(y) 帮助(f) ご ご ご ご ご	- □ × <u> 接收()</u>		
 近非小人证书, 点面 守人 /女祖。 IBM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 密钥数据库文件(f) 创速(c) 查看(W 帮助(H) ② ③ ④ ② ③ ③ ③ 密钥数据库信息 数据库类型: CMS 文件名(f): C:\Users\CFCA\Desktop\key.kdb 令牌标签(f): C:\Users\CFCA\Desktop\key.kdb 零钥数据库内容 个人证书 密钥数据库内容 个人证书 资替证书 个人证书 	- C × 接收()		
近 排 1 八 证 十 3 , 从 古 守八 (女 扣。 IBM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 密钥数据库文件 0 创建 (2 查看 () 帮助(1) ご ご ご ご ご ご ご ご ご ご 密钥数据库信息 数据库类型: CMS 文件名(F): C:\Users\CFCA\Desktop\key.kdb 全障标签(T):	- □ × 接收() 勝除(D) 重看/熟辑(W) 耳新創建请求(A) 重命名(M)		
近非小、人证十, 从 古 守八 按 1 。	- □ × <u> 接收()</u>		
近すギー人证书, 只古 守八 1女祖。 IBM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 密钥数据库信息 密钥数据库信息 数据库装型: CMS 文件名(F): C:Users\CFCA\Desktop\key.kdb 全操标签(T): 密钥数据库内容 个人证书 密钥数据库内容 个人证书 密閉数据库内容 个人证书	× <u> 務收()</u> 一 一		
近年11人址于1,点面 守八 妆钮。 BM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 宮锡数据库文件(E) 创建(C) 查看(V) 帮助(E) ご ご ご ご ご ご ご ご ご ご ご 窓钥数据库信息 数据库类型: CMS 文件名(f): C:\Users\CFCA\Desktop\key.kdb 全禅标签(T): 名钥数据库内容 个人证书 答習者证书 个人证书	- □ × 接收() 一 一 一 上 一 一 × 一 二 、 、 、 、 、 、 、 、 、 、 、 、 、		
近律小人证书,点击 守八 按钮。 BM 密钥管理 - [C:\Users\CFCA\Desktop\key.kdb] 容银数据库文件① 创建① 查看② 帮助① ○ ご ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	- □ × <u>移取()</u> <u> 一</u> <u> 一</u> <u> 一</u> <u> 一</u> × <u> 一</u> <u> 一</u> × <u> 一</u> <u> </u> <u> </u>		

选择 PKCS12 类型,选择 PFX 文件。

	打开	×
密钥文件类型(<u>K</u>)	PKCS12	
文件名(E):	server.pfx	浏览(B)
位置(L):	C:\Users\CFCA\Desktop]
	确定(<u>O</u>) 取消(<u>C</u>)	

输入 PFX 密码。

	密码提示	×	A
密砖(P): ●●●●	••••		es 1/2
确定(<u>0</u>)	重新设置(R)	取消(<u>C</u>)	A C
名称。			2

输入标签名称。

更改标签	×
在完成导入过程之前更改这些标签吗? 要更改的标签(<u>S</u>): er	确定(<u>0</u>) 取消(<u>C</u>)
-	
新标签(E):	
er 应用(<u>A</u>)]
	更改标签 在完成导入过程之前更改这些标签吗? 要更改的标签(S): er 新标签(E): er

<u>6</u>		IBM 密钥管理	- [C:\Users\CFCA\D	esktop\key.kdb]		- 🗆 ×
密钥数据库文件(E) 创]建(<u>C)</u> 查看(⊻)	帮助(H)				
🗅 🚄 🖥 💈	2 🚯 🔙					
			密钥数据库信息			,[
教据库类型:	CMS					
文件名(F):	C:\Users\CFCA\	esktop\key.kdb				
令牌标签(T):						
			密钥数据库内容			
个人证书					-	接收(!)
server						删除(D)
						查看/编辑(<u>W</u>)
						导出/导入(X)
						重新创建请求(A)
						重命名(<u>M</u>)
						新建自签名(<u>G</u>)
						抽取证书(<u>1</u>)
请求的操作已成功完成	; !					

证书信息中,勾选"将此证书设置为缺省证书"。

X

and a set of the set
server
密钥大小(E): 2048 证书属性: 版本(V): X509 V3 序列号: 10 00 00 00 00 00 00 00 00 00 00 79 63 99 顺发给:
CN=*.cfca.com.cn, OU=Web Servers, OU=CFCA TEST OCA21, O=CFCA OCA2, C=CN
顺发者: O=CFCA RSA TEST OCA21, C=CN
有效性: 有效期从 2013年4月7日 至 2014年4月7日 指纹(SHA1 摘要): 7B:DF:C1:E9:67:D0:12:26:A6:4F:E1:38:5C:BC:1B:CC:90:AB:9E:B6 签名算法(S): SHA1withRSA (1.2.840.113549.1.1.5)
查看详细信息(V)
✓ 将该证书设置为缺省证书(S) 确定(0)

而后保存 KDB 文件即可。

3.5.8 KYR 格式证书制作

KYR 格式证书制作, 依赖 IBM Domino Server 软件, 使用 KyrTool 命令行工具进行操作。另需要 IBM Domino Server 升级到 9.0.1FP3 及以上, 方能支持 sha256 算法证书。

由于 IBM Domino Server 为付费软件,故 KYR 格式证书需在用户环境中完成转换,本文档提供转换方法:

准备工作:

1、 已将服务器升级到 9.0.1 以上版本并成功安装 Kyrtool 的命令行工具

kyrtool.zip (将 kyrtool 工具放入 C:\Program Files\IBM\Domino 目录)

操作步骤:

1、进入 Domino 目录

cd C:\Program Files\IBM\Domino

2、 检查 KyrTool 工具是否已就绪

kyrtool -h

KyrTool 就绪示例



3、创建 kyr 文件,并设置密码

kyrtool create -k "D:\server.kyr" -p password

4、将私钥文件,证书,中级证书,根证书,按照自上至下的顺序,合并为

server.txt 文件,完成后可通过以下命令检查是否正确

kyrtool =notes.ini verify D:\server.txt

检查结果

C:\Program Files\IBM\Domino>kyrtool =notes.ini verify D:\server.txt

KyrTool v1.0

- Successfully read 2048 bit RSA private key INFO: Successfully read 3 certificates INFO: Private key matches leaf certificate INFO: IssuerName of cert 0 matches the SubjectName of cert 1 INFO: IssuerName of cert 1 matches the SubjectName of cert 2 INFO: Final certificate in chain is self-signed

5、生成最终证书文件

kyrtool =notes.ini import all -k D:\server.kyr -i D:\server.txt

3.6 证书部署方法

证书部署方式,请优先咨询提供 Web 应用软件的软件或者硬件厂商,本章 节提供了部分 Web 应用软件部署证书的方式,仅供参考。

3.6.1 Apache 证书配置

Apache 使用 KEY 和 CRT 格式的证书,证书制作方式请参考"3.4.3 使用 OpenSSL 工具制作证书"。

将中级证书和根证书打开,依次将其代码复制到文本文件中(包括"-----BEGIN CERTIFICATE-----"和 "-----END CERTIFICATE-----"),并保存成 cfca.crt。如下:

-----BEGIN CERTIFICATE-----中级证书编码 -----BEGIN CERTIFICATE-----根证书编码 -----END CERTIFICATE-----

将服务器证书文件 server.key 和 server.crt,以及证书链文件 cfca.crt,配置在 Apache 中。

用文本编辑器打开 Apache 根目录下的 conf/httpd.conf 文件,去掉下述两行的注释符号#。

#LoadModule ssl_module modules/mod_ssl.so

#Include conf/extra/httpd-ssl.conf

用文本编辑器打开 Apache 根目录下的 conf/extra/httpd-ssl.conf 文件,修改以下内容:

<VirtualHost 127.0.0.1:443>

DocumentRoot "/var/www/html"

ServerName

SSLEngine on

SSLProtocol all -SSLv2 -SSLv3

SSLCertificateFile server.crt 路径

SSLCertificateKeyFile server.key 路径

SSLCertificateChainFile cfca.crt 路径

</VirtualHost>

其中:

禁用 SSLv2、SSLv3 协议: SSLProtocol all -SSLv2 -SSLv3

公钥文件: SSLCertificateFile server.crt 路径

私钥文件: SSLCertificateKeyFile server.key 路径

证书链文件: SSLCertificateChainFile cfca.crt 路径

上述设置完成过后,重新启动 Apache。

可选: 设置 HTTP 请求自动跳转 HTTPS

修改 httpd.conf 文件

在 httpd.conf 文件中的<VirtualHost *:80> </VirtualHost>中间,添加以下重定向代码。

```
RewriteEngine on
RewriteCond %{SERVER_PORT} !^443$
RewriteRule ^(.*)$ https://%{SERVER NAME}$1 [L,R]
```

3.6.2 Tomcat 证书配置

Tomcat 使用 JKS 格式的证书,证书制作方式请参考"3.4.3 使用 Keytool 工具制作证书"。

将服务器证书文件(server.jks),配置在 Tomcat 中。

文本编辑器打开 Tomcat 安装目录下 conf 目录中的 server.xml 文件,更新以下内容。

Tomcat8.5 以下配置

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
```

maxThreads="150" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS"

keystoreFile="jks 路径"

keystorePass="jks 密码"

truststoreFile="jks 路径"

truststorePass="jks 密码" />

其中:

SSL访问端口: port="443"

禁用 SSLv2、SSLv3 协议: sslProtocol="TLS"

证书文件: keystoreFile="jks 路径"

证书密码: keystorePass="jks 密码"

信任证书链文件: truststoreFile="jks 路径"

信任证书链密码: truststorePass="jks 密码"

```
Tomcat8.5 及以上配置:
```

<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"

maxThreads="150" SSLEnabled="true" clientAuth="false">

<SSLHostConfig>

<Certificate

certificateKeystoreFile="jks 路径"

certificateKeyAlias="jks 证书别名"

certificateKeystorePassword="jks 密码"

type="RSA" />

</SSLHostConfig>

//其他站点复制多个 SSLHostConfig

</Connector>
其中:

SSL访问端口: port="443"

证书文件: certificateKeystoreFile ="jks 路径"

证书别名: certificateKeyAlias="jks 证书别名"

证书密码: certificateKeystorePassword ="jks 密码"

配置完成后,重新启动 Tomcat。

可选: 开启 HTTP 强制跳转 HTTPS。

配置 web.xml 文件,在文件</welcome-file-list>后添加以下内容

```
<legin-config>
<!-- Authorization setting for SSL -->
<auth-method>CLIENT-CERT</auth-method>
<realm-name>Client Cert Users-only Area</realm-name>
</login-config>
<security-constraint>
<!-- Authorization setting for SSL -->
<web-resource-collection >
<web-resource-name >SSL</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

3.6.3 Nginx 证书配置

Nginx 使用 KEY 和 CRT 格式的证书,证书制作方式请参考"3.4.3 使用 OpenSSL 工具制作证书"。

将服务器证书、中级证书和根证书打开,依次将其代码复制到文本文件中(包括"-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE-----"),并保存成 server.crt。如下:

-----BEGIN CERTIFICATE-----服务器证书编码 -----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----中级证书编码 -----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----根证书编码 -----END CERTIFICATE-----

将服务器证书文件 server.key 和 server.crt, 配置在 Nginx 中。

如果是单向 SSL,用文本编辑器打开 Nginx 根目录下 conf/nginx.conf 文件,

更新以下内容:

server {

listen 443;

server_name 127.0.0.1;

ssl on;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl_certificate server.crt;

ssl_certificate_key server.key;

}

其中:

启用 SSL 功能: ssl on

禁用 SSLv2、SSLv3 协议: ssl_protocols TLSv1 TLSv1.1 TLSv1.2

公钥文件: ssl_certificate server.crt 路径

私钥文件: ssl_certificate_key server.key 路径

上述设置完成过后,重新启动 Nginx。

如果是双向 SSL,用文本编辑器打开 Nginx 根目录下 conf/nginx.conf 文件, 更新以下内容: server {

listen 443;

server_name 127.0.0.1;

ssl on;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl_certificate server.crt;

ssl_certificate_key server.key;

ssl_client_certificate ca.crt;

ssl_verify_client on;

ssl_verify_depth 2;

}

其中:

启用 SSL 功能: ssl on

禁用 SSLv2、SSLv3 协议: ssl_protocols TLSv1 TLSv1.1 TLSv1.2

公钥文件: ssl_certificate server.crt 路径

私钥文件: ssl_certificate_key server.key 路径

证书链文件: ssl_client_certificate ca.crt 路径

启用双向 SSL: ssl_verify_client on

证书链深度: ssl_verify_depth 2 如果客户端使用 CFCA 证书,则该项必须为 2

上述设置完成过后,重新启动 Nginx。

可选: 设置 HTTP 请求自动跳转 HTTPS。

在需要跳转的 HTTP 站点下添加以下 rewrite 语句,实现 HTTP 访问自动跳转 到 HTTPS 页面。 server {

```
listen 80;
```

server_name localhost; #将 localhost 修改为您证书绑定的域名,例如:
www.example.com。

rewrite ^(.*)\$ https://\$host\$1 permanent; #将所有 http 请求通过 rewrite 重定向到 https。

location / {

index.html index.htm;

}

3.6.4 Weblogic 证书配置

Weblogic 使用 JKS 格式的证书,证书制作方式请参考 "3.4.2 使用 Keytool 工 具制作证书"。

打开 Weblogic 控制台,进入"服务器"。

		■ JMS 服务 ■ 古碑转	答器 安伊		● Jolt 连接池
		 47689, JMS 模拟 路径服; 桥接程) 数据源 持久性存储 XML 注册表 XML 实体高速緩 外部 JNDI 提供 工作上下文 jCOM 100 (2000) 	^{(1),} 史 务 序 发存 转程序		 診断 日志文件 诊断模块 诊断图像 请求性能 档案 上下文 SIMP 昭表和图形
已部署的资源 ▲ 部署		 邮件会话 File T3 			• 监视仪表盘 @
- Hh-B		• JTA			
选择部署的服务器。	0				
选择部署的服务器。	0				
选择部署的服务器。	0				
选择部署的服务器。 选择部署的服务器。	o 中的所有按钮。				
 → 世 选择部署的服务器。	o 中的所有按钮。			显示 1	·到 1个,共 1个 上一个 下一个
选择部署的服务器。 选择部署的服务器。	o 中的所有按钮。 集群	• JTA	状态	显示 1 健康状况	到 1个,共 1个 上一个 下一个 监听端口

在"一般信息"中, "启用 SSL 监听端口"。

Admin	Server	的设置	+=	2002-	•	ikeel	1 +	tabil (±n 99	肥材	- -	24-26	z				
	信息	4群	服祭	দেশ ক্রম	^四 钥库		6 33	다이 联合태	-11-16 日本	部署	- 又主 - 迁移	·±≁ 优化	+ 招裁	t I	健康状況监護	D	服务器自动 Web 服务
保存	1										100.00						
使用	此页可	以配置该	服务	器的-	一般功	り能	例如	默认阿	銘通	信.							
堂右	• IDI 4	d R.															
名称						Ad	ninSer	ver									此服务器实例的字母数字式名称。更多信息
计算	计算机: (None)										将要运行此服务器的 WebLogic Server 主机 (计算机)。 更多信息						
集群						(St	andalo	ine)									该服务器所属的集群, 或 WebLogic Server 实例组。更多信息
<u>6</u>	钙地加	t:															此服务器用于监听传入连接的 IP 地址或 DNS 名。 更多信息
	合用监察	听端口															指定是否可以通过默认的纯文本 (非 SSL)监听端口访问此服务器。更多信息
监听	端口:					7	001										此服务器用来监听常规 (非 SSL) 传入连接的默认 TCP 端口。 更多信息
	自用 5	5L 监听室															指示是否可以通过默认的 SSL 监听端口访问服务器。 更多信息
55L 1	御靖]:				7	143										此服务器监听 SSL 连接请求所使用的 TCP/IP 端口。 更多信息
	<u></u> 信用	客户机	正书	代理													指定 HttpClusterServlet 是否代理特殊标头中的客户机证书。 更多信息
Java	编译器					ja	vac										供此服务器上所有需要编译 Java 代码的应用程序使用的 Java 编译 器。 更多信息
	在密密信输	 " < 销 < 销 < 街 < 街 < 街 < 新 < 新 < 新 < 新 < 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 <th>¥F</th><th>日上前日戊</th><th>下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下</th><th>" Se</th><th>の 定 rv 入 保</th><th>面, 制相 se: 存。</th><th>示 示 i rv</th><th>配筐 识利 ks∣ er.</th><th>記 記</th><th>务^名制作 好径 的</th><th>器证 言任 和 部 路</th><th>こ ギョン 密 径</th><th>5(se ; 码; 和密研</th><th>n ろ ろ</th><th>ver.jks)。其中: ;</th>	¥F	日上前日戊	下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下下	" Se	の 定 rv 入 保	面, 制相 se: 存。	示 示 i rv	配筐 识利 ks∣ er.	記 記	务 ^名 制作 好径 的	器证 言任 和 部 路	こ ギョン 密 径	5 (se ; 码; 和密研	n ろ ろ	ver.jks)。其中: ;
Admin	Server	的设置															
配置	协议	日志は	录	调订	ť, ∦ ææ	监视	控	制	部署	服务	安全	注释	#77#	11	1年442月1163月		
一版	i i AB	9 स्वन /	以穷	-201	91/ 4 -	S	SL 1	吹古服	35	中19-14	1119	ин	迴載	198	Emetへの置視	8	עפבאסטיפא אווא איז איז איז איז איז איז איז איז איז אי
IK1T	。 Ng可以:	确保私有	密钥	和信任	£证书	500;	发机构	J (CA)	的安:	全存储和	管理。	在此页。	中, 您可	山道	E看和定义各科	种滋	吃钥库配置。这些设置有助于管理消息传输的安全。
密钥	车 :								3	定制标识	「和定制」	盲任 更	改				查找服务器的标识和信任密钥库时应该使用哪些配置规则?更多信息
— 标ì	片 ——	∄œ́∙							Г					1			标识孪钼库的路径和文件名。 更多信 自
+0'										c:\serv	er.jks						And the set of the set
定制	床识密	肖库类型	:						[jks							密钥库的类型。此项一般为 JKS。 更多信息
定制	尿识密	胡库密码	短语	•					[•••••	•••						定制标识密钥库的加密密码短语。如果为空或空值,打开密钥库时将不需要密码短语。更多信息
确认:	定制标	只密钥库	密码	短语	:					•••••	•••						
一信(£																

c:\server.jks

•••••

•••••

jks

定制信任密钥库:

保存

定制信任密钥库类型:

定制信任密钥库密码短语:

确认定制信任密钥库密码短语:

38

定制信任密钥库的路径和文件名。 更多信息...

密钥库的类型。此项一般为 JKS。 更多信息...

