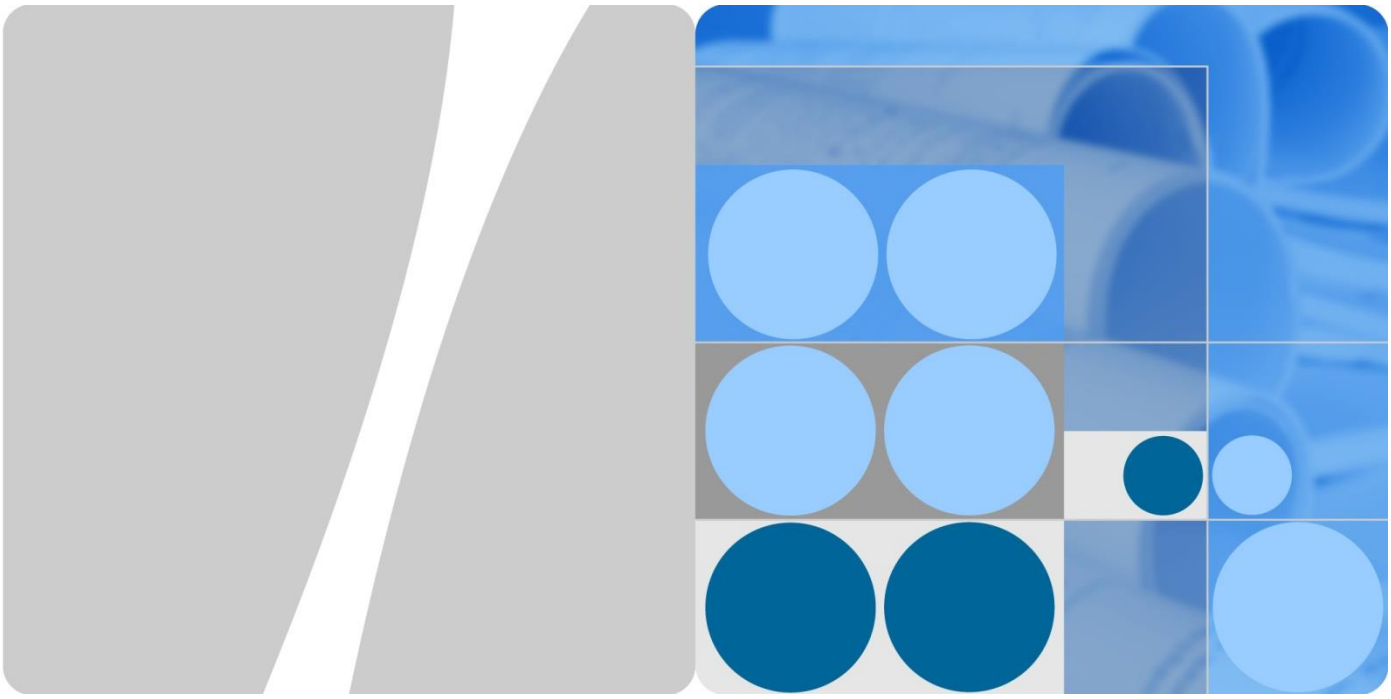


OpenPGP V100R001C00

签名验证指南

文档版本 04

发布日期 2020-10-09

华为技术有限公司

网络安全能力中心

商标声明

 和其他华为商标均为华为技术有限公司的商标。

 为华为网络安全能力中心的商标。

 为 PGPVerify 工具商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

概述

本指南主要介绍 OpenPGP 签名的验证工具及操作过程。

读者对象

本指南主要适用于以下工程师：

- 技术支持工程师
- 维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
 警告	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
 小心	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。
 注意	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。
 说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修改记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2014-11-20)

第一次版本发布。

文档版本 02 (2017-08-31)

1. 修改验证签名步骤的描述。
2. 将 PGP 验证工具升为 V100R001C00SPC310 版本。

文档版本 03 (2017-12-12)

1. 增加验证错误处理建议；
2. PGP 验证工具升级为 V100R001C00SPC320 版本。

文档版本 04 (2020-02-20)

增加了 OpenPGP 密钥长度为 4096 的验证指导。

PGPVerify 工具版本历史

历史记录累积了每次 PGPVerify 工具版本更新的内容。最新版本的文档包含以前所有 PGPVerify 工具版本的更新内容。

产品版本 V100R001C00SPC200：

1、 第一次版本发布，实现 PGP 校验功能。

产品版本 V100R001C00SPC310：

1、 更新 Openssl 组件到版本 1.1.0f；

2、 更换 PGPVerify Windows 版本界面图标；

3、 界面改为 Windows7 风格；

4、 退出时增加确认提示。

产品版本 V100R001C00SPC320：

1、 添加 Windows 版本的版本信息；

2、 添加 Windows 版本的时间戳签名。

目 录

1 OpenPGP 简介

OpenPGP 是一个开放式安全协议标准(RFC4880)，广泛应用于数据加密、数字签名。OpenPGP 拥有多个商业和非商业的实现，包括 PGP (Pretty Good Privacy) ，GnuPG (GNU Privacy Guard)等。其中 GnuPG 已被移植到 Linux, Windows 等多种平台上，绝大多数 Linux 发行版本都预装了该工具。

OpenPGP 包含一个独立的数字签名标准。与其他数字签名标准主要的区别在于密钥存储、公钥分发方式，消息摘要的计算过程、签名报文格式和验证过程。

本文介绍了三种验证工具：PGPVerify，GnuPG，Gpg4Win，其中 PGPVerify，Gpg4Win，这两种用于 windows 系统验证，GnuPG 用于 Linux 的验证。推荐使用 GnuPG 或 Gpg4Win 进行验证，在无法获取或者安装这两个软件的情况下可以使用华为公司自研的简易验证工具 PGPVerify 进行验证。

验证工具介绍

在不同的操作系统环境下，可以选用相应的工具完成 OpenPGP 签名的验证，如下表所示。

工具名称	操作系统	工具描述
GnuPG (The GNU Privacy Guard)	Linux	GnuPG 是一款免费开源的 GNU 工具，实现了由 RFC4880 定义的 OpenPGP 标准。 绝大多数 Linux 发行版都已预装。 官方网站：http://www.gnupg.org
Gpg4Win (GNU Privacy Guard for Windows)	Windows	GnuPG 的官方 Windows 版本，两者的功能和使用方法一致。 官方网站：http://www.gpg4win.org/
PGPVerify	Windows	PGPVerify 是一款华为自研的 PGP 简易验证工具。 下载地址： http://support.huawei.com/carrier/digitalSignatureAction

2 公钥文件说明

1. “KEYS.txt”文件为 OpenPGP 密钥长度为 2048 时的公钥文件。“KEYS4096.txt”文件为 OpenPGP 密钥长度为 4096 时的公钥文件。
2. “KEYS4096.txt”相比于“KEYS.txt”，密钥长度有所增加，签名结果长度也发生了相应的增加，安全性有所提高。

说明：运营商下载地址须保留部分用户工具的兼容性，所以KEYS.txt的公钥文件名为KEYS。

3 GnuPG（Linux）

为了防止软件包在传输过程中由于网络原因或者存储设备原因出现下载不完整或者文件破坏的问题，在获取到软件包后，需要对软件包的完整性进行校验，通过了校验的软件包才能部署。

3.1 背景信息

- GnuPG (GNU Privacy Guard) 是一款免费开源的 GNU 工具，该工具可对 SUSE Linux 操作系统下的 OpenPGP 签名进行校验。
- 软件包与签名文件是一一对应并放在同一目录下，一个软件包对应一个校验文件，签名文件由各产品与对应的软件包版本同时发布。
- 签名文件的后缀是“asc”，通常情况下名称和软件包名称相同，即当软件包名称是“V100R001C04.zip”时，对应的校验文件的名称为“V100R001C04.zip.asc”。

3.2 前提条件

3.2.1 GnuPG 安装

绝大多数 Linux 发行版本都预装了 GnuPG 工具。在 shell 中输入 gpg --version 命令，如果看到下面的回显信息，则表明已经安装。

```
signsrv:~ # gpg --version
gpg (GnuPG) 2.0.9
Copyright (C) 2008 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: ~/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA
```

```
Cipher: 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH
Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
Used libraries: gcrypt(1.4.5)
signsrv:~ #
```

如果当前系统没有安装，则可以到 GnuPG 的官方网站（http://www.gnupg.org/），按照网站的指引，完成工具安装。

3.2.2 获取公钥文件

从 Support 获取

- Support 运营商用户下载地址

  http://support.huawei.com/carrier/digitalSignatureAction

  打开网站后，可能显示为中文页面。如果需要英文显示，请单击“English”，切换成英文页面，如图 3-1 所示。解压下载后的压缩包，得到的文件名为“KEYS.txt”或“KEYS4096.txt”的文件即为公钥文件。

图3-1 Support 运营商用户下载地址页面

- Support-E 企业用户下载地址

  http://support.huawei.com/enterprise/zh/tool/software-digital-signature-validation-tool-%EF%BC%88pgp-verify%EF%BC%89-TL1000000054

  打开网站后，可能显示为中文页面。如果需要英文显示，请单击右上角地球标志选择英语，切换成英文页面，如图 3-2 所示。单击版本号，会跳转到文件下载页面。文件名为“KEYS.txt”或“KEYS4096.txt”的文件即为公钥文件。

