lang/python/examples/howto

gpgme.h

gpgme.h
gpgme.h

subprocessgpggpg2gpg.exegpg2.exe

subprocess

gpggpg2

python-gnupggnupg

gpgme.hgpgme.hgpgme.h.in

---

short-historyshort-history.html

```
   $PATH
   $PATHpythonpython3
   pythonpython2python2.7
   python3python3.7python3.6python3.5python3.4
   pythonpython3python2python2

README

makemake checkmake install
   lang/python/python2-gpg/lang/python/python3-gpg/site-packages
   site-packages
   sudo -Hlang/python/

/path/to/pythonX.Y setup.py build
/path/to/pythonX.Y setup.py build
/path/to/pythonX.Y setup.py install

   configuremakemake installsetup.pygpgme.h


     configure--enable-languages=$LANGUAGE
     makegmake-k



   site-packagesgpg/




   $PATH
.exe
```

---

python.org

gpgme.h

gpgme-tool.csrc/

/usr/local/opt/local

sites.pthsite-packages/

virtualenvpython3 -m venvpython3 -m virtualenv /path/to/install/virtual/thingy

```
import gpg

k = gpg.Context().keylist(pattern="258E88DCBD3CD44D8E7AB43F6ECB6AF0DEADBEEF")
keys = list(k)
```

```
import gpg

k = gpg.Context().keylist(pattern="0x6ECB6AF0DEADBEEF")
keys = list(k)
```

```
import gpg

k = gpg.Context().keylist(pattern="0xDEADBEEF")
keys = list(k)
```

```
import gpg

ncsc = gpg.Context().keylist(pattern="ncsc.mil")
nsa = list(ncsc)

pubring.kbxpubring.gpgsecring.gpg

import gpg

c = gpg.Context()
seckeys = c.keylist(pattern=None, secret=True)
pubkeys = c.keylist(pattern=None, secret=False)
```

```
seclist = list(seckeys)
secnum = len(seclist)

publist = list(pubkeys)
pubnum = len(publist)

print("""
  Number of secret keys:  {0}
  Number of public keys:  {1}
""".format(secnum, pubnum))


Context().get_key



import gpg

fingerprint = "80615870F5BAD690333686D0F2AD85AC1E42B367"
key = gpg.Context().get_key(fingerprint)

   secretTrue

import gpg

fingerprint = "DB4724E6FA4286C92B4E55C4321E4E2373590E5D"
key = gpg.Context().get_key(fingerprint, secret=True)



key_import()


import gpg
import os.path
import requests

c = gpg.Context()
url = "https://sks-keyservers.net/pks/lookup"
pattern = input("Enter the pattern to search for key or user IDs: ")
payload = {"op": "get", "search": pattern}

r = requests.get(url, verify=True, params=payload)
result = c.key_import(r.content)

if result is not None and hasattr(result, "considered") is False:
```

```
    print(result)
elif result is not None and hasattr(result, "considered") is True:
    num_keys = len(result.imports)
    new_revs = result.new_revocations
    new_sigs = result.new_signatures
    new_subs = result.new_sub_keys
    new_uids = result.new_user_ids
    new_scrt = result.secret_imported
    nochange = result.unchanged
    print("""
  The total number of keys considered for import was:  {0}

     Number of keys revoked:  {1}
   Number of new signatures:  {2}
      Number of new subkeys:  {3}
     Number of new user IDs:  {4}
  Number of new secret keys:  {5}
   Number of unchanged keys:  {6}

  The key IDs for all considered keys were:
""".format(num_keys, new_revs, new_sigs, new_subs, new_uids, new_scrt,
           nochange))
    for i in range(num_keys):
        print("{0}\n".format(result.imports[i].fpr))
else:
    pass
```

```
   0x0xDEADBEEF
   0ximport-keys-hkp.py
```

```
import gpg
import requests
import sys

print("""
This script searches the ProtonMail key server for the specified key and
imports it.
""")

c = gpg.Context(armor=True)
url = "https://api.protonmail.ch/pks/lookup"
ksearch = []

if len(sys.argv) >= 2:
```

```
    keyterm = sys.argv[1]
else:
    keyterm = input("Enter the key ID, UID or search string: ")

if keyterm.count("@") == 2 and keyterm.startswith("@") is True:
    ksearch.append(keyterm[1:])
    ksearch.append(keyterm[1:])
    ksearch.append(keyterm[1:])
elif keyterm.count("@") == 1 and keyterm.startswith("@") is True:
    ksearch.append("{0}@protonmail.com".format(keyterm[1:]))
    ksearch.append("{0}@protonmail.ch".format(keyterm[1:]))
    ksearch.append("{0}@pm.me".format(keyterm[1:]))
elif keyterm.count("@") == 0:
    ksearch.append("{0}@protonmail.com".format(keyterm))
    ksearch.append("{0}@protonmail.ch".format(keyterm))
    ksearch.append("{0}@pm.me".format(keyterm))
elif keyterm.count("@") == 2 and keyterm.startswith("@") is False:
    uidlist = keyterm.split("@")
    for uid in uidlist:
        ksearch.append("{0}@protonmail.com".format(uid))
        ksearch.append("{0}@protonmail.ch".format(uid))
        ksearch.append("{0}@pm.me".format(uid))
elif keyterm.count("@") > 2:
    uidlist = keyterm.split("@")
    for uid in uidlist:
        ksearch.append("{0}@protonmail.com".format(uid))
        ksearch.append("{0}@protonmail.ch".format(uid))
        ksearch.append("{0}@pm.me".format(uid))
else:
    ksearch.append(keyterm)

for k in ksearch:
    payload = {"op": "get", "search": k}
    try:
        r = requests.get(url, verify=True, params=payload)
        if r.ok is True:
            result = c.key_import(r.content)
        elif r.ok is False:
            result = r.content
    except Exception as e:
        result = None

    if result is not None and hasattr(result, "considered") is False:
        print("{0} for {1}".format(result.decode(), k))
    elif result is not None and hasattr(result, "considered") is True:
```

```
        num_keys = len(result.imports)
        new_revs = result.new_revocations
        new_sigs = result.new_signatures
        new_subs = result.new_sub_keys
        new_uids = result.new_user_ids
        new_scrt = result.secret_imported
        nochange = result.unchanged
        print("""
The total number of keys considered for import was:  {0}

With UIDs wholely or partially matching the following string:

        {1}

   Number of keys revoked:  {2}
 Number of new signatures:  {3}
    Number of new subkeys:  {4}
   Number of new user IDs:  {5}
Number of new secret keys:  {6}
 Number of unchanged keys:  {7}

The key IDs for all considered keys were:
""".format(num_keys, k, new_revs, new_sigs, new_subs, new_uids, new_scrt,
           nochange))
        for i in range(num_keys):
            print(result.imports[i].fpr)
        print("")
    elif result is None:
        print(e)
```

```
import gpg
import hkp4py
import sys

