

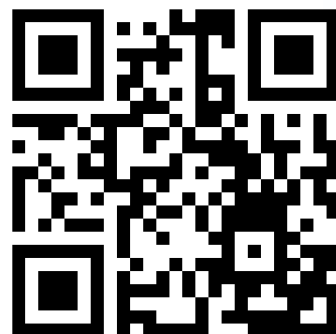


KMUTT MySign

Digital Signature Key Distribution

WUNCA #43 | 10-12 July 2023

Khon Kaen University



<https://kmutt.me/WUNCA-mysign>



AGENDA



MySign Architecture

CA Working Protocol

CA API Server

API Usage

KMUTT MySign 2.0

Q & A



MySign Architecture

Architecture



MySign
Application



CA
Automation
Server

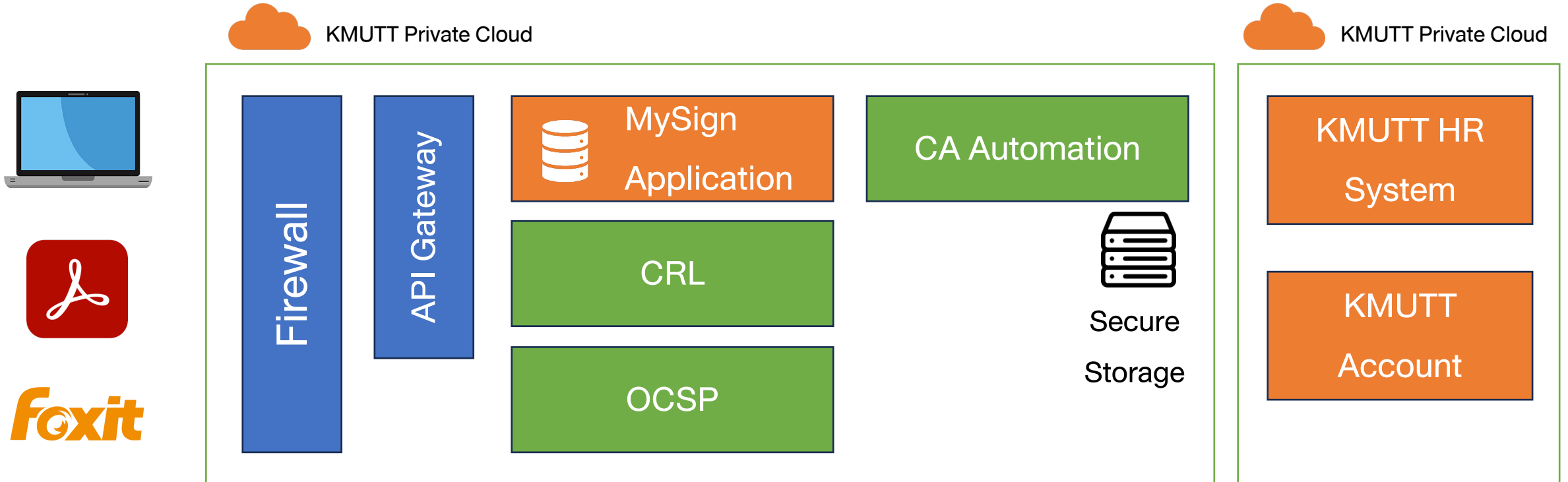


CRL Server

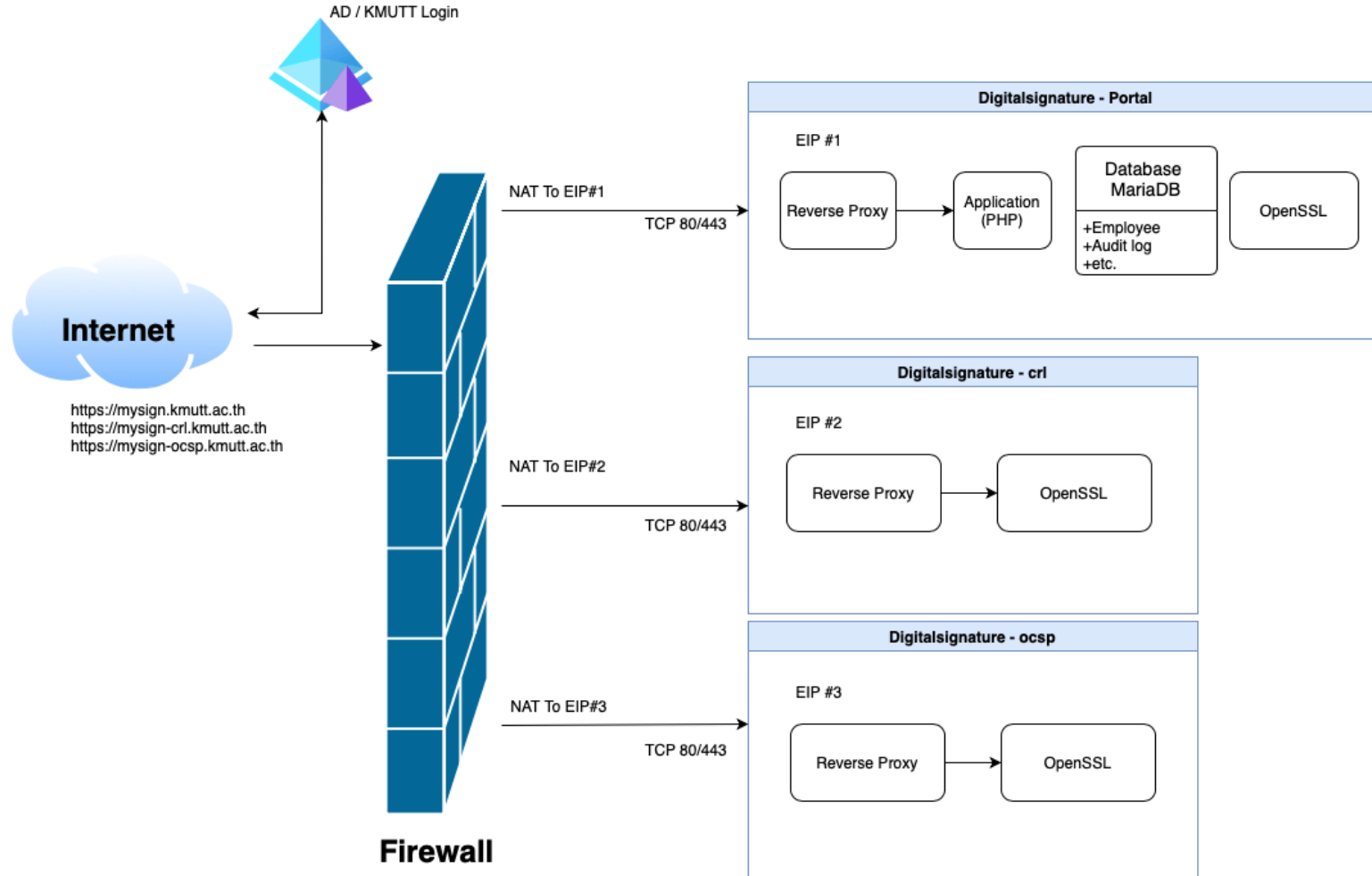


OCSP Server

Architecture



Architecture

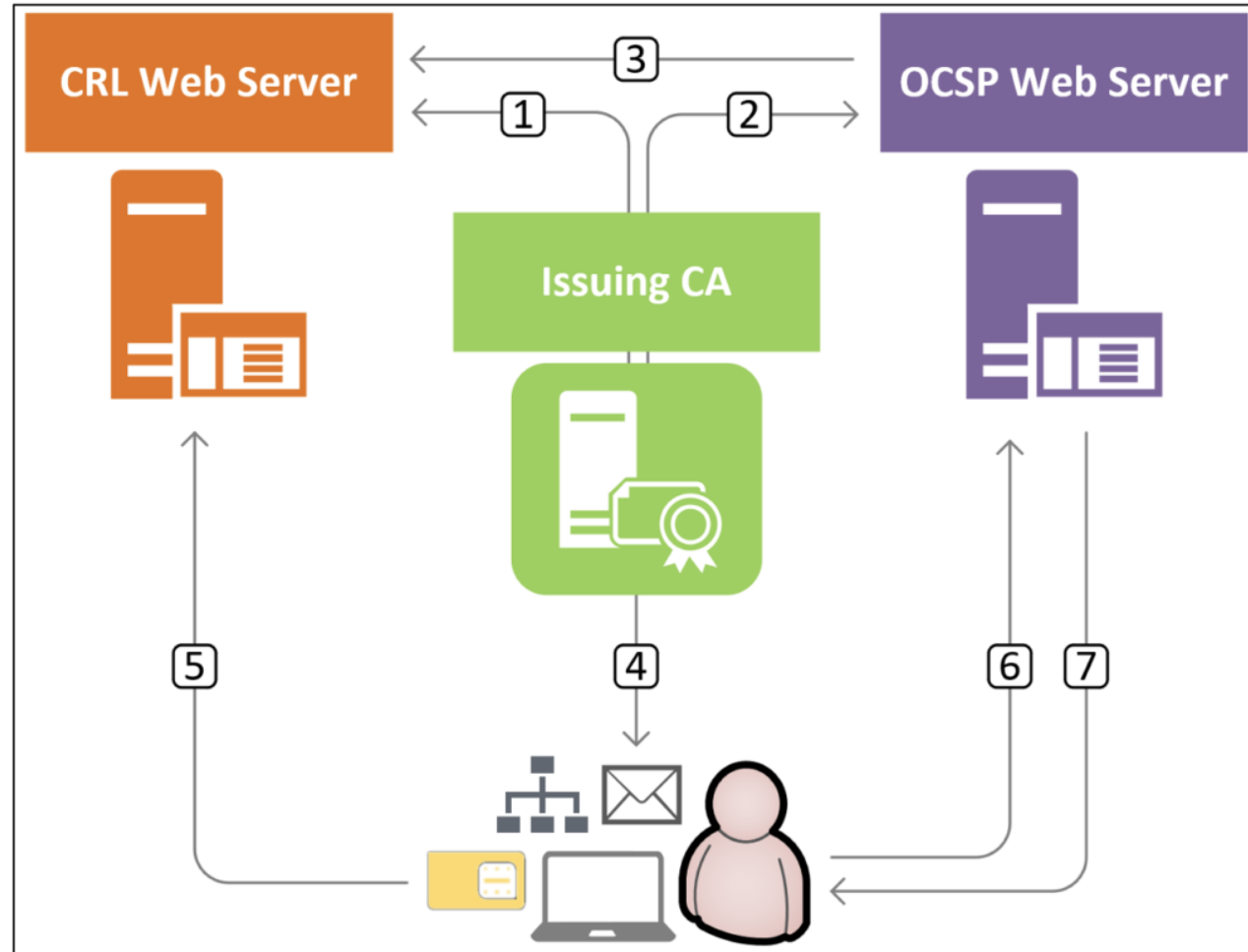




INNOVASIVE

CA Working Protocol

CA Architecture

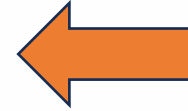


Digital ID Detail



Subject Name

Country or Region TH
State/Province Bangkok
Locality Thung Khru, Bang Mod
Organization King Mongkut's University of Technology Thonburi
Organizational Unit CCDEV
Common Name Nontawat Junsane
Email Address nontawat.jun@kmutt.ac.th



Nontawat Junsane

Country or Region TH
State/Province Bangkok
Locality Thung Khru, Bang Mod
Organization King Mongkut's University of Technology Thonburi
Organizational Unit CCDEV
Common Name Nontawat Junsane
Email Address nontawat.jun@kmutt.ac.th

Issuer Name
Country or Region TH
Organization King Mongkut's University of Technology Thonburi
Common Name King Mongkut's University of Technology Certification Authority

Serial Number 00 85 E5 91 9E 98 85 38 98 B0 25 06 82 37 02 57 7F
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters None

Not Valid Before Saturday, 8 July BE 2566 16:30:45 Indochina Time
Not Valid After Sunday, 7 July BE 2567 16:30:45 Indochina Time

Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters None
Public Key 512 bytes : E0 F9 F4 1F 7A CA 7D 14 ...
Exponent 65537
Key Size 4,096 bits
Key Usage Encrypt, Verify, Wrap, Derive

Signature 512 bytes : C3 16 AF 2D 08 37 3B 4F ...

