证书下载及导出流程

1. 证书下载流程

登入 CFCA 中国金融认证中心官网网址: <u>http://www.cfca.com.cn/</u>, 点击"证书自助"-"相关下载",

			访问旧版业	务相关 🕤 快速	通道 🕤 输入 🕯	长键词	0	内容检索
CFCA 中国金融认证中心 China Financial Certification Authority	首页	产品介绍	解决方案	信息安全	证书自助	服务支持	SSL证书	旗下品牌
					相关下载			
					体验平台			
CFCA		0.00						

 在生产证书下载选项中点击 → "证书下载" - "生产系统证书下载" - "新证书下 载平台(生产证书)";

	相关下载	★请在下载证书前务必阅读: <u>【C</u>] ★请各位客户在下载前阅读" <u>证书</u>] 了您能够正常下载和使用CFCA谈 补丁- <u>IE密钥长度补工</u>
证书体验平台	▶ 证书下载 生产系统证书下载 测试系统证书下载 新证书下载平台(独试证书)

3. 首次下载证书,请按照页面提示安装相应程序,以保证证书顺利下载;【如果安装控件有任何问题,请联系 cfca 官网的客服咨询。】

CFC ▲ 数字证书下	「载平台	用户证书下载	Web服务器证书下载	证书换发	证书查询	CRL下载	Ì
	你的安全我们来守护			_		下载控件	中文
	CFCA数字证书下载平台		>				
证书序》	尊敬的网上用户: 您的本机控件未安装,不具备下载证书所必需的条件, 件:点击下载控件->保存控件到本地->运行该控件->员 下载控件	请继续按照下面的; 则新本页面。	操作安装数字证书下载控				
选择。	ar - Iniciosofe base cryptographic r torrider +10	下載		1			(

4. 如果出现协议提示,请"接受此协议";

(本协议包含CFCA的免责条款,请认真阅读,尤其是粗体字内容)

尊敬的网上用户:

中金金融认证中心有限公司(即中国金融认证中心,简称"CFCA")是经国家有关管理机关审批 设立的电子认证服务机构,作为权威的第三方安全认证机构,通过数字证书注册机构(以下简称"RA")向网上用户(以下简称"订户")发放数字证书,为订户网上交易提供信息安全保障。 Ε

订户在申请使用CFCA签发的数字证书之前,应先阅读并同意"CFCA数字证书服务协议"(以下简称"本协议")。本协议构成订户与中金金融认证中心有限公司之间的权利义务约定,若不同意本协议 全部或部分条款,请勿申请使用CFCA数字证书。订户一旦完成CFCA数字证书的下载或初次使用, 即表明同意接受并愿意遵守本协议的所有条款。

一、证书订户的权利和义务

1、订户应遵循诚实、信用原则,在向RA申请数字证书时,应当提供其真实、完整、准确的信息和资料,并在这些信息、资料发生改变时及时通知原RA。如因订户故意或过失提供的资料不真实、不完整、不准确或资料改变后未及时通知CFCA或原RA,造成的损失由订户自己承担。

2、在通过RA的审核、信息注册后,订户即可获得数字证书的下载凭证,订户应妥善保管下载 凭证,亲自用该凭证从相关网站将数字证书下载在安全的容器里;订户也可以委托或授权他人通过其 他安全的方式获得数字证书。订户获得的下载凭证为一次性使用,有效期为14天。如果在14天内没

下载此协议	接受此协议
-------	-------

 输入 CFCA 提供的两码:证书序列号(也就是业务邮件里的参考号) & 授权码(也 就是业务邮件里的授权码)

【注:正式入网签约后,业务会发正式入网参数信息通知邮件给商户。用户参考号、用 户授权码是入网通知邮件里提供的。】

制证方式默认,软件 CSP 选择最后一项软证书,(注:CSP 选错是会报错的)。点击下 载。

CFCA)数字证书下载平	四台	用户证书下载	Web服务器证书下载	证书换发	证书查询 CRL下载
	你的 <mark>安全我们来守护</mark> _{防止网上交易信息被逻辑和基本}	01			下戰控件中文
证书序列号:					
授权码:					
选择CSP:	Microsoft Base Cryptographic Provider v1.0		w.		
	重置	下载			(

