

10分钟学会PGP加密

Miot 嵌入式

Exported on 01/03/2020

Table of Contents

1 安装	4
1.1 工具下载	4
1.2 安装	6
2 使用	8
2.1 首次使用	8
2.2 校验及解密	12

只需10分钟，即可让你的信息10倍安全。

1 安装

1.1 工具下载

去官方网站下载开源免费的GnuPG工具: <https://gnupg.org/download/>¹

官方提供了windows、MAC、linux各种版本, 这里以windows为例, 如果下载比较慢我们可以提供, **请勿下载非官方软件。**

1. 选择Gpg4win

OS	Where	Description
Windows	Gpg4win	Full featured Windows version of <i>GnuPG</i>
	download sig	Simple installer for the current <i>GnuPG</i>
	download sig	Simple installer for <i>GnuPG 1.4</i>
OS X	Mac GPG	Installer from the gpgtools project
	GnuPG for OS X	Installer for <i>GnuPG</i>
Debian	Debian site	GnuPG is part of Debian
RPM	rpmfind	RPM packages for different OS
Android	Guardian project	Provides a GnuPG framework
VMS	antinode.info	A port of GnuPG 1.4 to OpenVMS
RISC OS	home page	A port of GnuPG to RISC OS

¹ <https://gnupg.org/download/index.html>

2. 点击Download

[Home](#) » [Download](#)

Download

Gpg4win 3.1.11 (Released: 2019-12-17)

You can download the full version (including the Gpg4win compendium) of Gpg4win 3.1.11 here:

Gpg4win 3.1.11
Size: 27.6 MByte

[OpenPGP signature](#) (for gpg4win-3.1.11.exe)
SHA256: 156de9f3f50bb5a42b207af67ae4ebcb2d10a7aaf732149e9c468eaf74ce7ffc
[Changelog](#)


More Gpg4win-3.1.11 downloads

3. 这里是捐赠，选择捐赠数额，可以选择0免费使用，点击下载

Please donate for Gpg4win to support maintenance and development!
Pay what you want! – Thank you!

Donate with

- ☒ PayPal
- ☐ Bitcoin
- ☐ Bank transfer



\$0

\$10

\$15

\$25


\$ _____

USD

EUR

onetime

monthly

 **Download**

1.2 安装

1. 双击运行下载的gpg4win-3.1.11.exe安装包，点击“ok”选择中文安装引导



2. 一路“下一步”，选择“安装”



