



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม



คู่มือการใช้งานสำหรับนักพัฒนาระบบ
การลงนามไฟล์ JSON
รูปแบบ JWS

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

27 ธันวาคม 2565

สารบัญ

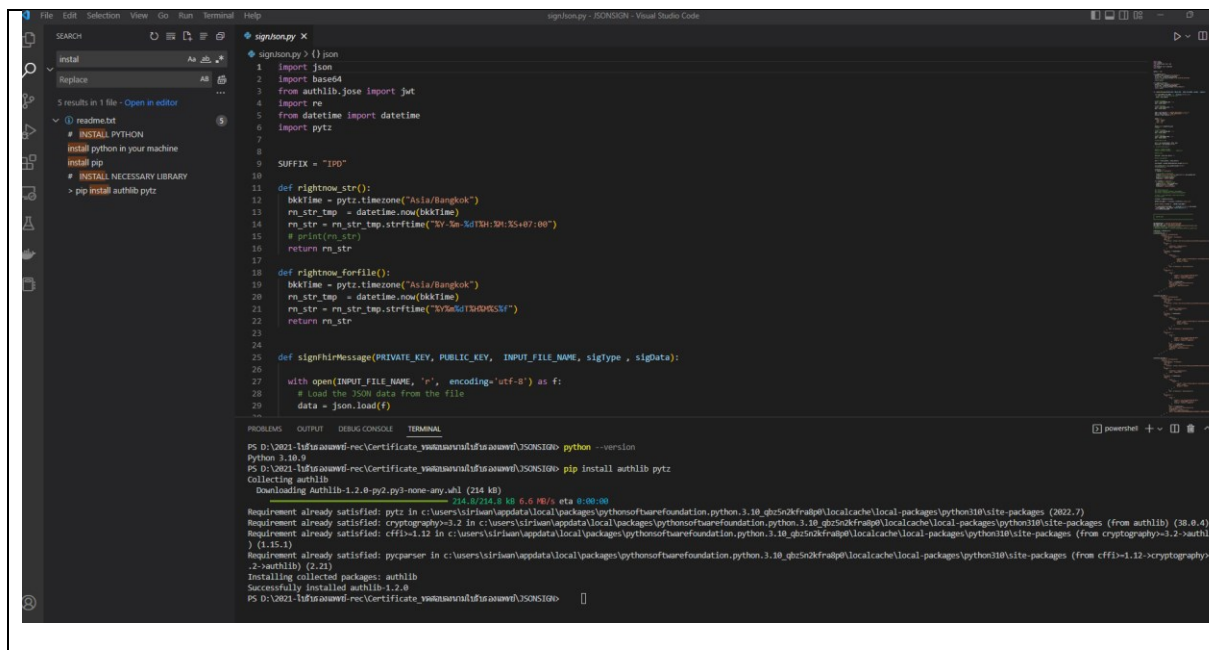
การกำหนดค่าสำหรับ Library	3
1. Environment และ Software ที่เกี่ยวข้อง.....	3
2. ตรวจสอบ Version ของ python	3
การใช้งาน Library	4
1. การกำหนดค่าสำหรับตัวแปร.....	4
2. การเรียกใช้ Command Line	6

การกำหนดค่าสำหรับ Library

1. Environment และ Software ที่เกี่ยวข้อง

Library นี้พัฒนาด้วยภาษา python ซึ่งมี environment และ software ที่จำเป็นในการใช้พัฒนา โดย Run คำสั่งดังนี้

