

Certificate Authority (CA)



DGIS



MEETING OBJECTIVE

Inform all of you:

- Launch Internal Certificate Authority
 - Request Certificate workflow
- Create Certificate Signing Request (CSR)



AGENDA

Why we need Internal CA?
Objective CA project
Certificate Criteria
Solution & Technical
Workflow
Timeline

Why we need Internal CA?

CERTIFICATE AUTHORITY (CA)



SSL ย่อมาจาก Secure Socket Layer ซึ่งเป็นมาตรฐาน ในการเข้ารหัสข้อมูล ก่อนส่งผ่านเครือข่าย internet

ซึ่งประโยชน์ของ SSL สามารถสรุปคร่าวๆ ได้ดังนี้

เพิ่มความปลอดภัยในการ รับ/ส่ง ข้อมูล

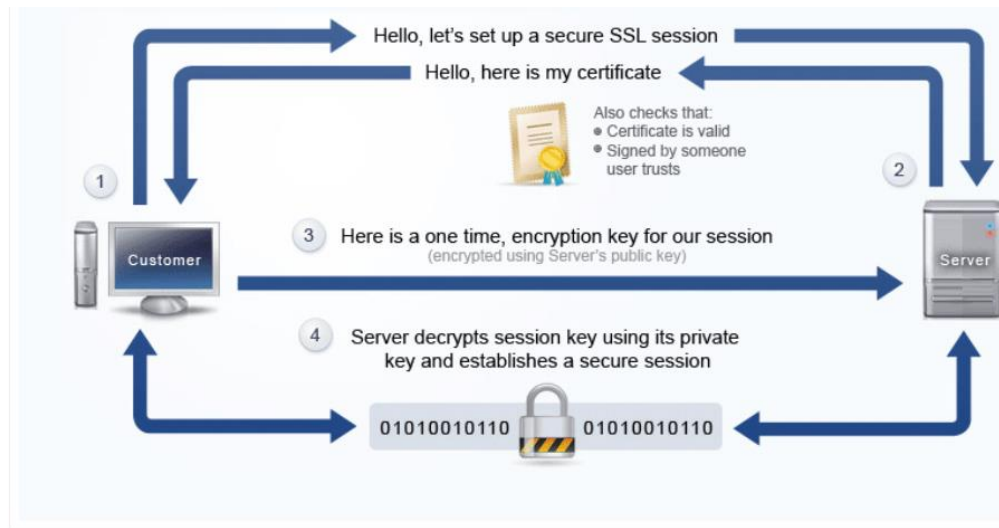
SSL ช่วยเข้ารหัสข้อมูล ก่อนส่งผ่านเครือข่าย internet ดังนั้น เมื่อมี Hacker หรือ มิจฉาชีพ ทำการดักจับข้อมูล (Sniffer) ที่วิ่งไปมา บนเครือข่าย ก็ไม่สามารถ อ่านข้อมูล ที่ดักจับได้ ดังนั้นจึงทำให้ข้อมูลสำคัญ ที่ส่งผ่านเครือข่าย อย่างเช่น เลขที่บัตรเครดิต หรือ รหัสผ่านต่างๆ มีความปลอดภัย มากขึ้น นอกจาก

ใช้ยืนยันตัวตน

SSL สามารถนำมาใช้ ในการยืนยันตัวตน ว่าเป็นบุคคลนั้นจริง ตามที่ระบุ ไม่ได้ถูกปลอมแปลงขึ้นมา ยกตัวอย่างเช่น เว็บไซต์ ที่เกี่ยวข้องกับ การทำธุรกรรมการเงิน ที่สำคัญ อย่างเช่น ธนาคาร จะใช้ SSL ระดับสูง ที่เป็น green bar และมีชื่อธนาคาร กำกับชัดเจน แต่ถ้าเป็นหน้าเว็บ ที่ถูกปลอมแปลงขึ้นมา อาจไม่ได้ใช้ SSL (URL นำหน้าด้วย http:// ธรรมดา) หรือ ถ้ามีการใช้ SSL (URL นำหน้าด้วย https://) ตัว browser ก็จะมีระบบแจ้งเตือน ให้ทราบ ในกรณีที่ใบรับรอง SSL ไม่ถูกต้อง เพื่อให้ผู้ใช้ ทราบว่า เว็บไซต์ที่กำลังใช้งาน อาจไม่ปลอดภัย

SSL Certificate Authority

SSL Certificates คือ ใบรับรองความปลอดภัยของข้อมูลที่รับ-ส่งผ่านทางอินเทอร์เน็ตซึ่งจะถูกออกโดยผู้ให้บริการ CA (Certificate Authority)



ภาพแสดงการทำงานของ SSL

- 1 Client ขอเชื่อมต่อกับ Server ผ่านโปรโตคอล SSL (URL นำหน้าด้วย https://)
- 2 Server ส่ง Certificate ที่ใช้ในการยืนยันตัวตน กลับมาให้ Client
- 3 Client สร้าง Key สำหรับเข้ารหัส แล้วส่งกลับไปให้ Server
- 4 Server ใช้ Key ที่ได้รับ สร้างช่องทางการเชื่อมต่อ ที่ปลอดภัย (Secure Session)

