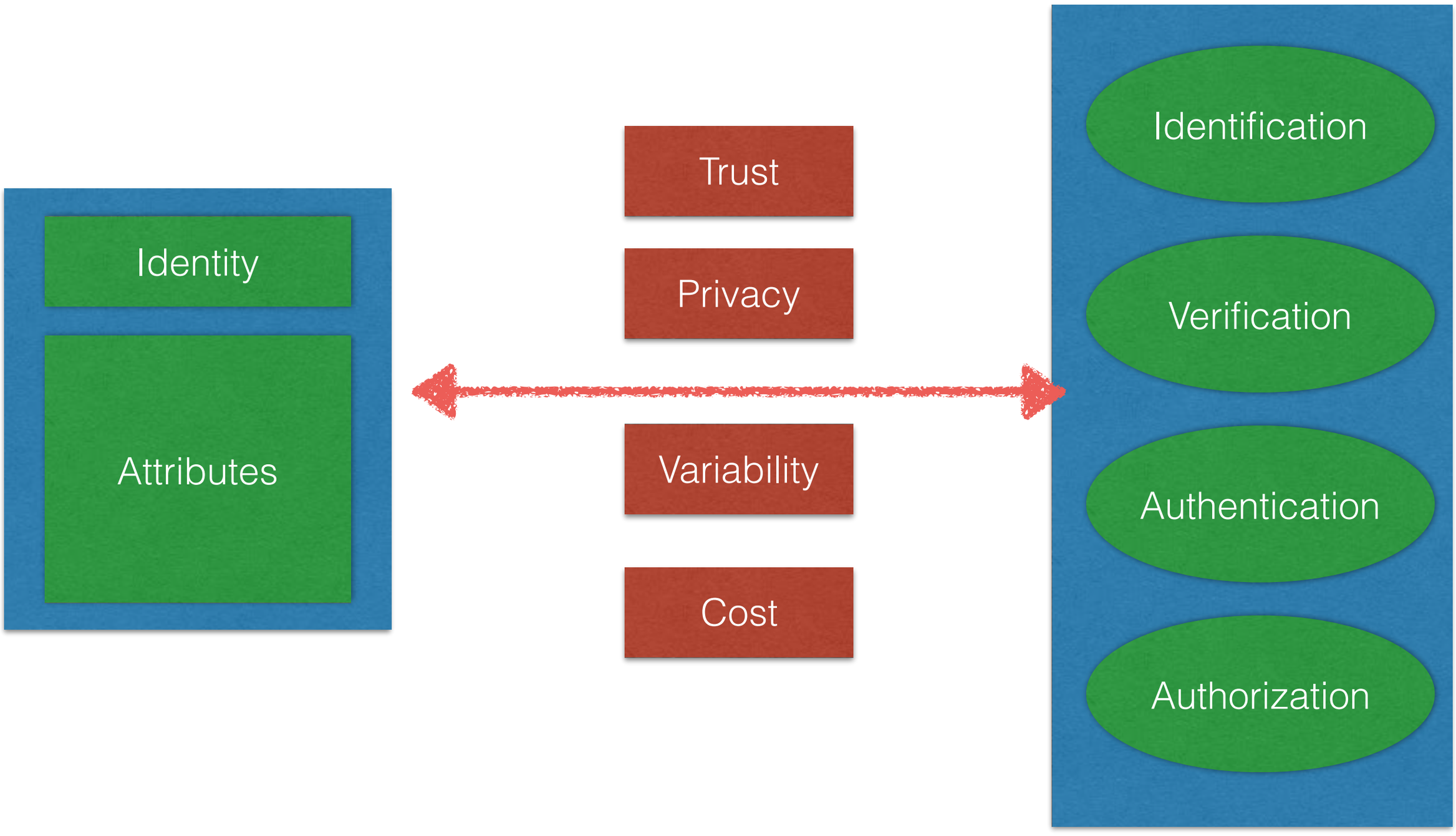
E-KYC and Digital Identity

Bhume Bhumiratana, Ph.D.

eKYC


Identity
Attributes
Trust
Privacy
Variability
Cost
Identification
Verification
Authentication
Authorization

Core Requirements

- Security and Trust — รองรับการใช้เทคโนโลยีด้านความมั่นคงปลอดภัยที่ทันสมัย สามารถต่อยอดให้รองรับเทคโนโลยีใหม่ๆได้ และมีความน่าเชื่อถือ ปลอดภัย