。 定制信任密钥库的密码短语。如果为空或空值, 打开密钥库时将不需要 密码短语。 更多信息... 在"SSL"页签,配置 SSL选项。其中:标识和信任设置,选择"密钥库"; 私有密钥输入密钥别名和密码; 输入完成后,保存。

dminServer	的设置												
记置 协议	日志	记录	调试	监视	招	制部署	服务	安全	注释				
一般信息	集群	服务	密钥库	551		联合服务	部署	迁移	忧化	超載	健康状况监视	服务器启动	Web 服务
保存													
在此页中, 燧	可以查	看和定	②此服务	5器实例	列的	各种安全套	接字层	(SSL) 设	置。这些	些设置有	助于管理消息传	输的安全。	
🛃 标识和信	任位置	:				密約	明库 更改	坆				指示 SSL [信任 (信任	应在何处查找服务器的标识 (证书和私有密钥) 以及服务器的 任证书颁发机构)。 更多信息
- 标识 ——													
包有密钥位:	ٿ :					来	自定制标	识密钥属	ŧ			定义私有客	密钥文件位置的密钥库属性。更多信息
私有密钥别	ጀ፡					se	erver					定义用于有 多信息	存储和检索服务器私有密钥的字符串别名的密钥库属性。 更
🛃 私有密頓	密码短	语:				•		•				密钥库属性	生, 定义用来检索服务器私有密钥的密码短语。 更多信息
街 确认私有	密钥密	码短语	5:			•	•••••	•					
证书位置:						来	自定制标	识密钥属	牟			用于定义信	言任证书位置的密钥库属性。更多信息
- 信任													
信任证书簿2	发机构:					来	自定制信	任密钥属	车			用于定义证	正书颁发机构位置的密钥库属性。 更多信息
- 🖹 高級 —													
保存													

配置完成后,激活 Weblogic 更改,重新启动 Weblogic 服务。

注: 全球服务器证书为 SHA256 算法的,所以 weblogic 版本必须为 10.3.3 或者 更高版本,且这些版本的 weblogic 必须勾选"使用 JSSE SSL"。参考如下两个图:

1. SHA as HASH ALgorithm : If while signing the Certificate, signature hash algorithm used by CA is SHA256 (to find Algorithm, click certificate and then Details) then this is supported only on WebLogic 10.3.3 or higher version (for prior version of WebLogic use SHA1). For WebLogic 10.3.3 or higher with SHA256, select option Use JSSE SSL in SSL tab

XP)		
「 (四 允许未加密的 Null ?	祭 码	测试是否启用了 AllowUnEr 息
入站证书验证:	仅内置 SSL 验证	表示入站 SSL 的客户机证书
出站证书验证:	仅内置 SSL 验证	表示出站 SSL 的服务器证书
区 個 使用 JSSE SSL		选择要在 Weblogic 中使用的 信息

3.6.5 IBM Http Server 证书配置

IBM Http Server 使用 KDB 格式的证书,证书制作方式请参考"3.4.4 使用 iKeyman 工具制作证书"。

将制作好的 kdb、rdb、sth 文件放在同一个目录下,而后在 httpd.conf 文件 中配置。

Loa	dModule ibm_ssl_module modules/mod_ibm_ssl.so
List	en 443
	<virtualhost 127.0.0.1:443=""></virtualhost>
	ServerName 127.0.0.1
	SSLEnable
	SSLClientAuth required
	Keyfile "key.kdb 路径"
	SSLStashfile "key.sth 路径"
	SSLDisable

其中,KeyFile 所指定的为证书数据库路径,SSLStashfile 为密码文件路径。 配置完成后,重启启动 IBM HTTP Server。

3.6.6 JBoss 证书配置

JBoss 使用 JKS 格式的证书,证书制作方式请参考"3.4.2 使用 Keytool 工具制作证书"。

将服务器证书文件(server.jks),配置在 JBoss 中。

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,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="jks 路径"

keystorePass="jks 密码"

truststoreFile="jks 路径"

truststorePass="jks 密码"

sslProtocol = "TLS"/>

其中:

SSL访问端口: port="443"

证书文件: keystoreFile="jks 路径"

证书密码: keystorePass="jks 密码"

信任证书链文件: truststoreFile="jks 路径"

信任证书链密码: truststorePass="jks 密码"

配置完成后,重新启动 JBoss。

3.6.7 IIS 证书配置

IIS 可以直接使用 PFX 格式的证书文件, PFX 证书制作方式请参考 "2.5 证书 格式转换"。

在运行框中输入 MMC,进入管理控制台。

	E	运行	×
救		Windows 将根据你所输入的名称,为你打开相应的程序、 文件夹、文档或 Internet 资源。	
	打开(O):	mmc	~
		确定 取消 浏览(B)	

添加删除管理单元。

	abold on All		16- 11 -1-100			控制百1-[控制百恨刀从]	
	又件(F) 瘰	E(A) 查看(V)	収藏夹(O)	窗口(W)	帮助(H)		- 8 ×
	新建(N				Ctrl+N		
	打开(0	•			Ctrl+O	操作	
	保存(5)	、			Ctrl+S	这里没有任何项目。 控制台根节点	-
	为任内)	_			更多操作	•
	添加/册	徐管理单元(M).		(Ctrl+M		
	选项(P)						
	1 devr	gmt.msc					
	2 C:\U	rs\CFCA\Desl	ktop\控制台1.	msc			
	3 gpe	t.msc					
	4 secp	.msc					
	退出(X						
,							
						- 1 ³	

添加证书。 × 添加或删除管理单元 你可以在计算机上为此控制台选择可用的管理单元并配置所选的一组管理单元。对于可扩展的管理单元,你可以配置要启用哪些扩展项。 可用的管理单元(S): 所选管理单元(E): 管理单元 供应商 ~ 🎬 控制台根节点 编辑扩展(X)... 🍃 打印管理 Microsoft Cor... 删除(<u>R</u>) 🔍 服务 Microsoft Cor... ▲ 高级安全 Windows 防... Microsoft Cor... 👸 共享文件夹 Microsoft Cor... 上移(U) 🎥 计算机管理 Microsoft Cor... ④任务计划程序 Microsoft Cor... 下移(D) Microsoft Cor... 🛁 设备管理器 添加(<u>A)</u> > 🛃 事件查看器 Microsoft Cor... 70 授权管理器 Microsoft Cor... 📔 文件夹 Microsoft Cor... 他能监视器 Microsoft Cor... Microsoft Cor... 🗊 证书 🧾 狙策略对象编辑器 Microsoft Cor... 🖲 组件服务 Microsoft Cor... 高级(<u>V</u>)... 描述: 证书管理单元允许你浏览自己的、一个服务的或一台计算机的证书存储内容。 确定 取消

选择计算机账户。

		业书管块	里甲兀		
该管理单元将始终为	下列帐户管理证书:				
○ 我的用户帐户(M))				
○服务帐户(≦)					
● 计算机帐户(C)					
			< 上一步(B)	下一步(<u>N</u>) >	取消
フト・倫定					
之后,傰定。				-	
之后,确定。		添加或删除	管理单元	~	
之后, 備定。 ^{阿以在计算机上为此控制台}	选择可用的管理单元并配置	添加或删除	管理单元 单元。对于可扩展的管理	单元 , 你可以配置	要启用哪些扩展项。
之后, 備定。 ^{(初以在计算机上为此控制台}	选择可用的管理单元并配置	添加或删除 新选的一组管理	管理单元 单元。对于可扩展的管理: 选管理单元(E):	单元,你可以配置	要启用哪些扩展项。
乙后, 備定。 ^{阿以在计算机上为此控制台} I用的管理单元(<u>5)</u> : 管理单元	选择可用的管理单元并配置 供应商 个	添加或删除 断选的一组管理 所	管理单元 单元。对于可扩展的管理 选管理单元(E):	单元,你可以配置	要启用哪些扩展项。 编辑扩展(X)
乙后, 備定。 阿以在计算机上为此控制台 用的管理单元(S): 管理单元 ∰ 打印管理 ◎ 1710	选择可用的管理单元并配置 供应商 ^ Microsoft Cor	添加或删除 所选的一组管理 所	管理单元 单元。对于可扩展的管理 选管理单元(E): 量控制台根节点 ② 证书(本地计算机)	单元,你可以配置	更启用哪些扩展项。 编辑扩展(∑) ₩%⇔(8)
乙后, 備定。 河以在计算机上为此控制台 I用的管理单元(5): 管理单元 通打印管理 ③服务 ▲ 高级安全 Windows 防	选择可用的营理单元并配置 供应商 ^ Microsoft Cor Microsoft Cor	添加或删除 研选的一组管理 所	管理单元 单元、对于可扩展的管理 送管理单元(E): 全规治很节点 梁证书(本地计算机)		夏启用哪些扩展项。 編掲扩展(X) 删除(R)
乙后, 備定。 (前定。 (前定。 (前定。) (前定。) (前前に当れたりは控制台 (前前に当れたり) (前前に目的に当れたり) (前前に当れたり) (前前に目的に当れたり) (前前に目的に当れたり) (前前に目的に当れたり) (前前に目的に目的に目的に目的に目的に目的に目的に目的に目的に目的に目的に目的に目的に	选择可用的管理单元并配置 供应商 Microsoft Cor Microsoft Cor Microsoft Cor	添加或删除 研选的一组管理 所	管理单元 单元。对于可扩展的管理。 选管理单元(E): 全制台根节点 记记(本地计算机)		●启用哪些扩展项。 編纂扩展(爻)… 删除(图) 上移(U)
乙后, 備定。 尔可以在计算机上为此控制台 7用的管理单元(5): 管理单元 ● 新打印管理 ● 最级安全 Windows 防 ◎ 武學文件央 ● 计算机管理 ● 在冬汁切椒度	选择可用的管理单元并配置 供应商 Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	添加或删除 研选的一组管理 所	管理单元 单元。对于可扩展的管理 选管理单元(5): 量控制台根节点 口证书(本地计算机)		要启用哪些扩展项。 编辑扩展(2) 删除(B) 上移(U)
乙后, 備定。 河以在计算机上为此控制台 河以在计算机上为此控制台 可以在计算机上为此控制台 可以在计算机上为此控制台 曾世界中元 ◎ 打印管理 ◎ 共享文件夹 ◎ 计算机管理 ③ 任务计划程序 ④ 设备管理器	选择可用的管理单元并配置 Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	<mark>添加或删除</mark> 所选的—组管理 所 [【] 】	管理单元 单元。对于可扩展的管理 选管理单元(E): 量控制台根节点 ② 证书(本地计算机)		腰倉用哪些扩展项。 編編扩展(2) 創除(B) 上移(U) 下移(D)
乙 后 , 備 定 。 (前 定 。) (前 以 在 计算机上为此控制台) (前 以 在 计算机上为此控制台) (前 的管理单元(S): 管理单元 (前 打 印管理 (前 表 段 安全 Windows 防 (副 共享文件央 (計 算机管理 (④ 任务计划程序 (圖 事件查看器)	法揮可用的管理单元并配置 Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	<mark>添加或删除</mark> 研选的一组管理 所 添加(<u>A)</u> >	管理单元 单元。对于可扩展的管理 选管理单元(E): 量 控制台根节点 ② 证书(本地计算机)		要启用哪些扩展项。 編辑扩展(2)… 創除(R) 上珍(U) 下移(D)
乙后, 備定。	选择可用的营理单元并配置 供应商 ^ Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	<mark>添加或删除</mark> 研选的一组管理 所 。 添加(Δ) >	管理单元 单元。对于可扩展的管理 法管理单元(E): 社制台根节点 梁证书(本地计算机)		長启用哪些扩展项。 編編扩展(2)… 創除(B) 上移(U) 下移(D)
乙后, 備定。 (前)以在计算机上为此控制台 (1)用的管理单元(5): 管理单元 (2)服务 新口的管理 ③服务 新育取管理 ④ 育取安全 Windows 防 (2)共享文件夹 ③ 计算机管理 ④ 任务计划程序 ④ 设备管理器 ③ 資料管理器器 ③ 資料使管理器 ③ 文件夹 ③ 性影じ知器	选择可用的管理单元并配置 供应商 ^ Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	<mark>添加或删除</mark> 研选的一组管理 所 。 添加(Δ) >	管理单元 单元。对于可扩展的管理 法管理单元(E): ■ 控制台根节点 ☞ 证书(本地计算机)		要启用哪些扩展项。 编辑扩展(2)… 删除(R) 上移(U) 下移(D)
乙 / 后 , 備 定 。 「何以在计算机上为此控制台 」用的管理单元(5): 管理单元 ● 打印管理 ● 前印管理 ● 高級安全 Windows 防 ● 共享文件共 ● 计算机管理 ● 任务计划程序 ● 设备管理器 ■ 非律言者器 ■ 读得管理器 ■ 文件共 ● 生態监视器 ■ 证书	选择可用的管理单元并配置 供应商 ^ Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	<mark>添加或删除</mark> 研选的一组管理 所 。 添加(Δ) >	管理単元 単元、対于可扩展的管理 送管理単元(E): 記想名根节点 ② 近书(本地计算机)		要雇用哪些扩展项。 編編扩展(2) 一 一 上移(1) 下移(2)
之后, 備定。 (第可以在计算机上为此控制台 可用的管理单元(<u>S</u>): 管理单元 (新打的管理 一篇一次件夹 《 任务计划程序 《 设备管理器 》 任务计划程序 《 设备管理器 》 计算机管理 《 任务计划程序 《 设备管理器 》 计算机管理 》 任书 》 近的 " 工书 』 组策略对象编辑器	选择可用的管理单元并配置 供应商 ^ Microsoft Cor Microsoft Cor	<mark>添加或删除</mark> 研选的一组管理 所 。 添加(Δ) >	管理单元 单元、对于可扩展的管理 送管理单元(E): 全制台根节点 梁证书(本地计算机)		費启用哪些扩展项. 編編扩展(∞)… 删除(R) 上移(U) 下移(D)
之后, 備定。 称可以在计算机上为此控制台 可用的管理单元(5): 管理单元 通打印管理 服务 會 高级安全 Windows 防 武夫享机管理 任务计划程序 通 委件性理器 國 委权管理器 國 委权管理器 國 委任教管理器 國 委校管理器 國 委校的专士者	选择可用的管理单元并配置 Microsoft Cor Microsoft Cor	添加或删除 研选的一组管理 所 。 汤加(A) >	管理单元 单元。对于可扩展的管理: 选管理单元(E):		集局用哪些扩展项. 集集扩展(公) 新除(E) 上移(L) 下移(D) 高级()
乙 后, 備 定。 (你可以在计算机上为此控制名 可用的管理单元(5): 管理单元 論 股务 ☞ 高级安全 Windows 防 ③ 共享文件夹 圖 共享文件夹 圖 计算机管理 ④ 任务计划程序 圖 没备管理器 圖 要件查看器 圖 授权管理器 圖 文件夹 (⑤ 性能监视器 ■ 文件夹 (⑤ 性能监视器 ■ 近番 ③ 组集略对象编辑器 ● 通 组版务 ■ 通 細胞系	送揮可用的管理单元并配置 Microsoft Cor Microsoft Cor	添加或删除 研选的一组管理 添加(△) >	管理单元 单元。对于可扩展的管理 法管理单元(上): 全制台根节点 ② 证书(本地计算机)		●信用哪些扩展项. ● 编辑扩展() ● 编辑扩展() ● 第一次の目前の目前の目前の目前の目前の目前の目前の目前の目前の目前の目前の目前の目前の
乙 后, 備 定。 「「「」」」 「一」 「一	送揮可用的管理单元并配置 供应商 Microsoft Cor Microsoft Cor	添加或删除 研选的一组管理 所 添加(A) >	管理单元 单元,对于可扩展的管理 送管理单元(E): ■ 注制台根节点 ☞ 证书(本地计算机)		● 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一
之后, 備定。 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ 位 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	选择可用的管理单元并配置 Microsoft Cor Microsoft Cor	添加或删除 研造的一组管理 所 。 添加(Δ) > 算机的证书存储内	管理单元 单元、对于可扩展的管理: 送管理单元(2): ● 控制台根节点 ● 证书(本地计算机)		費扁用哪些扩展项. 编辑扩展(公) 通除(R) □ □ 上移(U) □ 下移(D) □ 高级(U)

在受信任的根证书颁发机构中,导入根证书。

· 🖀 控制台1 -	[控制台根节点	\让书(本地计算机)\受信任的相	↓让书颁发机构∖	证书]							
🚰 文件(F) 操作(A) 查看(V) 收藏夹(O) 窗口	(W) 帮助(H)					- 8 ×					
控制台根节点 _ 颁发给	*	颁发者	截止日期	预期 ^	操作						
▲ 💭 证书(本地计算机) 🔄 AddTrust Ex	ternal CA Root	AddTrust External CA Root	2020/5/30	服务	证书						
▶ 📫 个人 🔤 🖓 Baltimore C	yberTrust Root	Baltimore CyberTrust Root	2025/5/13	服务	更多操作	•					
▲ 🧉 受信任的根证书颁发		Certum CA	2027/6/11	服务							
			4749/4/11	<所≹							
	• 导入([])	CS CA	2041/5/12	<所≹							
		CFCA CS CA	2041/5/12	<所者							
	CA	CFCA CS SM2 CA	2042/8/24	<所≹							
	CA	CFCA CS TEST CA	2032/8/29	<所≹							
◎ 务信任人	CA	CFCA CS TEST CA	2032/8/29	<所≹							
	SM2 CA	CFCA CS TEST SM2 CA	2032/8/29	<所≹							
▶ ■ 其他人 导出列表(L)	T	CFCA EV ROOT	2029/12/31	<所≹							
▷ 🧾 MSIEHis 帮助(H)	ROOT	CFCA EV SM2 ROOT	2029/12/31	<所者							
▷ 🧰 远程桌面 🛛 🖓 LFCA GT CA		CFCA GT CA	2026/6/9	服务							
▷ 🚞 证书注册申请 🛛 🖾 CFCA GT CA		CFCA GT CA	2042/8/21	<所者							
▷ 🧮 智能卡受信任的根 🛛 🖾 CFCA GT SM	12 CA	CFCA GT SM2 CA	2042/8/21	<所祥							
▶ 🧮 受信任的设备 🚽 📮 CFCA Opera	tion CA3	CFCA Operation CA3	2021/11/6	<所者							
▷ 🧾 Web 宿主 🗸 🐺 CFCA RCA		CFCA RCA	2022/6/4	<所≹ ↓							
< >> <				>							
将证书添加到存储											

在中级证书颁发机构中,导入中级证书。

	控制台1 - [控制台根节	5点\证书(本地计算机)\中间证	书颁发机构\证书	1	-	□ ×
🚰 文件(F) 操作(A) 查看(V)	收藏夹(O) 窗口(W) 帮助(H)					- 8 ×
🗢 🄿 🖄 📅 🚺 🙆 📄	?					
控制台根节点	颁发给 ^	颁发者	截止日期	预期 ^	操作	
⊿ 🗊 证书(本地计算机)	BOC	CFCA	2031/5/11	<所祥	证书	
▶ 🖺 个人	BOC SM2	CFCA CS TEST SM2 CA	2032/7/23	<所者	更多操作	•
▲ 📔 受信任的根证书颁发	GCFCA CS OCA11	CFCA CS CA	2031/5/15	<所≇		
	GCFCA CS SM2 OCA11	CFCA CS SM2 CA	2031/5/15	<所≹		
▷ 🗋 企业信任	CFCA EV OCA	CFCA EV ROOT	2029/12/29	<所種		
▲ ■ 中间证书颁发机构	CFCA EV SM2 OCA	CFCA EV SM2 ROOT	2029/12/29	<所種		
● 业书市钥列表	🖙 CFCA GT OCA21	CFCA GT CA	2026/6/7	<所≇		
	(K) ト 長入の)	A GT CA	2026/6/7	<所種		
	UCA21	CFCA GT SM2 CA	2026/6/7	<所種		
	•	CFCA PCA	2022/6/4	<所種		
	建窗口(W)	CFCA CS CA	2031/5/16	<所種		
新任务板	视图(T)	CFCA CS CA	2031/5/16	<所種		
		CFCA GT CA	2026/6/9	<所種		
▶ MSIEHi		CFCA GT CA	2032/8/15	<所種		
▷ 📫 远程桌口	(L) on CA	CFCA Policy CA	2020/6/12	<所者		
▷ 🚞 证书注册 帮助(H)	on CA1	CFCA Root CA	2020/6/12	<所種		
> 📔 智能卡受信任的根 🗸	CFCA Operation CA2	CFCA Root CA	2019/11/21	<所≹ ↓		
< >	<			>		
将证书添加到存储						

在个人证书中,导入 PFX 证书文件。

a		控	制台1 - [控制台)	限节点\汕	书(本地计算机)\イ	个人\证书]			
🚟 文件(F) 操作(A) 🗄	查看(V) 收藏夹(O)	窗口(W)	帮助(H)						_ 8 ×
(= -) 🖄 📅 📋	Q 🔒 🛛 🖬								
□□ 控制台根节点	∧ 価労会	~	97	行生去		裁正日期	新聞日本	操作	
▲ 副 证书(本地计算机)			10	CAL H		HOLL HIND	120401414.	(二十)	
4 🛗 个人				这里没有低	壬何项目。			虹や	-
🧰 证书								更多媒作	•
▷ 📔 受信任的	所有任务(K)	•	申请新证书(R).		1				
▷ 🧰 企业信任	查看(V)	•	导入(I)						
> 📔 中间证书	从这里创建窗口(W)		高级操作(A)	•					
▷ 🧮 受信任的		- 'r			1				
	新任劳恢倪图(1)								
	刷新(F)								
	导出列表(L)								
▶□目/」则灵	帮助(H)								
MSIEHistory	Journa								
▷ 📔 远程桌面									
▷ 📔 证书注册申请									
▷ 🎬 智能卡受信任	的根								
▷ 🧮 受信任的设备									
▷ 🎬 Web 宿主	~								
<	> <						>		
将证书添加到存储									

导入时,选择个人信息交换(PFX、P12)。

E	打开			×
ⓒ ⋺ ▾ ↑ 🏪 ▸ 这台	ê电脑 → 本地磁盘(C:) →	✓ C	叟索"本地磁盘 (C:)"	Q
组织 ▼ 新建文件夹				
▲ 桌面	名称		修改日期	类型
🔀 CFCA	퉬 inetpub		2013/11/29 11:01	文件夹
📕 这台电脑	퉬 Program Files		2013/11/21 12:00	文件夹
🔒 视频	퉬 Program Files (x86)		2013/11/29 8:40	文件夹
■ 图片	퉬 Windows		2013/11/29 11:02	文件夹
	🌗 用户		2013/11/21 13:27	文件夹
▶ 下载	🦻 CFCA.pfx		2013/5/8 8:32	Personal In
▶ 桌面				
🏪 本地磁盘 (C:)				
🧰 本地磁盘 (D:)				
🥽 库 🗸 🗸	(>
文件名(N: CFCA.pfx	~	个人信息交换(*.pfx;*.p1 打开(<u>O</u>)	2) v 取消

