

A close up of a sign

Description automatically generated

**คู่มือการใช้งานสำหรับนักพัฒนาระบบ  
XAdES Signer (.NET)**

**โครงการ จ้างที่ปรึกษาเพื่อบริหารโครงการปรับเปลี่ยนบริการภาครัฐที่เกี่ยวกับการออกใบอนุญาต หรือหลักฐานสำคัญ ให้เป็นดิจิทัล ด้วยมาตรฐานที่จำเป็น**

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

23 เมษายน 2564



Strategy Consulting & Digital Transformation

**บริษัท ฟรอนทิส จำกัด**

สารบัญ

[การกำหนดค่าสำหรับ Library 3](#_Toc70076392)

[1. Environment และ Software ที่เกี่ยวข้อง 3](#_Toc70076393)

[2. การกำหนด Dependencies 3](#_Toc70076394)

[ข้อมูลรายละเอียด Library 4](#_Toc70076395)

[1. Class and method 4](#_Toc70076396)

[การใช้งานและการ Deploy library 8](#_Toc70076397)

[1. การเตรียม Project 8](#_Toc70076398)

[2. การเรียกใช้งานสำหรับการทดสอบ (Debug) 9](#_Toc70076399)

[5. การ Deploy library (Release exe) 10](#_Toc70076400)

[การเรียกใช้งานผ่าน Command-line interface 11](#_Toc70076401)

[1. รายละเอียด Argument 11](#_Toc70076402)

[2. ตัวอย่างการเรียกใช้งาน 12](#_Toc70076403)

# การกำหนดค่าสำหรับ Library

## Environment และ Software ที่เกี่ยวข้อง

Library นี้พัฒนาด้วยภาษา .NET ซึ่งมี environment และ software ที่จำเป็นในการใช้พัฒนา ดังนี้

1. NET Framework 3.5
2. Visual Studio 2019

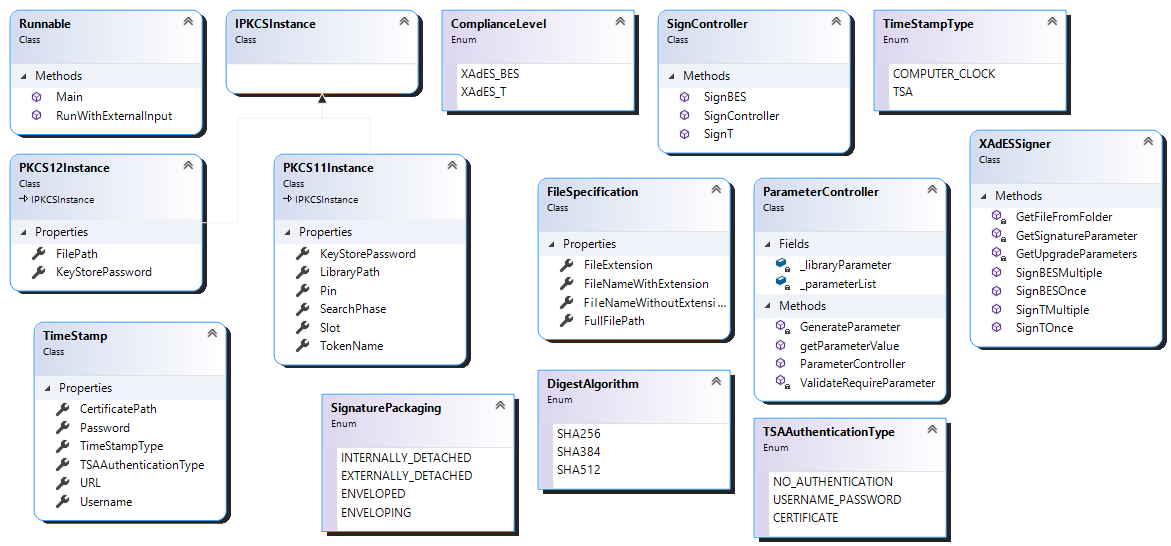
## การกำหนด Dependencies

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

| **#** | **groupId** | **version** |
| --- | --- | --- |
| 1 | BouncyCastle | 1.8.9 |

