CA Knowledge Sharing Series #4 in 2024

Thailand Public Key Infrastructure (PKI) D-Day

Session

Certification Authority & Business Opportunities

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

Digital Trends

ปัจจุบัน การทำธุรกรรมต่าง ๆ จะเป็นรูปแบบอิเล็กทรอนิกส์เป็นหลัก ดังนั้น การยืนยันตัวตนบนโลกออนไลน์ เพื่อทำธุรกรรมทางอิเล็กทรอนิกส์ จึงเป็นสิ่งสำคัญอย่างยิ่ง

Certificate Authority (CA) จึงเข้ามามีบทบาทสำคัญในการเสริมสร้างความมั่นคง และความน่าเชื่อถือในโลกดิจิทัล เพื่อช่วยให้สามารถใช้ประโยชน์จากเทคโนโลยีได้อย่างมั่นใจ และปลอดภัย ยิ่งขึ้น

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

ประโยชน์ของ Certificate Authority (CA) ในยุคดิจิทัล

การยืนยันตัวตน (Authentication)

CA ช่วยในการยืนยันตัวตนของผู้ใช้งานหรือองค์กรในโลกออนไลน์ ซึ่งทำให้เราสามารถมั่นใจได้ว่าการติดต่อสื่อสารหรือธุรกรรมที่เราทำมีความถูกต้องและปลอดภัย

การเข้ารหัสข้อมูล (Data Encryption)

CA ช่วยในการออกใบรับรองที่สามารถนำไปใช้ในการเข้ารหัสข้อมูล ทำให้ข้อมูลที่ส่งผ่านเครือข่ายอินเทอร์เน็ต ซึ่งเป็นช่องทางหลักในการสื่อสาร และทำธุรกรรมออนไลน์ในปัจจุบัน มีความปลอดภัยจากการถูกดักข้อมูล

การลงลายเซ็นดิจิทัล (Digital Signatures)

CA ช่วยให้สามารถใช้ลายเซ็นดิจิทัลในการรับรองความถูกต้องและความเป็นเจ้าของเอกสาร หรือข้อมูล ทำให้มั่นใจได้ว่าข้อมูลที่ได้รับมานั้นไม่ถูกปลอมแปลง

การสร้างความเชื่อมั่นในธุรกรรมออนไลน์ (Trust Establishment)

ด้วยการใช้ใบรับรองดิจิทัลจาก CA การทำธุรกรรมออนไลน์ต่างๆ จะมีความน่าเชื่อถือ และปลอดภัยมากขึ้น ซึ่งช่วยให้ผู้ใช้สามารถทำธุรกรรมและสื่อสารได้อย่างมั่นใจ

การปกป้องข้อมูลส่วนบุคคล (Protecting Personal Data)

CA มีบทบาทในการปกป้องข้อมูลส่วนบุคคล และความเป็นส่วนตัวของผู้ใช้งาน ซึ่งเป็นสิ่งสำคัญในยุคที่ข้อมูลส่วนบุคคลมีการแชร์และใช้งานอย่างแพร่หลาย

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

กระบวนการทำงานของ Certification Authority (CA)

การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance)

การขอใช้ใบรับรองฯ การตรวจสอบ การออกใบรับรองฯ

การตรวจสอบสถานะ และ การเพิกถอนใบรับรอง (Certificate Revocation)

การตรวจสอบสถานะใบรับรอง การเพิกถอน

การบริหารจัดการใบรับรอง (Certificate Management)

การต่ออายุใบรับรองฯ (Renewal) การเปลี่ยนแปลงข้อมูลใบรับรองฯ (Certificate Modification) การเก็บรักษากุญแจส่วนตัว (Private Key)

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

กระบวนการให้บริการ Certificate Authority (CA)

การออกใบรับรองอิเล็กทรอนิกส์ (Certificate Issuance)

การขอใช้ใบรับรองฯ

สามารถสมัครในนามบุคคล หรือนิติบุคคล โดยบุคคลที่ได้รับมอบหมาย ผู้ใช้บริการส่งคำขอใช้ใบรับรองไปยัง CA จะต้องระบุข้อมูลที่ต้องการให้ปรากฏในใบรับรอง เช่น ชื่อ สกุล ผู้ขอใช้ ชื่อหน่วยงาน/องค์กร

การตรวจสอบ

CA จะตรวจสอบข้อมูลที่ได้รับเพื่อยืนยันความถูกต้องและความสมบูรณ์ของคำขอ เช่น การตรวจสอบตัวตนของผู้ขอใบรับรอง หรือ การยืนยันสิทธิ์การเป็นเจ้าของโดเมน และ หลักฐานการสมัครก่อนออกใบรับรองให้

