

代码签名证书提取指南

更新日期: 2022-07-01

GlobalSign China Co., Ltd.

https://www.globalsign.cn Email: support-china@globalsign.com 电话: 021-61479027

第一部分: 普通型代码签名证书提取

本例介绍普通型代码证书提取过程, EV 增强型证书提取请参考下文第二部分。

(一) 提取证书

a.使用 Microsoft Edge 打开提取链接,提取链接在 Globalsign 邮件中,例如: <u>https://system.globalsign.com/pc/public/certificate/install.do?p=XXXXXXXXXXX</u> 输入提取密码:(提取密码咨询客服人员)

◎技术支持中心 学联系我们
安装证书
Importanti Before you begin:
 Please install the R3-R45 cross certificate in advance. Install the token driver: Safenet USB Driver. When using a Certificate Signing Request (CSR) for certificate pickup, make sure the Common Name in the CSR matches the requested Common Name for your order
Please enter the certificate pick-up password you set during the ordering process. If you've forgotten the contribute point on the contribute parameter, you must cancer and reporter. Or center your Administrator if the certificate was ordered for you.
ण्यम्भ
Globa/Sign China Co., Ltd.

b.输入提取密码,点击"下一步",弹出新页面,如下图所示

pts to Allow Certificate Ge wing the installation to proceed. Yo of, depending on security settings.	u may also be prompted to allow the installation	
tion.	Web 访问确认。	×
Token. Due to the large size of t	此网站正在尝试代表你执行数字证书操作。 https://system.globalsign.com/pc/public/certificate/install.do;jsessioni d=DAEE7F0C4D148A26015E4A1ADAD9974C 你应该只允许已知网站代表你执行数字证书操作。 是否要允许此操作?	
nent - Version 5.0 FULLY BEFORE USING THE CE PLVING FOR A CERTIFICATE, EMENT. IF YOU DO NOT AGRE THIN SEVEN (7) DAYS OF TH IF YOU HAVE PROBLEMS UNDE obalsign.com	是(Y) 否(N) YOU ARE AGREEING TO BE E TO THE TERMS OF THIS E AVAILABILITY OF THE RSTANDING THIS ELWEEN Global Sign and the]

In can take up to a minute, and it might seem like not much is happening. atient and don't use the browser back button or refresh the page.

□ 我同意接受此订购协议

c.点击"是",出现下图页面,选择加密提供商"Microsoft Enhanced Cryptographic Provider v1.0",点击"我同意接受订购协议",最后点击"下一步"

GlobalSign Certificate Center	× +			
\leftarrow \rightarrow C \bigcirc $ $ \bigcirc $ $	https://system.globalsign.com/pc/public/o	ertificate/install.do		
你正使用 Internet Explorer 模式。大多	数页面在 Microsoft Edge 中工作效果更佳。	在 Microsoft Edge 中打开	在工具栏中显示	
Pleas be a Enrol If so, uses or Po	e notel Depending on your browser / Operating nformation bar or Pop Up asking you to install * ment Control* displayed at the top of this page. you MUST allow this to run. It is a safe program to install your certificate. To run it, click on the in b Up and follow the instructions.	System setup, there may dicrosoft Certificate that your browser formation bar		
	加密服务提供商	eToken Base Cryptographic Microsoft Base Smart Card (Microsoft Enhanced Cryptog Microsoft Strong Cryptograp	Provider Crypto Provider graphic Provider v1.0	1选择加密服务提供商
	GlobalSign Subscriber Agreement - PLEASE READ THIS AGREEMENT CAREFU YOU OR YOUR ORGANIZATION. 5Y APEL BOUMD BY THE TERMS OF THIS AGREEM AGREEMENT, CANCEL YOUR ORDER WITH CERTIFICATE FOR A FULL REFUND. IF AGREEMENT, E-MAIL US AT legal@glo	Version 5.0 LLY BEFORE USING THE CERTIFIC TING FOR A CERTIFICATE, YOU & BORT. IF YOU DO NOT AGREE TO T IN SEVEN (7) DAYS OF THE AVAI YOU HAVE PROBLEMS UNDERSTAND Dalsign.com	CATE ISSUED TO RE AGREEING TO BE THE TERMS OF THIS ILABILITY OF THE NING THIS	
	This GlobalSign Subscriber Agreem Subscriber must use one of the following i GlobalSign recommends Subscribers use me 1. A Trusted Platform Module (TPM) that gen 2. A hardware crypto module with a unit desig 3. Another type of hardware storage token wi	ent (the "Agreement") between methods to generate and protect the thod 1 or 2 over method 3: erates and secures a key pair. In form factor certified as conforming to h a unit design form factor of SD Card	a GlobalSign and the ir Code Signing Certificate p at least FIPS 140 Level 2 or USB token (not recomme	Private Keys.
	请点击下一步并等待。这个过	☑ 我同意接受此订购协议 2公分 理可能需要几秒钟,请不要重复点击下- 下一步	选同意接受 -步,也不要关闭浏览器。 3点击下一步	
				GlobalSign China Co., Ltd.