# ข้อมูลรายละเอียด Library

## Class and method



**Class** XAdESSigner

| **Method name** | **Parameter in** | **Return** | **Remark** |
| --- | --- | --- | --- |
| XAdESSigner | - | **-** | Class Constructor |
| signBESOnce | **string** inputFilePath,  **string** outputFilePath, **IPKCSInstance** pKCSInstance, **DigestAlgorithm** digestAlgorithm,  **SignaturePackaging** signaturePackaging,  **string** externalSignatureFilePath | - | Sign XAdES-BES ไฟล์เดียว |
| signBESMultiple | **string** inputFolderPath, **string** outputFolderPath, **string** outputSuffix, **IPKCSInstance** pKCSInstance,  **DigestAlgorithm** digestAlgorithm, **SignaturePackaging** signaturePackaging,  **string** externalSignatureFilePath | **-** | Sign XAdES-BES หลายไฟล์ |
| signTOnce | **string** inputFilePath,  **string** outputFilePath, **IPKCSInstance** pKCSInstance, **DigestAlgorithm** digestAlgorithm,  **SignaturePackaging** signaturePackaging,  **string** externalSignatureFilePath, **TimeStamp** timeStamp | **-** | Sign XAdES-T ไฟล์เดียว |
| signTMultiple | **string** inputFolderPath, **string** outputFolderPath, **string** outputSuffix, **IPKCSInstance** pKCSInstance, **DigestAlgorithm** digestAlgorithm,  **SignaturePackaging** signaturePackaging,  **string** externalSignatureFilePath, **TimeStamp** timeStamp | **-** | Sign XAdES-T หลายไฟล์ |
| GetSignatureParameter | **DigestAlgorithm** digestAlgorithm, **SignaturePackaging** signaturePackaging,  **string** externalSignatureFilePath, **IPKCSInstance** pKCSInstance | **SignatureParameters** | เตรียม parameter สำหรับการ sign Baseline-B |
| GetUpgradeParameters | **TimeStamp** timeStamp | **UpgradeParameters** | เตรียม parameter สำหรับการ sign Baseline-T |
| getFileFromFolder | **String** folderPath | **List<FileSpecification>** | แสดงรายชื่อไฟล์ทั้งหมดในโฟล์เดอร์ที่เลือก |

**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** PKCS11Instance

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

| **Method name** | **Parameter in** | **Return** | **Remark** |
| --- | --- | --- | --- |
| SignController | **-** | - | Default constructor |
| SignBES | **string** inputFilePath,  **string** outputFilePath, **SignatureParameters** signatureParameters | - | Call third-party เพื่อ sign xml ที่ Baseline-B |
| SignT | **string** inputFilePath,  **string** outputFilePath, **SignatureParameters** signatureParameters, **UpgradeParameters** upgradeParameters | - | Call third-party เพื่อ sign xml ที่ Baseline-T |