- Privacy Protection and Privacy Enhancing by design — ระบบต้องดูแลปกป้องไม่ให้เกิดความเสียหายต่อข้อมูลส่วนบุคคลหรือสิทธิการเข้าถึงหรือการละเมิดสิทธิเกี่ยวกับข้อมูลส่วนบุคคล

- Open, Accessible, and Inclusive — ระบบต้องเป็นระบบเปิด ให้บุคคลและองค์กรต่างๆเข้าถึงและใช้ประโยชน์ได้อย่างปลอดภัยและเคารพสิทธิของบุคคล และต้องให้บุคคลสามารถเข้าถึงและควบคุมข้อมูลของตนเองได้

- Robustness and Scalability — มีความมั่นคง ให้บริการได้ ตลอดเวลา (24/7 ตลอด 365 วัน) ไม่มีความเสี่ยงเรื่องการล่มของระบบ สามารถทนทานต่อปัญหาที่เกิดขึ้นได้ สามารถขยายเพื่อรองรับการใช้งานในระยะยาวได้เมื่อมีการทำธุรกรรมเพิ่มมากขึ้น

- Transparency and Governance — ระบบต้องสามารถถูกตรวจสอบความน่าเชื่อถือได้ทั้งจากรัฐ เอกชน และภาคประชาสังคม การดูแลบริหารจัดการต้องมีโครงสร้างการจัดการที่มีธรรมาภิบาล ตรวจสอบได้ ไม่มีบุคคลใดสามารถเอาเปรียบหรือใช้ประโยชน์จากระบบอย่าที่ไม่ควร

- Convenience — ใช้ง่าย ปลอดภัย ไม่เป็นที่ลำบากต่อผู้ใช้

- Data Minimization — จำกัดการเก็บข้อมูลส่วนบุคคลในระบบกลางเพื่อลดความเสี่ยง

Benefit

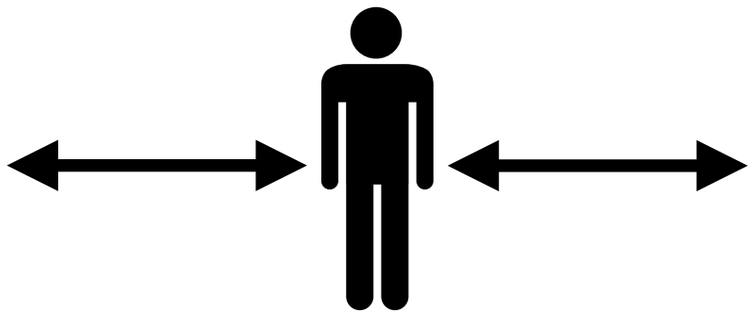
- Reduce cost of doing business online
  - ลดต้นทุนในการทำธุรกรรมดิจิทัล ลดความเสี่ยง (เช่น ความเสี่ยงด้าน KYC)
- Accelerate speed and convenience
  - เพิ่มความเร็วและความสะดวกสบาย
- Secure and Increase trust
  - มั่นคงปลอดภัย น่าเชื่อถือ ทำให้ธุรกรรมดิจิทัลมีความน่าเชื่อถือมากขึ้น

Design Principle

- The system must have the following properties
- Open and extensible system — ต้องเป็นระบบเปิด ที่สามารถต่อยอดเพื่อใช้งานในภาคเอกชนได้
- Support Cross-Verification among relevant parties (such as between relying parties, or relying parties and authoritative party)
    - สามารถต่อยอดให้องค์กรต่างๆสามารถทำการแบ่งปันหรือร่วมกันทำการยืนยันตัวบุคคลได้
- Support Cross-Authentication
    - Enable multiple method of authentication to be plugged in to the system — สามารถต่อยอดเทคโนโลยีการยืนยันตัวตน ให้รองรับเทคโนโลยีอื่นๆที่องค์กรต่างๆอาจนำมาใช้เพิ่มเติมได้
    - Support offline authentication (Face-to-Face Authentication or paper based authentication)
        - สามารถรองรับการทำธุรกรรมทั่วไป (นอกระบบ ดิจิทัล) ได้ เช่นการให้บริการที่สาขา หรือการส่งข้อมูลนอกระบบ ที่สามารถตรวจสอบและยืนยันได้
- Single truth shared among all parties without sharing raw data
    - ระบบสามารถใช้เป็นแหล่งยืนยันความถูกต้องของข้อมูลกลางที่น่าเชื่อถือได้ โดยไม่เพิ่มความเสี่ยงต่อการเข้าถึงข้อมูล
- Support Proxy or Delegate authentication and service model (สำหรับคนที่ยังเข้าไม่ถึงเทคโนโลยี ก็สามารถฝากผู้อื่นใช้บริการได้อย่างตรวจสอบได้)
- Identities can be extended to support Foreigner Identity and Business (สามารถรองรับการให้บริการต่อบุคคลต่างชาติ หรือนิติบุคคล ได้ในอนาคต)

