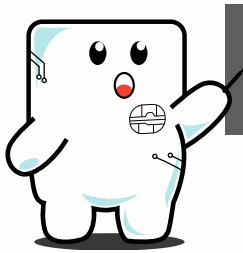
Electronic health record security and patients' data privacy

สุรางคณา วายุภาพ

ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)



สพธอ.ทำอะไร

มูลค่า e-Commerce ในภาคเอกชน

3.4

แสนล้านบาท

ประเภทธุรกรรมทางอิเล็กทรอนิกส์

e-COMMERCE

e-Certificate

e-trading & services

e-Payment

e-Health

จำนวนคนใช้อินเทอร์เน็ต

24

ล้านคน

จำนวนการใช้มือถือ

77.6

ล้านเลขหมาย

มูลค่า e-Payment ในระบบ การชำระเงิน

795

ล้านล้านบาท

พัฒนาส่งเสริมและสนับสนุน

e-COMMERCE

e-Payment

SMEs

สถิติภัยคุกคาม ตามประเภทภัยคุกคาม ในปี 2555 ไทย.ซิร์ตได้รับแจ้ง.เป็นจำนวน

792 เรื่อง

PHISHING 69.3%

MALWARE 10.3%

HACKING ATTEMPT 7.4%

ส่วนสนับสนุน

NRCA

ศึกษาความต้องการโครงสร้างพื้นฐานสารสนเทศ

40 ใบ

ส่งเสริมสนับสนุน เผยแพร่ความรู้

e-Time Stamping Authority

e-Notary Service

e-Archive & Record Management Service

ศึกษา วิจัย และพัฒนา ICT ที่เกี่ยวข้องกบธุรกรรมทางอิเล็กทรอนิกส์

คณะกรรมการบริหาร สพธอ.
(ตุลาคม ๒๕๕๕)

1 นายจรัมพร โชติกเสถียร
ประธานกรรมการ

2 นายไชยยันต์ พึ่งเกียรติไพโรจน์
กรรมการโดยตำแหน่ง

3 นางสาววิลาวรรณ วนดุรงค์วรรณ
กรรมการผู้ทรงคุณวุฒิ
(ด้านการเงิน)

4 นายวรวิทย์ จำปีรัตน์
กรรมการโดยตำแหน่ง

5 นายทวีศักดิ์ กออนันตกูล
กรรมการโดยตำแหน่ง

6 นายอภิรมย์ น้อยอ่ำ
กรรมการผู้ทรงคุณวุฒิ
(ด้านพาณิชย์อิเล็กทรอนิกส์)

7 นายธีระ อภัยวงศ์
กรรมการผู้ทรงคุณวุฒิ
(ด้านวิทยาการคอมพิวเตอร์)

8 นายชวลิต อัตถศาสตร์
กรรมการผู้ทรงคุณวุฒิ
(ด้านนิติศาสตร์)

9 นายปรีชา ปรมาพจน์
กรรมการผู้ทรงคุณวุฒิ
(ด้านการเงิน)

10 นายสมพรต สาระโกเศศ
กรรมการผู้ทรงคุณวุฒิ
(ด้านสังคมสตร์)

11 นางสุรางคณา วายุภาพ
กรรมการและเลขานุการ

Related Strategic plans

ยุทธศาสตร์ประเทศไทย

ยุทธศาสตร์ที่ 1: การพัฒนาระบบโลจิสติกส์ โครงสร้างพื้นฐาน พลังงาน และ ICT เพื่อทำให้เกิดความเชื่อมโยงทั้งภายในและต่างประเทศ

