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

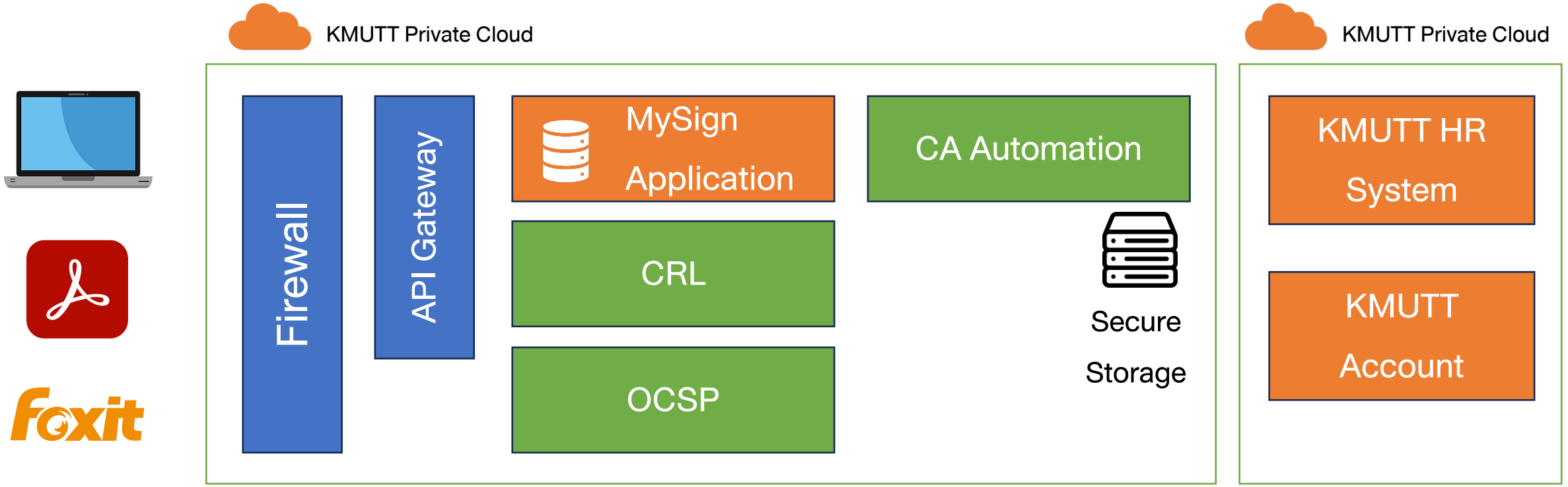
MySign Application

CA Automation Server

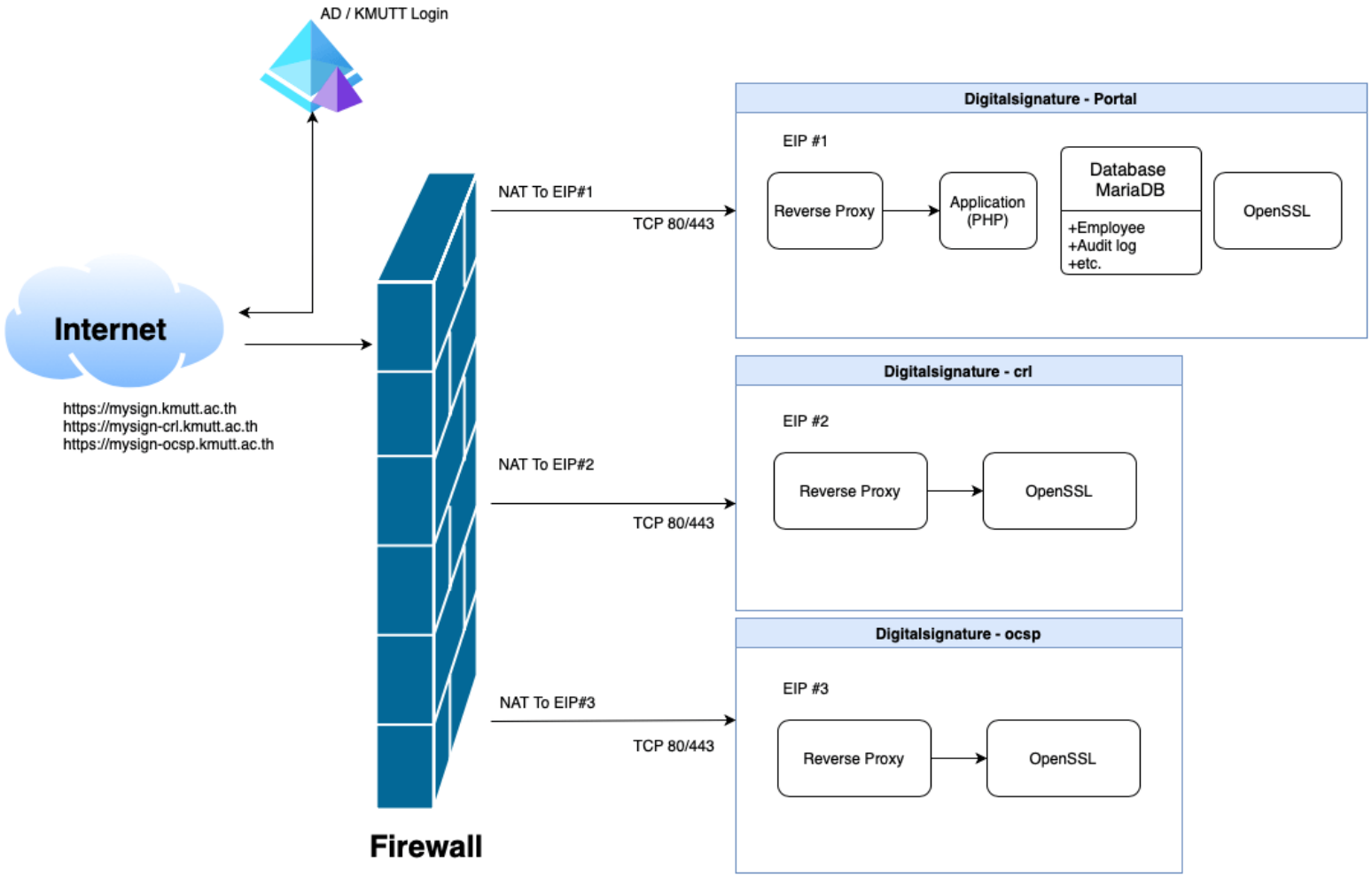
CRL Server

OCSP Server

Architecture

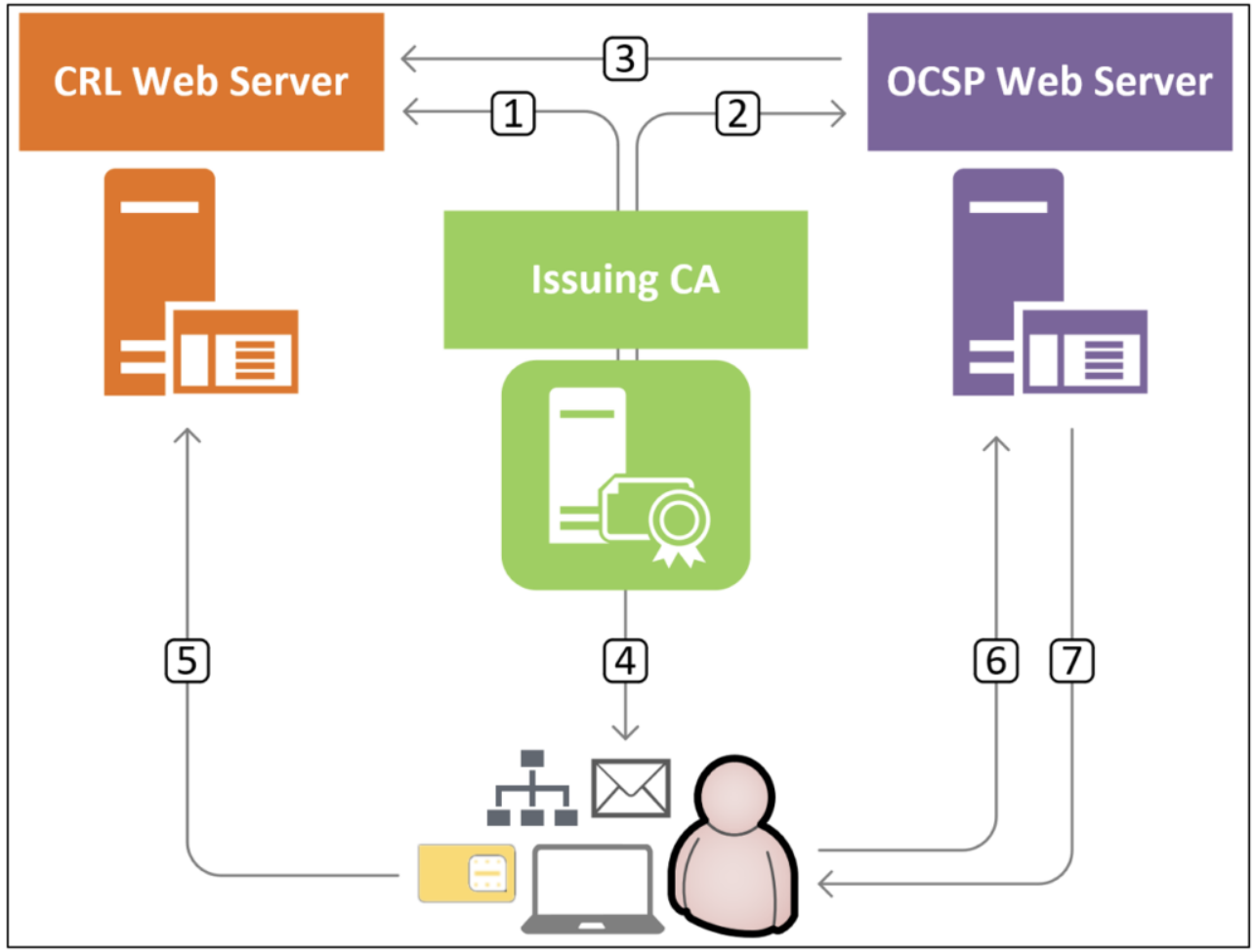


Architecture



CA Working Protocol

CA Architecture



Digital ID Detail

Subject Name

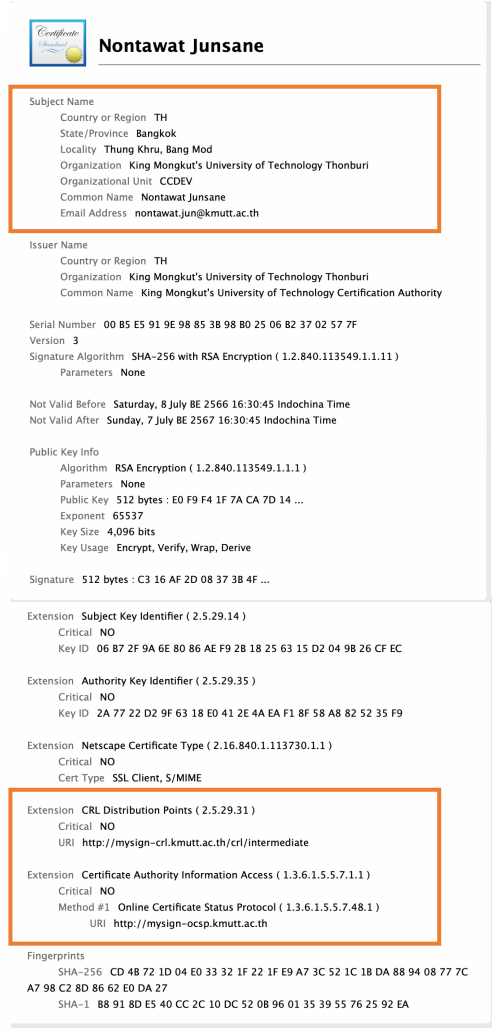
- Country or Region TH
- State/Province Bangkok
- Locality Thung Khru, Bang Mod
- Organization King Mongkut's University of Technology Thonburi
- Organizational Unit CCDEV
- Common Name Nontawat Junsane
- Email Address nontawat.jun@kmutt.ac.th

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



Nontawat Junsane

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

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 B5 E5 91 9E 98 85 3B 98 B0 25 06 B2 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