Relying Party
(Service provider)

Government Agencies
Banking Services
Hospital
School
E-Commerce
Insurance
Capital Market Services



Individual

Authoritative Party
(LoA 1-4)

Government Agencies
- Citizen Card
- Driver's license
- ...

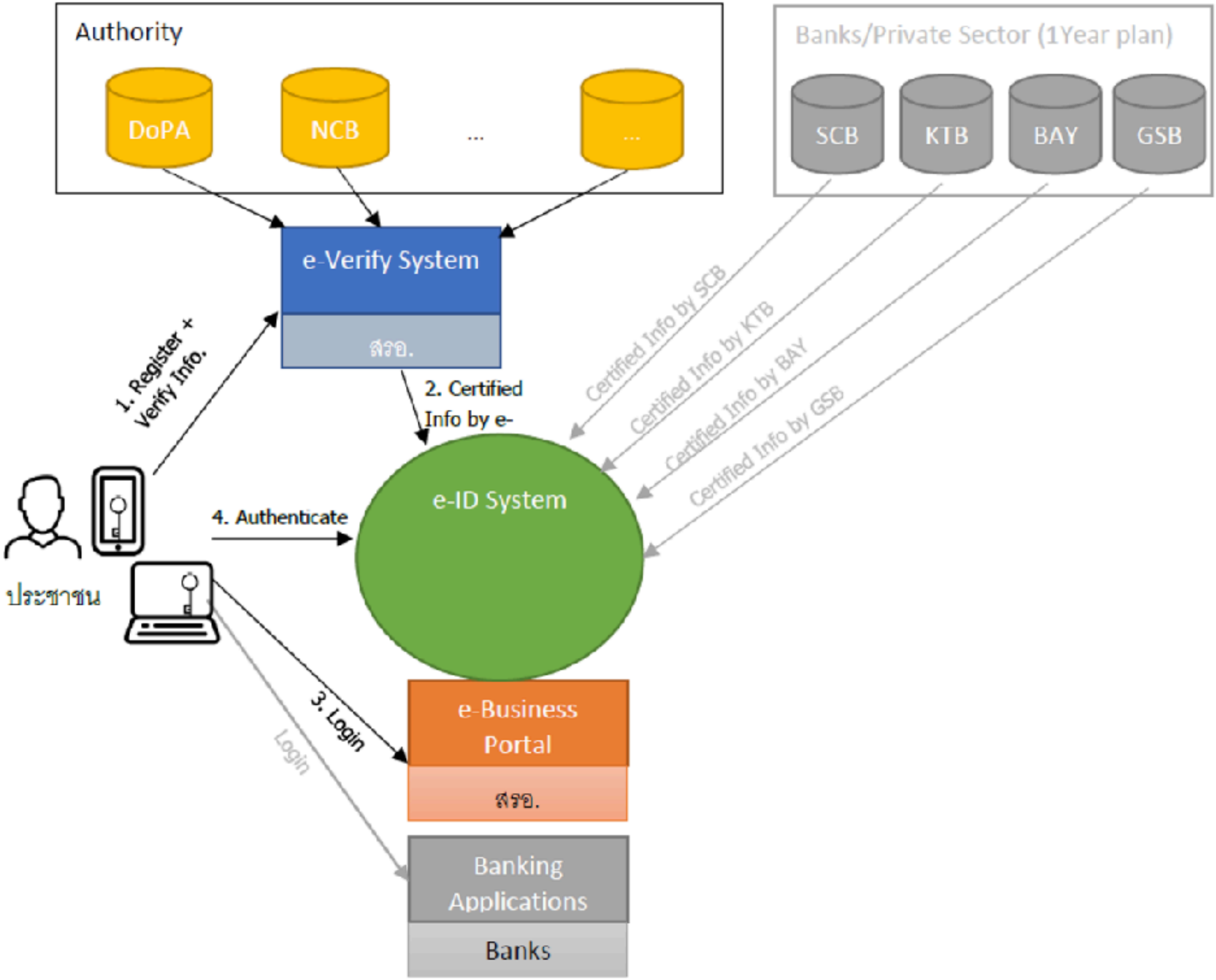
Regulated Entities
- Financial Institution
- Telco