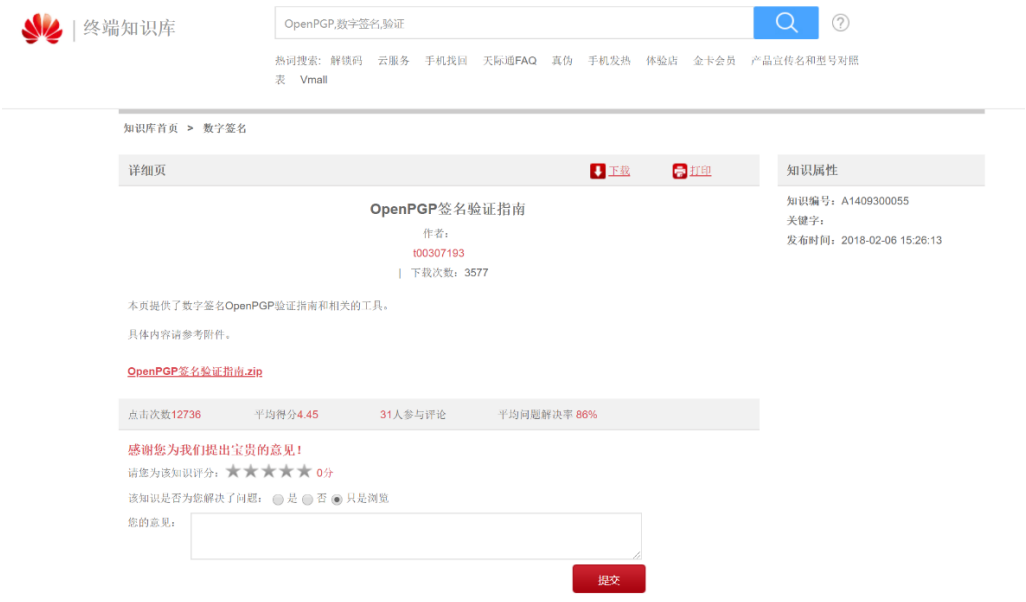
图3-2 Support-E 企业用户下载地址页面

- 终端知识库下载地址
  - 中文
    http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146681
  - 英文
    http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146680

具体操作步骤如下：

步骤 1 根据需要，选择打开对应语言的网站地址。所示是打开地址后的页面。

图3-3 终端知识库下载地址页面



步骤 2 单击“Download”，下载 OpenPGP 的验证指南。

若已有权限，但是打开链接后，页面报错，此时请选择正确的语言页面。

步骤 3 解压下载后的 OpenPGP 验证指南压缩包。

下载后的 OpenPGP 验证指南是压缩包，“KEYS.txt”或“KEYS4096.txt”文件即为公钥文件。

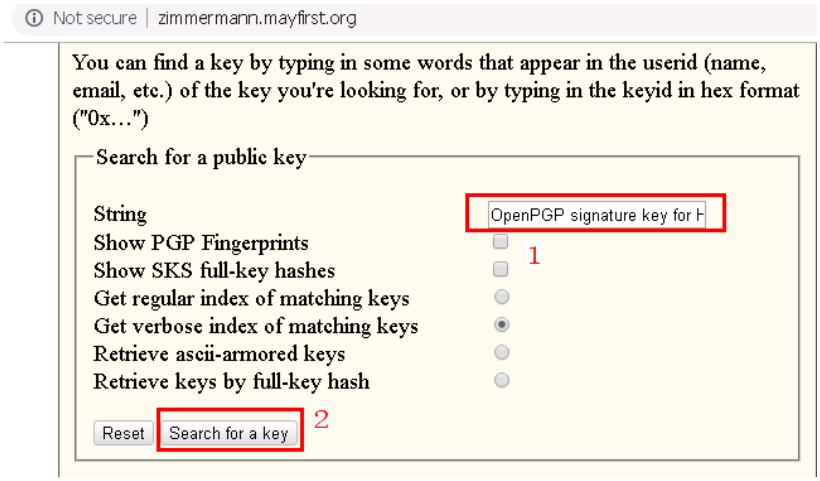
----结束

从公钥服务器获取

步骤 1 访问公钥服务器地址。https://zimmermann.mayfirst.org

界面显示结果如图 3-4 所示。

图3-4 公钥服务器地址页面



在 String 的框内输入“OpenPGP signature key for Huawei software”，然后点击“Search for a key”搜索公钥结果 。

图3-5 公钥服务器搜索结果

步骤 2 单击搜索公钥结果上的公钥 ID“27A74824”，可以查看完整的公钥信息，如图 3-6 所示（如果公钥长度为 4096，则对应 ID 为 6ADE4A56）。

图3-6 完整公钥信息

步骤 3 将公钥信息拷贝至文本文件，保存为“KEYS.txt”文件（如果公钥长度为 4096，则保存为“KEYS4096.txt”文件）。

----结束

3.2.3 导入公钥

步骤 1 以普通用户登录待校验软件包所在服务器。

步骤 2 导入公钥文件，其中“/home/openpgp/keys”是公钥文件“KEYS.txt”所在的路径，请修改为实际路径。

进入 KEYS.txt 公钥文件所在的目录，执行如下命令。

```
# gpg --import "/home/openpgp/keys/KEYS.txt"
```

若签名时选择的OpenPGP密钥长度为4096，公钥文件请选择KEYS4096.txt。

2048 长度的 OpenPGP key 显示：

```
gpg: key 27A74824: public key "OpenPGP signature key for Huawei software (created
on 30th Dec,2013) <support@huawei.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

4096 长度的 OpenPGP key 显示：

```
gpg: key 6ADE4A56: public key "OpenPGP signature key for Huawei software (created
on 15th Jun,2019) <support@huawei.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

注意

命令行中“--import”import 前为两个横杠。

步骤 3 执行如下命令查看公钥导入结果。

```
# gpg --fingerprint
```

如果屏幕显示如下信息，表示导入成功。

2048 长度的 OpenPGP key 显示：

```
pub   2048R/27A74824 2013-12-30
      Key fingerprint = B100 0AC3 8C41 525A 19BD  C087 99AD 81DF 27A7 4824
uid      OpenPGP signature key for Huawei software (created on 30th Dec,2013)
support@huawei.com
```

4096 长度的 OpenPGP key 显示：

```
pub   4096R/6ADE4A56 2019-06-15
      Key fingerprint = E128 5E9D 7E7F 0DB0 A659  48AF FAAA 7A2E 6ADE 4A56
uid    OpenPGP signature key for Huawei software (created on 15th Jun,2019)
<support@huawei.com>
```

注意

命令行中“--fingerprint” fingerprint 前为两个横杠。

----结束

3.2.4 验证公钥

步骤 1 通常情况下，OpenPGP 公钥的合法性需要根据公钥的 ID、指纹、uid 等信息与发布公钥的主体进行合法性验证。华为公司当前对外发布的 OpenPGP 公钥信息如下：

2048 长度的 OpenPGP key 公钥

- 公钥 ID：27A74824
- 公钥指纹(Key fingerprint)：B100 0AC3 8C41 525A 19BD　C087 99AD 81DF 27A7 4824
- 用户 ID(uid)：OpenPGP signature key for Huawei software (created on 30th Dec,2013) support@huawei.com

4096 长度的 OpenPGP key 公钥

- 公钥 ID：6ADE4A56
- 公钥指纹(Key fingerprint)：E128 5E9D 7E7F 0DB0 A659　48AF FAAA 7A2E 6ADE 4A56
- 用户 ID(uid)：OpenPGP signature key for Huawei software (created on 15th Jun,2019) <support@huawei.com>

核实无误后，可以对该公钥设置信任级别。

步骤 2 执行如下命令设置公钥的信任级别。

```
# gpg --edit-key "OpenPGP signature key for Huawei software (created on 30th Dec,2013)" trust
```

设置4096长度的OpenPGP key公钥的信任级别

```
#gpg --edit-key "OpenPGP signature key for Huawei software (created on 15th Jun,2019)" trust
```

屏幕显示类似如下信息，其中粗体部分需要手工输入，“Your decision?”后输入“5”，表示“I trust ultimately”；“Do you really want to set this key to ultimate trust? (y/N)”后输入“y”。

```
gpg (GnuPG) 2.0.9; Copyright (C) 2008 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub  2048R/27A74824  created: 2013-12-30  expires: never      usage: SC
                     trust: ultimate      validity: ultimate
[ultimate] (1). OpenPGP signature key for Huawei software (created on 30th
Dec,2013) <support@huawei.com>

pub  2048R/27A74824  created: 2013-12-30  expires: never      usage: SC
                     trust: ultimate      validity: ultimate
[ultimate] (1). OpenPGP signature key for Huawei software (created on 30th
Dec,2013) <support@huawei.com>

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu

Your decision? 5
Do you really want to set this key to ultimate trust? (y/N) y
```

```
pub  2048R/27A74824  created: 2013-12-30  expires: never      usage: CS
                  trust: ultimate      validity: unknown
[ unknown] (1). OpenPGP signature key for Huawei software (created on 30th
Dec,2013) <support@huawei.com>
Please note that the shown key validity is not necessarily correct
unless you restart the program.
```

注意

命令行中“--edit”edit 前为两个横杠。

步骤 3 执行如下命令退出。

```
quit
```

----结束

3.3 验证签名

签名文件必须与软件包在同一路径下。“/home/openpgp/soft”是签名文件所在的路径，请修改为实际路径。执行如下命令验证签名。

```
# gpg --verify "/home/openpgp/soft/V100R001C041.zip.asc"
```

如果使用 2048 的 key 签名，输出类似如下信息。

```
gpg: Signature made Thu Jan  9 15:29:06 2014 CST using RSA key ID 27A74824
```

gpg: Good signature from "OpenPGP signature key for Huawei software (created on 30th Dec,2013) <support@huawei.com>"其中粗体部分为 27A74824，并且提示中无 WARNING 提示信息时，表明此签名为华为发布的有效签名。

如果使用 4096 的 OpenPGP key 签名，输出类似如下信息。

```
pg: Signature made Mon Dec 30 12:16:07 2019 CST using RSA key ID 6ADE4A56
```

gpg: Good signature from "OpenPGP signature key for Huawei software (created on 15th Jun,2019) <support@huawei.com>"其中粗体部分为 6ADE4A56，并且提示中无 WARNING 提示信息时，表明此签名为华为发布的有效签名。

注意

- 某个版本存在多个需要签名验证的文件时，只有当所有文件的验证结果都为 PASS 时，该版本才是安全。如果验证结果存在 WARNING 或 FAIL，则表示验证未通过，存在安全风险，请参照表 3-1 中处理建议解决。
- 命令行中“--verify”verify 前为两个横杠。