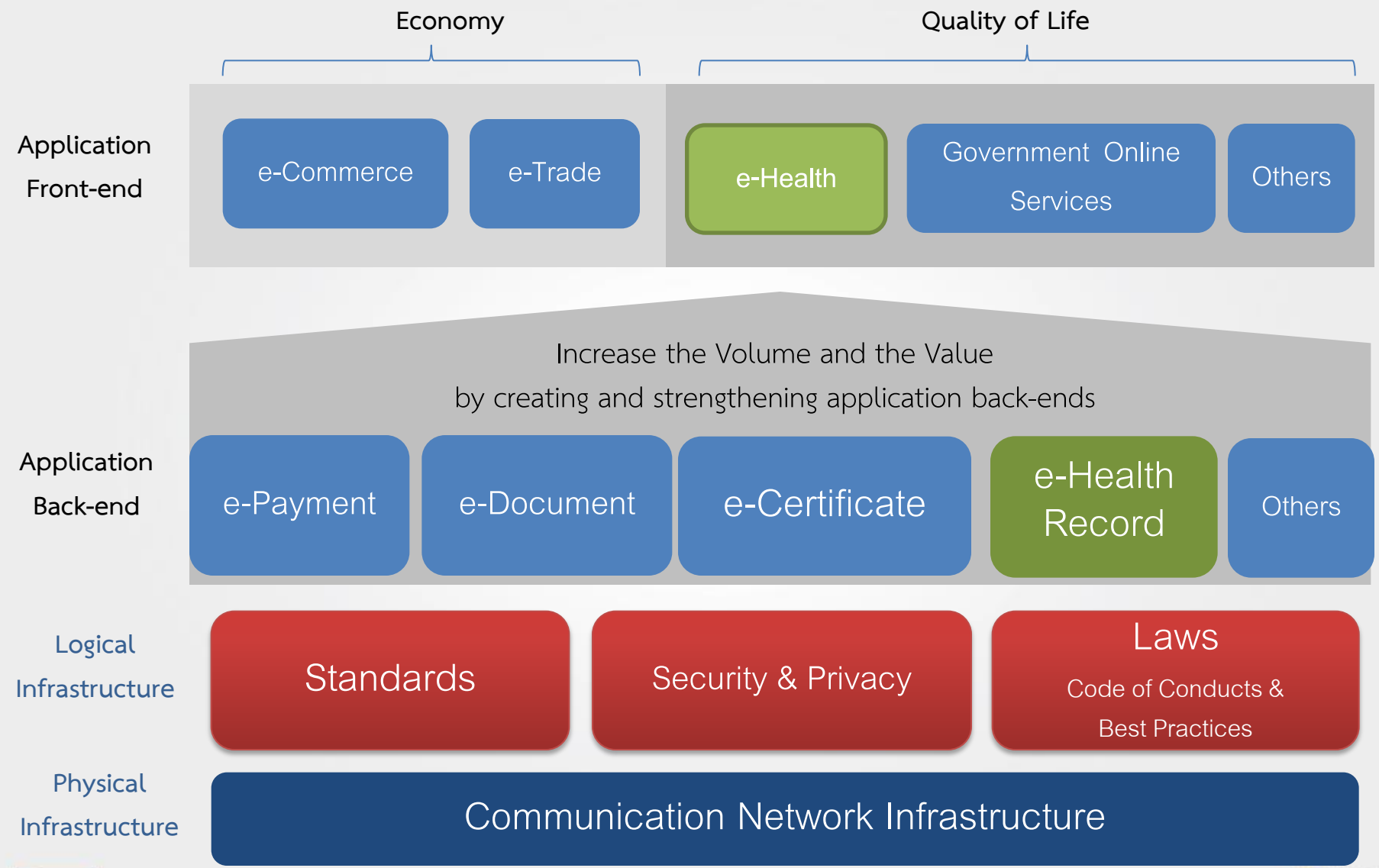
(ร่าง) แผนแม่บทธุรกรรมทางอิเล็กทรอนิกส์

ผลักดันให้เกิดระบบบริการทางการแพทย์และสุขภาพผ่านทางอิเล็กทรอนิกส์เพื่อคุณภาพชีวิตที่ดีขึ้นของประเชาชน

ยุทธศาสตร์ที่ 5

- มีองค์กรระดับประเทศเพื่อกำหนดทิศทางสำหรับการพัฒนาระบบสารสนเทศและเทคโนโลยีสารสนเทศสุขภาพของประเทศได้อย่างมีประสิทธิภาพ — กลยุทธ์ที่ 5.1
- จัดทำและปรับปรุงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยและข้อมูลสุขภาพส่วนบุคคล — กลยุทธ์ที่ 5.2
- พัฒนามาตรฐานข้อมูลสุขภาพเพื่อรองรับการเชื่อมโยงข้อมูลได้อย่างปลอดภัย — กลยุทธ์ที่ 5.3

(ร่าง) แผนแม่บทเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทย (2556-2560)



