

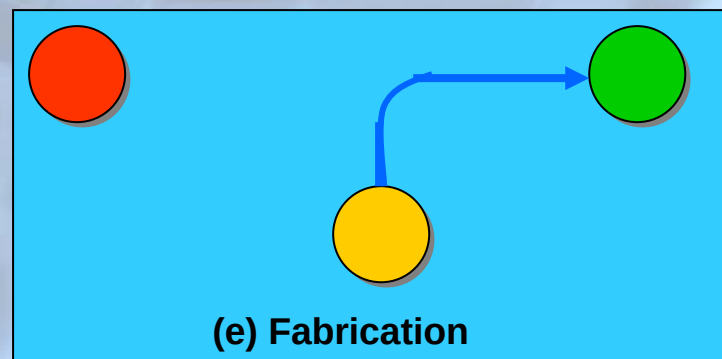
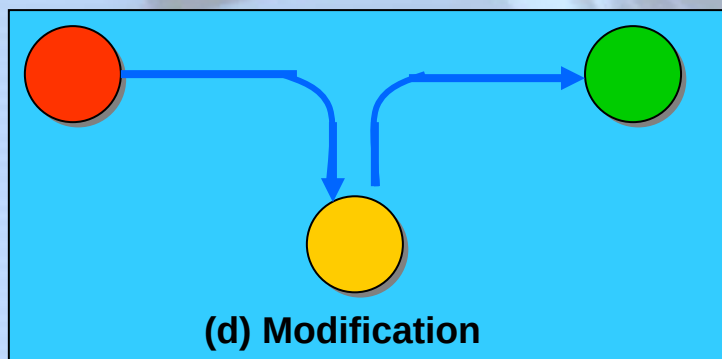
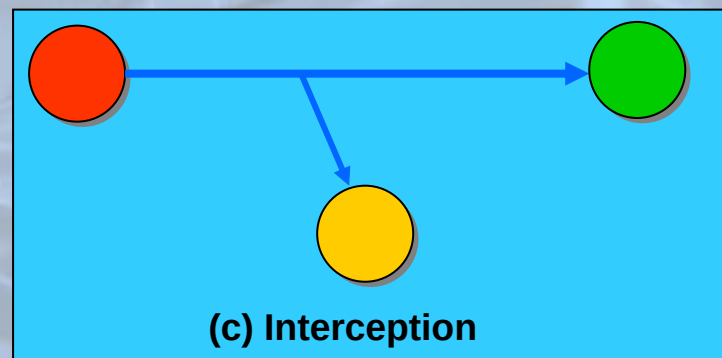
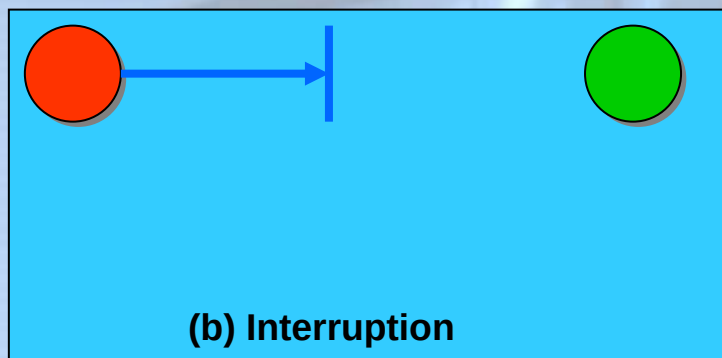
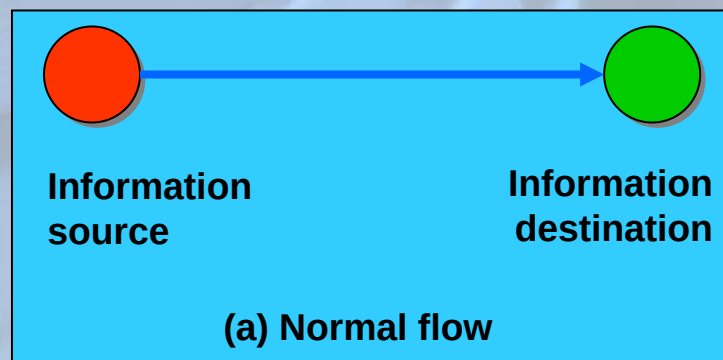


TOT Certificate Authority

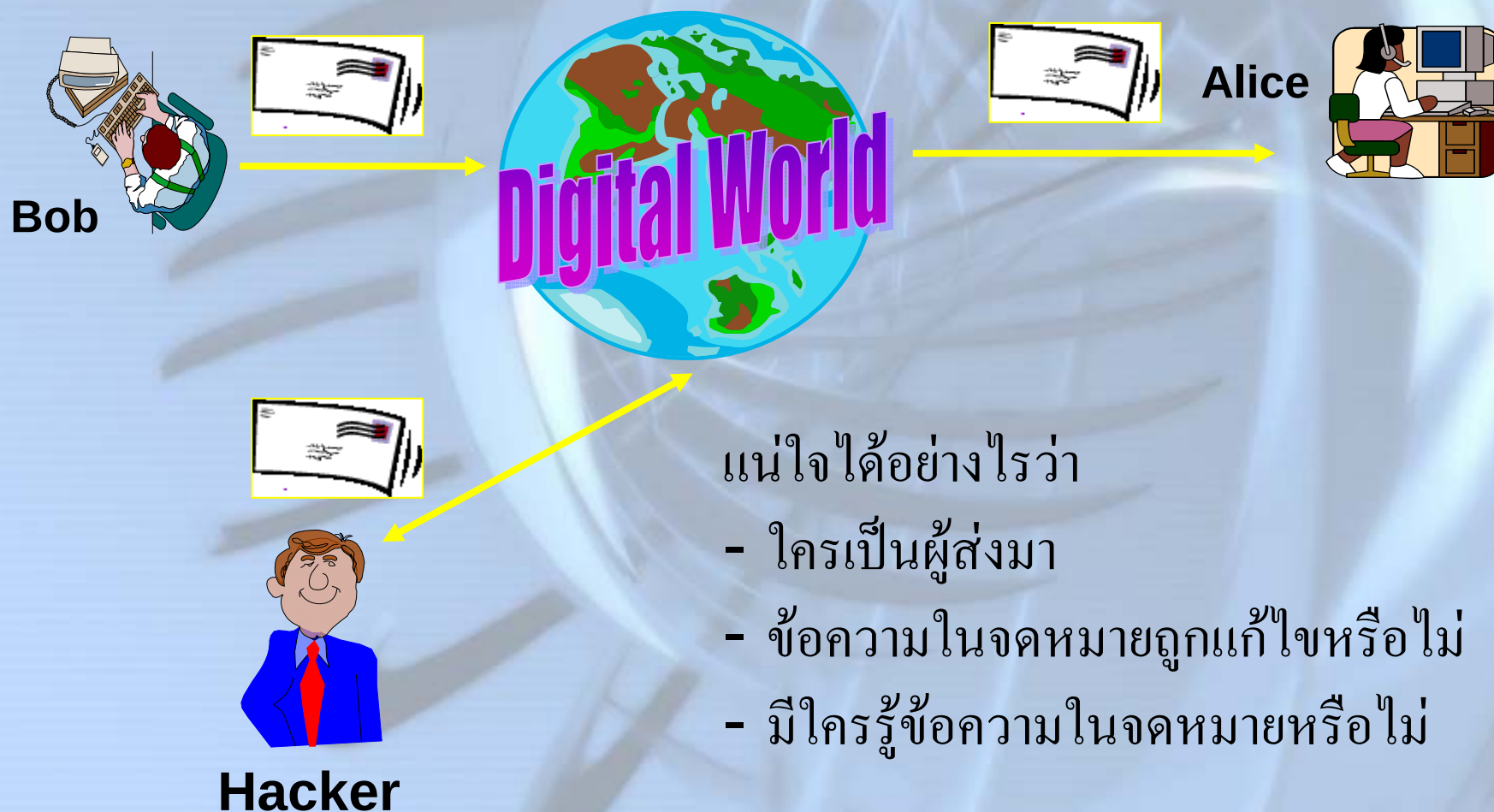
TOT CA

ส่วนพัฒนาธุรกิจอิเล็กทรอนิกส์ (ชมพ.)