การออกใบรับรองฯ

CA จะออกใบรับรองดิจิทัล ซึ่งประกอบด้วยข้อมูลที่เกี่ยวข้องของผู้ขอใบรับรอง โดย CA จะลงลายมือชื่อดิจิทัลเพื่อรับรองความถูกต้องไว้ในใบรับรองของผู้ขอใช้ฯ และใบรับรองที่ผ่านการรับรองแล้ว จะถูกเผยแพร่ผ่านทาง X.500 Directory ของ CA

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

กระบวนการให้บริการ

Certificate Authority (CA)

การตรวจสอบสถานะ และ การเพิกถอน
ใบรับรอง (Certificate Revocation)

การตรวจสอบสถานะใบรับรอง

หากมีการร้องขอเพื่อตรวจสอบสถานะของใบรับรองว่า เป็นใบรับรองฯ ที่ถูกเพิกถอน ระบบ CA จะให้ข้อมูลเกี่ยวกับสถานะของใบรับรองนั้นผ่านทาง CRL (Certificate Revocation List) หรือ OCSP (Online Certificate Status Protocol)

การเพิกถอน (Revocation)

หากพบว่าใบรับรองถูกทำลายหรือไม่ปลอดภัย เช่น กุญแจส่วนตัว/Private Key สูญหาย ผู้ใช้บริการสามารถแจ้ง CA เพื่อให้เพิกถอนใบรับรองนั้นได้ ใบรับรองที่ถูกเพิกถอนจะถูกบันทึกใน CRL หรือ OCSP เพื่อให้ทราบว่าใบรับรองนั้นไม่สามารถใช้ได้อีกต่อไป

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

กระบวนการให้บริการ Certificate Authority (CA)

การบริหารจัดการใบรับรอง (Certificate Management)

การต่ออายุการใช้งานใบรับรองฯ (Renewal)

ใบรับรองมีระยะเวลาการใช้งานตามที่กำหนด เช่น 1 ปี 2 ปี หรือ 3 ปี เมื่อล่วงเลยช่วงเวลาดังกล่าว ผู้ถือใบรับรองสามารถขอต่ออายุการใช้ใบรับรองฯ จาก CA เพื่อให้สามารถใช้งานได้อย่างต่อเนื่อง

การเปลี่ยนแปลงข้อมูลใบรับรองฯ (Certificate Modification)

หากมีการเปลี่ยนแปลงแก้ไข เช่น เปลี่ยนชื่อ สกุล ผู้ใช้ใบรับรองฯ เปลี่ยนชื่อหน่วยงาน เปลี่ยนเลขประจำตัวนิติบุคคล ผู้ใช้หรือเจ้าของใบรับรองจะต้องเป็นผู้แจ้ง CA เพื่อขอยกเลิกใบรับรองฯ เดิม และ ขอให้ออกใบรับรองฯ ใหม่

การเก็บรักษากุญแจส่วนตัว (Private Key)

ผู้ใช้บริการมีหน้าที่ในการจัดเก็บรักษากุญแจส่วนตัว (Private Key) ให้มีความปลอดภัย และ นำไปใช้งานให้เหมาะสมกับประเภทของใบรับรองที่ CA ออกให้

Next, through Technology

NTCA

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) หรือ National Telecom Public Company Limited (NT) เป็นองค์กรรัฐวิสาหกิจสังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) ที่ให้บริการโทรคมนาคม และบริการดิจิทัล เล็งเห็นถึงความสำคัญในด้านความปลอดภัยของข้อมูล และการทำธุรกรรมทางอิเล็กทรอนิกส์ จึงมี “บริการออกใบรับรองอิเล็กทรอนิกส์หรือ CA” ตั้งแต่ปี พ.ศ. 2548 ในนาม บมจ. กสท โทรคมนาคม หรือ CAT Telecom และ บมจ. ทีโอที

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

ปัจจุบัน NT มีการออกใบรับรองอิเล็กทรอนิกส์ 2 Packages

Package : CAT CA

ยุติการให้บริการ Package CAT CA
ตั้งแต่ วันที่ 1 กันยายน 2567 เป็นต้นไป

Package : TOT CA

สำหรับ Package TOT CA สามารถติดต่อสอบถามการขอใช้บริการ ได้จากเจ้าหน้าที่ฝ่ายขายของ NT ทั่วประเทศ หรือ ติดต่อ Call Center 02-575-8912