6. 下载的证书自动存放在 IE 浏览器-Internet 选项-"内容"-"证书"-"个人"
【注:不管是否有下载成功的提示,均请至 IE 浏览器-Internet 选项-"内容"-"证书"-"个人"查看下是否已有下载的证书。证书只能下载一次的,不能重复下载。】
【注:如果 14 天没下载证书授权码过期、找不到证书了等这类问题出现,是需联系业务运营重新申请证书的。可登陆 https://merchant.unionpay.com/portal/login.jsp 服务单管理-创建服务单,提服务单,向业务运营申请新的证书。】

2. 证书导出流程

1. 打开浏览器, 点选 工具 → Internet 选项 → 内容 → 证书;



 以商户号:7000000000001为例说明整个导出流程 在个人证书中找到相对应的证书,点选导出;

٠X	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	行者	1
颁发	给			颁发	者	1
0 🔜 0	41@7001340 41@8100000)145110058@00134014)0000189 <mark>83@305440</mark> 3	45110058:SIGN@00000001 59609940:SIGN@00000001	CFCA CFCA	Operat Operat	i j
	41082012-1	1-02070000000000000	001:SIGN@00000001	CFCA	TEST C	4
00 00 00 00 00	4108310000 4108310000 4108310000)000083040@1045004)000083040@10465004)000083040@30544039	48140006:SIGN@00000213 59609204:SIGN@00000236	CFCA CFCA	Operat Operat Operat	i i
0	4108310000		59609905:SIGN@00000117	CFCA	Operat	i
入口))(导		(<u>R</u>)	(高级(4).
【 《务器	hown and 验证,客F	9端验证,代码签名,	安全电子邮件,时间戳		查看仪)

3. 跳出证书导出向导对话框,点击下一步;

证书导出向导	
	欢迎使用证书导出向导
	这个向导帮助您从证书存储区将证书、证书信任列 表和证书吊销列表复制到磁盘。
	由证书颁发机构颁发的证书是确认您的身份的文件, 它含有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。
	要继续,请单击"下一步"。
	《上一步图》下一步图 》 取消

4. 选择导出私钥

选择:"是,导出私钥",点击"下一步"。

证书导出向导 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	×
导出私钥 您可以选择将私钥跟证书一起导出。	
私钥受密码保护。如果要将私钥跟证书一起导出,您必须在后面一页上键入密码。 要将私钥跟证书一起导出吗? ○ 是,导出私钥 (2) ○ 不,不要导出私钥 (0)	
< 上一步 (b) 下一步 (b) > 取消	

5. 导出私钥文件格式默认点击下一步;

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) @)
○Base64 编码 X.509 (.CER) (S)
○加密消息语法标准 - PKCS #7 证书(P7B)@)
如果可能,将所有证书包括到证书路径中(E)
●私人信息交換 - PKCS #12 (PFX) (P)
🤄 如果可能,将所有证书包括到证书路径中 🕐
☑ 启用加强保护(要求 IK 5.0, NT 4.0 SP4 或更高版本)(E)
□ 如果导出成功,删除密钥(K)
< 上一步 (B) 下一步 (B) > 取消

或者



或者:

● 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(<u>K</u>)

✓ 导出所有扩展属性(A)

□ 启用证书隐私(E)

7 键入证书私钥密码, <u>(必须)</u> 设置为六位数字(仅限数字,请勿设 置字母及符号);

证书导出向导	
密码 要保证安全,您必须用密码保护私钥	•
键入并确认密码。 密码 (£):	
确认密码 (C):	
	< 上一步 @) 下一步 @) > 取消

7. 指定导出证书的文件名,并选择目录存放证书,点击下一步;