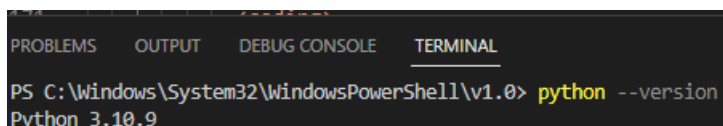
1. install pip
2. install pip> pip install authlib pytz



```
signhon.py 2 | json
1 import json
2 import base64
3 from authlib.jose import jwt
4 import re
5 from datetime import datetime
6 import pytz
7
8 SUFFIX = ".ISO"
9
10 def rightnow_str():
11     bkktime = pytz.timezone("Asia/Bangkok")
12     rn_str_tmp = datetime.now(bkktime)
13     rn_str = rn_str_tmp.strftime("%Y-%m-%dT%H:%M:%S+07:00")
14     # print(rn_str)
15     return rn_str
16
17 def rightnow_forfile():
18     bkktime = pytz.timezone("Asia/Bangkok")
19     rn_str_tmp = datetime.now(bkktime)
20     rn_str = rn_str_tmp.strftime("%Y-%m-%dT%H:%M:%S+07:00")
21     return rn_str
22
23 def signhonMessage(PRIVATE_KEY, PUBLIC_KEY, INPUT_FILE_NAME, sigtype, sigdata):
24
25     with open(INPUT_FILE_NAME, 'r', encoding='utf-8') as f:
26         # Load the JSON data from the file
27         data = json.load(f)
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
```

```
PS D:\2021-ไม่ลงนามพรี-rec\Certificate_ทดลองลงนามไม่ลงนามพรี\JSGS100> python --version
Python 3.10.9
PS D:\2021-ไม่ลงนามพรี-rec\Certificate_ทดลองลงนามไม่ลงนามพรี\JSGS100> pip install authlib pytz
Collecting authlib
  Downloading Authlib-1.2.0-py2.py3-none-any.whl (214 kB)
    Downloading Authlib-1.2.0-py2.py3-none-any.whl (214 kB)
Requirement already satisfied: pytz in c:\users\sirisaen\appdata\local\packages\pythonsoftwarefoundation.python.3.10_gi5n2kfrapq\localcache\local-packages\python310\site-packages (2022.7)
Requirement already satisfied: cryptography>=3.2 in c:\users\sirisaen\appdata\local\packages\pythonsoftwarefoundation.python.3.10_gi5n2kfrapq\localcache\local-packages\python310\site-packages (from authlib) (38.0.4)
Requirement already satisfied: cffi>=1.12 in c:\users\sirisaen\appdata\local\packages\pythonsoftwarefoundation.python.3.10_gi5n2kfrapq\localcache\local-packages\python310\site-packages (from cryptography>=3.2->authlib) (1.15.1)
Requirement already satisfied: pycparser in c:\users\sirisaen\appdata\local\packages\pythonsoftwarefoundation.python.3.10_gi5n2kfrapq\localcache\local-packages\python310\site-packages (from cffi>=1.12->cryptography>=3.2->authlib) (2.21)
Installing collected packages: authlib
Successfully installed authlib-1.2.0
PS D:\2021-ไม่ลงนามพรี-rec\Certificate_ทดลองลงนามไม่ลงนามพรี\JSGS100>
```

