National Digital ID

e-KYC / e-Consent / e-Identity / Easy of Doing Business / Doing Business Portal

มองจากคนภายนอก DIGITAL ID คืออะไร

มุมมอง User ที่ต้องการใช้บริการ

1.สามารถทำธุรกรรมต่างๆผ่านระบบ Online ได้ตลอด 24 ชม. ผ่านช่องทางอะไรก็ได้

2. ไม่ต้องเสียเวลากรอกใบสมัคร หรือเอกสารต่างๆ

3.ไม่ต้องมีเอกสารประกอบ เมื่อทำธุรกรรม (Full Version)

4.ใช้อะไรยืนยันตัวตนก็ได้ -> บัตรประชาชน หรือวิธีการยืนยันตัวตนของหน่วยงานที่เคยยืนยันตัวตนเรามาแล้ว

มุมมองของผู้ให้บริการ

1.สามารถทำธุรกรรมที่มีความสำคัญได้ผ่านช่องทาง Online ผ่านผู้ประกอบธุรกิจ Identity Provider (IdP) ยืนยันตัวตนให้

2.ยกระดับการทำธุรกรรมต่างๆ ให้มีความน่าเชื่อถือ และเหมาะสมกับประเภทธุรกรรมมากขึ้น

3.ได้รับข้อมูลจาก Trusted Source โดยตรง ซึ่งสามารถป้องกันการปลอมแปลงเอกสารได้

4.ธุรกรรมที่แต่เดิมต้องใช้ระยะเวลาพิจารณา 5-7 วัน สามารถรู้ผลการให้บริการได้ทันที

5.ต้นทุนการบริการอาจต่ำกว่า 10% ของต้นทุนการให้บริการแบบเดิม

มองจากคนทำงาน DIGITAL ID คืออะไร

1

สร้างมาตรฐานการพิสูจน์และการยืนยันตัวตนของประเทศไทย และยกระดับการทำธุรกรรมต่างๆ ให้มีความน่าเชื่อถือมากขึ้น