Application back-end components

e-Certificate

- การรับรองสิทธิ์ เป็นการรับรองหรืออนุญาตให้ใช้สิทธิ์ตามเงื่อนไขที่กำหนดไว้ ในรูปแบบต่างๆ เช่น ใบอนุญาต ใบรับรอง การขึ้นทะเบียน เป็นต้น

e-Payment

- การชำระเงินทางอิเล็กทรอนิกส์ การโอนสิทธิการถือครองเงิน หรือการโอนสิทธิการถอนเงิน หรือหักเงินจากบัญชีเงินฝากของผู้ใช้บริการที่เปิดไว้กับผู้ให้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน

e-Health

- การนำวิธีการสื่อสารทางอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศมาประยุกต์ใช้กับงานด้านสาธารณสุข

e-Health record

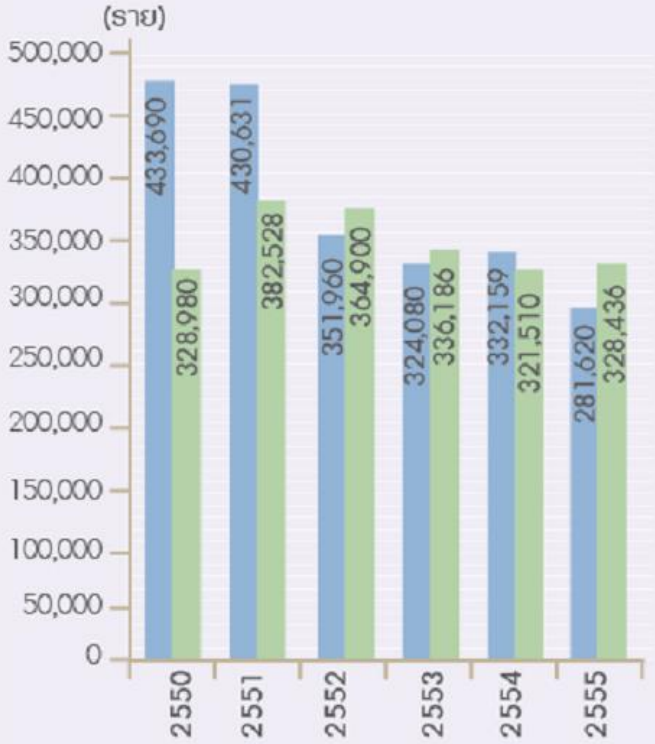
- ข้อมูลอิเล็กทรอนิกส์ทางการแพทย์/สถานพยาบาล/ผู้ป่วย

e-Document

- การจัดทำรายงานและเผยแพร่ในรูปแบบอิเล็กทรอนิกส์ ซึ่งผู้ใช้สามารถดาวน์โหลดได้ทางออนไลน์ หรือการรับ-ส่ง และจัดเก็บหนังสือทางอิเล็กทรอนิกส์ ซึ่งเป็นระบบหนังสือราชการทางออนไลน์ จะช่วยให้ผู้ใช้สามารถเรียกใช้และอัพโหลดไฟล์เหล่านั้นผ่านอินเทอร์เน็ตได

e-Medical record statistic

แผนภาพที่ 22 ปริมาณเวชระเบียนอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์



CAGR	Growth	Rate
2550-2555	2553-2554	2554-2555
-8.3%	2.5%	-15.2%
-0.03%	-4.4%	-2.2%

ที่มา: โรงพยาบาลที่มีการผลิตบุคลากรทางการแพทย์ ได้แก่ ร.พ. ศิริราช ร.พ. จุฬาลงกรณ์ และ ร.พ. มหาราชนครเชียงใหม่ เป็นต้น