Security Threats



ตัวอย่างการส่งข้อมูลโดยไม่ใช้ใบรับรองอิเล็กทรอนิกส์



ตัวอย่างการส่งข้อมูลโดยใช้ใบรับรองอิเล็กทรอนิกส์



ปัญหาของการทำธุรกรรมอิเล็กทรอนิกส์

- ไม่สามารถระบุตัวตนที่แท้จริงได้
- ไม่สามารถรับรองได้ว่าเป็นข้อมูลจริง
- ไม่สามารถรักษาความลับของข้อมูลได้
- สามารถปฏิเสธความรับผิดชอบในการทำธุรกรรมได้

Digital Certificate

- ใบรับรองอิเล็กทรอนิกส์

ด้วยการเข้ารหัส และ ลายมือชื่อดิจิตอล ในการทำธุรกรรม เราสามารถรักษาความลับของข้อมูล สามารถรักษาความถูกต้องของข้อมูล และ สามารถระบุตัวบุคคลได้ระดับหนึ่ง เพื่อเพิ่มระดับความปลอดภัยในการระบุตัวบุคคลโดยสร้างความเชื่อถือมากขึ้นด้วยใบรับรองดิจิตอล (Digital Certificate) ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า องค์กรรับรองความถูกต้อง (Certification Authority - CA) จะถูกนำมาใช้สำหรับ ยืนยันในตอนทำธุรกรรมว่าเป็นบุคคลนั้นๆ จริงตามที่ได้อ้างไว้

เทคโนโลยีที่ใช้ในใบรับรองอิเล็กทรอนิกส์

- เทคโนโลยีในการเข้า-ถอดรหัสข้อมูล

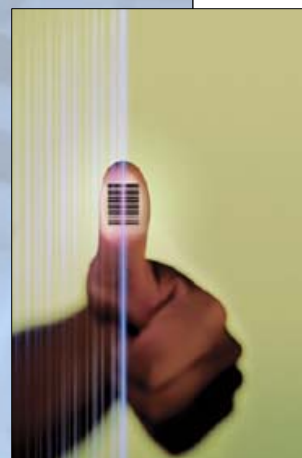
(Cryptography Technology)



Encrypt Decrypt

- เทคโนโลยีลายมือชื่อดิจิตอล

(Digital Signature)



Cryptography Technology

การเข้ารหัส

(Encryption)



หมายถึง การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปหนึ่งที่สามารถอ่านได้ (plaintext) ให้อยู่ในรูปแบบหนึ่งที่เปลี่ยนแปลงไปจากเดิมและอ่านไม่ได้ (cipher text)

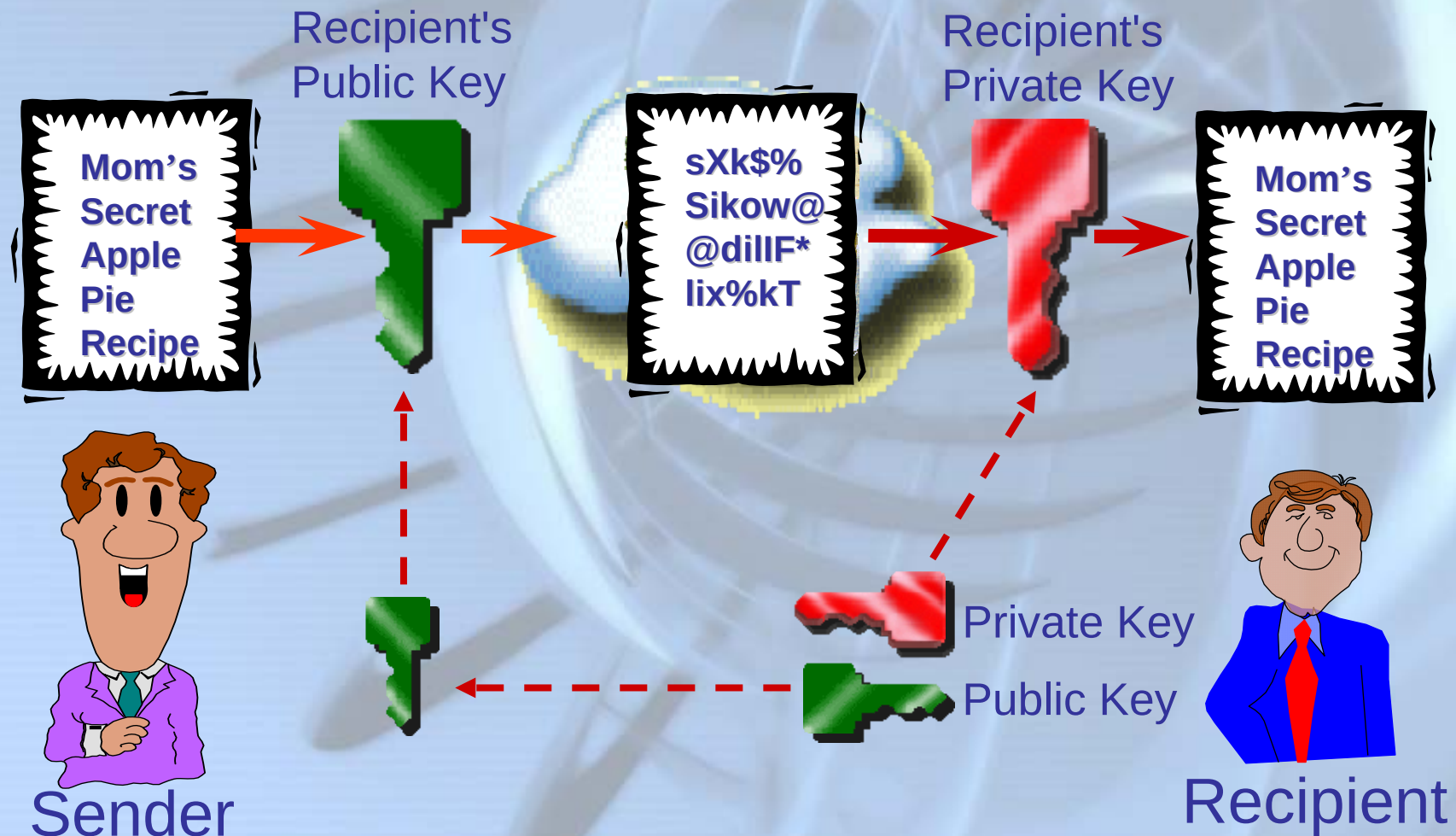
การถอดรหัส

(Decryption)



การแปลงข้อความหรือข้อมูลอิเล็กทรอนิกส์จากรูปแบบที่ถูกเปลี่ยนแปลงไปจากเดิม (cipher text) ให้กลับไปอยู่ในรูปของข้อความหรือข้อมูลอิเล็กทรอนิกส์รูปแบบเดิมก่อนการเปลี่ยนแปลง (plaintext)

