

A close up of a sign

Description automatically generated

**คู่มือการใช้งานสำหรับนักพัฒนาระบบ  
PAdES Signer (.NET)**

**โครงการ จ้างที่ปรึกษาเพื่อบริหารโครงการปรับเปลี่ยนบริการภาครัฐที่เกี่ยวกับการออกใบอนุญาต หรือหลักฐานสำคัญ ให้เป็นดิจิทัล ด้วยมาตรฐานที่จำเป็น**

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

23 เมษายน 2564



Strategy Consulting & Digital Transformation

**บริษัท ฟรอนทิส จำกัด**

สารบัญ

[การกำหนดค่าสำหรับ Library 3](#_Toc70075274)

[1. Environment และ Software ที่เกี่ยวข้อง 3](#_Toc70075275)

[2. การกำหนด Dependencies 3](#_Toc70075276)

[ข้อมูลรายละเอียด Library 4](#_Toc70075277)

[1. Class and method 4](#_Toc70075278)

[การใช้งานและการ Deploy library 9](#_Toc70075279)

[1. การเตรียม Project 9](#_Toc70075280)

[2. การเรียกใช้งานสำหรับการทดสอบ (Debug) 10](#_Toc70075281)

[5. การ Deploy library (Release exe) 11](#_Toc70075282)

[การเรียกใช้งานผ่าน Command-line interface 12](#_Toc70075283)

[1. รายละเอียด Argument 12](#_Toc70075284)

[2. ตัวอย่างการเรียกใช้งาน 14](#_Toc70075285)

# การกำหนดค่าสำหรับ Library

## Environment และ Software ที่เกี่ยวข้อง

Library นี้พัฒนาด้วยภาษา .NET ซึ่งมี environment และ software ที่จำเป็นในการใช้พัฒนา ดังนี้