Extension Subject Key Identifier (2.5.29.14)
Critical NO
Key ID 06 B7 2F 9A 6E 80 86 AE F9 2B 18 25 63 15 D2 04 9B 26 CF EC

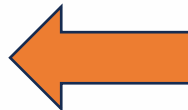
Extension Authority Key Identifier (2.5.29.35)
Critical NO
Key ID 2A 77 22 D2 9F 63 18 E0 41 2E 4A EA F1 8F 58 A8 82 52 35 F9

Extension Netscape Certificate Type (2.16.840.1.113730.1.1)
Critical NO
Cert Type SSL Client, S/MIME

Extension CRL Distribution Points (2.5.29.31)
Critical NO
URI http://mysign-crl.kmutt.ac.th/crl/intermediate

Extension Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical NO
Method #1 Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI http://mysign-ocsp.kmutt.ac.th

Fingerprints
SHA-256 CD 48 72 1D 04 E0 33 32 1F 22 1F E9 A7 3C 52 1C 1B DA 88 94 08 77 7C
A7 98 C2 8D 86 62 E0 DA 27
SHA-1 88 91 8D E5 40 CC 2C 10 DC 52 0B 96 01 35 39 55 76 25 92 EA



Extension CRL Distribution Points (2.5.29.31)

Critical NO

URI <http://mysign-crl.kmutt.ac.th/crl/intermediate>

Extension Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)

Critical NO

Method #1 Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)

URI <http://mysign-ocsp.kmutt.ac.th>

Digital ID Detail



The screenshot displays a PDF viewer interface with a document titled "COVID-19-43.pdf". The document content is in Thai, discussing COVID-19 measures. A "Certificate Viewer" dialog box is open, showing the following details:

Certificate Viewer
This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

Show all certification paths found

▼ Thai University Consort
▼ King Mongkut's Univ
Suvit Tia <suvit.ti

Summary Details Revocation Trust Policies Legal Notice

Name	Value
Validity ends	2023/02/09 12:08:17 +07'00'
Authority info a...	<see details>
CRL distributio...	<see details>
Extended key u...	Client Authentication, Email Protect

Method = OCSP
URI = http://mysign-ocsp.kmutt.ac.th

i The selected certificate path is valid.
The path validation and revocation checks were done as of the signing time:
2022/11/01 19:45:20 +07'00'
Validation Model: Shell

