

邮件证书

实践教程





【版权声明】

©2013-2024 腾讯云版权所有

本文档(含所有文字、数据、图片等内容)完整的著作权归腾讯云计算(北京)有限责任公司单独所有,未经腾讯云 事先明确书面许可,任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成 对腾讯云著作权的侵犯,腾讯云将依法采取措施追究法律责任。

【商标声明】

🔗 腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的 商标,依法由权利人所有。未经腾讯云及有关权利人书面许可,任何主体不得以任何方式对前述商标进行使用、复 制、修改、传播、抄录等行为,否则将构成对腾讯云及有关权利人商标权的侵犯,腾讯云将依法采取措施追究法律责 任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况,部分产品、服务的内容可能不时有所调整。 您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则, 腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务,及相应的技术售后服务,任何问题请联系 4009100100或 95716。



文档目录

实践教程

MacOS For Outlook 配置邮件证书 MacOS For Thunderbird 配置邮件证书 Windows For Outlook 配置邮件证书 Windows For Thunderbird 配置邮件证书 使用 Apple Mail 发送 S/MIME 加密邮件

实践教程 MacOS For Outlook 配置邮件证书

最近更新时间: 2023-10-08 09:26:41

本文档将指导您如何在 macOS 系统下为 Outlook 配置邮件(<mark>S/MIME</mark>)证书,本文以 macOS 10.13.6、 Outlook 2013 版本为例进行说明。

前提条件

- 已在 macOS 系统上安装 Outlook 客户端。
- 已申请购买邮件(S/MIME)证书。

操作步骤

步骤1:密钥导入

- 1. 购买邮件(S/MIME)证书并信息审核通过后,线下业务人员将发送给您邮件证书压缩包,获取邮件证书压缩包 至 macOS 系统,并进行解压。
- 2. 在 Finder 中,双击 *.p12 后缀证书文件,打开"钥匙串访问"应用程序。
- 3. 在提示框中,输入*.p12 后缀证书文件的使用密码,单击确定,即可安装完成。

 说明 密码可在 	E邮件证书压约	宿包中获取。	
	Enter the p Password:	oassword for "aaron_russell.p12":	
		Cancel OK	

4. 安装完成后,可在计算机中进行查看证书,并可供 Apple Mail 和其他应用程序使用。



••• + (i)				Q Search	
Keychains Iogin iCloud System System Roots	Certificate	Aaron Russell Issued by: SSL.com Clier Expires: Wednesday, Mai This certificate is valid	nt Certificate Intermedia rch 17, 2021 at 2:32:10 F	te CA RSA R1 M Central Daylight Time	
	Name	^	Kind	Expires	Keych
	🕨 📷 Aaron R	Russell	certificate	Mar 17, 2021 at 2:32:10 PM	login
Category	🕨 📷 com.app	ole.id8662f7870513d3d	certificate	Apr 26, 2019 at 8:40:06	login
 All Items Passwords Secure Notes My Certificates Keys 					

步骤2: Outlook 配置 S/MIME 证书

1. 打开 Outlook ,在上方菜单中选择工具 > 账户。



2. 选择您的证书所属的账户,然后单击高级。

• • •	帐户
全部显示	
默认能户 ●	E 2
	Exchange/Office 365 帐户
	帐户描述:
	个人信息
	全名: Test-Email
	电子邮件地址:
	身份验证
	方法: 用户名和密码 📀
	用户名:
	密码:
	高级
+• - &	



3. 单击安全性标签,勾选并选择相关信息,配置可参考下图方式进行选择。

()	说明		
	签名算法 SHA-1 比 SHA256 兼容性好,	SHA256	更加安全。

	<u> </u>
签名算法: SHA-256	\$
 ✓ 给待发邮件签名 ✓ 以明文方式发送 ✓ 在签名邮件中包含 	皆有数字签名的邮件 含我的证书
加密	
证书:	\$
加密算法: AES-256 (更安全)	\$
加密待发邮件	
证书身份验证	
客户端证书: 未选择内容	\$

字段说明:

○ 数字签名:

○ 证书:请选择您导入证书名称。

- 签名算法: 可选择 SHA-1 或 SHA-256, 建议选择 SHA-256 兼容性与安全性更好。
- 给待发邮件签名:如需使用邮件证书完成功能,请勾选此处。
- 以明文方式发送带有数字签名的邮件:如需使用邮件证书完成功能,请勾选此处。
- **在签名邮件中包含我的证书**:如需使用邮件证书完成功能,请勾选此处。
- 加密:
 - 证书:请选择您导入证书名称。
 - 加密算法: 建议选择 AES-256, 安全性更好。
 - 加密待发邮件:可根据实际情况进行勾选。
- 证书身份验证:

客户端证书:不进行选择。

4. 单击确认,保存设置。



证书:	
签名算法: S	HA-256
	给待发邮件签名
	以明文方式发送带有数字签名的邮件
	在签名邮件中包含我的证书
加密	
证书:	
加密算法: A	ES-256 (更安全)
	加密待友邮件
证书身份验证	
各尸端业书: 才	<边摔闪容

