

National Root Certification Authority Thailand PKI D-Day

Thailand National Root Certification Authority (NRCA)
ETDA (Thailand)

DR.CHAICHANA MITRPANT

Executive Director of the Electronic Transactions Development Agency

Thursday 22nd August 2024

09.30 – 09.50



DR. CHAICHANA MITRPANT

Founder of Thailand NRCA and CEO of ETDA

Educations:

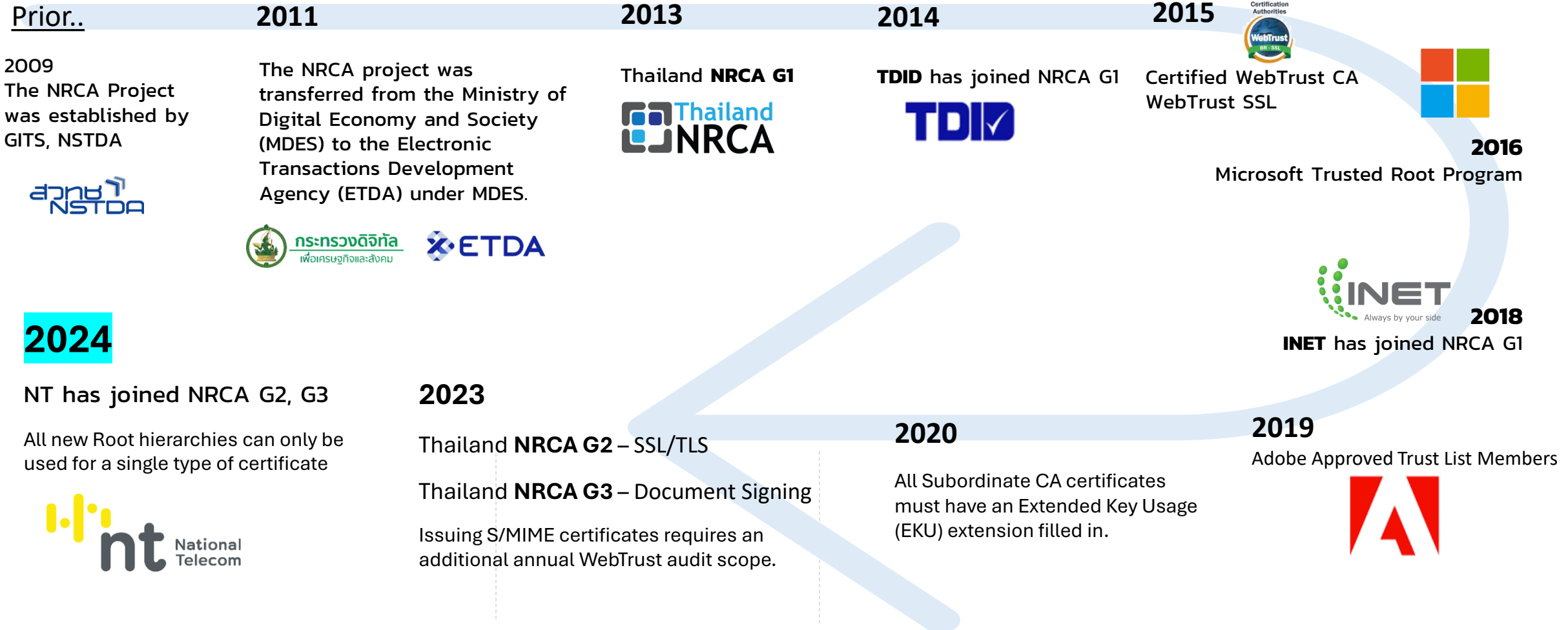
- PhD in Engineering from the Universitaet DuisburgEssen (Germany)
- MS in Electrical Engineering from the University of Michigan (US)
- BS in Electrical Engineering from Rice University (US).

Dr. Chaichana Mitrpant is currently the Executive Director of the Electronic Transactions Development Agency, Ministry of Digital Economy and Society of Thailand, a primary government agency responsible for developing, promoting, and supporting electronic transactions in Thailand.