d.出现安装证书页面,点击"安装我的证书"

安装证书 安装您的数字证书和中级CA证书 您的证书已经生成,请点击 安装我的证书按钮,将证书安装至您的电脑。 我们检测到您使用的是EC浏览器。 请点击 安装规约证书 按钮,安装正书和所有的 祖关的中级CA证书,以确保您的证书是可信的。	
安装您的数字证书和中级CA证书 您的证书已经生成,请点击 安装我的证书 按钮,将证书安装至您的电脑。 我们检测到您使用的是正浏览器。 请点击 安装我的证书 按钮,安装证书和所有的 相关的中级CA证书,以确保您的证书是可信的。	
您的证书已经生成,请点击 安装我的证书 按钮,将证书安装至您的电脑。 我们检测到您使用的是に浏览器。 请点击 安装我的证书 按钮,安装证书和所有的 相关的中级CA证书,以确保您的证书是可信的。	
我们检测到您使用的是正浏览器。 请点击 安装我的证书 按钮,安装证书和所有的 相关的中级CA证书,以确保您的证书是可信的。	
我们检测到您使用的是正浏览器。 请点击 安装我的证书 按钮,安装证书和所有的 相关的中级CA证书,以确保您的证书是可信的。	
安装我的证书 点击安装证书	

What to do next. Now you have your Certificate please review the Product Guide support pages for instructions on how to use your Certificate. Go to Product Guide pages

e.在弹出页面点击"是"

GMONTENET CACUP	安装证书 安装您的数字 您的证书已经生成 此用私正在實驗代集份执行数字证书操作。 https://system.globalsign.com/pc/public/certificate/install.do 位应该只允许已知同為代集份执行数字证书操作。 是百要为许规则作?	
	#0 第四	
	What to do next. Now your have your Certificate please review the Product Guide support pages for instructions on how	w to use your Certificate.

f.在弹出页面点击"确定",完成证书下载

GlobalSign.		1211 1211 1211 1211 1211 1211 1211 121
	安装证书	
	安装您的数字证书和中级CA证书	
	您的证书已经生成,请点击 安装我的证书报来自网页的满意 × 电脑。	
	史陵成功	
	点击 确定 等值用的变形 调效器。 书 提出、安装证书和所有的 以确保您的证书是可信的。	
	安装我的证书 0	
	What to do next.	
	Now you have your Certificate please review the Product Guide support pages for instructions on how to use Go to Product Guide pages	your Certificate.

(二) 导出证书

a.打开 Microsoft Edge 右上角三个点调出菜单,在"隐私、搜索和服务"中找到 "安全性",点击"管理证书",在"个人"中找到证书,选中后点击下方的 "导出"按钮。

$\leftarrow \rightarrow$	C C Edge edge://settings/p	privacy	ĩ0	£≡	Ē	
		合 你的组织前选择已托管				
设	王 探索(合)新	安全性 管理 Microsoft Edge 的安全设置				
8	个人资料隐私、搜索和服务	管理证书 管理 HTTPS/SSL 证书和论置				
- C) 外观 开始、主页和新建标签页	Microsoft Defender Smartscreen 使用 Microsoft Defender Smartscreen 帮助我抵急部遭网站和下载的强害				
¢	,共享、复制和谐贴 Cookie 和网站权限	阻止可能不需要的应用 眼止下気可能导致意外行为的结合贯展应用				
⊑ ⊈	, 默认浏览器 下载	打开站点安全服务,以获取有关你访问站点的详细信息 石记起此后中选择和出版说,允许Microsoft Edge 直接 Microsoft 必应,获取更多站在选员				
8 21	7 家庭安全 语言	使用安全的 DNS 指定如何查找网站的网络地址 取认该现下、Microsoft Edge 使用电压解的服务提供用。每用 DNS 提供自可能会导致系统站在形法的网。				
0 0	 アノドリカル 系統和性能 (第二) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1					
	手机和其他设备					
0	关于 Microsoft Edge	の対機器的安全機式是否與意? ろ Q				