表 3-1 签名验证结果判断示例

验证结果场景	输出信息举例	验证结果	处理建议
签名验证通过，没有异常	gpg: Signature made Thu Jan 9 15:29:06 2014 CST using RSA key ID 27A74824 gpg: Good signature from "OpenPGP signature key for Huawei software (created on 30th Dec,2013) <support@huawei.com>"	PASS	NA
签名验证失败	gpg: Signature made Thu Jan 9 15:29:06 2014 CST using RSA key ID 27A74824 gpg: BAD signature from "OpenPGP signature key for Huawei software (created on 30th Dec,2013) <support@huawei.com>"	FAIL	重新下载目标文件或者联系产品接口人
找不到公钥	gpg: Signature made Thu Jan 9 15:20:01 2014 CST using RSA key ID 27A74824 gpg: Can't check signature: public key not found	FAIL	重新下载公钥，见：获取公钥文件
签名验证通过，但是公钥没有被设置为完全信任	gpg: Signature made Thu Jan 9 15:29:06 2014 CST using RSA key ID 27A74824 gpg: Good signature from "OpenPGP signature key for Huawei software (created on 30th Dec,2013) <support@huawei.com>" gpg: WARNING: This key is not certified with a trusted signature! gpg: There is no indication that the signature belongs to the owner. Primary key fingerprint: B100 0AC3 8C41 525A 19BD C087 99AD 81DF 27A7 4824	WARNING	确认 KeyID 为 27A74824 后，将华为公钥设置为可信，见：验证公钥
找不到对应的源文件	gpg: no signed data gpg: can't hash datafile: No data	FAIL	重新下载目标文件或者联系产品接口人

验证结果场景	输出信息举例	验证结果	处理建议
签名已到期	gpg: Signature made 04/24/13 10:50:29 CST using RSA key ID 133B64E5 gpg: Expired signature from " OpenPGP signature test key <support@huawei.com>" gpg: Signature expired 04/25/13 10:50:29 CST	FAIL	下载更新过签名的目标文件或者联系产品接口人
签名验证通过，但是公钥已被撤销	gpg: Signature made 06/13/13 11:14:49 CST using RSA key ID 133B64E5 gpg: Good signature from " OpenPGP signature test key <support@huawei.com>" gpg: WARNING: This key has been revoked by its owner! gpg: This could mean that the signature is forged. gpg: reason for revocation: Key is no longer used gpg: revocation comment:	WARNING	下载最新公钥和更新了签名的目标文件或者联系产品接口人
源文件找不到对应的签名文件	无	WARNING	下载目标文件对应的签名文件或者联系产品接口人

4 Gpg4Win（Windows）

为了防止软件包在传输过程中由于网络原因或者存储设备原因出现下载不完整或者文件破坏的问题，在获取到软件包后，需要对软件包的完整性进行校验，通过了校验的软件包才能部署

4.1 背景信息

- Gpg4Win (GNU Privacy Guard for Windows)是一款免费开源的 GNU 工具，该工具可对 windows 操作系统下的 OpenPGP 签名进行校验，与 GnuPG 的功能和使用方法一致，官方网站 http://www.gpg4win.org/。
- 软件包与签名文件是一一对应并放在同一目录下，一个软件包对应一个校验文件，签名文件由各产品与对应的软件包版本同时发布。
- 签名文件的后缀是“asc”，通常情况下名称和软件包名称相同，即当软件包名称是“V100R001C04.zip”时，对应的校验文件的名称为“V100R001C04.zip.asc”。

4.2 前提条件

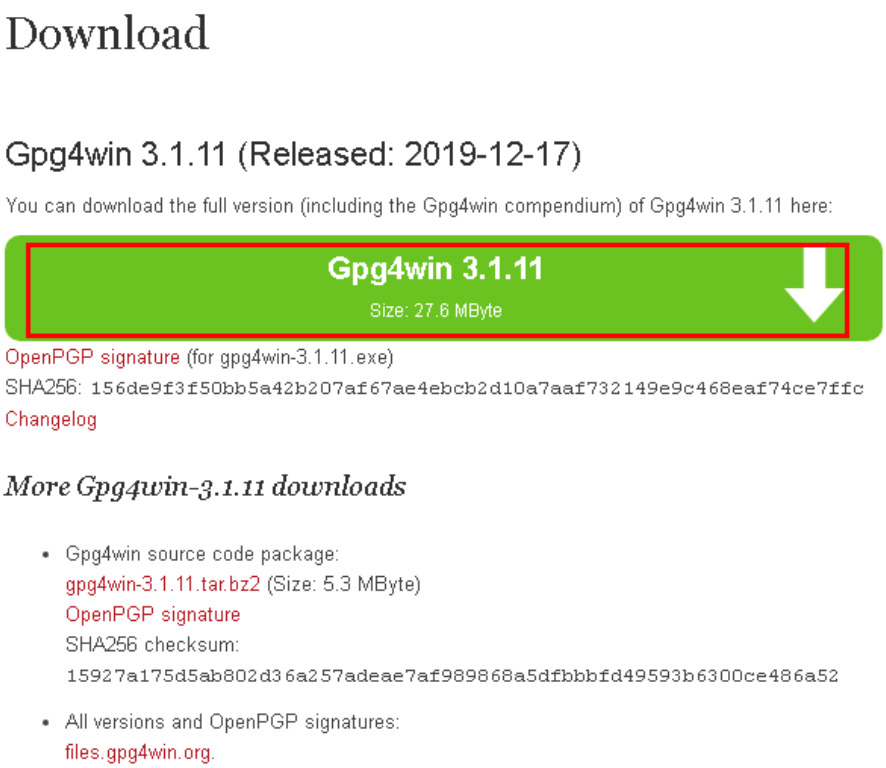
4.2.1 Gpg4Win 安装

首先请按照以下步骤下载安装包：

步骤 1 访问 https://www.gpg4win.org/download.html

步骤 2 点击图 4-1 中红框标记的下载链接（可能最新的版本不是本文档示例中的 3.1.11，但是下载链接不会改变，在后续步骤中可忽略安装包的版本信息）。

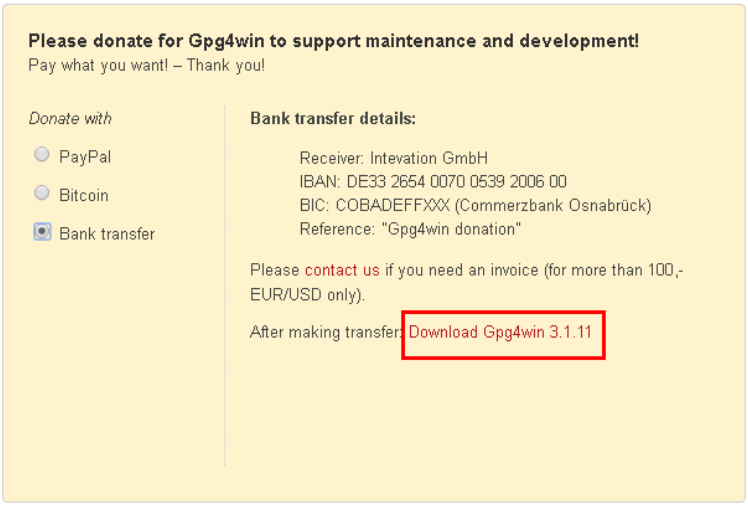
图4-1 Gpg4win 下载步骤 1



步骤 3 选择图 4-2 中红框标记的选项后，点击图 4-3 中红框标记的链接下载。

图4-2 Gpg4Win 下载步骤 2

图4-3 Gpg4Win 下载步骤 3



步骤 4 双击 gpg4win-3.1.11.exe，按照安装向导，默认安装即可。

图4-4 Gpg4Win 安装步骤

步骤 5 查看是否安装成功。

安装完成后，在命令行窗口中，进入程序的默认安装路径 **C:\Program Files (x86)\GNU\GnuPG>**(这个默认安装路径为 x86_64 平台的安装路径，在 x86 平台上的默认安装路径为 **C:\Program Files\GNU\GnuPG>**)，输入 gpg.exe --version，如果看到类似下面的显示，表示安装成功。