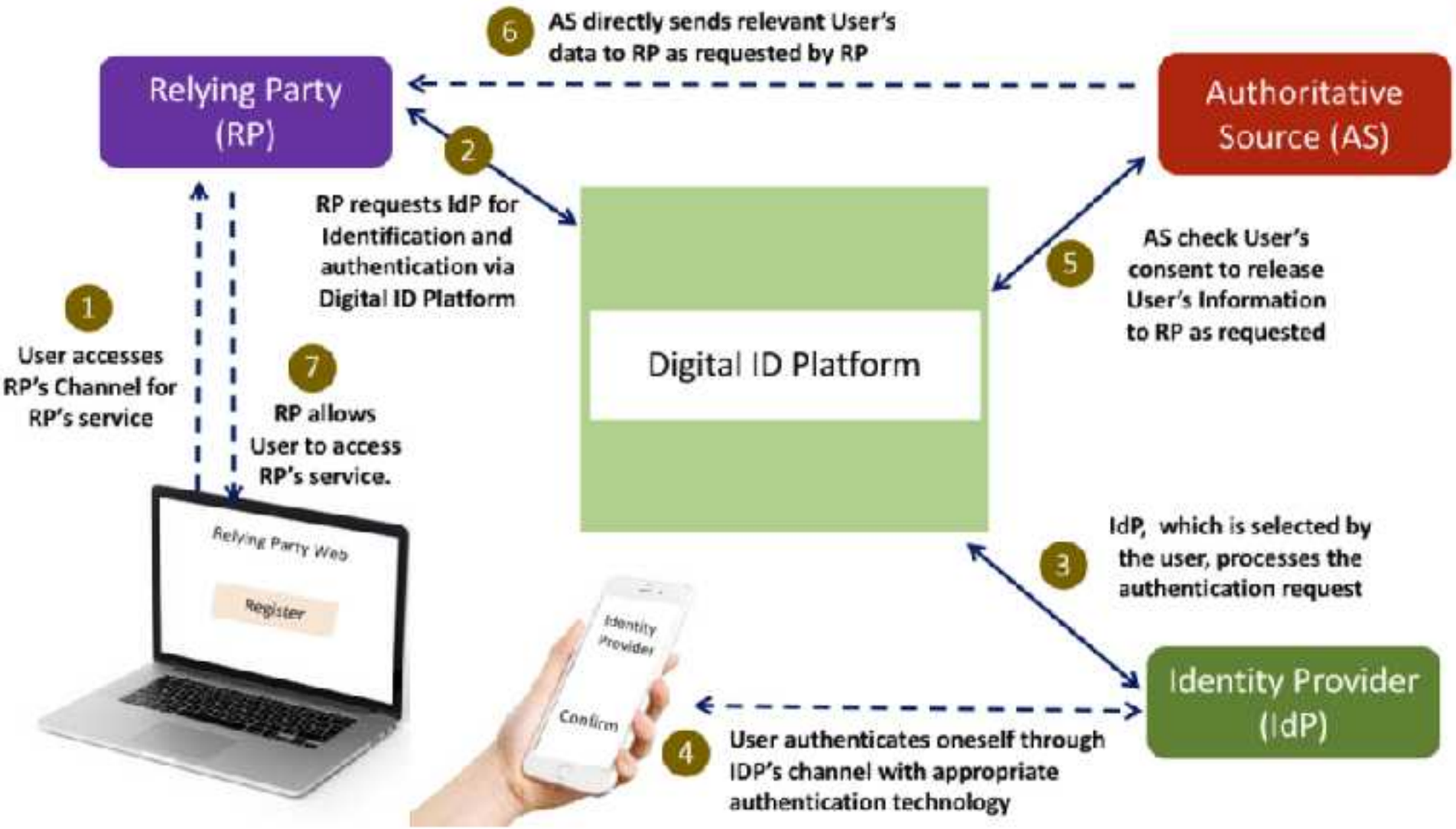
2

สามารถพิสูจน์และยืนยันตัวตนผ่านช่องทาง Online Self Service ได้

3

สร้างระบบ Data Sharing โดยเป็นเพียงถนนเพื่อเชื่อมต่อระหว่างหน่วยงานต่างๆ (ไม่มีการรวมศูนย์เก็บข้อมูล) และการ Share ต้องได้รับการ Consent จากเจ้าของข้อมูลก่อน

กระบวนการยืนยันตัวตน และขอข้อมูลผ่านระบบ National Digital ID



จุดสำคัญของ Model

1.แบ่งหน่วยงานตาม Role ไม่ใช่ตามหน่วยงาน ซึ่งหน่วยงานหนึ่ง อาจมีมากกว่า 1 Role

2.การยืนยันตัวตนใช้เทคโนโลยีอะไรก็ได้ แต่ต้องทำผ่านช่องทาง IdP เท่านั้น

3.ภายใน Platform เป็น Distributed Ledger ทำให้ไม่มีการเก็บข้อมูลที่ใดที่หนึ่ง ซึ่งจะปลอดภัยกว่า

4.AS จะส่งข้อมูลตรงไปยัง RP โดยไม่ผ่าน Platform แค่เข้ามาตรวจสอบ Consent บน Platform เท่านั้น

Version 020518

Authenticator ที่ออกจากการทำ IAL แบบ Face2Face และ KIOSK สามารถนำไปเป็นใช้เป็น Authenticator (AAL) บนระบบ NDID เพื่อไปสมัครใช้บริการกับ RP อื่นได้

Digital ID

Identity Assurance Level (IAL)

Face2Face

Non F2F - Kiosk

IAL3 (เอกสาร 2 ชิ้น+ เก็บ Biometric)

Dip Chip Online to DOPA And  ดึงข้อมูลจาก Passport + Digital Signature + 

F2F: ถ่ายรูปเก็บ (ตามมาตรฐาน)
KIOSK: ถ่ายรูป (ตามมาตรฐาน)