步骤3:发送邮件

• 发送签名文件

新建邮件,编辑内容后,在上方导航中,单击签名,即可将邮件添加数字签名。

● ● ○ 邮件 ;	思ち	~ €	9					
HTML 设置文本格式	· 密件 抄送	Q 缩放	加密	Q 签名	ABC	语言	○ ▼ 请求回执	(1) 检查 辅助功能
收件人:			1					
抄送: 主题:	S/MIME证书	う测试						
□ 将给此邮	件添加数字领	签名。						
S/MIME 证:	书测试							

• 发送加密文件

新建邮件,编辑内容后,在上方导航中,单击**加密**及签名,即可将邮件添加数字签名并进行加密。

⚠ 注意

发送加密邮件需要拥有对方公钥信息,否则加密邮件无法发送成功。如果需要对方的公钥信息,可让对 方先发送一封签名邮件到您的邮箱账户中,即可给对方发送加密邮件。



7件人: 1999年1997年1997年1997年1997年1997年1997年1997	▲ 检查	请求回执	语言	胡写和语法	□□□ ▼ ♀ 加密 签名	く縮放	密件抄送	TML O
抄送:					1			(件人: [
十四, 0,0,0,0,7,7,2,0,2							1. 41. 4 - 1.7 -	抄送:
王题:S/MIME让书测试						节测试 第2011年1月	/MIME证书	王題: 5



MacOS For Thunderbird 配置邮件证书

最近更新时间: 2023-10-08 09:26:41

本文档将指导您如何在 macOS 系统下,为 Thunderbird 配置邮件(S/MIME)证书,本文以 macOS 10.13.6 版本为例进行说明。

前提条件

- 已在 macOS 系统上安装 Thunderbird 客户端。
- 已申请购买邮件(S/MIME)证书。

操作步骤

步骤1:对 Thunderbird 配置 S/MIME 证书

- 1. 购买邮件(S/MIME)证书并信息审核通过后,线下业务人员将发送给您邮件证书压缩包,获取邮件证书压缩包 至 macOS 系统,并进行解压。
- 2. 在 macOS 首页,选择Thunderbird > 首选项。





3. 在弹框中选择证书标签,并单击管理证书。

••• • 🔞 10	174603500@qq.com	🌣 首选项	×			
¢	常规	反馈	网络&磁盘空间	更新	证书	
.≎	当某个服务器索取我的	个人证书时:				
1	● 自动选择 ○	每次均询问				
Q	查询 OCSP 响应用	服务器以确认证	书的当前有效性			
~						
a	管理证书安全设	备				
0						
Ē						
٤						

4. 在证书管理器弹窗中,单击**导入**,选择对应邮箱 S/MIME 证书。

		证书	管理器		
	您的证书	个人	服务器	证书颁发机构	
您有下列组织的	证书可以识别约	您自己			
证书名称	安全	设备	序列号	过期时间	E
查看	备份 全	部备份	}入 删除	ĝ	
查看	备份 全	部备份	身入 删版	ĵ	

5. 在弹出的密码输入框中,输入证书密码,单击确定,即可完成配置。

() 访 密	钆明 译码可在邮件证书压缩包中获取。	汉 。
0	需要输入密码 请输入被用来加密此证书备份的密码:	码:
	取消 确定	ŧ

步骤2: 证书配置

1. 在 macOS 首页左上角,选择**工具 > 账户设置**。



 在弹出框中选择需要配置证书的邮箱,单击安全,在"数字签名"及"加密"模块,单击选择,选择对应邮箱的 证书。

账户操作			
🕑 发送 (SMTP) 服务器	¹¹¹⁷⁷ 管理证书 安全设备		
磁盘空间	277.48		
垃圾邮件设置			
📃 本地文件夹	 必需(所有接收者必须有证书,否则不发送消息) 		
安全	 从不 (不要加密) 		
回执	发送消息时默认加密设置:		
磁盘空间	透	Ŷ	清空
週111 17日本 1月11日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月111日 1月1111 1月1111 1月1111 1月1111 1月1111 1月1111 1月11111 1月11111 1月11111 1月11111 1月11111 1月11111 1月111111	使用如下证书对友达结恋的消息进行加密和解密:		
副本和文件夹			
服务器			
0	□ 刈泪志致子並名 (飲以)		
安全	□ みぶ自動中館々 (長江)		
回执	选择	¥	清空
同步 & 存储	使用如下证书对您发送的消息进行数字签名:		
垃圾邮件设置	数字签名		
通讯录		1911 1 204	
副本和文件本	要发送和接收已签名或者已加密的消息 您必须指定一个数字签名证	书和一个加	廖证书。