图4-5 Gpg4Win 使用向导图

```
D:\Program Files (x86)\GnuPG\bin>gpg --version
gpg (GnuPG) 2.2.19
libgcrypt 1.8.5
Copyright (C) 2019 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: C:/Users/hwx490755/AppData/Roaming/gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

注意

命令行中“--version” version 前为两个横杠。

----结束

4.2.2 获取公钥文件

从 Support 获取

- Support 运营商用户下载地址

  http://support.huawei.com/carrier/digitalSignatureAction

  打开网站后，可能显示为中文页面。如果需要英文显示，请单击“English”，切换成英文页面，如图 4-6 所示。解压下载后的压缩包，得到的文件名为“KEYS.txt”或“KEYS4096.txt”的文件即为公钥文件。

图4-6 Support 运营商用户下载地址页面

- Support-E 企业用户下载地址

  http://support.huawei.com/enterprise/en/tool/software-digital-signature-validation-tool-%EF%BC%88pgp-verify%EF%BC%89-TL1000000054

  打开网站后，可能显示为中文页面。如果需要英文显示，请单击右上角的地球图标，选择英文以切换为英文页面（中文页面提供中文文档下载，英文页面提供英文文档下载），如图 4-7 所示。

图4-7 Support-E 企业用户下载地址页面

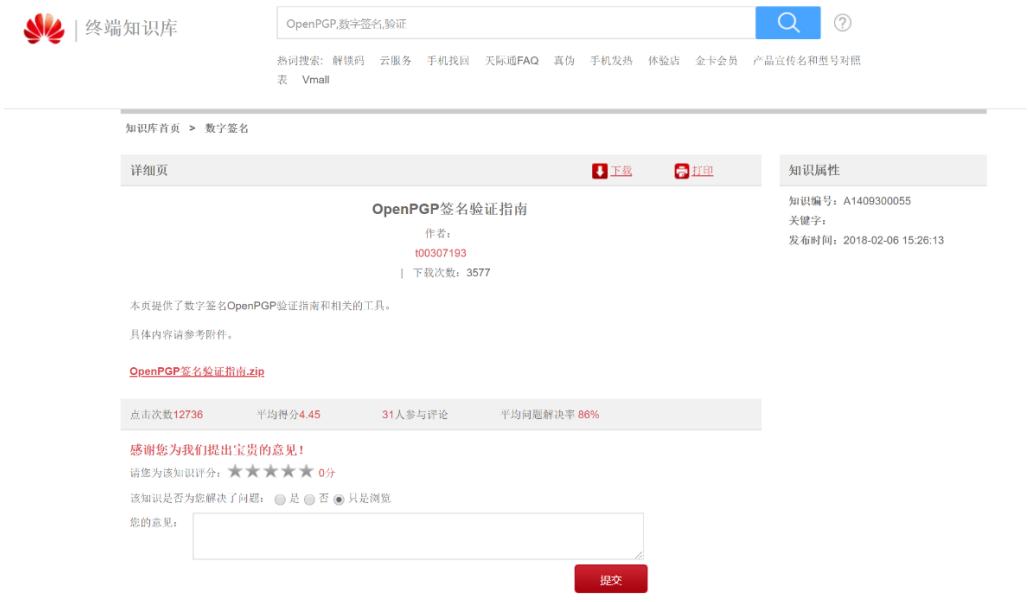
单击版本号，会跳转到文件下载页面。文件名为“KEYS.txt”或“KEYS4096.txt”的文件即为公钥文件。

- 终端知识库下载地址
  - 中文
    http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146681
  - 英文
    http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146680

具体操作步骤如下：

步骤 1 根据需要，选择打开对应语言的网站地址。如图 4-8 所示是打开地址后的页面。

图4-8 终端知识库下载地址页面



步骤 2 单击“Download”，下载 OpenPGP 的验证指南。

若已有权限，但是打开链接后，页面报错，此时请选择正确的语言页面。

步骤 3 解压下载后的 OpenPGP 验证指南压缩包。

下载后的 OpenPGP 验证指南是压缩包，“KEYS.txt”或“KEYS4096.txt”文件即为公钥文件。

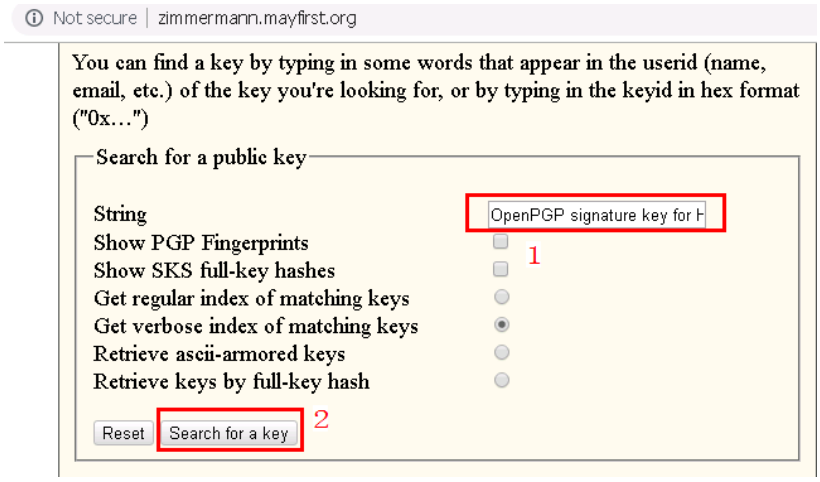
----结束

从公钥服务器获取

步骤 1 访问公钥服务器地址：https://zimmermann.mayfirst.org

界面显示搜索结果如图 4-9 所示。

图4-9 公钥服务器地址页面



在 String 的框内输入“OpenPGP signature key for Huawei software”，然后点击“Search for a key”搜索公钥结果 。

图4-10 公钥服务搜索结果

步骤 2 单击搜索公钥结果上的公钥 ID“27A74824”，可以查看完整的公钥信息，如图 4-11 所示（如果公钥长度为 4096，则对应 ID 为 6ADE4A56）。

图4-11 完整公钥信息

步骤 3 将公钥信息拷贝至文本文件，保存为“KEYS.txt”文件（如果公钥长度为 4096，则保存为“KEYS4096.txt”文件）。

----结束

4.2.3 导入公钥

步骤 1 以管理员用户登录待校验软件包所在服务器，并进入命令行窗口。

步骤 2 执行如下命令导入公钥文件，其中“C:\Users\”是公钥文件“KEYS.txt”所在的路径，请修改为实际路径。

步骤 3 进入 KEYS.txt 公钥文件所在的目录，执行如下命令。

```
gpg --import "C:\Users\KEYS.txt"
```

若签名时选择的OpenPGP密钥长度为4096，公钥文件请选择KEYS4096.txt。

2048 长度的 OpenPGP key 显示：

```
gpg: key 27A74824: public key "OpenPGP signature key for Huawei software (created
on 30th Dec,2013) <support@huawei.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

4096 长度的 OpenPGP key 显示：

```
gpg: key 6ADE4A56: public key "OpenPGP signature key for Huawei software (created
on 15th Jun,2019) <support@huawei.com>" imported
gpg: Total number processed: 1
```

```
gpg:               imported: 1  (RSA: 1)
```

注意

命令行中“--import”import 前为两个横杠。

步骤 4 执行如下命令查看公钥导入结果。

```
gpg --fingerprint
```

如果屏幕显示如下信息，表示导入成功。

2048 长度的 OpenPGP key 显示：

```
pub   2048R/27A74824 2013-12-30
      Key fingerprint = B100 0AC3 8C41 525A 19BD  C087 99AD 81DF 27A7 4824
uid      OpenPGP signature key for Huawei software (created on 30th Dec,2013)
support@huawei.com
```

4096 长度的 OpenPGP key 显示：

```
pub   4096R/6ADE4A56 2019-06-15
      Key fingerprint = E128 5E9D 7E7F 0DB0 A659  48AF FAAA 7A2E 6ADE 4A56
uid    OpenPGP signature key for Huawei software (created on 15th Jun,2019)
<support@huawei.com>
```

注意

命令行中“--fingerprint”fingerprint 前为两个横杠。

----结束

4.2.4 验证公钥

步骤 1 通常情况下，OpenPGP 公钥的合法性需要根据公钥的 ID、指纹、uid 等信息与发布公钥的主体进行合法性验证。华为公司当前对外发布的 OpenPGP 公钥信息如下：

2048 长度的 OpenPGP key 公钥

- 公钥 ID：27A74824
- 公钥指纹(Key fingerprint)：B100 0AC3 8C41 525A 19BD C087 99AD 81DF 27A7 4824

- 用户 ID(uid)：OpenPGP signature key for Huawei software (created on 30th Dec,2013) support@huawei.com

4096 长度的 OpenPGP key 公钥

- 公钥 ID：6ADE4A56
- 公钥指纹(Key fingerprint)：E128 5E9D 7E7F 0DB0 A659　48AF FAAA 7A2E 6ADE 4A56
- 用户 ID(uid)：OpenPGP signature key for Huawei software (created on 15th Jun,2019) <support@huawei.com>

核实无误后，可以对该公钥设置信任级别。

步骤 2 执行如下命令设置公钥的信任级别。

```
gpg --edit-key "OpenPGP signature key for Huawei software (created on 30th Dec,2013)" trust
```

设置4096长度的OpenPGP key公钥的信任级别

```
gpg --edit-key "OpenPGP signature key for Huawei software (created on 15th Jun,2019)" trust
```

屏幕显示类似如下信息，其中粗体部分需要手工输入，“Your decision?”后输入“5”，表示“I trust ultimately”；“Do you really want to set this key to ultimate trust? (y/N)”后输入“y”。

```
gpg (GnuPG) 2.0.9; Copyright (C) 2008 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub  2048R/27A74824  created: 2013-12-30  expires: never      usage: SC
                     trust: ultimate      validity: ultimate
[ultimate] (1). OpenPGP signature key for Huawei software (created on 30th
Dec,2013) <support@huawei.com>

pub  2048R/27A74824  created: 2013-12-30  expires: never      usage: SC
                     trust: ultimate      validity: ultimate
[ultimate] (1). OpenPGP signature key for Huawei software (created on 30th
Dec,2013) <support@huawei.com>

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu
```

```
Your decision? 5
Do you really want to set this key to ultimate trust? (y/N) y

pub  2048R/27A74824  created: 2013-12-30  expires: never       usage: CS
                  trust: ultimate      validity: unknown
[ unknown] (1). OpenPGP signature key for Huawei software (created on 30th
Dec,2013) <support@huawei.com>
Please note that the shown key validity is not necessarily correct
unless you restart the program.
```

注意

命令行中“—edit”edit 前为两个横杠。

步骤 3 执行如下命令退出。

```
quit
```

----结束

4.3 验证签名

签名文件必须与软件包在同一路径下。“C:\Users\”是签名文件所在的路径，请修改为实际路径。执行如下命令验证签名。

```
gpg --verify "C:\Users\V100R001C041.zip.asc"
```

如果使用 2048 的 key 签名，输出类似如下信息。

```
gpg: Signature made Thu Jan  9 15:29:06 2014 CST using RSA key ID 27A74824
```

gpg: Good signature from "OpenPGP signature key for Huawei software (created on 30th Dec,2013) <support@huawei.com>"其中粗体部分为 27A74824，并且提示中无 WARNING 提示信息时，表明此签名为华为发布的有效签名。

如果使用 4096 的 OpenPGP key 签名，输出类似如下信息。

```
gpg: Signature made Mon Dec 30 12:16:07 2019 CST using RSA key ID 6ADE4A56
```

gpg: Good signature from "OpenPGP signature key for Huawei software (created on 15th Jun,2019) <support@huawei.com>"其中粗体部分为 6ADE4A56，并且提示中无 WARNING 提示信息时，表明此签名为华为发布的有效签名。

注意

- 某个版本存在多个需要签名验证的文件时，只有当所有文件的验证结果都为 PASS 时，该版本才是安全。如果验证结果存在 WARNING 或 FAIL，则表示验证未通过，存在安全风险，请参照表 4-1 中处理建议解决。
- 命令行中“--verify”verify 前为两个横杠。