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

กลุ่มลูกค้าที่ใช้บริการใบรับรองอิเล็กทรอนิกส์ (CA) ของ NT

01

กลุ่มผู้ประกอบการนำเข้า/ส่งออก

- ผู้ประกอบการ Shipping
- ผู้ประกอบการ นำเข้า ส่งออก Importer/Exporter
- ผู้ประกอบการ Freight Forward
- ผู้ประกอบการ Customer Broker

02

กลุ่มหน่วยงานภาครัฐและเอกชนที่นำไปใช้ในระบบ National Single Window (NSW)

- กรมการขนส่งทางบก
- การยางแห่งประเทศไทย
- กรมโรงงานอุตสาหกรรม
- สำนักงานพาณิชย์จังหวัด
- บริษัท การบินไทย จำกัด (มหาชน)
- บริษัท ไปรษณีย์ไทย จำกัด เป็นต้น

03

หน่วยงานที่นำไปใช้เป็นการเฉพาะภายในกลุ่มสมาคมธนาคารไทย

- ธนาคารพาณิชย์ต่างๆ
- กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
- สำนักคณะกรรมการตุลาการศาลยุติธรรม
- สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด
- สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

04

หน่วยงานที่ต้องรายงานการทำธุรกรรมฯ ไปยัง ปปง.

- ผู้ประกอบการร้านทองต่างๆ
- บริษัท หลักทรัพย์จัดการกองทุนต่างๆ เป็นต้น

บทบาทของ NT ในฐานะ NSW Operator และ NT e-Tax Service Provider

ให้บริการด้านดิจิทัล เพื่อลดการใช้กระดาษ (Paperless)

National Single Window (NSW)

e-Tax (ใบกำกับภาษีอิเล็กทรอนิกส์)

CA (ใบรับรองอิเล็กทรอนิกส์)

ภาพรวมระบบ NSW ที่ให้บริการโดย NT

NSW User

- Shipping Line
- Air Line
- Importer
- Exporter
- Freight Forward
- Customs Broker

NSW Service Provider (NSP) : 8 NSPs

TIFFA
EGS
THAI TRADE NET
A Member Of SMART TELECOMS
EDI SIAM
Web Application for Logistics
Trade Siam International Co.,Ltd.

B2G

B2B

NSW Operator

NSW Thailand National Single Window

nt NSW Operator

bsi ISO/IEC 27001 Information Security Management CERTIFIED

bsi ISO/IEC 27701 Privacy Information Management CERTIFIED

bsi ISO 22301 Business Continuity Management CERTIFIED

Cross Border Trade Exchange

B2G e-Form

B2G / B2B Exchange

B2B e-Form

- NSW Website
- ระบบลงทะเบียน
- ระบบ SSO
- ระบบ e-Tracking
- Help Desk & Call Center

G2G Exchange

G2G

Government Agency

Customs Department	Board of Investment
Department of Foreign Trade	Defense industrial Department
Department of Industrial Works	Industrial Estate Authority of Thailand
Excise Department	Department of Mineral Fuels
Department of Livestock Development	Department of Fisheries
Food and Drug Administration	Office of the Cane and Sugar Board
National Bureau of Agricultural Commodity and Food Standards	Department of Land Transport
Department of Agriculture	Department of National Parks Wildlife and Plant Conservation
Department of Energy Business	Department of Medical Sciences
Department of	Department of ...
Department of	Department of ...
Department of	Department of ....