- 🔗 腾讯云
 - 3. 在弹框中选中对应证书,并将加密签发选项更改成如下图所示,单击**确认**,即可完成证书配置。

∠ 通讯求	◇标金▼	1) 厌迷师远	Q 投系 <あれ>	=
证书:	[0E:47:F8:7	E:F2:F0:A8:02:87:90:I	3:DD:8F:CF:4A:5D]	
选定证书的详	细信息:			
	the second second second		and the second se	
签发给:				
签发给: 0E:47:F8:7E: 左放 白 2020	F2:F0:A8:02:87	7:90:E3:DD:8F:CF:4A:	50	
签发给: 0E:47:F8:7E: 有效 自 2020 签名,密钥加速	F2:F0:A8:02:87 年2月21日 GMT	7:90:E3:DD:8F:CF:4A: F+8 上午8:00:00 至 20	5D 23年2月21日 GMT+8 下午8:00:00	
签发给: 0E:47:F8:7E: 有效 自 2020 签名,密钥加密 电子邮件:	F2:F0:A8:02:87 年2月21日 GMT 8	7:90:E3:DD:8F:CF:4A: F+8 上午8:00:00 至 20	5D 23年2月21日 GMT+8 下午8:00:00	
签发给: 0E:47:F8:7E: 有效 自 2020 签名,密钥加密 电子邮件: 签发者: CN=	:F2:F0:A8:02:87)年2月21日 GMT ⁸ TrustAsia Secu	7:90:E3:DD:8F:CF:4A: r+8 上午8:00:00 至 20 re Enterprise Email CA	5D 23年2月21日 GMT+8 下午8:00:00 ,OU=www.trustasia.com,O="TrustAsia	
 签发给: 0E:47:F8:7E: 有效自2020 签名,密钥加语 电子邮件: 签发者: CN= Technologies, Technologies, 	F2:F0:A8:02:87)年2月21日 GMT TrustAsia Secur Inc.",C=CN	7:90:E3:DD:8F:CF:4A: r+8 上午8:00:00 至 20 re Enterprise Email CA	5D 23年2月21日 GMT+8 下午8:00:00 ,OU=www.trustasia.com,O="TrustAsia	

步骤3:邮件加密签名配置

选择完成对应的签名和加密证书后,可将默认配置调整如下图所示:

副本和文件夹 通讯录 垃圾邮件设置	数字签名 使用如下证书对您发送的消息进行数字签名: (0E:47:F8:7E:F2:F0:A8:02:87:90:E3:DD: 选择 清空
磁盘空间 回执 安全	☑ 对消息数字签名(默认)
 → → → → → → → → → → → → → → → → → → →	加密 使用如下证书对发送给您的消息进行加密和解密: [0E:47:F8:7E:F2:F0:A8:02:87:90:E3:DD: 选择 清空
	发送消息时默认加密设置:
	 从不(不要加密) 必需(所有接收者必须有证书,否则不发送消息)
账户操作	

步骤4:邮件发送

• 签名邮件发送

新建邮件,编辑内容后,在上方导航中,选择**安全 > 对此消息数字签名**,即可发送签名邮件。



• • •		撰写:S/MIME签名邮件测试 - Thunderbirg
★ 发送 ★ 描写 ×	🔒 安全 💙 🖬 保存 🗸	
来自: 发至:	加密此消息 水 对此消息数字签名	a a com
发至:	查看安全信息	
主题: S/	/MIME签名邮件测试	
段落 이	变宽度 🔷 文	
S/MIME签名邮件测	试	

• 加密邮件发送

新建邮件,编辑内容后,在上方导航中,选择**安全 > 加密此消息**和对此消息数字签名,即可发送签名邮件。

▲ 注意

发送加密邮件需要对方公钥信息,如果需要对方的公钥信息,可让对方先发送一封签名邮件到您的邮箱 账户中,即可给对方发送加密邮件。





Windows For Outlook 配置邮件证书

最近更新时间: 2023-10-08 09:26:41

本文档将指导您如何在 Windows10 系统下为 Outlook 配置邮件(S/MIME)证书,本文以 Outlook 1902 版 本为例进行说明。

前提条件

- 已在 Windows10 系统上安装 Outlook 客户端。
- 已申请购买邮件(S/MIME)证书。

操作步骤

步骤1:安装证书文件

- 1. 购买邮件(S/MIME)证书并信息审核通过后,线下业务人员将发送给您邮件证书压缩包,获取邮件证书压缩包 至 Windows10 系统中,并进行解压。
- 2. 在 Windows10 中,双击 *.pfx 后缀证书文件。
- 3. 在弹出的"证书导入向导"中,如果需要设置密码,可将私钥密码输入,单击下一步,即可设置成功。

and blow	
为了保证	安全,已用密码保护私钥。
为私钥键	入密码。
密码(P):	
••••	•••••
	示密码(D)
导入选项	(1):
□ 启) 示。	<mark>用强私钥保护(E)。如果启用</mark> 这个选项,每次应用程序使用私钥时,你都会收到揽
□标	5此密钥为可导出的密钥(M)。这将允许你在稍后备份或传输密钥。
回使	围虚拟化安全保护私钥(不可导出)(P)

