

服务器证书安装配置指南

IIS6.0

二〇二一年一月



# 目 录

1. 生成证书请求	. 2
1.1 生成证书请求文件(CSR)	. 2
1.2 提交证书请求	5
2. 安装中级CA 证书	. 5
2.1 获取中级CA 证书	5
2.2 配置中级CA证书	5
3. 安装服务器证书	8
3.1获取服务器证书	8
3.2 进入IIS 控制台	8
4. 服务器证书的备份及恢复1	LO
4.1 服务器证书的备份	10
4.2 服务器证书的恢复	11



## 服务器证书安装配置指南(IIS6.0)

### 1. 生成证书请求

#### 1.1 生成证书请求文件(CSR)

进入IIS 管理控制台,选择需要配置证书的站点,右键选择"属性"➡"目录安全性"

- 「人住」 操作	HTTP 头 自定义结误 ASP NET	그버즈
← → 💽 🗟 🖡	网站 IEAPI 筛选器 主日录 文档 日录完全性	
¥)Internet 信息 □ _ 网站 교 ゐ 默认网i	<ul> <li>         匿名访问和身份验证控制          允许匿名访问资源及编辑身份验证万          法。</li></ul>	
	IP 地址和域名限制 使用 IP 地址或 Internet 域名授权或 拒绝对资源的访问。	
	编辑 (I) 安全通信	
	访问资源时,要求安全通信并启用客 户证书。 	
<b>«</b>		

"服务器证书" ➡"新建证书"





为证书输入名称,并设置服务器证书密钥对位长。服务器证书要求密钥位长2048。

IIS 计书向导 🛛 🗙
名称和安全性设置 新证书必须具有名称和特定的位长。
输入新证书的名称。此名称应易于引用和记忆。 名称(M):
默认网站密钥的位长决定了证书的加密程度。位长越长,安全性越高。然而,位长过长
将使性能降低。 位长 00 · 2048
□服务器网关加密 (SGC)证书 (仅适用于导出版本) (S)
< 上一步 (B) 下一步 (B) > 取消

## 输入公司名称及部门信息。

IIS 证书向导 X
<b>单位信息</b> 证书必须包含您单位的相关信息,以便与其他单位的证书区分开。
选择或输入您的单位和部门名称。通常是指您的合法单位名称及部门名称。
如需详细信息,请参阅证书颁发机构的网站。
单位 (0):
GlobalSign China Co., Ltd
都门(1):
IT lept.
< 上一步 (B) (下一步 (B) 》 取消



115 证书向导 🛛 🛛 🛛 🛛
<b>站点公用名称</b> 站点公用名称是其完全合格的域名。
输入站点的公用名称。如果服务器位于 Internet 上,应使用有效的 DWS 名。如果服务器 位于 Intranet 上,可以使用计算机的 NetBIOS 名。
如果公用名称发生变化,则需要获取新正书。
公用名称 (C):
cn.globalsign.com
<上→步(2) 下→步(2) > 取消

## 输入公司所在地国家、地区信息

115 证书启导	×
<b>地理信息</b> 证书颁发机构要求下列地理信息。	
国家 (地区) (C) : CNF (中国)	
Shanghai	<b>~</b>
市县 (L):	
Shanghai	<b>~</b>
省/自治区和市基必须是完整的官方名称,且不能包含缩写.	
<上一步(1) (丁 <del>二</del> 步(1) (入	取消



#### 导出证书请求文件

IIS 证书向导 🛛 🗙
<b>证书请求文件名</b> 以指定的文件名将证书请求保存为文本文件。
输入证书请求的文件名。
文件名 (E):
c:\certreq.txt [浏览(图)
<上一步®)下一步®)> 取消

### 1.2 提交证书请求

将证书请求文件certreq.txt 提交给我们,等待证书签发。

## 2. 安装中级CA 证书

#### 2.1 获取中级CA 证书

为保障服务器证书在IE7 以下客户端的兼容性,服务器证书需要安装两张中级CA证书(即中级证书和 交叉证书)。从邮件中获取中级证书和交叉证书:将证书签发邮件中的从BEGIN 到 END 结束的两张 中级CA 证书内容(包括"-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE-----")分 别粘贴到记事本等文本编辑器中,并修改文件扩展名,保存为intermediate1.cer 和 intermediate2.cer文件。

#### 2.2 配置中级CA证书

点击开始菜单,在"运行"中输入"mmc",打开控制台窗口。



警 控制台1		
文件(2) 操作(2) 査者(2) 収縮(共(2)) 窗の	口 (4) 希助 (4)	
		_
· 論 控制台根节点		
	此视图中没有可显示的项目。	

点击"文件➡添加删除管理单元"

漆加/圖除管理单元 ? 🗙
独立 扩展
使用此页来添加或删除控制台的管理单元。
管理单元添加到 (2): 💼 控制台根节点 🔽 💼
点击"添加"
<b>添加①</b> 删除 ®) 关于 ®)
确定 取消



选择"证书",然后点击"添加":

漆加独立管理单元	? 🛛
可用的独立管理单元:	
管理单元	供应商 🔷
可移动存储管理	Microsoft Corpora
■ 设备管理器	Microsoft Corpora
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Microsoft Corpora
🔊 索引服务	Microsoft Corpora
(二) 文件夹	Microsoft Corpora
一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	Microsoft Corpora
國正书	Microsoft Corpora 📄
⑤ 組策略对象编辑器	Microsoft Corpora
④组件服务	Microsoft Corpora 🗸
· <mark>描述</mark> 证书管理单元允许您浏览自己的、·	一个服务的或一台计算机的证书
存储内容。	
	点击"添加"
	添加(A) 关闭(C)