แผนภาพที่ 23 ปริมาณการใช้บริการภาพเวชระเบียนอิเล็กทรอนิกส์

CAGR	Growth	Rate
2550-2555	2553-2554	2554-2555
85.1%	1.0%	36.2%

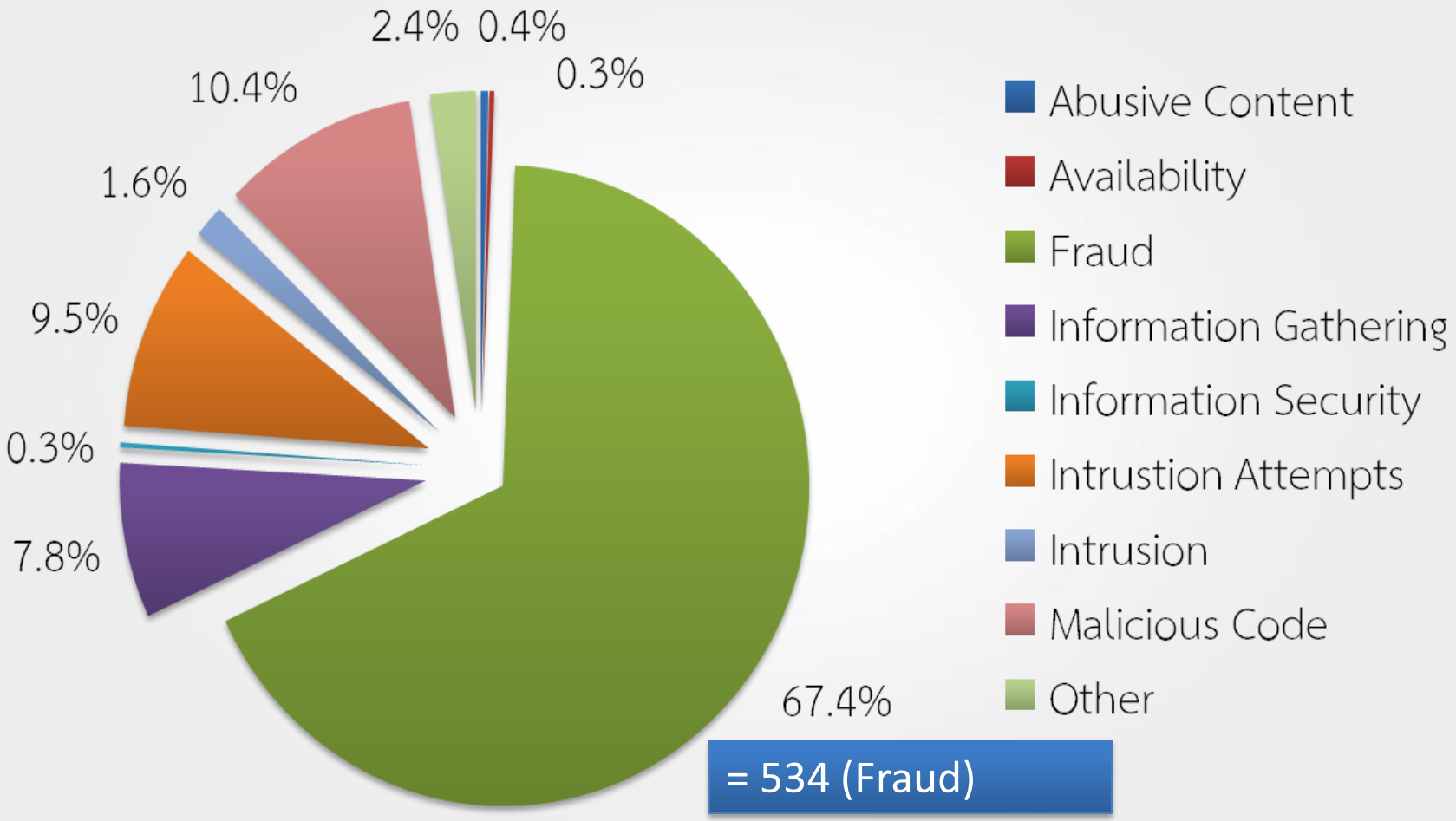
ที่มา: โรงพยาบาลที่มีการผลิตบุคลากรทางการแพทย์ ได้แก่ โรงพยาบาลศิริราช โรงพยาบาลจุฬาลงกรณ์ และโรงพยาบาลมหาราชนครเชียงใหม่ เป็นต้น

สัดส่วน รพ. ที่มีการแลกเปลี่ยนข้อมูลหรือส่งต่อข้อมูลผ่านระบบสารสนเทศต่างๆ พ.ศ. 2553

ประเภทของข้อมูล	ภายในโรงพยาบาล	ภายนอกโรงพยาบาล
ข้อมูลทั่วไปของผู้ป่วย	48.8%	11.1%
ประวัติการเจ็บป่วยและบันทึกทางการแพทย์ในแผนกผู้ป่วยนอก	41.4%	8.6%
ประวัติการเจ็บป่วยและบันทึกทางการแพทย์ในแผนกผู้ป่วยใน	46.4%	12.5%
การวินิจฉัยโรคของผู้ป่วยนอก	50.9%	10.4%
การวินิจฉัยโรคของผู้ป่วยใน	30.8%	7.3%
ยาที่แพทย์สั่งให้ผู้ป่วยนอก	40.3%	11.6%
ยาที่แพทย์สั่งให้ผู้ป่วยใน	41.3%	9.1%
รายการผ่าตัดและการทำหัตถการ	32.4%	9.1%
ผลการตรวจทางห้องปฏิบัติการ	43.8%	8.6%
ภาพและผลการตรวจทางรังสีวิทยา	15.3%	3.8%

ที่มา: Theera-Ampornpunt N. Thai hospitals' adoption of information technology: a theory development and nationwide survey [dissertation]. Minneapolis (MN): University of Minnesota; 2011 Dec. 376 p.