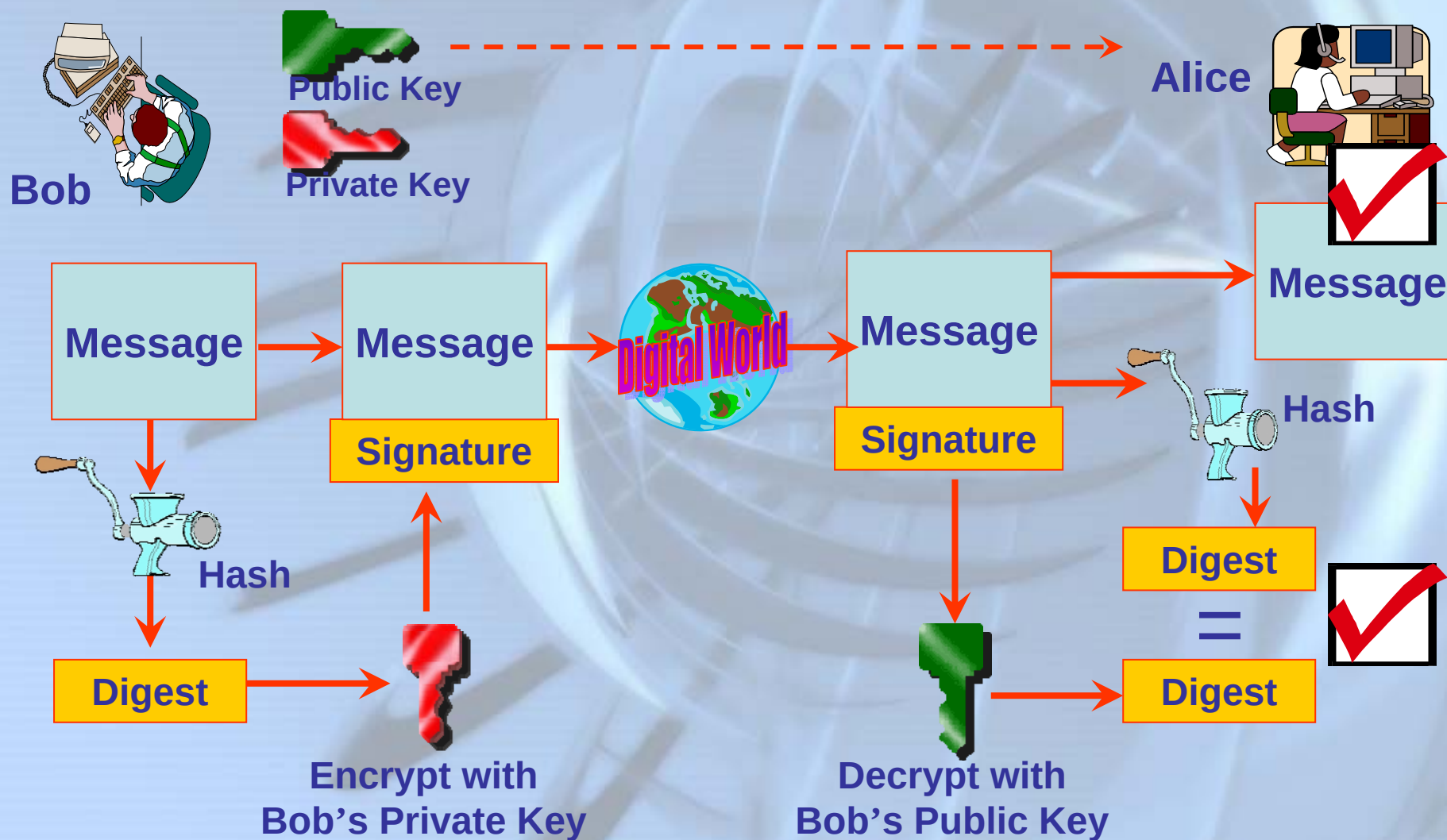
Asymmetric Key / Public Key



Digital Signature

- Digital Signature เป็นลายมือชื่ออิเล็กทรอนิกส์ ที่สร้างจากเทคโนโลยีเข้ารหัสด้วยกุญแจสาธารณะ ในการลงลายมือชื่อดิจิทัลกำกับข้อความที่ต้องการส่งผ่านเครือข่าย ผู้ส่งข้อความจะใช้กุญแจส่วนตัวของตนในการลงลายมือชื่อโดยอ่านกระบวนการทางคณิตศาสตร์ ผู้รับจะสามารถตรวจสอบความถูกต้องของลายมือชื่อดังกล่าวโดยใช้กุญแจสาธารณะของผู้ส่ง ซึ่งลายมือชื่อของผู้ส่งจะถูกรับรองด้วยองค์การออกใบรับรอง (Certification Authority) โดย

Digital Signature

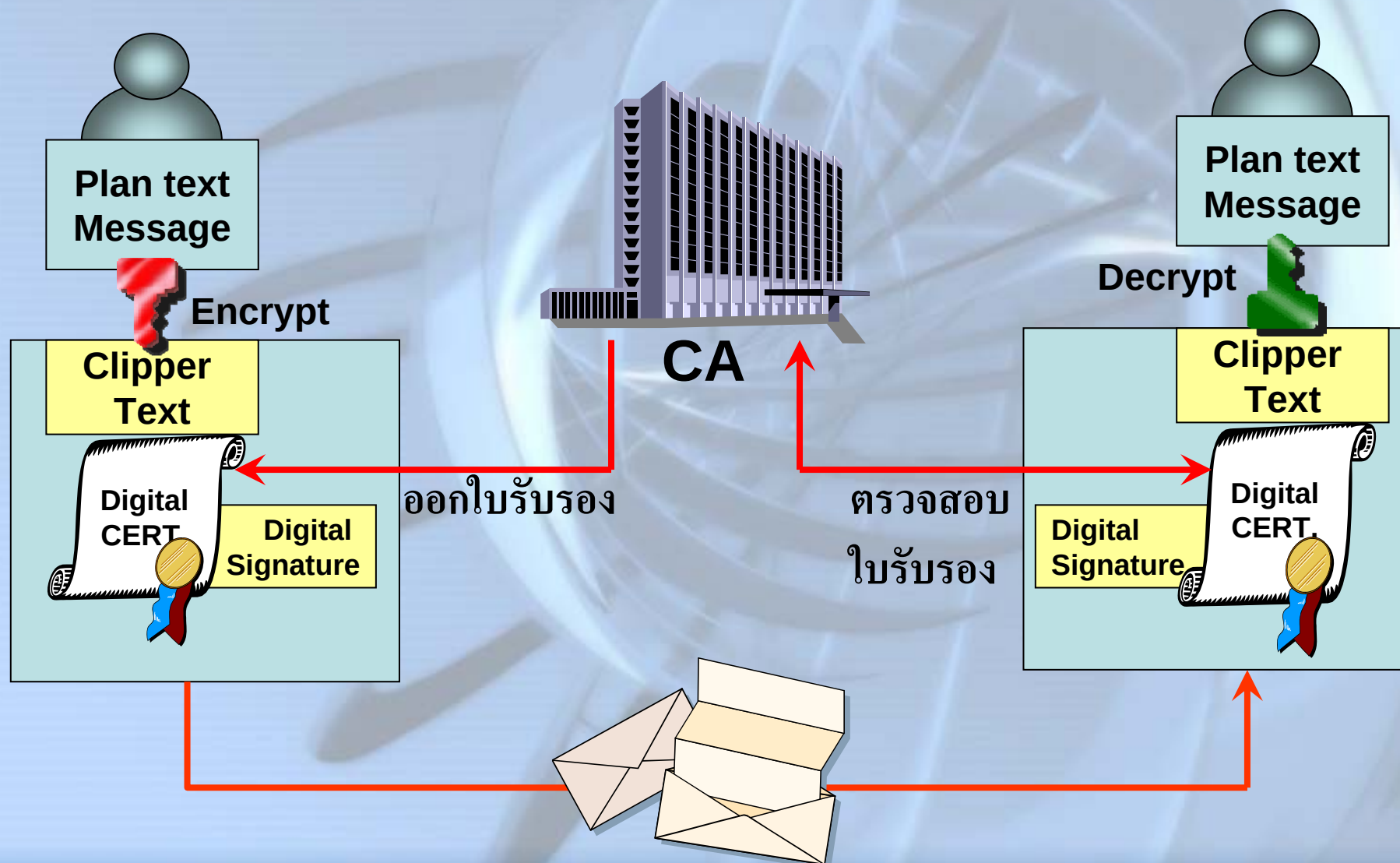


Certificate Authority (CA)

Certificate Authority เป็นองค์กรที่เป็นที่เชื่อถือ ที่ทำหน้าที่เป็นบุคคลที่สามดำเนินการออกใบรับรองดิจิทัล ให้กับผู้ทำธุรกรรมอิเล็กทรอนิกส์ ที่ขอใช้บริการ โดยบริการต่างๆขององค์กรออกใบรับรอง ได้แก่

1. การให้บริการเทคโนโลยีการรหัส ได้แก่ การสร้างกุญแจสาธารณะ และกุญแจลับ การส่งมอบกุญแจลับ การสร้าง และการรับรองลายมือชื่อดิจิตอล
2. การให้บริการเกี่ยวกับการออกใบรับรอง ได้แก่ การออก การเก็บรักษา การยกเลิก การตีพิมพ์เผยแพร่ ใบรับรองดิจิทัล รวมทั้งการกำหนดนโยบายการออกและอนุมัติใบรับรอง
3. บริการเสริมอื่นๆ ได้แก่ การตรวจสอบสัญญาต่างๆ การทำทะเบียน การกู้กุญแจ

ภาพรวมของระบบใบรับรองอิเล็กทรอนิกส์



TOT CA

➤ ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certificate Authority : CA) แก่บุคคลทั่วไป นิติบุคคล และองค์กรต่างๆ โดยใช้เทคโนโลยี PKI (Public Key Infrastructure) เพื่อความมั่นใจในการรักษาความปลอดภัยของการทำธุรกรรม ผ่านทางอินเทอร์เน็ตโดยการใช้การเข้ารหัสข้อมูลด้วยกุญแจคู่ที่เรียกว่า กุญแจสาธารณะ (Public Key) และกุญแจส่วนตัวบุคคล (Private Key)