3. 提示安装完成, “下一步”-》“完成”即可完成安装。



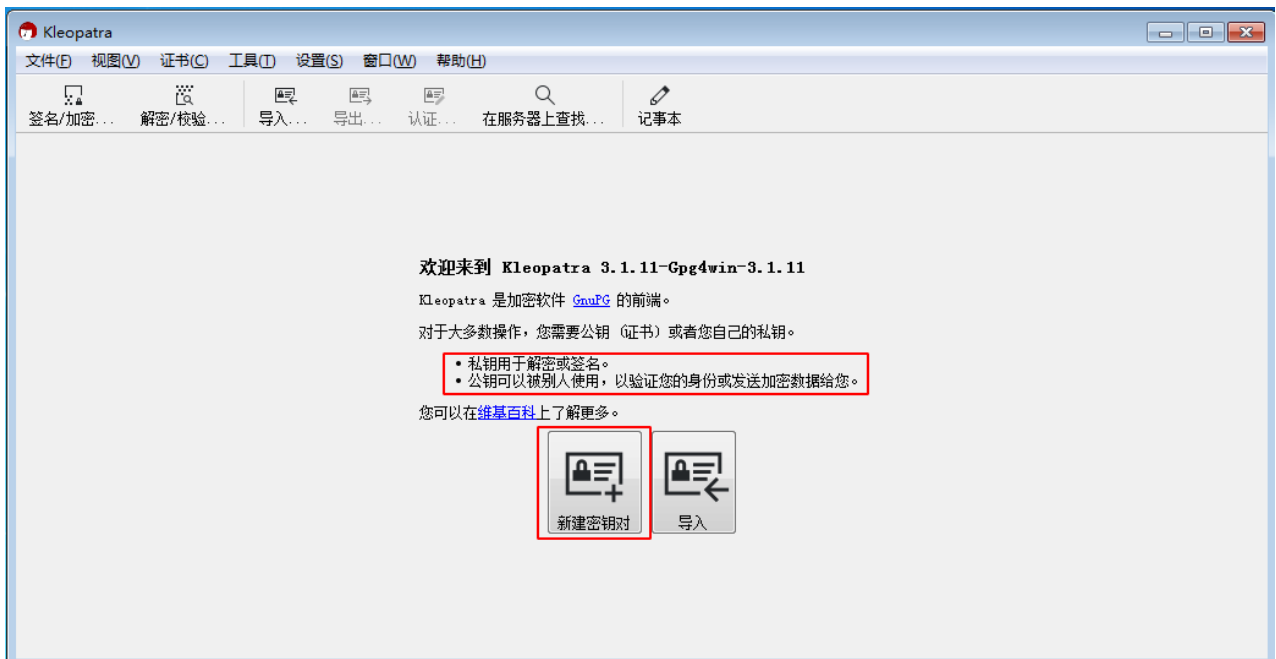
2 使用

2.1 首次使用

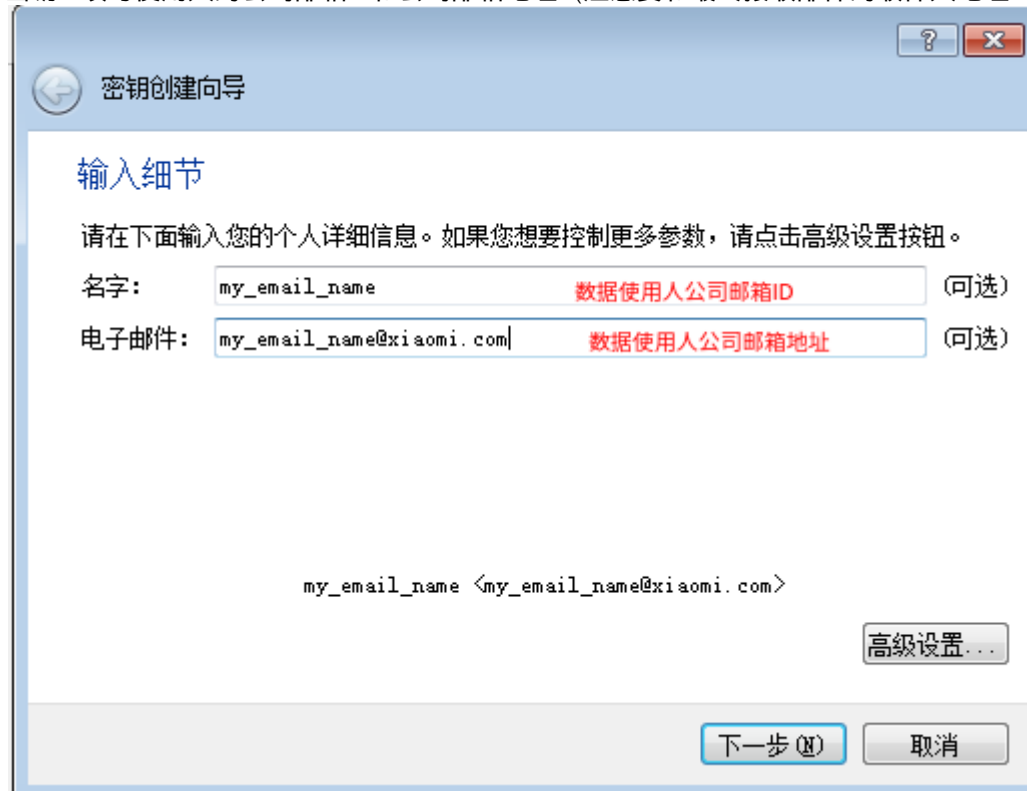
本步骤只需在首次安装后执行一次，如已配置过，请跳过。

首次使用，需要进行必要的配置，生成本机独一无二的加密密钥。

安装完成，默认会打开Kleopatra管理器，选择新建密钥对（即私钥和公钥），