ThaiCERT: 792 Security Incidents in 2012



Healthcare data breaches Trends: 2012

Breaches by Type	2010	2011	2012 (Q1 and Q2)	2012 (Projected)
Theft	107	82	41	88
Loss	34	15	6	13
Unauthorized Access/Disclosure	22	20	5	17
Incorrect Mailing	10	10	5	9
Improper Disposal	11	9	3	7
Hack	11	8	6	12

Theft continues to dominate as the most likely cause of a breach in healthcare.

Breaches by Source	2010	2011	2012 (Q1 and Q2)	2012 (Projected)
Desktop Computer	26	15	5	10
Laptop Computer	49	32	23	40
Mobile Media	36	28	7	15
Network Server	16	15	6	15
Paper Records	49	41	12	32
System/Application	12	5	3	9

The breaches involving laptops and mobile media, of which we continue to see high numbers

Reference: “A Look Back: U.S. Healthcare Data Breach trend” By Hitrust

Facts on Healthcare data breaches in USA: 2012

1. The healthcare industry in US loses $7 billion a year due to health data breaches
2. The average economic impact of a data breach has increased by $400,000 to a total of $2.4 million since 2010
3. 94% of healthcare organizations have had at least one data breach in the last two years
4. The average number of lost or stolen records per breach is 2,769
5. Only 40% of organizations have confidence that they are able to prevent or quickly detect all patient data loss or theft
6. 18% of healthcare organizations say medical identity theft was a result of a data breach
7. Annual security risk assessments are done by less than half (48%) of organizations
8. 48% of data breaches in 2012 involved medical files
9. The primary activity conducted by healthcare organizations to comply with annual or periodic HIPAA privacy and security is awareness training of all staff (56%), followed by vetting and monitoring of third parties, including business associates (49%)

Reference: http://www.datafiletechnologies.com/hipaa-breach-statistics-2012/#.Ug3xHtJkNf8

กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (Data privacy)

ข้อมูลด้านสุขภาพของบุคคล เป็นความลับส่วนบุคคล ผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายมิได้ เว้นแต่การเปิดเผยนั้นเป็นไปตามของบุคคลนั้นโดยตรงหรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย แต่ไม่ว่าในกรณีใดๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่น เพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลมิได้

มาตรา ๗ พ.ร.บ. สุขภาพแห่งชาติ

เปิดเผย การรักษาความลับเป็นข้อยกเว้น คุ้มครองข้อมูลข่าวสารส่วนบุคคล ไม่รวมเครื่องหมายชี้ตัวบุคคลซึ่งเป็นสิ่งที่สมมุติขึ้นแทนตัวตน เช่น ชื่อ, นามสกุล, รหัส, ตำแหน่ง, เพศ, สัญชาติ แต่มิใช่ข้อมูลแสดงสิ่งเฉพาะตัวหรือข้อมูลเฉพาะตัวบุคคล (แต่หมายถึงข้อมูลส่วนตัวหรือข้อมูลสถานะของบุคคล) เป็นเพียงสิ่งที่ทำให้รู้ตัวบุคคลเท่านั้น ไม่สามารถสื่อถึงเรื่องราวของบุคคลนั้นได้

พ.ร.บ. ข้อมูลข่าวสารของราชการพ.ศ. ๒๕๔๐

พระราชกฤษฎีกาฉบับนี้กำหนดว่าในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูลหรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคลไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลด้วย เช่น

1. ประกาศคณะกรรมการธุกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์

พ.ร.ฎ.กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

กฎหมายที่เกี่ยวข้องกับการยืนยันตัวบุคคล (Authentication)

พระราชบัญญัตินี้มิได้มีบทบัญญัติเกี่ยวกับ e-authentication โดยตรง แต่ได้กำหนดหลักการเรื่องการพิสูจน์ตัวตนโดยการใช้ลายมือชื่ออิเล็กทรอนิกส์ไว้