表 4-1 签名验证结果判断示例

验证结果场景	输出信息举例	验证结果	处理建议
签名验证通过，没有异常	gpg: Signature made Thu Jan 9 15:29:06 2014 CST using RSA key ID 27A74824 gpg: Good signature from "OpenPGP signature key for Huawei software (created on 30th Dec,2013) <support@huawei.com>"	PASS	-
签名验证失败	gpg: Signature made Thu Jan 9 15:29:06 2014 CST using RSA key ID 27A74824 gpg: BAD signature from "OpenPGP signature key for Huawei software (created on 30th Dec,2013) <support@huawei.com>"	FAIL	重新下载目标文件或者联系产品接口人
找不到公钥	gpg: Signature made Thu Jan 9 15:20:01 2014 CST using RSA key ID 27A74824 gpg: Can't check signature: public key not found	FAIL	重新下载公钥，见：获取公钥文件
签名验证通过，但是公钥没有被设置为完全信任	gpg: Signature made Thu Jan 9 15:29:06 2014 CST using RSA key ID 27A74824 gpg: Good signature from "OpenPGP signature key for Huawei software (created on 30th Dec,2013) <support@huawei.com>" gpg: WARNING: This key is not certified with a trusted signature! gpg: There is no indication that the signature belongs to the owner. Primary key fingerprint: B100 0AC3 8C41 525A 19BD C087 99AD 81DF 27A7 4824	WARNING	确认 KeyID 为 27A74824 后，将华为公钥设置为可信，见：验证公钥
找不到对应的源文件	gpg: no signed data gpg: can't hash datafile: No data	FAIL	重新下载目标文件或者联系产品接口人

验证结果场景	输出信息举例	验证结果	处理建议
签名已到期	gpg: Signature made 04/24/13 10:50:29 CST using RSA key ID 133B64E5 gpg: Expired signature from " OpenPGP signature test key <support@huawei.com>" gpg: Signature expired 04/25/13 10:50:29 CST	FAIL	下载更新过签名的目标文件或者联系产品接口人
签名验证通过，但是公钥已被撤销	gpg: Signature made 06/13/13 11:14:49 CST using RSA key ID 133B64E5 gpg: Good signature from " OpenPGP signature test key <support@huawei.com>" gpg: WARNING: This key has been revoked by its owner! gpg: This could mean that the signature is forged. gpg: reason for revocation: Key is no longer used gpg: revocation comment:	WARNING	下载最新公钥及更新了签名的目标文件或者联系产品接口人
源文件找不到对应的签名文件	无	WARNING	下载目标文件对应的签名文件或者联系产品接口人

5 PGPVerify（Windows&Linux）

为了防止软件包在传输过程中由于网络原因或者存储设备原因出现下载不完整或者文件破坏的问题，在获取到软件包后，需要对软件包的完整性进行校验，通过了校验的软件包才能部署。

5.1 背景信息

- PGPVerify 是一款华为自研的 PGP 验证工具，运行环境为 Windows 7，Windows Server 2008，Windows 8，以及 Windows 10。
- 软件包与签名文件是一一对应并放在同一目录下，一个软件包对应一个校验文件，签名文件由各产品与对应的软件包版本同时发布。
- 签名文件的后缀是“asc”，通常情况下名称和软件包名称相同，即当软件包名称是“V100R001C04.zip”时，对应的校验文件的名称为“V100R001C04.zip.asc”。

5.2 前提条件

5.2.1 PGP 简易验证工具获取

PGP 简易验证工具无需安装，可直接运行，通过以下三种方式下载。

Support 下载地址

运营商用户下载地址如下：

http://support.huawei.com/carrier/digitalSignatureAction

打开网站后，可能显示为中文页面。如果需要英文显示，请单击“English”，切换成英文页面（中文页面提供中文文档下载，英文页面提供英文文档下载），如图 5-1 所示：

图5-1 Support 运营商用户下载地址页面

具体操作步骤如下：

步骤 1 单击“下载”按钮，下载“OpenPGP 签名验证指南”压缩包，并解压。

步骤 2 继续解压文件夹中的“VerificationTools.zip”。

步骤 3 打开解压后的文件夹“VerificationTools”，可以得到 PGPVerify 验证工具。

----结束

Support-E 下载地址

企业用户下载地址如下：

http://support.huawei.com/enterprise/en/tool/software-digital-signature-validation-tool-%EF%BC%88pgp-verify%EF%BC%89-TL1000000054

打开网站后，可能显示为中文页面。如果需要英文显示，请单击右上角的地球图标，选择英文以切换为英文页面（中文页面提供中文文档下载，英文页面提供英文文档下载），如图 5-2 所示：

图5-2 Supprot-E 企业用户下载地址页面

具体操作步骤如下：

步骤 1 单击列表中的版本号，进入文件下载页面；

步骤 2 选择文件“VerificationTools.zip”，单击下载；

步骤 3 解压下载的压缩包，并打开解压后的文件夹“VerificationTools”，可以得到 PGPVerify 签名验证工具。

----结束

终端知识库下载

下载地址如下：

- 中文

  http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146681

- 英文

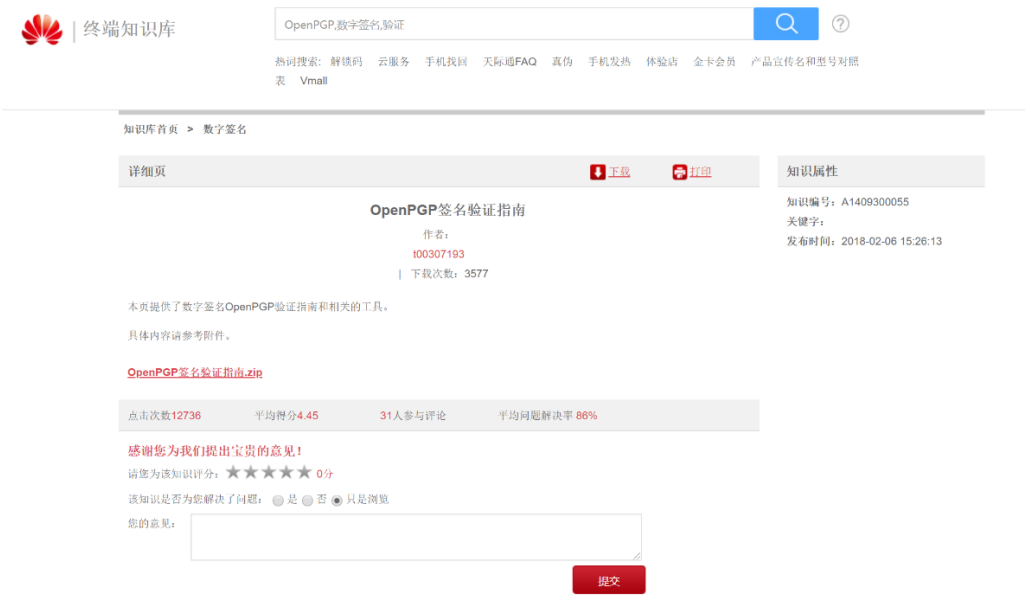
  http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146680

具体操作步骤如下：

步骤 1 根据需要，选择打开对应语言的网站地址（中文地址下载中文文档，英文地址下载英文文档）。

下图所示是打开中文地址后的页面。

图5-3 终端知识库下载地址页面



步骤 2 单击“下载”，下载 OpenPGP 的验证指南；

若已有权限，但是打开链接后，页面报错，此时请选择正确的语言对应页面。

步骤 3　解压下载后的 OpenPGP 验证指南压缩包，得到 PGPVerify 签名验证工具。

----结束

5.2.2 公钥文件获取

从 Support 获取

- Support 运营商用户下载地址

  http://support.huawei.com/carrier/digitalSignatureAction
- Support-E 企业用户下载地址

  http://support.huawei.com/enterprise/zh/tool/software-digital-signature-validation-tool-%EF%BC%88pgp-verify%EF%BC%89-TL1000000054
- 终端知识库下载地址
  - 英文

    http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146680
  - 中文

    http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146681

说明

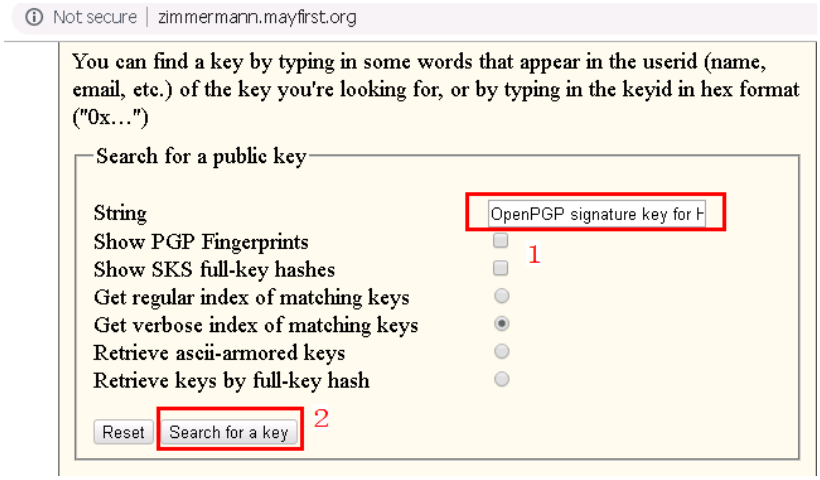
因为验证工具与公钥文件打包在一个文件里，因此下载路径不变；公钥文件名称是“KEYS.txt”“KEYS4096.txt”。

从公钥服务器获取

步骤 1　访问公钥服务器地址。https://zimmermann.mayfirst.org

界面显示结果如图 5-4 所示。

图5-4 公钥服务器地址页面



在 String 的框内输入“OpenPGP signature key for Huawei software”，然后点击“Search for a key”搜索公钥结果 。

图5-5 公钥服务器搜索结果

步骤 2 单击搜索公钥结果上的公钥 ID“27A74824”，可以查看完整的公钥信息，如图 5-6 所示（如果公钥长度为 4096，则对应 ID 为 6ADE4A56）。