+  Biometric Comparison อย่างน้อย 1 อย่าง +  ใช้ Finger Print (Optional)  VDO Call (Required For KIOSK)

IAL2 (เอกสารจริงปลอมแปลงไม่ได้ 1 ชิ้น) (Identification + Verification)

IAL 2.3 (เทียบ Bio ด้วยระบบ)

Dip Chip Online to DOPA or  ดึงข้อมูลจาก Passport + Digital Signature + 

F2F: ถ่ายรูปเก็บ
KIOSK: ถ่ายรูป – Liveness

+  Biometric Comparison อย่างน้อย 1 อย่าง +  ใช้ Finger Print (Optional)  VDO Call (Optional For KIOSK)

IAL 2.2 (Dip Chip Online)

Dip Chip Online to DOPA or  ดึงข้อมูลจาก Passport + Digital Signature + 

ผ่าน F2F: ถ่ายรูปเก็บ
ผ่าน KIOSK: ถ่ายรูปเก็บ + Liveness

+  ใช้ Finger Print (Optional)  VDO Call (Optional For KIOSK)

IAL 2.1 (Dip Chip Offline)

Dip Chip (Offline) or  ดึงข้อมูลจาก Passport + 

ผ่าน KIOSK: ถ่ายรูปเก็บ
ผ่าน F2F: Optional

IAL1 (Identification)

IAL 1.3 (แสดงบัตรตัวจริง)

แสดงบัตรประชาชน และ ถ่ายสำเนาบัตรเก็บไว้ + Verify โดยเจ้าหน้าที่

 เครื่อง SCAN บัตรประชาชน  ถ่ายรูปเก็บ (Optional) Verify โดยเจ้าหน้าที่

IAL 1.2 (สำเนาบัตรประชาชน)

ถ่ายสำเนาบัตรมา (ไม่มีการแสดงบัตรตัวจริง) + Verify โดยเจ้าหน้าที่

  Upload รูปบัตรประชาชนจาก Cloud หรือระบบอื่นๆ  ถ่ายรูปเก็บ (Optional)

IAL 1.1 (ไม่มีเอกสารเลย)

ไม่มีหลักฐานอะไรเลย เชื่อตามที่ลูกค้าแจ้งมาทั้งหมด

ไม่มีหลักฐานอะไรเลย เชื่อตามที่ลูกค้าแจ้งมาทั้งหมด  ถ่ายรูปเก็บ (Optional)

หมายเหตุ: โปรดอ่านรายละเอียด ฉบับเต็มใน www.digitalid.or.th ประกอบ

Version 280418

AAL อ้างอิงตามมาตรฐานของ NIST แต่เนื่องจาก AAL3 ในประเทศไทย ยังไม่มีอุปกรณ์ประเภท Crytographic Device แพร่หลาย จึงเพิ่มความน่าเชื่อถือของ AAL 2 เป็น 2 ระดับย่อย

AAL3

Something you have (Strong - cryptographic device) + Something you know (Encrypt) + Something you have (Regular) + Something you are

Two Factors with Hardware Authenticator
(ใช้อะไรคู่อะไรก็ได้ ขอให้มี Sth u have (Strong)

Example

บัตร Chip Card (Dip Chip)

+  ใช้ User&Pass หรือ Pin Code

*Note: Sth u have (Strong) - Online
ยังไม่มีใช้แพร่หลายในประเทศไทย

AAL2

AAL2.2 (3 Factors): Something you have (Regular) + Something you know (Encrypt) + Something you are

+ Factor ที่สามารถป้องกัน Replay Attack ได้

Example

 OR

ใช้เบอร์ที่ลงทะเบียน Login ผ่านซิม หรือเครื่องที่เคย Login

+  ใช้ User&Pass หรือ Pin Code

+  Face Recognition

ยังไม่ได้ข้อสรุป ยังอยู่ระหว่างการหารือ

AAL2.1 (2 Factors): Something you have (Regular) + Something you know (Encrypt)