During his tenure at ETDA, he has represented Thailand at various international fora and helped negotiate successful collaborations and bilateral meetings at ASEAN, APT, ITU, and the UN. Additionally, he has provided his expert opinions and recommendations to other organizations on numerous occasions.

15 YEARS of TRUST

Thailand National Root Certification Authority (NRCA)



Certification Authority landscape in Thailand

Domestic players Sub CA



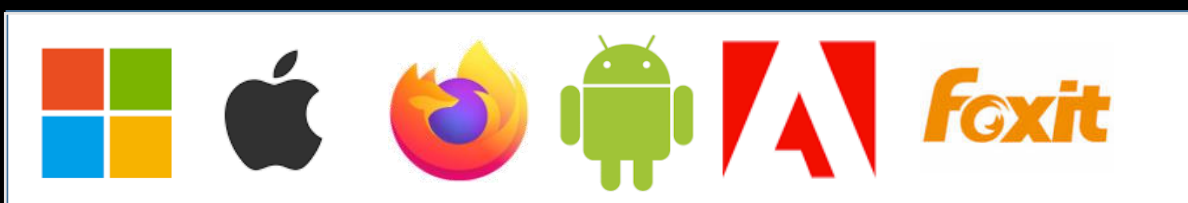
Standard organizations



International Partners



Trust stores – Global Root Certificates



Regulators



National Policy Laws & regulations Technical aspects

หมายเหตุ: BMSP อยู่ระหว่างการทำ Pre-Audit

ตัวอย่างการใช้ประโยชน์เทคโนโลยี PKI

Public Key Infrastructure (PKI)

กลุ่มธุรกิจ	รูปแบบการใช้งาน
 รัฐบาล	<ul style="list-style-type: none">การสื่อสารที่ปลอดภัยระหว่างหน่วยงานภาครัฐการยืนยันตัวของประชาชน และการเข้าถึงบริษัท E-Government อย่างปลอดภัยการปกป้องข้อมูลที่สำคัญของประเทศและโครงสร้างพื้นฐาน
 การเงิน/ธนาคาร	<ul style="list-style-type: none">การรักษาความปลอดภัยแพลตฟอร์มธนาคารบนมือถือและออนไลน์การป้องกันการฟิชชิ่งและการฉ้อโกงโดยการรับรองความถูกต้อง
 การยืนยันตัวตน/การรับรองความถูกต้อง	<ul style="list-style-type: none">ระบบการระบุตัวตนด้วยลายนิ้วมือและสมาร์ทการ์ดโดยใช้ใบรับรองอิเล็กทรอนิกส์การตรวจสอบสิทธิ์แบบสองปัจจัย เพื่อการเข้าถึงระบบและบริการอย่างปลอดภัยการเข้าสู่ระบบเพียงครั้งเดียว (SSO) สำหรับการตรวจสอบสิทธิ์ผู้ใช้แบบรวมศูนย์
 การทำธุรกรรมออนไลน์	<ul style="list-style-type: none">การทำธุรกรรมออนไลน์อย่างปลอดภัยผ่านการเข้ารหัส SSL/TLSการใช้ใบรับรองอิเล็กทรอนิกส์เพื่อรับรอง ตรวจสอบความถูกต้องของเว็บไซต์ และหลีกเลี่ยงการฟิชชิ่งการป้องกันระบบการชำระเงินโดยการเข้ารหัสและการพิสูจน์ตัวตนจริง
 บล็อกเชน	<ul style="list-style-type: none">การจัดการ และความคุ้มค่าการเข้ารหัสสำหรับการรักษาความปลอดภัยของกระเป๋าเงินบล็อกเชนและทรัพย์สินบล็อกเชนการเสริมสร้างความแข็งแกร่งระบบการจัดการข้อมูลเพื่อแสดงตัวตนแบบกระจายศูนย์
 ความปลอดภัย	<ul style="list-style-type: none">การเข้ารหัสข้อมูลระหว่างการส่งผ่านและข้อมูลที่เหลืออยู่การตรวจสอบสิทธิ์การเข้าถึงอุปกรณ์ ผู้ใช้ และระบบการบังคับใช้นโยบายการควบคุมการเข้าถึงด้วยใบรับรองอิเล็กทรอนิกส์
 เครือข่ายสังคม	<ul style="list-style-type: none">การป้องกันการแอบอ้างบุคคลอื่นและการฉ้อโกงผ่านการจัดการตัวตน
 ไอโอที	<ul style="list-style-type: none">การตรวจสอบความสมบูรณ์ของเฟิร์มแวร์ เพื่อป้องกันการอัปเดตที่ไม่ได้รับอนุญาตการเปิดใช้งานการเข้าถึงและการควบคุมจากระยะไกลอย่างปลอดภัยด้วย IoT
 การสื่อสารผ่านอินเทอร์เน็ต	<ul style="list-style-type: none">การรักษาความปลอดภัยการสื่อสารทางอีเมล โดยใช้ใบรับรองอิเล็กทรอนิกส์ S/MIMEการปกป้อง VoIP และการส่งข้อความโต้ตอบกันที่ด้วยการเข้ารหัสและการตรวจสอบตัวตนการเปิดใช้งานการเข้ารหัส SSL/STL เพื่อการท่องเว็บและถ่ายโอนข้อมูลอย่างปลอดภัยซอฟต์แวร์สำหรับการใช้ลงนามดิจิทัลเพื่อรับรองความถูกต้อง