1. NET Framework 3.5
2. Visual Studio 2019

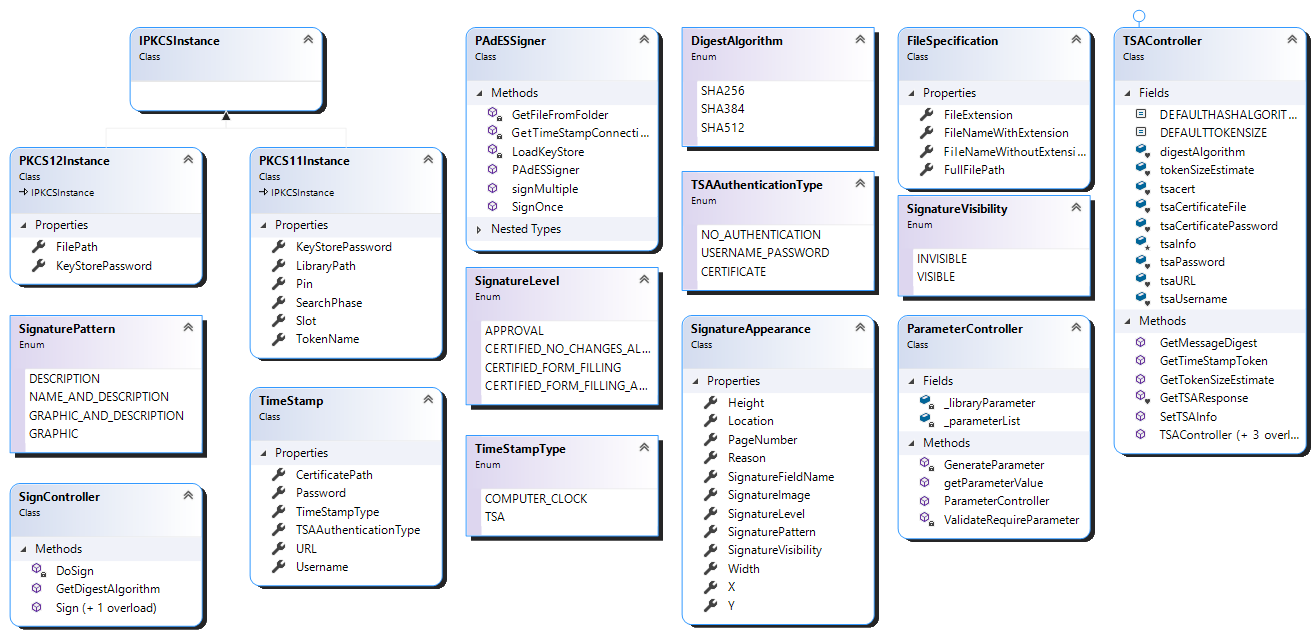
## การกำหนด Dependencies

Library มีการใช้งาน library อื่น ๆ เพิ่มเติมประกอบในการพัฒนา เพื่อให้ Library สามารทำงานได้อย่างสมบูรณ์ จึงจำเป็นต้องติดตั้ง Dependency ที่เกี่ยวข้องทั้งหมด ดังนี้

| **#** | **groupId** | **version** |
| --- | --- | --- |
| 1 | BouncyCastle | 1.8.9 |
| 2 | iTestSharp | 5.5.13.2 |

# ข้อมูลรายละเอียด Library

## Class and method



**Class** PAdESSigner

| **Method name** | **Parameter in** | **Return** | **Remark** |
| --- | --- | --- | --- |
| PAdESSigner | - | - | Class constructor |
| signOnce | **String** inputFilePath,  **String** outputFilePath, **IPKCSInstance** pkcsInstance,  **DigestAlgorithm** digestAlgorithm, **SignatureAppearance** signatureAppearance, **TimeStamping** timeStamping | - | Sign PDF ไฟล์เดียว โดยใช้ข้อมูลที่กำหนด |
| signMultiple | **String** inputFolderPath, **String** outputFolderPath, **String** outputSuffix, **IPKCSInstance** pkcsInstance,  **DigestAlgorithm** digestAlgorithm, **SignatureAppearance** signatureAppearance, **TimeStamping** timeStamping | - | Sign PDF หลายไฟล์ (Bulk sign) โดยใช้ข้อมูลที่กำหนด |
| getFileFromFolder | **String** folderPath | List<FileSpecification> | แสดงรายการไฟล์ทั้งหมดในโฟล์เดอร์ที่กำหนด |
| getTimeStampConnection | **TimeStamp** timeStamp | ITSAClient | สร้าง TimeStamp instance จากข้อมูลที่กำหนด |
| LoadKeyStore | **IPKCSInstance** pkcsInstance | CertificateKeyPack | Load keystore จากตาม patameter ที่กำหนดไว้ใน IPKCSInstance |

**(Internal) Class** CertificateKeyPack

|  |  |  |  |
| --- | --- | --- | --- |
| **Method name** | **Parameter in** | **Return** | **Remark** |
| PrivateKey | **ICipherParameters** | **ICipherParameters** | กำหนด/คืนค่า private key |
| CertificateChain | **X509Certificate** | **X509Certificate** | กำหนด/คืนค่า certificate chain |
| CertificateInstance | **X509Certificate2** | **X509Certificate2** | กำหนด/คืนค่า Certificate |

**Class** ParameterController

|  |  |  |  |
| --- | --- | --- | --- |
| **Method name** | **Parameter in** | **Return** | **Remark** |
| ParameterController | **String[]** args | - | Class constructor |
| generateParameter | **String[]** args | - | ประมวลผล external จาก Main method |
| ValidateRequireParameter | **String[]** args | **boolean** | ตรวจสอบความครบถ้วนของ parameter ที่จำเป็น |
| getParameterValue | **String** key | **String** | คืนค่าของ parameter ตาม key ที่ส่งค่าเข้ามา |