CERTIFICATE AUTHORITY (CA)

xxx Baht



xxxx Baht



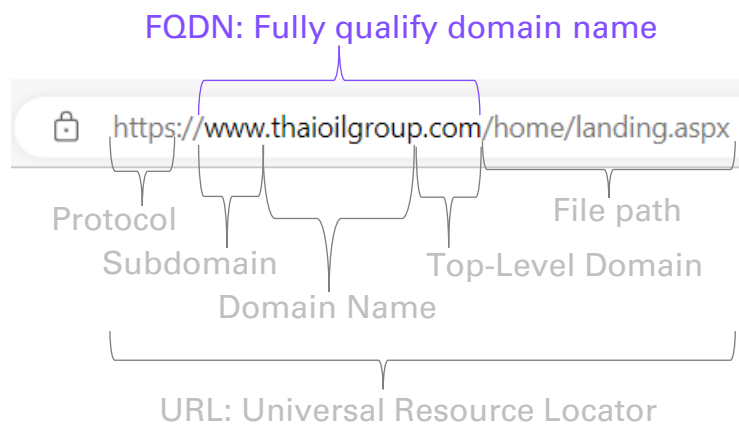
Wildcard Certificate

CERTIFICATE AUTHORITY (CA)

CA Type	Certificate Type	Thai Oil Direction
Public CA	* wildcard	Not Used
	per FQDN	For URL that need to serv public devices
	SAN cert (Multi FQDN)	For URL that need to serv public devices and project consist of many FQDN
Internal CA	* wildcard	Not Used
	per FQDN only thaioilgroup.com	Recommended
	SAN cert (Multi FQDN)	Recommended
Self Generated	Self-Signed Cert	Not Used

4. SSL แบบ WildCard SSL Certificate

Certificate ชนิดนี้จะมีการตรวจสอบแบบ Domain Validation (DV) และ Organization Validation (OV) โดยที่ใบรับรองความปลอดภัยของโดเมนหลัก (Base Domain) จะครอบคลุมการใช้งานทุกๆ โดเมนย่อย (multiple sub-domains) ภายใน Server ที่มีการติดตั้งใบรับรอง ยกตัวอย่างเช่น *.yourdomain.com, www.yourdomain.com, mail.yourdomain.com เป็นต้น สำหรับระยะเวลาออกใบรับรอง ขึ้นอยู่กับชนิดของการตรวจสอบว่าเป็นแบบ DV หรือ OV



tdcs.thaioilgroup.com/CHR/web/MainBoards.aspx

Certificate Viewer: *.thaioilgroup.com

General Details

Issued To **Wildcard Certificate**

Common Name (CN) *.thaioilgroup.com
Organization (O) Thai Oil Public Company Limited
Organizational Unit (OU) <Not Part Of Certificate>

Issued By

Common Name (CN) DigiCert TLS RSA SHA256 2020 CA1
Organization (O) DigiCert Inc
Organizational Unit (OU) <Not Part Of Certificate>

Validity Period

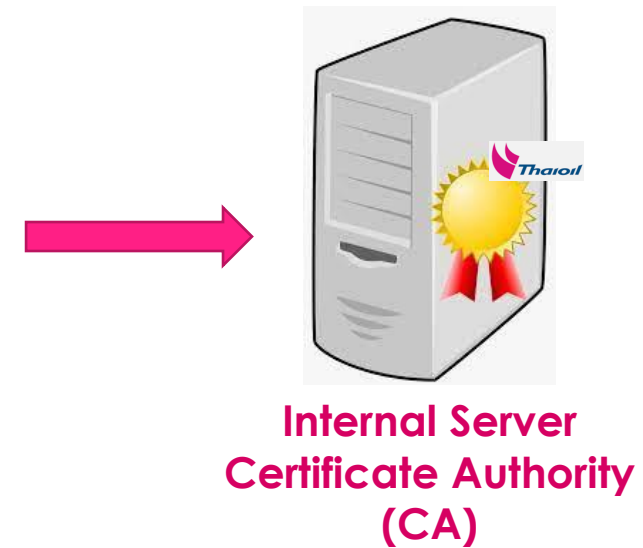
Issued On Tuesday, December 14, 2021 at 7:00:00 AM
Expires On Sunday, January 15, 2023 at 6:59:59 AM

Fingerprints

SHA-256 Fingerprint B8 97 32 33 4A 63 2E C1 76 FA C3 8B 68 54 2C 58
13 10 F3 0B C1 6B 6C AF 3C BF 3F DB 7A CE 64 CF
SHA-1 Fingerprint 62 89 3A 1A 07 9C 01 67 B7 03 3E 90 6E 1B 07 2D
D6 48 25 CD

Internal Certificate Authority

CERTIFICATE AUTHORITY (CA)