OK



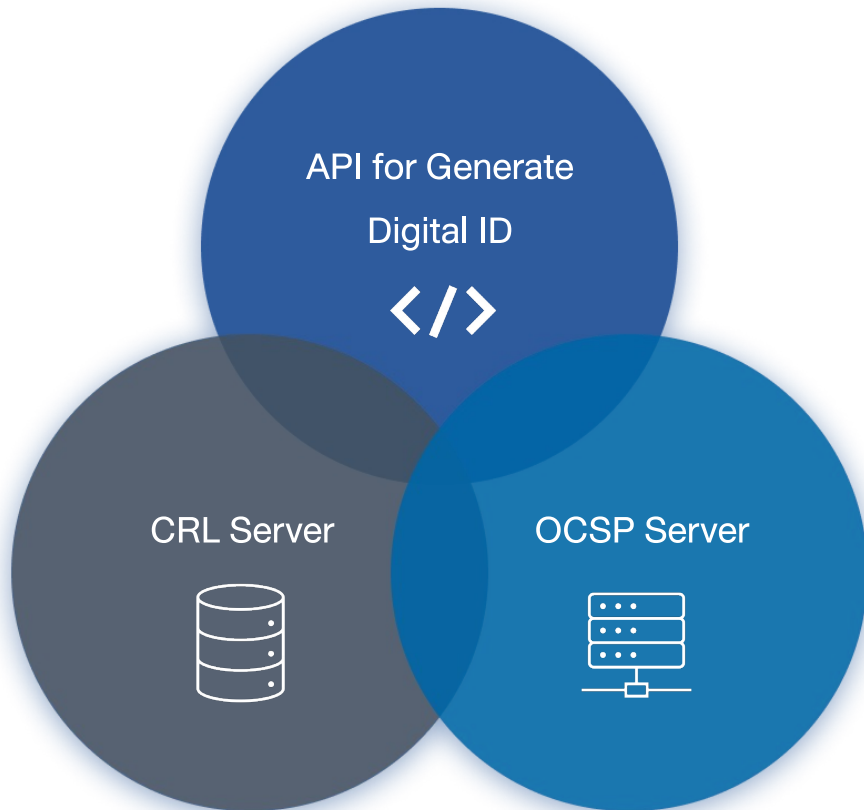
สำนักคอมพิวเตอร์
Computer Center



INNOVASIVE

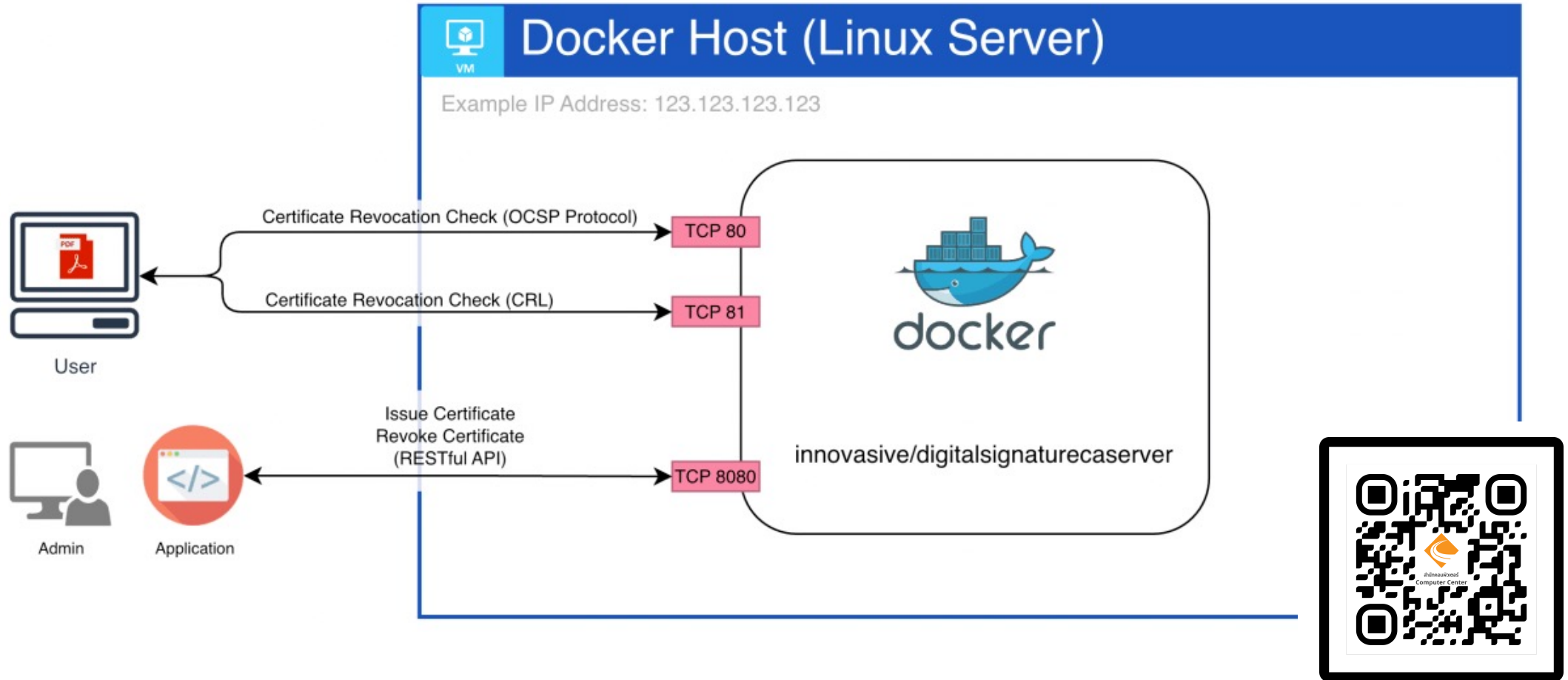
CA API Server

CA API Server



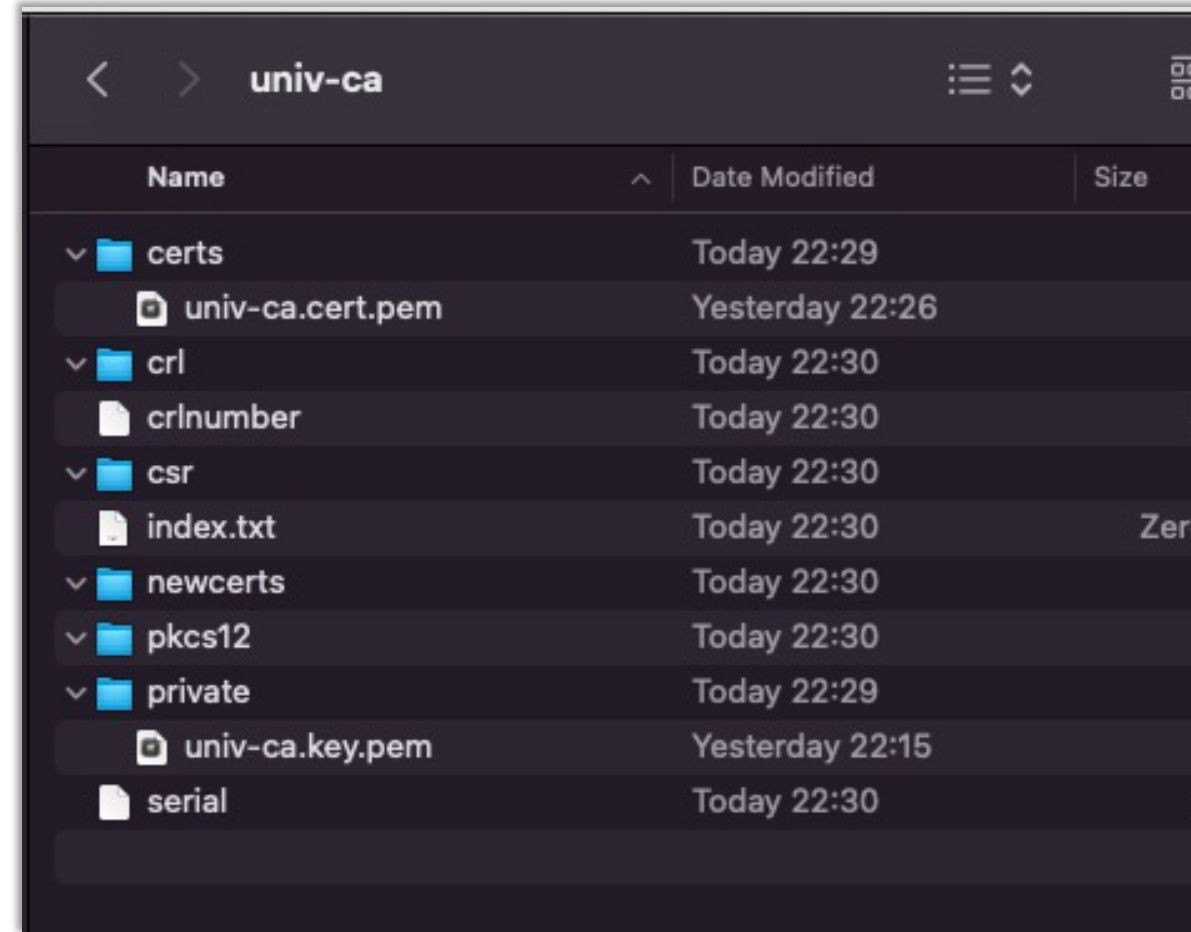
SCAN ME

CA API Server



Preparation

- Server for Docker
- Public IP and Domain Name
- /univ-ca
 - Private
 - csr



STEP 1

- สร้าง config file ชื่อ .env โดยมีเนื้อหาดังนี้

```
OCSP_BASE_URL={OCSP_URL}
```

```
CRL_BASE_URL={OCSP_URL}
```

```
CA_PRIVKEY_PASSWORD={PASSWORD}
```

```
API_KEY={API_KEY}
```

```
.env — digitalsignaturecaserver

.env x
.env
1 OCSP_BASE_URL=http://ca-poc.innovasive.co.th
2 CRL_BASE_URL=http://ca-poc.innovasive.co.th:81
3 CA_PRIVKEY_PASSWORD=password
4 API_KEY=developmentkey
5
```