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์

1. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
2. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง การรับรองสิ่งพิมพ์ออก พ.ศ. ๒๕๕๕
3. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
ซึ่งได้มีบทบัญญัติที่เกี่ยวข้องกับการยืนยันตัวตน (Authentication)

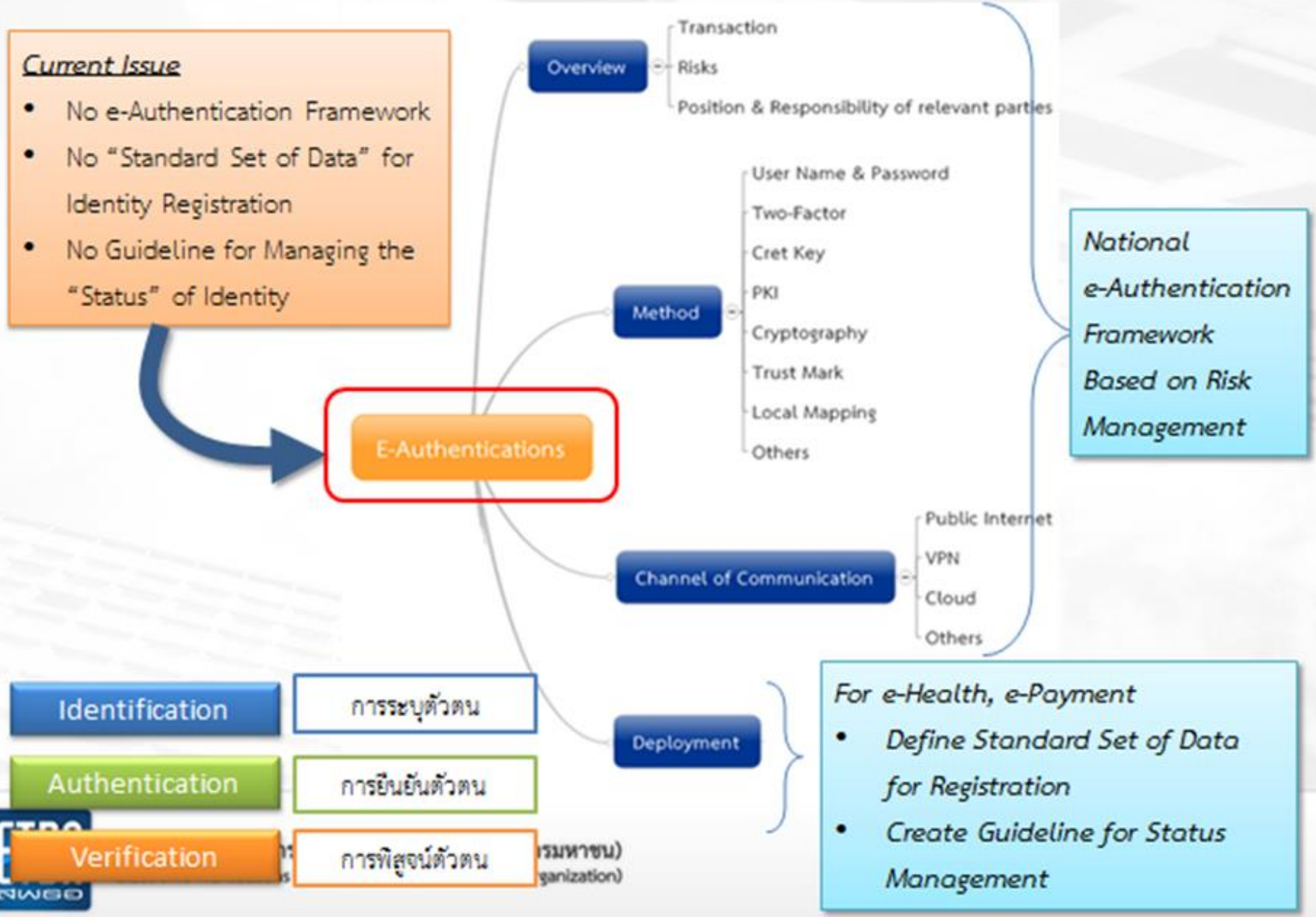
ประกาศธนาคารแห่งประเทศไทย ที่ สขร. ๓/๒๕๕๒ เรื่อง นโยบายและมาตรการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์