2. ตรวจสอบ Version ของ python

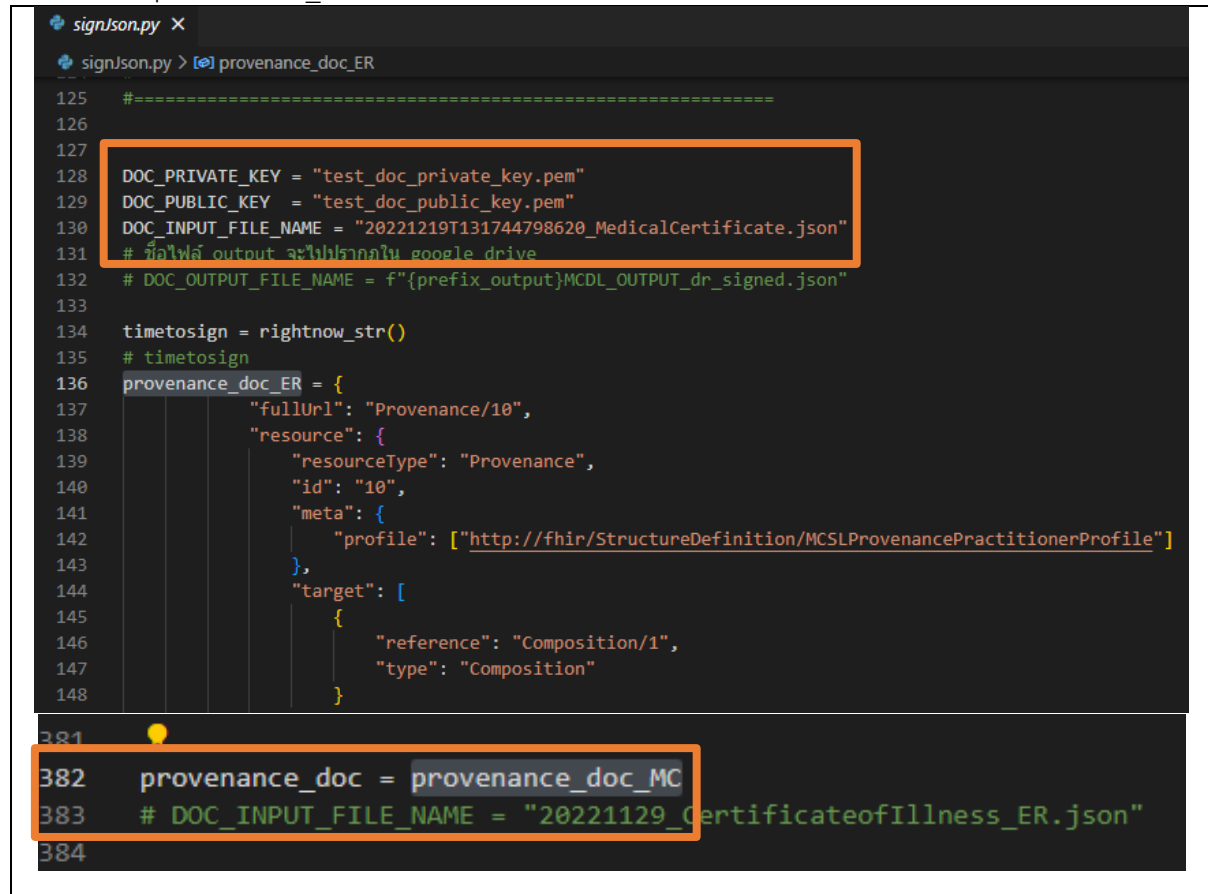


```
PS C:\Windows\System32\WindowsPowerShell\v1.0> python --version
Python 3.10.9
```

การใช้งาน Library

1. การกำหนดค่าสำหรับตัวแปร

1. กำหนดค่าตัวแปรในการลงนามของแพทย์ดังนี้
 - 1.1 DOC_PRIVATE_KEY = private key ของแพทย์
 - 1.2 DOC_PUBLIC_KEY = public key ของแพทย์
 - 1.3 DOC_INPUT_FILE_NAME = ชื่อไฟล์ที่ต้องการลงนามเป็นไฟล์ Json
 - 1.4 provenance_doc = เป็นค่า Provenance



```
signJson.py X
signJson.py > [🔍] provenance_doc_ER

125 #=====
126
127
128 DOC_PRIVATE_KEY = "test_doc_private_key.pem"
129 DOC_PUBLIC_KEY = "test_doc_public_key.pem"
130 DOC_INPUT_FILE_NAME = "20221219T131744798620_MedicalCertificate.json"
131 # ชื่อไฟล์ output จะไปปรากฏใน google drive
132 # DOC_OUTPUT_FILE_NAME = f"{prefix_output}MCDL_OUTPUT_dr_signed.json"
133
134 timetosign = rightnow_str()
135 # timetosign
136 provenance_doc_ER = {
137     "fullUrl": "Provenance/10",
138     "resource": {
139         "resourceType": "Provenance",
140         "id": "10",
141         "meta": {
142             "profile": ["http://fhir/StructureDefinition/MCSLProvenancePractitionerProfile"]
143         },
144         "target": [
145             {
146                 "reference": "Composition/1",
147                 "type": "Composition"
148             }
149         ]
150     }
151 }
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182 provenance_doc = provenance_doc_MC
183 # DOC_INPUT_FILE_NAME = "20221129_CertificateofIllness_ER.json"
184
```