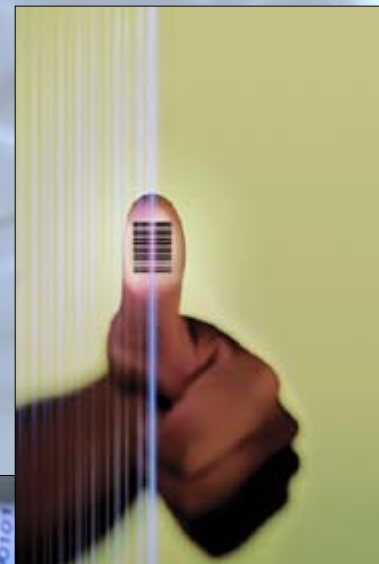
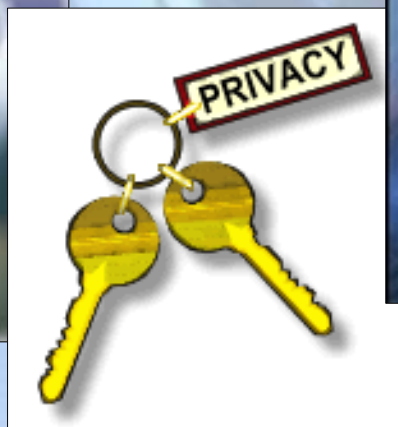


หน้าที่การให้บริการของ TOT CA

- เป็นผู้ให้บริการออกใบรับรองดิจิทัล (Digital Certificate)
- เป็นบุคคลที่สามทำหน้าที่สร้างกุญแจคู่ (Key Pair) ตามคำขอของผู้ขอใช้บริการใบรับรองเพื่อยืนยันตัวตนบุคคล
- จัดเก็บกุญแจสาธารณะในฐานข้อมูล (Directory Service)
- เปิดเผยกุญแจสาธารณะต่อบุคคลทั่วไปที่ติดต่อทางเครือข่าย
- ยืนยันตัวตนบุคคลที่เป็นเจ้าของกุญแจสาธารณะตามคำขอของบุคคล
ต่างๆ ไป
- ให้บริการอื่นๆ ที่เกี่ยวข้อง โดยใช้เทคโนโลยี PKI