步骤2: 配置 Outlook 客户端

1. 打开 Outlook ,在主菜单中,单击**文件**。



2. 在左侧导航中,单击**选项**。

信息	帐户信息
打开和导出	Microsoft Exchange
另存为	 ◆ 添加帐户
打印	● 休户设置 更改此帐户的设置或设置更多的连接。 ● 在网上访问此帐户。
Office 帐 户	-
反馈	
选项退出	自动答复(外出) 使用自动答复通知其他人你正外出、休假或无法响应电子邮

3. 在"Outlook 选项"窗口的左侧导航中,单击信任中心,在"Microsoft Outlook 信任中心"模块,单击信任中心设置。

Outlook 选项		?	×
常规	前期保持文档和计算机的安全以及计算机的状况良好。		
自己件	· ·		
日历	安全和其他信息		
组	请访问 Office.com 以了解有关保护你的隐私和安全的详细信息。		
人员任务	Microsoft 信任中心		
搜索	Microsoft Outlook 信任中心		
语言 轻松访问	信任中心包含安全设置和隐私设置。这些设置有助于保护计算机的安全。建议不要更改这些设置。	信任中心设置	i(])
高级			
自定义功能区			
快速访问工具栏			
加戴项			
信任中心			
		确定	取消

4. 在"信任中心"窗口的左侧导航中,单击**电子邮件安全性**,并在"数字标识(证书)模块",单击**导入/导出**。



受信任的发布者	加密电子邮件
隐私选项	
基于表单的登录	
电子邮件安全性	
附件处理	
自动下载	
宏设置	默认设置():
编程访问	数字标识(证书)
	数字标识或证书是一种可让您在用子路经由证定身份的文档。 发布到全球通讯簿(2)
	读现为纯文本
	以纯文本格式读取所有标准邮件(A)
	□ 以纯文本格式读取所有数字签名邮件(M)
	文件夹中的脚本
	□ 允许在共享文件夹中使用脚本(L)
	□ 允许在公用文件夹中使用脚本(F)
	· · · · · · · · · · · · · · · · · · ·
	IPDXL PDVIE

5. 在"导入/导出数字标识"窗口中,勾选"从某文件导入现有的数字标识",然后单击**浏览…,选取证书文件, 单击确定**。

导入/导出数字标识				×
 从某文件导入现有的 将数字标识从文件导入 	数字标识(l) 到计算机。您必	必须使用将证	书导出到该文件	#时所输入的密
码。			_	
导入文件(F):				浏览(B)
密码(P):				
数字标识名称(D):				
○将数字标识导出到某	文件中(E)			
将数字标识信息导出到	某文件中。请辅	俞入密码以帮	助保护该信息。	
数字标识:				选择(S)
文件名(F);				浏览(W)
密码(R):				
确认(C):				
」与 Microsoft Inter	net Explorer 4	1.0 兼容(安全	:性 - 低)(M)	
□ 将数字标识从系统中	□删除(L)			
			确定	取消

6. 输入在 步骤1 中设置的证书密码,单击确定。



7. 在弹出的安全对话框中,单击确定。



步骤3:电子邮件证书配置

- 1. 打开 Outlook ,在主菜单中,单击**文件**。
- 2. 在左侧导航中,单击选项。





3. 在 "Outlook 选项" 窗口的左侧导航中,单击**信任中心**,在 "Microsoft Outlook 信任中心" 模块,单击**信任** 中心设置。

Dutlook 选项			?	\times
常规	📦 帮助保持文档和计算机的安全以及计算机的状况良好。			
邮件	•			
日历	安全和其他信息			
组	请访问 Office.com 以了解有关保护你的隐私和安全的详细信息。			
人员	Minner & Perference			
任务	WICHSOLIBITION			
搜索	Microsoft Outlook 信任中心			
语言	信任中心包含安全设置和隐私设置。这些设置有助于保护计算机的安全,建议不要更改这些设置。	信任中	പക്ഷി	D
轻松访问		Debre 1	U OCAL	
高级				
自定义功能区				
快速访问工具栏				
加戴项				
信任中心				
			_	

4. 在"信任中心"窗口的左侧导航中,单击电子邮件安全性,并在"加密电子邮件模块",单击设置。

信任中心			?	\times
受信任的发布者	加密电子邮件			
國私达坝 基于表单的登录 电子邮件安全性 附件处理 自动下载 宏设置 使用之时	加密待发邮件的内容和附件(E)			
	数字伝识或证书是一种可让您在电子简务中证实身份的文档。 发布到全球通訊簿(P)<			
	文件夹中的脚本 ☆井在共享文件夹中使用脚本(L) ✓ /元井在公用文件夹中使用脚本(E)			
		确定	取	消