图5-6 完整公钥信息

步骤 3 将公钥信息拷贝至文本文件，保存为“KEYS.txt”文件（如果公钥长度为 4096，则保存为“KEYS4096.txt”文件）。

----结束

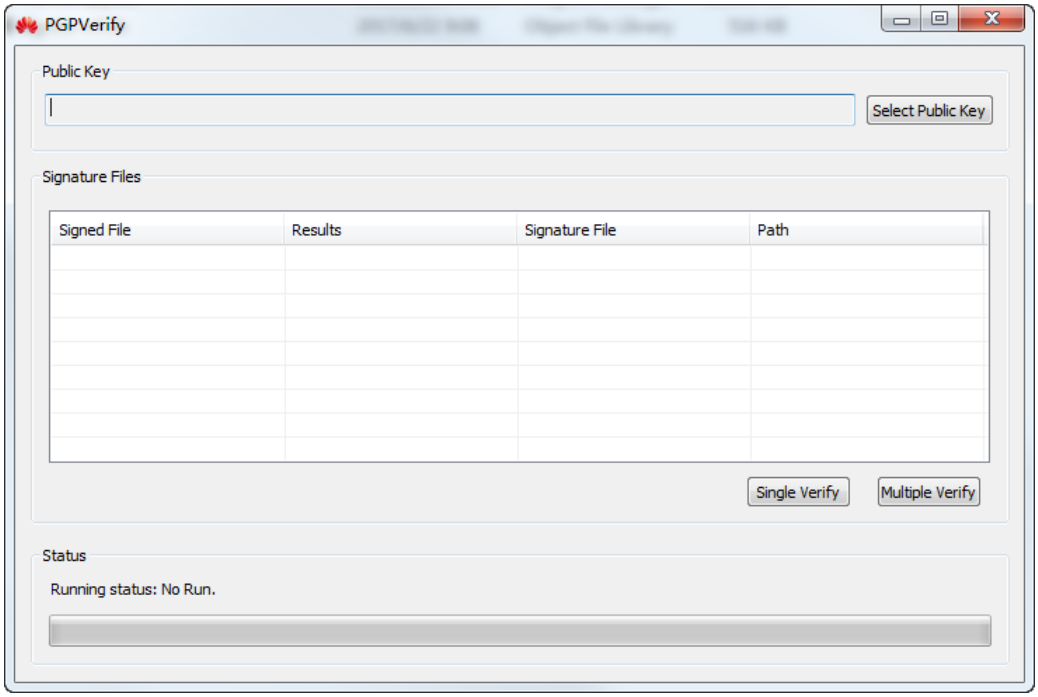
5.3 验证签名

签名文件必须与软件包在同一路径下。例如，“C:\PGP\”是签名文件所在的路径，“C:\”是软件包所在路径，因此必须把签名文件也移动到“C:\”目录下。

5.3.1 通过界面操作验证

步骤 1　双击 PGPVerify.exe 程序，启动验证工具，如图 5-7 所示。

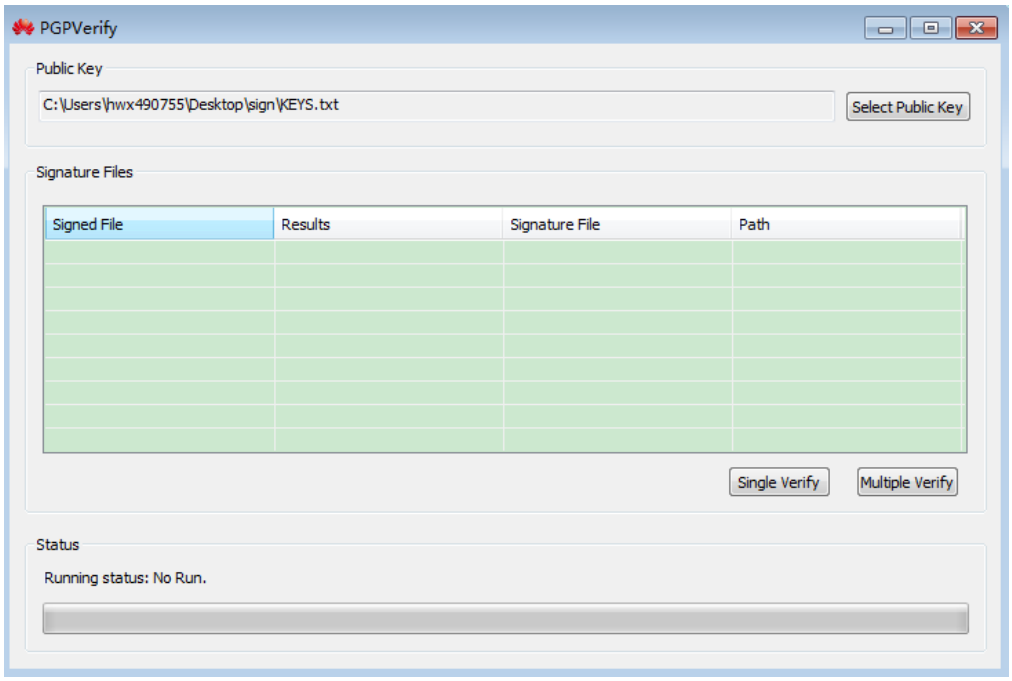
图5-7 PGP 简易验证工具



步骤 2　加载公钥文件。

单击“Select Public Key”选择 5.2.2 章节下载的 KEYS.txt 文件。

图5-8 PGP 简易验证工具加载公钥



若签名时选择的 OpenPGP 密钥长度为 4096，公钥文件请选择 KEYS4096.txt。

如果以前在本机上使用过此验证工具，当再次在本机上使用此工具时，最后一次使用的密钥会自动加载。

步骤 3 验证文件。

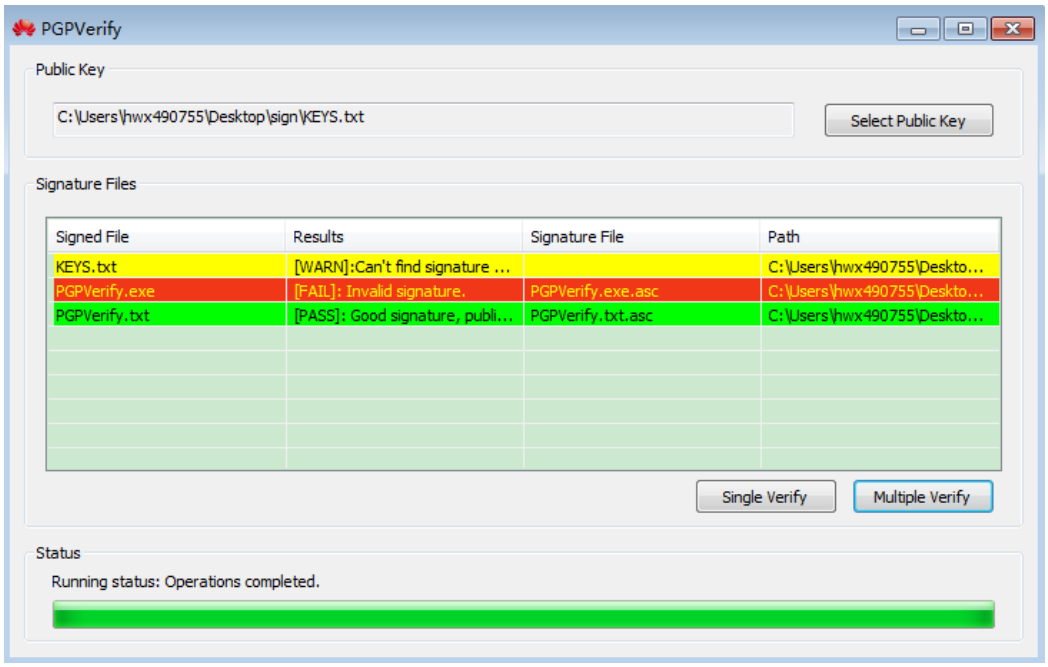
- 验证单个文件

  单击“Single Verify”选择.asc 签名验证文件。

- 验证目录下所有文件

  单击“Multiple Verify”选择“C:\PGP\”目录，验证结果如图 5-9 所示。

图5-9 PGP 简易验证工具验证结果



步骤 4 结果确认。

- 当验证条目为黄色，此条目[Results]栏标记为[WARN]时，表明签名因特定原因无法进行验证。
- 当验证条目为红色，此条目[Results]栏标记为[FAIL]时，表明签名验证失败。
- 当验证条目为绿色，此条目[Results]栏标记为[PASS]时，表明签名使用指定公钥验证通过。
- 当验证条目为绿色，并且[Results]列中显示的 Public key fingerprint 为 B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824 时，则表明此签名文件为华为 OpenPGP 密钥长度为 2048 颁发的有效签名，否则此签名不可信。
- 当验证条目为绿色，并且[Results]列中显示的 Public key fingerprint 为 E128 5E9D 7E7F 0DB0 A659　48AF FAAA 7A2E 6ADE 4A56 时，则表明此签名文件为华为 OpenPGP 密钥长度为 4096 颁发的有效签名，否则此签名不可信。

注意

某个版本存在多个需要签名验证的文件时，只有当所有文件的验证条目都为绿色，[Results]列被标记为[PASS]，并且 Public key fingerprint 均为 **B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824**（OpenPGP 密钥长度为 4096 时，为 **E1285E9D7E7F0DB0A65948AFFAAA7A2E6ADE4A56**）时,才能表明此版本为华为发布的有效软件版本，否则请重新下载软件包。

----结束

5.3.2 通过命令行验证（Windows）

签名文件必须与软件包在同一路径下。例如，“C:\PGP\”是签名文件所在的路径，“C:\”是软件包所在路径，因此必须把签名文件也移动到“C:\”目录下。

步骤 1 验证文件

- 验证单个文件

进入命令行窗口，执行如下命令验证签名（.asc 获取方法请参考“如何获取.asc 文件”）。

```
"C:\PGPVerify.exe" -k "C:\KEYS.txt" -f "C:\PGP\Tecal CH224.zip.asc"
```

C:\KEYS.txt 文件为公钥文件（若签名时选择的 OpenPGP 密钥长度为 4096，公钥文件请选择 KEYS4096.txt），C:\PGP \Tecal CH224.zip.asc 为签名文件。

OpenPGP 密钥长度为 2048 时，屏幕显示类似如下信息：

```
[PASS]:Good Signature. File path: C:\PGP\Tecal CH224.zip.asc, Public key
fingerprint: B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824
[INFO]: Verify Complete.
```