导入完成。

	控制台1 - [控制	台根节点\证书(本地计算机)\个	人\证书]		-	□ ×
	收藏夹(Q) 窗口(W) 帮助(H)					_ 8 ×
🗢 🄿 🙍 🖬 🗟 🖬						
🧰 控制台根节点 🔷	颁发给	颁发者	截止日期	预期目的	操作	
⊿ 🗊 证书(本地计算机)	www.cfca.com.cn	CFCA OCA2	2016/5/7	客户端身	证书	•
4 🗎 个人					更多操作	•
2 证书						
▶ 📄 受信任的根证书颁发						
▶ _ 12业信性						
▷ 🚆 第三方根证书颁发机						
▶ 🛄 受信任人						
▶ 📑 客户端身份验证颁发						
▷ 🎬 其他人						
MSIEHistoryJourna						
▷ 🚰 远程桌面						
▷ 🧰 证书注册申请						
▷ 🧮 智能卡受信任的根						
▷ 🧮 受信任的设备						
▷ 🛗 Web 宿主 🗸 🗸						
< >	<			>		
个人 存储含有 2 个证书。						

在 IIS 管理控制台,选择站点,点击"绑定"。

8)	Internet Information Services (IIS)管理器	- 🗇 🗙
€ → ZHANGCHENG	i → 网站 → Default Web Site →	🖬 🛛 🟠 🔞 •
文件(F) 视图(V) 帮助(H)		
连接	🙆 Default Web Site 主页	操作
		浏览
▲ MangCHENG (ZHANGCH	(特选: ▼ 〒 开始(G) ▼ ↓ 全部显示(A) 分组依据: 区域 ▼ Ⅲ ▼	编辑仪限
4 🙆 网站		潮电内中 绑定
😜 Default Web Site		□ 基本设置
	HTTP 順应标 MIME 英型 SSL设置 处理程序映 错误页 模块 默认文档 目录浏览 请求筛选 日志头 射	查看应用程序 查看虚拟目录
		管理网站 📀
	A478	● 停止
		浏览网站
	100 (AL20)	◎ 浏览 *:80 (http)
	此且外销的	高级设宜
		限制
		😢 帮助
< >	III 功能规图 C 内容视图	
就绪	// A	€ <u>∎</u>
点击"羽	如",选择"https",选择SSL证书,点击确定。	

类型	主机名	端口	IP 地址	绑定信息	ļ.		添加(A)
http		80	*				编辑(E)
			添加國	网站绑定		?	× R)
	光型(四)	IP 地均	E(I):		端口(<u>O</u>):		В)
	https	v 192.1	68.2.86		v 443]	
	主机名(出):						
	server						
	🗌 需要服务器名称	指示(N)					
_	SSL 证书(E):						
	server			~	选择(<u>L</u>)	查看(<u>V</u>)	C)
	- L State and a						
	未选定						

重新启动 IIS 即可。

3.6.8 Websphere 证书配置

Websphere 使用 JKS 格式的证书,证书制作方式请参考"3.4.2 使用 Keytool 工具制作证书"。

将准备好的 JKS 文件放在适当的目录中,如 Websphere 主目录\AppServer\bin 中。

然后打开 WebSphere 管理控制台:

🗲 🕗 🗢 🙋 https://localhost:9043/ib	et Exploren	gin. do?action=secu	🔽 😵 证书错误 🛛 😽 🗙 ಶ Bing	1	
文件 (E) 编辑 (E) 查看 (V) 收藏夹 (A) 二	工具(II) 帮助	<u>መ</u>			
🍃 收藏夹 🛛 🍰 🔁 建议网站 👻 💋 免费 Ho	tmail 🙋 升台	级浏览器 ▼			
🏉 集成解决方案控制台		1	🏠 🔹 🗔 👻 🖃 📥 🔹 页面 🕑 🔹 安全 🔅	<u>s</u>) • 工具(0)	• 🕢 •
ntegrated Solutions Console 🛛 admin, 🗴	大迎您		帮助 注销		IBM.
视图: 所有任务	SL ILTOPHE	191 B 192			-
- 欢迎		□ 消息			
田指导性活动		▲ 已更改 直接	了您的本地配置。您可以:		
田服务器			主配置。		
国应用程序		 ▲ 査査 	#之前 改。		
田资源		可在 <u>首选</u>	④中启用在保存之后同步多个节点中的配置的选项。		
日安全性		23-3- H.Z	些更以主义;可能需要重制后构版分替。		
= 安全管理、应用程序和基础	CCI 27-8-8	त्र अद्यास	车 和):广北		
■ SSL 证书和密钥管理	<u> </u>		キイルビマ RACE(R) CMS lava(TM) 別的方信件産業刑		
36 6 b and 6 101.	XC.X. (1) (4) (4)				
= 总线安全性	田 首洗顶				
 思线安全性 Web Service 	田 首选项	11460 六倍效率	8 7		
 总线安全性 Web Service 图环境 	田 首选项 新建 日	删除 交换签署	馨者		
 - 忌残安全性 - Web Service - 国环境 - 国系統管理 	田 首选项 新建 日 □ □ 1	删除 交換签署	著者		
 - 总核安全性 - Web Service - 田环境 - 国环统管理 - 国户和组 	田 首选项 新建 册 尼 日 共 选择 名称	删除 文换签署 業 ¹ 2 ◆	著者 路径 ◇	远程管理 ≎	主机
 - 起线女全性 - Web Service - 新統管理 - 和戶和組 - 田戶和組 	田 首选项 新建 册 尼 C 4 选择 名称	删除 交换签署 世 孧 ≎ ÞefaultKeyStore	著者 路径 ☆ \${CONFIG_ROOT}/cells/WinServer2003Cell01/key.p12	远程管理 ≎ false	主机
 - 总线女全性 - Web Service B环境 国系统管理 B用户和组 B出视和调整 B故障诊断 	田 首选项 新建 。 后 节 法择 名称 「 <u>CellD</u> 「 <u>CellD</u>	删除 交换签表 ☆)efaultKeyStore)efaultTrustStore	器者 路径 ☆ \${CONFIG_ROOT}/cells/WinServer2003Cell01/key.p12 \${CONFIG_ROOT}/cells/WinServer2003Cell01/trust.p12	远程管理 💸 false false	主机
 - 息核安全性 - Web Service B环境 回系统管理 回用户和组 回监视和调整 回监视和调整 田放降诊断 国服务集成 	田 首选项 新建 月 远择 名称 C CellD	删除 交换签表 ᠅ "♀ シefaultKeyStore JefaultTrustStore TPAKeys	諸者 路径 \${CONFIG_ROOT}/cells/WinServer2003Cell01/key.p12 \${CONFIG_ROOT}/cells/WinServer2003Cell01/trust.p12 \${CONFIG_ROOT}/cells/WinServer2003Cell01/trust.p12	远程管理 ≎ false false	主机
 总线安全性 Web Service 田环境 田戶和組 田戶和組 出版和调整 田放障诊断 副服务集成 UDDI 	 田 首法项 新建 新建 ・ <li< td=""><td>删除 交换签署 같 好 ≎ 2efaultKeyStore 2efaultTrustStore TPAKeys</td><td>路径 ≎ \${CONFIG_ROOT}/cells/WinServer2003Cell01/key.p12 \${CONFIG_ROOT}/cells/WinServer2003Cell01/trust.p12 \${CONFIG_ROOT}/cells/WinServer2003Cell01/trpa.jceks</td><td>远程管理 ≎ false false false</td><td>主机</td></li<>	删除 交换签署 같 好 ≎ 2efaultKeyStore 2efaultTrustStore TPAKeys	路径 ≎ \${CONFIG_ROOT}/cells/WinServer2003Cell01/key.p12 \${CONFIG_ROOT}/cells/WinServer2003Cell01/trust.p12 \${CONFIG_ROOT}/cells/WinServer2003Cell01/trpa.jceks	远程管理 ≎ false false false	主机
 - 总线安全性 - Web Service 田环境 国系统管理 国用户和组 回监视和调整 回 盐牌诊断 田服务集成 UDDI 	 田 首法項 新建 新建 「 ご ご ご ご ご こ 	删除 交换签署 学 学 ≎ 2efaultKeyStore 2efaultTrustStore TPAKeys	諸征 路径 令 \${CONFIG_ROOT}/cells/WinServer2003Cell01/key.p12 \${CONFIG_ROOT}/cells/WinServer2003Cell01/trust.p12 \${CONFIG_ROOT}/cells/WinServer2003Cell01/ttpa.jceks	远程管理 ≎ false false false	主机

选择"SSL证书和密钥管理"->"密钥库和证书"->"新建",

	net Explorer		>
COO - E https://localhost:9043/i	bm/console/login.do?action=secur 🗾 😵 证书错误	🖄 🔶 🗶 🌠 Bing	P -
文件(E) 编辑(E) 查看(V) 收藏夹(A)	工具(T) 帮助(H)		
🖕 收藏夹 🛛 🏤 🔁 建议网站 🗸 🙋 免费 H	fotmail 👩 升级浏览器 -		
🏉 集成解决方案控制台		🏠 • 🔊 - 🖃 🖶 • 页面化) • 安	全⑤・工具①・②・
Integrated Solutions Console admin,	欢迎您	帮助 注销	IBM
视图: 所有任务	常规尾性	应用或保存了此项的常规属性后	
- 欢迎		其他属性才可用。	帮助
田指导性活动	WAS_SSL	<u>其他雇性</u>	字段帮助
田服务器	* 路径	 ・ ・ ・	要获取字段帮助信
■应用程序	bSphere\AppServer\bin\key.jks	■ 11入址书 ■ 个人证书请求	签或选择列表标让
田资源	密码	 定制属性 	页面帮助
日安全性	•••		关于此页面的更多
= 安全管理、应用程序和基础	确认密码		
= SSL 证书和密钥管理	•••		
■ 总线安全性	类型		
 Web Service 	JKS		
田环境	□ 远程管理		
田系统管理	主机列表		
田用户和组			
田监视和调整	□ 只读		
田 故障诊断	□ 在启动时初始化		
田服务集成	□ 左種供設条上自用加容操作		
I UDDI			
	应用 确定 复位 取消		
	A STATE PAIR		
			▶
DARWA		- store mer	14m - 1 - 100% +

输入 JKS 文件信息,并单击"应用"。



然后选择"SSL证书和密钥管理"->"SSL配置"->"新建",

⊘集成解决方案控制台 - Windows Inte	rnet Explorer			
	ibm/console/login.do?action=secur	💌 😵 证书错误 🛛 😣 😽 💈	🗙 ಶ Bing	₽ -
文件(E) 编辑(E) 查看(Y) 收藏夹(A)	工具(T) 帮助(H)			
🚖 收藏夹 🛛 🏤 🔽 建议网站 👻 🥭 免费	Hotmail 🙋 升级浏览器 -			
《 集成解决方案控制台		🙆 • 6	🛯 - 🖃 🖶 - 页面(2) - 安全(3)• 工具(0)• 🕢•
Integrated Solutions Console admin,	欢迎您	帮	助 注销	IDM.
视图 : 所有任务 = 欢迎 用指导性活动	SSL 证书和密钥管理 > SSL 定义安全容接字层(SSL)配置列	<mark>記置</mark> > 新建 康。		▲ 帮助 字段费
田服务器	配置			
■应用程序				12 宜木指 将此证书
田资源	常規属性		应用或保存了此项的常规属性后 其他属性才可用。	接子层(
日安全性	* 治称 WASSSL		其他属性	页面帮
 安全管理、应用程序和基础 SSL证书和密钥管理 总结安全性 	信任库名 WAS_SSL	•	 保护质量(QoP)设置 定制属性 	<u>关于此页</u>
Web Service	密钥库名 WAS_SSL	₹ 又 秋 取 证 书 別 名		
田	缺省服务器证书别名 <mark>Was</mark> ▼			
国用户和组	缺省客户机证书别名			
田监视和调整	was 💌			
田	管理作用域 (cell):WinServer2003Ce	201		
€UDDI	应用 确定 复位	取消		
完成			New York With Stranger	🖓 🕶 🔍 100% 👻 🎢

输入"名称",选择刚才创建的"信任库名"和"密钥库名"后,单击"获 取证书别名",然后单击"应用"。



再次进入"SSL证书和密钥管理"->"SSL配置",选择刚才创建的配置"WASSSL",

🌈 集成解决方案控制台 - Windows Inter	net Explorer	
COO - Attps://localhost:9043/	bm/console/login.do?action=secur 🗨 😵 证书错误 🛛 😣 😽 🗙 🌈 Bing	₽ -
文件(E) 编辑(E) 查看(V) 收藏夹(A)	工具 (I) 帮助 (H)	
🚖 收藏夹 🛛 🍰 🔁 建议网站 👻 💋 免费)	lotmail 💋 升级浏览器 -	
🏉 集成解决方案控制台	🏠 ▼ 🗟 ァ 🖻 🖶 ▼ 页面 🕑 ▼ 安全 ⑤)・ 工具 (0)・ (2)・
Integrated Solutions Console admin,	欢迎您	II EM.
 Web 服务器 集群 集群拓扑 一般服务器集群 WebSphere MQ Serv 田核心组 	 ▲ 已更改了您的本地配置。您可以: 直接 ● 保存到注配置。 保存或放弃之前 ● 查看更改。 可在查述项中启用在保存之后同步多个节点中的配置的选项。 ▲ 要使这些更改生效,可能需要重新启动服务器。 	帮助 字段帮 要获取寻 出现考出 经或选择
 □ 应用程序 □ 资源 □ 安全性 	<u>SSL 証书和密钥管理</u> > <u>SSL 配置</u> > WASSSL 定义安全客接字层(SSL) 配置列表。 配置	页面帮 <u>关于此页</u>
 安全管理、应用程序和: SSL证书和密钥管理 总线安全性 Web Service 	常規屋性 其他屋性 * 名称 = 保护质量(QoP)设置 WASSSL 量 信任年冬 = 定制属性	
田系统管理	WAS_SSL	
田用户和组 田监视和调整	密钥库名 WAS_SSL 获取证书别名	
 田 故障诊断 田 服务集成 	缺省服务器证书别名 Was ▼	
	(2) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	▼ ▼
	www.andreamet	🐴 • 🔍 100% • //