**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 |

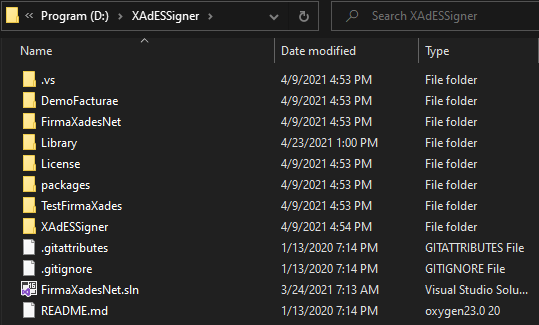
**Class** FileSpecification

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

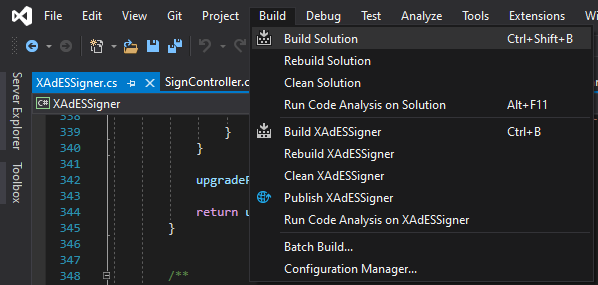
# การใช้งานและการ Deploy library

## การเตรียม Project

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

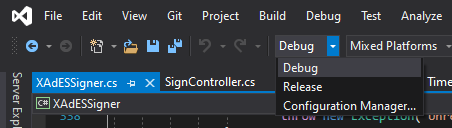


1. เลือกไปที่ Build > Build solution จากนั้นโปรแกรมจะทำการติดตั้ง library ที่จำเป็นและ build project ให้พร้อมใช้งาน

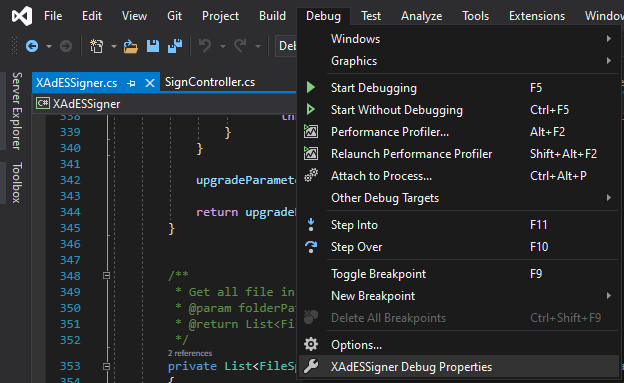


## การเรียกใช้งานสำหรับการทดสอบ (Debug)

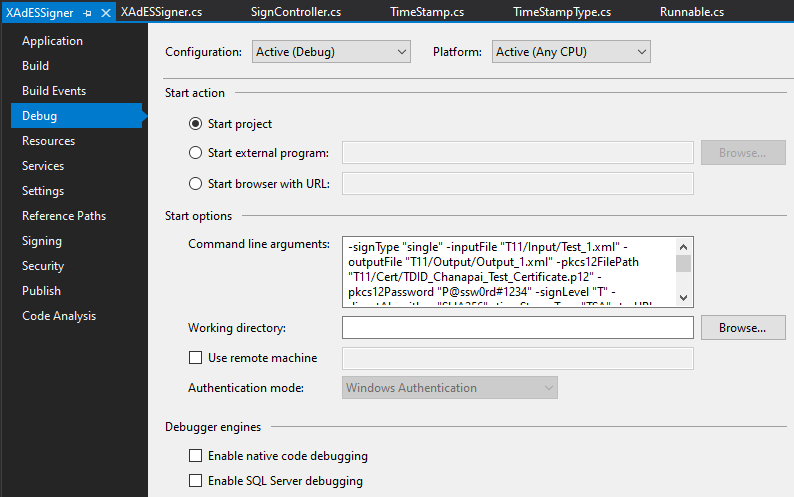
1. ที่ menu bar เลือกเป็น Debug



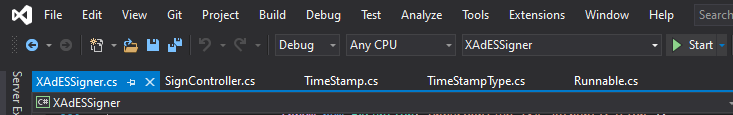
1. เลือก Debug > XAdESSigner Debug properties