สำรวจความต้องการการใช้งานใบรับรองอิเล็กทรอนิกส์

Digital Signature, https, s/mime, code signing - ความต้องการโต 2 digits ยอดขายโต 3 digits



หน่วยงานรัฐ/รัฐวิสาหกิจ

การเติบโตใน 3 ปีข้างหน้า

+36.6% 2027F



เอกชน/อื่นๆ

+2.5%

การเติบโตใน 5 ปีข้างหน้า

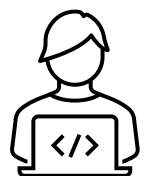
+45.1% 2029F

+5.0%

อัตราการเติบโตเฉลี่ยต่อปี

10.6% AAGR

0.9%



code signing
17%



https
29%



digital certificates
38%

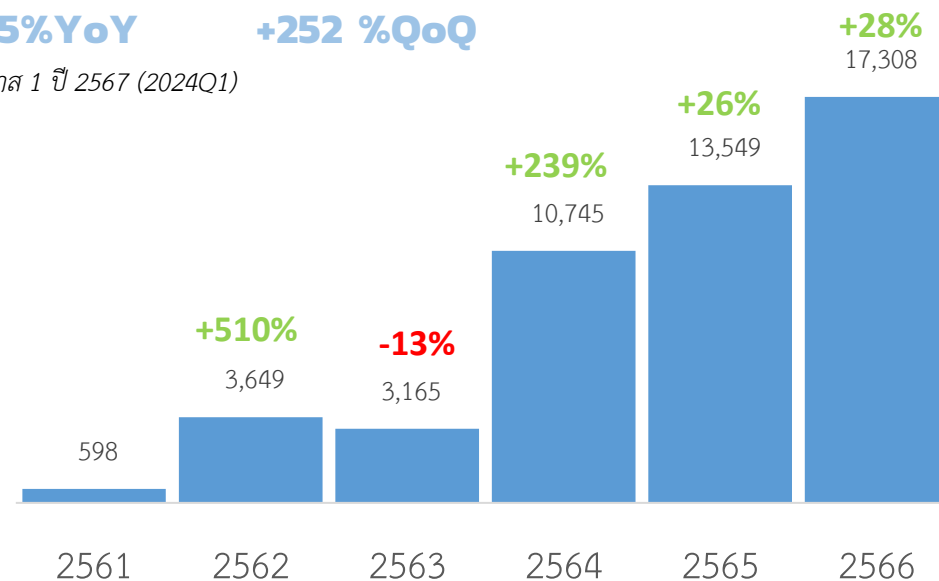


s/mime
16%

จำนวนใบรับรองภายใต้โครงการ NRCA

1,215%YoY **+252 %QoQ**

ไตรมาส 1 ปี 2567 (2024Q1)