STEP 2

- Run คำสั่งสำหรับการสร้าง docker

```
docker run -d --restart always --name digitalsignaturecaserver \
```

```
--publish 8080:8080 \
```

```
--publish 80:80 \
```

```
--publish 81:81 \
```

```
--env-file .env \
```

```
--volume ./univ-ca:/univ-ca \
```

```
innovative/digitalsignaturecaserver:0.1
```

```
chakree@Chakrees-MacBook-Pro digitalsignaturecaserver %  
docker run -d --name digitalsignaturecaserver \  
--publish 8080:8080 \  
--publish 80:80 \  
--publish 81:81 \  
--env-file .env \  
--volume ./univ-ca:/univ-ca \  
innovative/digitalsignaturecaserver:0.1  
  
Unable to find image 'innovative/digitalsignaturecaserver:0.1' locally  
0.1: Pulling from innovative/digitalsignaturecaserver  
a880266d3b77: Already exists  
0e81258012aa: Pull complete  
1b1ef9a0c36a: Pull complete  
3acd653ed006: Pull complete  
fe5f9afdd97c: Pull complete  
cd24ffcb4b1c: Pull complete  
d93ce17932f4: Pull complete  
5e31d0bb945c: Pull complete  
Digest: sha256:a8880f4484391ec094e6ab293a348ab3ac1545f11ce553f058ee82058ce79  
Status: Downloaded newer image for innovative/digitalsignaturecaserver:0.1  
33a7bf05d7264b43c15c570f77f2b40cf4dd9cddca4051d0ad7d1b7cc662a403  
chakree@Chakrees-MacBook-Pro digitalsignaturecaserver %
```


STEP 3

- Run คำสั่งสำหรับการสร้าง docker

docker logs digitalsignaturecaserver

```

chakree@Chakrees-MacBook-Pro univ-ca % docker logs digitalsignaturecaserver
      -+*****-.:++++=-+*****+:+++++=.
      *#####. ++++++*****-*****+
      *#####+ =+++++*= *****-
      :#####+ -+++++. :*****-
      -#####= =*****+ :*****=
      -#####- =*****+++++ +*****+
      +#####: +*****+:+++++= *****+
      *#####* +*****+ ++++++ =*****+
      *#####* *****+ =+++++ -*****+
      *#####+ *****= =+++++. :*****-
      :#####= *****- =+++++. :*****=
      -#####= *****: -+++++ :*****=
      *#####. ***** ++++++ +*****+
      *#####: *****= =+++++ -*****-
      *#####* +*****+ ++++++ -*****+:
      +#####+ +*****+ ++++++ =*****+
      =#####: +*****: ++++++ -*****-
      -#####- *****: ++++++ -*****+
      :#####+ *****+++++ :---: *****=
      *#####: ****+++++. :++: *****=
      *#####* :*****+ .==-.:+++++
      *#####* :+++++. =*****+
      +#####*: ++++++* =*****+.
      =#####- -+++++*****: +*****=
      .-----:-----:-----:-----
Digital Signature CA API Server for POC by Innovasive Co., Ltd.

Checking if /univ-ca is mounted correctly
/univ-ca is mounted, OK
/univ-ca/index.txt does not exists, creating empty file...

/univ-ca/crlnumber does not exists, creating file...

/univ-ca/serial does not exists, creating file..

/univ-ca/csr does not exists, creating folder...

/univ-ca/newcerts does not exists, creating folder...

/univ-ca/pkcs12 does not exists, creating folder...

/univ-ca/ocsp does not exists, creating folder...
  
```



สำนักคอมพิวเตอร์
Computer Center



INNOVASIVE

API Usage

API Doc



- API Document

- กำหนด API Key Header:

X-INNOVASIVE-API-KEY:

{API_KEY_ENV_FILE}

CA Server API

Share Fork 0

Overview **Authorization** Pre-request Script Tests Variables Runs

This authorization method will be used for every request in this collection. You can override this by specifying one in the request.

Type

The authorization header will be automatically generated when you send the request. [Learn more about authorization](#)

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

Key

Value

Add to

API Doc

- Issue Certificate API
- Revoke Certificate API
- Download PKCS12 By Certificate Serial Number
- List Certificates from CA Index Database

Issue Certificate API

Web Services: RESTful JSON

HTTP Method: **POST**

Content Type: x-www-form-urlencoded

Character Encoding: UTF-8

URL: `http://<docker-host>:8080/api/v1/issue`

Request

No.	Parameter	Type	Size	Mandatory	Description	Example Values
1	cn	String	64	Y	Common Name of Certificate	Somchai Jaidee
2	email	String	64	Y	Email of Certificate	somchai@example.ac.th
3	password	String	64	Y	PKCS12 Encryption Password	P@ssw0rd
4	days	Integer	3	Y	Certificate Validity Periods in days	90

Issue Certificate API

Response

No.	Parameter	Type	Size	M	Description	Example Values
1	success	Boolean	1	Y	Response Success Indicator	true
2	code	Integer	3	Y	Response Code	200
3	serial	String	20	N	Certificate Serial Number	1000
4	certificate_file	String	-	N	Certificate File Full Path In univ-ca Folder	/univ-ca/certs/1000.cert.pem
5	private_key_file	String	-	N	Private Key File Full Path In univ-ca Folder	/univ-ca/private/1000.key.pem
6	pkcs12_file	String	-	N	PKCS12 File Full Path In univ-ca Folder	/univ-ca/pkcs12/1000.p12
7	errors	Array of String	-	N	Array Content of Strings for Error Details	-