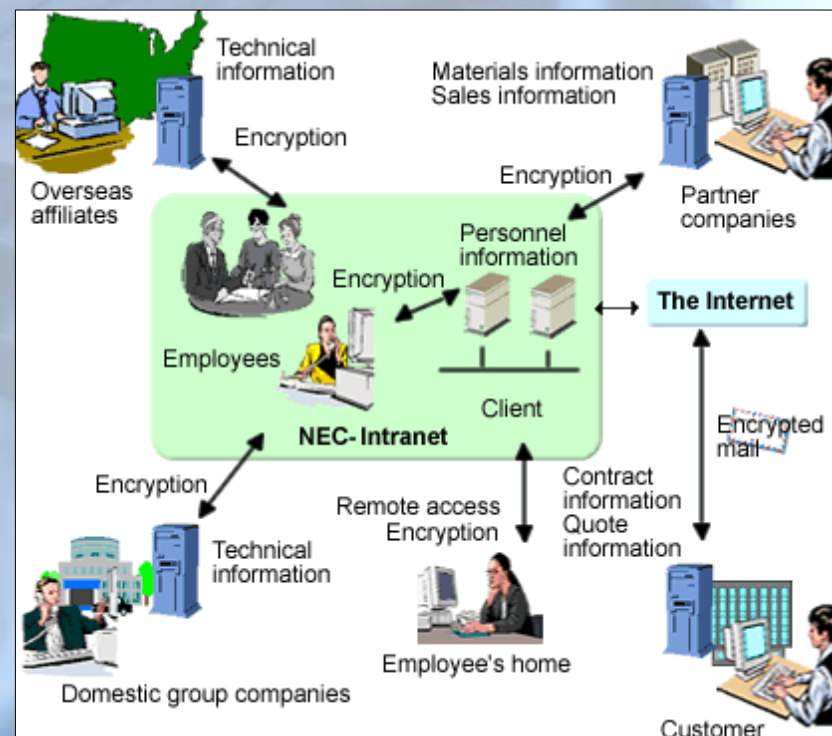
ประโยชน์ของการใช้ใบรับรองอิเล็กทรอนิกส์

- Authentication
- Data Integrity
- Data Confidentiality
- Non-Repudiation

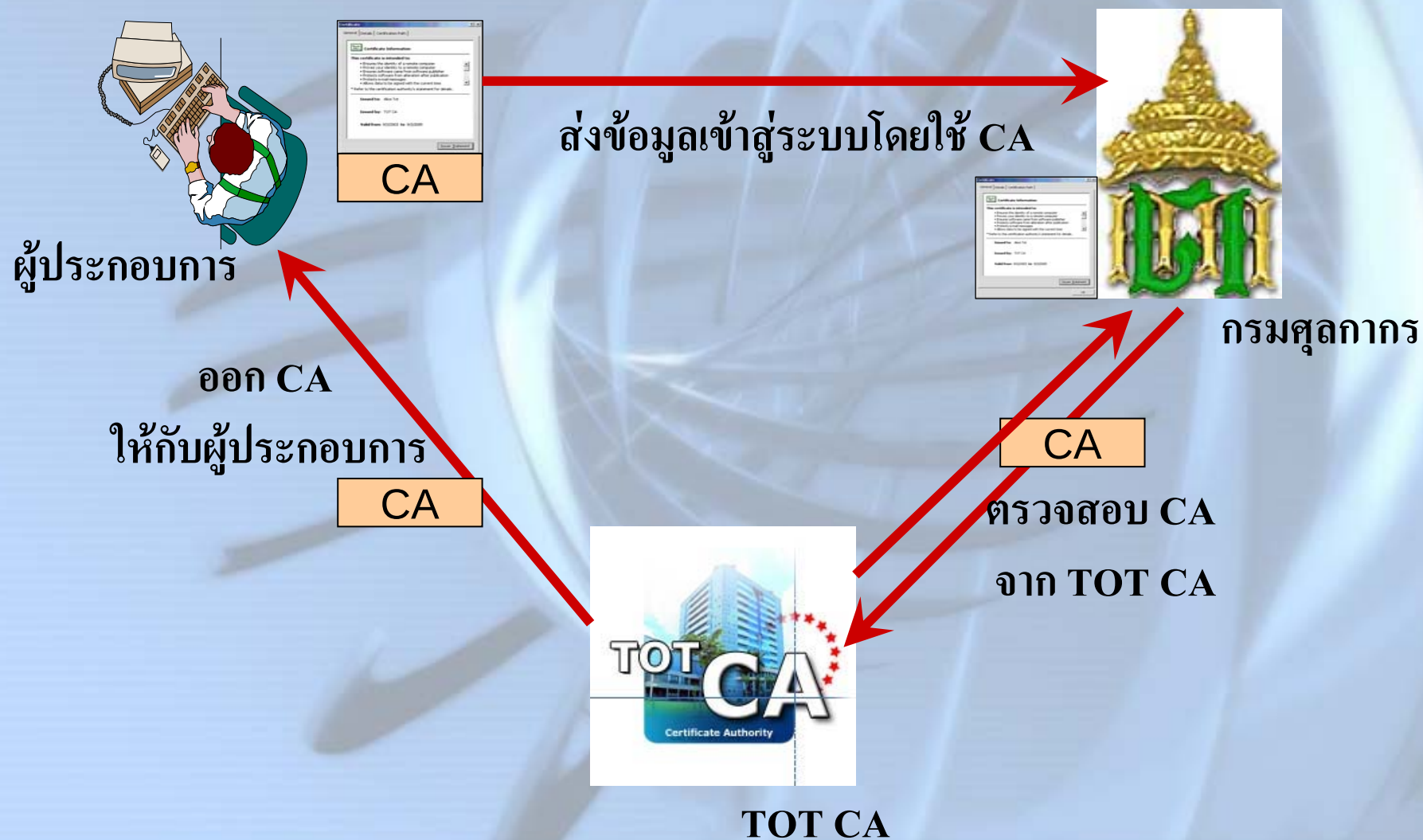


Using and Apply

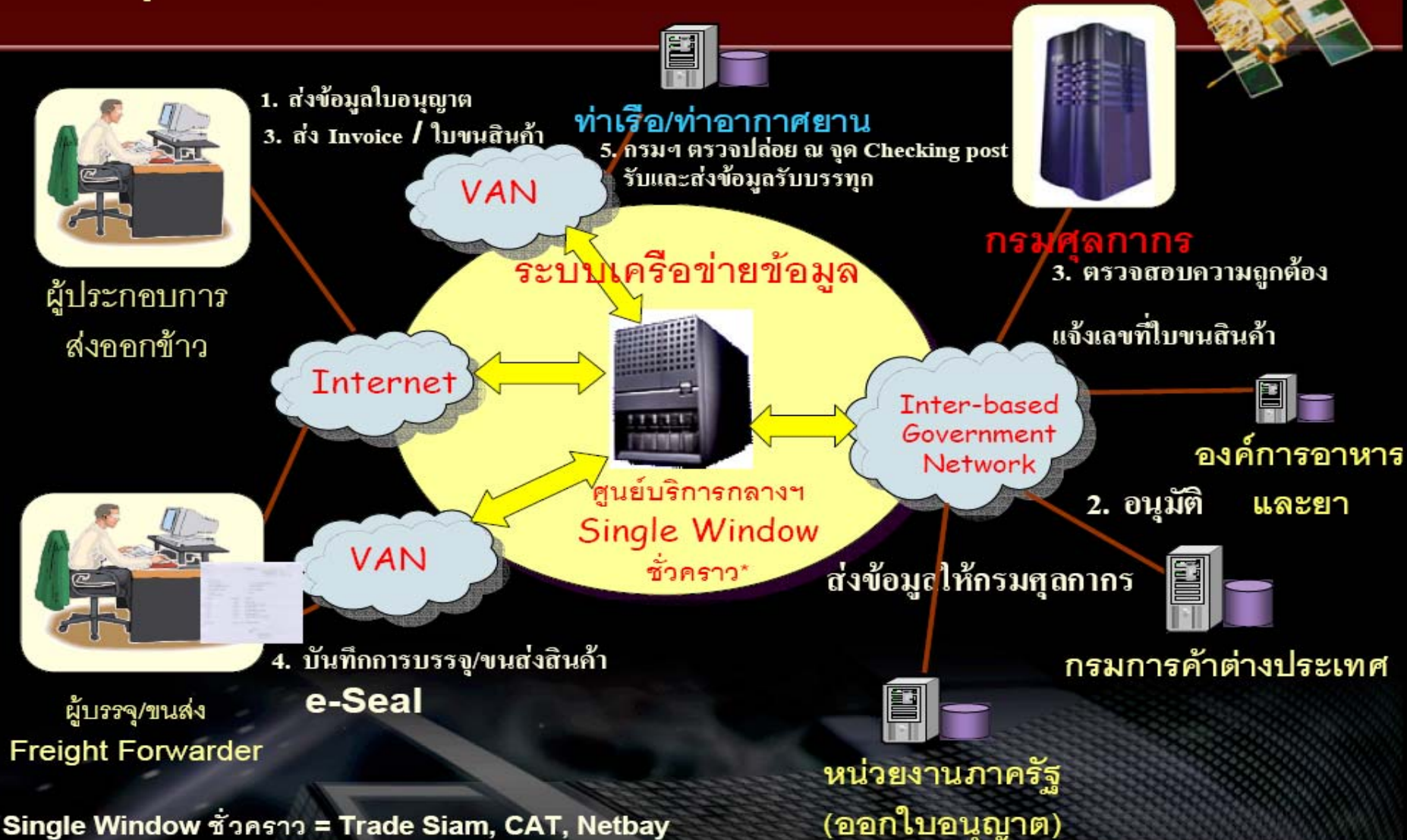
- Secure Electronic Mail System
- User or Client Authentication
- e-Document (Paperless)
- e-Commerce (Purchasing)
- e-Payment
- e-Auction
- e-Logistics
- Other Application