CA project

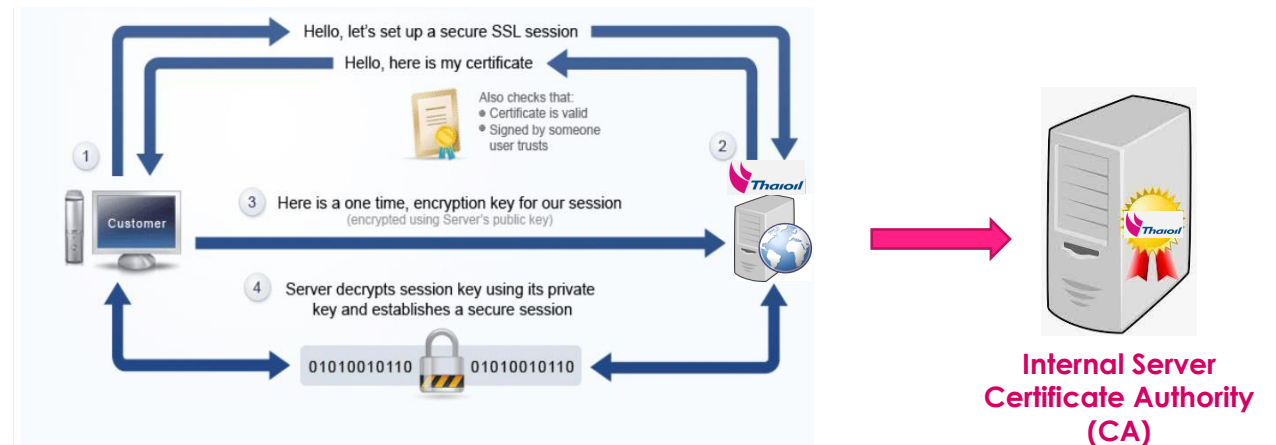
CERTIFICATE AUTHORITY (CA)

Objective:

- Improve Security
- Implement Internal CA
- Replace Public Wildcard Cert. by
 - Private Certificate issued by Internal CA or
 - Public Certificate Single Cert.
- Support Domain “.thaioilgroup.com” only

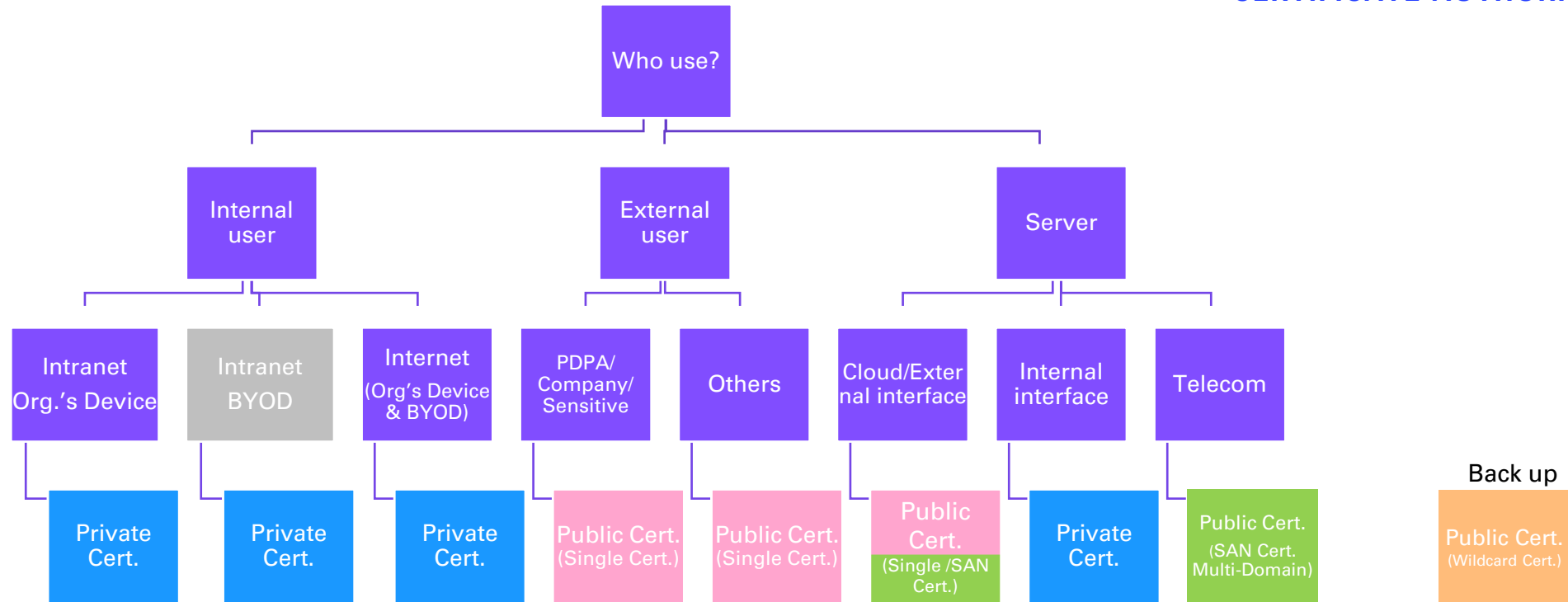
Assumption:

- Public Single Cert. < 10 items



Certificate Criteria

CERTIFICATE AUTHORITY (CA)

