# 私有云自签名证书导入操作手册

## 【使用须知】

对于强制要求使用HTTPS协议进行安全通信的情况,若无法提供由正规CA机构签发的SSL域名证书,小鱼侧可为其提供免费的SSL证书代签和管理服务,前提是用户需要在系统正式交付前阅读、理解并同意该项服务的免责声明:

您了解并同意,小鱼云视讯平台提供的SSL证书管理服务(SSL Certificate Manager 简称SCM)是小鱼易连为保证视讯云服务和应用安全的前提下 提供的免费SSL证书。您使用该SSL证书管理服务即表明您已经充分阅读、理解和同意本免责声明的全部内容。

1. 该SSL证书管理服务仅限于小鱼云视讯平台服务和终端内部进行安全通信时使用,小鱼方提供基于HTTPS协议通信所需的加密证书,禁止泄露或用于其它用途,若您不慎泄露导致的服务不可用或产生的任何法律后果将由您承担。

2. 对于非因小鱼方原因导致的损失,包括但不限于您手动配置部分、证书本身缺陷,证书被破解等情况导致的损失,小鱼易连将配合用户解决,但 小鱼易连对此不承担责任。

3. 小鱼易连保留对本免责声明进行解释,并随时更新的权利。

## 【操作系统导入证书方式】

Mac 操作系统

Mac搜索"钥匙串访问",点击"证书"栏下面的"+",导入ca.pem (ca.crt)

•	钥匙	串访问	
点按以锁定"叠	录"钥匙串。		Q. 搜索
<ul> <li>钥匙串</li> <li>登录</li> <li>▲ 本地项目</li> <li>系統</li> <li>第統根证书</li> </ul>	Complete         *.li-rui.top           整双者:Let's Encrypt Authority X3            已过期:2019年1月6日 星期日 中国制 0 此证书已标记为受此帐户信任	准时间 下午4:49:12	
	名称	< 种类	过期时间 钥匙串
	📑 *.li-rui.top	证书	2019年1月6日 下午4:49:12 登录
	*.xylink.com	证书	2021年1月17日 上午10:42: 登录
	<b>1</b>	证书	1年1月1日 上午8:05:43 登录
	<b>1</b>	证书	1年1月1日 上午8:05:43 登录
	<b>1</b>	证书	1年1月1日 上午8:05:43 登录
	<b>1</b> 7	证书	1年1月1日 上午8:05:43 登录
	<b>1</b>	证书	1年1月1日 上午8:05:43 登录
种类	172.17.100.15	证书	2045年2月8日 上午11:04: 登录
66 de 18 FB	Default Company Ltd	证书	2020年1月8日 下午7:19:58 登录
(所有项目	ecs-2019822974	证书	2020年7月17日 下午6:15: 登录
. 密码	kubernetes-master	证书	2027年7月31日 下午4:01: 登录
安全备注	localhost.localdomain	证书	2027年11月23日 下午7:39 登录
1 我的证书	Iocalhost.localdomain	证书	2030年9月11日 上午12:20 登录
密钥	private-docker-main@1573023497	证书	2020年11月5日 下午1:58:17 登录
证书	private-docker-main@1582535533	证书	2021年2月23日 下午4:12:13 登录
	private.clouds.dev	证书	2022年6月12日 下午6:20: 登录
	synology.com	证书	2037年5月10日 下午5:40: 登录
	www.nemo-private-cloud.com	证书	2026年4月21日 下午4:22: 登录
	xylink.com	证书	2030年6月10日 下午3:20: 登录
	+ i 將贝	19 项	

### 选择"登录",点击"添加" 完成导入

000		钥匙串访问			
	"钥匙串。			Q xvlink	
				添加证书	
<ul> <li>(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</li></ul>			Certificate 新根证书应被添加 有用户共享,则加	a.pem"的证书添加到钥匙 加到当前用户的登录钥匙 应被添加到系统钥匙串。	<b>ఓ串中吗?</b> B,如果它将被这台机器的所
	家 ^	种类			
	<ul> <li>console.cloudtao@xylink.com)</li> <li>dev381.xylinkmin@xylink.com)</li> <li>devcdn.xylink.com (cky)</li> <li>dms.consoleokaiyang@xylink)</li> <li>ehr.xylink.com (15107113591)</li> <li>harboc.best-xylink.com (admin)</li> </ul>	网页表单密码 网页页表单密码 网页页表单密码 网页页表单密码 网页页表单密码 网页页表单密码		钥匙串:	<u></u> 登录
	mail.xylink.com (caokaiyang)	Web form passwor			
种类	ng2019-2.xylimin@xylink.com)	网页表单密码	查看证书		取消 添加
🕅 所有项目	oa.xylink.com (caokaiyang)	网页表单密码			
/ 密码	passport.aliyukaiyang@xylink)	网页表单密码	2018年12月20日 上午10:5	本	地項目
🧉 安全备注	passport.aliyuuan@xylink.com)	网页表单密码	2020年5月9日下午2:35:44	本	地項目
□ 我的证书	passport.aliyuster@xylink.com)	网贝农半密约	2020年4月23日下午5:39	ф т	地域日
	pops.kylink.com (caokalyang)	网页表半面词	2020年5月25日「十7.42	*	-0
📴 证书	pro-jumpservom (caokalyang)	网页表单密码	2018年10月24日下午4:12	本 本	10-25日
	signin.alivun.ckaivang@xylink.	网页表单密码	2020年1月30日下午9:45:	*	地項目
	signin.alivun.cuan@xvlink.com)	网页表单密码	2019年6月26日上午9:54:	本	地項目
	wiki.xylink.com (caokaiyang)	网页表单密码	2019年7月31日 下午6:43:	<b>本</b>	地項目
	www.katacodang@xylink.com)	网页表单密码	2019年4月24日 下午6:13:	本	地項目
	xylink.com	证书	20	30年6月10日 下午3:20: 登	<b>₽</b>
	<b>+ ( 1 1 1 1</b>		39 10		