证书导出向导	
要导出的文件 指定要导出的文件名。	
文件名 @): 	浏览 (2)

8. 点击完成, 证书导出成功。

2 证书导出向导	正在完成证书导出向导	}	Σ
	您已成功地完成证书导出向导 您已指定下列设置:	•	
Y	文件名 导出密钥 数据包括证书路径中所有证 文件格式	D:\苑\北部湾店.p 是 书 是 个人信息交换(*.p	
	<	•	
21	< 上一步 (B)	完成 取消	í

9、请再从浏览器导出. cer 公钥 选择:"不,不要导出私钥",点击"下一步"。

计出私钥 您可以选择将私	钥跟证书一起导出。
秋钼受恋码保护	。加里要将秋铜踢证书→起导出,您必须在后面→页上键入交
码。 要将私钥跟证书	
() 是,导出	私钥①
○不,不要	导出私钥 (0)

选择公钥格式,银联在线支持 DER 编码及 BASE64 编码,可根据贵司系统编码规则选择其中之一,若无特殊要求,可直接下一步;

E书辑 导	計1向导 ■本 出文件格式 可以用不同的文件格式导出证书。
25	选择要使用的格式:
	◉ 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,则数据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,则数据包括证书路径中的所有证书(V) 加果与出成市,删除利润(X)
	□ 与出所有扩展属性 (A)
	◎ Microsoft 序列化证书存储(.SST)(T)
7	解 <u>证书文件格式</u> 的详细信息
	< 上一步 (B) 下一步 (M) > 取消

3. 公钥证书上传及启用

1. 用户成功通过商户服务网站(<u>https://merchant.unionpay.com/</u>),在主页选择【安全证书上传及下载】



2. 选择要上传的证书,以及选择证书的类型;如果是 cer 格式证书,需要 输入密码;

文主 位 门 工 行 以 一 以		
又任者	S Y L I L	
	浏览 *	
	上传	银联公钊

3、确认证书启用

通过平台目录"用户中心"——"安全管理"——"安全证书管理"进入

首页	用户中心	查询对账	业务办理	服务中心	资金服务
	用户管理 >	基本信息管理 用户信	急管理 审计日;	志查询	
	商户管理 >	关联商户申请 关联商	5户状态查询 商	户信息查询	
	安全管理 >	安全证书上传及下载	安全证书管理	共享关系查询	交易密钥管理

4、启用证书,点击记录后面的启用链接,如下图:



欢迎您 test001 退出 商户号: 824440359620006

切换商户

安全证书	管理							
	序列号		证书起始时间	证书过期时间	启用标志	证书类型	CA类型	操作
7115	55424199377814998406675809	71694553	20140725	20160416	启用	商户证书	CFCA	禁用
7115	55424199377814998406675809	71694553	20140725	20150526	禁用	商户证书	CFCA	
	69264034116		20141029		禁用	商户证书	Verisign	息用 删版
	69264034116		20141029		禁用	商户证书	CFCA	启用删

给出提示,如下图:

安全证书	這管理							
	序列号		定共存代的	Contract the state of the state	自用标志	证书类型	CA类型	操作
711	155424199377814998406	667580971694553	信息提示		× 启用	商户证书	CFCA	禁用
7115542419937781499840667580971694553 69264034116 69264034116		📀 你确认要。	⊘ 你确认要启用该证书吗? 禁		商户证书	CFCA	自用的	
			林 古 用238	禁用	商户证书	Verisign	<u> 倉用 冊</u> 郎	
			柳花三日以月		商户证书	CFCA	自用的	
- 条记录: 4	±1页			首页	上一页 1	下一页 末页	跳转至第	一页 確

点击确定, 启用完成, 给出操作结果。证书启用成功, 贵司已完成证书上传工作。

【注: 启用 10 分钟才生效,请 10 分钟后再发生产交易。】