DidiSoft OpenPGP Library for .NET / 1.9

Table of contents

Introduction

This manual describes **DidiSoft OpenPGP Library for .NET**.
The reader is assumed to have a background in Microsoft .NET Framework.

About the Library

DidiSoft OpenPGP Library for .NET is a **pure 100% managed library** with no external dependencies.

The library provides high level functions for OpenPGP encryption, decryption, signing and verification of signed data, clear text signing, one pass signing and encryption, key generation, key signing, key revocation, etc.

Internally the library uses the open source BouncyCastle.NET library.

Installation folder

The **default installation folder** for the library is :

C:\Program Files\OpenPGP Library for .NET 1.7.13

Library contents

After setup the library installation folder contains the following files and subfolders:

\Bin	Library DLL files
\Examples	Example projects (in C# and VB.NET)
\Help	Library API Help files
\License	License agreement
ReleaseNotes.txt	Release notes files
Documentation.pdf	**this file** in PDF format
Documentation.doc	**this file** in doc format (Wordpad, MS Word compatible)

NuGet

Trial Version

PM> Install-Package DidiSoft.Pgp.Trial

Production Version

Private Nuget Repository: (see below how to register it in Visual Studio)
https://repo.didisoft.com/repository/nuget/

The production NuGet feed is only for existing customers. It is protected with username and password. Below are the details that you have to use in order to access the production feed.

Username: your email address used to access DidiSoft customers' section all lowercase
Password: your email address used to access DidiSoft customers' section all lowercase

Uninstall the trial package before installing the production

PM> Uninstall-Package DidiSoft.Pgp.Trial

Install the production package

PM> Install-Package DidiSoft.Pgp

Registering the Private NuGet feed in Visual Studio

In Microsoft Visual Studio *select Tools > NuGet Package Manager > Package Manager Settings*

In the tree view select Package Sources - and add new source with details:
Name: *DidiSoft.Pgp*
Source: *https://repo.didisoft.com/repository/nuget/*

Setup

The library installer will create a folder containing the library DLL files, documentation and examples.

When we install a **production version** or an **updated version** over an **existing installation** (for example the **trial version**), it will usually **overwrite** the library DLL files (which is Ok, as we assume that the production version is preferred over the trial and the updated is better than the old one).

If we wish to **keep the old version files**, we have to **manually copy** them somewhere or **choose a different installation folder** during the setup process.

Deployment

The class library's runtime is royalty free which means it may be freely distributed with your application.

The only files that should be distributed with your application are the class library DLL files.

Alternative way to reference the library DLL files is to place them in the **GAC** (Global Assembly Cache).

To install them in the GAC you can use the command line tool **gacutil** that ships with the .NET Framework SDK.
Below are shown sample executions of gacutil that install the DLL files:

```
gacutil.exe /i DidiSoft.Pgp.dll
gacutil.exe /i BouncyCastle.CryptoExt.dll
```

Switch from Trial to Production version

Please follow these instructions in order to **switch** from the **trial /evaluation/ version** of the library to the **production version** after a successful purchase. The same process should be applied also for **upgrade** to a newer version of the library.

You will receive an order confirmation email with details on how to download the production copy of the library. After installation of the production version there will be **\Bin** folder where the production library DLL files are located. This is usually the same location where the trial version files were installed

Library Files in the application folder (Default setup)

If your project is already referencing the trial version DLL files, then please first delete the old references.

Add a reference to the library DLL files located in the **\Bin** folder of the production installation directory, **rebuild and redeploy** your application.