หมายเหตุ:

[1] แบบสำรวจเข้าร่วมงาน PKI D-DAY จำนวน 151 ตัวอย่าง เมื่อวันที่ 15 ส.ค. 2567

[2] ข้อมูลจำนวนใบรับรองโครงการ NRCA รายงานช่วง 2024Q1 [3] พ.ร.บ. ปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565

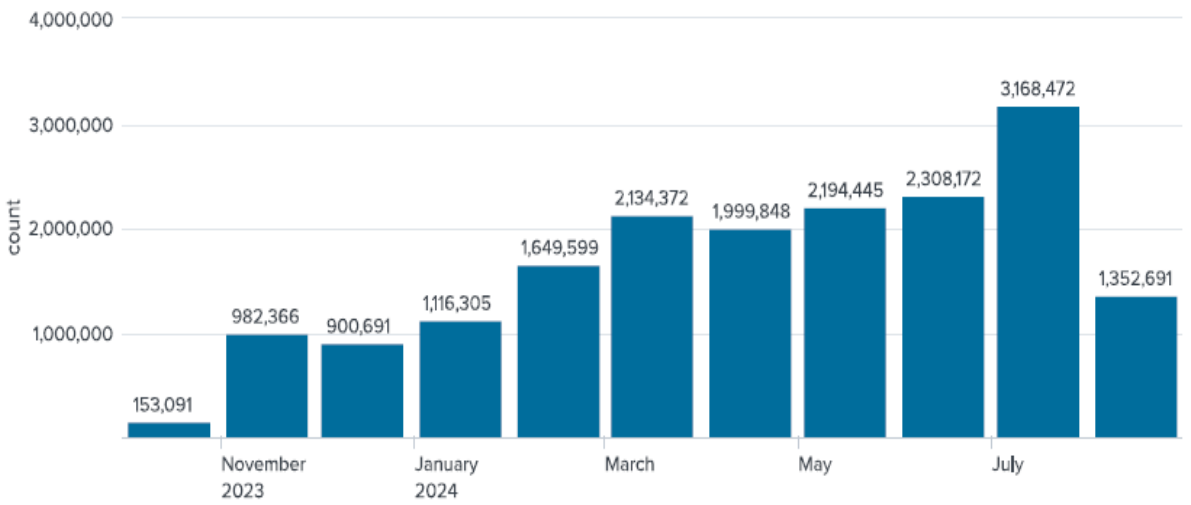
เอกสารลงนามดิจิทัลมากกว่า 25 ล้านครั้งใน 10 เดือน

การลงนามดิจิทัล (digital signing) การตรวจสอบลายเซ็นอิเล็กทรอนิกส์ (signature verification) และการตรวจสอบเว็บไซต์ (https)

✓ 17,960,052 events (10/1/23 12:00:00.000 AM to 8/14/24 12:00:00.000 AM) No Event Sampling