c = gpg.Context()
server = hkp4py.KeyServer("hkps://hkps.pool.sks-keyservers.net")
results = []
keys = []

if len(sys.argv) > 2:
    pattern = " ".join(sys.argv[1:])
```

```
elif len(sys.argv) == 2:
    pattern = sys.argv[1]
else:
    pattern = input("Enter the pattern to search for keys or user IDs: ")


if pattern is not None:
    try:
        key = server.search(hex(int(pattern, 16)))
        keyed = True
    except ValueError as ve:
        key = server.search(pattern)
        keyed = False

    if key is not None:
        keys.append(key[0])
        if keyed is True:
            try:
                fob = server.search(pattern)
            except:
                fob = None
            if fob is not None:
                keys.append(fob[0])
        else:
            pass
    else:
        pass

    for logrus in pattern.split():
        try:
            key = server.search(hex(int(logrus, 16)))
            hexed = True
        except ValueError as ve:
            key = server.search(logrus)
            hexed = False

        if key is not None:
            keys.append(key[0])
            if hexed is True:
                try:
                    fob = server.search(logrus)
                except:
                    fob = None
                if fob is not None:
                    keys.append(fob[0])
```

```
            else:
                pass
        else:
            pass


if len(keys) > 0:
    for key in keys:
        import_result = c.key_import(key.key_blob)
        results.append(import_result)

for result in results:
    if result is not None and hasattr(result, "considered") is False:
        print(result)
    elif result is not None and hasattr(result, "considered") is True:
        num_keys = len(result.imports)
        new_revs = result.new_revocations
        new_sigs = result.new_signatures
        new_subs = result.new_sub_keys
        new_uids = result.new_user_ids
        new_scrt = result.secret_imported
        nochange = result.unchanged
        print("""
The total number of keys considered for import was:  {0}

   Number of keys revoked:  {1}
 Number of new signatures:  {2}
    Number of new subkeys:  {3}
   Number of new user IDs:  {4}
Number of new secret keys:  {5}
 Number of unchanged keys:  {6}

The key IDs for all considered keys were:
""".format(num_keys, new_revs, new_sigs, new_subs, new_uids, new_scrt,
           nochange))
        for i in range(num_keys):
            print(result.imports[i].fpr)
        print("")
    else:
        pass

   keys
```

```
pmkey-import-hkp.py

import gpg
import hkp4py
import os.path
import sys

print("""
This script searches the ProtonMail key server for the specified key and
imports it.

Usage:  pmkey-import-hkp.py [search strings]
""")

c = gpg.Context(armor=True)
server = hkp4py.KeyServer("hkps://api.protonmail.ch")
keyterms = []
ksearch = []
allkeys = []
results = []
paradox = []
homeless = None

if len(sys.argv) > 2:
    keyterms = sys.argv[1:]
elif len(sys.argv) == 2:
    keyterm = sys.argv[1]
    keyterms.append(keyterm)
else:
    key_term = input("Enter the key ID, UID or search string: ")
    keyterms = key_term.split()

for keyterm in keyterms:
    if keyterm.count("@") == 2 and keyterm.startswith("@") is True:
        ksearch.append(keyterm[1:])
        ksearch.append(keyterm[1:])
        ksearch.append(keyterm[1:])
    elif keyterm.count("@") == 1 and keyterm.startswith("@") is True:
        ksearch.append("{0}@protonmail.com".format(keyterm[1:]))
        ksearch.append("{0}@protonmail.ch".format(keyterm[1:]))
        ksearch.append("{0}@pm.me".format(keyterm[1:]))
    elif keyterm.count("@") == 0:
        ksearch.append("{0}@protonmail.com".format(keyterm))
        ksearch.append("{0}@protonmail.ch".format(keyterm))
        ksearch.append("{0}@pm.me".format(keyterm))
```

```
    elif keyterm.count("@") == 2 and keyterm.startswith("@") is False:
        uidlist = keyterm.split("@")
        for uid in uidlist:
            ksearch.append("{0}@protonmail.com".format(uid))
            ksearch.append("{0}@protonmail.ch".format(uid))
            ksearch.append("{0}@pm.me".format(uid))
    elif keyterm.count("@") > 2:
        uidlist = keyterm.split("@")
        for uid in uidlist:
            ksearch.append("{0}@protonmail.com".format(uid))
            ksearch.append("{0}@protonmail.ch".format(uid))
            ksearch.append("{0}@pm.me".format(uid))
    else:
        ksearch.append(keyterm)

for k in ksearch:
    print("Checking for key for: {0}".format(k))
    try:
        keys = server.search(k)
        if isinstance(keys, list) is True:
            for key in keys:
                allkeys.append(key)
                try:
                    import_result = c.key_import(key.key_blob)
                except Exception as e:
                    import_result = c.key_import(key.key)
        else:
            paradox.append(keys)
            import_result = None
    except Exception as e:
        import_result = None
    results.append(import_result)

for result in results:
    if result is not None and hasattr(result, "considered") is False:
        print("{0} for {1}".format(result.decode(), k))
    elif result is not None and hasattr(result, "considered") is True:
        num_keys = len(result.imports)
        new_revs = result.new_revocations
        new_sigs = result.new_signatures
        new_subs = result.new_sub_keys
        new_uids = result.new_user_ids
        new_scrt = result.secret_imported
        nochange = result.unchanged
        print("""
```

```
The total number of keys considered for import was:  {0}

With UIDs wholely or partially matching the following string:

        {1}

   Number of keys revoked:  {2}
 Number of new signatures:  {3}
    Number of new subkeys:  {4}
   Number of new user IDs:  {5}
Number of new secret keys:  {6}
 Number of unchanged keys:  {7}

The key IDs for all considered keys were:
""".format(num_keys, k, new_revs, new_sigs, new_subs, new_uids, new_scrt,
           nochange))
        for i in range(num_keys):
            print(result.imports[i].fpr)
        print("")
    elif result is None:
        pass



homedir


import gpg
import hkp4py