Issue Certificate API

Example

CA Server API / Issue

POST {{ENDPOINT}}/issue

Params Auth Headers (8) Body Pre-req. Tests Settings Cookies

x-www-form-urlencoded

	Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/>	cn	Somchai Jaidee			
<input checked="" type="checkbox"/>	email	somchai@example.ac.th			
<input checked="" type="checkbox"/>	password	test1234			
<input checked="" type="checkbox"/>	days	30			

Body 200 OK 914 ms 378 B Save as Example

Pretty Raw Preview Visualize JSON

```
1 {
2   "success": true,
3   "code": 200,
4   "serial": "01",
5   "certificate_file": "/univ-ca/certs/01.cert.pem",
6   "private_key_file": "/univ-ca/private/01.key.pem",
7   "pkcs12_file": "/univ-ca/pkcs12/01.p12"
8 }
```

Revoke Certificate API

Web Services: RESTful JSON

HTTP Method: **POST**

Content Type: x-www-form-urlencoded

Character Encoding: UTF-8

URL: `http://<docker-host>:8080/api/v1/revoke`

Request

No.	Parameter	Type	Size	Mandatory	Description	Example Values
1	cn	String	64	Y	Common Name of Certificate	Somchai Jaidee
2	serial	String	64	Y	Certificate Serial Number	1000

Revoke Certificate API

Response

No.	Parameter	Type	Size	M	Description	Example Values
1	success	Boolean	1	Y	Response Success Indicator	true
2	code	Integer	3	Y	Response Code	200
3	errors	Array of String	-	N	Array Content of Strings for Error Details	-

Revoke Certificate API

Example

The screenshot shows a REST client interface for a CA Server API. The request is a POST to `{{ENDPOINT}}/revoke` with a body of `x-www-form-urlencoded`. The body contains two parameters: `serial` with value `01` and `cn` with value `Somchai Jaidee`. The response is a 200 OK status with a response time of 55 ms and a body size of 195 B. The response body is displayed in JSON format as `{ "success": true, "code": 200 }`.

CA Server API / Revoke

POST `{{ENDPOINT}}/revoke` Send

Params Auth Headers (8) **Body** Pre-req. Tests Settings Cookies

x-www-form-urlencoded

	Key	Value	Description	...	Bulk Edit
<input checked="" type="checkbox"/>	serial	01			
<input checked="" type="checkbox"/>	cn	Somchai Jaidee			

Body Cookies Headers (5) Test Results 200 OK 55 ms 195 B Save as Example

Pretty Raw Preview Visualize JSON

```

1 {
2   "success": true,
3   "code": 200
4 }
```

Download PKCS12 By Certificate Serial Number



Web Services: RESTful JSON

HTTP Method: GET

Character Encoding: UTF-8

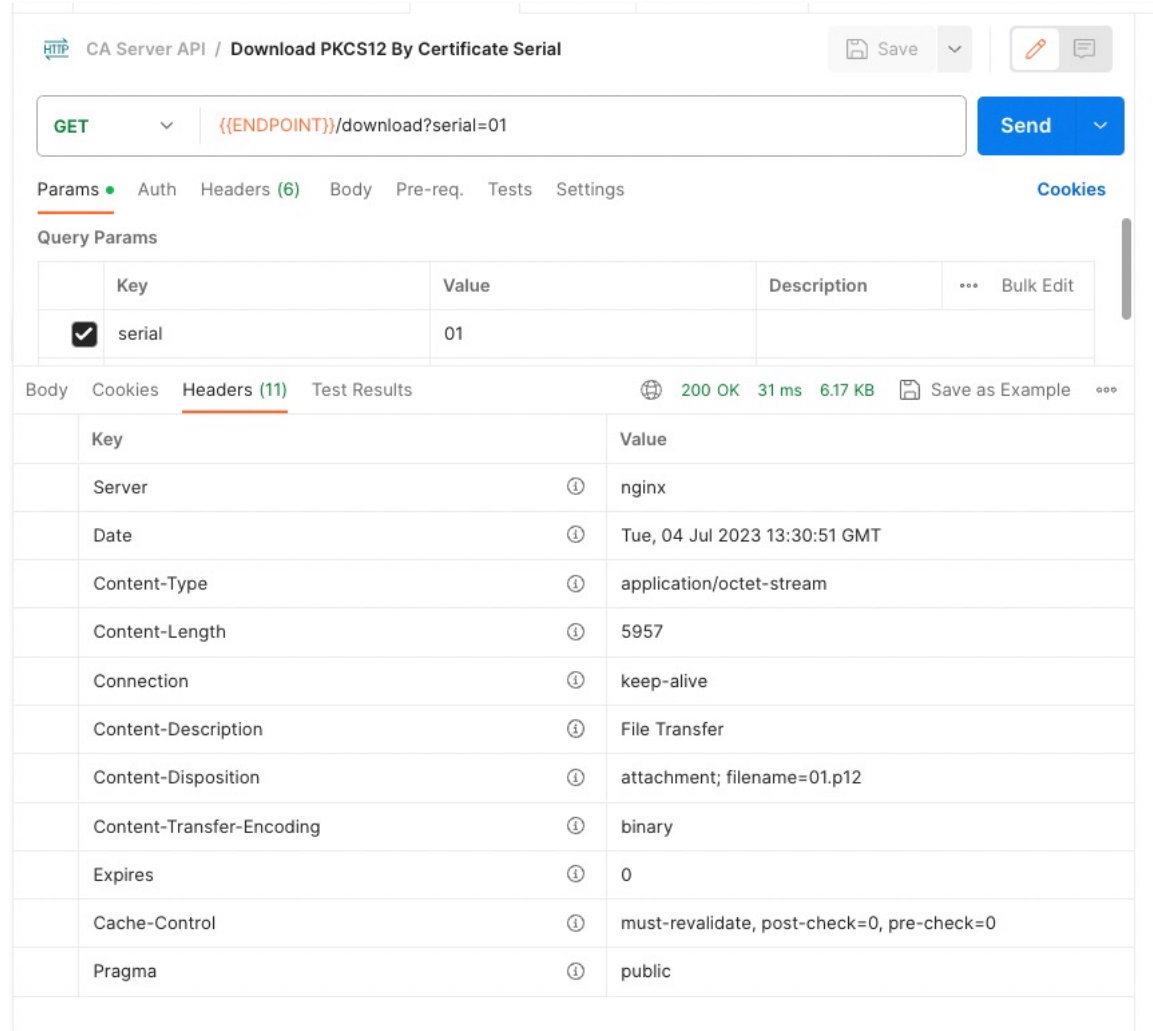
URL: http://<docker-host>:8080/api/v1/download