Visualization

AAGR +76%

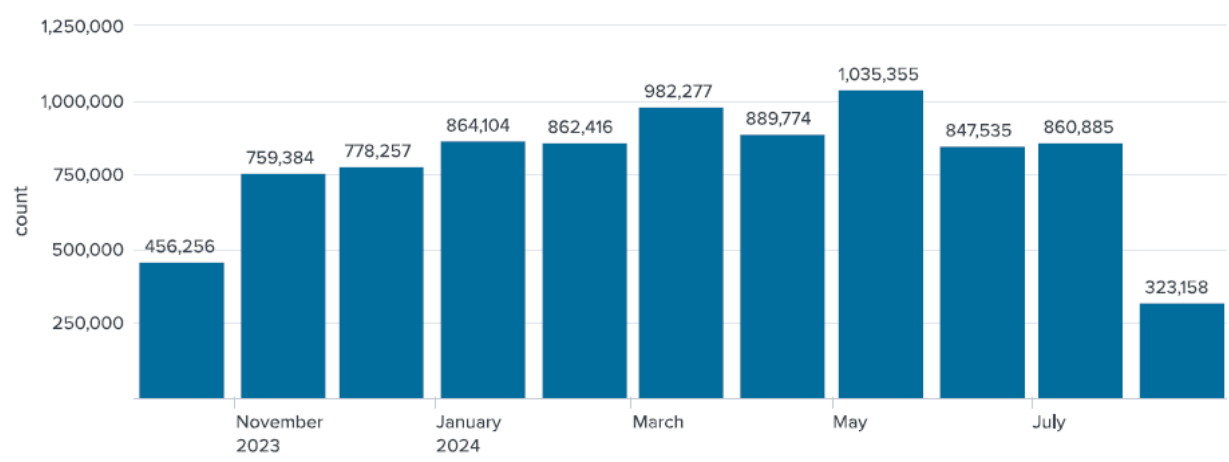


แบบออนไลน์ Online Certificate Status Protocol (OCSP) กว่า 17 ล้านครั้ง

✓ 8,659,401 events (10/1/23 12:00:00.000 AM to 8/14/24 12:00:00.000 AM) No Event Sampling

Visualization

AAGR +9%



แบบดาวน์โหลด Certificate Revocation List (CRL) กว่า 8 ล้าน

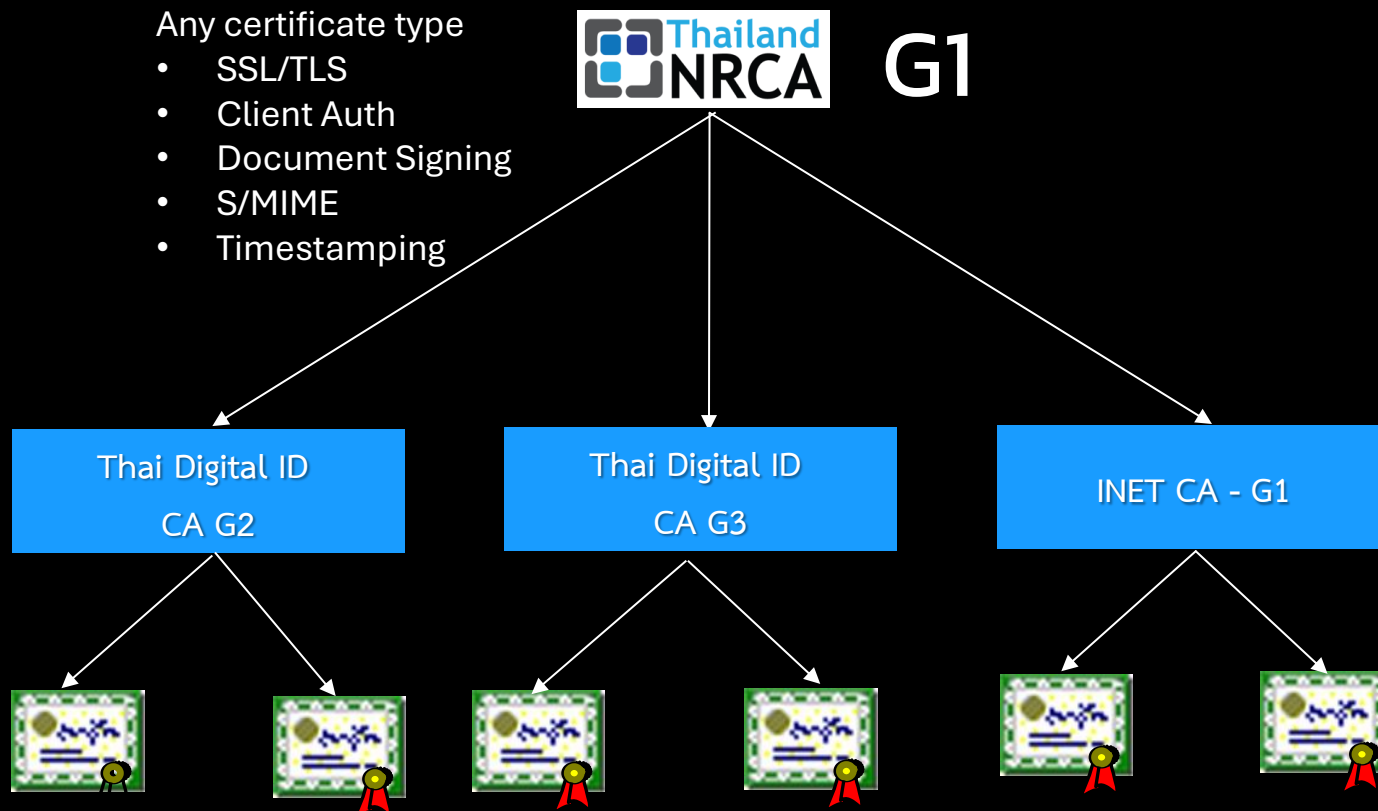
หมายเหตุ: ข้อมูล transactional ณ ช่วง 1 ต.ค.2566 – 14 ส.ค.2567