公钥后续可以导出发给别人，**私钥打死谁都不能给**，只能自己保管。



1. 密钥ID填写使用人的公司邮箱ID和公司邮箱地址（注意要和最终接收邮件的收件人地址一致）；



密钥创建向导

输入细节

请在下面输入您的个人详细信息。如果您想要控制更多参数，请点击高级设置按钮。

名字: 数据使用人公司邮箱ID (可选)

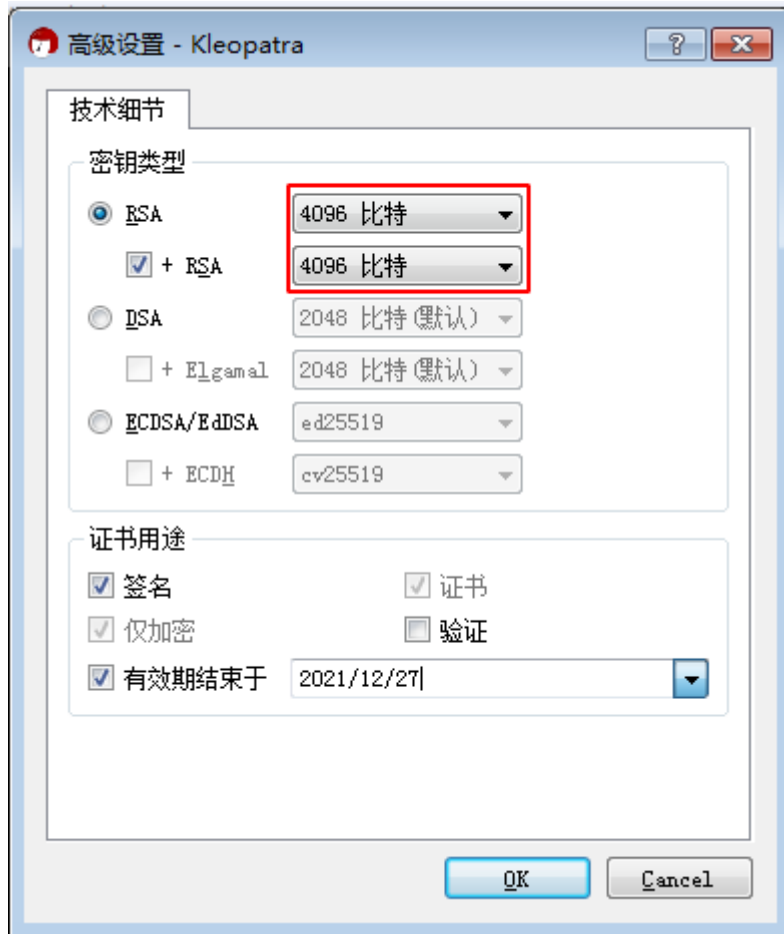
电子邮件: 数据使用人公司邮箱地址 (可选)