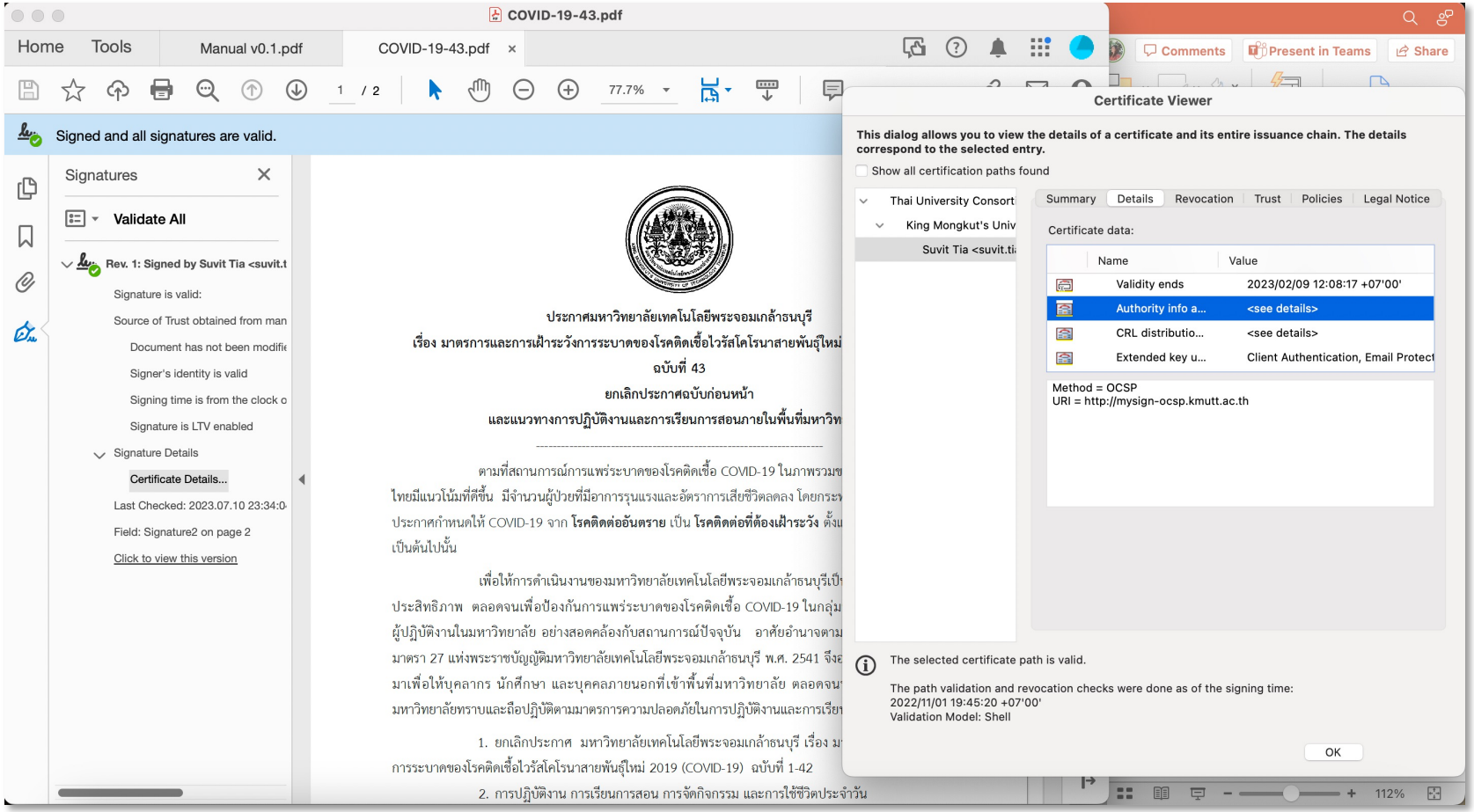
Extension Netscape Certificate Type (2.16.840.1.113730.1.1)
Critical NO
Cert Type SSL Client, S/MIME

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

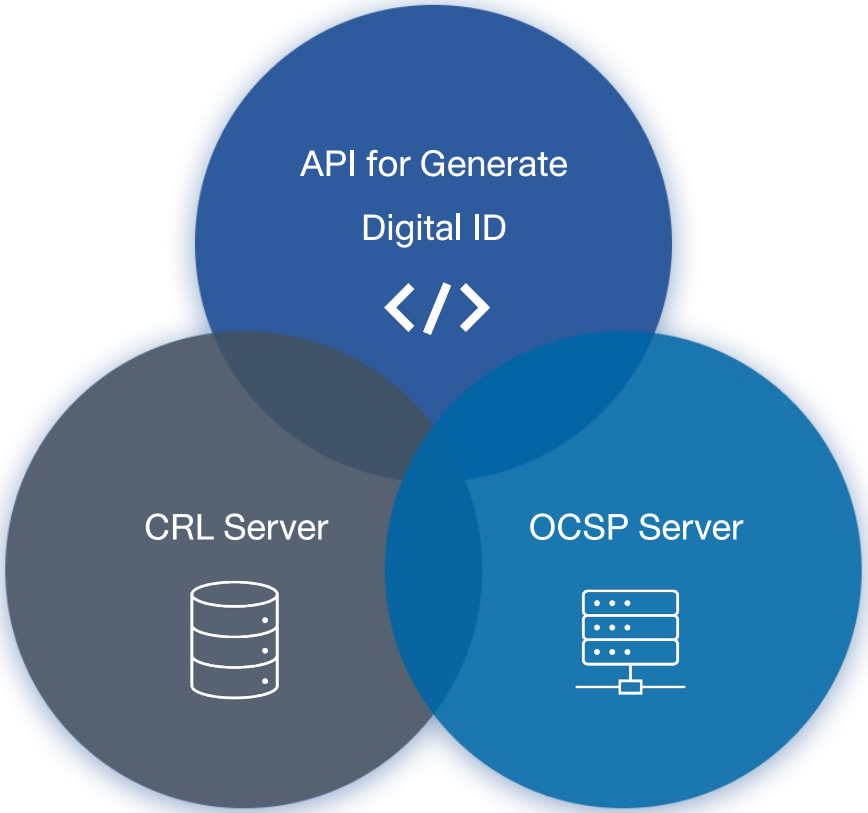
Fingerprints
SHA-256 CD 48 72 1D 04 E0 33 32 1F 22 1F E9 A7 3C 52 1C 1B DA 88 94 08 77 7C A7 98 C2 8D 86 62 E0 DA 27
SHA-1 B8 91 8D E5 40 CC 2C 10 DC 52 0B 96 01 35 39 55 76 25 92 EA