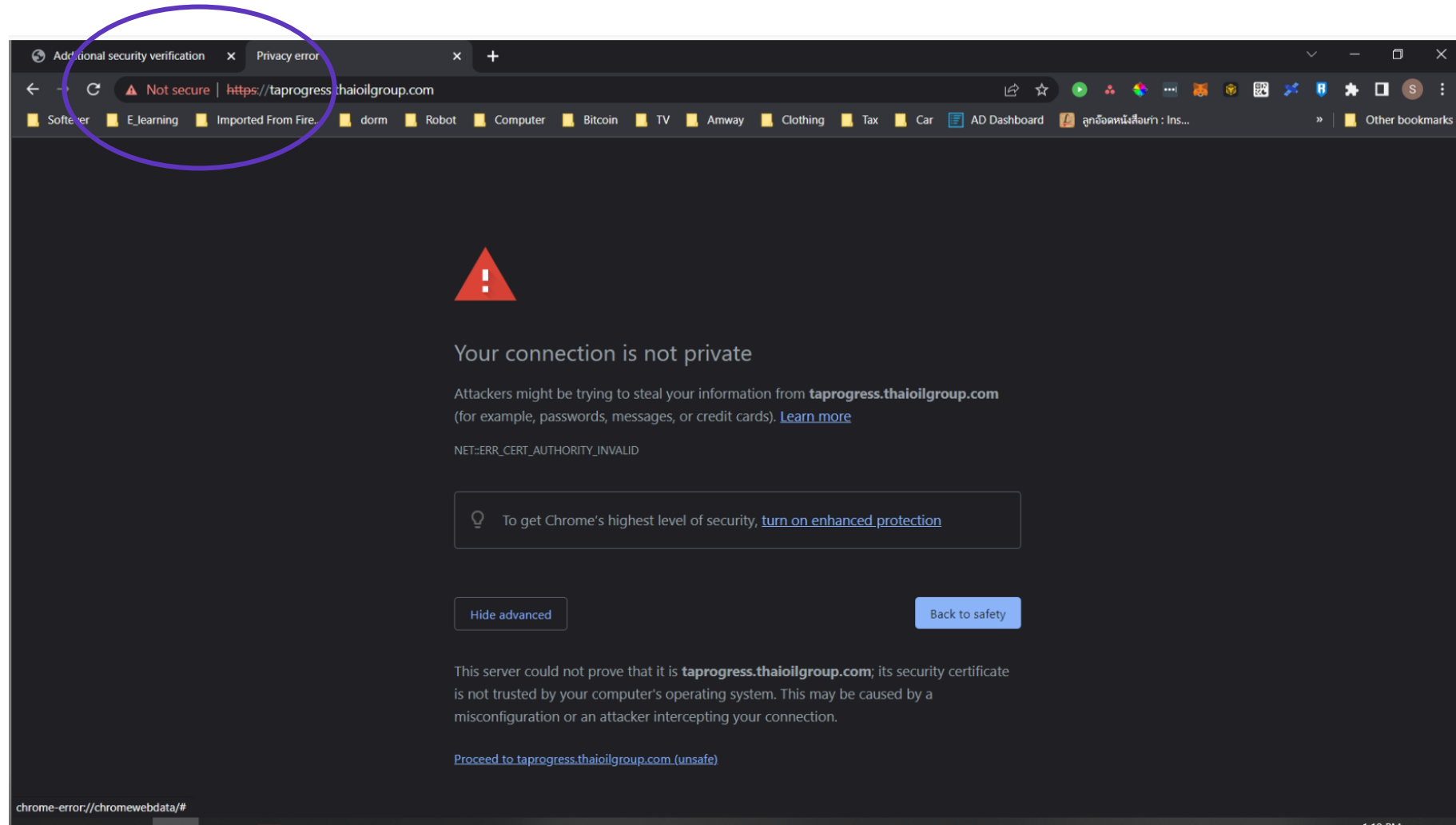


Noted:

- Sensitive is Financial, Commercial
- Private Cert. is provided by TOP CA only domain: thaioilgroup.com.
- Public Cert (Single Cert.) is purchased from public company for 1 Fully Qualify domain name (FQDN) PRD only, QAS and DEV use Private Cert. Est. budget 13,000 Baht/year
- Public Cert (Wild Cert.) is purchased from public company for multi-FQDN. Est. budget 32,000 Baht/year

Not secure notice

CERTIFICATE AUTHORITY (CA)



Public Cert: Single Cert. list

CERTIFICATE AUTHORITY (CA)

No.	FQDN
1	careers.thaioilgroup.com
2	cfpprodoc.thaioilgroup.com
3	dcc.thaioilgroup.com
4	onlinedriver.thaioilgroup.com
5	taprogress.thaioilgroup.com
6	thaioilsmartbiz.thaioilgroup.com
7	topcms.thaioilgroup.com
8	topir.thaioilgroup.com
9	voc.thaioilgroup.com
10	www.thaioilgroup.com