Library Files installed in the GAC

If you have **installed** the evaluation library DLL files in the **Global Assembly Cache (GAC)**, please first **remove** them from there, and afterwards **install** the production library DLL files

To **check** are there any versions of the DLL files in the GAC you can use the command line tool **gacutil** that ships with .NET Framework SDK

```
gacutil.exe /l DidiSoft.Pgp
gacutil.exe /l BouncyCastle.CryptoExt
```

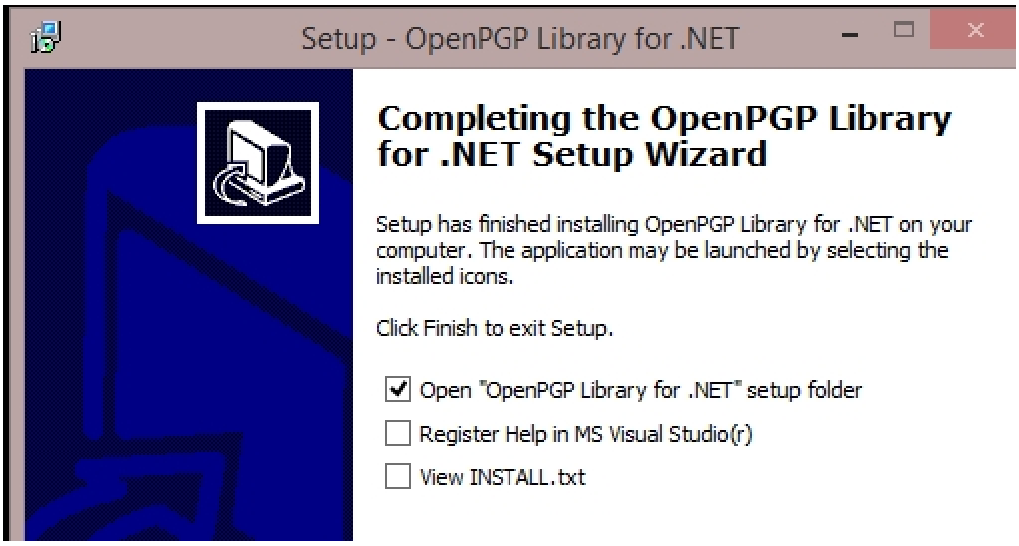
To **remove** the already installed evaluation version you can type:

```
gacutil.exe /u DidiSoft.Pgp
gacutil.exe /u BouncyCastle.CryptoExt
```

The same commands can be use to upgrade to a newer production version.
If you have any trouble with the replacement of the evaluation copy with the production one, do not hesitate to contact us.

Register the help in MS Visual Studio

In previous versions of the installer the help was automatically registered in the help system of the Microsoft Visual Studio IDE.
As of version 1.7.11.8 this is offered as an optional step at the end of the setup wizard:



Setup - OpenPGP Library for .NET

Completing the OpenPGP Library for .NET Setup Wizard

Setup has finished installing OpenPGP Library for .NET on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

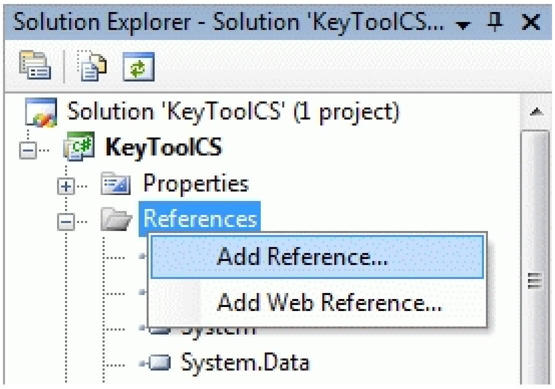
☑ Open "OpenPGP Library for .NET" setup folder
☐ Register Help in MS Visual Studio(r)
☐ View INSTALL.txt

If you have skipped this offering, you can manually run it by executing the batch file:
[setup folder]\Help\Register_Help_VS.bat