选择"保护质量(QoP)设置",

neeps.))rucan	host:9043/ibm/console/se	🔽 😵 证书错误 🛛 😽 🗙 ಶ	Bing	Q
文件(17) 编辑(17) 査看(17) に	皮藏 妻(a) ゴ 且(rr) 翻目			
			📑 📥 🗸 页面(P)	▼ 安全(S) ▼ 千具(0) ▼ 📦
Integrated Solutions Console	wasadmin, 次迎您	帯切「	注钥	
视图: 所有任务				
- 欢迎	SSL 证书和密钥	管理 > <u>SSL 配置</u> > <u>WASSSL</u> >	保护质量(QoP)i	受置
田指导性活动	指定安全性级别、	密码和相互认证设置。		
田服务器	配置			
田应用程序				
田资源	當規屋性			
日安全性	客户机认证			
 安全管理、应用程 	必需 -	1		
■ SSL 证书和密钥管	500 this	•		
■ 总线安全性	SSL_TL	5 🔻		
口环培				
回到現	提供程序 福田市の	, 为 1SSF 担世程定		指定一个包,这个包实现了
回 求奶 昌 柱 页 田 白 和 组	** 现定又:			程接口(API)的一小部分密 java.security 文件中列出的
由用厂相组	选择教	記法程序 10™J33E2 ▲		展(JSSE)提供程序名称。
田監倪和调整	い定制に	SSE 提供程序		伏」距洪推升。
田政陣诊断	定制技			
田脈勞集成		·\ቢም		
UDDI	■ 密閉写件	7.2.1		N
			★+地 T=+++=++	
在"客户机认证 _{集成解决方案控制} 合 - Tindows	"中选择"」	必需的",然后单	击"应用	"。
在"客户机认证 集成解决方案控制合 - Tindows) 》 》 https://localhost (件@) 编辑@ 查看创 收藏:	"中选择"」 Internet Explorer 9043/ibm/console/login.do? 来鱼 工具① 帮助创	必需的",然后单 action=sect▼ ♀ 证粉错误 ≥ 49 2	击"应用 [?] × ಶ Bing	"。
在"客户机认证 集成解决方案控制合 - Tindows) · P Attps://localhost 2件 @ 编辑 @ 查看 @ 收藏: * 收藏夹 @ D 建议网站 · @	"中选择"」 Internet Explorer 9043/ibs/consols/login.do? 来(A) 工具① 帮助做 免费 Hotmail @ 升级浏览	必需的",然后单 action≂sect <mark>、梁证粉</mark> 瓣梁 钟 2 ■→	击"应用 [?] × 🏹 Bing	"。
在 "客户机认证 集成解决方案登制合 - Tindows	"中选择"」 Internet Explorer (9043/ibm/console/login.do? 来(4) 工具(1) 帮助(1) 免费 Hotmail 2 升级浏览器	必需的",然后单 action=sect▼ ♀ 证书错误	击"应用 ³ × M ^{B Bing}	" 。 〕 2)、安全⑤、工具⓪、 ④
在 "客户机认证 集成ft决方案登制台 - Tindows 全 () () () () () () () () () () () () () () () () () () () () () () () () () ("中选择" Internet Explorer 9043/1bm/console/login.do? 来 (4) 工具 (7) 帮助 (8) 免费 Hotmail (2) 升级浏览。 min, 欢迎您	必需的",然后单 action=sect▼ ② 证书错误	击"应用 [*] × P ^{Bing} 	"。 (1) (2)、安全(5)、I具(0)、(1) I目 IIII
在 "客户机认证 集成解决方案控制台 - Tindows 全 《 Mths://localhost 2件 ② 编辑 ② 查看 ① 收藏 2 收藏来 读 ② 建议网站 - @ 《 集成解决方案控制台 ntegrated Solutions Console adu 初图: 所有任务	····································	必需的",然后单 action=sect▼ ≩ 证书错误 ≧ 4/2 a- a # #	击"应用 [;] × 译 ^{Bing} 	"。 ————————————————————————————————————
在 "客户机认证 集成解决方案控制合 - Tindows 全 《 https://localhost 2件 ② 编辑 ② 查看 ① 收藏 w藏来 编 ② 建议网站 · 《 集成解决方案控制台 ntegrated Solutions Console add 初图. 所有在务 。 欢迎	 "中选择 "」 Interact Explorer 8043/ibm/console/login.do? 来(A) 工具(T) 帮助(B) 免费 Hotmail 2 升级浏览 min, 次迎您 应用程序服务器 应用程序服务器 	心需的",然后单 ≝ction=secy▼ ❷ 证书错误	击"应用" × 译 ^{Bing} > - ⁻ - ⁻ - ⁻ - ⁻ - ⁻ - ⁻	"。 (1) (2)、安全(s)、工具(s)、(s) (1) (1) (1) (1) (1) (1) (1) (1
在 "客户机认证 集成解决方案控制合 - Tindows	 "中选择 "」 Interact Explorer 3043/1bm/console/login.487 来(山) 工具(1) 帮助(1) 免费 Hotmail 2) 升级浏览 min, 次迎窓 应用程序服务器 回用程序服务器 目消息 	心需的",然后单 action≅sect▼ ♀ 证错错误	击"应用 ³ × ▶ ➡ ♣ • 页面 助 注销	。 ■□□ ● ● ● ● ● ● ● ● ● ● ● ● ●
在 "客户机认证 集成解决方案控制合 - Tindows () 、 () https://localhost () 、 () 、 () () () () () () () () () () () () ()	 "中选择 "」 Interact Explorer 3043/1bm/console/login.487 来(山) 工具(1) 帮助(1) 免费 Hotmail 2) 升级浏览 如前, 次迎您 应用程序服务器 回用程序服务器 目消息 合理 	心需的",然后单 action=sact ▼ ♥ 证粉错误	击"应用 ³ × ▶ ➡ ♣ • 页面 助 注销	************************************
在 "客户机认证 集成解决方案控制合 - Tindors	 "中选择 "」 Internet Explorer (9045/ibb/console/login.do? 来(a) 工具(1) 帮助(1) 免费 Hotmail 2 升级浏览器 min, 次迎您 应用程序服务器 应用程序服务器 回用程序服务器 	必需的",然后单 action=sect ♥ 证书错误 @ ↔ 2 g - @ - 6 零 源政了您的本地配置。您可以: 程有1注配置。 家政算之前	击"应用 ³ × ▶ Bing 3 - ■ ♣ - 页面 助 注销	2 。 ■ 」 ● 2 、 安全(S) 、 工具(O) ・ ④ ■ 2 、 安全(S) ・ 工具(O) ・ ④ ■ 2 、 (O) ● ■ 2 、 (O) ● ■ 2 、 (
在 "客户机认证 集成解决方案登制合 - Tindors (中定) 编辑 ② 查看 ① 收潮 ☆ 收藏来 ☆ ○ 建议网站 - @ ● 集成解决方案控制台 ntegrated Solutions Console add 初图: [所有任务 = 欢迎 回指导性活动 日服务器 = 应照程序服务器 = 一般服务器 = 一般服务器 = 一般服务器	 "中选择 "」 Internet Explorer (9043/ibm/console/login.de? 来(a) 工具(2) 帮助(2) 免费 Hotmail 2 升级浏览器 min, 次迎您 应用程序服务器 回用程序服务器 目消息 会員 資格 	 公需的",然后单 action=sect ▼ 2 证书错误 2 4 2 g - g - w - 6 (更改了您的本地配置。您可以: (原改)年之前 (原改)年之前 (原改)年2 	击"应用" × ♪ Bing - □ 鳥 • 页面 助 注销	
在 "客户机认证 集成解决方案登制合 - Tindors (中定) 编辑 ② 查看 ① 收编: ② ● ② https://localhost ② ● ③ ● 建议网站 - ② ③ 集成解决方案控制台 ntegrated Solutions Console adu 初图: 所有任务 = 次迎 回指导性活动 日服务器 = ◎ 開程序服务器 = 一般服务器 = 一般服务器 = 一般服务器 = ① 代理服务器 = 305 Server V5	 "中选择 "」 Internet Explorer (9043/1bm/console/login.de? 来(山) 工具(1) 帮助(1) 免费 Hotmail 2) 升级浏览器 前面, 次迎您 应用程序服务器 应用程序服务器 自消息 資源 資源 資源 資源 資源 資源 資源 資源 資源 	 公需的",然后单 action=sect ▼ 2 证书错误 2 4 2 action=sect ▼ 2 10 10 10 10 10 10 10 10 10 10 10 10 10	击"应用" × ♪ Bing → □ 鳥 • 页面 助 注销	・ ・
在 "客户机认证 また#決方業登録合 - Tindors また#決方業登録合 - Tindors (中で) 編輯 ② 查看 ② 收壊: 2 收蔵来 会 ○建议网站 - @ ● 集成解決方案控制台 ntegrated Solutions Console add 初密: 所有任务 = 次迎 回指导性活动 日服务器 = <u>©用程序服务器</u> = 一般服务器 = 一般服务器 - 分服务器 - 分服务器	 "中选择 "」 Interact Explorer (9043/1bm/console/login.do? 来(a) 工具(1) 帮助(b) 免费 Hotmail @ 升级浏览器 min, 次迎您 应用程序服务器 应用程序服务器 目消息 企具直接 保存 通 	必需的",然后单 ▲ction=sect 文 证书错误 ④ ↔ 2 ▲ ▲ ▲ ▲ ▲ 本 本 本 本 本 本 本 本 本 本 本 本 本	击"应用" × ♪ Bing → □ 喇 - 页面 助 注销	・ ・
在 "客户机认证	 "中选择 "」 Internet Explorer (9043/1bm/console/login.do? (9043/1bm/c	公需的",然后单 ▲tion=seet ♥ ♥ 证书错误 ● ♥ 2 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	击"应用" × Ping × · · · · · · · · · · · · · · · · · · ·	・ ・
在 "客户机认证		必需的",然后单 actionesee、 ◎ 证书错误	击"应用" * 『 ^{Bing} * 『 · 页面 助 · 注销 · · · · 页面 · · · · 页面 · · · · 页面 · · · · · · · · · · · · · · · · · · ·	** ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
在 "客户机认证 ま成ftp;方案登制合 - 1 indows ま成ftp;方案控制合 - 1 indows	····································	公需的",然后单 actioneseet ♥ @ 证书错误 ● ♥ 2 actioneseet ♥ @ unit # # # # # # # # # # # # # # # # # # #	击"应用" × P Bing × 页面 助 : 注销 	・ ・
在 "客户机认证 ま成ffty方案登制合 - 1 indows ま成ffty方案控制合 上ttp://localhost 文件 ② 編輯 ③ 查看 ③ 收壊 文件 ③ 編輯 ③ 查看 ④ 收壊 文件 ③ 編輯 ③ 查看 ④ 收壊 本 中國 中心 一	·"中选择 "」 Interact Explorer (9043/1bm/console/login.do?) (9043/1bm/console/login.do?) (9043/1bm/console/login.do?) (9043/1bm/console/login.do?) (9043/1bm/console/login.do?) (9043/1bm/console/login.do?) (9043/1bm/console/login.do?) (9043/1bm/console/login.do?) (9043/1bm/console/login.do?) (905) (905) (906) (907)	公需的",然后单 ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	击"应用 * ^[] ^{Bing} * ^[] ^[] • 页面 助 : 注销 ^[] ^[] ^[] ^[] ^[] ^[]	・ ・
在 "客户机认证 ま成ftyj5案を教会 - lindows () () () () () () () () () () () () () (·"中选择 "」 Interact Explorer (3043/1bm/console/login.do?) (3043/1bm/console/login.do?) (3043/1bm/console/login.do?) (3043/1bm/console/login.do?) (3043/1bm/console/login.do?) (4) 工具(1) 帮助(2) (5) 我想 Motional @ 月級調鑑 (5) 如用程序服务器 (5) 如用程序服务器 (5) 四用程序服务器 (6) 四用程序服务器 (7) 日清息 (7) 日清息 (7) 日清息 (7) 日清息 (7) 日清息 (7) 日常	 ○公需的",然后单 ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	击"应用" × P Bing > - 页面 助 : 注销 - 页面 - 页 - 页面 - 页 - 页 - 页 - 页 - 页 - 页 - 页 - 页	 ・ 安全(S)・ 工具(O)・ (P) ・ 安全(S)・ 工具(O)・ (P) ・ 安全(S)・ 工具(O)・ (P) ・ 正計 ・ 正計<
在 "客户机认证 ま成前決方案登制合 - Jindows () · · · · · · · · · · · · · · · · · · ·	····································	公需的",然后单 ■ 世報書课 ● ● ● ■ 世報書课 ● ● ● ■ ● ■ ● ■ ● ■ ● <	击 "应用 ; × ▶ Bing > → 页面 功 : 注销 902置的 g. SaBiottás. 还可以	***********************************
在 "客户机认证 ま成解决方案登制合 - Jindows () · · · · · · · · · · · · · · · · · · ·	Interact Explorer 10003/1 bm/console/login.do? 8003/1 bm/console/login.do? 80043/1 bm/console/login.do? 90444 90445 9045	公需的",然后单 ■ 1000年4月19日、1000年4月19月	击 "应用 ★ 『● Bing → □ ● • 页面 助 注销 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	** ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
在 "客户机认证 ************************************	Interact Explorer 10003/1bm/console/login.do? 2003/1bm/console/login.do? 2003/1bm/	 込需的",然后单 ■ (1005260) (2014) ■ (2014) <	击 "应用 ★ 『● Bing → □ ● • 页面 助 注销 ▲ ● • 页面 ・ 页面 ・ □ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • ○ ● • • • •	・ ・
在 "客户机认证 集成前决方案控制合 - Jindows	Internet Explorer 10003/1bm/console/login.do? 2003/1bm/console/login.do? 2003/1bm	公需的",然后单 ▲ (1005560) 、《证书错误》 、《、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、	击 "应用" × ▷ 用 · 页面 助 注销 - ○ ● · 页面 助 注销 - ○ ● · 页面 - 页 - 页 - 页 - 页 - 页 - 页 - 页 - 页	・ ・
在 "客户机认证 ************************************	Interact Explorer S043/1bm/console/Login.407 第043/1bm/console/Login.407 要求 Astronail @ 升级浏览 勉強 Hotmail @ 升级浏览 DD用程序服务器 D用程序服务器 D用程序服务器 D用程序服务器 D用程序服务器 D用程序服务器 D目程序服务器 D目程序服务器 D目程序服务器 D目程序服务器 D目程序服务器 D目程序服务器 D目程序服务器 D目程序服务器 E D目程序服务器 D目程序服务器 D目目 D目 D目 D目 D目 D目 D目 D目 D目 DE DE <t< td=""><td>公需的",然后单 action=sect ▼ 2 证书错误 2 4 7 2 action=sect ▼ 2 10 2 4 7 2 bit ○ 10 2 10 2 10 2 10 2 10 2 10 2 10 2 10</td><td>击 "应用" × ▶ Bing → ● → 页面 助 注 → ○ ● → 页面 助 注 → ○ ● → 页面 → ○ ● → ○ ● → 页面 → ○ ● → ○ ● → ○ → ○ → ○ → ○ → ○ → ○ → ○</td><td>・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・</td></t<>	公需的",然后单 action=sect ▼ 2 证书错误 2 4 7 2 action=sect ▼ 2 10 2 4 7 2 bit ○ 10 2 10 2 10 2 10 2 10 2 10 2 10 2 10	击 "应用" × ▶ Bing → ● → 页面 助 注 → ○ ● → 页面 助 注 → ○ ● → 页面 → ○ ● → ○ ● → 页面 → ○ ● → ○ ● → ○ → ○ → ○ → ○ → ○ → ○ → ○	・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・

进入"服务器"->"应用程序服务器",选择"server1",

▲ 「「「「」」 「」」 「」」 「」」 「」」 「」」 「」」			
		±4#22 💿 🍖 🗙 🌌 Ring	
又件使) 調釋(E) 查看(Y) 收藏夹(E)	工具(1) 報助(4)		
😭 收藏夹 🛛 🍰 💽 建议网站 👻 🖉 免费 💈	Hotmail 🏉 升级浏览器 🗸		
🏉 集成解决方案控制台		🚹 🕶 🗟 👻 🖃 🖶 🕶 页面 🕲	▼ 安全(S)▼ 工具(0)▼ 🕢
Integrated Solutions Console admin,	欢迎您	帮助 注销	IEM.
视图:所有任务	应用程序服务器 > server1		*
- 欢迎	使用此页面来配置应用程序服务器。应用程	序服务器是提供运行企业应用程序所需服务	帮助
田指导性活动	的服务器。		字段帮助
日服务器	育C 宜		要获取字段帮助信息,请征 出现帮助光标时选择字段#
- 应用程序服务器			签或选择列表标记。
■ 一般服务器	常規尾性	容器设置	页面帮助
= 代理服务器	名称	■ <u>会话管理</u>	关于此页面的更多信息
 JMS Server V5 	the formation of the fo	I SIP 容器设置	
= Web 服务器	WinServer2003Node01	曰 Web 容器设置	1
= 集耕		= <u>Web 容器</u>	
 ● 未付3口31 ●		■ <u>Web 容器传输链</u>	P
WebSphere MO Serv	▶ 开行启动	田 Portlet 容器设置单击以配置通序	句 Web 容器的传输通道服务链。
田核心组	い いん いっぽう いっぽう いっぽう いっぽう いっぽう しんしょう ●	■ EJB 容器设置	
用 应田程序		容器服务	
日资源	特定于服务器的应用程序设置	■ 业务流程服务	
日安全性	突張八諸東略 多个 ▼	应用程序	
	***	■ 已安装的应用程序	
- SSL 证书和密钥管理	首先装入父类	服务器消息传递	
 总线安全性 		- 消息传递引擎	
		····································	
https://localhost:9043/ibm/console/com.i	bm.ws.console.channelfw.forwardCmd.do?for	—————————————————————————————————————	🖓 • 🔍 100% • //

选择"Web 容器设置"->"Web 容器传输链",

		/			
	et Explorer				_ 🗆 🗵
🕞 😔 🗢 🙋 https://localhost:9043/ibm,	/console/login.do?action=sect💌 😵	🛛 证书错误 🛛 😣 😏	🗙 ಶ Bin	c .	₽ -
文件 (ℓ) 编辑 (ℓ) 查看 (ℓ) 收藏夹 (៤) 工	具(T) 帮助(H)				
🖕 收藏夹 🛛 🍰 建议网站 🗸 👩 免费 Hota	mail 🙋 升级浏览器 🔹				
🏉 集成解决方案控制台		🟠 -	s - 🗆 🤅	• 页面 (2) •	安全 (3) • 工具 (0) • 🕢 •
Integrated Solutions Console admin, 🕱	迎您	君	₨助 注铂		IEM.
 祝留:所有任务 双迎 西指导性活动 四指导性活动 	▲ 已更改了您的本地的 直接 <u>保存到</u>主配置。 保存或放弃之前 查看更改。 查看可找。 中日百代 	2置。您可以: 2度之后同步多个节点中	的配置的法		帮助 字段帮助 要获取字段帮助信息,请
■ 应用程序服务器 ■ 一般服务器 ■ 代理服务器	项。	,可能需要重新启动服务	器.		出现帮助光标时选择于段相签或选择列表标记。 页面帮助 关于此页面的更多信息
■ JMS Server V5 ■ Web 服务器 ■ 集群	使用此页面来查看和管理传输链。传输 栈。 田 首选项	19 日本18 年1914年 链表示在客户机或服务器	8中操作的网络	络协议堆	
■ 集群拓扑 ■ 一般服务器集群	新建删除				
= WebSphere MQ Serv			h.l		
	选择 名称 🛟	已启用 王机 ◇	嗝□ ◇ ,	启用 SSL	
田屋用程序	WCInboundAdmin	已启用 *	9061	已禁用	
田资源	WCInboundAdminSecure	已启用 *	9044	已启用	
	WCInboundDefault	已启用 *	9080	已禁用	
■ 安全管理、应用程序和 CCLごTお知念提等理	WCInboundDefaultSecure	已启用 *	9443	已启用	
= SSL 址书和密钥官理 = 总线安全性	总数 4				*
完成			- J 🛛 😼 z	本地 Intranet	🖓 🕶 🔍 100% 👻 🖉

选择"WCInboundDefaultSecure",



选择"SSL入站通道(SSL_2)",



在"SSL 配置"中,选择"特定于此端点",然后在"选择 SSL 配置"中,选择刚才创建的 SSL 配置"WASSSL",单击"应用"。

②集成解决方案控制台 - Windows Inter → → → → http://localbast-9043/il	net Explorer	
🍟 収藏夹 🍰 🕒 建议网站 👻 🖉 先费 K	otmail 🟉 升级调览器 ▼	
🏉 集成解决方案控制台		页面(2) - 安全(3) - 工具(0) - 🕡 -
Integrated Solutions Console admin, 2	欢迎您 帮助 注销	
视图: 所有任务	安全管理、应用程序和基础结构	
- 欢迎	当管理受限制时,应用程序处理环境就受到全面的保护。应用程序以及支持管理和应用	程序的基础结构也受到保护。
田指导性活动	配置	
田服务器		
国应用程序		
田资源	安全配署向导 安全配署报告	
日安全性		
- 安全管理、应用程序和基础	管理安全性	认证
■ SSL 证书和密钥管理		□ 使用域限定的用户名
■ 总线安全性	= <u>自任祖用CL</u>	■ WeD 安全性
 Web Service 	应用程序安全性	
田环境	□ 启用应用程序安全性	= <u>CSIV2 八站队证</u> - CSIV2 出站认证
田系统管理		<u>CSIv2 出站沃祉</u> ■ CSIv2 入站传输
田用户和组		= CSIv2 出站传输
田监视和调整	☑ 记用 Java 2 文主任未被而述用程序仍同本地员保 ☑ 如果对应用程序授予定制许可权则发出警告	∃ Java 认证和授权服务
田故障诊断	□ 限制对资源认证数据的访问	= 认证机制和到期
田服务集成	田户帐户存储库	
	当前域定义	从刘博拉博佛祖南
	联合存储库	
	可用的域定义	
	联合存储库 ■ 配置 设置为当前	
		×
	□ □ □ □	tranat

进入"安全性"->"安全管理、应用程序和基础结构"->"认证"->"RMI/IIOP 安全性",选择"CSIv2入站认证",

🌈 集成解决方案控制台 - Windows Inte	rnet Explorer
🕞 😔 🗢 🙋 https://localhost:9043/	ibm/console/login.do?action=secur 💌 😵 证书错误 💀 🐓 🗙 ಶ Bing 🖉 🔸
文件(E) 编辑(E) 查看(V) 收藏夹(A)	工具 (I) 帮助 (H)
🚖 收藏夹 🛛 🍰 🦲 建议网站 👻 💋 免费	Hotmail 🙋 升级浏览器 -
🥖 集成解决方案控制台	🚹 • 🗟 - ፲ඛ 🐑 • 页面 🕑 • 安全 S) • 工具 🕛 • 🕡 •
Integrated Solutions Console admin,	欢迎您 帮助 注销 #助 注销 # #助 注销 # ###.
视图:所有任务	安全管理、应用程序和基础结构 > CSIv2 入站认证
= 欢迎	使用此面板来指定此服务器使用对象管理组(OMG)公共安全互操作性(CGI)
田指导性活动	
田服务器	
■应用程序	万面帮助
田资源	常規雇性 大丁以美国的更多情息
日安全性	基本认证
= 安全管理、应用程序和基础	
 SSL 证书和密钥管理 	○ 2.565 ○ 必需
= 忌线安全性 Web Convice	
web Service	客户机证书认证
田环境	
田系统管理	C 必需
田用户和组	
田监视和调整	□ 身份声明
田故障诊断	可信标识
田服务集成	
■ UDDI	▶ 有状态会话
	登录配置
	RMI_INBOUND
	☑ 安全属性传播
完成	本地 Intranet 4 100% - /

在"客户机证书认证"中,选择"必需",单击"应用"。然后再选择"CSIv2

出站认证",

集成解决方案控制台 - Windows Inter	net Explorer		
🕞 🕞 🗢 👩 https://localhost:9043/i	bm/console/login.do?action=secure 📃 😵 证	书错误 😣 😽 🗙 ಶ Bing	P •
文件(E) 编辑(E) 查看(Y) 收藏夹(A)	工具 (I) 帮助 (H)		
🖕 收藏夹 🛛 🍰 🔁 建议网站 👻 🙋 免费 H	iotmail 🙋 升级浏览器 -		
🌈 集成解决方案控制台		👌 • 🗟 - 🖻 🖨 •	・ 页面 (2) ・ 安全 (3) ・ 工具 (0) ・ 😯 ・
Integrated Solutions Console admin,	欢迎您	帮助 注销	IBM.
视图: 所有任务 : 次迎 □指导性活动 □服务器 □应用程序 □资源 □安全性 · <t< th=""><th>常規羅性 基本认证 ○从不 ○必需 客户机证书认证 ○从不 ○支持的 ○返需</th><th></th><th>孫助 字段帮助 从不 页面帮助 关于此页面的更多信息</th></t<>	常規羅性 基本认证 ○从不 ○必需 客户机证书认证 ○从不 ○支持的 ○返需		孫助 字段帮助 从不 页面帮助 关于此页面的更多信息
 ■ 起线交至112 ■ Web Service ■ 环境 ■ 系统管理 ■ 用户和组 ■ 监视和调整 ■ 故障诊断 ■ 融务集成 ■ UDDI 	□ 身份声明 ④ 使用服务器信任的标识 ④ 指定备用可信标识 可信标识 □ □ □ □ □ □ □ □ □ □ □ □ □		
	□ 定制出站映射		T
完成			Intranet 🖓 🔹 🔍 100% 🔹 🎢

在"客户机证书认证"中,选择"必需",单击"应用"。配置完成。

3.6.9 IHS+WAS 证书配置

安装 IHS 和 WAS,

安装 WAS 插件,

将准备好的 kdb 和 sth 文件复制到适当的目录中,如 C:\bin 中, KDB 文件的 生成方法请参考 3.4.4,

打开 IHS 的 conf 目录中的 httpd.conf 文件,在文件末尾加入如下内容: LoadModule ibm_ssl_module modules\mod_ibm_ssl.so

<IfModule mod_ibm_ssl.c>

Listen 443

<VirtualHost *:443>

ServerName 192.168.17.128

SSLEnable

SSLClientAuth Required

</VirtualHost>

</IfModule>

KeyFile "c:\bin\key.kdb"

SSLDisable

重启服务,配置完成!