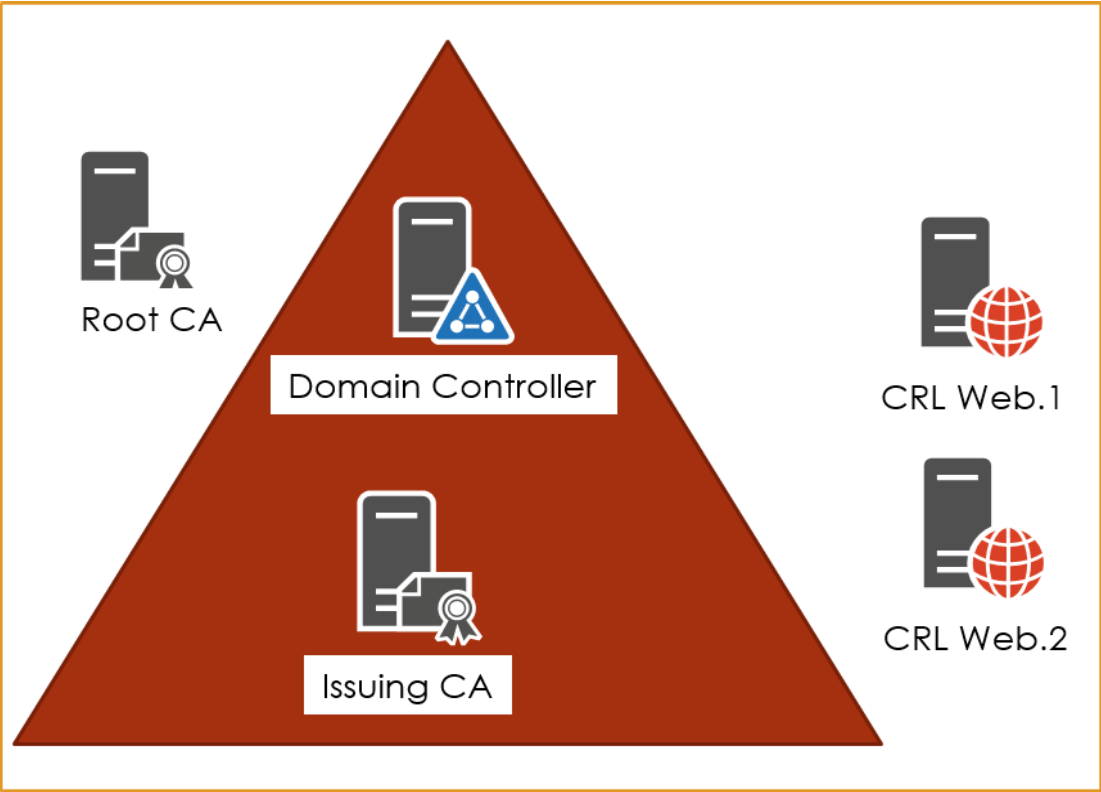
+

•

Purchase Certificate List 2.xlsx

CA server architecture

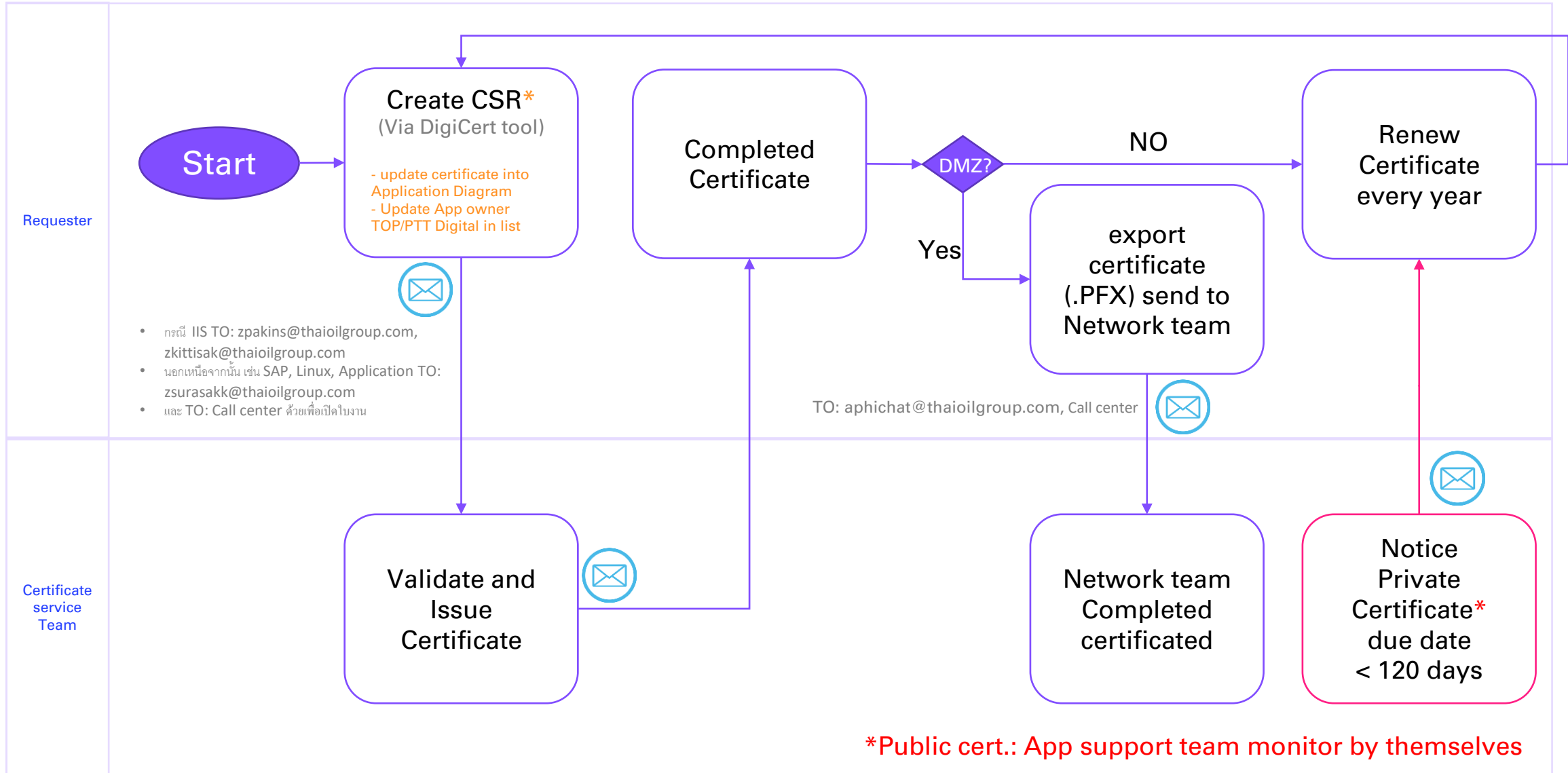
CERTIFICATE AUTHORITY (CA)