CA Provider
NT, INET, TDID

Global Trade
ASW
ePhyto
IPPC Hub

P2P

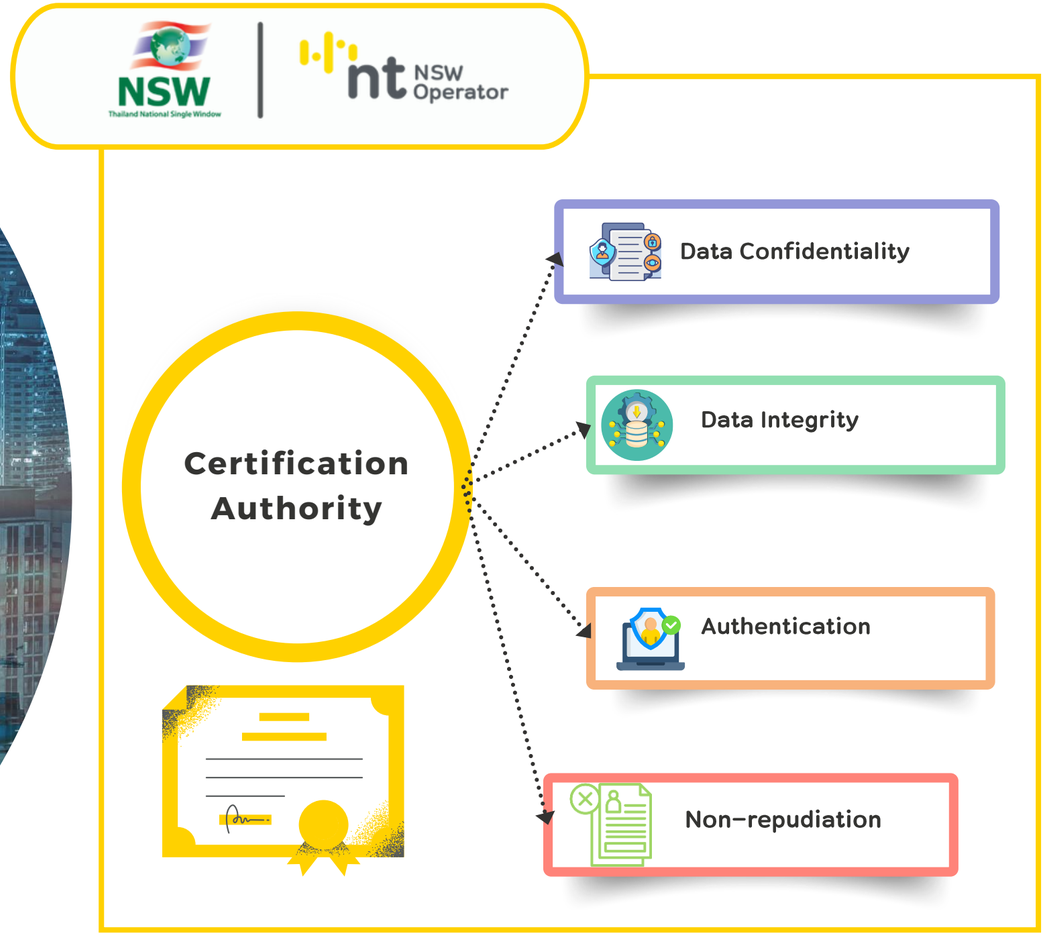
ASW
ebXML
AEC Community

Bank & Insurance
ITMX
ebXML

National Telecom

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

nt NSW Operator



- การเชื่อมโยงแลกเปลี่ยนข้อมูลผ่านระบบ National Single Windows ในรูปแบบข้อมูลอิเล็กทรอนิกส์ หรือ Paperless จำเป็นจะต้องใช้ใบรับรองอิเล็กทรอนิกส์ (CA) เพื่อเป็นการยืนยันตัวบุคคล/นิติบุคคล เจ้าของลายมือชื่อที่ยื่นเอกสารทางอิเล็กทรอนิกส์ผ่านระบบ NSW ตรวจสอบได้ว่าข้อมูลที่รับ-ส่ง นั้นถูกต้องครบถ้วนหรือไม่ และจะต้องไม่ถูกแก้ไขเปลี่ยน
- การนำ CA มาใช้ในระบบ NSW จะช่วยให้ข้อมูลมีความปลอดภัยมั่นคงครอบคลุม คุณสมบัติ 4 ด้าน ได้แก่ Data Confidentiality, Data Integrity, Authentication และ Non-repudiation

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

การนำ Digital Certificate ช่วยเพิ่มโอกาสทางธุรกิจได้อย่างไร

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

โอกาสทางธุรกิจ

ในการเป็น Certification Authority

1. บทบาทการเป็น NSW Operator ของประเทศ
2. บทบาทการเป็น e-Tax Service Provider
3. พ.ร.บ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565
4. การเป็น Subordinate Certificate Authority (SubCA) ของ National Root Certification Authority (NRCA)

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

NRCA Thailand

- เพื่อยกระดับความปลอดภัยให้เป็นไปตามมาตรฐานสากลยิ่งขึ้น NT เตรียมเข้าเป็น Subordinate Certificate Authority (SubCA) ของ National Root Certification Authority (NRCA) ซึ่งได้ดำเนินการทำ Key Ceremony ไปแล้ว เมื่อวันที่ 31 กรกฎาคม และ วันที่ 1 สิงหาคม 2567 โดยได้รับเกียรติจาก NRCA เข้าร่วมเป็นสักขีพยานในการทำ Key Ceremony

- คาดว่าจะสามารถเข้าร่วมเป็น SubCA กับ NRCA ได้ภายในปี 2567

Thanks

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

NRCA Thailand