5. 在"更改安全设置"窗口中,选择"安全设置名称"并勾选"该安全邮件格式的默认加密设置"与"所有安全邮件的默认加密设置"。



更改安全设置	×
安全设置首选参数	
安全设置名称(S):	
S/MIME SETTING	~
加密格式(F): S/MIME	\sim
☑ 该安全邮件格式的默认加密设置(T)	
☑所有安全邮件的默认加密设置(M)	
安全标签(U) 新建(N) 删除(D)	
证书和算法	
签名证书:	选择(C)
哈希算法(A):	
加密证书:	选择(H)
加密算法(L): ~	
☑将证书与签名邮件一同发送(E)	
确定	取消

6. 在签名证书右侧,单击选择,选择签名证书。

更改安全设置	×
安全设置首选参数	
安全设置名称(S):	
S/MIME SETTING	~
加密格式(F): S/MIME	\sim
☑ 该安全邮件格式的默认加密设置(T)	
☑所有安全邮件的默认加密设置(M)	
安全标签(U) 新建(N) 删除(D)	
证书和算法	
签名证书:	选择(C)
哈希算法(A): ~	
加密证书:	选择(H)
加密算法(L):	
☑ 将证书与签名邮件一同发送(E)	
确定	取消

7. 弹出的确认对话框中,单击确定。

Windows	Windows 安全中心 >			
选择证	E书			
?	颁发者: DigiCert SHA2 / 有效期: 2019/8/13 至 2 单击此处查看证书属性	Assured ID CA 021/8/13	L.	
	确定		取消	

8. 在加密证书右侧,单击选择,选择加密证书,单击确定,关闭"更改安全设置"窗口即可。

更改安全设置			×
安全设置首选参数			
安全设置名称(S):		
S/MIME SET	TING		~
加密格式(F):	S/MIME		\sim
☑该安全邮件	格式的默认加密设置(T)		
☑ 所有安全邮	件的默认加密设置(M)		
安全	标签(U) 新建(N)	删除(D)	
证书和算法 -			
签名证书:			选择(C)
哈希 <i>算</i> 法(A):		~	
加密证书:			选择(H)
加密算法(L):		\sim	
☑将证书与签	名邮件一同发送(E)		
		确定	取消

步骤4: S/MIME 加密邮件配置

如果需要发送加密邮件,电子邮件安全性中默认配置需调整操作步骤如下:

1. 打开 Outlook ,在主菜单中,单击**文件**。



2. 在左侧导航中,单击**选项**。

会	帐户信息
打开和导出	Kicrosoft Exchange
另存为	 ◆ 添加帐户
打印 	● 在网上访问此帐户。
Office 帐 户	
反馈	
选项	自动答复(外出) 使用自动答复通知其他人你正外出、休假或无法响应电子邮/

3. 在 "Outlook 选项" 窗口的左侧导航中,单击**信任中心**,在 "Microsoft Outlook 信任中心" 模块,单击**信任** 中心设置。

Outlook 选项			?	\times
常规	前期保持文档和计算机的安全以及计算机的状况良好。			
邮件				
日历	安全和其他信息			
组	请访问 Office.com 以了解有关保护你的隐私和安全的详细信息。			
人员				
任务	<u>Microsoft</u> 信任中心			
搜索	Microsoft Outlook 信任中心			
语言	信任中心包含安全设置和隐私设置。这些设置有助于保护计算机的安全。建议不要更改这些设置。	信任由心	v沿粤(TT	
轻松访问			NXE(L)	
高级				
自定义功能区				
快速访问工具栏				
加戴项				
信任中心				
		确定	取	肖

4. 在"信任中心"窗口的左侧导航中,单击**电子邮件安全性**,并在"加密电子邮件模块",勾选"加密待发邮件的 内容和附件""给待发邮件添加数字签名"及"对所有 S/MIME 签名邮件要求 S/MIME 回执"。



受信任的发布者	加密电子邮件
隐私选项 基于表单的登录 电子邮件安全性 附件处理 自动下载 宏设置	
编程访问	数字标识(证书)
	数字标识或证书是一种可让您在电子商务中证实身份的文档。 发布到全球通讯簿(D) 导入/导出(U)
	□ 以社文本格式读取所有数字签名邮件(M)
	文件夹中的脚本
	 □ 允许在共享文件夹中使用脚本(L) ☑ 允许在公用文件夹中使用脚本(E)
	确定 取消

步骤5:发送邮件

• 签名邮件发送

新建邮件,编辑内容后,在上方导航中,单击签署,即可发送签名邮件。

د 🖻	O		Ŧ					
文件	邮件	插入	选项	设置文本格:	式前	副 帮助	Q	操作说明搜索
→ 主题 ↓	颜色 ▼] 字体 ▼] 效果 ▼ 主题	くうして 页面颜色	密件 显示	□□ ● 少送 加密 字段 加	2 签署 密	● ● 伊用 投票按钮 ·	□请	求送达回执 求已读回执 ¹ 3
『『 发送(S)	发件/ 收代 抄递	人(M) ▼ 隼人 É(C)						
	主题(U)		S/MIN	ME邮件测试				
S/MIME	邮件测	दि⇔						