import os.path
import sys

print("""
This script searches the ProtonMail key server for the specified key and
imports it.  Optionally enables specifying a different GnuPG home directory.

Usage:  pmkey-import-hkp.py [homedir] [search string]
   or:  pmkey-import-hkp.py [search string]
""")

c = gpg.Context(armor=True)
server = hkp4py.KeyServer("hkps://api.protonmail.ch")
keyterms = []
ksearch = []
allkeys = []
results = []
```

```
paradox = []
homeless = None

if len(sys.argv) > 3:
    homedir = sys.argv[1]
    keyterms = sys.argv[2:]
elif len(sys.argv) == 3:
    homedir = sys.argv[1]
    keyterm = sys.argv[2]
    keyterms.append(keyterm)
elif len(sys.argv) == 2:
    homedir = ""
    keyterm = sys.argv[1]
    keyterms.append(keyterm)
else:
    keyterm = input("Enter the key ID, UID or search string: ")
    homedir = input("Enter the GPG configuration directory path (optional): ")
    keyterms.append(keyterm)

if len(homedir) == 0:
    homedir = None
    homeless = False

if homedir is not None:
    if homedir.startswith("~"):
        if os.path.exists(os.path.expanduser(homedir)) is True:
            if os.path.isdir(os.path.expanduser(homedir)) is True:
                c.home_dir = os.path.realpath(os.path.expanduser(homedir))
            else:
                homeless = True
        else:
            homeless = True
    elif os.path.exists(os.path.realpath(homedir)) is True:
        if os.path.isdir(os.path.realpath(homedir)) is True:
            c.home_dir = os.path.realpath(homedir)
        else:
            homeless = True
    else:
        homeless = True

# First check to see if the homedir really is a homedir and if not, treat it as
# a search string.
if homeless is True:
    keyterms.append(homedir)
    c.home_dir = None
```

```
else:
    pass

for keyterm in keyterms:
    if keyterm.count("@") == 2 and keyterm.startswith("@") is True:
        ksearch.append(keyterm[1:])
        ksearch.append(keyterm[1:])
        ksearch.append(keyterm[1:])
    elif keyterm.count("@") == 1 and keyterm.startswith("@") is True:
        ksearch.append("{0}@protonmail.com".format(keyterm[1:]))
        ksearch.append("{0}@protonmail.ch".format(keyterm[1:]))
        ksearch.append("{0}@pm.me".format(keyterm[1:]))
    elif keyterm.count("@") == 0:
        ksearch.append("{0}@protonmail.com".format(keyterm))
        ksearch.append("{0}@protonmail.ch".format(keyterm))
        ksearch.append("{0}@pm.me".format(keyterm))
    elif keyterm.count("@") == 2 and keyterm.startswith("@") is False:
        uidlist = keyterm.split("@")
        for uid in uidlist:
            ksearch.append("{0}@protonmail.com".format(uid))
            ksearch.append("{0}@protonmail.ch".format(uid))
            ksearch.append("{0}@pm.me".format(uid))
    elif keyterm.count("@") > 2:
        uidlist = keyterm.split("@")
        for uid in uidlist:
            ksearch.append("{0}@protonmail.com".format(uid))
            ksearch.append("{0}@protonmail.ch".format(uid))
            ksearch.append("{0}@pm.me".format(uid))
    else:
        ksearch.append(keyterm)

for k in ksearch:
    print("Checking for key for: {0}".format(k))
    try:
        keys = server.search(k)
        if isinstance(keys, list) is True:
            for key in keys:
                allkeys.append(key)
                try:
                    import_result = c.key_import(key.key_blob)
                except Exception as e:
                    import_result = c.key_import(key.key)
        else:
            paradox.append(keys)
            import_result = None
```

```
            except Exception as e:
                import_result = None
            results.append(import_result)

        for result in results:
            if result is not None and hasattr(result, "considered") is False:
                print("{0} for {1}".format(result.decode(), k))
            elif result is not None and hasattr(result, "considered") is True:
                num_keys = len(result.imports)
                new_revs = result.new_revocations
                new_sigs = result.new_signatures
                new_subs = result.new_sub_keys
                new_uids = result.new_user_ids
                new_scrt = result.secret_imported
                nochange = result.unchanged
                print("""
        The total number of keys considered for import was:  {0}

        With UIDs wholely or partially matching the following string:

                {1}

           Number of keys revoked:  {2}
         Number of new signatures:  {3}
            Number of new subkeys:  {4}
           Number of new user IDs:  {5}
        Number of new secret keys:  {6}
         Number of unchanged keys:  {7}

        The key IDs for all considered keys were:
        """.format(num_keys, k, new_revs, new_sigs, new_subs, new_uids, new_scrt,
                   nochange))
                for i in range(num_keys):
                    print(result.imports[i].fpr)
                print("")
            elif result is None:
                pass


key_export()key_export_minimal()

import gpg
import os.path
import sys
```

```
print("""
This script exports one or more public keys.
""")

c = gpg.Context(armor=True)

if len(sys.argv) >= 4:
    keyfile = sys.argv[1]
    logrus = sys.argv[2]
    homedir = sys.argv[3]
elif len(sys.argv) == 3:
    keyfile = sys.argv[1]
    logrus = sys.argv[2]
    homedir = input("Enter the GPG configuration directory path (optional): ")
elif len(sys.argv) == 2:
    keyfile = sys.argv[1]
    logrus = input("Enter the UID matching the key(s) to export: ")
    homedir = input("Enter the GPG configuration directory path (optional): ")
else:
    keyfile = input("Enter the path and filename to save the secret key to: ")
    logrus = input("Enter the UID matching the key(s) to export: ")
    homedir = input("Enter the GPG configuration directory path (optional): ")

if homedir.startswith("~"):
    if os.path.exists(os.path.expanduser(homedir)) is True:
        c.home_dir = os.path.expanduser(homedir)
    else:
        pass
elif os.path.exists(homedir) is True:
    c.home_dir = homedir
else:
    pass

try:
    result = c.key_export(pattern=logrus)
except:
    result = c.key_export(pattern=None)