	Server	IP Address	Operating Systems
CRL Web.1	TSR-CER-CRLWEB01	10.66.12.181	Windows Server 2022 Standard (64-bit)
CRL Web.2	TSR-CER-CRLWEB02	10.66.12.182	Windows Server 2022 Standard (64-bit)
Issuing CA	TSR-CER-ENT	10.66.25.52	Windows Server 2022 Standard (64-bit)
Root CA	TSR-ROOTCA-02	10.66.19.92	Windows Server 2012

Workflow Private Certificate

CERTIFICATE AUTHORITY (CA)

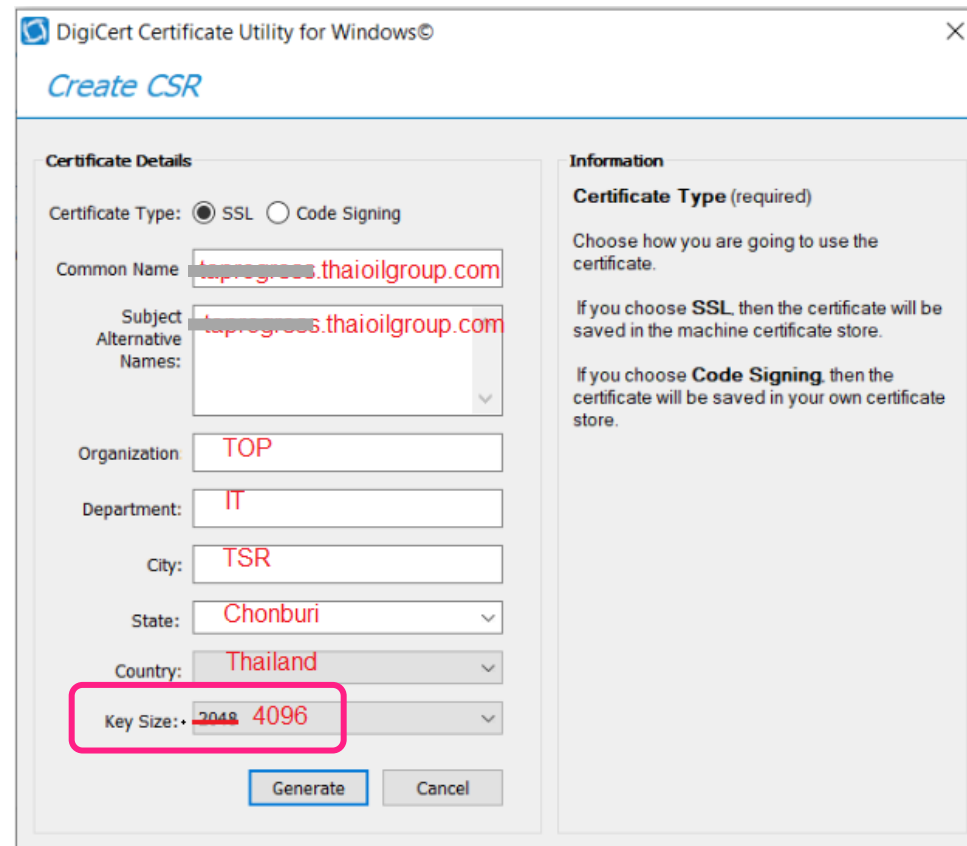


Create CSR via DigiCert.

CERTIFICATE AUTHORITY (CA)

Tools DigiCert <https://www.digicert.com/kb/util/csr-creation-microsoft-servers-using-digicert-utility.htm>

Example:



The screenshot shows the 'DigiCert Certificate Utility for Windows' window with the 'Create CSR' tab selected. The 'Certificate Details' section on the left contains the following fields:

- Certificate Type:** ☒ SSL ☐ Code Signing
- Common Name:**
- Subject Alternative Names:**
- Organization:**
- Department:**
- City:**
- State:**
- Country:**
- Key Size:**

The 'Information' section on the right provides instructions on where the certificate will be saved based on the type chosen. At the bottom, there are 'Generate' and 'Cancel' buttons. A red box highlights the 'Key Size' field, and a red line is drawn through the '2048' value, indicating a change to '4096'.