证书管理单元 2010年1月1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1	×
该管理单元将始终为下列帐户管理证书: ○ 我的用户帐户 @) ○ 服务帐户 (S) ○ 計算和帐户 (C)	
< 上一步 (B) 下一步 (B) > 取消	]

选择"计算机帐户" ➡"本地计算机"



## 在添加的证书管理单元中,选择"证书" ➡"中级证书颁发机构" ➡"证书"

🎦 控制台1 - 【控制台根节点\证书(本地)	十算机) \中级证书颂发机构 \证书	1			
🌇 文件(E) 操作(a) 查看(E) 收藏夹(D)	窗口(12) 帮助(130)				_ 5 ×
□ 控制合根节点	御发给 /	御发者	対朝日朝	预期目的	研记的名称
<ul> <li>□ 控制台根节点</li> <li>□ 節 证书(本地计算机)</li> <li>□ ① 交信(在)的根证书顶发机构</li> <li>□ ① 交信(在)的根证书顶发机构</li> <li>□ □ ① 交信(在)的成行者</li> <li>□ ① 交信(在)的发行者</li> <li>□ ① 交信(在)の定行者</li> <li>□ ① 交信(在)</li> <li>□ ① SPC</li> </ul>	新世紀 イ 「日本日本日本 「日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本	初友老 Root SGC Authority Not SGC Authority Microsoft Eoot Authority Microsoft Eoot Authority Root SGC Authority Root SGC Authority Root SGC Authority Root SGC Authority Root SGC Authority Root SGC Authority Class 1 Public Primary Carti Class 2 Public Primary Carti	 近日月日日月 2014-1-23 2006-2-23 2002-12-31 2010-1-1 2010-1-1 2010-2-25 2017-2-10 2004-1-1 2009-10-16 2004-7-17 2019-6-24 2008-5-13 2004-1-7 2004-1-6	<u>33時目的</u> 1.3.6.1.4.1.311 1.3.6.1.4.1.311 代码差名、Yindo 現等器验证、1.3 代码差名、时间 (所有) 1.3.6.1.4.1.311 1.3.6.1.4.1.311 1.3.6.1.4.1.311 (所有) (所有) 2.18.840.1.1137	49.余余、余余、余余、余、余、余、余、余、余、余、余、余、余、余、余、余、余、余
	C				>
中级证书惯发机构 存储含有 15 个证书。					

空白处右键点"所有任务" ➡"导入",将服务器证书的两张中级CA证书intermediate1.cer

和intermediate2.cer 分别导入。

## 3. 安装服务器证书

#### 3.1 获取服务器证书

将证书签发邮件中的从BEGIN 到 END 结束的服务器证书内容 (包括 "-----BEGIN CERTIFICATE--

----"和"-----END CERTIFICATE-----")粘贴到记事本等文本编辑器中,并修改文件扩展名,保存

为server.cer 文件。

### 3.2 进入IIS 控制台

进入IIS 控制台,并选中需要配置服务器证书的站点,"属性"→"目录安全性"



	HTTP 头	自定义错误	ASP	. NET
Internet 信息服务 网站 I My 默认网站	阿站         ISAFI           匿名访问和身份验证指 允许匿名试 法。         九许匿名试 法。           IP 地址和域名限制         一           原用 IP 指绝对资源         拒绝对资源	师远器 王日求 空制 方问资源及编辑身份验证方 地址或 Internet 域名授权] 愿的访问。		
	安全通信 交全通信 一 一 ご 行 ご 书。	村,要求安全通信并启用客	编辑 ① <b>服务器证书 (</b> ) 查看证书 () 编辑 0).	
				TELL

选择"服务器证书" ➡"处理挂起的请求并安装证书"

IIS 证书向导 🛛 🔀
<b>挂起的证书请求</b> 挂起的证书请求是指证书颁发机构尚未响应的请求。
存在挂起的证书请求,如何处理?
●处理挂起的请求并安装证书 @)
○ 删除挂起的请求 @)
< 上一步 (B) 下一步 (B) >  取消



#### 选中您的服务器证书文件

IS 证书向导	
<b>处理挂起的请求</b> 通过检索包含证书颁发机构响应的	文件来处理挂起的证书请求。
输入包含证书颁发机构响应的文件的	的路径和名称。
路径和文件名(2):	
C:\server.cer	浏览(B)
	< 上一步 (B) 下一步 (B) > 取消

配置默认的https 访问端口443, 重启IIS 并使用https 方式访问测试站点证书安装。

#### 4. 服务器证书的备份及恢复

在您成功的安装和配置了服务器证书之后,请务必依据下面的操作流程,备份好您的服务器证书,以防

证书丢失给您带来不便。操作流程如下:

#### 4.1 服务器证书的备份

进入IIS 控制台,选择安装有服务器证书的站点,右键选择"属性" ➡"目录安全性" ➡"服务器证

书" ➡ "将当前站点证书导出到一个.pfx 文件"





#### 4.2 服务器证书的恢复

进入IIS 控制台,选择安装有服务器证书的站点,右键选择"属性" ➡"目录安全性" ➡"服务器证

书"➡"从.pfx 文件导入证书"

IIS 证书向导	×
<b>服务器证书</b> 以下是为网站分配证书的方法。	
选择此网站使用的方法:	
○ 新建证书 (C)。	
○ 分配现有证书(点)。	
○ 从密钥管理器备份文件导入证书 (2)。	
○ 从 .pfx 文件导入证书(图).	
○ 将远程服务器站点的证书复制或移动到此站点 (ឬ)。	
〈上一步(18) 下一步(18) 〉	取消

配置 https 默认访问端口 443, 重新安装中级 CA 证书文件, 重启 IIS 完成证书的恢复。

请注意,此文档会不定期更新!

GlobalSign China Co., Ltd

环玺信息科技 (上海)有限公司

2021年1月