if result is not None:
    with open(keyfile, "wb") as f:
        f.write(result)
else:
    pass

   NoneNone
```

```
import gpg
import os.path
import sys

print("""
This script exports one or more public keys in minimised form.
""")

c = gpg.Context(armor=True)

if len(sys.argv) >= 4:
    keyfile = sys.argv[1]
    logrus = sys.argv[2]
    homedir = sys.argv[3]
elif len(sys.argv) == 3:
    keyfile = sys.argv[1]
    logrus = sys.argv[2]
    homedir = input("Enter the GPG configuration directory path (optional): ")
elif len(sys.argv) == 2:
    keyfile = sys.argv[1]
    logrus = input("Enter the UID matching the key(s) to export: ")
    homedir = input("Enter the GPG configuration directory path (optional): ")
else:
    keyfile = input("Enter the path and filename to save the secret key to: ")
    logrus = input("Enter the UID matching the key(s) to export: ")
    homedir = input("Enter the GPG configuration directory path (optional): ")

if homedir.startswith("~"):
    if os.path.exists(os.path.expanduser(homedir)) is True:
        c.home_dir = os.path.expanduser(homedir)
    else:
        pass
elif os.path.exists(homedir) is True:
    c.home_dir = homedir
else:
    pass

try:
    result = c.key_export_minimal(pattern=logrus)
except:
    result = c.key_export_minimal(pattern=None)

if result is not None:
    with open(keyfile, "wb") as f:
        f.write(result)
```

```
else:
    pass

pinentrygpg-agent


import gpg
import os
import os.path
import sys

print("""
This script exports one or more secret keys.

The gpg-agent and pinentry are invoked to authorise the export.
""")

c = gpg.Context(armor=True)

if len(sys.argv) >= 4:
    keyfile = sys.argv[1]
    logrus = sys.argv[2]
    homedir = sys.argv[3]
elif len(sys.argv) == 3:
    keyfile = sys.argv[1]
    logrus = sys.argv[2]
    homedir = input("Enter the GPG configuration directory path (optional): ")
elif len(sys.argv) == 2:
    keyfile = sys.argv[1]
    logrus = input("Enter the UID matching the secret key(s) to export: ")
    homedir = input("Enter the GPG configuration directory path (optional): ")
else:
    keyfile = input("Enter the path and filename to save the secret key to: ")
    logrus = input("Enter the UID matching the secret key(s) to export: ")
    homedir = input("Enter the GPG configuration directory path (optional): ")

if len(homedir) == 0:
    homedir = None
elif homedir.startswith("~"):
    userdir = os.path.expanduser(homedir)
    if os.path.exists(userdir) is True:
        homedir = os.path.realpath(userdir)
    else:
        homedir = None
else:
```

```
    homedir = os.path.realpath(homedir)

if os.path.exists(homedir) is False:
    homedir = None
else:
    if os.path.isdir(homedir) is False:
        homedir = None
    else:
        pass

if homedir is not None:
    c.home_dir = homedir
else:
    pass

try:
    result = c.key_export_secret(pattern=logrus)
except:
    result = c.key_export_secret(pattern=None)

if result is not None:
    with open(keyfile, "wb") as f:
        f.write(result)
    os.chmod(keyfile, 0o600)
else:
    pass

   .gpg.asc

import gpg
import os
import os.path
import subprocess
import sys

print("""
This script exports one or more secret keys as both ASCII armored and binary
file formats, saved in files within the user's GPG home directory.

The gpg-agent and pinentry are invoked to authorise the export.
""")

if sys.platform == "win32":
    gpgconfcmd = "gpgconf.exe --list-dirs homedir"
else:
```

```
    gpgconfcmd = "gpgconf --list-dirs homedir"

a = gpg.Context(armor=True)
b = gpg.Context()
c = gpg.Context()

if len(sys.argv) >= 4:
    keyfile = sys.argv[1]
    logrus = sys.argv[2]
    homedir = sys.argv[3]
elif len(sys.argv) == 3:
    keyfile = sys.argv[1]
    logrus = sys.argv[2]
    homedir = input("Enter the GPG configuration directory path (optional): ")
elif len(sys.argv) == 2:
    keyfile = sys.argv[1]
    logrus = input("Enter the UID matching the secret key(s) to export: ")
    homedir = input("Enter the GPG configuration directory path (optional): ")
else:
    keyfile = input("Enter the filename to save the secret key to: ")
    logrus = input("Enter the UID matching the secret key(s) to export: ")
    homedir = input("Enter the GPG configuration directory path (optional): ")

if len(homedir) == 0:
    homedir = None
elif homedir.startswith("~"):
    userdir = os.path.expanduser(homedir)
    if os.path.exists(userdir) is True:
        homedir = os.path.realpath(userdir)
    else:
        homedir = None
else:
    homedir = os.path.realpath(homedir)

if os.path.exists(homedir) is False:
    homedir = None
else:
    if os.path.isdir(homedir) is False:
        homedir = None
    else:
        pass

if homedir is not None:
    c.home_dir = homedir
else:
```

```
    pass

if c.home_dir is not None:
    if c.home_dir.endswith("/"):
        gpgfile = "{0}{1}.gpg".format(c.home_dir, keyfile)
        ascfile = "{0}{1}.asc".format(c.home_dir, keyfile)
    else:
        gpgfile = "{0}/{1}.gpg".format(c.home_dir, keyfile)
        ascfile = "{0}/{1}.asc".format(c.home_dir, keyfile)
else:
    if os.path.exists(os.environ["GNUPGHOME"]) is True:
        hd = os.environ["GNUPGHOME"]
    else:
        try:
            hd = subprocess.getoutput(gpgconfcmd)
        except:
            process = subprocess.Popen(gpgconfcmd.split(),
                                       stdout=subprocess.PIPE)
            procom = process.communicate()
            if sys.version_info[0] == 2:
                hd = procom[0].strip()
            else:
                hd = procom[0].decode().strip()
    gpgfile = "{0}/{1}.gpg".format(hd, keyfile)
    ascfile = "{0}/{1}.asc".format(hd, keyfile)

try:
    a_result = a.key_export_secret(pattern=logrus)
    b_result = b.key_export_secret(pattern=logrus)
except:
    a_result = a.key_export_secret(pattern=None)
    b_result = b.key_export_secret(pattern=None)

if a_result is not None:
    with open(ascfile, "wb") as f:
        f.write(a_result)
    os.chmod(ascfile, 0o600)
else:
    pass

if b_result is not None:
    with open(gpgfile, "wb") as f:
        f.write(b_result)
    os.chmod(gpgfile, 0o600)
else:
```

```
    pass
```