3.6.10 F5 设备证书配置

F5 设备具体配置请以厂商手册为准,如下内容为参考:导入证书公钥如果是导入已经存在的域,则根据之前其他 F5 上的命名规则填写名称,如果为新建则使用如下命名规则, 域名_ssl_版本和根证书_域名_版本,例如: login_ssl_v3 和 parent_login_v3, Improt Type 选择"certificate", 找到 server.cer 公钥,选择"Improt"

L Certificate/Key Source	
Import Type	Certificate
Certificate Name	● Create New ○ Overwrite Existing 填写证书名称
Certificate Source	● Upload File ● Paste Text 选择文件 主法探文件

导入证书的私钥 Key 文件为生成 csr 时生成的文件(第一步中下载压缩包 内容 key 文件),如果是导入已经存在的域,则根据之前其他 F5 上的命名规则填 写名 称,如果为新建则必须与证书名称相同,例如:证书名称为 login_ssl_v3, key 的名称也与证书名相同, Improt Type 选择"key",找到 server.key 私钥,选择 "Improt"

Local Traffic » SSL Cer	tificates » Import SSL Certificates and Keys	
SSL Certificate/Key Sour	ce	
Import Type	Key	
Key Name	 Create New Overwrite Existing 名称必须与SSI证书名称相同 	
Key Source	 ● Upload File ● Paste Text 选择文件 未选择文件 	
Cancel Import		か

导入 CA 中级证书 选择 Local Traffic-〉SSL Certificates 在 SSL Certificate List 主界面点击右上角"Import",证书邮件保存的 intermediate.cer 使用"Certificate"方 式导入。

SL Certificate/Key Sour	ce
Import Type	Certificate
	Overwrite Existing
Certificate Name	ca-bundle
Cartificata Source	Upload File O Paste Text
Certificate Source	c:\ intermediate.cer 浏览

导入成功后, F5 将自动识别导入的证书为 Certificate Bundle。

配置服务器证书 选择"Local Traffic"-"Vitual Servers"-"Profiles" 选择"Proflie" 中, "SSL"下的"Clent"进入"Client SSL Profile"设置 如果您需要为站点配置一个全 新的 SSL 证书,则您需要新建一个 Client SSL Profile。如果您需要为一个已有 证 书的站点更新服务器证书,则仅需点击已存在的 Profile,进行编辑更新操作即可。



在新建的 Profile 中,选择当前 Profile 所使用的证书(Certificate)、私钥 (key),以及在 Chian 处,设置与 该证书应用相关联的证书链(之前导入的中 级 CA 证书)。完成后,选择"Update"保存

	Traffic Summary		General Properties		
	Performance Statistics		Name	test SSL	
				Tuedoor	
Local Traffic		Parent Profile	clientssl 💌		
-0	Network Map				
	Virtual Servers	+	Configuration: Advanced V		Custom
	Profiles	Ŧ	Certificate	test_cert 💌	
	II iRules	Ŧ			-
	Pools	+	Key	test_cert	
	D Nodes	+	Pass Phrase		
	Monitors	+			
	Rate Shaping	+	Confirm Pass Phrase		
	SNATs	+	Chain	ca-bundle V	
	SSL Certificates	+			
	Network		Trusted Certificate Authorities	Tione Y	
	Interfaces, Routes, Self IPs, Fiters, Spanning Tree, Trunk VLANs, ARP	Packet s,	Ciphers	DEFAULT	
System				8	8
Licensing, Platform, High Availability, Archives, Preferences, SNMP, Logs,		Options	Options List ~		
	usera, console			Enabled Options	

在证书成功配置后,需要创建一个 443 端口的 Virtual Server,并加载上面的 Client SS Profile 对应该站点 启用 SSL 证书。

3.6.11 SAP 证书配置

导入个人信息交换文件,事务码 STRUST,双击文件节点

☞ PRD(1)/900 信任管理器:	更改		
🖉 💽 👻 🧧	🔍 😪 l 🖨 li 🖨 l 🞗) 🔁 📮 🖬 🛛 😨 🖳 😨 💭	
信任些硼೪, 雨水			
海江自坯罐: 丈以			
69 🕅			
▶ 💼 系统个人安全环境	文件		
・ X SNC SAP 密码库	自己的证书		T.
・ 🗶 SSL 服务器 标准	主题		
・ X SSL 客户端 SSL 客户端 (置名) ・ X SSL 客户端 SSL 客户端 (标准)			
・ 🗙 Web 服务安全性 标准		颁发者证书	
・ 🔀 Web 服务安全性 其他系统加密证书			
・ X Web 服务安全性 Web 服务安全性能			
		x	
・ 🗶 安全存储和转发 协作集成库: oAut			
・ 🞽 安全存储和转发 在线学习			
・ 🖸 安全存储和转发 登录票证	证书列表		
		主题	
		•	
	6		

选择 pfx 个人信息交换文件

+

111/1				
查找范围(I):	大童保险域名证书) 🎓 🔛 🛄 🖌		
名称	ř.	修改日期	类型	大小
	214032051140911.key	2017/7/7 17:58	KEY 文件	2 KB
快速访问	214032051140911.pfx	2017/7/7 17:58	Personal Informati	5 KB
桌面				
库				
此电脑				
网络				
7.7				
输入 pfx	密码			
		ĸ		
• 🛪 SMI	ME标准			
・ 🗘 文件				
・ 🔀 安全	存储和转发 协作集成库:oAut		_	
・ 🔀 安全	1 □ PRD(1)/900 文件	×		
・ 🗗 安全	1			
	· 密码 ******	<mark>akakakakakakaka</mark> ka		
				主题

显示如下,会提示缺少证书主体

<mark>1</mark> 🕝 PRD(1)/900 导入	、密钥对 (PKCS12)		
1 私钥	01 alias	•	
主题	CN=*.dtinsure.com, OU=IT, O=\u5927\u	17AE5\u4FDD\u9669\u9500\u552E\u670D\u52A1\u670	9\u96
颁发者	CN=GeoTrust SSL CA - G3, O=GeoTrust	Inc., C=US	
所缺少证书的主体			
CN=GeoTrust G	lobal CA, O=GeoTrust Inc., C=US		
主体		颁发者	
CN=*.dtinsure.com,	OU=IT, O=\u5927\u7AE5\u4FDD\u9669\u9500\u	CN=GeoTrust SSL CA - G3, O=GeoTrust Inc., C=US	
CN=GeoTrust SSL C	A - G3, O=GeoTrust Inc., C=US	CN=GeoTrust Global CA, O=GeoTrust Inc., C=US	
			-
< ><		4	F
_			
			X

certmgr.msc 进入证书管理器,导出主体证书

t Root Certificate Aut...

Microsoft Root Certificate A...

🚘 certmgr - [证书 - 当前用户\受信任的根证书颁发机构\证书] 文件(F) 操作(A) 查看(V) 帮助(H) 🗢 🔿 📷 🖌 🗞 🗮 🗶 🖬 🖬 🗊 证书 - 当前用户 颁发给 価労者 截止日期 预期目的 友好名称 > 📔 个人 🗔 DST Root CA X3 DST Root CA X3 2021/9/30 安全电子邮件, 服务... DST Root CA X3 🧮 受信任的根证书颁发机构 Entrust Root Certification Au... Entrust Root Certification Auth... 2026/11/28 服务器身份验证,客... Entrust 📔 证书 Entrust Root Certification Au... Entrust Root Certification Auth... 2030/12/8 服务器身份验证,客... Entrust.net □ 企业信任 🔄 Equifax Secure Certificate Au... Equifax Secure Certificate Auth... 2018/8/23 安全电子邮件,服务... GeoTrust > 📔 中间证书颁发机构 📮 erp6ehp8.sgsap.com erp6ehp8.sgsap.com 2018/4/6 <所有> <无> > 📔 Active Directory 用户对象 2038/1/1 ☐ fk1.dtinsure.com fk1.dtinsure.com <所有> <无> > 📔 受信任的发布者 Flex GateWay CA Flex GateWay CA 2026/7/24 <所有> <无> > 📔 不信任的证书 GDCA TrustAUTH R5 ROOT GDCA TrustAUTH R5 ROOT 2040/12/31 服务器身份验证,客... GDCA TrustAUTH > 📔 第三方根证书颁发机构 GeoTrust Global CA 服务器身份验证,客... GeoTrust Global ... GeoTrust Global CA 2022/5/21 > 📔 受信任人 GeoTrust Primary Certificatio... GeoTrust Primary Certification ... 2036/7/17 服务器身份验证,客... GeoTrust > 📔 客户端身份验证颁发者 GeoTrust Primary Certificatio... GeoTrust Primary Certification ... 2037/12/2 服务器身份验证,客... GeoTrust Primarv... > 📔 其他人 > 📔 MSIEHistoryJournal 🔄 GlobalSign GlobalSign 2029/3/18 服务器身份验证,客... GlobalSign 🔄 GlobalSign Root CA GlobalSign Root CA 2028/1/28 服务器身份验证, 客... GlobalSign > 📔 证书注册申请 服务器身份验证, 客... Go Daddy Class 2... > 🧮 智能卡受信任的根 🔄 Go Daddy Class 2 Certificati... Go Daddy Class 2 Certification... 2034/6/30 Go Daddy Root Certificate A... Go Daddy Root Certificate Aut... 2038/1/1 服务器身份验证,客... Go Daddy Root C... GTE CyberTrust Global Root GTE CyberTrust Global Root 2018/8/14 安全电子邮件, 客户... DigiCert Global R... 🔄 Microsoft Root Authority Microsoft Root Authority 2020/12/31 <所有> Microsoft Root A... Microsoft Root Certificate A... Microsoft Root Certificate Aut... 2021/5/10 Microsoft Root C... <所有> Flex GateWay CA 2026/7/24 Flex GateWay CA <所有> <无> 🔄 GDCA TrustAUTH R5 ROOT GDCA TrustAUTH R5 ROOT 2040/12/31 服务器身份验证,客... GDCA TrustAUTH .. GeoTrust Glob 服务器身份验证 客 GeoTrust Globa 打开(0) 🔄 GeoTrust Prim Primary Certification 2036/7/17 服务器身份验证, 客... GeoTrust 所有任务(K) GeoTrust Prim 打开(O) 服务器身份验证,客... GeoTrust Primary... 2037/12/2 🔄 GlobalSign 2029/3/18 服务器身份验证, 客... GlobalSign 剪切(T) 导出(E)... 服务器身份验证, 客... GlobalSign 🔄 GlobalSign Ro 2028/1/28 复制(C) 🗔 Go Daddy Cla Class 2 Certification... 2034/6/30 服务器身份验证, 客... Go Daddy Class 2... 删除(D) Go Daddy Roc Root Certificate Aut... 2038/1/1 服务器身份验证,客... Go Daddy Root C... 属性(R) GTE CyberTrue rTrust Global Root 2018/8/14 安全电子邮件, 客户... DigiCert Global R... 🖾 Microsoft Roo Root Authority 2020/12/31 <所有> Microsoft Root A... 帮助(H)

2021/5/10

<所有>

Microsoft Root C...



导出文件格式

可以用不同的文件格式导出证书。

选择要使用的格式:

- 〇 DER 编码二进制 X.509 (.CER)(D)
- Base64 编码 X.509(.CER)(S)
- ○加密消息语法标准 PKCS #7 证书(.P7B)(C)
- 如果可能,则包括证书路径中的所有证书(I)
- 个人信息交换 PKCS #12(.PFX)(P)
 - 🗌 如果可能,则包括证书路径中的所有证书(U)
 - 🗌 如果导出成功 , 删除私钥(K)
 - 导出所有扩展属性(A)
 - 启用证书隐私(E)
- Microsoft 系列证书存储(.SST)(T)

下一步(N)

取消

 \times



- 👩 WED 服务女子性 县他系统加给		
・ × Web 服务安全性 Web 服务安全		
・ 🗙 SMIME 标准	☞ PRD(1)/900 号》证书	· · ·
・ 🛇 文件		· · ·
・ 🔀 安全存储和转发 协作集成库:0	文件 数据库 地址簿 目录服务 SAP 系统	
・ 🗶 安全 🕞 PRD(1)/900 导入密钥		
	文件路径 C:\Users\Solor\Desktop\大童保险减多证书\GeoTrust.ced	
私钥		
主题 CN=		2A1\u6709\u96
颁发者 CN=		
所缺少证书的主体		
CN=CeoTrust Clobs		
主体		
CN=*.DTINSURE.COM, C	<i>I</i>	US
CN=GEOTRUST SSL CA -	•	US
		_
4 🕨		
4 >		
	-	

另存为服务器个人安全文件

¢		证书(C) 环境(⊻) 系统(Y) 帮助(出)
6	导入(I)	
	写出(E) 另存为(<u>S</u>)	
6	创建个人安全环境验证(⊻) 	_
	全部检查(A) F5 全部分配(1) F6	服务器 标准 已的证书
1	业(区) Shift+F3	CN=*.dtinsure.com, OU=IT, O=\u5927\u7AE5\u4FDD\u9669\u9500\u552E\u670D\ CN=*.dtinsure.com, OU=IT, O=\u5927\u7AE5\u4FDD\u9669\u9500\u552E\u670D\
	 ズ SSL 客戸端 (标准) X Web 服务安全性 标准 X Web 服务安全性 其他系統加密证书 X Web 服务安全性 Web 服务安全性 X Web 服务安全性 Web 服务安全性 X SMIME 标准 ○ 文件 	
	 苯 安全存储和转发 协作集成库: oAut 苯 安全存储和转发 在线学习 □ 安全存储和转发 登录票证 	☑信任颁发者证书



浏览器输入域名测试,显示证书安全,则证书导入成功

人

登录 X						()	idar) (=	0	23
← → C ● 安全 https://fk.dtin	sure.com/fk1				☆	0 0	6	۲	:
	用户								
노랫 삶 집 것을	密码								
	语言	ZH - 中文		۲					
	2010 2010		再改变 和	4					
		~	ZMER	,	A				
			1	Y					
							13	3	
	S			Copyright ©	2017 DATC	ING INSUF	E. All righ	s reserv	ed.

3.6.12 阿里云通用证书配置

1、进入 SSL 证书管理页面 https://www.aliyun.com/product/cas, 点击 SSL 证书管理台进入证书管理页面。

	C REAL 1966. M. MANERER & R IX 24 24 216 RR C () R ()
51.E46	如何使用证书中品。
- 	公告 7章110
▼ 105000 ± 10000 ⊕ -000000000000000000000000000000000000	日本語の時間 日本語を時代 日本語を特合な原則両属 日日 日日 日日 日日 日日 日日 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 同様 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の時間 日本語の 日本語の 日本語の 日本日の日本日の日 日本日の日 日本日の日 日本日の日 日本日の日 日本日の日 日本日の日日 日本日の日日 日本日の日日 日本日の日日 日本日の日日 日本日の日日 日本日の日日 日本日の日日 日本日の日日 日本日の日日 日本日日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日
部送没有证书,可以通过以下方式送出证书 同日 期度证书	第30時間 55 55 55 55 55 55 55 55 55 5
	安全振动
ID 完成	⑦ (1) 角 (0) ④ 100%

2、点击上传证书按钮,输入证书名称,证书文件。证书私钥,点击确认完 成证书上传。

上传证书

*

•证书名称:

测试1

名称仅支持英文字母、数字、下划线、中线

• 证书文件:



• 证书私钥:

rYnLsBloaoGHWTE+/6t6xQlxJlsPeJv01Br0GXEBmp2DZ38xRA6GAdn6ajOjjjMOv rYJrhGGDGWVAwvmfT5dbCfLj31X8OANuWOVfdqTLtN/nVa6s+h/wUbol7xheshz1 bTXWfQKBgAMtcwvWYkyJNvVe3cNTSckcUkx2aDx58H1H7YkzBMOyJt/7XO93yG8A tY/CM0AktC68DCOMN6uiXIJASkmKamdQUhe73XVt2tYgQXg9T6XJReXgRGgD6LFu KQOfKfakOYIshR/8Zfzvtx51q5Rha1YXR2Ry1bR4sMW/ZP159qug -----END RSA PRIVATE KEY-----

为了更好的保护您的证书数据安全,上传的证书不支持下载!

确定 取消

证书名称:名称仅支持英文字母、数字、下划线、中线

证书文件:公钥证书,即 CFCA 邮件中:单位名称.cer 文件内容

证书私钥: 生成 csr 时产生的 key 文件。如果有密码,需要去除密码后上传

pem 文件。如果是 jks 或者 pdf 文件,见本文档 3.5 章节证书格式转化。

3、选择证书,点击部署根据需求部署到对应网站即可

				Q 搜索文档, 控制台, 1	PL 解决方案和资源	勝用 工単 警査 企	业 支持 1	n 🖸 🖞 🗑 🕷 🧕
SSL证书								如何使有正书严量?
正ちき数 ◎	BRRIZMBOJERS € O) 审核失败的证书 ()	已过期的证书 ()					公告 [重要] DigiCet系统升级公告
実際定時 企上伸延時 印一線町代目195 全部状态 > 全部規準	✓ 证书加名	Q					88 =	1) 年回新示明 新版本控制台使用描闻 SSL证书安岐描闻(包含途种报务器) Symentec SSL数字证书升级漏迹强示
征书	品牌	状态	潮定域名	签发时间/到期时间 #	5# 8		操作	20/00
962 509- (20)	Ona	DEx				710 ES -	TH DO	
▷ 完成								○ 4 金 ○ 0 € 100%

3.6.13 阿里云 LSB 证书配置

- 1、以下地址进入 SLB: https://slbnew.console.aliyun.com/slb。
- 2、负载均衡 SLB-证书管理-创建证书

≡ сЭ阿里云	华东1 (杭州) 🔻	Q 搜索			费用	工単	备案	企业 支持与服务	⊠ Ų, jä	() ନି	简体中文 🌔
负载均衡 SLB	▲ 负载均衡 SLB / 证	日本管理									 ④ 证书要求
概览	证书管理	₽									
实例	2 创建证书	删除全部过期证书	搜索证书		Q						C 🕸
实例管理	证书名称/ID	证书城名	创建时间小	过期时间 1	关联监听			关联扩展城名	证书类型 ▽	证书来源	操作
回收站											
证书管理 1					没有	数据					
访问控制											
日志管理											
操作日志											
访问日志											
健康检查日志											_
SLB 实验室											API
闲置实例											e
配额管理											88
3、上传目	下阿里云签	这发证书	—填空	写证书:	名称						

	Q 擔东	嘉用 工单 輪索 企业 支持与服务 🖸 🗳 🖓 🕜 🏠 简体中文 🌔
负载均衡 SLB	负载均衡 SLB / 证书管理	创建证书 ×
截流	证书管理	^
实例	创建证书 删除全部过期证书 接卖证书	远禅词里云盔发证书 上传非问里云盔发证书 I
实例管理	证书名称/ID 证书域名 创建时间 4 过期时间 4 关款监听	* 11 BAR (
回收站		
证书管理		* 证书部署地域
访问控制		华东1 (杭州) × ×
日志管理		* 证书关型
操作日志		
访问日志		
健康检查日志		 公明证书: ● 1
SLB 实验室		
闲置实例		
配版管理 https://certlogik.com/ssl-checker/		NTRE ROOM

4、证书类型选择--服务器证书,填写公钥证书内容及私钥

☰ (-)阿里云	Q 搜索	费用 工单 备案 企业 支持与服务 🖸 🗳 🗟 🔞 简体中文 🍥
负载均衡 SLB	▲ 负载均衡 SLB / 证书管理	创建证书
概范	证书管理	· 证书类型
实例	创建证书 删除全部过期证书 搜索证书	
实例管理	证书名称//D 证书域名 创建时间 4 过期时间 4 :	U CA社书 关联监听
间收站		* 公明证书: ②
证书管理		
访问控制		
日志管理		
操作日志		上传 荒容NGINX推式 查看样例
访问日志		* 秋钥: 💿
健康检查日志		1
SLB 实验室		
闲置实例		
配颜管理		新建取消
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		

#### 说明:

公钥证书:此处包括 SSL 证书及中级证书,格式如下:

----BEGIN CERTIFICATE-----

SSL 公钥证书(BASE64 编码)—CFCA 邮件中:单位名称.cer 文件内容

-----END CERTIFICATE-----

!!!中间不可有空行!!!