证书						×
预期目的(N):	<所有>					~
个人 其他人 中间证	书颁发机构	受信任的根证书	颁发机构	受信任的发布者	未受信任的发布者	
颁发给	顶发者	截止日	友好名称			^
		2031/	<无>			
		2023/	<无>			
		2023/	<无>			
		2023/	<无>			
		2023/	<无>			
		2023/	<无>			
		2023/	<无>			
· · · · · · · · · · · · · · · · · · ·		2023/	<无>			
■ 环玺信息科技… (GlobalSign C	Co 2023/	环玺信息和	斗		
						~
导入(1) 長	≩出(E)	删除(R)			高级	(A)
证书的预期目的						
华田恢复						
化构立在					查看(V)	
					关闭	(C)

b.出现证书导出向导,点击"下一步"

~	F	证书导出向导	×
		欢迎使用证书导出向导	
		这个向导可帮助你将证书、证书信任列表和证书吊销列表从证书存储复制到磁盘。	
		由证书颁发机构颁发的证书是对你身份的确认,它包含用来保护数据或建立安全网络连接的信 息。证书存储是保存证书的系统区域。	
		单击"下一步"继续。	
		点击 下一步	
		下一步(N) 取消	

c.在新的页面选择"是,导出私钥",点击"下一步"

←	参 证书导出向导	×
	导出私钥 你可以选择将私钥和证书一起导出。	
	私钥受密码保护。如果要将私钥跟证书一起导出,你必须在后面一页上键入密码。	
	你想将私钥跟证书—起导出吗? ●是,导出私钥(Y) 〇 不,不要导出私钥(Q)	
	2,点击下一	步
	下一步(N) 取消	

d.在导出文件格式页面,选择"个人信息交换-PKCS12(PFX)",然后点击"下一步"

 \times

~	چ	证书导出向导
---	---	--------

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:

- DER 编码二进制 X.509 (.CER)(D)
- Base64 编码 X.509(.CER)(<u>S</u>)
- ○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(<u>A</u>)
 - ✓ 启用证书隐私(E)
- Microsoft 系列证书存储(.SST)(<u>T</u>)

下一页(<u>N</u>)	取消

e.在新的页面"安全",设置证书的密码,点击"下一步"

] 密码(₽): ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●			
确认密码(<u>C</u>): 设置密码	☐ 密码(₽):		
	确认密码(<u>C</u>):	设置密码	

加密:

Tri	p	eDES-SHA1	\sim	

下一页(<u>N</u>)	取消

f.为导出的签名证书文件选择路径和命名,点击"下一步""完成"以及"确定", 完成证书导出。

← 🏼 🐓 证书导出向导

正在完成证书导出向导

你已成功完成证书导出向导。		
你已指定下列设置:	证书导出向导 X	
文件名 C:\U 导出密钥 是 句括证书路径中的所有证书 是	导出成功。	ctop\test.pfx
文件格式 个人	确定	▲●●●● 点击 确定

第二部分: 增强型(EV)代码签名证书提取

a.安装 token 驱动(注意:安装驱动时 token 不要插在电脑里)

名称 ^	修改日期	类型	大小
📓 GlobalSign-Safenet-Authentication-Tools-Windows-x32-10.8-R2.zip	2021/5/28 15:58	WinRAR ZIP 压缩	9,983 KB
📴 GlobalSign-Safenet-Authentication-Tools-Windows-x64-10.8-R2.zip	2021/5/24 17:37	WinRAR ZIP 压缩	12,712 KB

b.插入 token, 驱动界面显示如下图所示则驱动识别成功

SafeNet Authentication Client Tools	ion Client	- · × - · · × - · · · · · · · · · · · · · · · · · · ·
SafeNet eToken 510x		重命名设备
	***	更改设备 密码
	-	解锁令牌
	\otimes	删除设备内容
	2	查看令牌信息
	<u> ا</u>	断开 SafeNet 虚拟令牌
T 4 9 3 15664005 5\1441 A 50\$66455 6 6 0 1 7 260 5 H		www.safenet-inc.com