hkp4py

```
import gpg
import hkp4py
import os.path
import sys

print("""
This script sends one or more public keys to the SKS keyservers and is
essentially a slight variation on the export-key.py script.
""")

c = gpg.Context(armor=True)
server = hkp4py.KeyServer("hkps://hkps.pool.sks-keyservers.net")

if len(sys.argv) > 2:
    logrus = " ".join(sys.argv[1:])
elif len(sys.argv) == 2:
    logrus = sys.argv[1]
else:
    logrus = input("Enter the UID matching the key(s) to send: ")

if len(logrus) > 0:
    try:
        export_result = c.key_export(pattern=logrus)
    except Exception as e:
        print(e)
        export_result = None
else:
    export_result = c.key_export(pattern=None)

if export_result is not None:
    try:
        try:
            send_result = server.add(export_result)
        except:
            send_result = server.add(export_result.decode())
        if send_result is not None:
            print(send_result)
        else:
            pass
    except Exception as e:
```

```
        print(e)
else:
    pass
```

send-key-to-keyserver.py
hkp4py

```
text
gpg.Context().encrypt()
```

recipientssignTruesinkNonepassphraseNonealways_trustFalseadd_encrypt_toencrypt-to default-keygpg.confFalseprepareFalseexpect_signFalsecompressTrue

```
import gpg

a_key = "0x12345678DEADBEEF"
text = b"""Some text to test with.

Since the text in this case must be bytes, it is most likely that
the input form will be a separate file which is opened with "rb"
as this is the simplest method of obtaining the correct data format.
"""

c = gpg.Context(armor=True)
rkey = list(c.keylist(pattern=a_key, secret=False))
ciphertext, result, sign_result = c.encrypt(text, recipients=rkey, sign=False)

with open("secret_plans.txt.asc", "wb") as afile:
    afile.write(ciphertext)
```

gpg.conf

```
import gpg

a_key = "0x12345678DEADBEEF"

with open("secret_plans.txt", "rb") as afile:
    text = afile.read()

c = gpg.Context(armor=True)
rkey = list(c.keylist(pattern=a_key, secret=False))
ciphertext, result, sign_result = c.encrypt(text, recipients=rkey, sign=True,
                                            always_trust=True,
                                            add_encrypt_to=True)

with open("secret_plans.txt.asc", "wb") as afile:
    afile.write(ciphertext)
```