**Class** SignController

| **Method name** | **Parameter in** | **Return** | **Remark** |
| --- | --- | --- | --- |
| sign | **String** src**,  String** dest**,  Org.BouncyCastle.X509.X509Certificate[]** chain**,  ICipherParameters** pk**,**  **DigestAlgorithm** digestAlgorithm**,  PdfSigner.CryptoStandard** subfilter**,**  **SignatureAppearance** signatureAppearance**, Collection<ICrlClient>** crlList**,**  **IOcspClient** ocspClient**, ITSAClient** tsaClient**,**  **int** estimatedSize | - | เตรียม parameter สำหรับเรียกใช้ third-party สำหรับ sign PDF (กรณี PKCS12) |
| sign | **string** src**,  string** dest**,  Org.BouncyCastle.X509.X509Certificate[]** chain**,  X509Certificate2** certificateInstance**, DigestAlgorithm** digestAlgorithm**, CryptoStandard** subfilter**,**  **SignatureAppearance** signatureAppearance**, ICollection<ICrlClient> crlList,**  **IOcspClient** ocspClient**,  ITSAClient** tsaClient**,**  **int** estimatedSize |  | เตรียม parameter สำหรับเรียกใช้ third-party สำหรับ sign PDF (กรณี PKCS11) |
| DoSign | **String** src**,  string** dest**, Org.BouncyCastle.X509.X509Certificate[]** chain**,  IExternalSignature** pks**,  CryptoStandard** subfilter**,**  **SignatureAppearance** signatureAppearance**, ICollection<ICrlClient>** crlList**,**  **IOcspClient** ocspClient**,  ITSAClient** tsaClient**,  int** estimatedSize |  | ทำการเรียกใช้ third-party library เพื่อ sign เอกสาร PDF ด้วยรูปแบบและข้อมูลที่กำหนด |
| GetDigestAlgorithm | **DigestAlgorithm** digestAlgorithm | string | Pass ค่า Digest Alogorithm |

**Class** FileSpecification

|  |  |  |  |
| --- | --- | --- | --- |
| **Method name** | **Parameter in** | **Return** | **Remark** |
| FileNameWithoutExtension | **String** | **String** | กำหนด/คืนค่าชื่อไฟล์แบบไม่มีนามสกุล |
| FileNameWithExtension | **String** | **String** | กำหนด/คืนค่าชื่อไฟล์พร้อมนามสกุล |
| FileExtension | **String** | **String** | กำหนด/คืนค่านามสกุลไฟล์ |
| FullFilePath | **String** | **String** | กำหนด/คืนค่าตำแหน่งเต็มของไฟล์ |

**Class** PKCS11Instance

|  |  |  |  |
| --- | --- | --- | --- |
| **Method name** | **Parameter in** | **Return** | **Remark** |
| LibraryPath | **String** | **String** | คืนค่าตำแหน่งของไฟล์ .dll ของ PKCS11 |
| TokenName | **String** | **String** | คืนค่า Token name |
| Pin | **String** | **String** | คืนค่า Token Pin |
| Slot | **int** | **int** | คืนค่า PKCS11 Slot |
| KeyStorePassword | **String** | **String** | คืนค่ารหัสผ่านของ KeyStore |
| SearchPhase | **String** | **String** | กำหนด/คืนค่าคำค้นหา Certificate |

**Class** PKCS12Instance

|  |  |  |  |
| --- | --- | --- | --- |
| **Method name** | **Parameter in** | **Return** | **Remark** |
| FilePath | **String** | **String** | กำหนด/คืนค่าตำแหน่งของไฟล์ PFX, P12 |
| KeyStorePassword | **String** | **String** | กำหนด/คืนค่ารหัสผ่านของ KeyStore |

**Class** SignatureAppearance

|  |  |  |  |
| --- | --- | --- | --- |
| **Method name** | **Parameter in** | **Return** | **Remark** |
| X | **Float** | **float** | กำหนด/คืนค่าตำแหน่ง X ของ Signature |
| Y | **Float** | **float** | กำหนด/คืนค่าตำแหน่ง Y ของ Signature |
| Width | **Float** | **float** | กำหนด/คืนค่าความกว้างของ Signature |
| Height | **Float** | **float** | กำหนด/คืนค่าความสูงของ Signature |
| PageNumber | **int** | **int** | กำหนด/คืนค่าหมายเลขหน้า |
| SignatureFieldName | **String** | **String** | กำหนด/คืนค่าชื่อ Signature form |
| Reason | **String** | **String** | กำหนด/คืนค่าเหตุผลในการ Sign |
| Location | **String** | **String** | กำหนด/คืนค่าตำแหน่งในการ Sign |
| SignatureLevel | **SignatureLevel** | **SignatureLevel** | กำหนด/คืนค่าระดับของ Signature |
| SignatureImage | **String** | **String** | กำหนด/คืนค่ารูป Signature |
| SignaturePattern | **SignaturePattern** | **SignaturePattern** | กำหนด/คืนค่ารูปแบบ Signature |
| SignatureVisibility | **SignatureVisibility** | **SignatureVisibility** | กำหนด/คืนค่าการมองเห็นของ Signature |