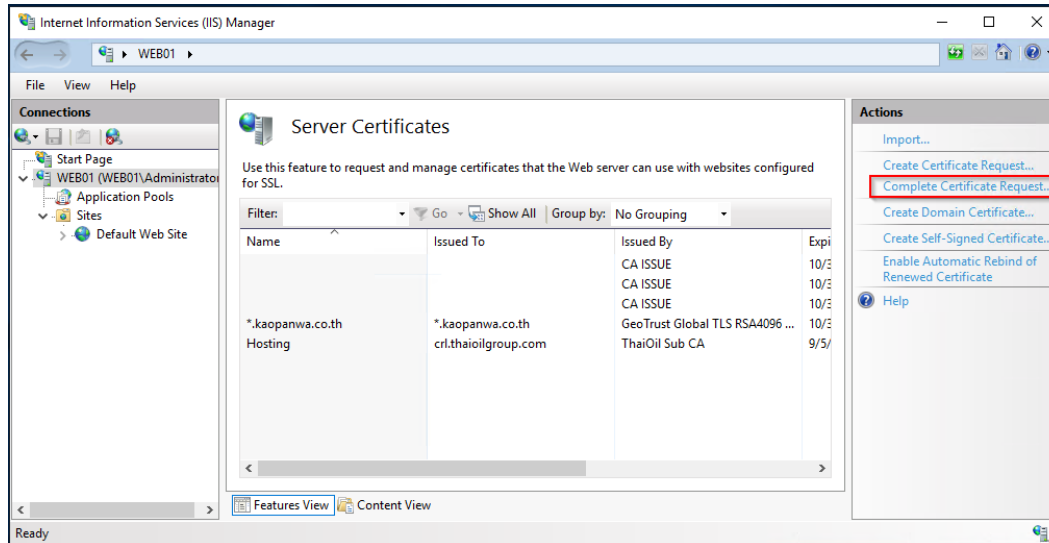
+

•

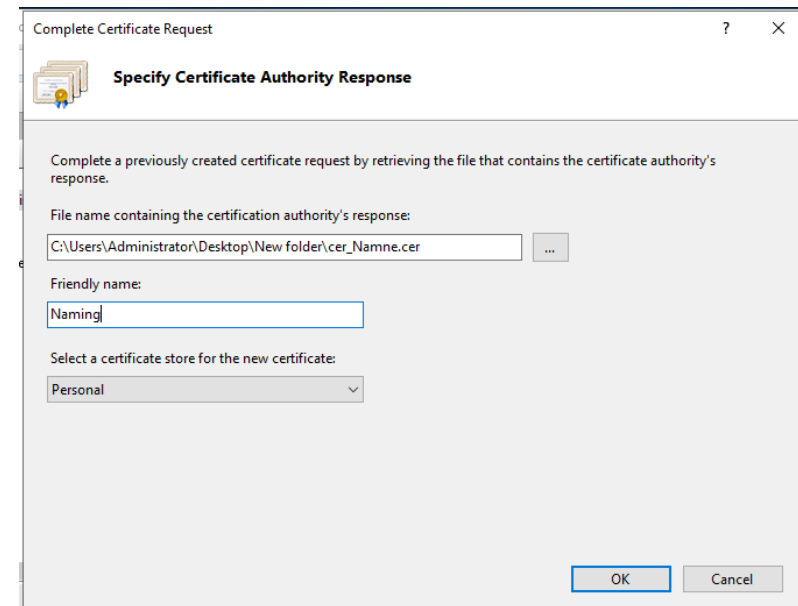
IIS: Completed Cert.

CERTIFICATE AUTHORITY (CA)

1. Click Complete Certificate Request



2. Select certificate file and fill information. Click OK



Others e.g., Linux please contact Infra team directly

Export certificate (.PFX) send to Network team

CERTIFICATE AUTHORITY (CA)

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
*.thaioilgroup.com	*.thaioilgroup.com	DigiCert TLS RSA SHA256 202...	1/15/2023 6:59:59 ...	62893A1A079C0167B7033E906...	Personal
*.thaioilgroup.com	*.thaioilgroup.com	DigiCert TLS RSA SHA256 202...	1/10/2022 6:59:59 ...	FF719711ABD602832CCE901E...	Personal
pconboardself	TSR-QDMZ-APP02.thaioil.localnet	TSR-QDMZ-APP02.thaioil.loc...	12/20/2020 7:00:00...	1C054CDC667E8E15D649E891...	Personal
QTopmarkupCert	qac-topmarkup.thaioilgroup.com	ThaiOil SubCA	10/31/2024 1:40:51...	3B8A6F8ADFC2A5FBD77A793...	Personal
star_thaioil		DigiCert SHA2 Secure Server ...	1/27/2021 7:00:00 ...	398F2385344304312F0609B169...	Personal

2. Export

3. จะได้ไฟล์ .PFX

4. ตั้งรหัสผ่าน

5. ส่งไฟล์ .PFX และรหัสให้ network team

Trust root cert.