2. กำหนดค่าตัวแปรในการลงนามของสถานพยาบาล ดังนี้
 - 2.1 HOSP_PRIVATE_KEY = private key ของสถานพยาบาล
 - 2.2 HOSP_PUBLIC_KEY = public key ของสถานพยาบาล
 - 2.3 hospitalSignature = เป็นค่า Bundle.Signature

กรณีใบรับรองแพทย์ (ขออนุญาตเข้ารับ) การกำหนดค่าตัวแปร 1.4 provenance_doc และ 1.5 hospitalSignature ดังนี้

1.3 DOC_INPUT_FILE_NAME = ไฟล์ต้องเป็นข้อมูลใบรับรองแพทย์ (ขออนุญาตเข้ารับ)

1.4 provenance_doc = provenance_doc_MCLD

1.5 hospitalSignature = hospitalSignature_MCDL

```
382   provenance_doc = provenance_doc_MCLD
383   # DOC_INPUT_FILE_NAME = "20221129_CertificateofIllness_ER.json"
453   hospitalSignature = hospitalSignature_MCDL
454   signFhirMessage(HOSP_PRIVATE_KEY, HOSP_PUBLIC_KEY, HOSP_INPUT_FILE_NAME, "signature", hospitalSignature)
```

กรณีใบรับรองแพทย์ (ตรวจสอบสุขภาพ) การกำหนดค่าตัวแปร 1.4 provenance_doc และ 1.5 hospitalSignature ดังนี้

1.3 DOC_INPUT_FILE_NAME = ไฟล์ต้องเป็นข้อมูลใบรับรองแพทย์ (ตรวจสอบสุขภาพ)

1.4 provenance_doc = provenance_doc_MC

1.5 hospitalSignature = hospitalSignature_MC

```
382   provenance_doc = provenance_doc_MC
383   # DOC_INPUT_FILE_NAME = "20221129_CertificateofIllness_ER.json"
384
453   hospitalSignature = hospitalSignature_MC
454   signFhirMessage(HOSP_PRIVATE_KEY, HOSP_PUBLIC_KEY, HOSP_INPUT_FILE_NAME, "signature", hospitalSignature)
```

กรณีใบรับรองแพทย์ (รับรองอาการป่วย) กำหนดค่าตัวแปร 1.4 provenance_doc และ 1.5 hospitalSignature ดังนี้

1.3 DOC_INPUT_FILE_NAME = ไฟล์ต้องเป็นข้อมูลใบรับรองแพทย์ (รับรองอาการป่วย)

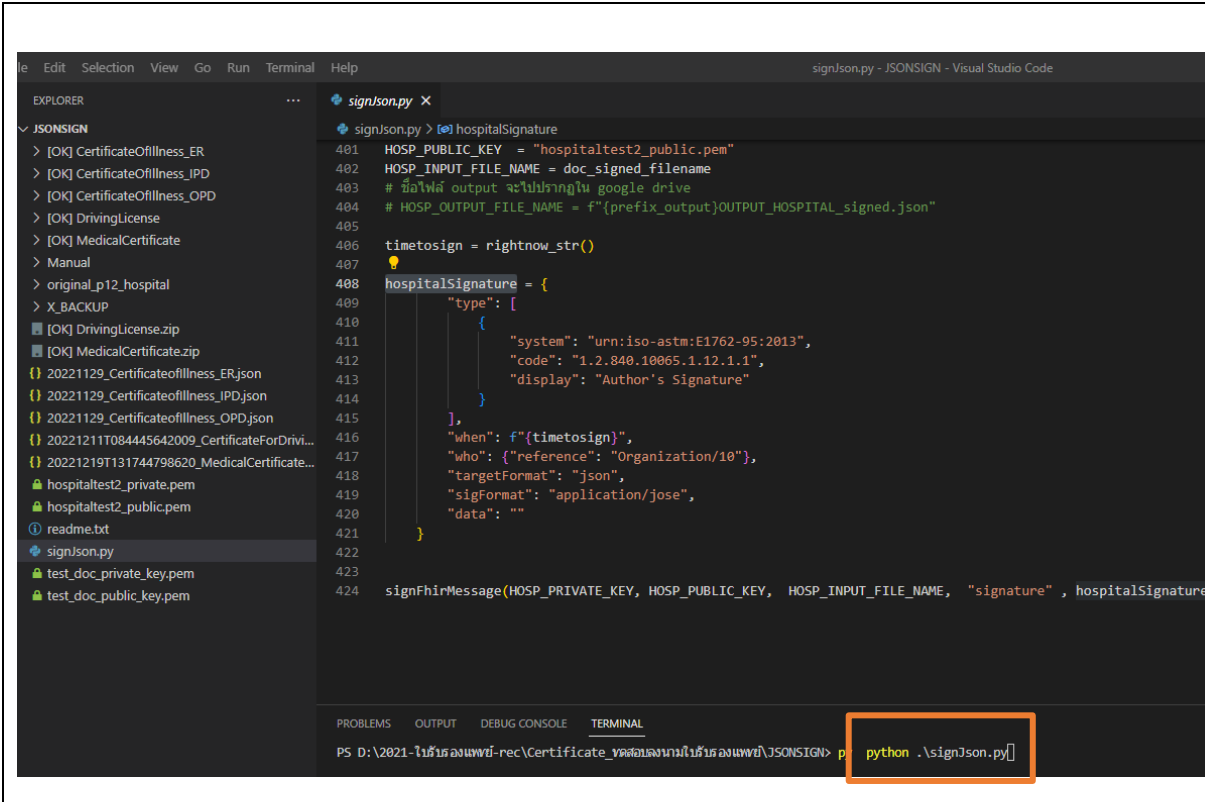
1.4 provenance_doc = provenance_doc_MCSL