----BEGIN CERTIFICATE-----

中级公钥证书(BASE64 编码)—CFCA 邮件中: CFCA_OV_OCA. cer (OV 证书添加此文件内容) **CFCA_EV_OCA. cer**(EV证书添加此文件内容)

-----END CERTIFICATE-----

**私钥:**与 CSR 同时产生保存的. key 文件,格式如下:

----BEGIN RSA PRIVATE KEY-----

证书私钥(BASE64 编码)

----END RSA PRIVATE KEY-----

5、证书类型选择—CA证书

	Q 搜索	费用 工单 音繁企业 支持与服务 🖸 🕻 🏹 🕜 🏫 简体中文 🌔
介 负载均衡 SLB	贪裁均衡 SLB / 征书管理	创建证书 ×
概造	证书管理	
实例	· · · · · · · · · · · · · · · · · · ·	・ バーオフの 安 Webet
实例管理	证书名称/ID 证书域名 创建时间4 过期时间4 关联监听	NET DIALWEAKSAR 半年1 (杭州) × ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
回收站		* ① 书乐当
证书管理		
访问控制		● CA证书
日志管理		
操作日志		* 客户調CA公钥证书 ②
访问日志		
健康检查日志		
SLB 实验室		
闲晋车例		上传 兼容NGINX格式 查看样例
		新建 取消

CA 证书: CFCA 根证书,格式如下

----BEGIN CERTIFICATE-----

CA 公钥证书(BASE64 编码) -- CFCA 邮件中: CFCA_EV_ROOT.cer 文件内容 ------END CERTIFICATE------

6、完成证书上传

7、进行实例管理,依次:实例管理-监听配置向导

	华东1	(杭州) 🔻	Q 搜索			费用 工	单备案	企业 支持与服务 🖸	⊐ Q. A	0	
负载均衡 SLB	^	负载均衡	SLB / 实例管理								⑦ 什么是负载均衡实例
概览		实例	管理								
实例	-	ARRES	また 法法 なん マ			#お入交役 in	aDiotatica (Malanda			0	
实例管理	1	BUILD N	1929+1002 *	PU/DE2 - 3EAP * 1	#14013£36 * Hj	880/ (10199), 10	20017-02211-0-19694003	Lat Q		U	
回收站			实例名称/ID	服务地址 🖓	状态 🔽	监控	实例体 检	端口/健康检查/后端服务器	~		操作
证书管理			auto_named_slb lb-bp1etvultrdfv2bxzc3xu	47.111.206.172(公网IPv4)	✓ 运行中		æ	点我开始配置		2	监听配置向导 添加后满服务薪
访问控制	- h		未设置标签								更多▼
日志管理			启动 停止 释放设置	编辑标签							
操作日志											
访问日志											
健康检查日志											
SLB 实验室	1										API
闲置实例											
配额管理											
	/										
8、 🖞	配置	HTT	PS								

☰ (-)阿里云	Q 擔张	费用 工单 备案	企业支持与服务 🖸 🚺 🙀	🕐 🍙 ^{简体中文} 🌔
へ 负载均衡 SLB				
概览				
实例	1 协议&监听 2 SSL证书	3 后端服务器	4 健康检查	5 配置审核
实例管理	选择负载均衡协议			
回收站	TCP UDP HTTP HTTPS 1			
证书管理	后端协议			
访问控制				
日志管理	2 请描写负载均衡SLB对外服务的端口			
操作日志				
访问日志	高级配置 ∠ 修改			
健康检查日志	调度算法 会话保持	HTTP2.0	访问控制	_
SLB 实验室	加权轮询	已开启	关闭	API
闲置实例	3			e
配额管理	下一步 取消			8
9、选择	上传的证书			
	Q 推定	费用 工单 备案	企业 支持与服务 🖸 🗳 📮	<ul> <li>⑦ 合 简体中文 </li> </ul>
■ (-) 阿里云 ○裁均衡 SLB	Q 推測 负载均衡 SLB / 负载均衡业务配置向导	费用 工单 备室	企业 支持与服务 🖸 🗘 🕁	<ul> <li>⑦ 合 简体中文 ①</li> <li>① 监听介绍</li> </ul>
■ (-) 阿里云	Q ## 2#### SH 2##############################	表用 工单 留室	<u> 企业 支持与服务</u> 四 <u> </u> () 只	<ul> <li>⑦ 命 陽雄中文 </li> <li>⑦ 箇所介绍</li> </ul>
(一) 阿里云     (丸能均衡 SLB     (広     (大))     (大)     (-     (-     (-     (-     (-     (-     (-     (-     (-     (-     (-     (-     (-     (-	Q ### ☆ #### 518 / ☆ ###################################	表用 工单 备金		⑦         合         简体中文         ①           ⑦         出版行外組
<ul> <li>         ・) 阿里云         ・         ・         ・</li></ul>	Q 注意 负载功衡 SLB / 负载均衡业务配置向导 ← 负载均衡业务配置向导 → 协议&监听 2 SSL证书	表用 工单 备尝 3 后端服务器	企业 支持与服务 []         ①         〕         □         〕         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □         □ <t< td=""><td><ul> <li>⑦ 合 简体中文 ④</li> <li>⑦ 医听介绍</li> <li>3 配置审核</li> </ul></td></t<>	<ul> <li>⑦ 合 简体中文 ④</li> <li>⑦ 医听介绍</li> <li>3 配置审核</li> </ul>
<ul> <li>         ・         ・         ・</li></ul>	Q ##	表用 工单 智玄 3 后续服务器 ——	企业 支持与服务      口 ① 异       (4) 健康检查	⑦     合     簡体中文     ②       ⑦     监听介绍
<ul> <li>         ・) 阿里云         ・         ・         ・</li></ul>	Q ## ① ## ② 数均衡 业务配置向导  ④ 负载均衡 业务配置向导  ③ 防政&监听  ② SSL证书  ① RESSL证书U编程短的业务受知如常保护并得到权益机构的身份认证  ③ 透露的证书 1	费用 工单 备案 3 后端服务器	<ul> <li>企业 支持与服务 □ ↓ 〒</li> <li>④ 健康检查</li> </ul>	⑦         品         能体中文         ⑩           ①         監听介紹           5         配置审核
<ul> <li>○)阿里云</li> <li>久税均衡 SLB</li> <li>成法</li> <li>交例</li> <li>文例管理</li> <li>回收站</li> <li>证书管理</li> <li>访问控制</li> </ul>	Q ## 文載功者 SLB / 文載均衡业务和置向导 全 负载均衡业务配置向导 ② \$SL证书 ① RX型SAULEHU编程的加紧要到加密值中并得到形成能机构的身份认证 * 选择服务器证书 1 请选择	表用 工单 會室 3 后端服务器 ^ C 新建服务器任	<ul> <li>企业 支持与服务 E ▲ 平</li> <li>4 健康检查</li> <li>8</li> <li>8</li> <li>9</li> <li>9</li> <li>7</li> <li>8</li> <li>7</li> <li>8</li> <li>7</li> <li>8</li> <li>7</li> <li>8</li> <li>7</li> <li>8</li> <li>7</li> <li>8</li> <li>8</li> <li>9</li> <li>8</li> <li>9</li> <li>9<!--</td--><td>⑦     合     简体中文     ④       ⑦     监听介绍       3     配置审核</td></li></ul>	⑦     合     简体中文     ④       ⑦     监听介绍       3     配置审核
この時間では、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいいでは、またいでは、またいいいでは、またいいいいでは、またいいいいでは、またいいいいでは、またいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいい	Q 注意 负载均衡 5LB : 负载均衡 边务配置向导 <	表用 工単 敏変 ③ 后硫酸劣器 へ C 新建販売器は1	<ul> <li>企业 支持与服务 □ ① ↓</li> <li>4 健康检查</li> <li>8 购买证书</li> </ul>	⑦     合     節体中文     ④       ①     監听介绍
<ul> <li>         ・         ・         ・</li></ul>	Q ##	表用 工単 触玄 3 后端服务器	企业 支持与服务 □ ↓ 〒 4 健康检查  8 购买证书	⑦     合     節体中文     ②       ⑦     盈新介绍       5     配置审核
この時間には、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいでは、またいいでは、またいいいでは、またいいいいは、またいいいいは、またいいいいは、またいいいいは、またいいいいは、またいいいいは、またいいいいは、またいいいいは、またいいいいいは、またいいいいは、またいいいいは、またいいいいは、またいいいいは、またいいいいは、またいいいいいいいいいい	Q ##	表用 工单 新玄 3 后端服务器	<ul> <li>企业 支持与服务 □ ↓ 〒</li> <li>4 健康检查</li> <li>8 购买证书</li> </ul>	<ul> <li> <ul> <li></li></ul></li></ul>
<ul> <li>         への理要な         <ul> <li>                  への理事な                  </li> <li>                        への理事な</li></ul></li></ul>	Q ##	週用 工単 無玄 ③ 后端服务器 ④ C 新建服务器は1 2	企业 支持与服务 D 介 P 4 健康检查 8 购买证书	<ul> <li></li></ul>
た) 阿里云   久雄坊街 SLB   久雄坊街 SLB   気いていたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいたい	Q EE	表用 工単 留案       3     后端服务器         4     C         1     C         2	企业 支持与服务 口 () 下       4       4       6       第       約天正书	<ul> <li>● 益 陈体中文 ●</li> <li>● 盒新介紹</li> <li>● 盒新介紹</li> <li>● ③ 盒新介紹</li> <li>● ③ 盒新介紹</li> <li>● ③ 盒新介紹</li> <li>● ④ 盒新介紹</li> </ul>
た) 阿里云   久様均衡 SLB   風な   気がのです。   のなな   日本若理   日本若理   日本若理   日本若理    日本若理   日本若理    日本若理   日本若理    日本若理   日本若理    日本若理   日本若理    日本若理   日本若理    日本若理   日本若理    日本若理   日本若理    日本若理   日本若理    日本若理   日本若理    日本若理   日本若理    日本若理    日本若理    日本古生	C III SARAWA SU MUMAUANA ANA ANA ANA ANA ANA ANA ANA ANA AN	表用 工単 敏玄 ③ 后端服务器 2	<ul> <li>企业 支持与服务 □ ▲ 〒</li> <li>④ 健康检查</li> <li>6 限天正书</li> </ul>	<ul> <li></li></ul>
た) 阿里云   久健均衡 SLB   低流   次例管理   回次站   回次站   日本常現   日本常見   日本の   日本の <	Q ##	表用 工单 新玄 ③ 后端服务器 2	<ul> <li>企业 支持与服务 □ ↓ 〒</li> <li>4 健康检查</li> <li>8 购买证书</li> </ul>	⑦       品       簡体中文       ②         ⑦       魚新介州         ⑤       配置申板

依次完成: 后端服务器-健康检查-配置审核等操作

# 3.6.14 腾讯云证书配置

1、进入 SSL 证书管理页面 https://console.cloud.tencent.com/ssl

	网络蜂蛇 田													•
SSL证书	证书列表	全部項目 ▼												
首 操作记录			1、由于CARU 城),之前已	5和证书代理南策略 反发的证书在有效规	调整,从2018年1月1 内使用不受影响(注:	日起。同一主城最多只能) 即将到期的证书需要184	■遺20张亚洲城信品牌免费量 ■1月1日以后重新申遺时、会	DV版SSL证书(一级域名及其行 研到上述简略的限制)。 若您却	- 城名均属于同一主城。 业务因此次调整受限。	例如 domain.com。ssl 建议您购买乏城名型SSI	domain.com, ssl.ssl.domain.com 迂市 pa	却属于同一主		
			2、证书申请成	助之后可以直接下	版到本地。									
			购买证书	申请免费证书	上伸连带	更多操作					E书ID / 翻注名 / 週用名称	Q		
			ID		通用名称	证书类型	200813161 +	所规项目	关联云资源	状态	操作			
							证书列表为	空,您可以 申请证书或 <mark>上修证</mark>	6					
			已选0项,共0	坝										
5 京成													2 11	A 6

2、点击上传证书按钮,输入证书,私钥证书,点击确认完成证书上传。

上传证书	×							
上传后腾讯云将保管您第三方申请的SSL证书,安全可靠。								
证书 a+OUGIUCE2Qnc4av1tqu2ZYJ450WaCg2YrIS/MDKKOeYnobtuKKIW9CKt v6LCH+z NGq2wvxSEFqN5ljcl5/LRb/FU5PtInm9QjqwIPnZbNs32i7YWvkG0CjI2C aR+bbx A+IW3PFch5b5jb5aEHsYMs3SD8yvCtyZXs2Snw9XoA== END CERTIFICATE								
请输入证书内容(包含证书链) あまたのでのでは、 DTXWTQKBgAMtCwwwYkyJNVVe3CNTSCKCUKX2aDX58HTH7YK2BM0yJt /7X093yG8A tY/CM0AktC68DCOMN6uiXIJASkmKamdQUhe73XVt2tYgQXg9T6XJRe XgRGgD6LFu KQ0fKfak0YlshR/8Zfzvtx51q5Rha1YXR2Ry1bR4sMW/ZP159qug END RSA PRIVATE KEY								
所属项目 式 🗐 🐨 🐨 🐨 🐨 🐨 🐨 🐨 🐨 🐨 🐨 🐨 🐨 🐨								

证书:证书公钥,即 CFCA 邮件中:单位名称.cer 文件内容

证书私钥: 生成 csr 时产生的 key 文件。如果有密码,需要去除密码后上传
pem 文件。如果是 jks 或者 pdf 文件,见本文档 3.5 章节证书格式转化。

3、选择证书,点击更多根据需求部署到对应网站即可

	- 网络新盒 田										岛 天±我才。	展用▼	IM 🖻 🖲 ()
SSL证书	证书列表 🚽	全部项目 🔻											
128 延书管理 121 遍作记录		1、由于C 划)。之/ 2、证书#	A机构和证书代理商策略 約已統发的证书在有效期 1週成功之后可以重接下!	8调整,从2018年1月1日結 約内使用不受影响(注:即 账到本地。	8、同一主城最多只能中请2 特到期的证书需要18年1月1	「米亚洲城信品牌免费型DV版 日以后重新申请时,会受到」	SSL证书(一级域 送策略的限制)。	名及其子城名均種于同一主城,例內 若切的业务因此次调整受限,建议	」domain.com。ssl.d 思想英王城名型SSL词	lomain.com, ssi.s E15 🖸	isl.domain.com 新耀子	词一主	
		9255E-15	申请免费证书	LHE	更多操作				Ξ.	书ID / 新注名 / 通F	888	Q	
		ID		週用名称	证书类型	到期时间 \$	所腹项目	关联云资置	秋念	操作			
		- *3	096 85 /		CFCA OV OCA(24F)		目家以獲	Æ	上传托器	THE	當地 洋輝 更多 分配至灰目 都看到風内CON 都看到魚肉的香 重除		
		근용 6 제. :	共1项							<b>与</b> 克里示行	20 - 1		
Ξ  ▷ 完成										-		Ģ	∂ द⊪ ⊞ ⊚∘ ⊕
			X		FK	E Contraction of the second se							
×	X												

# 附录一、CFCA 全球信任证书(SSL证书)申 请表

# 申请表

		CFC	A 全球	信任服务器	证书申讨	青表		
	申请日期			证书数量		证书期限		
	业务类型			□新申请	□更新	口吊销		
1		0.000	□单域名⊂	Ⅳ服务器证书	□通配符OV	服务器证书		
]	证书类型	<u>о</u> үштэ	□多域名(	DV服务器证书				
		EVST #	□单域名E	V服务器证书				
		сvµ: р	□多域名	EV服务器证书				
证书	域 名							
申请信息		<b>注:</b> 1、多域名证: 2、通配符证: 3、IP类型只序 4、该处直接:	: . 多域名证书.默认以CSR中填写的域名为证书主域名.其他作为备用域名 、通配符证书.适用以*开头的域名.例如*.domain.com 、IP类型只限于申请公网IP.且只可申请OV单域名或者多域名(多个IP)证书 、该处直接填写域名即可.不需要添加http://或者https://					
	域名验证方式	□邮箱验证	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●				盖章文件)	
		1、采用邮箱 护. 我方无法 、postmaster 常回复邮件后 2、采用DNS 值或文件CFC	:* 、采用邮箱验证方式时,请确保whois隐私保护关闭,whois中管理员邮箱可用(若开启隐私保 4、我方无法查询明确的管理员邮箱,则默认向admin、administrator、webmaster、hostmaster postmaster开头的域名邮箱发送验证邮件,例如admin@domain.com形式,请确认上述邮箱可正 问复邮件后,再选择此种验证方式) 、采用DNS或文件验证方式时,需要域名管理员在域名解析服务商处的域名管理系统操作,记录 该文件CFCA会发送至本表格中经办人邮箱,按照邮件提示操作					
	申请企业/机构信息区(以下信息全部填写,不可留白)							
机	机构名称 (中文全称)							
构	和构证件类型	□企业营业は	照□组织	和构代码证 ■其它。	请注明:	统社会信用(	भिरुद	
信	机构证件号码		the manage	V(13)(x)µ ■ (C)	HALM	联系电话	(**)	
	联系地址					邮政编码		
由语	姓名		职务		电子邮件	10 - 10 - 10 - 10 - 10 - 10 - 10 - 10 -		
经办人	证件类型		证件号		联系电话			
由请	姓名		职务		电子邮件			
确认人	证件类型		证件号		联系电话			
申	本人/机构授权/ 同意遵守中金金 球信任体系电子	本表格中经办ノ 融认证中心有 认证业务规则	小理证书 限公司(C (CPS))	申请相关事宜.并承 FCA) 网站(http://v 》中规定的相关义务	诺以上信息资 vww.cfca.com [;] 。	料真实、有效。 cn)发布的《数等	本人/机构已认真阅读并 字证书服务协议》、《全	
声明	申请机构盖章					日期		
~~	备注							
<b>申请材料</b> 1、申请求 2、CSR(0 3、机构证 4、经办盖公 5、公四时请 6、如申请	<b>说明:</b> (加盖企业公章 SBR中信息精要与 (件复印件 身份证复印件 "证明國(仅当以 "证明國(仅当以 (BU证书,精要额	或带有公司名 同申请表中一致 若选择邮箱、 公网IP申请时 外提供律师函	称字样的部 、CSR生成 DNS或者文 需要,运営 、律师证	门公章) * 地址: https://ss 牛验证方式,此文件 商出具的加盖公章的	l.cfca.com.。 不需要提供) 约公网IP分配;	cn/Web/tool) 正明文件)	*	

# 附录二、CFCA 域名验证方式

目前 CFCA 支持邮箱验证、DNS 验证、文件验证及域名证书(盖章)四种域 名验证方式,本文介绍常用四种方法。

**注意事项:** 域名验证记录值有效期为 48 小时,自生成时开始计算。请务必在 48 小时内完成配置,如超时未进行配置或验证未通过,请联系赛尔网络工作人员,重新申请域名验证记录值并配置。

### 方法一: DNS 验证

下文介绍 SSL 证书 DNS 验证在各主流域名注册商下的域名解析方法,仅供参考,具体以各注册商实际为准。赛尔网络会将 DNS 记录值发送到证书申请经办人邮箱,请留意查收。

### DNS 验证注意事项:

当申请的域名不为主域名(如: domain.com),为二级域名时(如: www.domain.com),主机记录值需更新为:"_cfcachallenge.host.二级域名前缀",

### 即: _cfcachallenge.host.www

#### 阿里云操作示例:

(1)登陆域名管理控制台,查看【域名列表】,单击操作栏的【解析】,进入域名解析页面:

[-] 城名控制台	× +				- Ø ×
$\leftrightarrow$ $\rightarrow$ C $\cong$ dc.com	nsole.aliyun.com/next/index#/domain/list/all-dor	nain			☆ 💌 🖯 😆 🗄
☰ (-) 阿里云		Q 搜索文档、控制台、API、	解决方案和资源 费用 售后 f	略案 企业 支持 官网 🖸	4' 17 🕐 🖄 🍎
域名服务	城名列表 进入城名解析列表>>				② 域名简介
城名列表	♂您可能感兴趣的域名	O 换一换	查看更多 📅 城名资讯		
信息模板	rz.com bz.com ob.com 21.com 3w.com zfz.com cyq. klg.com zjy.com qfw.com ymb.com	com hfd.com czr.com htj.com	wjb.com 【共战疫情】全程在线,公 【爆品推荐】热门优选商标	公司/个体商户注册仅¥9.9,商标注册提; 示,海量资源库,即买即用	货券270元/张起
批量操作	全部域名 急需续费域名 急需赎回域名	3 未实名认证域名 预登	纪域名	导出列表	查看导出结果 域名分組管理
域名转入	wf2、 180 ) 180 0 出行曲击 wf2米刑, 今年	↓ 捕乞分組・ ☆照			
邮箱验证	到期日期: 辺 -	() <u>投來</u> 高级搜	\$		
操作记录					
我的下载	域名	类型 ⑦     域名状态	域名分组 注册日期 🜲	到期日期 🔷	操作
安全锁管理	david 14 E. com gTL	D 正常	未分组 2019-06-28 18.04.15	2020 05 26 16 34:15 #	壊 解析 安全锁◎   备注   管理