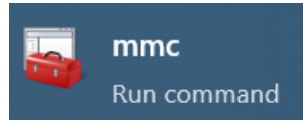
CERTIFICATE AUTHORITY (CA)

File: ThaioilRootCA.cer install @ Trusted root

File: ThaioilSubCA.cer install @ Intermediate

How to get root cert.

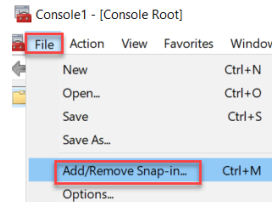
1. Open "mmc"



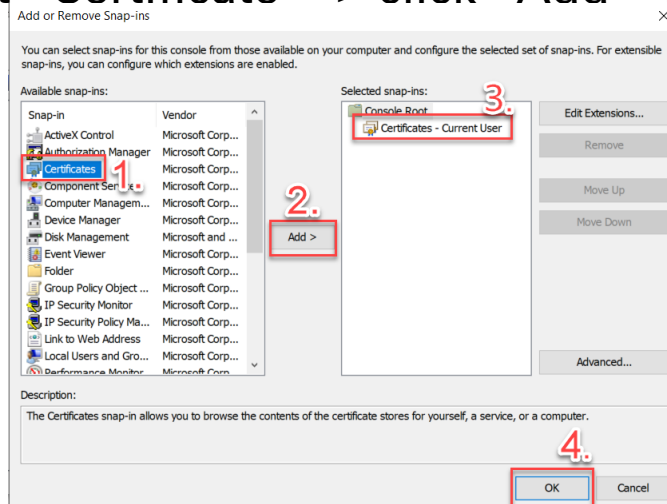
by typing "mmc" via search box



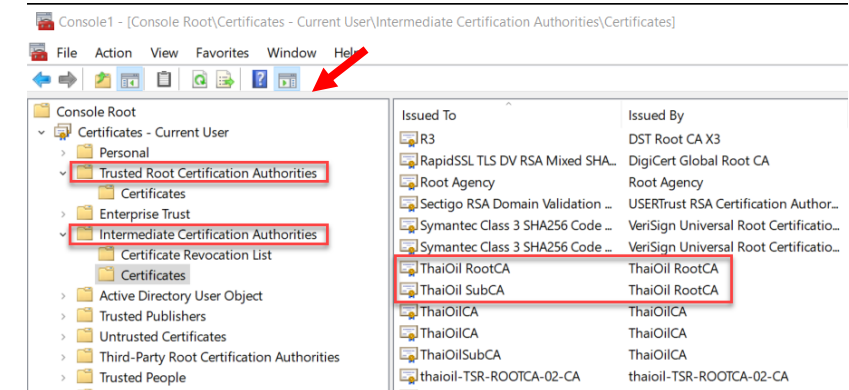
2. Menu "File->Add/Remove Snap-in.."



3. Select "Certificate" -> click "Add" -> click "OK"



4. Double click "Certificates"



Private Cert. prerequisite

CERTIFICATE AUTHORITY (CA)

1. Open connection to CRL web server, Firewall port 80 from Web server to CRL.thaioilgroup.com
2. Prepare URL (DEV, QAS, PRD)
3. Create CSR (via DigiCert) -> file.txt
4. Permission for App team
5. 1 Cert./1 App/1 Server

+



1. Public Cert purchase by Application team
2. Approve by CAB before Go-Live, first time only.
3. Public Cert budget include in project
 - Single cert. est. 13,000-25,000 Baht/year
 - SAN cert. est. 27,000 Baht/year
 - Wildcard cert. est. 32,000 Baht/year
4. Prepare OPEX budget for renew Public Cert. every year.



Certificate List

CERTIFICATE AUTHORITY (CA)

Data @17 Nov	No. FQDN
1. Private Cert. (PRD: 39, QAS/DEV: 45)	84
2. Public Cert. (Single Cert.) (for 1 FQDN)	
Internal Internet facing	22
External user: PDPA, Company and Sensitive	8
External user: Other	2
4. Public Cert. (Wildcard Cert.) (Fixed price for multi-FQDN)	2
3. Public Cert. (SAN Cert.) Telecom Cert. (Multi-domain)	5
5. Public Cert. (SAN Cert.) Cloud/External interface	4
TOTAL	127

Link to file : [Application Certificate List.xlsx](#)

The screenshot shows the Microsoft Teams interface. On the left, the 'Teams' list includes 'DGMO VA', which is highlighted with a red box. The main area shows the 'General' channel of the 'DGMO VA' team. On the right, the 'Files' tab is selected, showing a list of documents. The file 'Application Certificate List.xlsx' is highlighted with a red box. Other files visible include 'Application_DB_Servers.xlsx', 'DigiCertUtil.zip', 'Impact TS.xlsx', and 'Password Never Expired_summary_DGMO.x...'. The top navigation bar shows 'General', 'Posts', 'Files', and 'Wiki' tabs.

Timeline Replace Wildcard Cert.

CERTIFICATE AUTHORITY (CA)

Topic		Oct 22	Nov 22	Dec 22	1-15 Jan 23
1	Preparing URL				
2	Complete Private Cert. @DEV/ QAS				
3	Purchase Public cert.				
4	Complete Public and Private. @PRD				

CERTIFICATE AUTHORITY

+

o

.

THANK YOU