Request

No.	Parameter	Type	Size	M	Description	Example Values
1	serial	String	64	Y	Certificate Serial Number	1000

Download PKCS12 By Certificate Serial Number

Example



The screenshot shows a REST client interface for a CA Server API endpoint. The request is a GET method to `{{ENDPOINT}}/download?serial=01`. The response is a 200 OK status with a 31 ms response time and a 6.17 KB body. The response headers are displayed in a table below.

Key	Value
Server	nginx
Date	Tue, 04 Jul 2023 13:30:51 GMT
Content-Type	application/octet-stream
Content-Length	5957
Connection	keep-alive
Content-Description	File Transfer
Content-Disposition	attachment; filename=01.p12
Content-Transfer-Encoding	binary
Expires	0
Cache-Control	must-revalidate, post-check=0, pre-check=0
Pragma	public

List Certificates



Web Services: RESTful JSON

HTTP Method: GET

Character Encoding: UTF-8

URL: `http://<docker-host>:8080/api/v1/listCertificate`

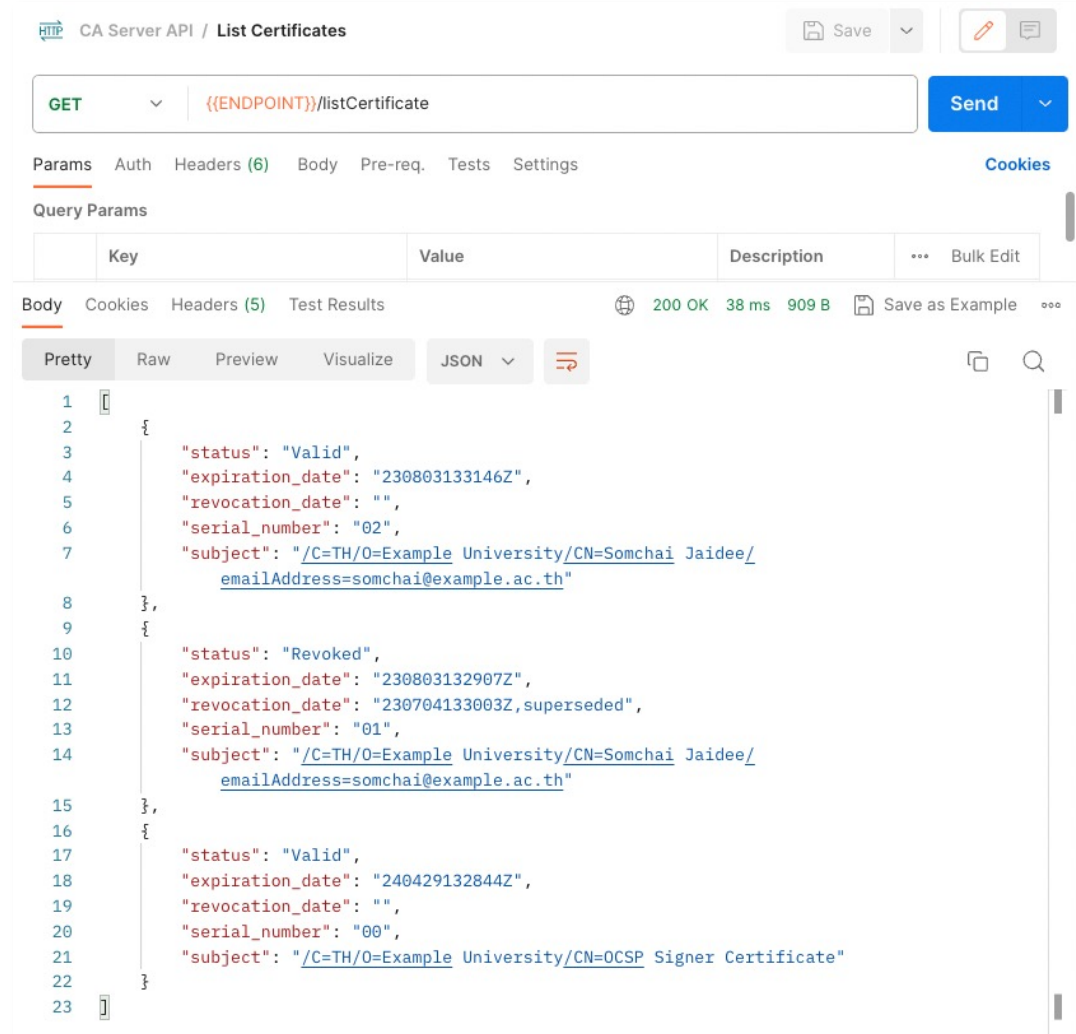
List Certificates

Response

No.	Parameter	Type	Size	M	Description	Example Values
1	status	String	-	Y	Certificate Status	Valid, Revoked, Expired
2	expiration_date	String	-	Y	Certificate Expiration Date	230803094143Z
3	revocation_date	String	-	N	Certificate Revocation Date	230704095756Z,superseded
4	serial_number	String	-	Y	Certificate Serial Number	1000
5	subject	String	-	Y	Certificate Subject	/C=TH/O=Example University/CN=Somchai Jaidee/emailAddress=somchai@exam ple.ac.th

List Certificates

Example



CA Server API / List Certificates

GET {{ENDPOINT}}/listCertificate

Params Auth Headers (6) Body Pre-req. Tests Settings Cookies

Query Params

Key	Value	Description	...	Bulk Edit
-----	-------	-------------	-----	-----------