ใช้บริการเพื่อยืนยันตัวบุคคล
ที่มาขอทำธุรกรรม

เข้าใช้บริการยืนยันตัวตน
ให้ความยินยอมและ
ควบคุม digital identity

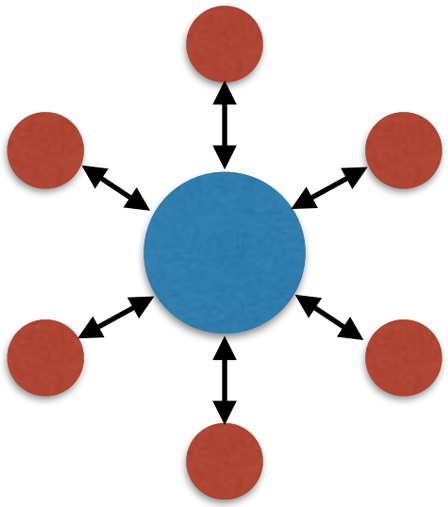
ยืนยันตัวบุคคล
และระดับความน่าเชื่อถือ

Digital Identity Platform
- Authentication
- Verification
- Consent and Digital Signatures

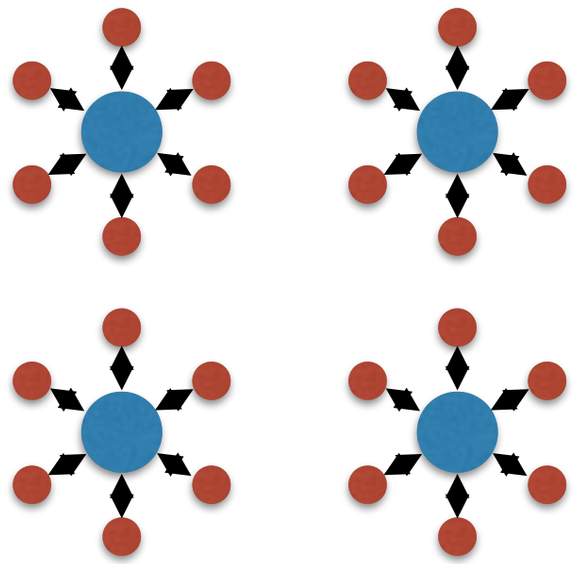

Authority
DoPA
NCB
...
...
Banks/Private Sector (1Year plan)
SCB
KTB
BAY
GSB
e-Verify System
สรอ.
1. Register + Verify Info.
2. Certified Info by e-
Certified Info by SCB
Certified Info by KTB
Certified Info by BAY
Info by GSB
e-ID System
4. Authenticate
ประชาชน
3. Login
Login
e-Business Portal
สรอ.
Banking Applications
Banks