Digital ID Detail



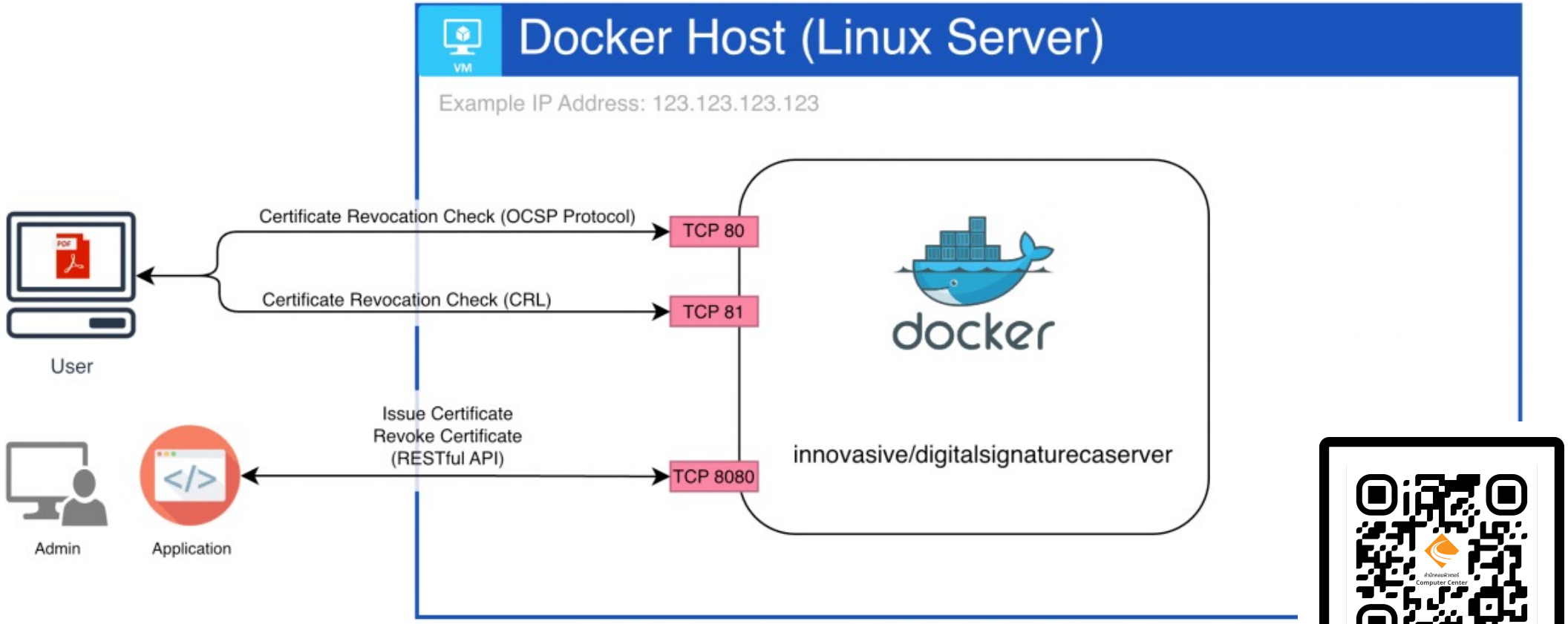
CA API Server

CA API Server



SCAN ME

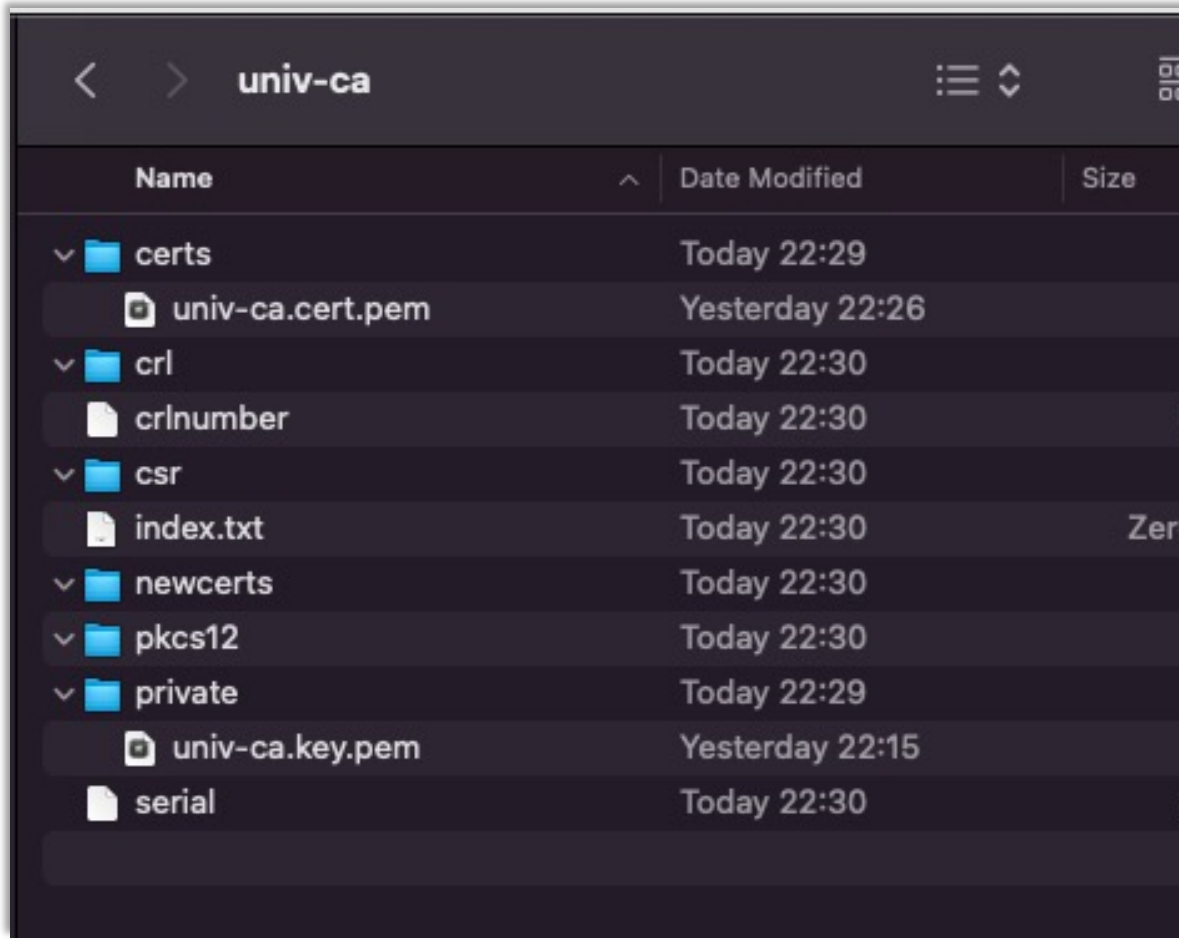
CA API Server



SCAN ME

Preparation

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



STEP 1

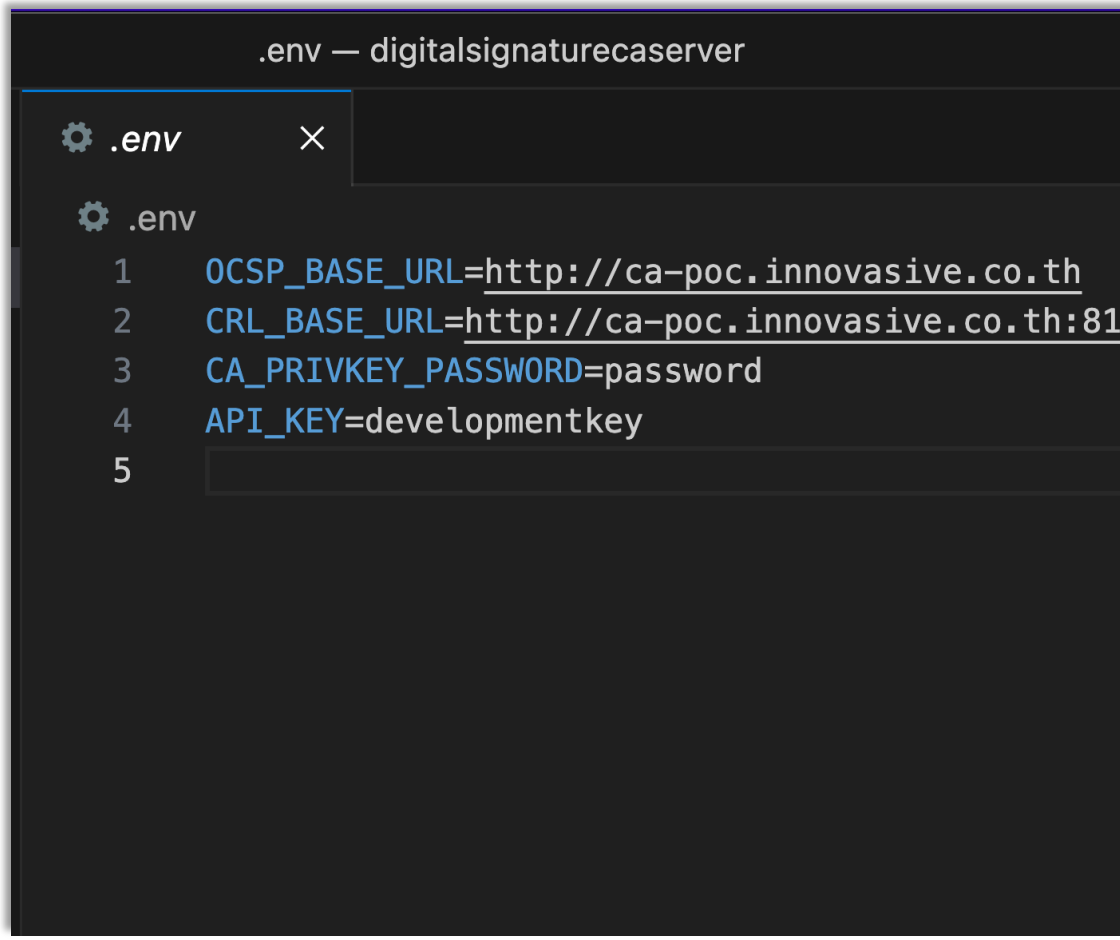
- สร้าง config file ชื่อ .env โดยมีเนื้อหาดังนี้

OCSP_BASE_URL={OCSP_URL}

CRL_BASE_URL={OCSP_URL}

CA_PRIVKEY_PASSWORD={PASSWORD}

API_KEY={API_KEY}



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 *

innovasive/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 \
innovasive/digitalsignaturecaserver:0.1