若 OpenPGP 密钥长度为 4096 时，屏幕显示类似如下信息：

```
[PASS]:Good Signature. File path: C:\PGP\Tecal CH224.zip.asc, Public key
fingerprint: E1285E9D 7E7F0DB0 A65948AF FAAA7A2E 6ADE4A56
[INFO]: Verify Complete.
```

- 验证目录下所有文件

进入命令行窗口，执行如下命令验证签名。

```
"C:\PGPVerify.exe" -k "C:\KEYS.txt" -d "C:\PGP"
```

C:\KEYS.txt 为公钥文件（若签名时选择的 OpenPGP 密钥长度为 4096，公钥文件请选择 KEYS4096.txt），C:\PGP 为待验证文件所在目录。

屏幕显示类似如下信息：

```
[INFO]:Filter file in directory, please wait...
[WARN]:Can't find signature file, signed file position: C:\PGP\Tecal CH221.zip.
```

```
[WARN]:Can't find signed file, signature file position: C:\PGP\Tecal CH222.zip.asc.
[FAIL]:Invalid Signature. File path: C:\PGP\Tecal CH223.zip.
[PASS]:Good Signature. File path: C:\PGP\Tecal CH224.zip, Public key fingerprint:
B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824
[INFO]: Verify Complete.
```

步骤 2 结果确认

- 当验证条目标记为[WARN]时，表明此条目签名因特定原因无法进行验证。
- 当验证条目标记为[FAIL]时，表明此条目签名验证失败。
- 当验证条目标记为[PASS]时，表明此条目签名使用指定公钥验证通过。
- 当验证条目标记为[PASS]，并且验证结果中的 Public key fingerprint 为 **B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824** 时，则表明此签名文件为华为 OpenPGP 密钥长度为 2048 颁发的有效签名，否则此签名不可信。
- 当验证条目标记为[PASS]，并且验证结果中的 Public key fingerprint 为 **E128 5E9D 7E7F 0DB0 A659 48AF FAAA 7A2E 6ADE 4A56** 时，则表明此签名文件为华为 OpenPGP 密钥长度为 4096 颁发的有效签名，否则此签名不可信。

注意

某个版本存在多个需要签名验证的文件时，只有当所有文件的验证都标记为[PASS]，并且 Public key fingerprint 均为 **B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824**（OpenPGP 密钥长度为 4096 时，为 **E1285E9D7E7F0DB0A65948AFFAAA7A2E6ADE4A56**）时,才能表明此版本为华为发布的软件版本，否则请重新下载软件包。

5.3.3 通过命令行验证（Linux）

签名文件必须与软件包在一起，例如“/usr1”是签名文件所在的路径，请修改为实际路径。工具和公钥文件可放在其它路径下。在这里，工具和公钥文件也放在“usr1”路径下。

步骤 1 验证文件

- 验证单个文件

执行以下命令以验证单个文件的签名：

```
./PGPVerify -k KEYS.txt -f scw.cab.asc
```

其中 KEYS.txt 为公钥文件（若签名时选择的 OpenPGP 密钥长度为 4096，公钥文件请选择 KEYS4096.txt），scw.cab.asc 为签名文件。

OpenPGP 密钥长度为 2048 时，屏幕显示类似如下信息：

```
[PASS]:Good Signature. File path: scw.cab.asc, Public key fingerprint: 97399A82
CD5D7160 13D181FC 0D7AC54D F0B00048.
```

```
[INFO]: Verify Complete.
```

若 OpenPGP 密钥长度为 4096 时，屏幕显示类似如下信息：

```
[PASS]:Good Signature. File path: scw.cab.asc, Public key fingerprint: E1285E9D
7E7F0DB0 A65948AF FAAA7A2E 6ADE4A56
[INFO]: Verify Complete.
```

- 验证目录下所有文件

例如“openpgp”为所有签名文件以及软件包所在路径，执行以下命令:

```
./PGPVerify -k KEYS.txt -d openpgp
```

其中 KEYS.txt 为公钥文件（若签名时选择的 OpenPGP 密钥长度为 4096，公钥文件请选择 KEYS4096.txt），scw.cab.asc 为待验证文件所在目录。

屏幕显示类似如下信息

```
[INFO]:Filter file in directory, please wait...
[PASS]:Good Signature. File path: openpgp/plugins-cloudtask-C01.zip.asc, Public key
fingerprint: FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[PASS]:Good Signature. File path: openpgp/twain.dll.asc, Public key fingerprint:
FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[PASS]:Good Signature. File path: openpgp/buildcloud-proxy.zip.asc, Public key
fingerprint: FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[PASS]:Good Signature. File path: openpgp/buildcloud_pvmtrans.zip.asc, Public key
fingerprint: FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[PASS]:Good Signature. File path: openpgp/plugins-cicloud-C01.zip.asc, Public key
fingerprint: FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[PASS]:Good Signature. File path: openpgp/ConfigCenter.war.asc, Public key
fingerprint: FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[PASS]:Good Signature. File path: openpgp/watcher-wrapper.zip.asc, Public key
fingerprint: FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[PASS]:Good Signature. File path: openpgp/watcher.zip.asc, Public key fingerprint:
FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[PASS]:Good Signature. File path: openpgp/rpm.war.asc, Public key fingerprint:
FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[PASS]:Good Signature. File path: openpgp/buildcloud-rpm.zip.asc, Public key
fingerprint: FA60975B 1160DF6D 0059662D 2689E7E3 393905AC.
[INFO]: Verify Complete.
```

步骤 2 结果确认

- 当验证条目标记为[WARN]时，表明此条目签名因特定原因无法进行验证。
- 当验证条目标记为[FAIL]时，表明此条目签名验证失败。
- 当验证条目标记为[PASS]时，表明此条目签名使用指定公钥验证通过。
- 当验证条目标记为[PASS]，验证结果中的 Public key fingerprint 为 **B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824** 时，则表明此签名文件为华为 OpenPGP 密钥长度为 2048 颁发的有效签名，否则此签名不可信。

- 当验证条目标记为[PASS]，验证结果中的 Public key fingerprint 为 **E128 5E9D 7E7F 0DB0 A659 48AF FAAA 7A2E 6ADE 4A56** 时，则表明此签名文件为华为 OpenPGP 密钥长度为 4096 颁发的有效签名，否则此签名不可信。

注意

某个版本存在多个需要签名验证的文件时，只有当所有文件的验证都标记为[PASS]，并且 Public key fingerprint 均为 **B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824**（OpenPGP 密钥长度为 4096 时，为 **E1285E9D7E7F0DB0A65948AFFAAA7A2E6ADE4A56**）时,才能表明此版本为华为发布的软件版本，否则请重新获取软件包。

如果步骤一中验证结果出现“Permission denied”错误，请使用 chmod 命令给验证程序添加可执行属性：“chmod u+x PGPVerify”

----结束

6 FAQ

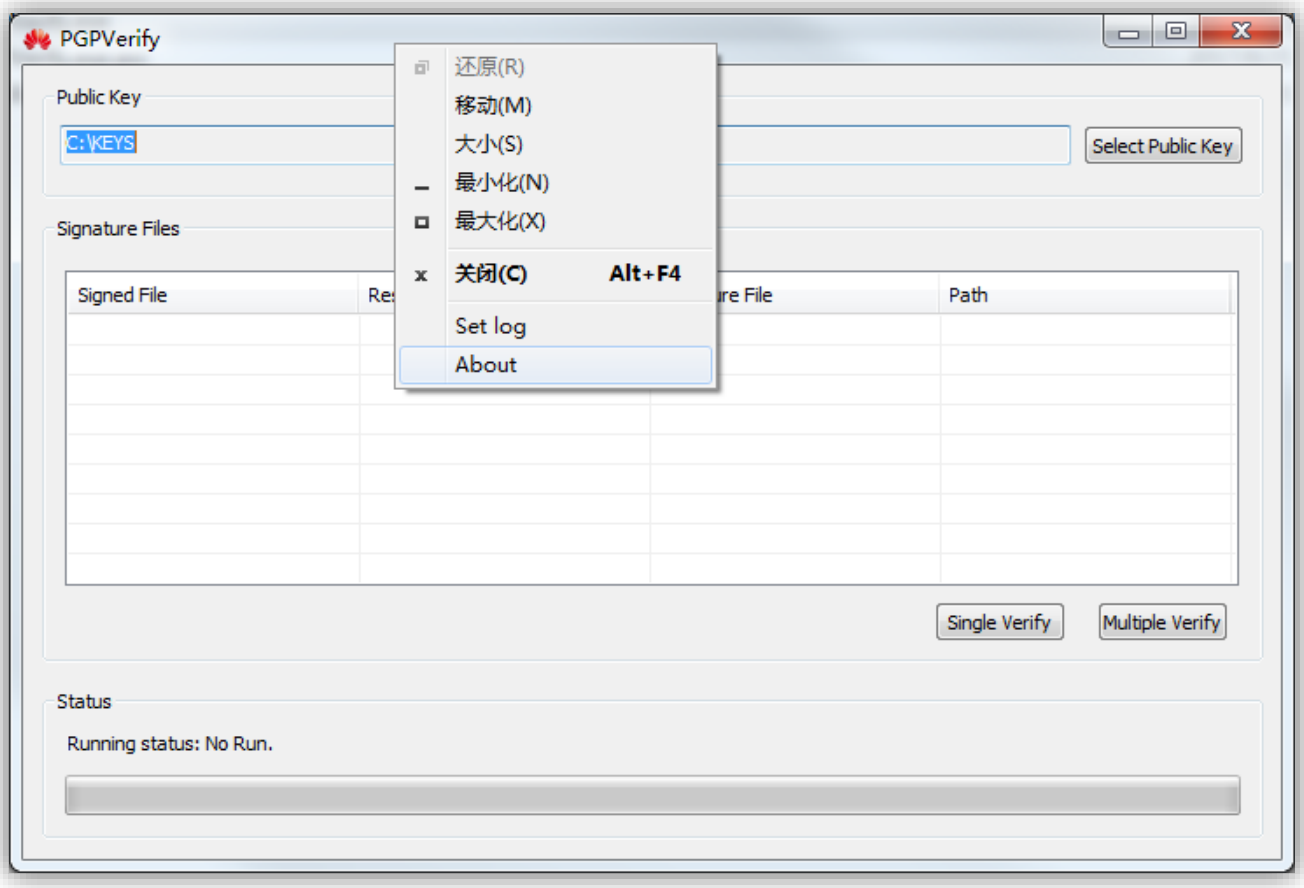
6.1 PGPVerify 验证工具使用场景

PGPVerify 验证工具是华为公司自研的简易验证工具，仅限于一线工程师针对华为版本发布包完整性手工验证，不支持作为一个商用组件集成到产品发布；另外，基于 PGPVerify 的定位，该工具也不会接触用户网络和用户数据。