+ Factor ที่สามารถป้องกัน Replay Attack ได้

Example

 OR 

ใช้เบอร์ที่ลงทะเบียน Login ผ่านซิม หรือเครื่องที่เคย Login

+  ใช้ User&Pass หรือ Pin Code

AAL1

Something you know | Something you have (Regular) | Something you are | Something you have (Strong - cryptographic device)

Single Factor Authentication

Example

 เครื่องที่ลงทะเบียน

OR

 ใช้ Username & Password

OR  ใช้ SMS OTP

OR  ใช้ Pin Code

หมายเหตุ: โปรดอ่านรายละเอียด ฉบับเต็มใน www.digitalid.or.th ประกอบด้วย

Version 280418

Authenticator ที่ออกจากการ Register แบบ Non-Face2Face
ในระยะทดลองยังไม่สามารถไปสมัครใช้บริการกับ RP อื่นได้

Digital ID FOR ALL

Non-Face2Face on Customer's Device (Limited IAL)

Non F2F – Citizen ID

Non F2F – Passport

LIAL3

✗

✗

LIAL2 (ใช้ IdP ช่วยยืนยัน)

LIAL 2.3 (มีการใช้ Biometric เข้าช่วย)


ถ่ายรูป + DOPA 5 Fields


Selfie

+

(2nd IdP (IAL2.3,AAL2.2+)
เทียบ Biometric บนช่อง IdP

or


2nd IdP (IAL2.2,AAL2.1+)
AS ต้องส่งรูปมาให้ RP เทียบ Biometric เอง)


NFC ดึงข้อมูล

+


Selfie

+


Biometric Comparison

LIAL 2.2


ถ่ายรูป + DOPA 5 Fields


Selfie

+

2nd IdP (IAL2.2+,AAL2.1+)
Authen 2 Factors

PIAL 2.1 & 2.2 จะให้ 2nd Tier IdP มาช่วยยืนยัน แต่จุดต่าง คือ PIAL2.1 - 2nd Tier IdP จะผ่าน IAL 2.1 / ส่วน PIAL 2.2 จะผ่าน IAL 2.2 มาแล้ว

NFC ดึงข้อมูล

+


Selfie

LIAL 2.1


ถ่ายรูป + DOPA 5 Fields


Selfie

+

2nd IdP (IAL 2.1+,AAL2.1+)
Authen 2 Factors

PIAL 2.2: หน่วยงานต้องมาตรวจสอบโดยเจ้าหน้าที่ก่อนอนุมัติให้บริการ
PIAL 2.3: ถ้าผลการเปรียบเทียบ ต่ำกว่าเกณฑ์ ให้หา Risk Mitigation เข้าช่วย เช่น Penny Test หรือหา Authenticator อื่นมาเสริม

หมายเหตุ: กรณี User มี Card Reader ยังไม่อนุญาตให้ทำธุรกรรมได้เอง

LIAL1 (ใช้บัตรประชาชนได้)