导入成功后,双击刚才导入的证书,打开"信任"选项,选择"始终信任",重启客户端即可。

钥匙串 <b>····· 登录</b>	Centificate 根证书颁发机构			xylink.com	
<ul> <li>         ■ 本地項目         ■ 系统      </li> <li>         ■ 系统根证书     </li> </ul>	ご期时间: 2030:     ○ 此证书已标记为     ○     ○     ○     □    □    □    □    □    □    □    □    □    □    □    □    □    □	■3月22日 星期五 中国 ○受此帐户信任	Centificate 根证书摄发机/ 计期时间: 20	1 約 20年2月22日 月期五 中国标准时间 上午	10:50:00
	名称	^ 种类	Q 此证书已标	记为受此帐户信任	10.30.00
	xylink.com	证书	▼ 信任		
	Adobe Content Certificate	10-5 证书	使用此证书时:	始终信任 ○ ?	
	Adobe Content Certificate	10-6 证书			
	Adobe Intermediate CA 10	-3 址书	加密套接字协议层 (SSL)	始终信任 ♀	
	Charles Prove acRook-Pro	-4 证书 a local) 证书	安全邮件 (S/MIME)	始终信任 ≎	
	xvlink.com	证书	可扩展认证协议 (EAP)	始终信任 ♀	
	<b>~</b>		IP安全(IPsec)	始终信任 ♀	
釉墨			代码签名	始终信任 ○	
◎ GE有酒日			时间载	始终信任 ○	
/ 家码			X.509基本策略	始终信任 ○	
→ 安全备注					
3 我的证书			▼ 細节		
♀ 密钥			主题名称		
1 证书			国家或地区 CN		
			省/市/目治区 上海市		
			加住地 上海市 组织 上海寓法	信息利结有限公司	
					A Mar
					Gilles -
					100

WIN10操作系统

1. 打开IE浏览器,点击设置,选择internet选项



### 2. 点击内容,选择导入证书,按如下图示将证书安装到受信任的根证书机构路径下

Internet 选项 ? ×	liui X	×
常规 安全 隐私 内容 连接 程序 高级	预期目的(N): <所有> >	← 🐉 证书导入向导
ビギ     使用加密造量和标序和原目     使用加密造量和标序和原目     使用加密造量和标序和原目     使用加密造量和标序和LI的在有用用上输入合     使用用用用用用用用用用用用用用用用用用用用用用用用用用用用用用用用用	个人 其他人 中间证书感觉机构 受信任的损证书感觉机构 受信任的发布者 未受信任的发布者           感发给         感发者         重止日         友好名称	<b>欢迎使用证书导入向导</b> 该向导可帮助你将证书、证书值任列表和证书用制列换从超盘算制到证书存储。 由证书或双机构或如的证书是对侦导的的确认,它包含用来保护教编或建立安全网络连接的值 意。证书存稿是保存证书的系统区域。
	身入()         資助(n)         資助(n)           原本的預期目的         (1)         (1)         (1)           发动()         其功()         (1)         (1)	単山"下一步"現後。 5 5 5 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7
<b>确定 取消</b> 应用(A)		9





← 🛛 🐓 证书导入向导

### 正在完成证书导入向导

单击"完成"后将导入证书。

用户选定的证书	存储 受信任的根证书颁发机构
内容	证书
文件名	D: _\ca.crt



### 安全警告

 $\times$ 

你即将从一个声称代表如下内容的证书颁发机构(CA)安装证书:

#### xylink.com

Windows 无法确认证书是否确实来自"xylink.com"。你应与" xylink.com"联系,以确认证书来源。下列数字将在此过程中对你有帮助:

指纹 (sha1): 25D7B743 249329F8 3335D444 765A4327 F5347648

#### 警告:

如果安装此根证书,Windows 将自动信任所有此证书颁发机构颁发的 证书。安装未经指纹确认的证书有安全风险。如果单击"是",则表示你 知道此风险。



 $\times$ 

1. 把ios证书下载到手机, "我的IPhone" 根目录



2. 找到手机--设置,进入设置后点击已下载描述文件,进入后点击安装,完成安装

			>
ETI	载描述文件		>
→	飞行模式	0	
?	无线局域网 gao	chao	>
*	蓝牙	打开	>
010	蜂窝网络		>
ම	个人热点	关闭	>
C	通知		>
<b>A</b> (4)	声音与触感		>
C	勿扰模式		>
X	屏幕使用时间		>
$\odot$	通用		>
8	控制中心		>
0	0:08 / 00:31	-	♦

3. 安装完成后点击通用,在里面找到"关于手机"-选择"信任证书设置",启用证书信任