GlobalSign.	
	安装证书
	Important! Before you begin:
	Please install the R3-R45 cross certificate in advance.
	Install the token driver:Safenet USB Driver.
	When using a Certificate Signing Request (CSR) for certificate pickup, make sure the Common Name in the CSR matches the requested Common Name for your order
	Please enter the certificate pick-up password you set during the ordering process.
	If you've forgotten the certificate perception of the certificate percepticate perception of the
	下一步
	GlobalSien China Co. 1.M

d.输入提取密码,点击"下一步",弹出新页面,如下图所示

GMOINTERNETCROUP	安装证书
	Step Two: Web 访问确认。 The CSP Is u 此用私正在實驗代表的執行数字证书操作。 We have lists 此用私正在實驗代表的執行数字证书操作。 Please notel 由太田/SSS120BCASB607278D2C8 Dease notel 检验读开始作已知同缺代表的執行数字证书操作。 Enrolment C 是言實於許證操作? Enrolment C 建訂該許證操作? Enrolment C 重宜的 Dran to instal 重宜的 Or Pop Up an 重位)
	Cryptographic Service Provider
	GlobalSign Subscriber Agreement - Version 3.9 PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT. CANCEL

e.点击"是"后,出现下图页面,选择加密提供商"eToken Base Cryptograhic Provider",点击"我同意接受订购协议",最后点击"下一步"

YOUR ORGANIZATION. BY APPLYING FOR A CERTIFICATE, YOU ARE AGREEING TO BE BOUND (1997) TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, CANCEL VOUR ORDER WITHIN SEVEN (7) DAYS OF THE AVAILABILITY OF THE CERTIFICATE FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT Legal@lobalsign.com This GlobalSign subscriber Agreement (the "Agreement") between GlobalSign and the Applicant or Subscriber Agreement (the "Agreement") between GlobalSign Certificate Private Keys. GlobalSign recommends Subscribers use method 1 or 2 over method 3: 1. A Trusted Platform Module (TFM) that generates and socures a key pair. 2. A hardware royto module with a unit design form factor of SD Card or USB token (not recommended) I A Trusted Platform Module (TFM) that generates and socures a key pair. 3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not recommended) I A Trusted Flatform bits is cyclider bits and methods to Card or USB token (not recommended) I A generates torage token with a unit design form factor of SD Card or USB token (not recommended) I Agne #generates is cyclider bits and socures a term of the tot of SD Card or USB token (not recommended) I Agne #generates is cyclider bits and socures a term of the tot of SD Card or USB token (not recommended) I Agne #generates is cyclider bits and factor of SD Card or USB token (not recommended) I Agne #generates is cyclider bits and factor of SD Card or USB token (not recommended) I Agne #generates is cyclider bits and factor of SD Card or USB token (not recommended) I Agne #generates is cyclider bits and factor of SD Card or USB token (not recommended) I Agne #generates is cyclider bits and the factor of SD Card or USB token (not recommended) I Agne #generates is cyclider bits and to cyclider	Cryptographic Service Provider	eToken Base Cryptographic Provider
Subscriber must use one of the following methods to generate and protect their Code Signing Certificate Private Keys. GlobalSign recommends Subscribers use method 1 or 2 over method 3: 1. A Trusted Platform Module (TPM) that generates and socures a key pair. 2. A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2 3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not recommended) ① 我同意接受此订购协议 读点由下一步并转得。这个过程可能需要几秒钟,请不要重复点击下一步,也不要关闭浏览器。 下一步 3. Addm T - 步升	YOUR ORGANIZATION. BY APPLYING TERMS OF THIS AGREEMENT. IF YOT YOUR ORDER WITHIN SEVEN (7) DAN REFUND. IF YOU HAVE PROBLEMS UN legal@globalsign.com This GlobalSign Subscriber Agre Applicant of Subscriber is eff Certificate (the "Effective Dat	FOR A CERTIFICATE, YOU ARE AGREEING TO BE BOUND THE J DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, CANCEL SO FT HE AVAILABLILTY OF THE CERTIFICATE FOR A FULL MDERSTANDING THIS AGREEMENT, E-MAIL US AT emennt (the "Agreement") between GlobalSign and the sctive as of the date of the application for the set of the state of the application for the
我同意接受此订购协议 2,3年同量接受订购协议 3,4击下一步 	Subscriber must use one of the followi GlobalSign recommends Subscribers use 1. A Trusted Platform Module (TPM) that 2. A hardware crypto module with a unit d 3. Another type of hardware storage toker	ng methods to generate and protect their Code Signing Certificate Private Keys. method 1 or 2 over method 3: generates and secures a key pair. esign form factor certified as conforming to at least FIPS 140 Level 2 with a unit design form factor of SD Card or USB token (not recommended)
	请点击下一步并够待。 这个	☑ 我同意接受此订购协议 2,急中周嘉兼受订购协议 2,总中周嘉兼受订购协议 2,总中周嘉兼受订购协议 3,点击下一步,也不要关闭浏览器。 下一步 3,点击下一步