LIAL 1.3

ถ่ายรูปจากบัตรตัวจริงด้วยเทคโนโลยีที่กำหนด เช่น OCR

เทียบเท่าแสดงบัตรตัวจริง

LIAL 1.2

Upload รูปจาก Gallery

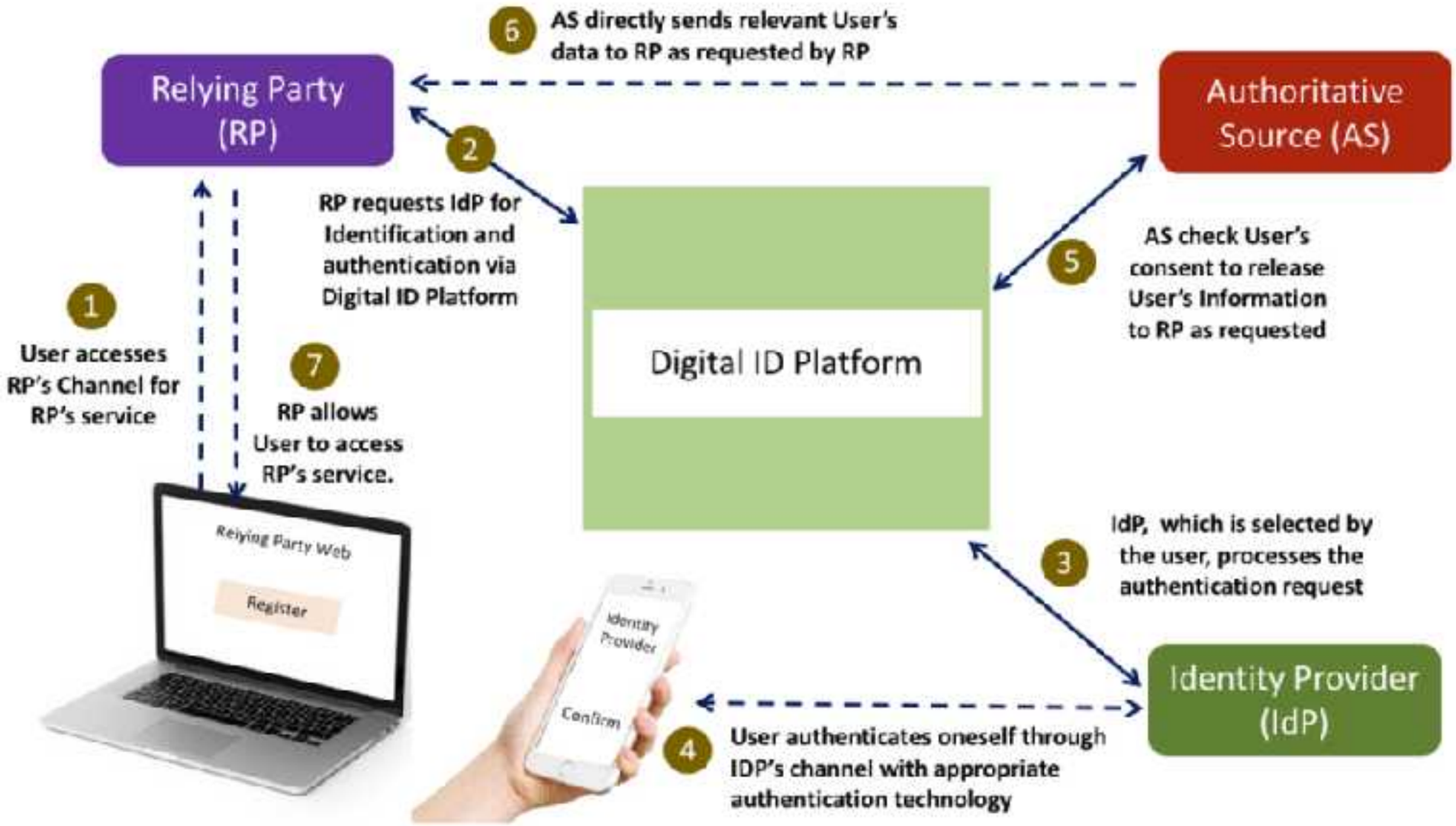
เทียบเท่าสำเนาบัตร

LIAL 1.1

ไม่มีการส่งเอกสารทางราชการ (อาจใช้ FB, SMS/Email OTP หรือให้ลูกค้ากรอกข้อมูลเอง)

หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

กระบวนการยืนยันตัวตน และขอข้อมูลผ่านระบบ National Digital ID



จุดสำคัญของ Model

1.แบ่งหน่วยงานตาม Role ไม่ใช่ตามหน่วยงาน ซึ่งหน่วยงานหนึ่ง อาจมีมากกว่า 1 Role

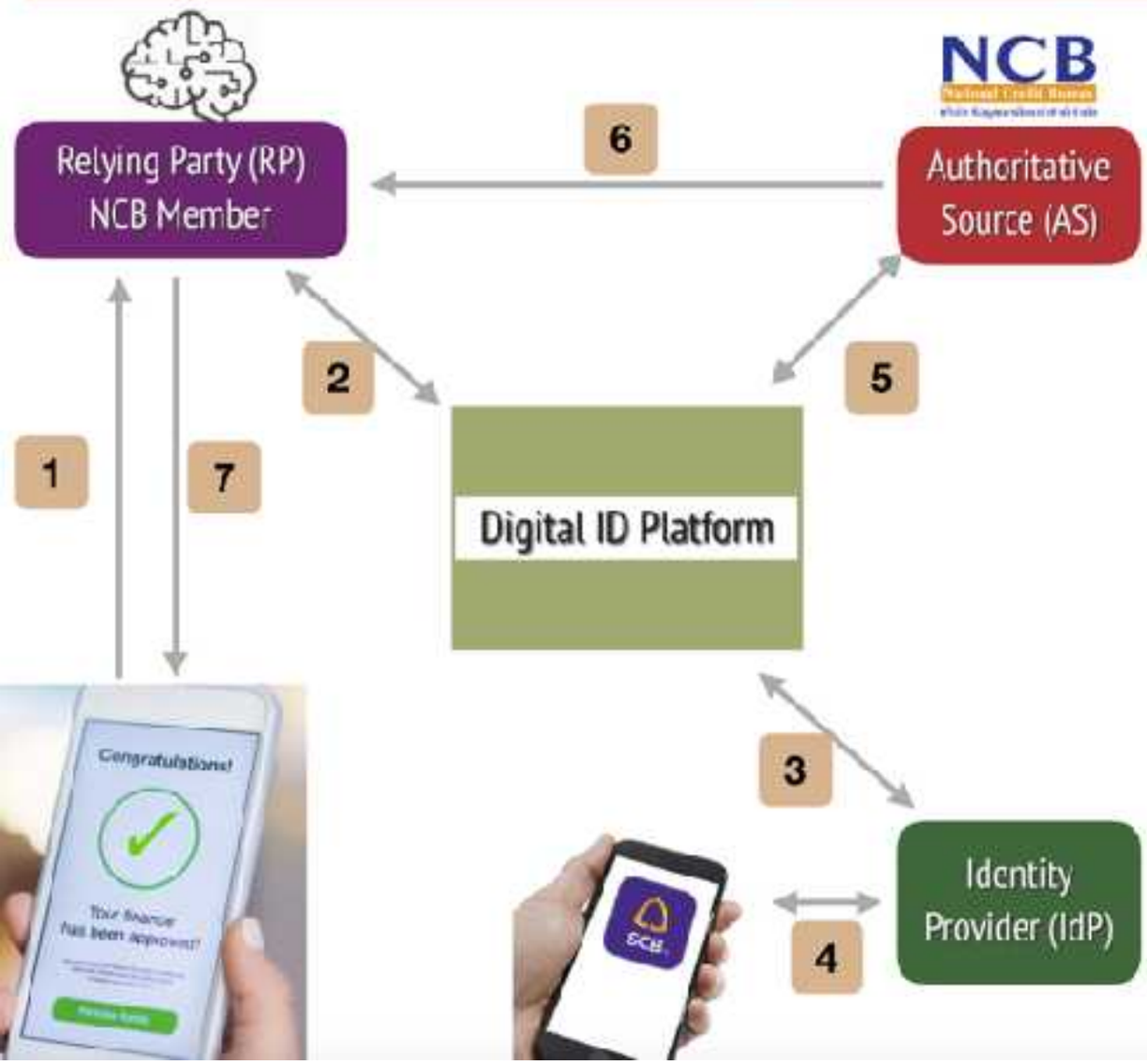
2.การยืนยันตัวตนใช้เทคโนโลยีอะไรก็ได้ แต่ต้องทำผ่านช่องทาง IdP เท่านั้น