my_email_name <my_email_name@xiaomi.com>

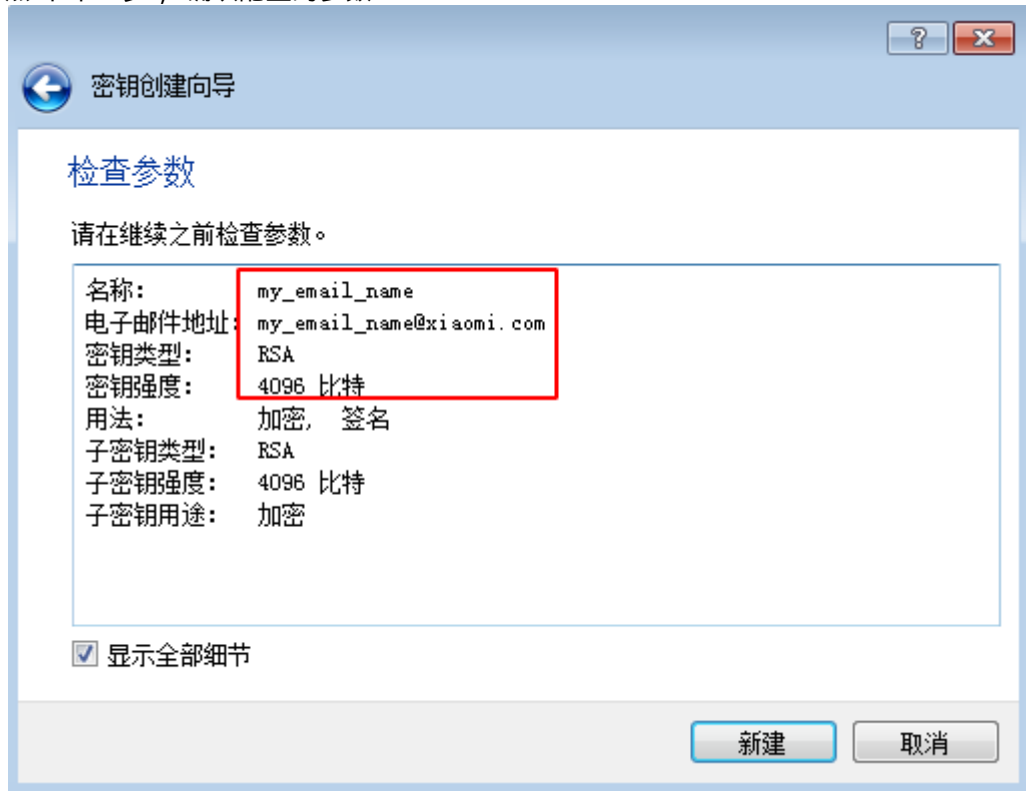
高级设置...