Unable to find image 'innovasive/digitalsignaturecaserver:0.1' locally
0.1: Pulling from innovasive/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 innovasive/digitalsignaturecaserver:0.1
33a7bf05d7264b43c15c570f77f2b40cf4dd9cddca4051d0ad7d1b7cc662a403
chakree@Chakrees-MacBook-Pro digitalsignaturecaserver %
```

STEP 3

- Run คำสั่งสำหรับการสร้าง docker

docker logs digitalsignaturecaserver

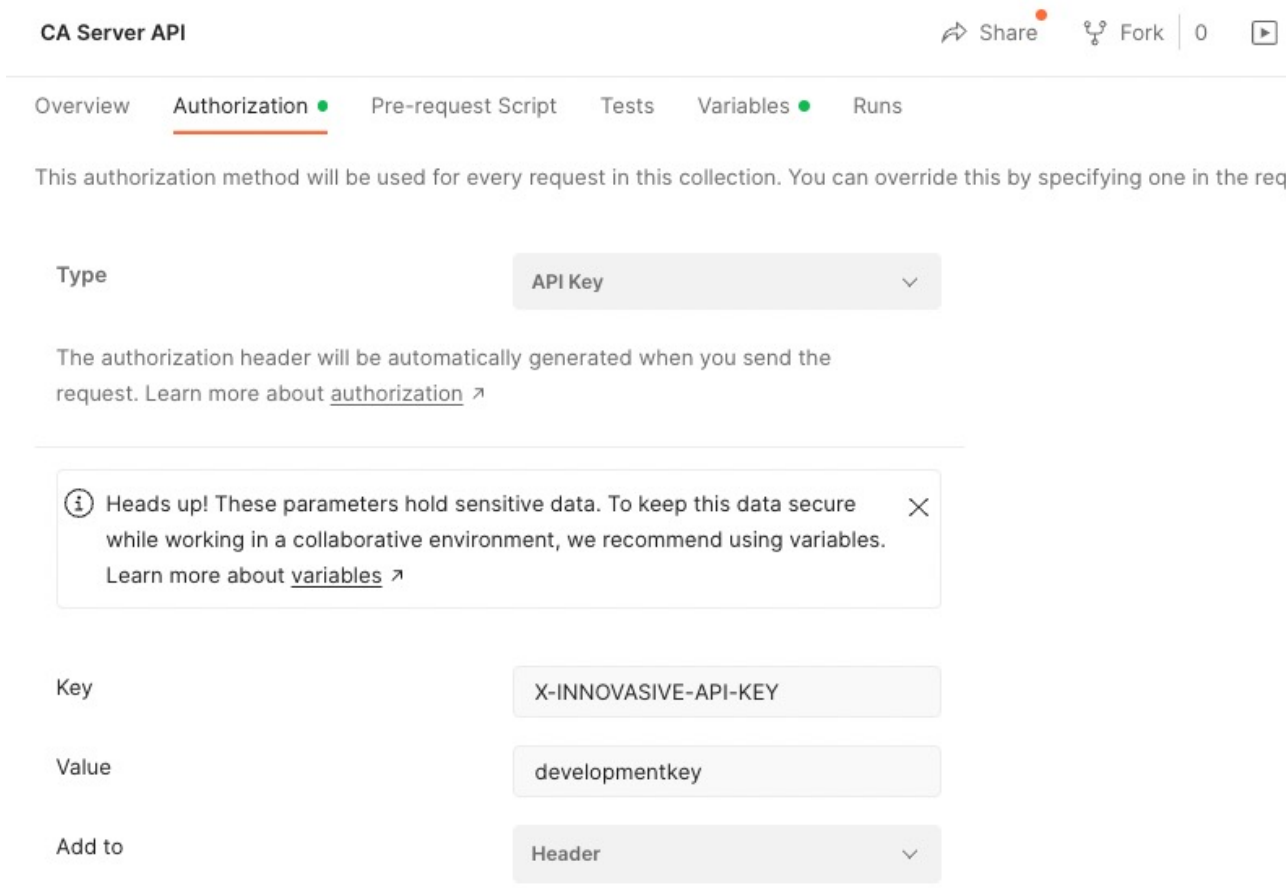
API Usage

API Doc

- API Document
  - กำหนด API Key Header:

    X-INNOVASIVE-API-KEY:

    {API_KEY_ENV_FILE}