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

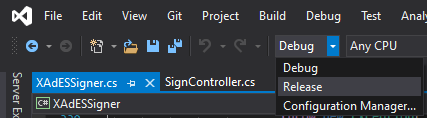


1. กดปุ่ม Start เพื่อดูผลลัพธ์

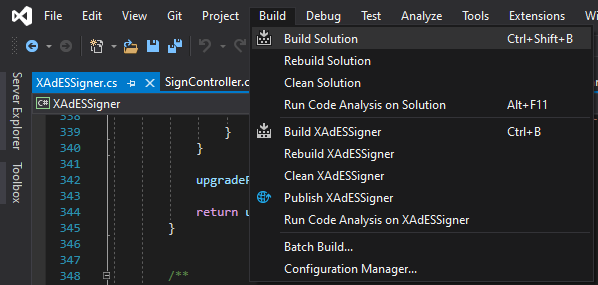


## การ Deploy library (Release exe)

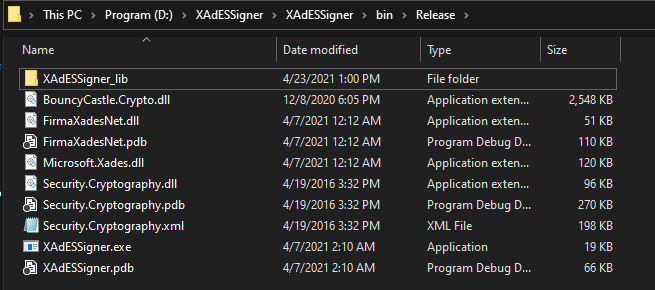
1. ที่ Menu bar เลือก Release



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
* **-signLevel “BES | T”** กำหนดระดับของ XAdES
* **-inputFile "<PATH\_TO\_FILE>"** กำหนดไฟล์นำเข้า
* **-outputFile "<PATH\_TO\_FILE>"** กำหนดไฟล์ผลลัพธ์
* **-inputFolder "<PATH\_TO\_FOLDER>"** กำหนดโฟลเดอร์นำเข้า
* **-outputFolder ""<PATH\_TO\_FOLDER>"** กำหนดโฟลเดอร์ผลลัพธ์
* **-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
* **-digestAlgorithm "<SHA256 | SHA384 | SHA512>"** กำหนด hash function

## ตัวอย่างการเรียกใช้งาน

* กรณี Sign XML แบบ XAdES Baseline-B ไฟล์เดียว

|  |
| --- |
| XAdESSigner.exe **-signType** "single" **-inputFile** "Input.xml" **-outputFile** " Output.xml" **-pkcs12FilePath** "User\_Certificate.p12" **-pkcs12Password** "password" **-signLevel** "BES" **-timeStampingType** "COMPUTER\_CLOCK" **-digestAlgorithm** "SHA256" |

* กรณี Sign XML แบบ XAdES Baseline-B แบบ Bulk (Sign ทั้ง Folder)

|  |
| --- |
| XAdESSigner.exe **-signType** "single" **-inputFolder** "Input/  **-outputFolder** "Output/" **-outputSuffix** "\_BES" **-pkcs12FilePath** "User\_Certificate.p12"  **-pkcs12Password** "password" **-signLevel** "BES" **-timeStampingType** "COMPUTER\_CLOCK"  **-digestAlgorithm** "SHA256" |

* กรณี Sign XML แบบ XAdES Baseline-T ไฟล์เดียว

|  |
| --- |
| XAdESSigner.exe **-signType** "single" **-inputFile** "Input.xml" **-outputFile** " Output.xml" **-pkcs12FilePath** "User\_Certificate.p12" **-pkcs12Password** "password"  **-signLevel** "T" **-timeStampType** "TSA**" -tsaURL** "https://TSA\_URL**"  -tsaAuthenticationT**ype “CERTIFICATE” **-tsaPKCS12File** "TSA\_Certification.p12"  **-tsaPKCS12Password** "password" **-digestAlgorithm** "SHA256" |

* กรณี Sign XML แบบ XAdES Baseline-T แบบ Bulk (Sign ทั้ง Folder)

|  |
| --- |
| XAdESSigner.exe **-signType** "single" **-inputFolder** "Input/  **-outputFolder** "Output/" **-outputSuffix** "\_BES" **-pkcs12FilePath** "User\_Certificate.p12"  **-pkcs12Password** "password" **-signLevel** "T" **-timeStampType** "TSA**"  -tsaURL** https://TSA\_URL **-tsaAuthenticationT**ype “CERTIFICATE” **-tsaPKCS12File** "TSA\_Certification.p12" **-tsaPKCS12Password** "password" **-digestAlgorithm** "SHA256" |