下一步(N) 取消

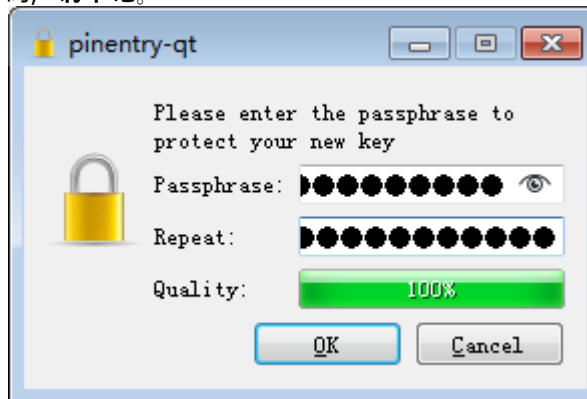
2. 在高级设置选项里, 选择密钥长度4096, 可选密钥过期时间



3. 点击“下一步”，确认配置的参数



4. 点击“新建”，会开始创建公私钥对，并提示输入私钥的保护密码，后续使用该软件时会需要使用该密码，请牢记。

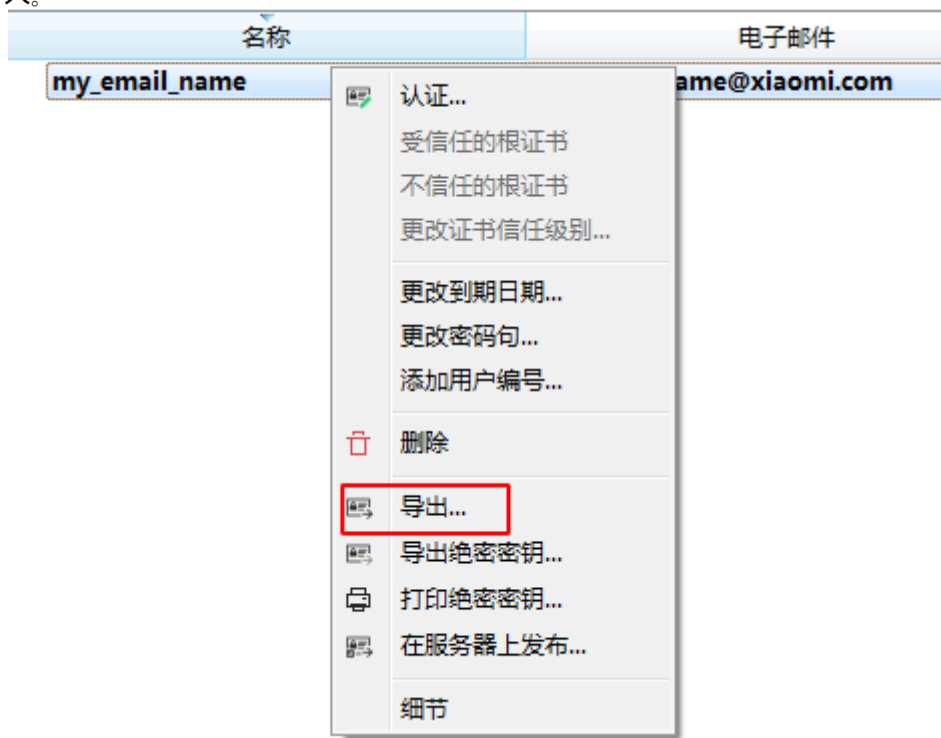


5. 密钥生成完成，如图所示

搜索... <Alt+Q>					
名称	电子邮件	用户编号	有效期开始自	有效期结束于	密钥 ID
my_email_name	my_email_name@xiaomi.com	认证的	2019/12/27		01C2 3FF9 AF8...

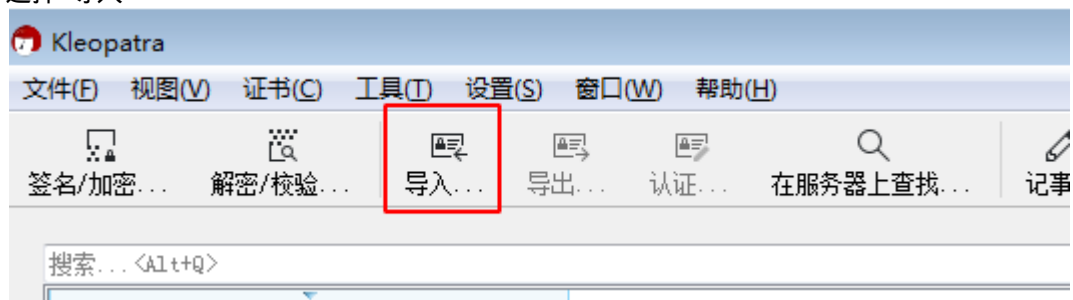
6. 在生成的密钥上右键->“导出”，会导出你的公钥，存到指定位置，后续邮件发给要和你安全通信的人。注意不是导出绝密私钥，绝密私钥不需要备份的话就不要导出了，导出了也要私密保管，不能给任何