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

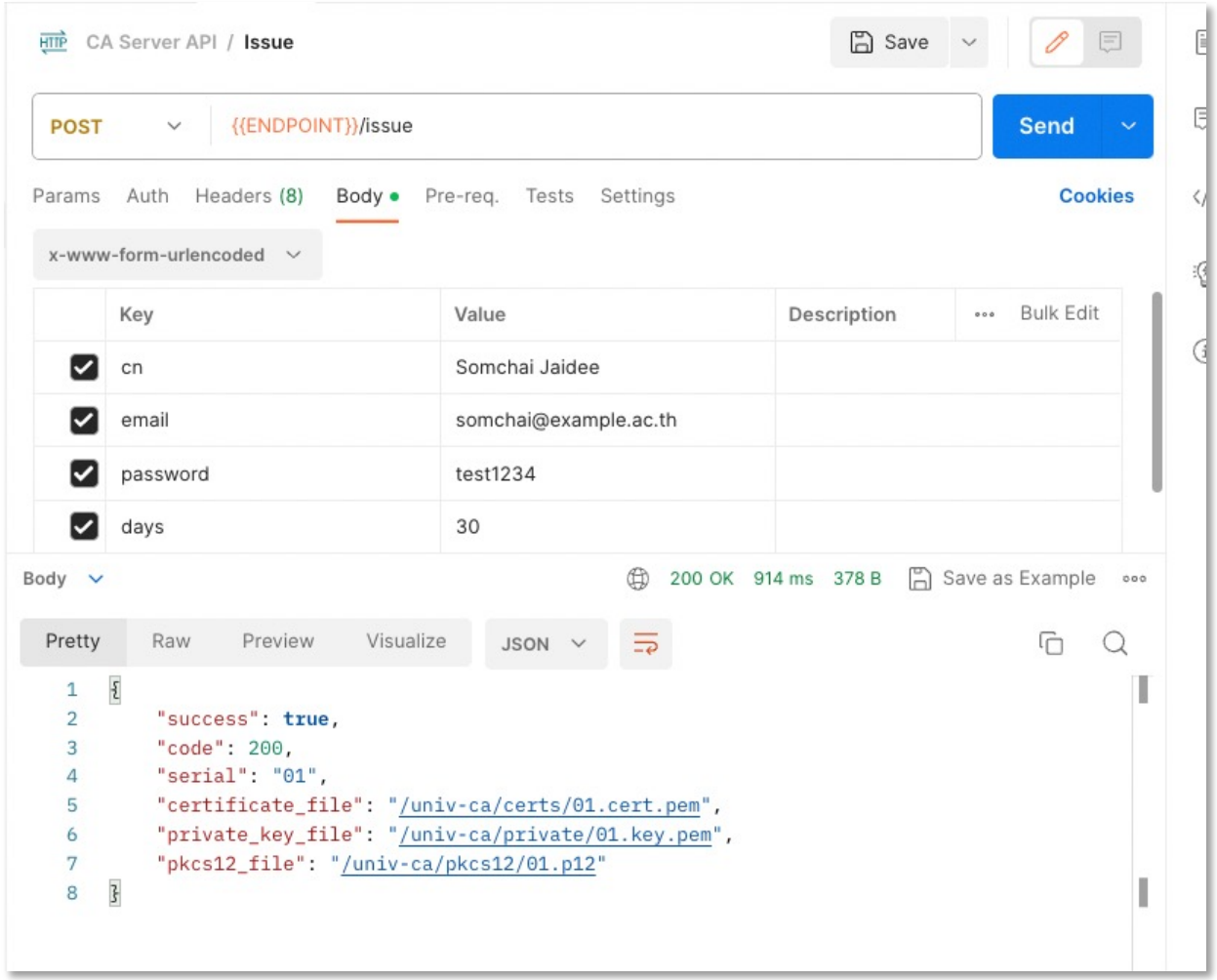
Issue Certificate API

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



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

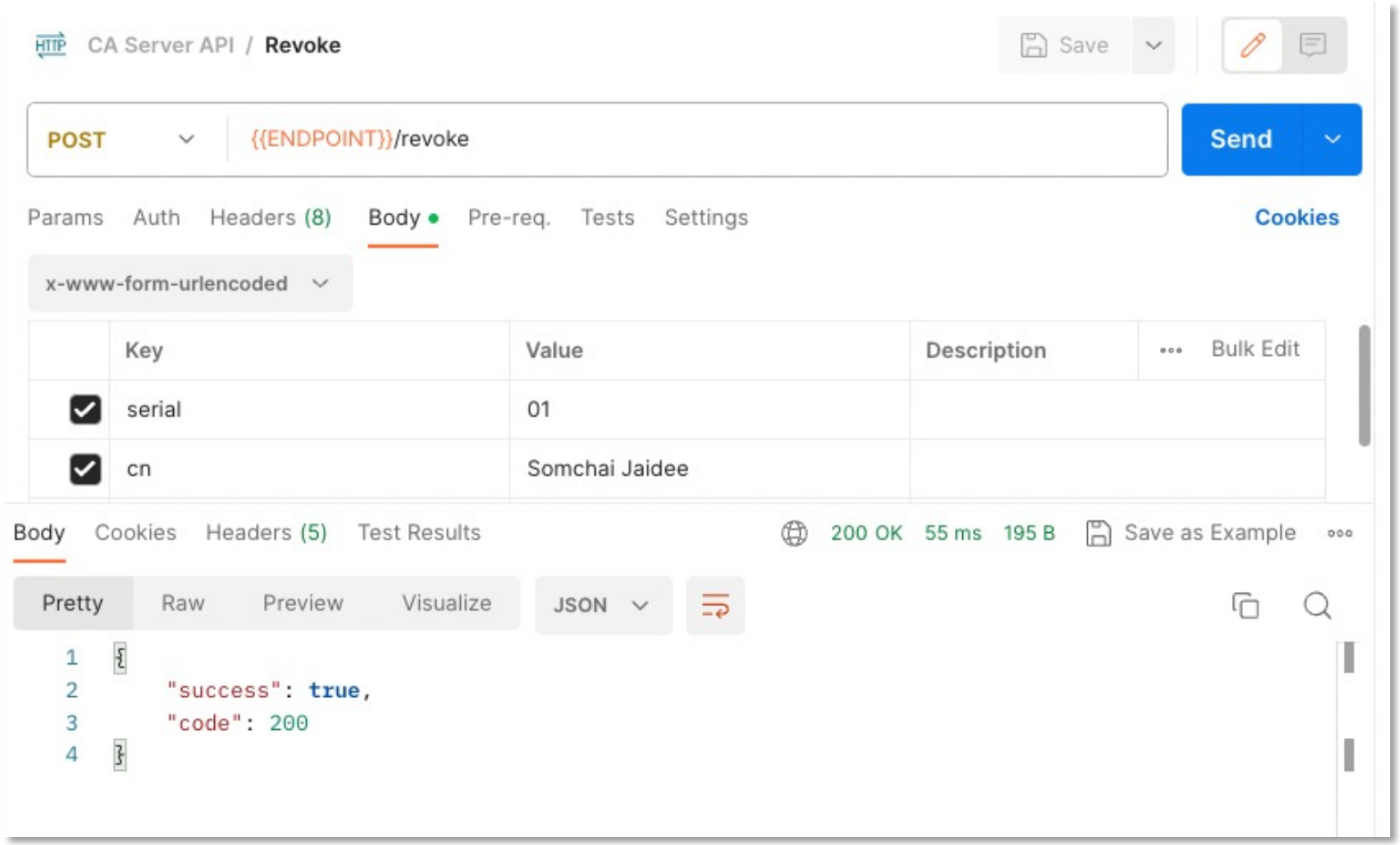
Revoke Certificate API

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



Download PKCS12 By Certificate Serial Number

Web Services: RESTful JSON

HTTP Method: GET

Character Encoding: UTF-8

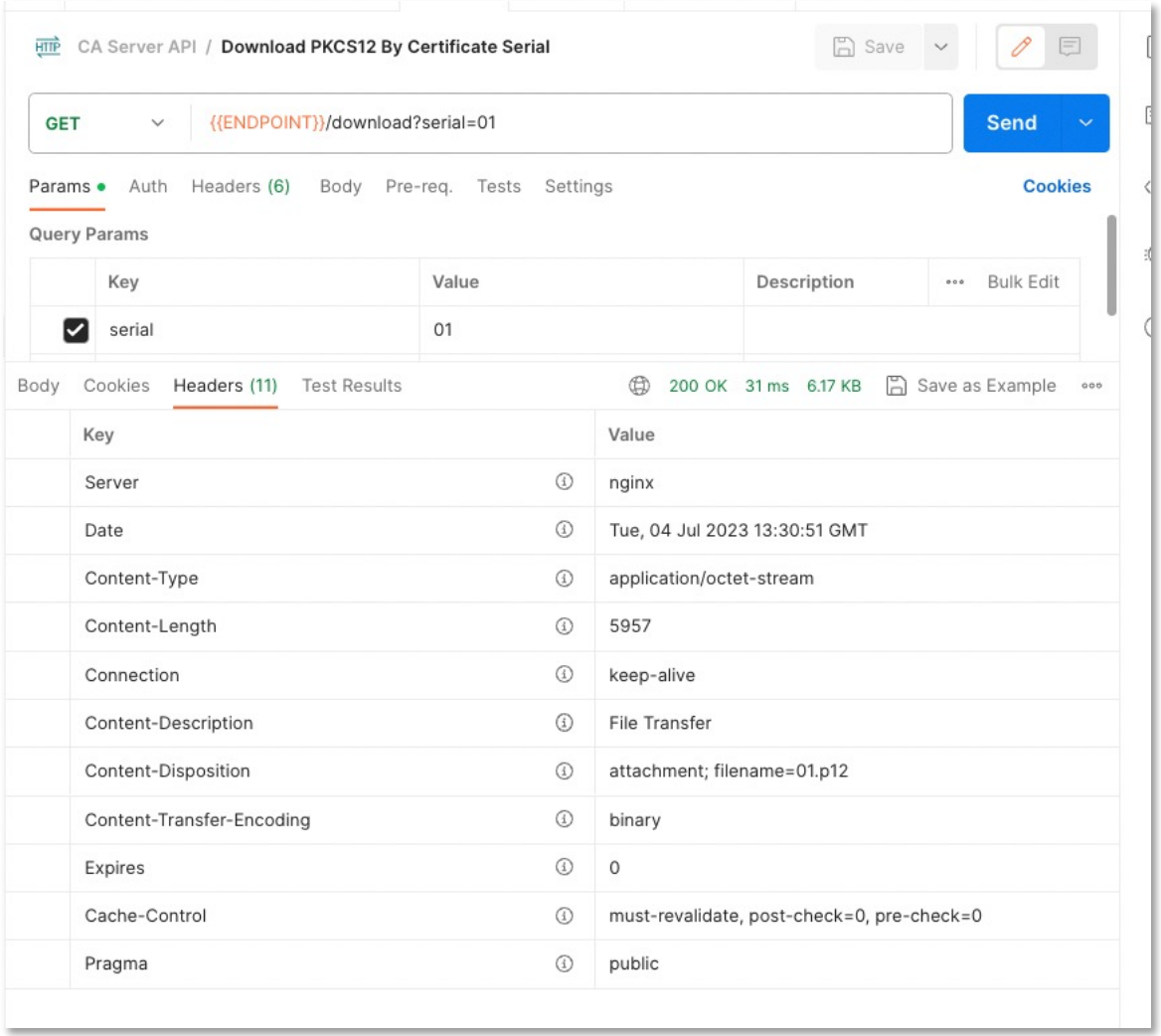
URL: http://<docker-host>:8080/api/v1/download