1.5 hospitalSignature = hospitalSignature_MCSL

```
283   provenance_doc = provenance_doc_MCSL
284   # DOC_INPUT_FILE_NAME = "20221129_CertificateofIllness_ER.json"
350   hospitalSignature = hospitalSignature_MCSL
351   signFhirMessage(HOSP_PRIVATE_KEY, HOSP_PUBLIC_KEY, HOSP_INPUT_FILE_NAME, "signature", hospitalSignature)
```

2. การเรียกใช้ Command Line

1. python .\signJson.py

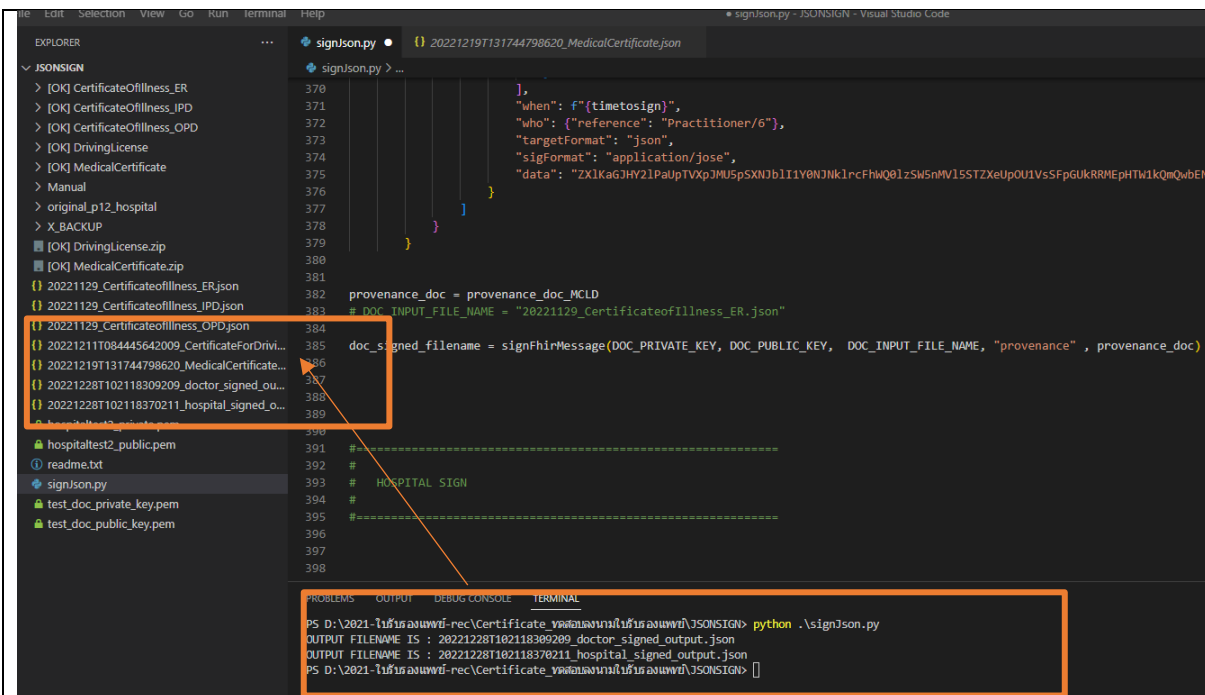


The screenshot shows the Visual Studio Code editor with the file `signJson.py` open. The file contains Python code for signing JSON documents. The Explorer pane on the left shows the project structure, including various certificate and key files. The Command Line interface at the bottom shows the command `python .\signJson.py` being executed.

```
signJson.py > hospitalSignature
401 HOSP_PUBLIC_KEY = "hospitaltest2_public.pem"
402 HOSP_INPUT_FILE_NAME = doc_signed_filename
403 # ชื่อไฟล์ output จะไปปรากฏใน google drive
404 # HOSP_OUTPUT_FILE_NAME = f'{prefix_output}OUTPUT_HOSPITAL_signed.json'
405
406 timetosign = rightnow_str()
407
408 hospitalSignature = {
409     "type": [
410         {
411             "system": "urn:iso-astm:E1762-95:2013",
412             "code": "1.2.840.10065.1.12.1.1",
413             "display": "Author's Signature"
414         }
415     ],
416     "when": f'{timetosign}',
417     "who": {"reference": "Organization/10"},
418     "targetFormat": "json",
419     "sigFormat": "application/jose",
420     "data": ""
421 }
422
423 signFhirMessage(HOSP_PRIVATE_KEY, HOSP_PUBLIC_KEY, HOSP_INPUT_FILE_NAME, "signature", hospitalSignature)