弹出 token 密码框,输入 token 密码 Token 初始密码: 88888888 (如果已更改密码则输入更改后的密码) Token 初始密码不安全,需要重置密码强度 100% (8 位以上大小写加数字)

f.点击"安装我的证书"

GlobalSign.		●技术支持中心 ← 联系我们
	安装证书	
	安装您的数字证书和中级CA证书	
	您的证书已经生成,请点击 安装我的证书 按钮,将证书安装至您的电脑。	
	我们检测到您使用的是正测宽器。 请点击 安装我的证书 按钮,安装证书和所有的 相关的中级CA证书,以确保您的证书是可信的。 安装我的证书	- 点击安装证书
	What to do next. Now you have your Certificate please review the Product Guide support pages for instructions on how to use y Go to Product Guide pages	our Certificate.

g.在弹出页面点击"是"

安装证书	●技术支持中心 🛩联系我们
安装您的数字 Web 以问确认。 您的证书已经生成 此网站正在摆放代表你我行数字证书操作。 https://bystem.globalsign.com/pc/public/certificate/install.do 必须说行公许已知问站代表你我行数字证书操作。 登園預公许已知问站代表你我行数字证书操作。 第的 83。 夏田 夏田 夏田 <td></td>	
What to do next. Now you have your Certificate please review the Product Guide support pages for instructions on how to use y Go to Product Guide pages	our Certificate.

h.在弹出页面点击"确定",完成证书下载

GlobalSign.		●技术支持中心 ←联系我们
	安装证书	
	安装您的数字证书和中级CA证书 您的证书已经生成、请点击 安装我的证书提来自网页的消息 × 8.66.	
	安禄成功 生命 職室 少健服的冠毛別S 外健服の設证非是可信的。 安装現的证书 安装現的证书 全社職室 生命 大田、安装证书和所有的 以确保您的证书是可信的。 (1) (1) (1) (1) (1) (1) (1) (1)	
	What to do next. Now you have your Certificate please review the Product Guide support pages for instructions on how to use y Go to Product Guide pages	your Certificate.

注:提取链接只能提取一次,如果提取显示私钥不存在,且 token 中没有证书,请联系客服查询

i. Safenet 界面如下图所示即为提取成功

SafeNet Authentication Client Tools		-		×		
SafeNet		8 ##554 858 879 ##7554 878 79 ##755 46 8 50 56 6 # 5540 36 55 # 5540 36 55 # 75 40 55 #	5664UGS A55 6 H	997765 05\16413 6+021W5		
SafeNet Authentication Client		۵۵ 🕲	1 ?	æ		
SafeNet Authentication Client Tools) 1					
∽ 👷 SafeNet eToken 510x	领发给	领发机构为	失效	目的		
> 151 用户业书 > 153 CA 证书	■环玺数字签名测	GlobalSign CodeSigning CA - G3 - Staging	9-No	代		
> - Ē 孤立对象 莽 设置 豫 客户端设置	100	and the second	21-5	ÿ		
< >	<			>		
3 15664U6S15\16415 A 6 50\$66A55 6 6 4 01 5 7 26D 5 H R 5F4 F 1						

此外,还需要手动导入中级证书,询问销售或者联系技术获取中级证书文件, 操作如下图所示:

SafeNet Authentication Client Tools		—	×
SafeNet Authe	ntication Clie	тнлц nt 🛯 🕸 💁 🛔 ?	ES
	或者点击这个图标		
feNet Authentication Client Tools 设备 梁 <u>Gl</u> obalSign eToken		GlobalSign eToken	^
	设备类别	硬件	
▶ ⊷ 신품	读卡器名称 原刊品(DVCC+11)	SafeNet Token JC 0	
客户端设置	序列亏 (FKLS#11) 剩今穴词 (aining continuted)	AU21UU486U754EBA	
PLA PROVIDE	深川天王円 (minimum estimated) Cord TD (CHTD)	0v-74800003C1R1107874800003C1R11078	
	24F4 ID (60ID) 立只夕狩	aTakap 5110 CC (940)	
	上来刑	TDPrime	
	Applet Version	IDPrime Tava Applet 4, 4, 2, A	
	撤码版本	G286	
	设备密码	存在	
	设备密码的剩余重试次数	5	
	最大设备密码重试次数	5	
	设备密码失效	未失效	
	管理员密码	存在	
	管理员密码重试剩余次数	5	
	最大管理员密码重试次数	5	
	FIPS	N/A	~
< >	< compared with the second sec		>
		thalesgroup.co	om

如有任何问题或疑问请直接与我们联系,谢谢! 邮箱: <u>support-china@globalsign.com</u>