人。

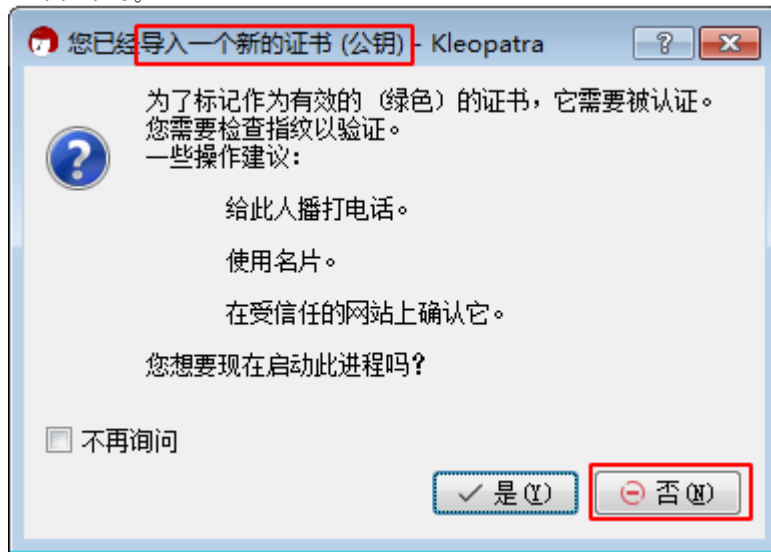


2.2 校验及解密

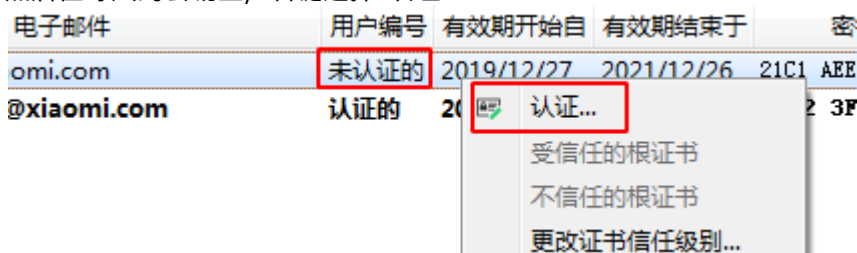
1. 导入对方的公钥；
 - a. 选择“导入”



- b. 选择对方发给你的 .asc公钥文件，由于是对方给你邮件发的，你们已经确认过了，所以这里选“否”即可。



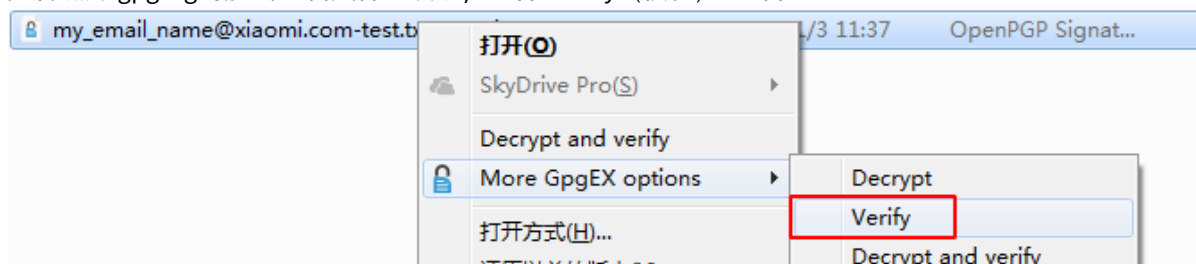
- c. 然后在导入的公钥上，右键选择“认证”



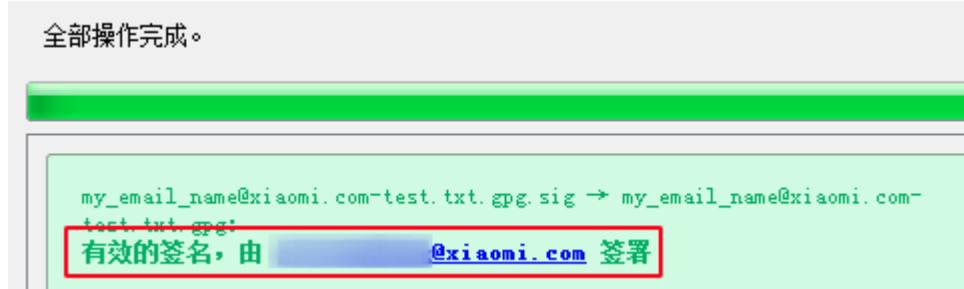
- d. ok，导入成功，可以校验和解密了。

电子邮件	用户编号	有效期开始自	有效期结束于
omi.com	认证的	2019/12/27	2021/12/26
@xiaomi.com	认证的	2019/12/27	

2. 在后缀为.gpg.sig的加密签名文件上右键，选择“Verify (校验)”签名；



3. 校验成功后如图，确认签名者身份正确，然后“Save All（保存）”，得到加密的.gpg文件；



4. 在校验成功的文件上右键选择“Decrypt（解密）”，则可“Save All”保存解密后的文件使用了。