```

Command Line: `PS D:\2021-ใบรับรองแพทย์-rec\Certificate_พดลงนามใบรับรองแพทย์\JSONSIGN> python .\signJson.py`

จากนั้น Lib จะทำการสร้างไฟล์ใบรับรองแพทย์ที่ลงนามโดยแพทย์และลงนามโดยสถานพยาบาลดังภาพ



The screenshot shows the Visual Studio Code editor with the file `signJson.py` open. The file contains Python code for signing JSON documents. The Explorer pane on the left shows the project structure, including various certificate and key files. The Command Line interface at the bottom shows the command `python .\signJson.py` being executed, and the output files are listed.

```
signJson.py > ...
370 ],
371 "when": f'{timetosign}',
372 "who": {"reference": "Practitioner/6"},
373 "targetFormat": "json",
374 "sigFormat": "application/jose",
375 "data": "ZX1KaGJHY2lPaUpTVXpJMU5pSXM7blliY08JNk1rcFhwQ01zSW5mV15STZKeUpOU1VsSFpGUKRRMEpHTW1kQmQwbE1"
376 }
377 ]
378 }
379 }
380
381 provenance_doc = provenance_doc_MCLD
382 # DOC_INPUT_FILE_NAME = "20221129_CertificateofIllness_ER.json"
383
384 doc_signed_filename = signFhirMessage(DOC_PRIVATE_KEY, DOC_PUBLIC_KEY, DOC_INPUT_FILE_NAME, "provenance", provenance_doc)
385
386
387
388
389
390
391 #=====
392 #
393 # HOSPITAL SIGN
394 #=====
395
396
397
398
```

Command Line: `PS D:\2021-ใบรับรองแพทย์-rec\Certificate_พดลงนามใบรับรองแพทย์\JSONSIGN> python .\signJson.py`

Output: `OUTPUT FILENAME IS : 20221228102118309209_doctor_signed_output.json`

Output: `OUTPUT FILENAME IS : 20221228102118370211_hospital_signed_output.json`

Command Line: `PS D:\2021-ใบรับรองแพทย์-rec\Certificate_พดลงนามใบรับรองแพทย์\JSONSIGN>`