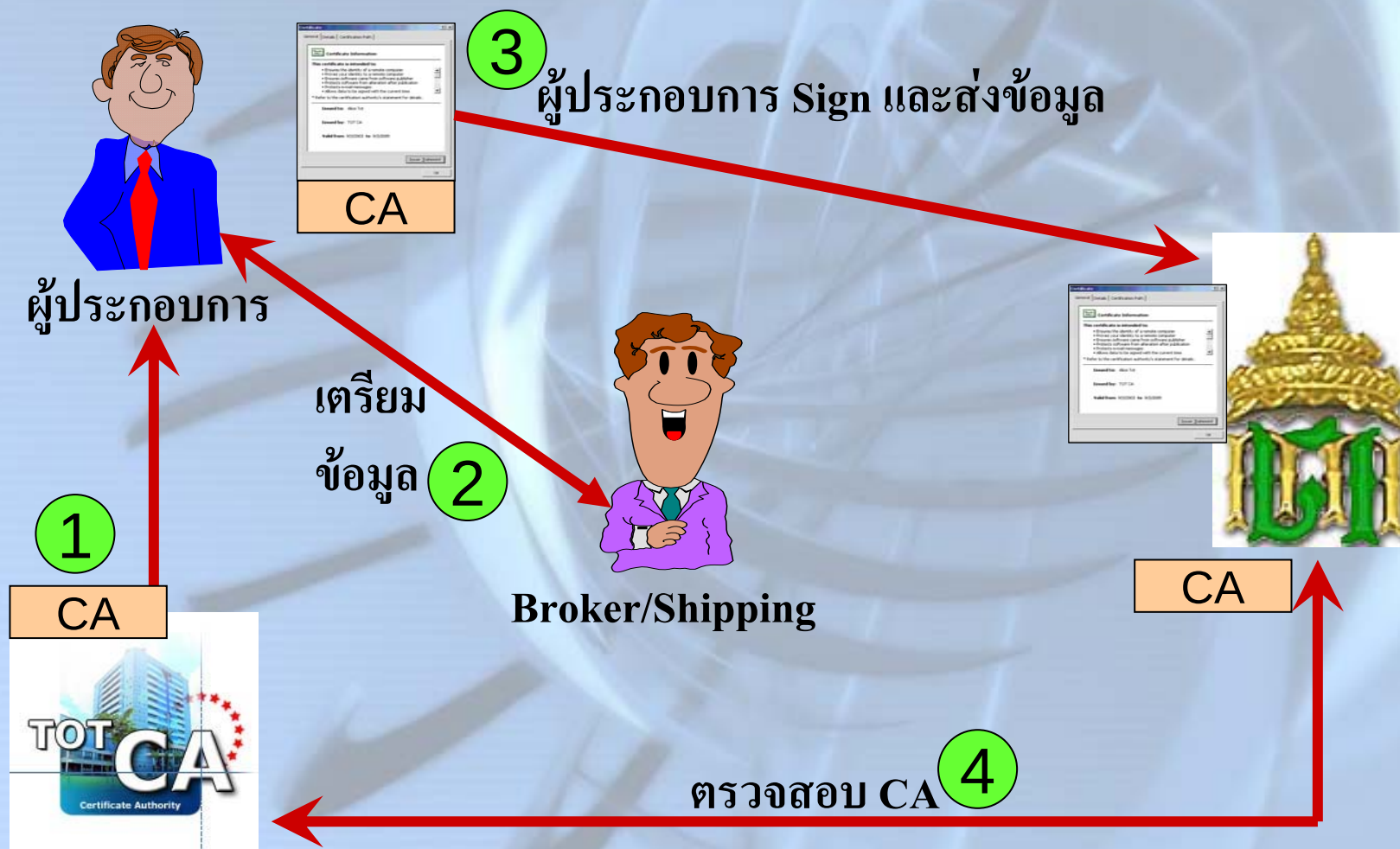
CA & Paperless



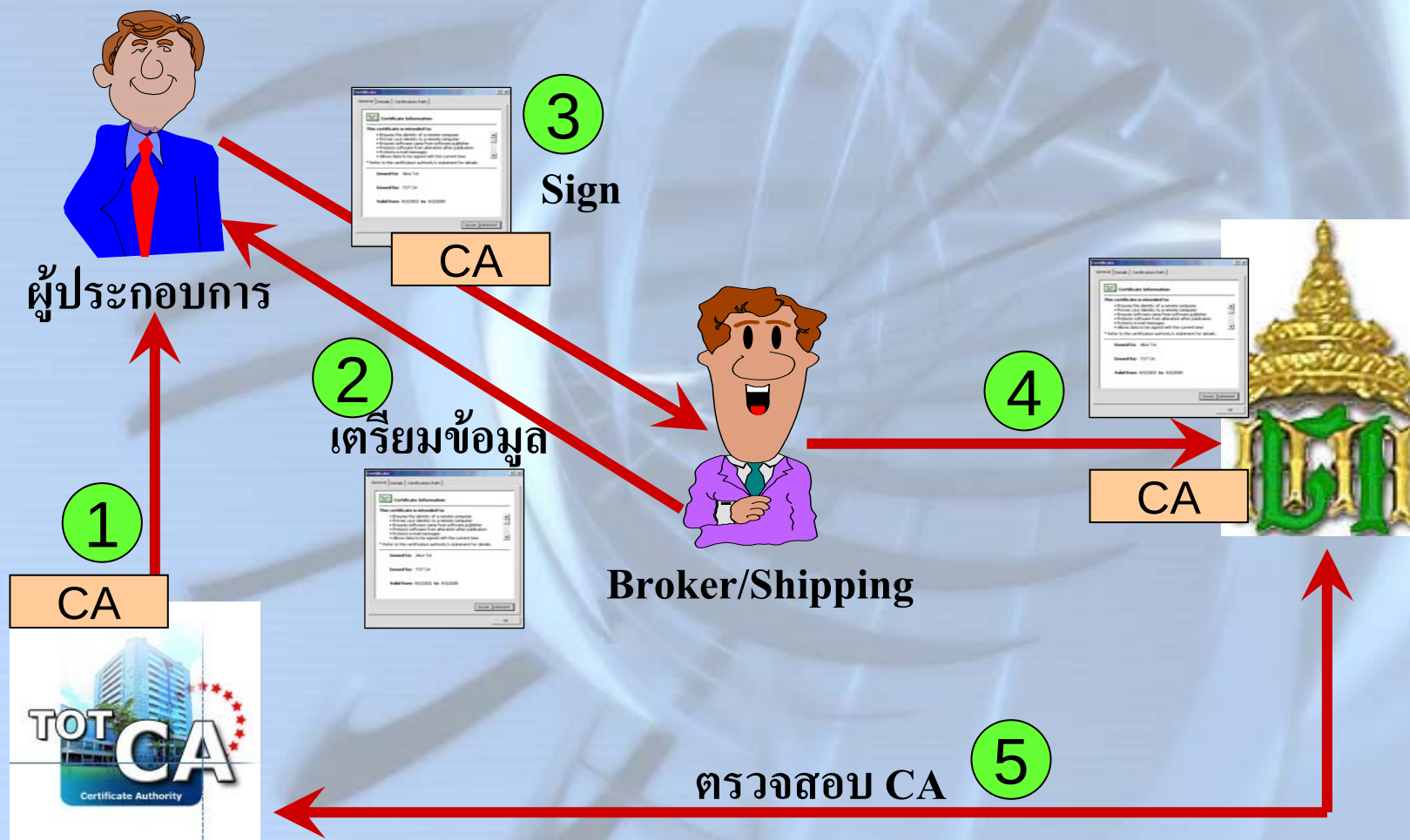
e-Export via e-Dtransit



ใครที่ต้องใช้ CA



ใครที่ต้องใช้ CA



TOT CA – Digital Certificate Properties

TOT CA (X.509 v.3)

Serial Number : ef96cd0b6379afg

Validity : 17 Feb 06 13.31.40 - 17 Feb 07 13.31.40

Signature Algorithms : sha1RSA-1024 bits
Issued Subject : Name /Organization / email