6.2 PGPVerify 如何查看版本号

- **UI 模式下（适用于 Windows®）：**

1. 右键点击程序标题栏，在菜单中点击 About 菜单：



2. 查看版本：

- **命令行模式下（适用 Windows®和 Linux）：**

1、 输入命令行：

```
PGPVerify -h
```

2、 以 Windows console 为例，显示结果如下（以 V100R001C00SPC310 为例）：

```
PGPVerify library version V100R001C00SPC310
Copyright (c) Huawei Technologies Co., Ltd. 2017. All rights reserved.


Command:
  -k: public key.
  -d: The directory which to be verified.
  -f: The file which to be verified.
  -l: Set log file.


Example:
  PGPVerify -k KEYS -d file-directory
  PGPVerify -k KEYS -f signed-file
```

第一行显示的即为版本号。

- **使用 powershell 提取版本号的方法（仅适用于 Windows®）：**

1、 输入命令行：

```
((.\PGPVerify.exe -h | findstr " V100" | Out-String).split(" ") | findstr V100).remove(0,1).replace("SPC",".").replace("C",".").replace("R",".")
```

注：版本中 V100 是固定的，将来不会有变动，所以可以作为搜索关键字

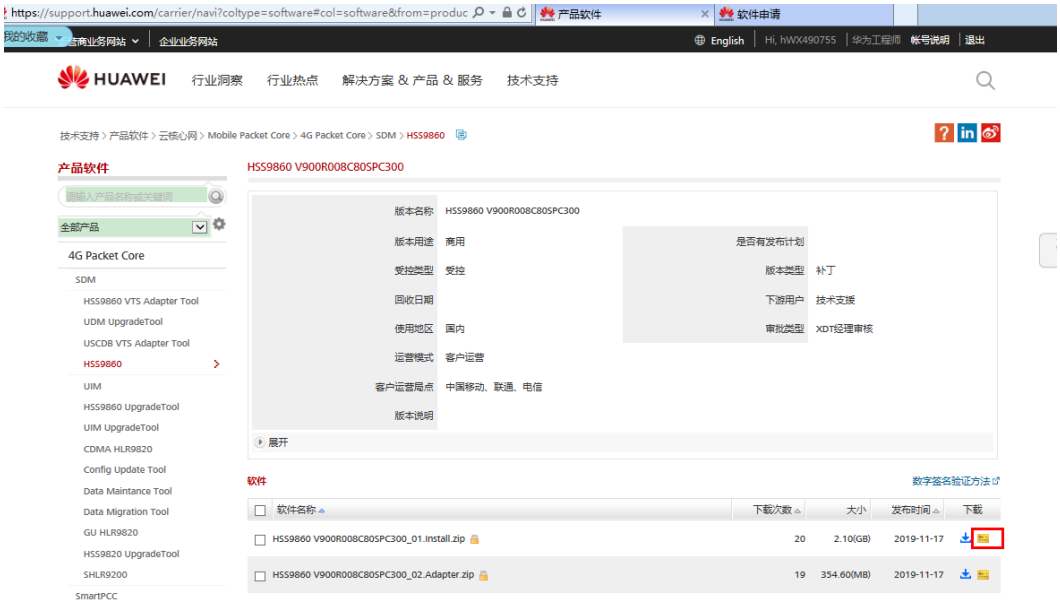
2、 显示结果如下（以 V100R001C00SPC310 为例）：

```
100.001.00.310
```

6.3 如何获取.asc 文件

以 support 为例，找到相关产品软件，如图 6-1 所示：

图6-1 Support 下载.asc 文件



在软件列表中，列出了相关软件产品。单击软件产品对应的“黄色信封”按钮，即可以得到对应的.asc 签名文件。

6.4 如何获取公钥或验证工具

- Support 运营商用户下载地址

  http://support.huawei.com/carrier/digitalSignatureAction

  打开网站后，可能显示为中文页面。如果需要英文显示，请单击“English”，切换成英文页面，如图 6-2 所示。

  解压下载后的“OpenPGP 签名验证指南”压缩包，得到的文件名为“KEYS.txt”或“KEYS4096.txt”的文件即为公钥文件。名称为“VerificationTools.zip”的压缩文件，这个文件就是签名验证工具，解压后得到 PGPVerify 验证工具。

图6-2 Support 运营商用户下载地址页面

- Support-E 企业用户下载地址

  http://support.huawei.com/enterprise/zh/tool/software-digital-signature-validation-tool-%EF%BC%88pgp-verify%EF%BC%89-TL1000000054

打开网站后，可能显示为中文页面。如果需要英文显示，请单击右上角的地球图标，选择英文以切换成英文页面，如图 6-3 所示。

单击版本号，会跳转到文件下载页面。文件名为“KEYS.txt”或“KEYS4096.txt”的文件即为公钥文件。名称为“VerificationTools.zip”为签名验证工具，解压后得到 PGPVerify 验证工具。

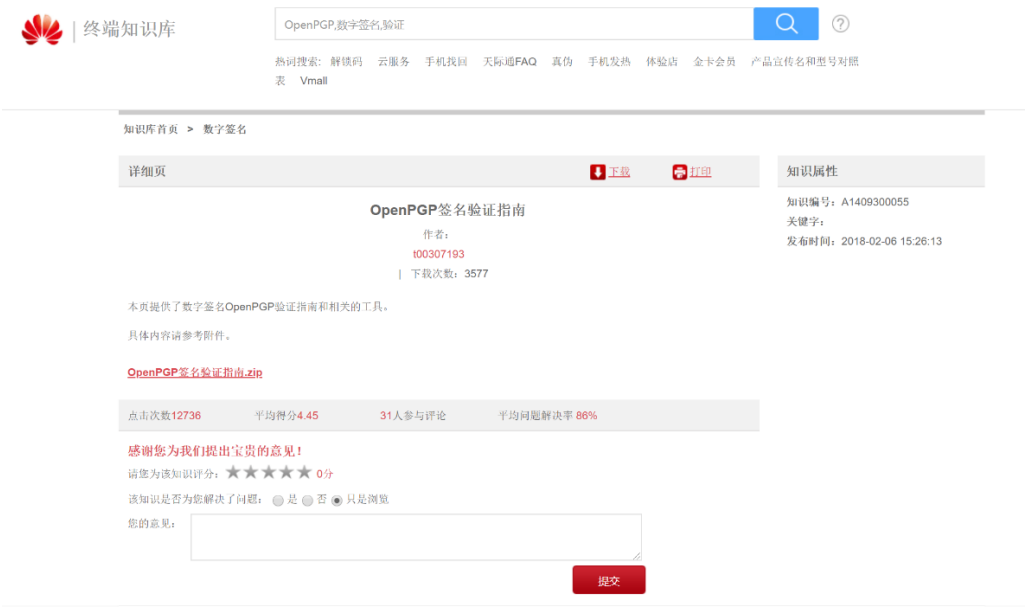
图6-3 Support-E 企业用户下载地址页面

- 终端知识库下载地址
  - 中文
    http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146681
  - 英文
    http://app.huawei.com/tkb/#!tservice/common/base/digit.html?resourceId=146680

具体操作步骤如下：

步骤 1 根据需要，选择打开对应语言的网站地址。如图 6-4 所示是打开地址后的页面。

图6-4 终端知识库下载地址页面



步骤 2 单击“Download”，下载 OpenPGP 的验证指南。

若已有权限，但是打开链接后，页面报错，此时请选择正确的语言页面。

步骤 3 解压下载后的 OpenPGP 验证指南压缩包。

- “KEYS.txt”或“KEYS4096.txt”文件即为公钥文件。
- “VerificationTools.zip”为验证工具。解压后 PGPVerify 验证工具。

----结束

6.5 签名验证的实现原理

签名验证的实现原理为：

- 本文总共提供三种 OpenPGP 的签名验证工具的验证步骤。签名验证需使用原文件及其对应签名文件(以.asc 为后缀的文件)进行验证。
- 公钥文件跟签名验证工具都放在同一下载路径中，在获取验证工具的时候就能够一起得到公钥文件。

6.6 PGPVerify.exe 命令行验证长路径验证失败解决方案

- 假如路径为本地路径，如下所示：

“D:\testfile.txt”

则路径需要添加\\?\前缀：

“\\?\D:\testfile.txt”

例如原始命令行为:

```
PGPVerify.exe -k D:\KEYS.txt -f D:\testfile.txt
```

修改后为:

```
PGPVerify.exe -k \\?\D:\KEYS.txt -f \\?\D:\testfile.txt
```

- 假如路径为网络路径，如下所示：

“\\10.172.12.12\sharedir\testfile.txt”

则路径需要添加\\?\UNC\前缀：

“\\?\UNC\10.172.12.12\sharedir\testfile.txt”

例如原始命令为：

```
PGPVerify -k \\10.172.12.12\sharedir\KEYS.txt -f
\\10.172.12.12\sharedir\testfile.txt
```

修改后命令为：

```
PGPVerify -k \\?\UNC\10.172.12.12\sharedir\KEYS.txt -f
\\?\UNC\10.172.12.12\sharedir\testfile.txt
```

6.7 PGPVerify（Linux）验证工具

此工具满足如下要求：

- 该工具的下载路径以及公钥获取方式与 PGPVerify（Windows）一致。
- 此工具不支持界面方式验证，命令行验证方法与 Windows 下命令行验证方式一致。