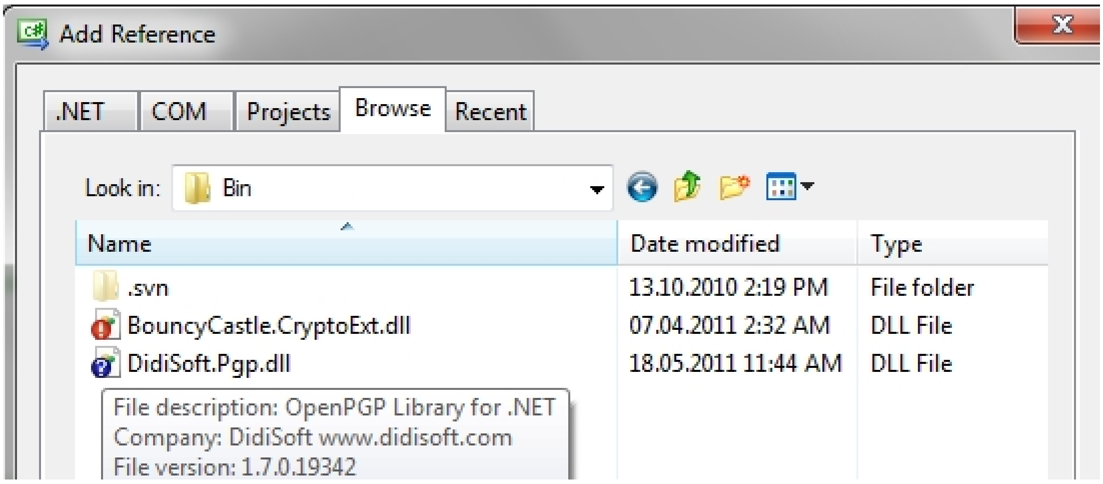
Referencing

To use the class library in **Visual Studio**, you need to add a reference to the class library DLL files from within your project.

With your project open, in the **Solution Explorer** right click the project and click **Add Reference....**



Click the **Browse tab** and browse to the class library DLL files (located in the **Bin** directory where you have installed the library)



Name	Date modified	Type
.svn	13.10.2010 2:19 PM	File folder
BouncyCastle.CryptoExt.dll	07.04.2011 2:32 AM	DLL File
DidiSoft.Pgp.dll	18.05.2011 11:44 AM	DLL File

File description: OpenPGP Library for .NET
Company: DidiSoft www.didisoft.com
File version: 1.7.0.19342

Once the reference has been added you can refer to the various classes from within your project by adding an import directive for the library **namespace**:

C#
using DidiSoft.Pgp;

VB.NET
Imports DidiSoft.Pgp

Library DLL files

OpenPGP Library for .NET DLL Files

The library consists of two DLL files, located at the **Bin** folder in the library installation folder.

They must be **referenced** in your project and **distributed** with your software in order the library to work.

Please check below for more details, how to target different variants of the .NET framework.

.NET Framework 4.0 - 6.0

The library consists of two main .NET DLL files, located within the **Bin** folder in the library installation folder.

For .NET Framework version from 4.0 to 6.0 there are separate folders:

.NET Framework 4.x

1) \Bin\NET4x\DidiSoft.Pgp.dll
2) \Bin\NET4x\DidiSoft.BouncyCastle.dll

LDAP keyserver connectivity

3) \Bin\NET4x\DidiSoft.Pgp.Net.LdapClient.dll

PGP\MIME support

3) \Bin\NET4x\DidiSoft.Pgp.Mail.dll

The above files must be **referenced** in your project and **distributed** with your software in order the library to work.

.NET Framework 5.0

1) \Bin\NET50\DidiSoft.Pgp.dll
2) \Bin\NET50\DidiSoft.BouncyCastle.dll

.NET Framework 6.0

1) \Bin\NET60\DidiSoft.Pgp.dll
2) \Bin\NET60\DidiSoft.BouncyCastle.dll

.NET Framework 2.0 - 3.5

The library consists of two main .NET DLL files, located within the **Bin** folder in the library installation folder.

Targeting **.NET Framework 2.0, 3.0, 3.5**

1) \Bin\NET20\DidiSoft.Pgp.dll
2) \Bin\NET20\DidiSoft.BouncyCastle.dll

and one optional DLL for LDAP keyserver connectivity

(Optional) \Bin\NET20\DidiSoft.Pgp.Net.LdapClient.dll

For **standard managed applications** that will run on **.NET Framework** (including Client profile) the above files must be **referenced** in your project and **distributed** with your software in order the library to work.

.NET Core 1.x, 2.x

.NET Core 1.x and .NET Core 2.x applications reference the library via **NuGet**

Trial Version

Install-Package DidiSoft.Pgp.Trial

Production Version

(Note: for existing customers only)

Install-Package DidiSoft.Pgp

UWP

The library DLL files for Universal Windows Applications are located in the **\Bin\UWP** folder in the library installation folder.