3.ภายใน Platform เป็น Distributed Ledger ทำให้ไม่มีการเก็บข้อมูลที่ใดที่หนึ่ง ซึ่งจะปลอดภัยกว่า

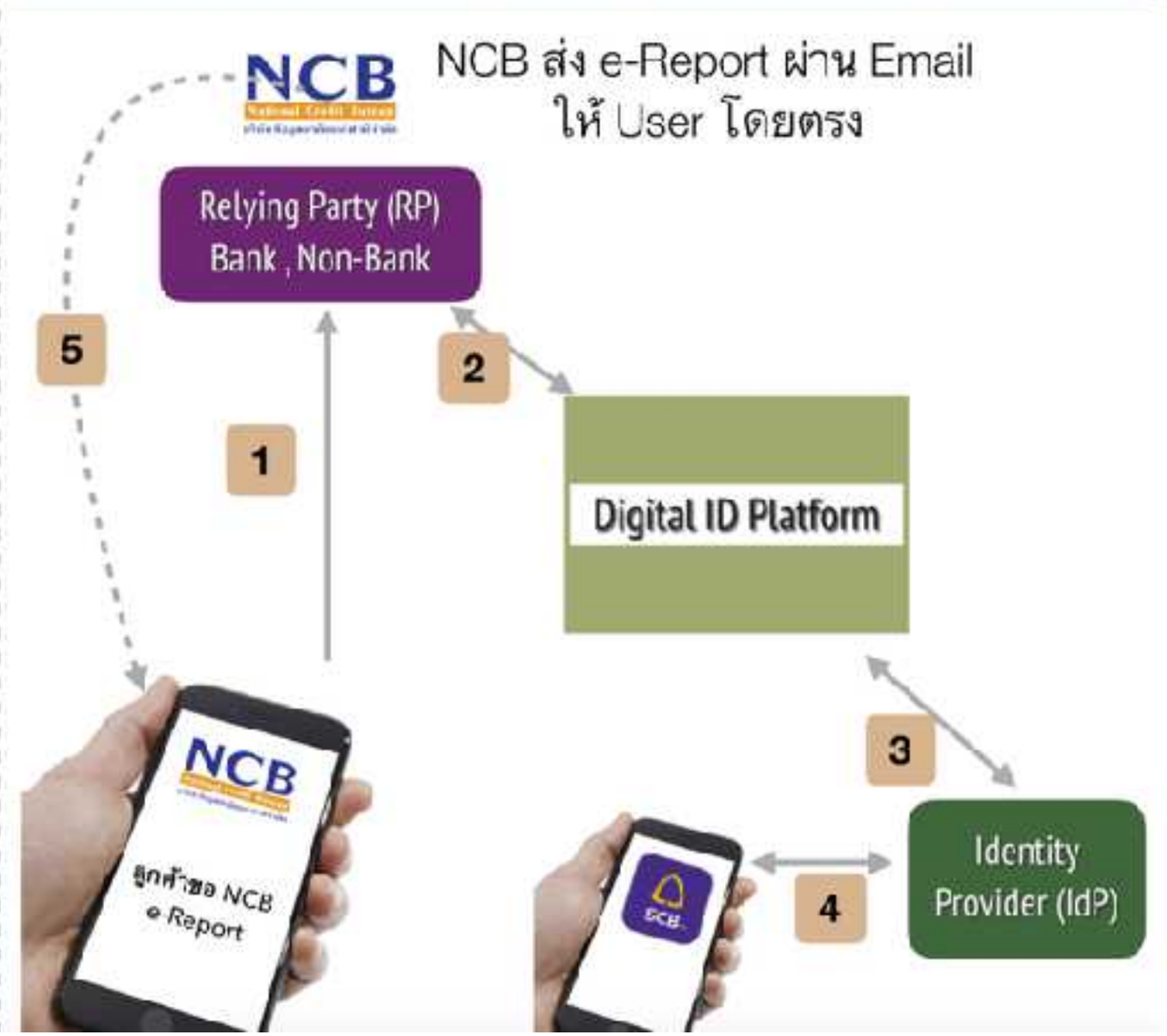
4.AS จะส่งข้อมูลตรงไปยัง RP โดยไม่ผ่าน Platform แค่เข้ามาตรวจสอบ Consent บน Platform เท่านั้น