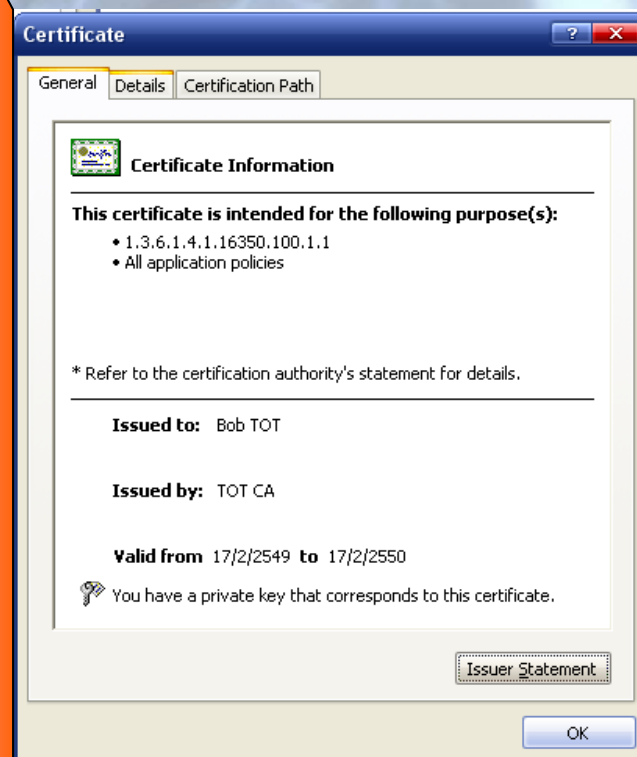
Holder's Public Key : RSA

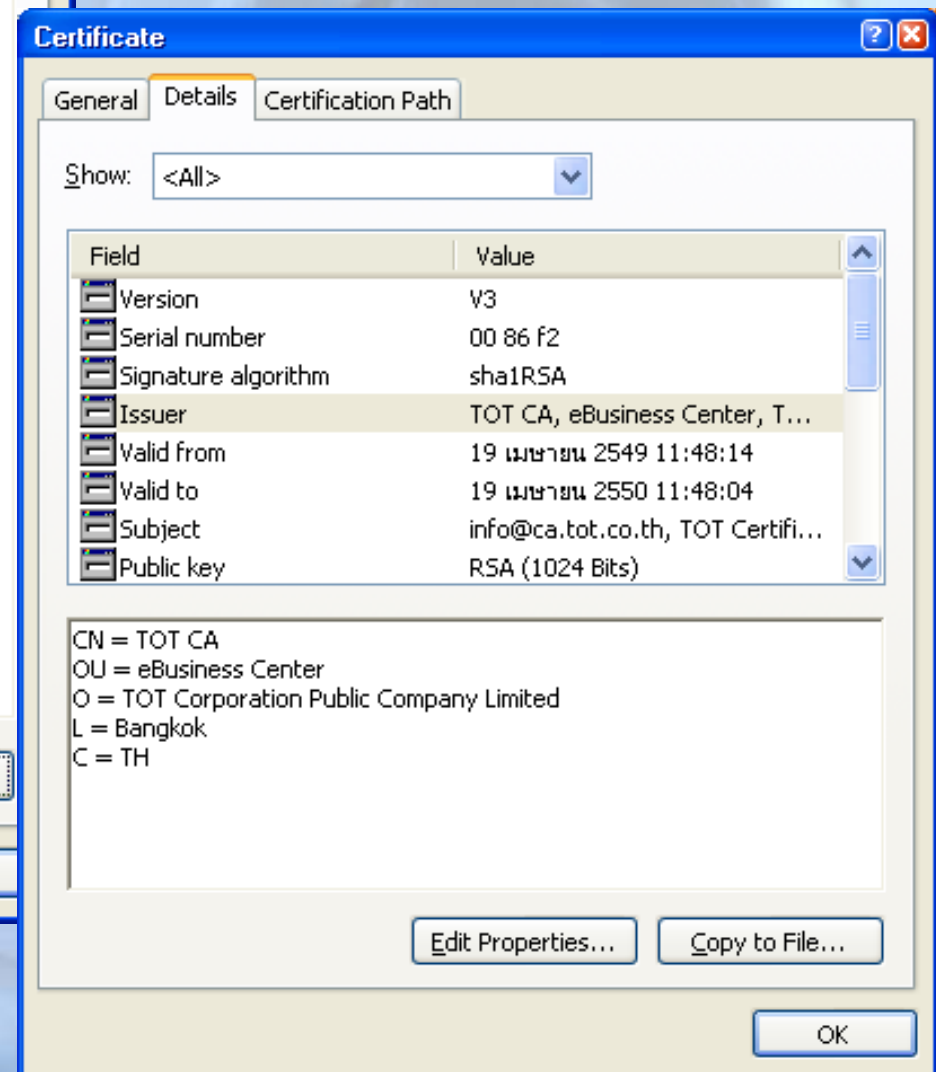
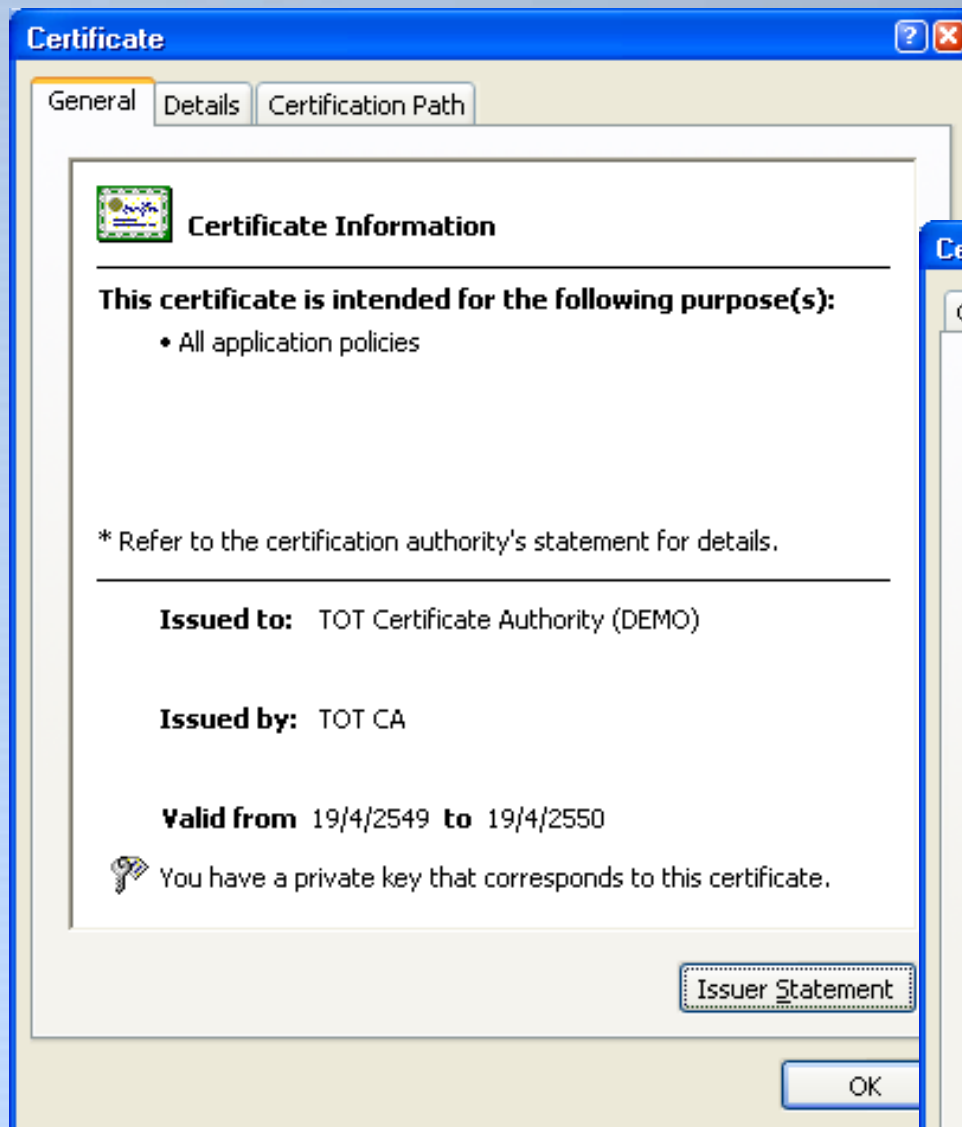
le86502hhd0viidywtoofkkrtgfgdserth;jpdml4554r3df3ddkias
736ed5viidywtoofkk5ewfgk98dszbcvcqm85k309nviidywjbkh

Signed by TOT CA

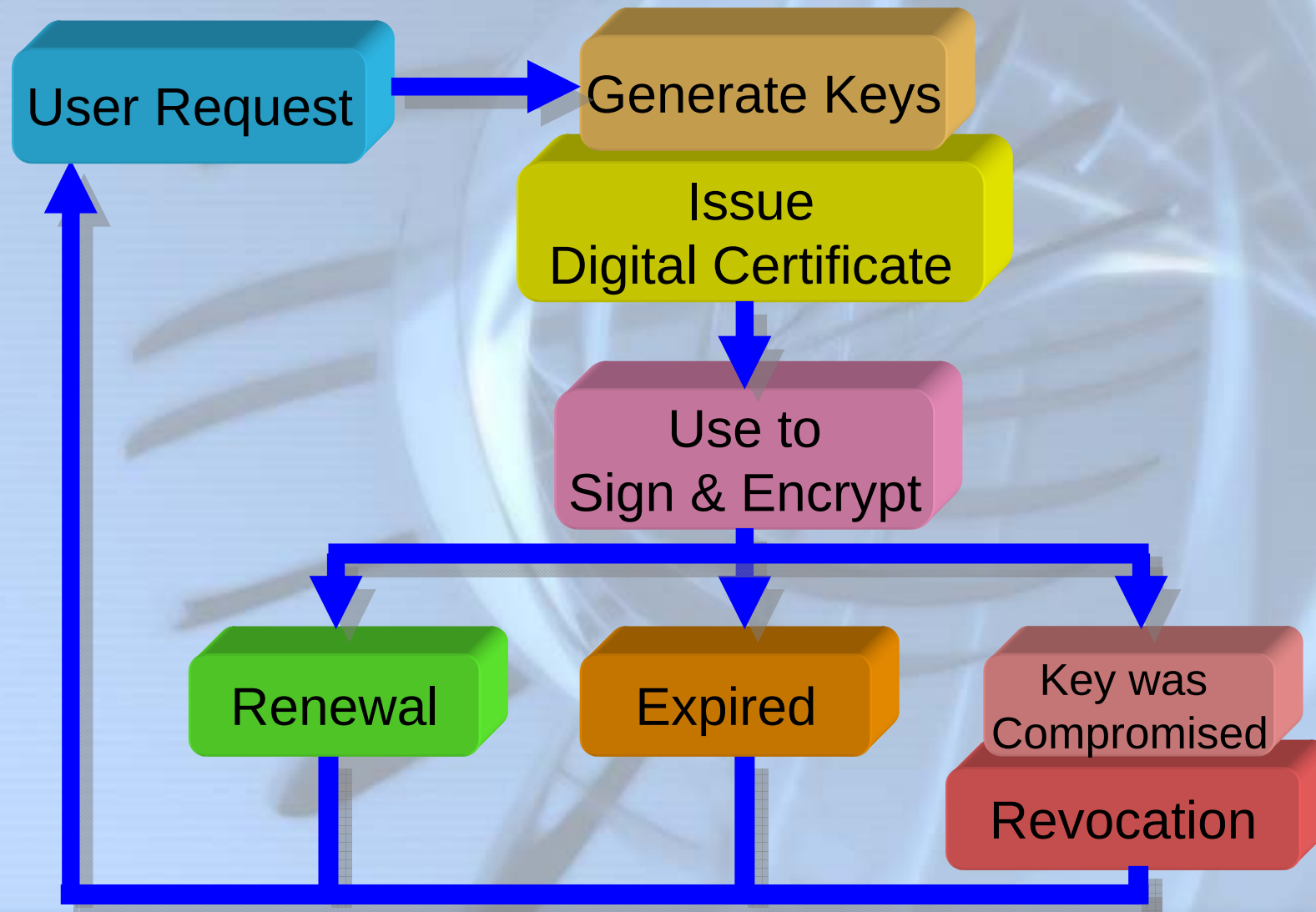
kdiowurei495729fd654df5646df3fgh5fgh153h3f1hshsg0925
h309afhwe09721h481903207akndnxnzkjaoiero10591328y5

Other Extension





Digital Certificate Life Cycle



TOT CA Product & Service

TOT CA Products and Price

TOT CA for Paperless Customs

Validity period 1 year

Key Store in Digital File
(PKCS#12)



Price : 500 ₪ / Year

- Must be install CA into your Computer
- Pass phase Protection

* Price not include VAT 7%

TOT CA Product & Service

TOT CA Products and Price

TOT Digital Certificate

Validity period 1 year

Key Store in Smart Card
(PKCS#11)



Price : 1,000 ฿ / Year

- CPU Smart Card
- Generate Keys and store in Smart Card
- Use Smart Card Reader
- PIN Code Protection
- More Security

* Price not include VAT 7%

TOT CA Product & Service

TOT CA Products and Price

TOT Digital Certificate

Validity period 1 year

Key Store in USB Token
(PKCS#11)