1) \Bin\UWP\DidiSoft.Pgp.dll
2) \Bin\UWP\DidiSoft.BouncyCastle.dll

and one optional DLL for LDAP keyserver connectivity

(Optional) \Bin\UWP\LDAP\DidiSoft.Pgp.Net.LdapClient.dll

Windows 8 WinRT

The library DLL files for Windows 8 WinRT .NET applications are located in the **\Bin\WinRT** folder in the library installation folder.

1) \Bin\WinRT\DidiSoft.Pgp.dll
2) \Bin\WinRT\BouncyCastle.WinRT.dll

due to WinRT platform specifics the above two DLLs do not support file parameters.

StorageFile and Javascript applications support

In addition to the above DLL files you have to include and reference the **.winmd file** mentioned below:

3) \Bin\WinRT\DidiSoft.Pgp.WinRT.winmd

This addional library file can also be used from JavaScript WinRT applications. It exposes a new namespace **DidiSoft.Pgp.WinRT** which provides asynchronous methods that accept paramaters of type Windows.Storage.StorageFile. Its API is available in a separate CHM file : DidiSoft.Pgp.WinRT.chm.

Windows Phone 8

The library DLL files for Windows Phone 8.x applications are located in the **\Bin\WinPhone** folder in the library installation folder.

1) \Bin\WinPhone\DidiSoft.Pgp.WinPhone.dll
2) \Bin\WinPhone\BouncyCastle.WinPhone.dll

Silverlight 3+

The library DLL files for Silverlight applications are located in the **\Bin\Silverlight** folder in the library installation folder.

1) \Bin\Silverlight\DidiSoft.Pgp.Silverlight.dll
2) \Bin\Silverlight\BouncyCastle.Silverlight.dll

Compact Framework 2+

The library DLL files for .NET Compact Framework 2.0 and 3.5 applications are located in the \Bin\Cf20 folder in the library installation folder.

1) \Bin\Cf20\DidiSoft.Pgp.Cf20.dll
2) \Bin\Cf20\BouncyCastle.Cf20.dll

Xamarin

The library DLL files for Xamarinapplications are located in the \Bin\Xamarin.X folder under the library installation folder

Support are Xamarin.iOS, Xamarin.Android, Xamarin.Mac

1) \Bin\Xamarin.X\DidiSoft.Pgp.Android.dll
2) \Bin\Xamarin.X\BouncyCastle.CryptoExt.dll

LDAP Key server access

3) \Bin\Xamarin.X\LDAP\DidiSoft.Pgp.Net.LdapClient.dll

PGP/MIME support

4) \Bin\Xamarin.X\Mail\DidiSoft.Pgp.Mail.dll

Mono

The library DLL files for Mono applications are located in the \Bin\Mono folder under the library installation folder

Supported Mono Version 4.6+

1) \Bin\Xamarin.X\DidiSoft.Pgp.Android.dll
2) \Bin\Xamarin.X\BouncyCastle.CryptoExt.dll

LDAP Key server access

3) \Bin\Xamarin.X\LDAP\DidiSoft.Pgp.Net.LdapClient.dll

PGP/MIME support

4) \Bin\Xamarin.X\Mail\DidiSoft.Pgp.Mail.dll

Upgrade

General rules

The **upgrade process** consists of replacing the library References in your project to point to the new DLL files and **rebuilding** and **redeploying** your application(s).

In most of the cases the upgrade process will be smooth without any code changes as we try to keep **backward compatibility**.

If you encounter compile time errors caused by changes which are not mentioned below, please do not hesitate to contact our techical support for assistance.