• 加密邮件发送

新建邮件,编辑内容后,在上方导航中,单击加密及签署,即可发送加密邮件。





发送加密邮件需要对方公钥信息,如果需要对方的公钥信息,可让对方先发送一封签名邮件到您的邮箱 账户中,即可给对方发送加密邮件。

🗄 ১	G	ή Ψ	Ŧ							
文件	邮件	插入	选项	设置	文本格式	审	司 帮助	Q	操作说明搜	索
	颜色 ▼ 字体 ▼ 效果 ▼ 主题		名 名 名 日 二 名 日 名 日 日 二 日 日 日 日 日 日 日 日 日	□□■●送	加密	2 签署	□□□ 使用 投票按钮	□请 ↓□请 跟踪	求送达回执 求已读回执 ∽	
⁼==" 发送(S)	发件ノ 收件 抄送 主题(U)	Ĺ(M) ▼ ‡人 ἑ(C)	S/MIN	VIE曲时(牛)	则试					
S/MIME	邮件测	दि≓								

书

Windows For Thunderbird 配置邮件证

最近更新时间: 2023-10-08 09:26:41

本文档将指导您如何在 Windows10 系统下为 Thunderbird 配置邮件(<mark>S/MIME</mark>)证书,本文以 Thunderbird 78.3.3 版本为例进行说明。

前提条件

- 已在 Windows10 系统上安装 Thunderbird 客户端。
- 已申请购买邮件(S/MIME)证书。

操作步骤

步骤1:安装证书文件

- 1. 购买邮件(S/MIME)证书并信息审核通过后,线下业务人员将发送给您邮件证书压缩包,获取邮件证书压缩包 至 Windows10 系统中,并进行解压。
- 2. 在 Windows10 中,双击 *.fpx 后缀证书文件。
- 3. 在弹出的"证书导入向导"中,如果需要设置密码,可将私钥密码输入,单击下一步,即可设置成功。

← 🐉 证书导入向导
私 胡保护 为了保证安全,已用密码保护私钥。
为私钥键入密码。
密码(P): ●●●●●●●
- 导入选项(I):
□ 启用骚私钥保护(E)。如果启用这个选项,每次应用程序使用私钥时,你都会收到提示。
□ 标志此密钥为可导出的密钥(M)。这将允许你在稍后备份或传输密钥。
□使用虚拟化安全保护私钥(不可导出)(P)
☑ 包括所有扩展属性(A)。
下一步(N) 取消