National/Shared E-KYC Models

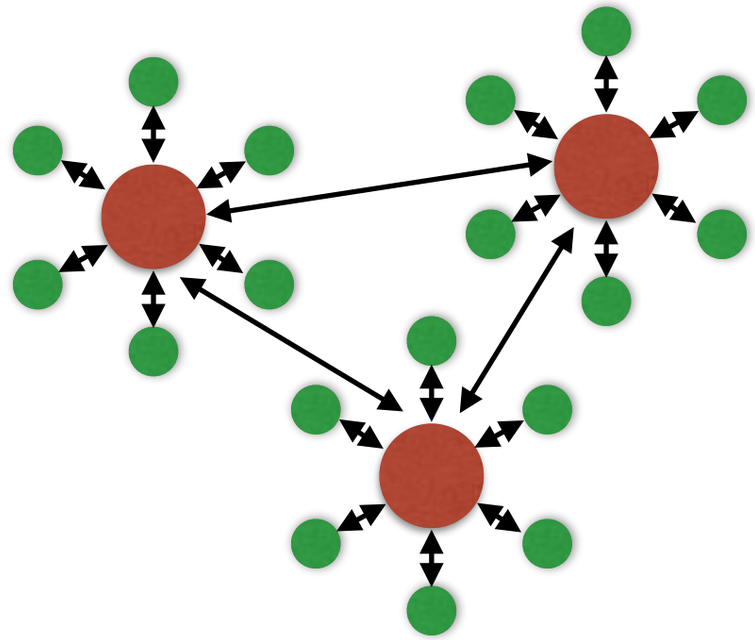
Centralized



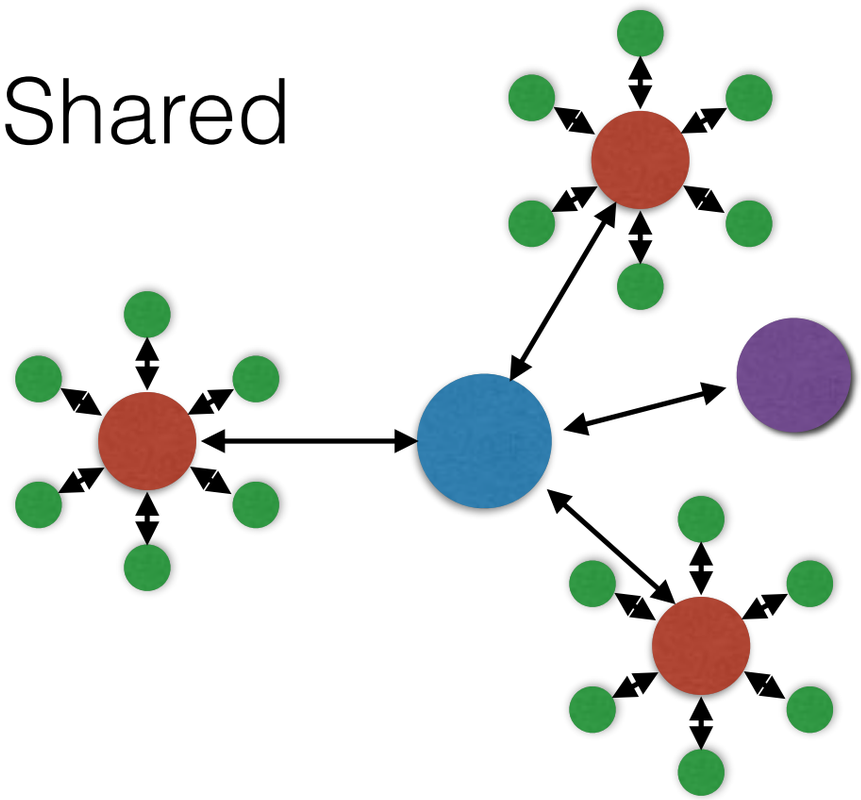
Separated



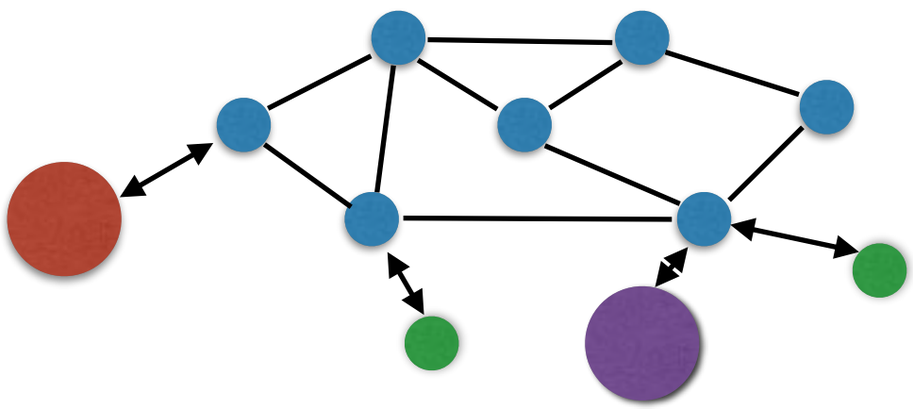
Federated



Shared



Distributed



Distributed