ม.28 พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562

ข้อมูลอาจมีการนับซ้ำได้ ขึ้นอยู่กับ Software ใช้งาน

NRCA Root architecture must evolve from G1 to G2, G3, G...

Currently issuing NRCA Root hierarchy



Replacing NRCA Root hierarchies under development



Thailand NRCA - Trust Store inclusions status

SubCA Application plays a major role in successful trust store inclusions.

Root	Purpose	Year	Trust Store						Market coverage	
			Microsoft	Adobe	Foxit	Chrome	Mozilla	Apple	AS IS	TO BE
G1	[Legacy]	2013 - 2036	Yes	Yes	3	No	No	No	13.13% (Web)	13.13%
									99.58% (PDF)	99.75%
									5.01% (email)	5.01%
G2	SSL/TLS	2023 - 2043	1, 4	n/a	n/a	2, 4	2, 4	2, 4	0%	96.68%
G3	Document Signing	2023 - 2043	1, 4	1, 4	3	n/a	n/a	n/a	0%	99.75%
G4	S/MIME	NEW (2025)	5	n/a	n/a	n/a	5	5	0%	89.05%
G5	Timestamping	TBC	4	n/a	n/a	n/a	n/a	4	n/a	n/a

Trust store 's status Number

1.Amendment of existing contract, **initiated** 2.CCADB Inclusion request, **initiated** 3.Need to contact for more information, GlobalSign agreed to help us
 4.Need to wait for Sub CA application (set up SSL/TLS test websites, create test certificate) 5.Secure Email EKU trust requires S/MIME certification
Yes = inclusion request completed **No** = Not complied to trust store policies

Market Coverage

0% – 30% | 30%-70% | 70%-100%

ETDA joins hands with partner agencies to enhance digital certificate issuance services with the Thailand NRCA (Thailand National Root Certification Authority) project.



On 9 November 2022, Thailand NRCA's work goes one step further. By moving towards cooperation to promote greater use between ETDA and 4 electronic certificate issuing agencies (Subordinate Certification Authority), namely Internet Thailand Public Company Limited, National Telecommunications Public Company Limited, Navani Company Limited, and Thai Digital ID Company Limited through the signing of an MOU to jointly drive operations in both improving and developing service operations regarding digital certificates to comply with laws and international standards as well as to follow the action plans of all parties and raise the level of digital certificate issuance services in Thailand.

NRCA conducts first cyber-threat response practice for electronic certificate operators in Asia-Pacific countries



ETDA with the Thailand NRCA organized a cyber-threat response exercise for digital certification operators (Sub CAs) under the topic CYBER EXERCISE FOR CERTIFICATION AUTHORITY (CA) 2023: PREPARE YOUR TRUST SERVICE for the first time in Thailand for Sub CAs and observers on 2-3 November 2023, to strengthen Response and Recovery and to prepare to deal with potential cyber threat situations.

THANK YOU

Electronic Transactions Development Agency

The Government Complex Commemorating His Majesty the King's 80th Birthday Anniversary,
5th December, B.E.2550 (2007), Building B, 6th Floor

CALL CENTER : 02 123 1234

email : info@etda.or.th

Web : www.etda.or.th



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