步骤2: Thunderbird 客户端 S/MIME 证书配置



1. 打开 Thunderbird 客户端,在需要配置的邮箱账户上方,单击鼠标右键,并单击设置。



2. 在设置的左侧导航中,单击端到端加密,并在"端到端加密"页面,单击管理 S/MIME 证书。

×		e –		×
				^
端到端加密				
右安友达经加密明	微子金名的消息,需配置 OpenPGP 或 S/MIME 加密技术。			
请选择您要用于(OpenPGP 的个人密钥,或用于 S/MIME 的个人证书。无论是	个人密钥或是i	止书,	
恣郁云有刈应时有	おり。 「千年」 」 房中			
OpenPGP				
👝 Thunde	bird 没有用于 @ @qq.com 的 OpenPGP 个			
人密钥		,丹 添加密钥(<u>A</u>)	
使用 OpenPGP	3钥管理器可以查看往来通信者的公钥,以及所有上方未列出的	口密钥。		
OpenPGP 密钥	查理器(K)			
open er ans				
C (BAILAE				
5/IVIIIVIE 个人数字签名证书	3:			
	选择()	[<u>S</u>) 清空	:(<u>C</u>)	
个人加廖证书·				
	选择(T) 清空	E(E)	
管理 S/ <u>M</u> IME i	E书 S/MIME 安全设备(Y)			
发送消息时的默	认设置			
若不进行端到端加	密,邮件服务提供商可以轻易获知您的邮件内容,并进行大规	!模监控。		
 默认不能 	3用加密(<u>N</u>)			
○ 默认要求	动密(<u>U)</u>			
若您要求加密	,须先获取每个收件人的公钥或证书才能发送消息。			
	 X 端到端加密 若要发送经加密或 病选择您要用于C 您都会有对应的税 OpenPGP の 使用 OpenPGP 整研 の の の 大加密证书: 管理 S/MIME 指 及送消息时的既 承 新人取 	× ● 端到端加密 若要发送经加密或数字签名的消息, 電配置 OpenPGP 或 S/MIME 加密技术、 海选择您要用于 OpenPGP 的个人密钥, 或用于 S/MIME 的个人证书, 无论是你都会有对应的私钥。 详细了解 OpenPGP ✓ Thunderbird 没有用于 ● Qq.com 的 OpenPGP 个人密钥 // 公司 ● // 公司 // 公司 <th>× 直日一 端到端加密 若要然送经加密或数字签名的消息, 集配置 OpenPGP 或 S/MIME 加密技术。 清选择您要用于 OpenPGP 的个人密钥, 或用于 S/MIME 的个人证书, 无论是个人密钥或是证念都会有对应的私钥。 详细了解 OpenPGP ① Thunderbird 没有用于 @ qq.com 的 OpenPGP 个 ▲ 添加密钥 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥。 ② 使用 OpenPGP 密钥管理器(X) ③ penPGP 密钥管理器(X) ③ 使用 OpenPGP 密钥管理器(X) ③ 应择(D)… 原空 ● 就认不信用加密(N) ■ 就认不信用加密(L) ■ 就认买求加密(L) ■ 就认买菜加密(L) ■ 就认买点, 须先就取得少数学说出表示。 ■ 就认买点, 须先就取得个数件人的公捐或证书才能说送消息。 ■ 就认买点, 须先就取得个数件人的公捐或证书才能说送消息。 ■ 就认知应的, 须先就取得个数件人的公捐或证书才能说送消息。 </th> <th>× ● 回 □ □ 端到端加密 若寒沈送她mo或数字签名的消息, 霜配置 OpenPGP 或 S/MIME 加密技术。 病选择您要用于 OpenPGP 的个人密钥, 或用于 S/MIME 的个人证书, 无论是个人密钥或是证书, 你都会有对应的私钥。 详细了解 OpenPGP ① @qq.com 的 OpenPGP 个 ▲ 添加密钥(山) @qq.com 的 OpenPGP 个 人密钥 @qq.com 的 OpenPGP 个 A more (a) 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥, 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥, 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥, 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥, 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥, </th>	× 直日一 端到端加密 若要然送经加密或数字签名的消息, 集配置 OpenPGP 或 S/MIME 加密技术。 清选择您要用于 OpenPGP 的个人密钥, 或用于 S/MIME 的个人证书, 无论是个人密钥或是证念都会有对应的私钥。 详细了解 OpenPGP ① Thunderbird 没有用于 @ qq.com 的 OpenPGP 个 ▲ 添加密钥 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥。 ② 使用 OpenPGP 密钥管理器(X) ③ penPGP 密钥管理器(X) ③ 使用 OpenPGP 密钥管理器(X) ③ 应择(D)… 原空 ● 就认不信用加密(N) ■ 就认不信用加密(L) ■ 就认买求加密(L) ■ 就认买菜加密(L) ■ 就认买点, 须先就取得少数学说出表示。 ■ 就认买点, 须先就取得个数件人的公捐或证书才能说送消息。 ■ 就认买点, 须先就取得个数件人的公捐或证书才能说送消息。 ■ 就认知应的, 须先就取得个数件人的公捐或证书才能说送消息。 	× ● 回 □ □ 端到端加密 若寒沈送她mo或数字签名的消息, 霜配置 OpenPGP 或 S/MIME 加密技术。 病选择您要用于 OpenPGP 的个人密钥, 或用于 S/MIME 的个人证书, 无论是个人密钥或是证书, 你都会有对应的私钥。 详细了解 OpenPGP ① @qq.com 的 OpenPGP 个 ▲ 添加密钥(山) @qq.com 的 OpenPGP 个 人密钥 @qq.com 的 OpenPGP 个 A more (a) 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥, 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥, 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥, 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥, 使用 OpenPGP 密钥管理器可以查看往来通信者的公钥, 以及所有上方未列出的密钥,



3. 在证书管理器窗口,单击导入,在资源管理器中,选择对应证书并输入步骤1 中设置的密码。

		证书管	理器		
您的证书	认证决策	个人	服务器	证书颁发机构	
您有下列组织的	的证书可以识别您	后自己			
证书名称	安全设备	E .	序列号	过期时间	E,
			_		
查看(V)	备份(<u>B</u>)	全部备份(K) 导入(M	D 删除(<u>D</u>)	

4. 单击确定,证书导入成功。

		证书管理	里器		
您的证书	认证决策	个人	服务器	证书颁发机构	
您有下列组织的	证书可以识别您	自己			
证书名称	安全设备	<u>ه الماريم الم</u>	序列号	过期时间	E
✓ DigiCert Ind	-				
	软件型安	全设备		. 2021年8月13日	
查看(<u>V</u>)	备份(<u>B</u>)	全部备份(K).	导入(M	1) 删除(<u>D</u>)	
				1	明正



5. 分别选择邮箱的"个人数字签名证书"及"个人加密证书",并单击确定即可完成设置。

~ ⊠@qq.com	请选择您要用于 OpenPGP 的个人密钥,或用于 S/MIME 的个人证书。无论是个人密钥或是证书, 您都会有对应的私钥。 详细了解
服务器 副本和文件夹	OpenPGP
通讯录 垃圾邮件设置	Thunderbird 没有用于 Market @ @qq.com 的 OpenPGP 个 人密钥
同步 & 存储 端到端加密	使用 OpenPGP 密钥管理器可以查看往来通信者的公钥,以及所有上方未列出的密钥。
回か↓ ◇ ` 本地文件夹 ☆招報(小公署)	OpenPGP 密钥管理器(<u>K</u>)
磁盘空间 图 发送 (SMTP) 服务器	S/MIME 个人数字签名证书:
	选择(<u>S</u>) 清空(<u>C</u>) 个人加密证书:
	选择(① 清空(E) 管理 S/ <u>M</u> IME 证书 S/MIME 安全设备(Y)