**Class** TimeStamp

|  |  |  |  |
| --- | --- | --- | --- |
| **Method name** | **Parameter in** | **Return** | **Remark** |
| TimeStampType | **TimeStampType** | **TimeStampType** | คืนค่ารูปแบบ TimeStamp |
| TSAAuthenticationType | **TSAAuthenticationType** | **TSAAuthenticationType** | คืนค่ารูปแบบ TSA Authentication |
| Username | **String** | **String** | คืนค่าชื่อผู้ใช้ |
| Password | **String** | **String** | คืนค่ารหัสผ่าน |
| CertificatePath | **String** | **String** | คืนค่าตำแหน่ง certificate |
| URL | **String** | **String** | คืนค่า URL |

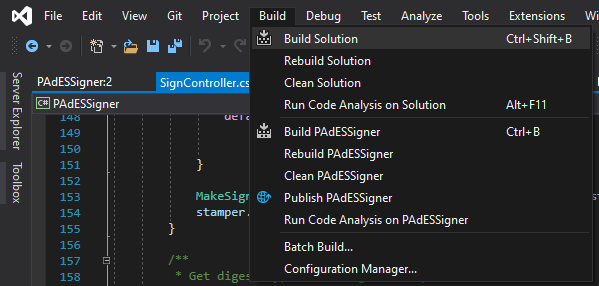
# การใช้งานและการ Deploy library

## การเตรียม Project

1. ที่ project folder ให้ double click ไฟล์นามสกุล .sln เพื่อเปิด project

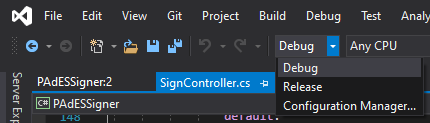


1. เลือกไปที่ Build > Build solution จากนั้นโปรแกรมจะทำการติดตั้ง library ที่จำเป็นและ build project ให้พร้อมใช้งาน

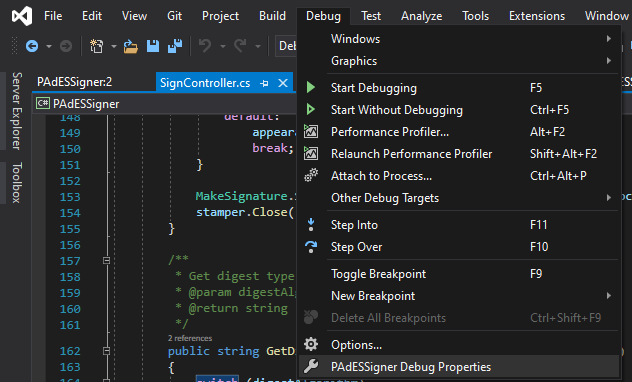


## การเรียกใช้งานสำหรับการทดสอบ (Debug)

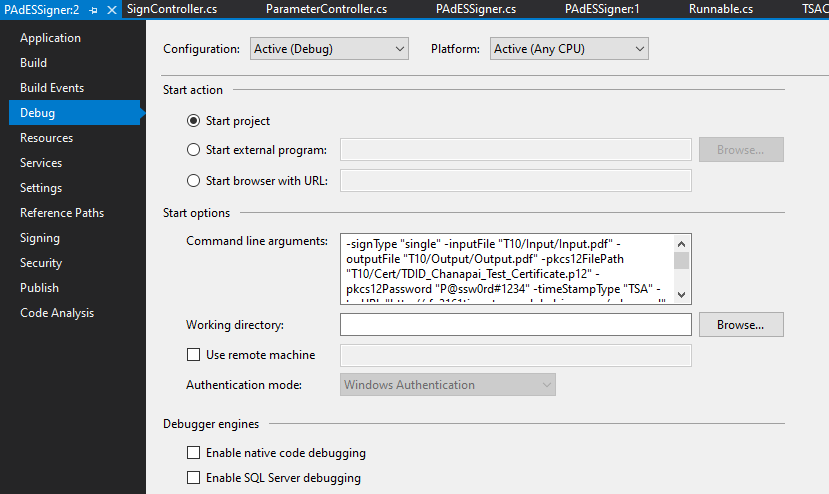
1. ที่ menu bar เลือกเป็น Debug



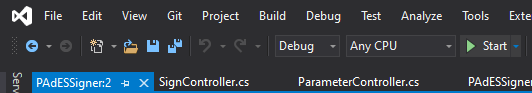
1. เลือก Debug > PAdESSigner Debug properties