From version 1.8 to 1.9.x

.NET Framework

\Bin\NETxx\BouncyCastle.CryptoExt.dll has been renamed to \Bin\NETxx\DidiSoft.BouncyCastle.dll

Windeos Phone 8 applications

1) \Bin\WinPhone\DidiSoft.Pgp.WinPhone.dll has been renamed to \Bin\WinPhone **\DidiSoft.Pgp.dll**
2) \Bin\WinPhone\BouncyCastle.WinPhone.dll has been renamed to \Bin\WinPhone **\DidiSoft.BouncyCastle.dll**

Xamarin.Android

1) \Bin\Xamarin.Android\DidiSoft.Pgp.Android.dll has been renamed to \Bin\Xamarin.Android **\DidiSoft.Pgp.dll**
2) \Bin\Xamarin.Android\BouncyCastle.CryptoExt.dll has been renamed to \Bin\Xamarin.Android **\DidiSoft.BouncyCastle.dll**

Xamarin.iOS

1) \Bin\Xamarin.iOS\DidiSoft.Pgp.iOS.dll has been renamed to \Bin\Xamarin.iOS\DidiSoft.Pgp.dll
2) \Bin\Xamarin.iOS\BouncyCastle.CryptoExt.dll has been renamed to \Bin\Xamarin.iOS **\DidiSoft.BouncyCastle.dll**

UWP

1) \Bin\UWP\BouncyCastle.UWP.dll has been renamed to \Bin\UWP\DidiSoft.BouncyCastle.dll

From version 1.8.1

0) User **DidiSoft.Pgp.PGPLibAsync** instead of DidiSoft.Pgp.Async.PGPLib

1) Xamarin.Android Projects

Reference \Bin\Xamarin.Android\BouncyCastle.CryptoExt.dll instead of \Bin\Xamarin.Android **\BouncyCastle.Android.dll**

2) Xamarin.iOS Projects

Reference \Bin\Xamarin.Android\BouncyCastle.iOS.dll instead of \Bin\Xamarin.Android

BouncyCastle.iOS.dll

3) .NET Core Projects

Reference \Bin\Core\BouncyCastle.CryptoExt.dll instead of \Bin\Core\BouncyCastle.Core.dll

From version 1.7.x to 1.8

Version 1.8 of the library references version 1.8 of the BouncyCastle crypto library.

Windows Phone

Version 1.8 offers DLLs only for Windows Phone 8 apps. If you still have to support Windows Phone 7 apps you have to stick with the DLLs from version 1,7.x

UWP and .NET Core

Additional DLL files have been added for the new .NET Framework additions - Universal Windows Platform (UWP) and .NET Core.

Asynchronous operations

Also the DLL files for .NET Framework 4.5.x now offer asynchronous operations in the namespace DidiSoft.Pgp.Async

From version 1.7.12

The library setup folder has been changed on 64 bit machines to be in *Program Files*\.

The main DLL files are now available for .NET Framework 2.0 - 3.5 under:
Setup folder/Bin/NET20/

and for .NET Framework 4.+ under:
Setup folder/Bin/NET40/

From version 1.7.9

This migraton step is needed only if you are using the LDAP keyserver connectivity features.

1) Add an additional reference to
\Bin\DidiSoft.Pgp.Net.LdapClient.dll

From version 1.7.7.5

The migration is needed ONLY for Windows 8 WinRT applications.

1) Replace your old references as follows
\Bin\WinRT\DidiSoft.Pgp.WinRT.dll -> \Bin\WinRT\DidiSoft.Pgp.dll
\Bin\WinRT\DidiSoft.Pgp.WinJS.winmd -> \Bin\WinRT\DidiSoft.Pgp.WinRT.winmd

2) Change everywhere:
using DidiSoft.Pgp.WinJS;
to
using DidiSoft.Pgp.WinRT;

From version 1.7.4

In version 1.7.5 the method

```
public void EncryptFile(
        string dataFileName,
        byte[][] publicKeysBytes,
        string outputFileName,
        bool asciiArmor,
        bool withIntegrityCheck
)
```

of the DidiSoft.Pgp.**PGPLib** class was **removed**.

Please use the method that accepts array of Streams instead, for example by converting each key bytes into a **System.IO.MemoryStream** object.

From version 1.6

In order to migrate from version 1.6, please perform the following steps:

1) Replace **PGPLib.dll** with **DidiSoft.Pgp.dll** (See section Add a reference)
2) Replace **BouncyCastle.CryptoExt.dll** with the one from this version (See section Add a reference)
3) Change the **namespace** in your code from **DidiSoft** to **DidiSoft.Pgp**

GAC
If you have installed previously version 1.6 in the Global Assembly Cache (GAC) please remove it with these commands:

To **check** are there any versions of the DLL file:
gacutil.exe /l PGPLib

To **remove** if there is an old version there**:**
gacutil.exe /u PGPLib

If you have any trouble with the upgrade, please drop us a line.