(2) 单击【添加记录】

<ul> <li>域名控制台</li> </ul>	× C- 云解析 DNS	× +									-	٥	×
$\leftarrow$ $\rightarrow$ C $$ dns.consol	e.aliyun.com/?spm=5176.100	251.111252.22.720	14f15hX8eXh#/dns	/setting/david" = 🗥	com						<u>ک</u>	6 0	) :
	资源 ▼	C	<b>)</b> 搜索文档、控制台、A	PI、解决方案和资源	费用	售后 备案	企业	支持 官网	Þ. (	) <b>.</b> Ä	0	简体	0
域名解析	云解析DNS / 域名解析 / 解析	设置						采购季用	则大促:新用	]户年付7折,	老用户纳	爽费越长起	自优准
解析设置	← 解析设置 •	lavid 📪 📭	.com								⑦ 如	何设置解	析?
DNS安全	未查询到域名DNS服务器	信息,请检查DNS服务器	设置或域名实名认证相关	展开									
权重配置													
自定义线路	添加记录 导入/导出	请求量统计新引	印导			全部记录 🗸	精确搜	素> 输入	关键字		۹ 1	級搜索	,
解析日志	主机记录 \$	记录关型 🗘 🧌 艏	析线路(isp) 💲	记录值	TTL	状态 备注	ŧ		操作				
	©	A B	5A	172.136.23.160	10 分钟	正常			修改	暫停   删	除 備〉	±	
	1 暂停 启用	删除 更换分	组						共1条	< 1	>	10 条/页	

### (3) 添加记录类型为 TXT 的 DNS 记录,单击【确定】完成添加

(3)称加尼	永尖望入 IXI	的 DNS に求, 毕击 【 确 足 】 元 成 祢 加	
▶ 城名控制台	× C 云解析 DNS	× +	- 0 ×
$\leftrightarrow$ $\rightarrow$ C $($ and dns.console	e.aliyun.com/?spm=5176.100251.1	11252.22.72014f15hX8eXh#/dns/setting/david1203.com	☆ 💌 \varTheta :
	资源 🔻	Q 遊览文档、拉射台、API、解决方面和资源 费用 售后 智囊企业 支持 首同 🖸	4° 🗑 🗑 🖄 🌀
域名解析	云解析DNS / 域名解析 / 解析设置	采购季税时大促:	新用户年付7折,老用户续费越长越优质
解析设置	← 解析设 添加记录	×	⑦ 如何设置解析?
DNS安全 权重配置	记录类型:	记录关重: TXT. こ本长度限制512, 通常做SPF记录(反垃圾邮件) ∨	
自定义线路 主机记:	录:	マ 輸入失墜字 土机记録・ rfachallanas hot	Q、 高级搜索 ▼
解析日志cfcac	hallenge.host		if F
		解析线路: 默认 - 必填! 未匹配到智能解析线路时, 返回 [默认] 线路设 > ⑦	改   暫停   删除   备注
记录值: 2020011755300261ex/NBw	YAj0JOSr	◆ 記录値: 2020011755300261±w/\LEw/\LEw/\LEvC9:06:GeC931g/TqC PmMS9m	条 < 1 > 10 条/页 >
		• TTL: 10 9th V	
		段浦 角定	<b>E</b>

### 腾讯云操作示例:

(1) 登陆域名管理控制台, 查看【我的域名】, 单击操作栏的【解析】, 进入 域名解析页面:

分 我的域名	× +			- 0 >	×
$\leftrightarrow$ $\rightarrow$ C $\cong$ console.c	loud.tencent.com/domain			☆) 💌   😝	:
	网站备案 王		o ci	9 ₁₂ sunny_ <b>_==</b> com マ 费用マ 工単 ⊠ ¹¹² () (?	Ð
<b>域名管</b> 理 《	我的域名			进入域名解析列表 📀 手机管理域名 🛄 描引	Â
我的域名	全部域名 即将到期 #	需续费 急需赎回 未实名	3认证 待转入		J
域名信息模板	r 垂葉通知1				
域名转入	- 现接相关注册局通知,域名注册后必须	王规定时间内完成城名实名认证,否则会被注册	册局暂停解析(Serverhold),无法正常访问。查	至吞洋情	
	注册域名 转入域名 批量排	fe <i>▼</i>		清榆入您要搜索的域名 Q	
	域名	服务状态 ()	注册时间	≠ 操作	
	ladovedsomcom.cn	正常	2016-06-01 21/23416-01	续费 解析 管理 更多 ▼	

(2) 单击【添加记录】

🔗 我的域名	× 🔗 解析管理	× +						– ø ×
$\leftrightarrow$ $\rightarrow$ C $$ console.c	cloud.tencent.com/cns/det	ail/belovedson.com.	cn/records					☆ 💌 \varTheta :
於 購 示 → 第	☆デ品 ~ │ 网站备案 +				Ø 12	▶ <mark>12</mark> 帮助 工单	é × 裁用 × 🧕	sunny_byl@l 26.com ∽
DNS 解析 DNSPod 《	belovedson.com	n.cn 全部项目 ▼						品手机管理域名
域名解析列表	记录管理 负载均衡	新 解析量统计	域名设置	自定义线路 线路分组				
付费套餐管理	添加记录 快速添加网	1站/邮箱解析 智停	开启 劃除	分配至项目			请逾	入您要搜索的记录 Q
的作士或名	主机记录	记录类型 ▼	线路类型	记录值	MX优先级	TTL (秒)	最后操作时间	操作
	@	A	默认	162.136.23.185	-	600	2020-02-02 1747-20	修改 智停 删除
	www	А	默认	123.56.110.100		600	2019-11-20 15:42:56	修改 智序 删 🤥

### (3) 添加记录类型为 TXT 的 DNS 记录,单击【保存】完成添加

公 我的域名 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	< <u> 公</u> 解析管理 × +	- 0 ×
$\leftrightarrow$ $\rightarrow$ C $$ console.cloud	I.tencent.com/cns/detail/belovedson.com.cn/records	☆) 😢   😆 🗄
	◇ │ 网站备案 +	5只 🕜 🖻 🎦 希助 工单 × 表用 × 🐧 sunny_bookev126.com ×
DNS解析 DNSPod 《 🔶	- beluvedison.com.cn 全部项目 -	BI 手机管理域名
域名解析列表	记录管理 负载均衡 解析量统计 域名设置 自定义线路 线路分	组
付券套餐管理	<b>添加记录 快速添加网站/邮箱解析</b> 暂停 开启 翻除 分配至项目	请输入您要搜索的记录 Q
1271 〒 1 282 44	主机记录 记录类型 ▼ 线路类型 记录值	MX优先级 TTL (秒) 最后操作时间 操作
	_cfcachaller TXT %% 2020011755300261e.	د · . 600 ·
	U         U         U           主机记录:         记录类型:         记录值:         记录值:           _cfcachallenge.host         TXT         2020011755300261ex/hDwwAJd005m	W122C5e0Hdhd7q0PmW59m36DQsZ4=

### 新网操作示例:

将记录类型选择为 TXT 纪录,在主机记录中输入邮件中提供的主机记录字段 信息,不包括网址信息,在记录值中输入邮件中的记录值字段**信息,点击添加** 

选择TXT记	₹ 1	输入s	sl证书验证时提供的记	录值	
记录类型	主机记录	记录值	MX优先级	ΠL	操作
请选择 ▼ 请选择			-	10分钟 🔻	添加
A记录 NS记录 CNAME记录	<b>记录类型说明:</b> ◆A记录:将域名指向一个IPv4地址(	例如:10.10.10.10),需要增加A记录			不可修改
MX记录 TXT记录	<ul> <li>NSIC家:或名解析服务都已录,如:</li> <li>◆CNAME记录:如果将域名指向一个</li> <li>◆MX记录:建立电子邮箱服务,将指</li> </ul>	来要将于观名指定吴小观名服务翻来解 V域名,实现与被指向域名相同的访问效 i向邮件服务器地址,需要设置MX记录	的,需要增加CNAME记录 效果,需要增加CNAME记录		不可修改
	◆TXT记录 : 可任意填写 ( 可为空 ) ,	通常用做SPF记录(反垃圾邮件)使用			
1 温馨提示:					
◆1、添加记 ◆2 占丰 "	录操作完成后新网的DNS服务器是立刻 关闭/开户解析" 操作后新网的DNS服务	生效的,但全球DNS刷新需要8-72小时 3.22公钟生效。但全球DNS刷新需要	扩生效; 18-72小时生效,		
*3、关闭解	所:将改变DNS解析的服务置于休眠状态	态,使其暂时停止服务,此界面中设置	的记录将不在生效;		
	后,可该关闭的DNIC钢板带新设入体用				

# 方法二: 文件验证

选择文件方式验证后,赛尔网络会发送记录值至证书申请经办人邮箱:

### 操作步骤

1、创建文件:

本地创建名称为"cfcafileauth.txt"的TXT文件,将邮件中"文件内容"字段,

X

复制到上述文件,保存(请不要增加空格等其他多余信息);

2、创建目录:

在站点根目录下创建/.well-known/pki-validation 子目录, 然后将 cfcafileauth.txt 文件上传至该目录;

注:

(1) 第一层目录是带点的隐藏目录, Windows 下命令为: mkdir .well-known Microsoft Windows [版本 10.0.17134.1099] (c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\thinkpad>cd C:\inetpub\wwwroot

C:\inetpub\wwwroot>mkdir .well-known

(2) 如果您的站点由于某种原因无法创建隐藏目录,请选择 DNS 验证方式

#### 3、域名解析至服务器

#### 4、 配置检测:

配置好之后,可通过浏览器访问地址,如正常输出配置的记录值,则表示配 置成功。

(1) HTTP 配置检测: http://您的域名/.well-known/pki-validation/cfcafileauth.txt

(2)HTTPS 配置检测:https://您的域名/.well-known/pki-validation/cfcafileauth.txt

若申请*.domain.com 类型的通配符证书时,访问检测地址为:

(1) HTTP 配置检测: http://domain.com/.well-known/pki-validation/cfcafileauth.txt

(2) HTTPS 配置检测: https://domain.com/.well-known/pki-validation/cfcafileauth.txt 注意事项:

(1) HTTP、HTTPS 任选其一验证通过即可, HTTP 方式需使用 80 端口, HTTPS 方式需使用 443 端口;

(2) 文件验证需要直接响应 200 状态码和文件内容,不支持任何形式的跳转。

### 方法三: 邮箱验证

邮箱验证,即通过 Whois 查询域名注册时预留的邮箱,赛尔网络向该注册邮箱发送 SSL 证书申请确认信息,若赛尔网络收到确认邮件,则可证明该邮箱被合法持有人控制,验证通过后可为其颁发服务器证书。

采用邮箱验证方式时,请确保 whois 隐私保护关闭,whois 中管理员邮箱可 正常回复邮件(若开启隐私保护,我方无法查询明确的管理员邮箱,则默认向 admin、administrator、webmaster、hostmaster、postmaster 开头的域名邮箱发送 验证邮件,例如 admin@domain.com 形式,请确认上述邮箱可正常回复邮件后, 再选择此种验证方式。

### Whois 邮箱查询地址:

https://www.whois.com/whois/



## 方法四: 盖章的域名证书

如上述几种方式均不能验证,可以向 CFCA 提供注册域名时,域名注册机构 发放的域名证书(提供盖章的电子版即可),CFCA 核实域名证书中信息与实际 申请信息一致后,也可发放对应域名的服务器证书。

# 附录三、CFCA 全球信任根证书获取方式

#### Windows Vista、Windows 7

Windows Vista 以及更高版本的操作系统,Windows 通过根证书自动更新机制分发 CFCA 全球信任根证书。即,用户访问含有 CFCA 全球信任证书的网站、读取含有 CFCA 全球信任证书的安全电子邮件、执行含有 CFCA 全球信任证书代码 签名的 ActiveX 控件及可执行程序时,Windows 证书链验证程序访问 Microsoft 根证书信任列表,自动下载 CFCA 全球信任根证书,并将其安装在用户 Windows 受信任根证书颁发机构存储区。整个过程自动完成,用户不会看到任何安全性对话框或警告。有关 Windows Vista、Windows 7 根证书更新的详细技术信息,请访问以下网站:

http://technet.microsoft.com/en-us/library/cc749331(WS.10).aspx

#### Windows XP

Windows XP 含有更新根证书组件(控制面板——添加或删除程序——添加/ 删除 Windows 组件),当用户访问含有 CFCA 全球信任证书的网站、读取含有 CFCA 全球信任证书的安全电子邮件、执行含有 CFCA 全球信任证书代码签名的 ActiveX 控件及可执行程序时,更新根证书组件将联系的微软 Windows Update 站 点检查根证书信任列表,自动下载 CFCA 全球信任根证书,并将其安装在用户 Windows 受信任根证书颁发机构存储区。有关 Windows XP 根证书更新的详细技 术信息,请访问以下网站:

http://technet.microsoft.com/en-us/library/bb457160.aspx

#### Firefox 浏览器

CFCA EV 根证书已经内置在 Firefox 浏览器中,包括 Windows、Linux、Mac OS X、Andriod 等平台。用户升级到 Firefox v38.0 及以上版本,即可获取 CFCA EV 根证书。

# 附录四、CFCA 全球信任证书链

CFCA 全球服务器证书体系如下:



主题: CN = CFCA EV ROOT

O = China Financial Certification Authority

C = CN

序列号: 18 4a cc d6

有效期: 2012 年 8 月 8 日 11:07:01 — 2029 年 12 月 31 日 11:07:01

摘要算法: SHA256

密钥长度: RSA(4096Bits)

----BEGIN CERTIFICATE----

MIIF jTCCA3WgAwIBAgIEGErM1 jANBgkqhkiG9w0BAQsFADBWMQswCQYDVQQGEwJD T jEwMC4GA1UECgwnQ2hpbmEgRm1uYW5 jaWFsIEN1cnRpZm1 jYXRpb24gQXV0aG9y aXR5MRUwEwYDVQQDDAxDRkNBIEVWIFJPT1QwHhcNMTIw0DA4MDMwNzAxWhcNMjkx M jMxMDMwNzAxW jBWMQswCQYDVQQGEwJDT jEwMC4GA1UECgwnQ2hpbmEgRm1uYW5 j aWFsIEN1cnRpZm1 jYXRpb24gQXV0aG9yaXR5MRUwEwYDVQQDDAxDRkNBIEVWIFJP T1QwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDXXWvNED8fBVnVBU03 sQ7smCu0FR36k0sXgiFxEFLXUWRwFsJVaU20FW2fvwwbwuCjZ9YMrM8irq93VCpL T1pTUnrD7i7es3E1we1dPe6hL6P3KjzJIx1qqx2hp/Hz7KDVRM8Vz3IvHW0X6Jn5 /Z0kVIBMUtRSqy5J35DNuF++P96hyk0g1CXohC1Tt7GIH//62pCfCqktQT+x8Rgp 7hZZLDRJGqgG16iI0gNyejLi6mhNbiyWZXvKWfry4t3uMCz7zEasxGPrb382KzRz EpR/38wmnvFyXVB1WY9ps4deMm/DGIq11Y+wejfeWkU7xzbh72fR0d0XW3NiGUgt hxwG+3SYIE1z8AXSG7Ggo7cbcN0Iab1a1 j j0Ytw1i3i/+0h+uFzJ1U9fpy25IGvP a931DfSCt/SyZi4QKPaXWnuWFo8BGS1sbn85WAZkgwGDg8NNkt0yxoekN+kWzqot aK8KgWU6cMGbrU1tVMoqLUuFG70A5nBFDWteNfB/07ic5ARwiRI1k9oKmSJgamNg TnYGmE69g60dWIolhdLHZR4tjsbftsbhf4oEIRUpdPA+nJCdDC7xij5aqgwJHsfV PKPt18MeNPo4+QgO48BdK4PRVmrJtqhUUy54Mmc9gn900PvhtgVguXDbjgv5E1hv cWAQUhC5wUEJ73IfZzF4/5YFjQIDAQABo2MwYTAfBgNVHSMEGDAWgBTj/i39KNAL tbq2osS/BqoFjJP7LzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAd BgNVHQ4EFgQU4/4t/SjQC7W6tqLEvwaqBYyT+y8wDQYJKoZIhvcNAQELBQADggIB ACXGumvrh8vegjmWPfBEp2uEcwPenStPuiB/vHiyz5ewG5zz13ku9Ui20vsXiObT ej/tUxPQ4i9qecsAIyjmHjdXNYmEwnZPNDatZ8POQQaIxffu2Bq41gt/UP+TqhdL jOztUmCypAbqTuvOaxn96/Ua4CUqmtzHQTb3yHQFhDmVOdYLO6Qn+gjYXB74BGBS ESgoA//vU2YApUo0FmZ8/Qmkrp5nGm9BC2sGE5uPhnEFtC+NiWYzKXZUmhH4J/qy P5Hgzg0b8zAarb8iXRvTvyUFTeGSGn+ZnzxEk8rUQE1sgIfXBDrDM111D1b4pd19 xIsNER9Tyx6yF7Zod1rg1MvIB6710i60N7fQAUtDKXeM0ZePg1r4UeWJoBjnaH9d Ci77oOcOPaYjesYBx4/IXr9tgFa+iiS6M+qf4TIRnvHST4D2GOCv0J4RUH1zEhLN 5mydLIhyPDCBBpEi61mt2hkuIsKNuYyH4Ga8cyNfIWRjgEj1oDwYPZTISEEdQLpe /v5WOaHIz16eGWRGENoXkbcFgKyLmZJ956LYBws2J+dIeWCKw9cTXPhyQN9Ky8+Z AAoACxGV21ZFA4gKn2fQ1XmxqI1AbQ3CekD6819kR5LLU7m7Wc5P/dAVUwHY3+vZ 5nbv0C070615s9UCKc2Jo5YPSjXnTkLAdc0Hz+Ys63su

-----END CERTIFICATE-----

主题: CN = CFCA EV OCA

O = China Financial Certification Authority C = CN

序列号: 00 b4 cf 94 32 66

有效期: 2012 年 8 月 8 日 14:06:31——2029 年 12 月 29 日 14:06:31

摘要算法: SHA256

密钥长度: RSA (2048Bits)

-----BEGIN CERTIFICATE-----

MIIFT jCCAzagAwIBAgIGALTP1DJmMA0GCSqGSIb3DQEBCwUAMFYxCzAJBgNVBAYT AkNOMTAwLgYDVQQKDCdDaG1uYSBGaW5hbmNpYWwgQ2VydG1maWNhdG1vbiBBdXRo b3JpdHkxFTATBgNVBAMMDENGQ0EgRVYgUk9PVDAeFw0xMjA4MDgwNjA2MzFaFw0y OTEyMjkwNjA2MzFaMFUxCzAJBgNVBAYTAkNOMTAwLgYDVQQKDCdDaG1uYSBGaW5h bmNpYWwgQ2VydG1maWNhdG1vbiBBdXRob3JpdHkxFDASBgNVBAMMCONGQ0EgRVYg TONBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAO20MsGFxFQIPMKVP oRaO9rHNX41xbq8jhnbdKOMDVbxfGa3b8QTKxMcmx1R1ULfsaieOcI1aR10AUcJP QH9ftekzh4T287xqsEAydYQHf77arWQ5nY3fR9RcoBq9pTCQbqw49S6/jHA5oPQa EoKbF0G8zfVKp5PrcKSufHMQyKo/Ez2UYT+gut36j4GYpAABuV6PbusPpjufsN9B r9+xqgyz8ubSp1W11qS1vQUQBhAJAH+a3NMhD0i11aGfTdWbF485a5Ni1MFGqJBa /kLVEYwG4aoKdV9vG/NFS0LKz3QVnB7bkrLjTkuGN/zQJP0daJ3CGAzmN+Cr2ujt XOfAYwIDAQABo4IBITCCAROwOAYIKwYBBQUHAQEELDAqMCgGCCsGAQUFBzABhhxo dHRwOi8vb2NzcC5jZmNhLmNvbS5jbi9vY3NwMB8GA1UdIwQYMBaAFOP+Lf0oOAu1 uraixL8GqgWMk/svMA8GA1UdEwEB/wQFMAMBAf8wRAYDVR0gBD0w0zA5BgRVHSAA MDEwLwYIKwYBBQUHAgEWI2hOdHA6Ly93d3cuY2ZjYS5jb2OuY24vdXMvdXMtMTIu aHRtMDoGA1UdHwQzMDEwL6AtoCuGKWh0dHA6Ly9jcmwuY2ZjYS5jb20uY24vZXZy Y2EvU1NBL2NybDEuY3JsMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUVQji3MyV bR9d3rNH60kWxsBFd8QwDQYJKoZIhvcNAQELBQADggIBAMmFEIoCE9UNmb2BYYhT RV12kNVucP6t683BaFTgJizIJw/ebvvTdWNTycyP5MQF1HKrIYwjvF09Rfw8+yIs sT3JFYiqsLBswvaMr3AIuA2mTnmasvZFe6P19qitzTRkz+TL6TFailrtnzudsvn2 SeVbRiX+6CsyNNMoPsRHTeZAEpkB7J3vh+ZAiv3gsIXtjtz5Y1iWWRZipemJ/qEf W2hDONB+T61GcEXHDi9dIkWcC/jFT4XPM64pagAz9gEGZg1PzFBE8QMxiwaDAOea G010e/HW4wJ1o4Zz0ELqZGJL1YhQ8AkBYR95NEtR9j5bWK98Lznyk1dk2MDLBD2m rIfMkVjMwEj4A8E1MXsLnWXXg41NN6gjUm2/IudKOaGqniPs5SZrN36O4B3NzsaZ dLznHH5H0+aksurjgme8RAG0A20AnRG3VXBWrxud7t0KDINLs+mxY7IR+xVZ2cw6 Cer8HnAVfKPJrbdq7vyJJkIpC11+mLHaGgvv3IqiU4rrr11E3NYjKG4Fk2MiYvZg 10KXA8t1YsLt8I/RcNmC2TvjZHYVE3tanbGw53TRGFk2Vq68X0kvoo0ardihwRkg qcOgUvouORuvSqT1kQizTFH6FTUt3xuuED4dnn5N/1ijcDt0N315ovoyH0VcYiO4 drCN96LHiUoiSfY0DmpXG2t1