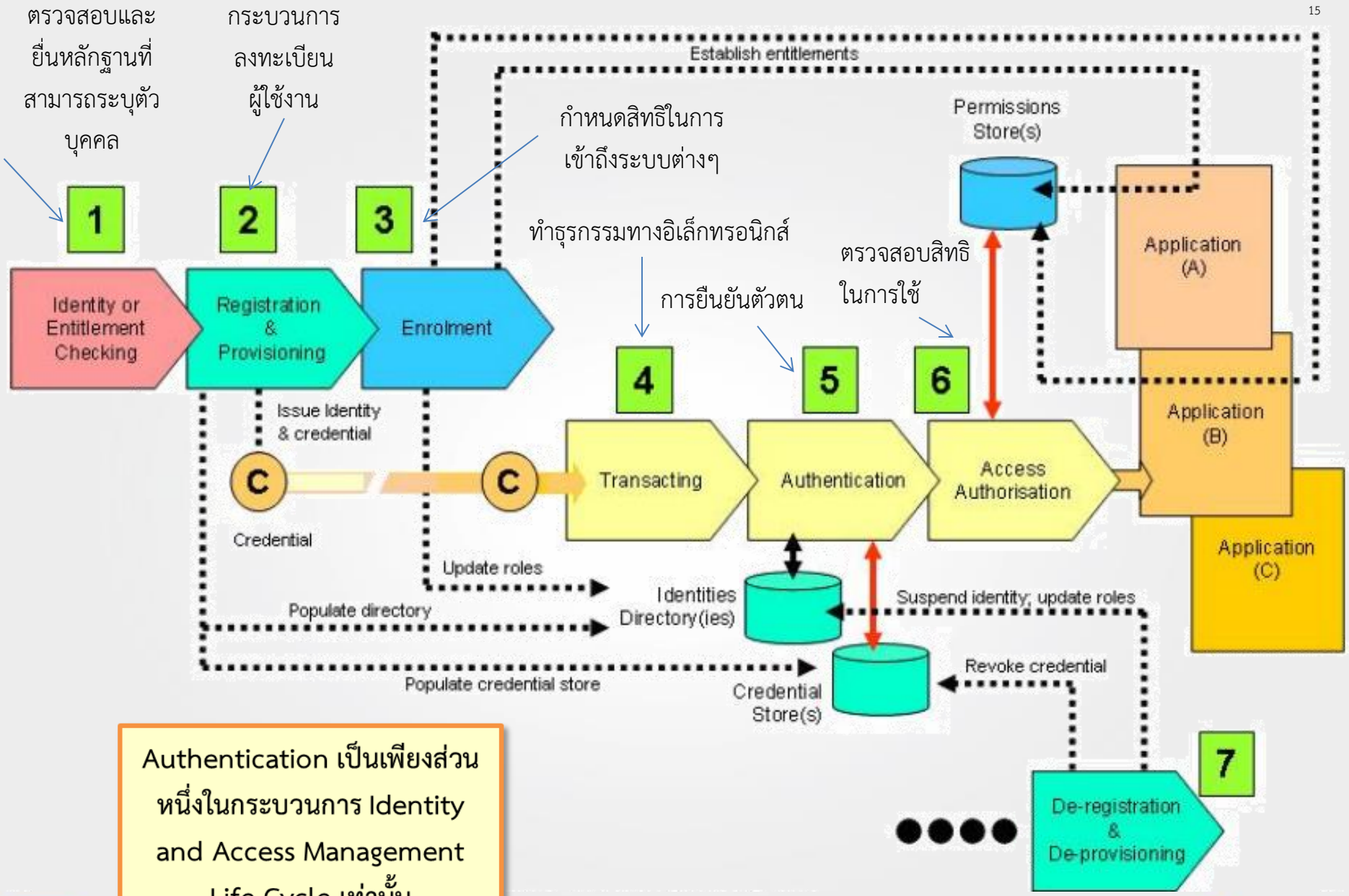
ประกาศธนาคารแห่งประเทศไทย

พระราชบัญญัติฉบับนี้ไม่ได้กำหนดเกี่ยวกับการยืนยันตัวตนไว้โดยตรง แต่ได้กำหนดโทษทางอาญาสำหรับผู้ที่เข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงไว้โดยเฉพาะโดยมิชอบ และมาตรการนั้นมิได้มีไว้สำหรับบุคคลนั้น

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

E-Authentication Overview





Authentication เป็นเพียงส่วนหนึ่งในกระบวนการ Identity and Access Management Life Cycle เท่านั้น

e-Authentication Definition Case studies

Case1: **ประเทศอเมริกา** (NIST) จะอธิบายความต้องการด้านเทคนิคสำหรับการระบุตัวตนผ่าน remote network (จึงไม่ได้พูดถึงเรื่อง biometrics)