Examples

All the examples below are available online at our web site:
http://www.didisoft.com/examples/net-pgp-example/

and as Visual Studio solutions located in the **Examples** folder within the library ZIP package.

Online

Introduction

Introduction to OpenPGP
Setup
Getting started with the Library
Exception handling guidelines

Main functions

Encrypting
Decrypting
Signing
Verifying
Signing and Encrypting in one pass
Decrypting and Verifying in one pass
Clear text signing
Detached signing

Keys and KeyStore

KeyStore basics
Properties of a key
Generating RSA keys
Generating DH/DSS keys
Generating ECC keys (New!)
Exporting from a KeyStore
Importing into a KeyStore
Changing key's password
Deleting key from a KeyStore

Analyzing OpenPGP archives

Analyzing OpenPGP archives

OpenPGP Mail

Sending OpenPGP Email messages

Preferences

Set preferred cypher (symmetric key algorithm)
Set preferred compression
Set preferred hashing
Content type
ASCII armored header

Key revocation

Key revocation basics
Direct key revocation
Using a revocation certificate
Using a designated revoker

Logging

Logging internal verbose information

WinRT development

WinRT development guide

Miscellaneous

Creating SFX executables
Encrypting with a key and an additional password
Using X.509 certificates as OpenPGP keys
JPEG photo images in OpenPGP keys

Haven't found an example or detail you were looking for?
Just drop us a line and we will send you a code snippet and a thorough explanation.

Example Applications

The class library ships with an example applications located in the **Examples** folder in the distribution package. You will need to rebuild the applications prior to running them. Below is a list with a short description of these applications:

PGPLibExampleCS – console examples in C#
PGPLibExampleVB – console examples in VB.NET

FileToolCS – WinForms C# application demonstrating the basic functions for OpenPGP archives
FileToolVB – WinForms VB.NET application demonstrating the basic functions for OpenPGP archives

KeyToolCS – WinForms C# application demonstrating operations with OpenPGP keys and the library KeyStore object
KeyToolVB – WinForms VB.NET application demonstrating operations with OpenPGP keys and the library KeyStore object

Appendix

Common Exceptions

As of version 1.7.5 the **DidiSoft.Pgp.Exceptions** namespace contains a full set of sub classes of DidiSoft.Pgp.PGPException that indicate the cause of the error.

Exporting keys from a GnuPG keystore

List key's in GnuPG keystore:

```
gpg --list-keys
```

Generate OpenPGP key pair

```
gpg --gen-key
```

Export Public key

```
gpg --export my_key -o my_public_key.gpg
```

Export Private key

```
gpg --export-secret-key my_key -o my_secret_key.gpg
```

Licensing

The End User **License Agreement** for DidiSoft OpenPGP Library for .NET / 1.9 is located in the folder **\License** in the file **EULA.rtf**.

The production version of the library can be distributed **royalty free without limitation** in binary form.

BouncyCastle license

DidiSoft OpenPGP Library for .NET / 1.9 uses the BouncyCastle cryptographic library which comes with a separate license: **The BouncyCastle License** which is contained in the folder **License\BC\**. The BouncyCastle License is an adaptation of the **MIT X11 License** and refers only to the BouncyCastle library and it's documentation and gives you the right to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the BouncyCastle library and it's documentation.

Support

Technical support

To receive general information or **technical support**, please contact us at support@didisoft.com.

Sales

For questions related to **sales**, volume licensing, or OEM licensing, please contact us at sales@didisoft.com.

Updates

If you have purchased the library you can access our Customers' Portal where you can **download new versions**.

Newsletter

To receive product **update news** you can subscribe to our Newsletter

For further information, visit us at www.didisoft.com

If you have any **ideas**, **wishes**, **questions** or **criticism**, don't hesitate to contact us.
We will be glad to hear from you.