Price : 2,500 ₪ / Year

* Price not include VAT 7%

TOT CA Product & Service

TOT CA Website

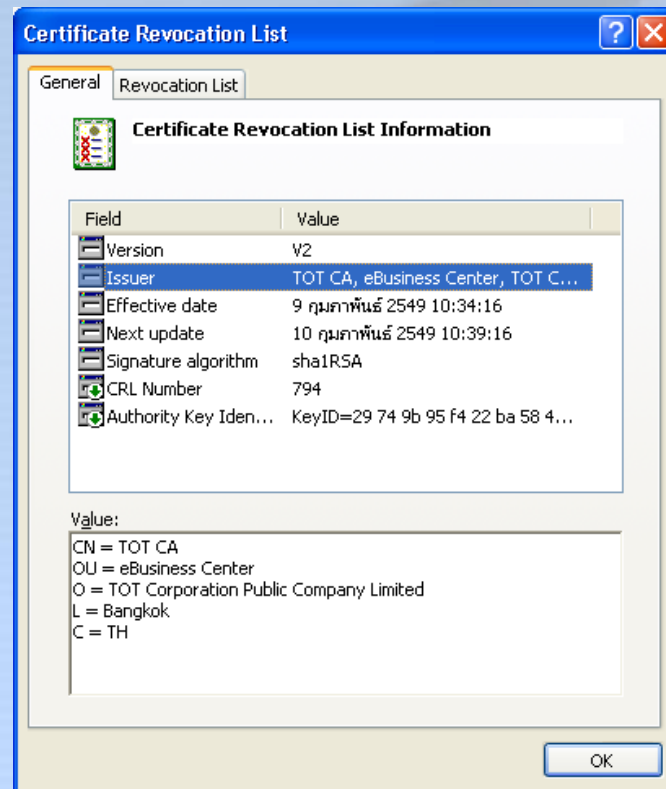
<https://www.ca.tot.co.th> (is updated Feb'06)



- Product List and Details
- PKI Knowledge
- Document & Manual (pdf)
- Download (Root, CRL, etc.)
- TOT CA Web board
- TOT CA Trial Register
- TOT CA Operation Flow
- TOT CA Contact and support
- TOT CA FAQ
- TOT CA CRL File
- Paperless Customs Info.

TOT CA Product & Service

TOT CA CRL Service

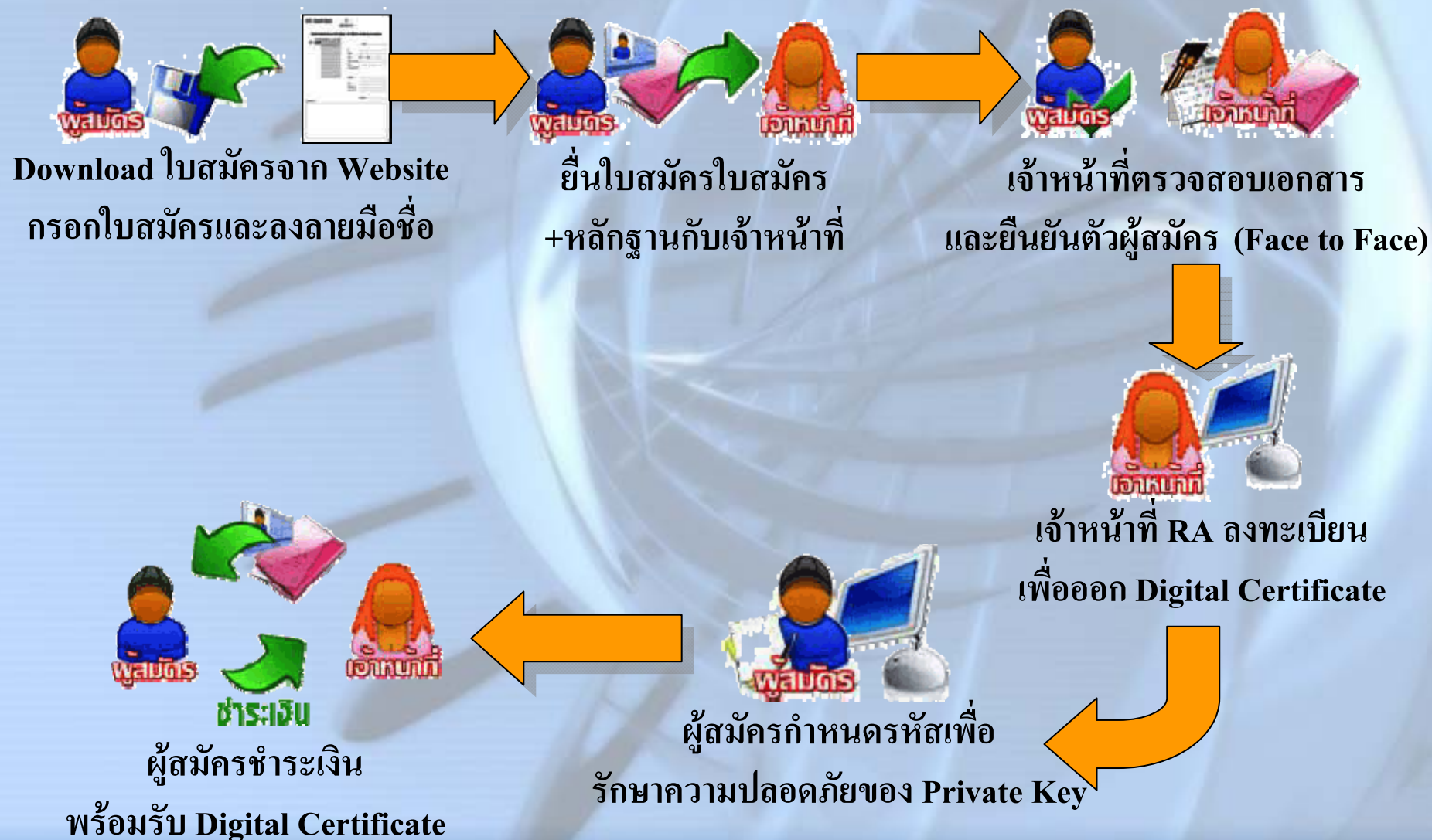


CRL (Certificate Revocation List)

- Generate every day
- Generate after Certificate is Revoked
- CRL File Service is available via HTTP and HTTPS
- CRL Properties Contained
 - Certificate Serial Number
 - Revocation Date
 - CRL Reason Code

https://www.ca.tot.co.th/download/totca_crl.crl

TOT CA Registration Flow



TOT CA Registration Flow

Document requirement for register

ประเภทบุคคล :

- ✓ สำเนาบัตรประจำตัวประชาชน หรือเอกสารทางราชการที่มีรูปถ่ายผู้ขอใช้บริการ
- ✓ สำเนาทะเบียนบ้าน

ประเภทนิติบุคคล :

- ✓ สำเนาทะเบียนพาณิชย์ หรือ สำเนาหนังสือรับรองการเป็นนิติบุคคล
- ✓ สำเนาบัตรประจำตัวประชาชนของผู้มีอำนาจ
- ✓ สำเนาบัตรประจำตัวประชาชนของผู้ยื่นคำขอฯ
- ✓ หนังสือมอบอำนาจให้ผู้ยื่นคำขอฯ เป็นผู้ดำเนินการพร้อมอากรแสตมป์ 10 บาท
- ✓ สำเนาใบทะเบียนภาษีมูลค่าเพิ่มของบริษัท (ภ.พ.20)
- ✓ กรณีที่เป็นชาวต่างชาติให้แนบใบสำคัญบุคคลต่าง ด้าว

TOT CA Registration Flow

Registration Place

- ศูนย์พาณิชย์อิเล็กทรอนิกส์
อาคาร 4 ชั้น 7 TOT สำนักงานใหญ่ ถ.แจ้งวัฒนะ
- ศูนย์บริการไปรษณีย์อิเล็กทรอนิกส์
อาคาร 120 ปี ชั้น 1 กรมศุลกากร (คลองเตย)
- บริการรับลงทะเบียนและออกใบรับรองฯ แบบเคลื่อนที่ (**Mobile RAO**)



TOT CA Helpdesk & Support

Phone : 0-2350-2093 , 0-2350-2079
0-2350-2108 , 0-2574-8912

Fax : 0-2350-2147 , 0-2574-8913

Website : <http://www.ca.tot.co.th>

Email : support@ca.tot.co.th