recipientspassphraseContext()

```
   textgnupg.org

import gpg

text = b"""Oh look, another test message.

The same rules apply as with the previous example and more likely
than not, the message will actually be drawn from reading the
contents of a file or, maybe, from entering data at an input()
prompt.

Since the text in this case must be bytes, it is most likely that
the input form will be a separate file which is opened with "rb"
as this is the simplest method of obtaining the correct data
format.
"""

c = gpg.Context(armor=True)
rpattern = list(c.keylist(pattern="@gnupg.org", secret=False))
logrus = []

for i in range(len(rpattern)):
    if rpattern[i].can_encrypt == 1:
        logrus.append(rpattern[i])

ciphertext, result, sign_result = c.encrypt(text, recipients=logrus,
                                            sign=False, always_trust=True)

with open("secret_plans.txt.asc", "wb") as afile:
    afile.write(ciphertext)

   c.encrypt

ciphertext, result, sign_result = c.encrypt(text, recipients=logrus,
                                            always_trust=True,
                                            add_encrypt_to=True)

   signTruealways_trustFalseadd_encrypt_toFalse
   always_trustTrue

import gpg

with open("secret_plans.txt.asc", "rb") as afile:
```

```
    text = afile.read()

c = gpg.Context(armor=True)
rpattern = list(c.keylist(pattern="@gnupg.org", secret=False))
logrus = []

for i in range(len(rpattern)):
    if rpattern[i].can_encrypt == 1:
        logrus.append(rpattern[i])

    try:
        ciphertext, result, sign_result = c.encrypt(text, recipients=logrus,
                                                    add_encrypt_to=True)
    except gpg.errors.InvalidRecipients as e:
        for i in range(len(e.recipients)):
            for n in range(len(logrus)):
                if logrus[n].fpr == e.recipients[i].fpr:
                    logrus.remove(logrus[n])
                else:
                    pass
        try:
            ciphertext, result, sign_result = c.encrypt(text,
                                                        recipients=logrus,
                                                        add_encrypt_to=True)
            with open("secret_plans.txt.asc", "wb") as afile:
                afile.write(ciphertext)
        except:
            pass



   gpg.Context()gpg.core.Context()cc

import gpg

ciphertext = input("Enter path and filename of encrypted file: ")
newfile = input("Enter path and filename of file to save decrypted data to: ")

with open(ciphertext, "rb") as cfile:
    try:
        plaintext, result, verify_result = gpg.Context().decrypt(cfile)
    except gpg.errors.GPGMEError as e:
        plaintext = None
        print(e)
```

```
if plaintext is not None:
    with open(newfile, "wb") as nfile:
    nfile.write(plaintext)
    else:
        pass
```

```
   plaintextresultverify_result
   gpg.Context().decrypt(cfile, verify=False)verify_resultNone
```

```
import gpg

logrus = input("Enter the email address or string to match signing keys to: ")
hancock = gpg.Context().keylist(pattern=logrus, secret=True)
sig_src = list(hancock)
```

```
   signers
```

```
   gpg.Context().armor
```

```
import gpg

text0 = """Declaration of ... something.

"""
text = text0.encode()

c = gpg.Context(armor=True, signers=sig_src)
signed_data, result = c.sign(text, mode=gpg.constants.sig.mode.NORMAL)

with open("/path/to/statement.txt.asc", "w") as afile:
    afile.write(signed_data.decode())
```

```
import gpg

with open("/path/to/statement.txt", "rb") as tfile:
    text = tfile.read()

c = gpg.Context()
signed_data, result = c.sign(text, mode=gpg.constants.sig.mode.NORMAL)

with open("/path/to/statement.txt.sig", "wb") as afile:
    afile.write(signed_data)
```

```
import gpg

text0 = """Declaration of ... something.

"""
text = text0.encode()

c = gpg.Context(armor=True)
signed_data, result = c.sign(text, mode=gpg.constants.sig.mode.DETACH)

with open("/path/to/statement.txt.asc", "w") as afile:
    afile.write(signed_data.decode())



import gpg

with open("/path/to/statement.txt", "rb") as tfile:
    text = tfile.read()

c = gpg.Context(signers=sig_src)
signed_data, result = c.sign(text, mode=gpg.constants.sig.mode.DETACH)

with open("/path/to/statement.txt.sig", "wb") as afile:
    afile.write(signed_data)



import gpg

text0 = """Declaration of ... something.

"""
text = text0.encode()

c = gpg.Context()
signed_data, result = c.sign(text, mode=gpg.constants.sig.mode.CLEAR)

with open("/path/to/statement.txt.asc", "w") as afile:
    afile.write(signed_data.decode())
```

```
import gpg

with open("/path/to/statement.txt", "rb") as tfile:
    text = tfile.read()

c = gpg.Context()
signed_data, result = c.sign(text, mode=gpg.constants.sig.mode.CLEAR)

with open("/path/to/statement.txt.asc", "wb") as afile:
    afile.write(signed_data)
```

```
import gpg
import time

filename = "statement.txt"
gpg_file = "statement.txt.gpg"

c = gpg.Context()

try:
    data, result = c.verify(open(gpg_file))
    verified = True
except gpg.errors.BadSignatures as e:
    verified = False
    print(e)

if verified is True:
    for i in range(len(result.signatures)):
        sign = result.signatures[i]
        print("""Good signature from:
{0}
with key {1}
made at {2}
""".format(c.get_key(sign.fpr).uids[0].uid, sign.fpr,
           time.ctime(sign.timestamp)))
else:
    pass
```

```
import gpg
import time
```

```
filename = "statement.txt"
asc_file = "statement.txt.asc"

c = gpg.Context()

try:
    data, result = c.verify(open(asc_file))
    verified = True
except gpg.errors.BadSignatures as e:
    verified = False
    print(e)

if verified is True:
    for i in range(len(result.signatures)):
        sign = result.signatures[i]
        print("""Good signature from:
{0}
with key {1}
made at {2}
""".format(c.get_key(sign.fpr).uids[0].uid, sign.fpr,
           time.ctime(sign.timestamp)))
else:
    pass

   data

with open(filename, "rb") as afile:
    text = afile.read()

if text == data:
    print("Good signature.")
else:
    pass

   c.verifydataNoneresult

import gpg
import time

filename = "statement.txt"
sig_file = "statement.txt.sig"

c = gpg.Context()
```

```
try:
    data, result = c.verify(open(filename), open(sig_file))
    verified = True
except gpg.errors.BadSignatures as e:
    verified = False
    print(e)

if verified is True:
    for i in range(len(result.signatures)):
        sign = result.signatures[i]
        print("""Good signature from:
{0}
with key {1}
made at {2}
""".format(c.get_key(sign.fpr).uids[0].uid, sign.fpr,
           time.ctime(sign.timestamp)))
else:
    pass

import gpg
import time

filename = "statement.txt"
asc_file = "statement.txt.asc"

c = gpg.Context()

try:
    data, result = c.verify(open(filename), open(asc_file))
    verified = True
except gpg.errors.BadSignatures as e:
    verified = False
    print(e)

if verified is True:
    for i in range(len(result.signatures)):
        sign = result.signatures[i]
        print("""Good signature from:
{0}
with key {1}
made at {2}
""".format(c.get_key(sign.fpr).uids[0].uid, sign.fpr,
           time.ctime(sign.timestamp)))
else:
    pass
```

```
   SECRET
   gpg.conf

expert
allow-freeform-uid
allow-secret-key-import
trust-model tofu+pgp
tofu-default-policy unknown
enable-large-rsa
enable-dsa2
cert-digest-algo SHA512
default-preference-list TWOFISH CAMELLIA256 AES256 CAMELLIA192 AES192 CAMELLIA128 AES BL
personal-cipher-preferences TWOFISH CAMELLIA256 AES256 CAMELLIA192 AES192 CAMELLIA128 AE
personal-digest-preferences SHA512 SHA384 SHA256 SHA224 RIPEMD160 SHA1
personal-compress-preferences ZLIB BZIP2 ZIP Uncompressed

create_keyuseridalgorithmexpires_inexpiressignencryptcertifyauthenticatepassphrase
forceuseridalgorithmexpires_inexpirespassphraseFalsealgorithmpassphraseNoneexpires_in
0expiresTrueuserid
   passphraseNonepassphrasepassphraseTruepassphraseNone

import gpg

c = gpg.Context()

c.home_dir = "~/.gnupg-dm"
userid = "Danger Mouse <dm@secret.example.net>"

dmkey = c.create_key(userid, algorithm="rsa3072", expires_in=31536000,
                     sign=True, certify=True)

   c.home_dir~/.gnupg
   temp-homedir-config.py
   GenkeyResult

print("""
 Fingerprint:  {0}
 Primary Key:  {1}
  Public Key:  {2}
  Secret Key:  {3}
 Sub Key:  {4}
User IDs:  {5}
""".format(dmkey.fpr, dmkey.primary, dmkey.pubkey, dmkey.seckey, dmkey.sub,
           dmkey.uid))
```

```
bash-4.4$ gpg --homedir ~/.gnupg-dm -K
~/.gnupg-dm/pubring.kbx
-----------------------
sec   rsa3072 2018-03-15 [SC] [expires: 2019-03-15]
      177B7C25DB99745EE2EE13ED026D2F19E99E63AA
uid           [ultimate] Danger Mouse <dm@secret.example.net>

bash-4.4$

   gpg.confgpg.conf

bash-4.4$ gpg --homedir ~/.gnupg-dm --edit-key 177B7C25DB99745EE2EE13ED026D2F19E99E63AA
Secret key is available.

sec  rsa3072/026D2F19E99E63AA
     created: 2018-03-15  expires: 2019-03-15  usage: SC
     trust: ultimate      validity: ultimate
[ultimate] (1). Danger Mouse <dm@secret.example.net>

[ultimate] (1). Danger Mouse <dm@secret.example.net>
     Cipher: TWOFISH, CAMELLIA256, AES256, CAMELLIA192, AES192, CAMELLIA128, AES, BLOWFI
     Digest: SHA512, SHA384, SHA256, SHA224, RIPEMD160, SHA1
     Compression: ZLIB, BZIP2, ZIP, Uncompressed
     Features: MDC, Keyserver no-modify

bash-4.4$

create_subkeyuseridkey


import gpg

c = gpg.Context()
c.home_dir = "~/.gnupg-dm"

key = c.get_key(dmkey.fpr, secret=True)
dmsub = c.create_subkey(key, algorithm="rsa3072", expires_in=15768000,
                        encrypt=True)



print("""
 Fingerprint:  {0}
 Primary Key:  {1}
```

```
  Public Key:  {2}
  Secret Key:  {3}
 Sub Key:  {4}
User IDs:  {5}
""".format(dmsub.fpr, dmsub.primary, dmsub.pubkey, dmsub.seckey, dmsub.sub,
           dmsub.uid))



bash-4.4$ gpg --homedir ~/.gnupg-dm -K
~/.gnupg-dm/pubring.kbx
----------------------
sec   rsa3072 2018-03-15 [SC] [expires: 2019-03-15]
      177B7C25DB99745EE2EE13ED026D2F19E99E63AA
uid           [ultimate] Danger Mouse <dm@secret.example.net>
ssb   rsa3072 2018-03-15 [E] [expires: 2018-09-13]

bash-4.4$


key_add_uidkeyuid

import gpg

c = gpg.Context()
c.home_dir = "~/.gnupg-dm"

dmfpr = "177B7C25DB99745EE2EE13ED026D2F19E99E63AA"
key = c.get_key(dmfpr, secret=True)
uid = "Danger Mouse <danger.mouse@secret.example.net>"

c.key_add_uid(key, uid)



bash-4.4$ gpg --homedir ~/.gnupg-dm -K
~/.gnupg-dm/pubring.kbx
----------------------
sec   rsa3072 2018-03-15 [SC] [expires: 2019-03-15]
      177B7C25DB99745EE2EE13ED026D2F19E99E63AA
uid           [ultimate] Danger Mouse <danger.mouse@secret.example.net>
uid           [ultimate] Danger Mouse <dm@secret.example.net>
ssb   rsa3072 2018-03-15 [E] [expires: 2018-09-13]

bash-4.4$
```

```
key_revoke_uid

import gpg

c = gpg.Context()
c.home_dir = "~/.gnupg-dm"

dmfpr = "177B7C25DB99745EE2EE13ED026D2F19E99E63AA"
key = c.get_key(dmfpr, secret=True)
uid = "Danger Mouse <danger.mouse@secret.example.net>"

c.key_revoke_uid(key, uid)

key_sign
   key_signkeyuidsexpires_inlocaluidsNoneexpires_inlocalFalse
   key
   uidsNone


import gpg

c = gpg.Context()
uid = "Danger Mouse <dm@secret.example.net>"

dmfpr = "177B7C25DB99745EE2EE13ED026D2F19E99E63AA"
key = c.get_key(dmfpr, secret=True)
c.key_sign(key, uids=uid, expires_in=2764800)



import gpg
import time

c = gpg.Context()
dmfpr = "177B7C25DB99745EE2EE13ED026D2F19E99E63AA"
keys = list(c.keylist(pattern=dmuid, mode=gpg.constants.keylist.mode.SIGS))
key = keys[0]

for user in key.uids:
    for sig in user.signatures:
        print("0x{0}".format(sig.keyid), "", time.ctime(sig.timestamp), "",
              sig.uid)


0x92E3F6115435C65A  Thu Mar 15 13:17:44 2018  Danger Mouse <dm@secret.example.net>
0x321E4E2373590E5D  Mon Nov 26 12:46:05 2018  Ben McGinnes <ben@adversary.org>
```

```
import gpg
import math
import pendulum
import time

hd = "/home/dm/.gnupg"
c = gpg.Context()
d = gpg.Context(home_dir=hd)
dmfpr = "177B7C25DB99745EE2EE13ED026D2F19E99E63AA"
dmuid = "Danger Mouse <dm@secret.example.net>"
dkeys = list(c.keylist(pattern=dmuid))
dmkey = dkeys[0]

c.key_import(d.key_export(pattern=None))

tp = pendulum.period(pendulum.now(tz="local"), pendulum.datetime(2019, 1, 1))
ts = tp.total_seconds()
total_secs = math.ceil(ts)
c.key_sign(dmkey, uids=dmuid, expires_in=total_secs)

d.key_import(c.key_export(pattern=dmuid))
keys = list(c.keylist(pattern=dmuid, mode=gpg.constants.keylist.mode.SIGS))
key = keys[0]

for user in key.uids:
    for sig in user.signatures:
        print("0x{0}".format(sig.keyid), "", time.ctime(sig.timestamp), "",
              sig.uid)
```

```
   keycount.pyexamples/howto/
   time

bash-4.4$ time keycount.py

Number of secret keys:  23
Number of public keys:  12112


real 11m52.945s
```

```
user 0m0.913s
sys 0m0.752s

bash-4.4$
```