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



List Certificates

Web Services: RESTful JSON

HTTP Method: GET

Character Encoding: UTF-8

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

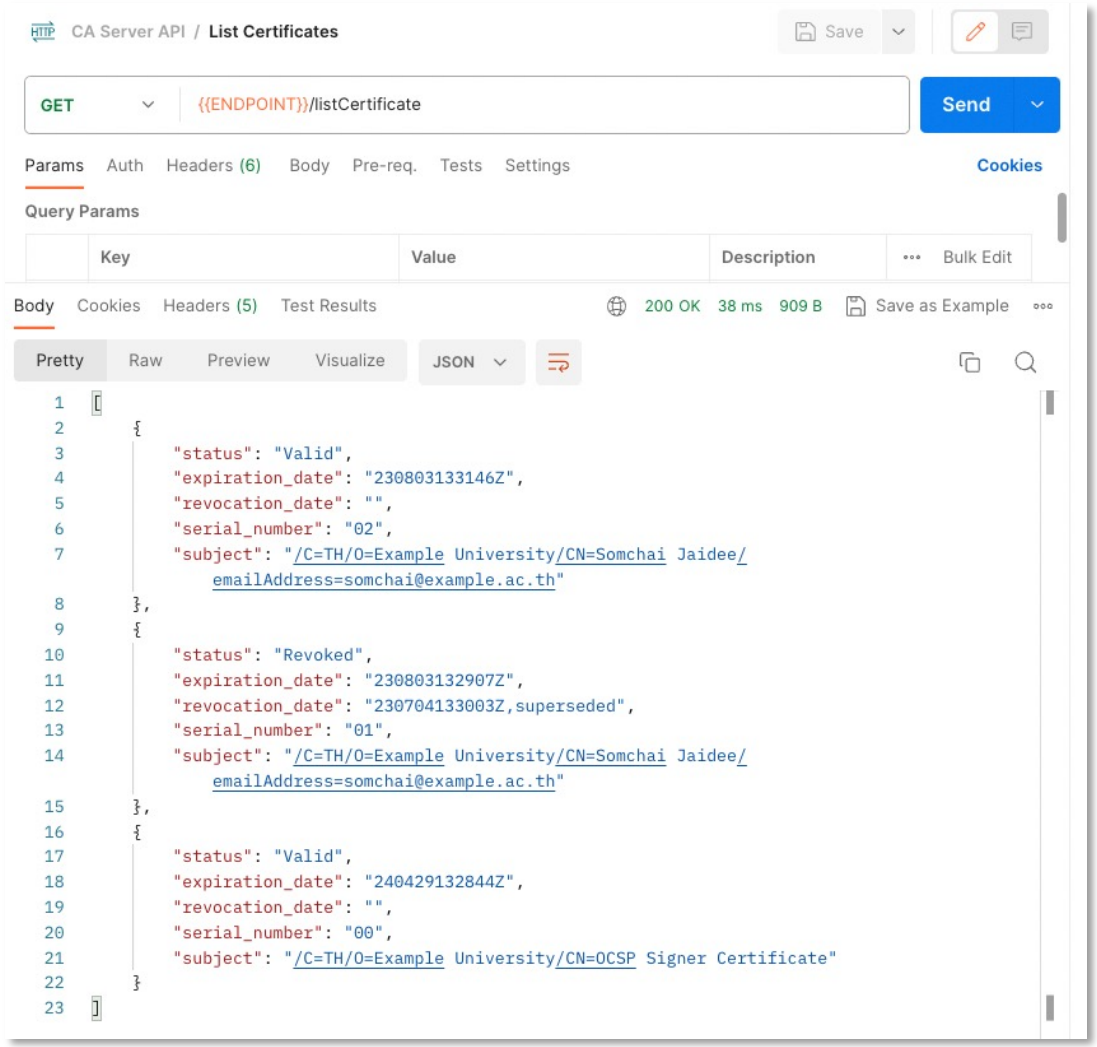
List Certificates

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@example.ac.th

List Certificates

Example



KMUTT MySign 2.0

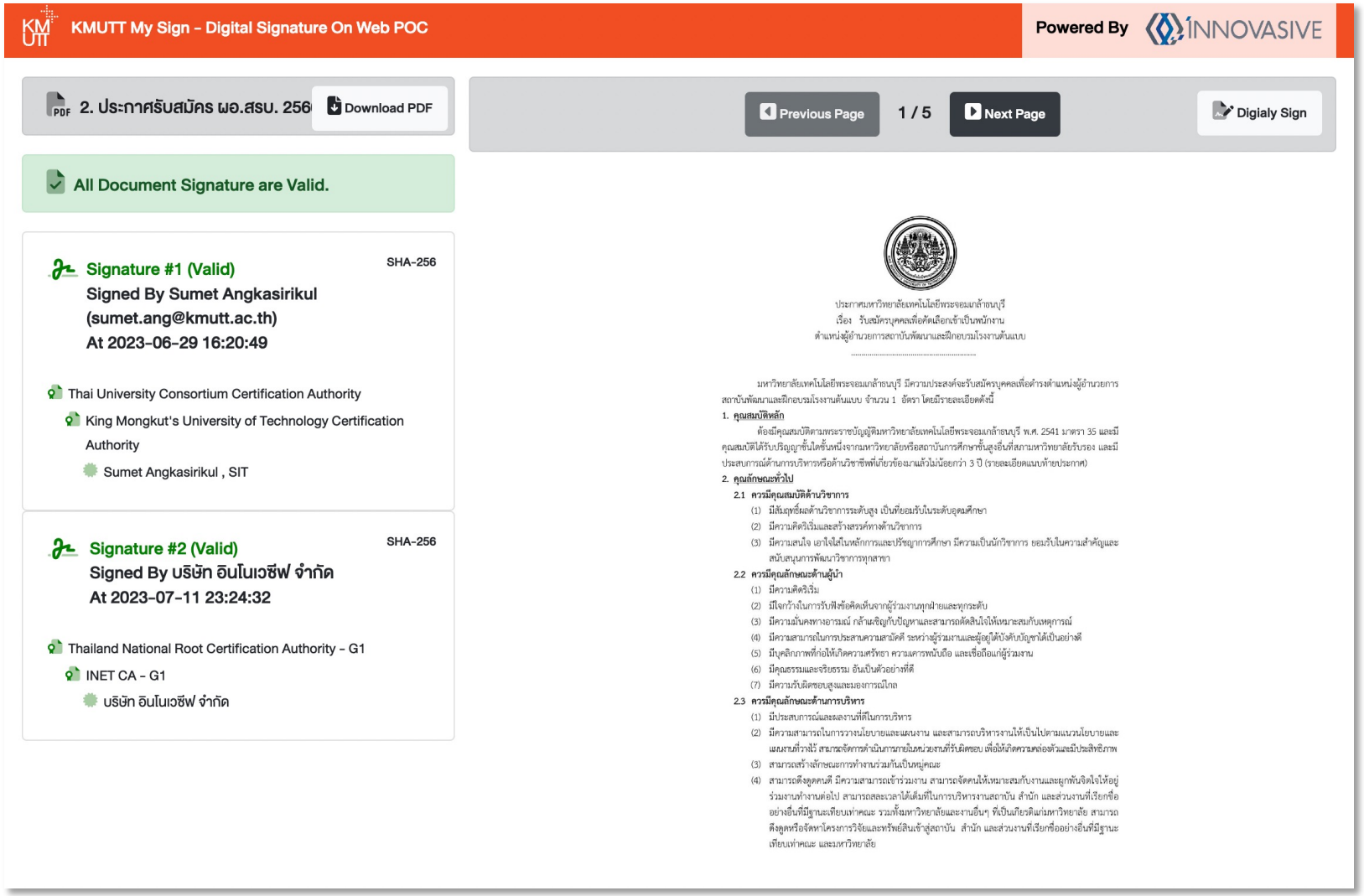
WUNCA #43 | 10–12 July 2023 at Khon Kaen University

KMUTT MySign 2.0

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

2.0

KMUTT MySign 2.0



Q & A

LINE