主题: CN = CFCA OV OCA

O = China Financial Certification Authority

C = CN

序列号: 00 f9 df 6a df f5 64 be a6 8b 82

有效期: 2015 年 3 月 25 日 10:02:56——2029 年 12 月 25 日 10:02:56

摘要算法: SHA256

密钥长度: RSA (2048Bits)

----BEGIN CERTIFICATE-----

MIIFfDCCA2SgAwIBAgILAPnfat/1ZL6mi4IwDQYJKoZIhvcNAQELBQAwVjELMAkG A1UEBhMCQ04xMDAuBgNVBAoMJ0NoaW5hIEZpbmFuY21hbCBDZXJ0aWZpY2F0aW9u IEF1dGhvcm10eTEVMBMGA1UEAwwMQ0ZDQSBFViBST09UMB4XDTE1MDMyNTAyMDI1 N1oXDTI5MTIyNTAyMDI1N1owVTELMAkGA1UEBhMCQ04xMDAuBgNVBAoMJ0NoaW5h IEZpbmFuY21hbCBDZXJ0aWZpY2F0aW9uIEF1dGhvcm10eTEUMBIGA1UEAwwLQ0ZD QSBPViBPQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDn14xTy0bH zkaeyACeq6ryfxxG5zZT1fCL41mw7sk6SVmOKNfE60Gf7W6orksrFVIbIMK+VrYp +aYyhScq8EJT9xXBgXK2HqtpaDGOec1spJvcs+rXn9t1T789NBp3i5U+nLE9M1bR CHSx3Hzu8p7Aeq11ou+8nZ2egaVbWFL1zC1JENupSSI9Yjbefhb06y/TVxQ0x4Zt zwPwLcd8NUtSruIdo1xPbhQeCZNJMPq1GKMxhd5pDwY4mCKxDeraqhTNXui9Aef3 qyi2Ic9EXmdNPARkZJU2XTJ9FJ+DE+ChaIvfJ/VwQfMOeG1Bn/SAaav54jBmRnec PeD6YfpuiJ8vAgMBAAGjggFKMIIBRjA4BggrBgEFBQcBAQQsMCowKAYIKwYBBQUH MAGGHGhOdHA6Ly9vY3NwLmNmY2EuY29tLmNuL29jc3AwHwYDVR0jBBgwFoAU4/4t /SjQC7W6tqLEvwaqBYyT+y8wDwYDVR0TAQH/BAUwAwEB/zBEBgNVHSAEPTA7MDkG BFUdIAAwMTAvBggrBgEFBQcCARYjaHROcDovL3d3dy5jZmNhLmNvbS5jbi91cy91 cy0xMi5odG0w0gYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL2NybC5jZmNhLmNvbS5j bi91dnJjYS9SU0EvY3JsMS5jcmwwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBRm s+/7VJWH6ay111au5n3t0tBD0TAnBgNVHSUEIDAeBggrBgEFBQcDAgYIKwYBBQUH AwQGCCsGAQUFBwMBMA0GCSqGSIb3DQEBCwUAA4ICAQDKER8qcBmZG0G8G0J670VW OSg3UovOoc7/xz2mE+enyEcSwn/OQrL8C5DSA6nMvBMrCWEytYPofGQUXTwt1u78 GLxYNn3A/RtzczJ+/BXIhoe3aOT4tQ+2s9vrFRfIXs4CkmqHhfYSvArokdayYmBd 78psIwS5LCUzGKSn7y8UmAgoxiy7RtrVt5c1wvJyeuYk1Z118MN1szPrmAb4HS/D qnB+0qdhFGvfOyv71g6/w1IAkN84cH1KNC3JvyFHaCIAyhTPgjUayUvBKFK7XwN9 utIX12L3IZX7zfxGS/J9+ZeNwyb1QKmd/MKydJu9Ak6+ZMLLgj1CFkihJIn9Ur8M 2KQigz7YPDVIJj0tS71j0QVGh88LPUnQ1fBY7RwagficS/xc1IOnaXhoyWzg7EcQ /T1/O4FkpMqKuOreaI5NExjAT8cKizyY2wcO0XKIYri3Ewnbm+00IaYYaiQRGUR6 pzFFKxdFMbStCtI40bN+A9tB7cnBCW4vz3sAJd/OgmLF38XTa+/km3c1nQ0fhCGs 6kx2heN/DgFAc+P71dObo/kgGQtR6tr02gyXCFWnLMtT0+CoNOYOo3T+LbEqYeKL W7p29G9sgHgoqLFibWNMSKG1QvevkhjUMOD/g48f/nMSYsbU++yEaLvjvRHbb5ON IPkcE28TRhQQKmDKI+DRIg==

-----END CERTIFICATE-----

# 附录五、SHA 摘要算法介绍

安全哈希算法(Secure Hash Algorithm)主要适用于数字签名标准 (Digital Signature Standard DSS)里面定义的数字签名算法(Digital Signature Algorithm DSA)。 对于长度小于 2^64 位的消息,产生一个消息摘要。消息摘要可以用来验证数据 的完整性。

SHA 家族的五个算法,分别是 SHA-1、SHA-224、SHA-256、SHA-384,和 SHA-512,后四者并称为 SHA-2。支持 SHA2 的操作系统包括:Windows 8.1、Windows 8、Windows 7、Windows Server 2012 R2、Windows Server 2012、Windows Server 2008 R2、Windows Server 2008、Windows Vista、Windows Server 2003 R2、Windows 2003 Server SP2、32 位 Windows XP SP3、64 位 Windows XP SP2。

由于 SHA1 摘要算法存在杂凑冲撞攻击,随着计算机运算能力越来越强,其 安全性受到越来越严重的威胁。微软、谷歌等陆续发布了弃用 SHA1 摘要算法的 时间表。微软方面,要求 CA 机构 2016 年之后不能再签发新的 SHA1 摘要算法的 SSL 站点证书。2017 年之后,Windows Vista、Windows Server 2008 及以上版本操 作系统将无法访问 SHA1 摘要算法 SSL 证书的网站。谷歌方面,Chrome 浏览器将 对 SHA1 摘要算法 SSL 证书的站点提示安全警告。



# 附录六、常见问题

### 1、CFCA 全球信任 SSL 证书支持的操作系统和浏览器

Windows 平台浏览器 100%支持,包括但不限于: Internet Explorer、Google Chrome、Mozilla Firefox、Opera,以及 360、搜狗、遨游、QQ、UC、猎豹、百度 等国产浏览器;

Windows Phone 平台浏览器 100%支持;

Andriod (Android 6.0 Marshmallow) 平台 100%支持;

Linux 平台浏览器 100%支持;

Mac OS(10.12.1 及更新版本)平台浏览器 100%支持,包括但不限于: Safari、

Google Chrome、Mozilla Firefox 等;

浏览器	Internet	Mozilla	Google	Apple
操作系统	Explorer	Firefox	Chrome	Safari
Windows	$\checkmark$		$\checkmark$	
Unix/Linux		*	$\checkmark$	
Mac OS		1	$\checkmark$	$\checkmark$
10.12.1 及更	X			
新版本	XY			
iOS 10.1 及更		$\checkmark$	$\checkmark$	$\checkmark$
新版本				
Andriod 6.0		$\checkmark$	$\checkmark$	
Marshmallow				
Windows	$\checkmark$	~	$\checkmark$	
Phone				

IOS(10.1 及更新版本)平台浏览器 100%支持;

√:表示该浏览器完全支持 CFCA 全球信任 SSL 证书;

×; 表示该浏览器不完全支持 CFCA 全球信任 SSL 证书,当浏览器访问含有 CFCA 全球信任 SSL 证书的网站时,会有不受信任提示;

一一: 表示该浏览器不支持此操作系统。

### 2、Windows XP SP2 操作系统使用 CFCA EV SSL 证书

CFCA EV SSL 证书采用 SHA256 摘要算法,而 Windows XP SP2 操作系统并不 支持该算法。在 Windows XP SP2 操作系统中,使用 IE 浏览器无法访问含有 CFCA EV SSL 证书的网站(包括使用其他 CA 机构 SHA256 摘要算法 SSL 证书的网站)。 可以将操作系统升级到 Windows XP SP3 及以上版本,即可正常访问。

此外,火狐(Firefox)、谷歌(Chrome)等浏览器不依赖操作系统,浏览器本身支持 SHA256 摘要算法。因而可以在 Windows XP SP2 操作系统上使用这些浏览器访问含有 CFCA EV SSL 证书的网站。

### 3、通过 HTTPS 访问,页面弹出警告"是否只查看安全传送的网页内

## 容"

当网页包括经加密传送的 HTTPS 内容和未经加密传送的 HTTP 内容时, IE 会 弹出警告询问用户是否允许接受未经加密的内容。

安全警告	×
<b>是否只查看安全传送的阿页内容?</b> 此网页包含的内容将不使用安全的 HTT 页的安全。	TPS 连接传送,可能危及到整个网
详细信息 (M)	<u>是(1)</u> 否(1)
只显示安全内容。  有何风险(W)?	显示所有内容(S)
可以在"工具"——"Internet 选项"-	——"安全"——"自定义级别"-

- "显示混合内容"设置为"启用",即可不再弹出该提示。

一般来说,当 HTTPS 页面引用外部 HTTP 链接时,会提示此内容不安全。可 以通过 Firefox 的 Web 控制台,或者 Chrome 的 JavaScript 控制台查看到具体的报 错代码行,并可以参考相关提示修改页面代码。



## 4、部署 CFCA 站点认证标识

办理 CFCA EV SSL 证书、CFCA OV SSL 证书的网站均可以在其网站页面上嵌入 CFCA 站点认证标识,用户点击该标识,可以跳转到 CFCA 站点认证页面,CFCA 将 对网站的相关信息予以认证说明,增强网站的可信度。

部署 CFCA 站点认证标识,需将站点认证图标和以下链接嵌入网站页面上。



<u>https://evwebverify.cfca.com.cn/WebVerify/webVerifyServlet?domain</u>=网站域名

注意:1、网站域名必须为完整的域名,如:www.cfca.com.cn

2、该 URL 和图标必须放在对应域名的页面上,如果 URL 中的域名和网页的 域名不一致则会认证失败;

3、如果网站既有 https 页面,也有 http 页面,则 https 页面嵌入的 URL 为 "https://",http 页面嵌入的 URL 为 "http://"。

5、Chrome、Firefox 提示"SSL 收到了一个弱临时 Diffie-Hellman 密钥"

全连接失败

连接 webverify.cfca.com.cn 时发生错误。 在服务器密钥交换握手信息中 SSL 收到了一个弱临时 Diffie-Hellman 密钥。 (错误码: ssl error weak server ephemeral dh key)

• 您尝试查看的页面无法显示,因为已收到数据的可靠性无法证实。

• 请联系网站的所有者,告知他们这个问题。

重试

回报此错误 -

Chrome、Firefox 等最新版本的浏览器,对客户端浏览器和网站服务器之间的 密钥算法有较高要求,不允许客户端浏览器和网站服务器之间使用相对较弱的密 钥算法。该问题需要调整 Web 应用服务器的相关配置,限定客户端浏览器和网 站服务器之间使用较高强度的密钥。

常用的 Web 应用服务器配置密钥算法的方式如下:

Apache:

在 httpd-ssl.conf 配置文件中增加如下内容:

SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:IaNULL:IENULL:IEXPORT:IDES:IRC4:IMD5:IPSK:IaECDH:IEDH-DSS-DES-CBC3-SHA:IEDH-RSA-DES-CBC3-SHA:IKRB5-DES-CBC3-SHA

Nginx:

在 conf/nginx.conf 配置文件中增加如下内容:

SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:IaNULL:IeNULL:IEXPORT:IDES:IRC4:IMD5:IPSK:IaECDH:IEDH-DSS-DES-CBC3-SHA:IEDH-RSA-DES-CBC3-SHA:IKRB5-DES-CBC3-SHA Tomcat:

在 conf/server.xml 配置文件中增加如下内容:

<Connector

ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_ WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_ SHA256,TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_1 28_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_SHA256,TLS_ECDHE_RSA_WITH_AE S_128_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_SHA,TLS_ECDHE_RSA_WITH_AES_2 56_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_SHA384,TLS_ECDHE_RSA_WITH_AE S_256_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_SHA384,TLS_ECDHE_RSA_WITH_AE S_256_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_SHA,TLS_DHE_RSA_WITH_AES_128 SHA256,TLS_DHE_RSA_WITH_AES_128_SHA,TLS_DHE_DSS_WITH_AES_128_SHA255 6,TLS_DHE_RSA_WITH_AES_256_SHA256,TLS_DHE_DSS_WITH_AES_256_SHA,TLS_D HE_RSA_WITH_AES_256_SHA" />

# 6. 客户反馈下载的服务器公钥证书总是在导入 jks 文件的时候报错 无法安装认证回复

- ▶ 确认 JKS 文件是否是当初生成 CSR 文件的证书文件
- ▶ 确认证书链是否已经导入:注意要先后导入根证书、中级证书
- > 确认证书链是否与公钥证书的证书路径一致
- ▶ 如是不相符的证书文件,只能重新办理,即重新产生 CSR 并且补发证书

# 7. pfx 导入 jks 出现如下问题"No key pairs present in KeyStore "

] Alias	Last Modified
Import Key Pair	×
Select a key pair for import:	
No key pairs present in KeyStore Algorithm:	cate Details
Import Canc	el

问题原因:造成此问题的原因是 pfx 出现问题,在 keytool 工具打开 pfx 文件

时,现象如图

<b>₿</b> Ĩ K	eyTool GUI - [C:\temp\22222222.pfx]	
<u>F</u> ile	<u>T</u> ools <u>H</u> elp	
	Alias	Last Modified
<u> </u>	serverssl	
1	serverssl	
Kev	Store Type: PKCS #12. Size: 2 entries	
1.103		

如果 pfx 文件正常,那么 keytool 工具打开时,效果如下图:

<pre>KeyTool GUI = [C:\temp\server.pfx]</pre>				
<u>File Tools Help</u>				
1 Alias	Last Modified			
serverss!				
KeyStore Type: PKCS #12, Size: 1 entry				

造成 pfx 出现上面另种情况的原因在于, ie 中看到的友好名称:

<b>1</b> 211日 1月11日 1月111日 1月111日 1月111日 1月111日 1月11111 1月1111111 1月11111 1月11111111				×
発売甘田田白気(N1)・ 【∠66歳	=>			-
	∃∕			<u> </u>
│ 个人 │其他人│中级证	书颁发机构 受信任的根	证书颁发机构	↓ 受信任的发布	者・
	(	1		
	颁发者	截止日期	友好名称	
🔄 *. com. cn	CFCA TEST OCA1	2020/1	〈无〉	
🔄 🔄 01101051986090	CFCA OCA1	2019/1/18	011010519860.	
<b>EQ</b> 041@0111111111	CFCA Operation CA2	2016/1	〈无〉	
<b>EQ</b> 041@1111111111	CFCA TEST CA	2017/6/15	〈无〉	
<b>1</b> 041@8200812250	CFCA TEST CA	2017/6/25	测试预植V2	
🟹 041@Z20090615@	CFCA Operation CA2	2015/9/11	〈无〉	
🕎 1. 1. 2. 1	CFCA TEST OCA1	2016/2/9	serverssl	
🔄 🔄 BOCtestra30_admin	BOC	2017/10/6	〈无〉	
IIICECACECA技术部20	CECA OCA1	2019/8/1	〈无〉	
- 导入(0)   导出(0)	.   删除(R)		5	高级(A)
┌证书的预期目的				
客户端身份验证,服务器身份验证				
			音響	≦(V)
了解证书的详细信息			÷	关闭(C)

解决方法:删除友好名称

1. 双击证书, 查看详细信息:

	a Internet 属性	<u>?</u> ×
	29. 业书 	×
	常规 详细信息 证书路径	
	显示 (S): <mark>&lt;所有&gt;</mark> ▼	
	字段         值           節版本         V3           節序列号         10 02 51 92 26           登名算法         shalRSA           登名官法         shal           節发者         CFCA TEST 0CA1, China F           節放射从         2015年11月9日 14:34:00           算到         2016年2月9日 14:34:00	
		5)
2 占井		2 2 2
		? X
	友好名称 (P): 「 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 1 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 田 1 1 1 1 1 1 1 1 1	
		(A)

3. 将友好名称删除

X

)证书				ĺ
☆期目的 (約): 【<所	有>		Y	<u>▼</u> 
个人  其他人 中级证	书颁发机构   受信任的相	。证书颁发机构	1 受信任的发布者	╡╵╹╹
颁发给	颁发者	截止日期	友好名称	
🔄 *. com. cn	CFCA TEST OCA1	2020/1	〈无〉	
🔄 🔄 01101051986090	CFCA OCA1	2019/1/18	011010519860	
041@0111111111	CFCA Operation CA2	2016/1	〈无〉	
041@11111111111	CFCA TEST CA	2017/6/15	〈无〉	
041@8200812250	CFCA TEST CA	2017/6/25	测试预植V2	
041@Z20090615@	CFCA Operation CA2	2015/9/11	〈无〉	
📊 1. 1. 2. 1	CFCA TEST OCA1	2016/2/9	〈无〉	
🛛 🔄 BOCtestra30_admin	BOC	2017/10/6	〈无〉	
IIICFCACFCA技术部20	CECA OCA1	2019/8/1	〈无〉	<u> </u>
导入(I)   与出(I).	删除(R)		高	级(A)
证书的预期目的				
				(V)
了解证书的详细信息			Ě	闭(C)

4. 之后再导出成 pfx。Jks 查看, pfx 文件正常:

<u>File Tools H</u> elp	
1 Alias	Last Modified
51E814AU-8D86-4278-B2DF-F43C6BD1C1F8	
<u> </u>	

5. 导入 jks 时可以正常选中密钥空间

KeyTool GVI - [C:\temp\serverssl.jks]		<u>- 🗆 ×</u>
1 Alias	Last Modified	
🔛 boc	2015-12-17 9:02:27	-
🖼 CfCa 🛛 🖬 Import Key Pair	× 8	
Image: cfca_cs_ca       Select a key pair for import:         Image: cfca_cs_cca       Select a key pair for import:	13	
Image: cita_ev_cod         (51E814A0-8D86-4278-B2DF-F43C6BD1C1F8)           Image: cita_ev_cod         Image: cita_ev_cod           Image: cita_ev_roo         Image: cita_ev_roo           Image: cita_ev_roo         Image: cita_ev_roo		
Image: cfca_gt_oca         Image: cfca_oca1         Image: cfca_oca2	.1 i2 i0	=
cfca_operari	ails 3	
🖼 cfca_ct_oca	2015-12-17 9:06:45	
📴 cfca_rsa_test_oca21	2015-12-17 9:07:15	
cfca_test_ca cfca_test_cs_ca	2015-12-17 9:07:35 2015-12-17 9:07:53	-
KeyStore Type: JKS, Size: 25 entries		

客户反馈证书配置正确,依旧提出证书不可信。建议客户对服务器进行抓包,确认服务器是否将中级证书和根证书发到客户端。经常发生的情况是客户的网关或者防火墙将中级证书和根证书屏蔽导致。

# 附录七、销售服务渠道和联系人

服务网站: HTTPS://SSL.CERNET.COM

联系电话:

010-62603952(用户支持) 010-62603854(证书咨询)

工作时间:

法定工作日 8:30-17:30 (紧急联系电话: 13552939468)

E-mail: <u>ssl@cernet.com</u>

高校用户可以联系赛尔网络有限公司各省分公司