1. ที่ Command line arguments เปลี่ยนเป็นค่าที่ต้องการ (สามารถดู Argument ได้ที่การเรียกใช้งานผ่าน Command-line interface)

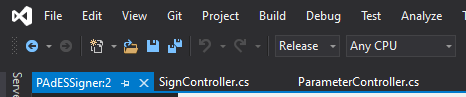


1. กดปุ่ม Start เพื่อดูผลลัพธ์

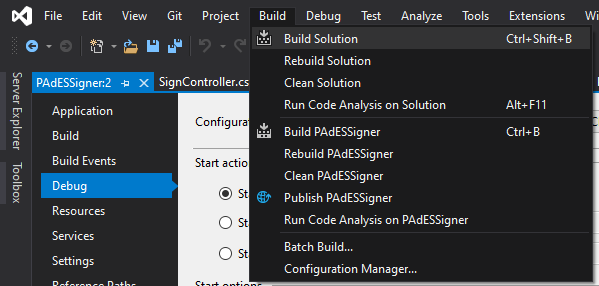


## การ Deploy library (Release exe)

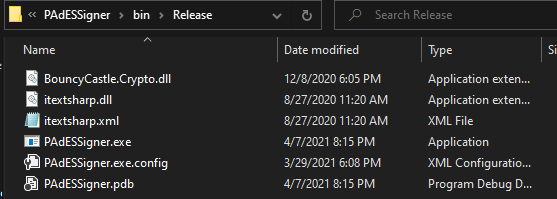
1. ที่ Menu bar เลือก Release



1. เลือกไปที่ Build > Build solution เพื่อ Deploy



1. Library ที่ deploy แล้วจะอยู่ภายใต้ folder bin/release



# การเรียกใช้งานผ่าน Command-line interface

## รายละเอียด Argument

ชุดโปรแกรมรองรับการเรียกใช้งานผ่าน Command line สำหรับ Executable program โดยมี Parameter ที่สามารถ input ค่าได้ ดังนี้

* -**signType "single | multiple"** กำหนดการ sign แบบไฟล์เดียวหรือหลายไฟล์
* **-inputFile "<PATH\_TO\_FILE>"** กำหนดไฟล์นำเข้า
* **-outputFile "<PATH\_TO\_FILE>"** กำหนดไฟล์ผลลัพธ์
* **-inputFolder "<PATH\_TO\_FOLDER>"** กำหนดโฟลเดอร์นำเข้า
* **-outputFolder "<PATH\_TO\_FOLDER>"** กำหนดโฟลเดอร์ผลลัพธ์
* **-outputSuffix "<ANY\_Text>"** กำหนดชื่อต่อท้ายไฟล์ที่ sign แล้ว
* **-pkcs11TokenName "<NAME>"** กำหนดชื่อ PKCS11 Token
* **-pkcs11LibraryPath "<PATH\_TO\_FILE>"** กำหนดชื่อ PKCS11 Token
* **-pkcs11Pin "<PASSWORD>"** Password ของ Token
* **-pkcs11KeyStorePassword "<PASSWORD>"** password ของ Ketstore
* **-pkcs11SeachKeyword "<ANY\_TEXT>"** คำค้นหา Certificate ใน Token
* **-pkcs12FilePath "<PATH\_TO\_FILE>"** ตำแหน่งของไฟล์ P12, PFX
* **-pkcs12Password "<PASSWORD>"** Password ของไฟล์ P12, PFX
* **-timeStampingType "TSA | COMPUTER\_CLOCK"** รูปแบบ Timestamp
* **-tsaURL "<URL>"** URL ของ TSA
* **-tsaAuthenticationType "<NO\_AUTHENTICATION | USERNAME\_PASSWORD | CERTIFICATE>"** รูปแบบการ Authentication ของ TSA
* **-tsaUsername "<USERNAME>"** Username ของ TSA
* **-tsaPassword "<PASSWORD>"** Password ของ TSA
* **-Location “<ANY\_TEXT>"** เหตุผลในการ Sign
* **-Reason “<ANY\_TEXT>"** เหตุผลในการ Sign
* **-X <NUMBER>** กำหนดแหน่งของ Signature
* **-Y <NUMBER>** กำหนดแหน่งงของ Signature
* **-Width <NUMBER>** กำหนดความสูงของ Signature
* **-Height <NUMBER>** กำหนดความสูงของ Signature
* **-SignatureFieldName "<NAME>"** กำหนด Signature form
* **-PageNumber <NUMBER>** กำหนดหน้าที่ต้องการแสดง Signature
* -**SignatureLevel "<APPROVAL | NO\_CHANGE | FORM\_FILLING | FORM\_FILLING\_AND\_ANNOTATION>"** กำหนดระดับของการ Sign
* **-SignatureVisibility "<VISIBLE | INVISIBLE>"** กำหนดการมองเห็นของ Signature
* **-SignaturePattern "<DESCRIPTION | NAME\_AND\_DESCRIPTION | GRAPHIC\_AND\_DESCRIPTION | GRAPHIC>"** กำหนด signature graphic
* **-digestAlgorithm "<SHA256 | SHA384 | SHA512>"** กำหนด hash function