gpg

```
import gpg

c = gpg.Context()
seckeys = c.keylist(pattern=None, secret=True)
pubkeys = c.keylist(pattern=None, secret=False)

seclist = list(seckeys)
secnum = len(seclist)

publist = list(pubkeys)
pubnum = len(publist)

print("""
    Number of secret keys:  {0}
    Number of public keys:  {1}

""".format(secnum, pubnum))
```

keycount.pyxsetup.py

```
from distutils.core import setup
from Cython.Build import cythonize

setup(
    ext_modules = cythonize("keycount.pyx")
)



bash-4.4$ python setup.py build_ext --inplace
bash-4.4$
```

keycount.py

```
bash-4.4$ time python3.7 -c "import keycount"

Number of secret keys:  23
Number of public keys:  12113
```

```
real 6m47.905s
user 0m0.785s
sys 0m0.331s

bash-4.4$
```

```
   keycount.pyxkeycount.obuild/keycount.cpython-37m-darwin.sokeycount.ckeycount.pyx
keycount.py

   keycount.pyxsetup.pyexamples/howto/advanced/cython/
```

```
import subprocess
import sys

if sys.platform == "win32":
    gpgconfcmd = "gpgconf.exe --list-options gpg"
else:
    gpgconfcmd = "gpgconf --list-options gpg"

process = subprocess.Popen(gpgconfcmd.split(), stdout=subprocess.PIPE)
procom = process.communicate()

if sys.version_info[0] == 2:
    lines = procom[0].splitlines()
else:
    lines = procom[0].decode().splitlines()

for line in lines:
    if line.startswith("group") is True:
        break

groups = line.split(":")[-1].replace('"', '').split(',')

group_lines = []
group_lists = []

for i in range(len(groups)):
    group_lines.append(groups[i].split("="))
    group_lists.append(groups[i].split("="))

for i in range(len(group_lists)):
    group_lists[i][1] = group_lists[i][1].split()
```

```
   group_linesgroup_lines[i][0]group_lines[i][1]
   group_listsgroup_lists[i][0]group_lines[i][0]group_lists[i][1]
   groups.pymutt-groups.pygpg.conf

   hkphttphkpshttps
r.textr.contentgpg.Context().key_import()
   searchhkp4py.KeyServer()key_import

for key in keys:
    if key.revoked is False:
        gpg.Context().key_import(key.key_blob)
    else:
        pass

   hkp4py.KeyServer().search()[i].keyhkp4py.KeyServer().search()
   lang/python/examples/howtoimport-keys-hkp.py

   gpg.version.versionstrgpg.version.versionlistgpgme-config --version


import gpg
import subprocess
import sys

gpgme_version_call = subprocess.Popen(["gpgme-config", "--version"],
                                      stdout=subprocess.PIPE,
                                      stderr=subprocess.PIPE)
gpgme_version_str = gpgme_version_call.communicate()

if sys.version_info[0] == 2:
    gpgme_version = gpgme_version_str[0].strip()
elif sys.version_info[0] >= 3:
    gpgme_version = gpgme_version_str[0].decode().strip()
else:
    gpgme_version = None

if gpgme_version is not None:
    if gpgme_version == gpg.version.versionstr:
        print("The GPGME Python bindings match libgpgme.")
    else:
        print("The GPGME Python bindings do NOT match libgpgme.")
else:
    print("Upgrade Python and reinstall the GPGME Python bindings.")
```

---

hkp4py

```
   gpg.version.versionintlist1.12.1-beta79


import gpg

try:
    if gpg.version.is_beta is True:
        print("The installed GPGME Python bindings were built from beta code.")
    else:
        print("The installed GPGME Python bindings are a released version.")
except Exception as e:
    print(e)

try:
    if gpg.version.versionintlist[0] == 1:
        if gpg.version.versionintlist[1] == 12:
            if gpg.version.versionintlist[2] == 1:
                print("This is the minimum version for using versionintlist.")
            elif gpg.version.versionintlist[2] > 1:
                print("The versionintlist method is available.")
            else:
                pass
        elif gpg.version.versionintlist[1] > 12:
            print("The versionintlist method is available.")
        else:
            pass
    elif gpg.version.versionintlist[0] > 1:
        print("The versionintlist method is available.")
    else:
        pass
except Exception as e:
    print(e)

   passExceptiongpgme.version.is_betagpgme.version.versionintlist
```

```
emacs gpgme-python-howto.org --batch -f org-texinfo-export-to-texinfo --kill
emacs gpgme-python-howto --batch -f org-texinfo-export-to-texinfo --kill


pandoc -f org -t rst+smart -o gpgme-python-howto.rst gpgme-python-howto.org
pandoc -f org -t rst+smart -o gpgme-python-howto.rst gpgme-python-howto


   rst
```