Body Cookies Headers (5) Test Results 200 OK 38 ms 909 B Save as Example

Pretty Raw Preview Visualize JSON

```
1 {
2   {
3     "status": "Valid",
4     "expiration_date": "230803133146Z",
5     "revocation_date": "",
6     "serial_number": "02",
7     "subject": "/C=TH/O=Example University/CN=Somchai Jaidee/
8       emailAddress=somchai@example.ac.th"
9   },
10  {
11    "status": "Revoked",
12    "expiration_date": "230803132907Z",
13    "revocation_date": "230704133003Z,superseded",
14    "serial_number": "01",
15    "subject": "/C=TH/O=Example University/CN=Somchai Jaidee/
16      emailAddress=somchai@example.ac.th"
17  },
18  {
19    "status": "Valid",
20    "expiration_date": "240429132844Z",
21    "revocation_date": "",
22    "serial_number": "00",
23    "subject": "/C=TH/O=Example University/CN=OCSP Signer Certificate"
24  }
25 }
```



INNOVASIVE

KMUTT MySign 2.0

KMUTT MySign 2.0

- Integration to KMUTT Mobile Service
- E-Document Workflow
- Sign on Web

2.0

KMUTT MySign 2.0



KMUTT My Sign - Digital Signature On Web POC Powered By **INNOVASIVE**

PDF 2. ประกาศรับสมัคร พอ.สсу. 256 Download PDF

Previous Page 1 / 5 Next Page Digialy Sign


All Document Signature are Valid.

Signature #1 (Valid) SHA-256
Signed By Sumet Angkasirikul
(sumet.ang@kmutt.ac.th)
At 2023-06-29 16:20:49

Thai University Consortium Certification Authority
King Mongkut's University of Technology Certification Authority
Sumet Angkasirikul , SIT

Signature #2 (Valid) SHA-256
Signed By อธิวิท อินโนเวชีพ จำกัด
At 2023-07-11 23:24:32

Thailand National Root Certification Authority - G1
INET CA - G1
บริษัท อินโนเวชีพ จำกัด



ประกาศมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
เรื่อง รับสมัครบุคคลเพื่อคัดเลือกเข้าเป็นพนักงาน
ตำแหน่งผู้อำนวยการสถาบันพัฒนาและฝึกอบรมโรงงานต้นแบบ

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี มีความประสงค์จะรับสมัครบุคคลเพื่อดำรงตำแหน่งผู้อำนวยการสถาบันพัฒนาและฝึกอบรมโรงงานต้นแบบ จำนวน 1 อัตรา โดยมีรายละเอียดดังนี้

- คุณสมบัติหลัก**
 - ต้องมีคุณสมบัติตามที่กำหนดโดยมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี พ.ศ. 2541 มาตรา 35 และมีคุณสมบัติได้รับปริญญาชั้นโทขึ้นไปจากมหาวิทยาลัยหรือสถาบันการศึกษาชั้นสูงอื่นที่สภามหาวิทยาลัยรับรอง และมีประสบการณ์ด้านการบริหารหรือด้านวิชาชีพที่เกี่ยวข้องมาแล้วไม่น้อยกว่า 3 ปี (รายละเอียดแนบท้ายประกาศ)
- คุณสมบัติทั่วไป**
 - 2.1 ความรู้และทักษะด้านวิชาการ**
 - (1) มีสัญชาติเป็นไทย
 - (2) มีความดีมีใจและสร้างสรรคทางด้านวิชาการ
 - (3) มีความสนใจ เอาใจใส่ในหลักการและปรัชญาการศึกษา มีความเป็นนักวิชาการ ยอมรับในความสำคัญและสนับสนุนการพัฒนาวิชาการทุกสาขา
 - 2.2 ความรู้และทักษะด้านผู้นำ**
 - (1) มีความคิดริเริ่ม
 - (2) มีใจกว้างในการรับฟังข้อคิดเห็นจากผู้ร่วมงานทุกฝ่ายและทุกระดับ
 - (3) มีความมีนทหาอารมณ์ ถ้าจำเป็นจึงใช้ปัญหาและสามารถตัดสินใจให้เหมาะสมกับเหตุการณ์
 - (4) มีความสามารถในการประสานความสัมพันธ์ระหว่างผู้ร่วมงานและผู้ปฏิบัติงานได้เป็นอย่างดี
 - (5) มีบุคลิกภาพที่ดีไม่เกิดความเครียด ความเคารพในเกียรติ และเชื่อถือในผู้ร่วมงาน
 - (6) มีคุณธรรมและจริยธรรม อันเป็นตัวอย่างที่ดี
 - (7) มีความรับผิดชอบสูงและองการดีไกล
 - 2.3 ความรู้และทักษะด้านการบริหาร**
 - (1) มีประสบการณ์และผลงานที่ดีในการบริหาร
 - (2) มีความสามารถในการวางนโยบายและแผนงาน และสามารถบริหารงานให้เป็นไปตามแนวนโยบายและแผนงานที่วางไว้ สามารถชักจูงนำทีมงานในหน่วยงานที่ได้รับมอบหมายเพื่อให้ได้ผลตามต้องการและมีประสิทธิภาพ
 - (3) สามารถสร้างลักษณะการทำงานร่วมกันเป็นหมู่คณะ
 - (4) สามารถคิดริเริ่มสร้างสรรค์ มีความสามารถเข้าร่วมงาน สามารถจัดตั้งทีมให้เหมาะสมกับงานและผูกพันกับจิตใจให้อยู่ร่วมงานทำงานต่อไป สามารถใช้เวลาได้เต็มที่ในการบริหารงานสถาบัน สำนัก และส่วนงานที่เกี่ยวข้อง อย่างไรก็ตามเทียบเท่าคณะ รวมทั้งมหาวิทยาลัยและงานอื่นๆ ที่เป็นเกียรติแห่งมหาวิทยาลัย สามารถคิดริเริ่มหรือจัดหาระบบการวิจัยและทรัพย์สินเข้าสู่สถาบัน สำนัก และส่วนงานที่เกี่ยวข้องอย่างอื่นที่มีฐานะเทียบเท่าคณะ และมหาวิทยาลัย

Q & A