步骤3:发送邮件

• 发送签名邮件

新建邮件,编辑内容后,在上方导航中,选择**安全 > 对此消息数字签名**,即可发送签名邮件。

▲发送 ▲拼写 ▼			4	安全 🖌 🖬 保存 🗸		
发件人(R) - 收件人 10			加密技术①		a company and a second second	
			•	不加密(<u>O</u>)		a.com
		10		要求加密(E)		
ŧ	题(<u>S</u>)	S/N	~	对此消息数字签名(<u>M</u>)		
的慈く	नय	安度		查看安全信息(1)		

• 发送加密邮件

新建邮件,编辑内容后,在上方导航中,选择**安全 > 要求加密**及对此消息数字签名,即可发送加密邮件。

▲ 注意

发送加密邮件需要对方公钥信息,如果需要对方的公钥信息,可让对方先发送一封签名邮件到您的邮箱 账户中,即可给对方发送加密邮件。



▲ 发送	A	拼写	-		安全 🖌 🖸 保存 🗸								
	发件)	(R)	-		加密技术(工)	>				1		. 17	
收件人 10			不加密(0)							1.1			
		•	要求加密(E)										
	主题	题(<u>S</u>)	S/N	~	对此消息数字签名(M)								
段落	~	可要	宽度	_	查看安全信息(1)		A' A	A	A	A	i≡	1-	(=) =



使用 Apple Mail 发送 S/MIME 加密邮件

最近更新时间: 2022-09-27 10:53:51

本文档将指导您如何在 macOS 系统下使用 Apple Mail 发送 S/MIME 加密邮件,本文以 macOS 10.13.6 版 本为例进行说明。

前提条件

已申请购买邮件(S/MIME)证书。

操作步骤

步骤1:安装证书文件

- 1. 购买邮件(S/MIME)证书并通过信息审核后,线下业务人员将发送给您邮件证书压缩包,获取邮件证书压缩包 至 macOS 系统,并进行解压。
- 2. 在 Finder 中,双击 *.p12 后缀文件,打开"钥匙串访问"应用程序。(文件扩展名是 .p12)。
- 3. 在提示框中,输入*.p12 后缀证书文件的使用密码,单击OK。

① 说明 密码词	可在邮件证书压缩包中获取。
	Enter the password for "aaron_russell.p12":
	Password:
	Show password
	Cancel OK

4. 该证书现已安装在您的计算机上,可供 Apple Mail 和其他应用程序使用。如下图所示:



• • • + (i)				Q Search			
Keychains login iCloud System System Roots	Certificate Standard	Aaron Russell Issued by: SSL.com Clier Expires: Wednesday, Mar This certificate is valid	te CA RSA R1 PM Central Daylight Time	CA RSA R1 Central Daylight Time			
	Name	^	Kind	Expires	Keychain		
	🕨 📷 Aaron R	ussell	certificate	Mar 17, 2021 at 2:32:10 PM	login		
Category	🕨 📷 com.app	le.id8662f7870513d3d	certificate	Apr 26, 2019 at 8:40:06	login		
 All Items Passwords Secure Notes My Certificates Keys Certificates 							

步骤2:邮件发送

i.

1. 打开 Apple Mail 邮件。

 ⚠ 注意 如果在安装证书时,已打开邮件,请重新启动。 ● 如果在"邮件"中配置了多个电子邮件地址,请确保已在"发件人"行中,选择为其颁发证书的地址。
 如果证书已正确安装,则在"主题"行右侧,应出现带有复选标记的蓝色 图标,表明该消息已签 名。如果您不想对消息进行签名,则可以单击 ,以取消选中。
• 如果您有收件人的公共密钥,则在"主题"行右侧,单击 🔒 ,将锁闭合锁,表示您的邮件将被加
密。如果由于某种原因不想加密电子邮件,请单击 🔒 ,将锁打开表示不对邮件进行加密。

То:	\oplus
Cc:	
Subject:	
From: Aaron Russell -	

2. 编辑完邮件,单击**发送**即可。

() 说明

若发送加密邮件,将弹出提示窗口,需输入 Mac 登录密码,授予 Mail 使用私钥对消息签名的权限,并单击 Allow 或 Always Allow。如果您单击 Always Allow,下一次使用证书签名电子邮



?

your keychain.

Password:

Always Allow

To allow this, enter the "login" keychain password.

	Ма	il wants to	sign usin	g key "pri	vateKey'	" in			
٠	如果您	使用的是安	R装在 Yu	biKey 上	的证书,	将提示您轴	俞入 PIN	码而不是登	録密码。
	件时,	将不会提示	家输入密	码。					

Deny

Allow