Case2: **ประเทศออสเตรเลีย** แบ่งเป็นการระบุตัวตนของกลุ่มภาคธุรกิจหรือตัวบุคคล และกลุ่มของเว็บไซต์ภาครัฐ และแบ่ง level ความสำคัญให้แก่ทั้งสามองค์ประกอบคือ (1) Registration (2) Credential Type (3) Credential Management

Case3: **ประเทศอินเดีย** เน้นเฉพาะกับการทำงานที่เกี่ยวข้องกับรัฐผ่านการใช้งานอินเทอร์เน็ตหรือมือถือ

Reference: (1) Electronic Authentication Guidance (NIST Special Publication 800-63), April 2006
National Institute of Standards and Technology, U.S. Department of Commerce
(2) Australia: National e-Authentication Framework (NeAF), January 2009:
Australian Government Information Management Office, Department of Finance and Deregulation
(3) India: Draft National e-Authentication Framework (NeAF) Version 1.0, Date -01-09-2011
National e-Government Division, Department of Information Technology

เปรียบเทียบ Definition

Case Studies

Assurance Level	Definition	Definition		
		US.	Australia	India
Null (level 0)	ไม่จำเป็นต้องระบุตัวตน	-	No confidence is required in the identity assertion	No assurance of identity is required
Minimal (level 1)	ความต้องการการระบุตัวตนน้อยมาก	Little or no confidence in the asserted identity's validity	Minimal confidence is required in the identity assertion	Minimal level of assurance of identity is required
Low (level 2)	ความต้องการการระบุตัวตนน้อย	Some confidence in the asserted identity's validity	Low confidence is required in the identity assertion	Minor level of assurance of identity is required
Moderate (level 3)	ความต้องการการระบุตัวตนปานกลาง	High confidence in the asserted identity's validity	Moderate confidence is required in the identity assertion	Significant level of assurance of identity is required
High (level 4)	ความต้องการการระบุตัวตนสูง	Very high confidence in the asserted identity's validity	High confidence is required in the identity assertion	Substantial level of assurance of identity is required

เปรียบเทียบ Authentication Mechanisms

Case Studies

Assurance Level	Credential Type		
	US.	Australia	India
Null (level 0)	-	ไม่ต้องมีการระบุตัวตน	ไม่ต้องมีการระบุตัวตน
Minimal (level 1)	Personal password	Pre-registered origin	ใช้ username/password
Low (level 2)	token on secure protocol	Memorized password User-supplied shared info Context-specific shared info Voice biometric	PKI X.509/Soft Token
Moderate (level 3)	Cryptographic protocol + Soft/hard/OTP + password	Code book Call back to pre-registered(voice, SMS OTP, email OTP) + memorize password SW crypto : Symmetric key SW crypto : Asymmetric key OTP device	2 factor authentication: Soft/hard token + username/password
High (level 4)	Secure protocol +only hard crypto token	HW crypto : Symmetric key HW crypto : Asymmetric key	Soft/hard token + biometric + username/password

ETDA roles for e-health security and privacy

Present | Future | External entity

e-Payment applications | e-Trade applications | e-Health applications | e-Invoice applications | e-Document applications

Application front-end

XML message validation Tools

Application Back-end

Transaction ID Management service (TIMS)

Trusted e-Document Authority (TeDA)

CAs

TDID | TOT | CAT

จัดเก็บและสืบค้นรายการรหัสข้อมูลสุขภาพที่เกี่ยวข้องเพื่อการอ้างอิง

Code and Message Repository (CMR)

e-Notary | e-Archive | e-Timestamp

National Root CA (NRCA)

(ร่าง) พ.ร.ฎ. ว่าด้วยการกำกับดูแลธุรกิจบริการการให้บริการออกใบรับรองอิเล็กทรอนิกส์

Logical Infrastructure

ITU-T X.660 / ISO/IEC 9834 (OID)

(ร่าง) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

(ร่าง) มาตรฐานข้อความและเอกสารทางอิเล็กทรอนิกส์เพื่อการส่งต่อผู้ป่วยด้วย HL7 CDA

พ.ร.บ.สุขภาพแห่งชาติ

รหัสยา (TMT) | NPMS | พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ | พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์

Standards | Security | Law