## ตัวอย่างการเรียกใช้งาน

* กรณี Sign PDF ไฟล์เดียว

|  |
| --- |
| PAdESSigner.exe **-signType** "single" **-inputFile** "Input.pdf" **-outputFile** " Output.pdf" **-pkcs12FilePath** "User\_Certificate.p12**" -pkcs12Password** "password"  **-timeStampType** "COMPUTER\_CLOCK" **-Location** "Bangkok" **-Reason** "To sign with PKCS12" **-X** 200 **-Y** 200 **-Width** 200 **-Height** 200 **-SignatureFieldName** "Test\_SIG" **-PageNumber** 1 **-SignatureLevel** "APPROVAL" **-SignatureVisibility** "VISIBLE"  **-SignaturePattern** "DESCRIPTION" -digestAlgorithm "SHA256" |

* กรณี sign แบบ Bulk (Sign ทั้ง folder)

|  |
| --- |
| PAdESSigner.exe **-signType** "multiple" **-inputFolder** "Input/" **-outputFolder** "Output.pdf" **-outputSuffix** "\_Signed" **-pkcs12FilePath** "User\_Certificate.p12**" -pkcs12Password** "password" **-timeStampType** "COMPUTER\_CLOCK" **-Location** "Bangkok" **-Reason** "To sign with PKCS12" **-X** 200 **-Y** 200 **-Width** 200 **-Height** 200 **-SignatureFieldName** "Test\_SIG" **-PageNumber** 1 **-SignatureLevel** "APPROVAL" **-SignatureVisibility** "VISIBLE" **-SignaturePattern** "DESCRIPTION" -digestAlgorithm "SHA256" |

* กรณี Sign โดยใช้ TSA Server

|  |
| --- |
| PAdESSigner.exe **-signType** "single" **-inputFile** "Input.pdf" **-outputFile** " Output.pdf" **-pkcs12FilePath** "User\_Certificate.p12**" -pkcs12Password** "password"  **-timeStampType** "TSA**" -tsaURL** "https://TSA\_URL**" -tsaAuthenticationT**ype “CERTIFICATE” **-tsaPKCS12File** "TSA\_Certification.p12" **-tsaPKCS12Password** "password" **-Location** "Bangkok" **-Reason** "To sign with PKCS12" **-X** 200 **-Y** 200 **-Width** 200 **-Height** 200 **-SignatureFieldName** "Test\_SIG" **-PageNumber** 1  **-SignatureLevel** "APPROVAL" **-SignatureVisibility** "VISIBLE" **-SignaturePattern** "DESCRIPTION" -digestAlgorithm "SHA256" |