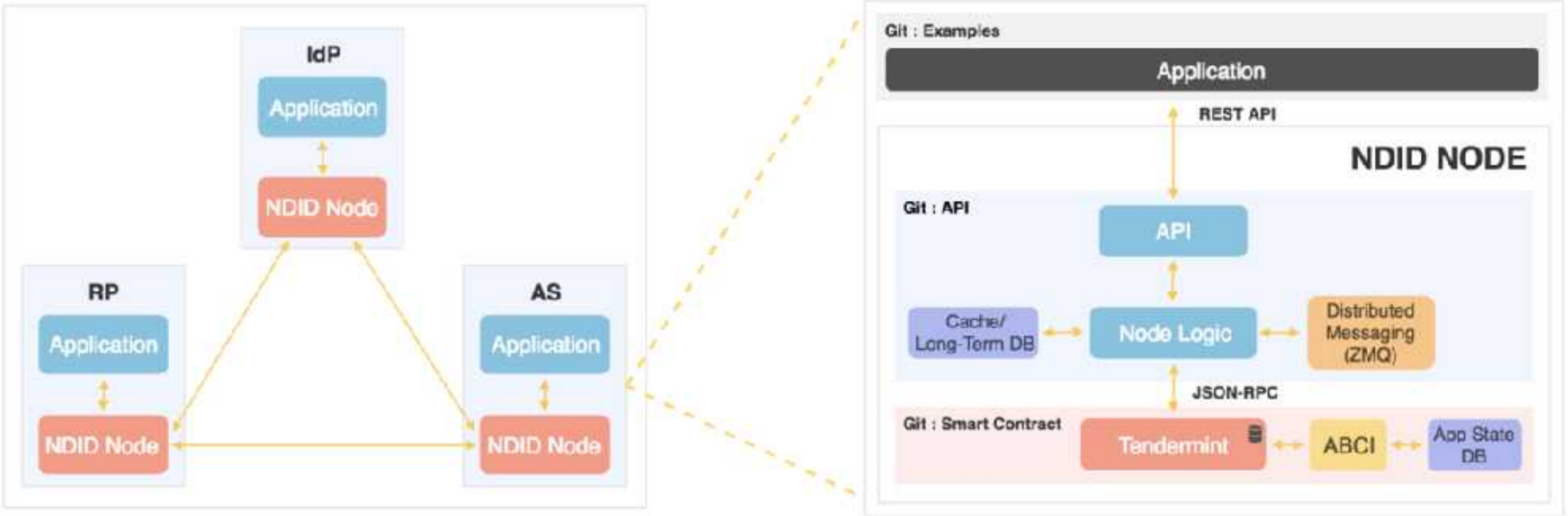
#1 NCB Business Case ที่ผ่าน Digital ID มี 2 Solutions:

NCB e-Consent for Digital Lending



NCB e-Report (NCB ส่งตรง)




IdP
Application
NDID Node
RP
Application
NDID Node
AS
Application
NDID Node
Git : Examples
Application
REST API
NDID NODE
Git : API
API
Cache/
Long-Term DB
Node Logic
Distributed
Messaging
(ZMQ)
JSON-RPC
Git : Smart Contract
Tendermint
ABCI
App State
DB

Git : Examples

Application

REST API

NDID NODE

Git : API

API

Cache/Long-Term DB

Node Logic

Distributed Messaging (ZMQ)

JSON-RPC

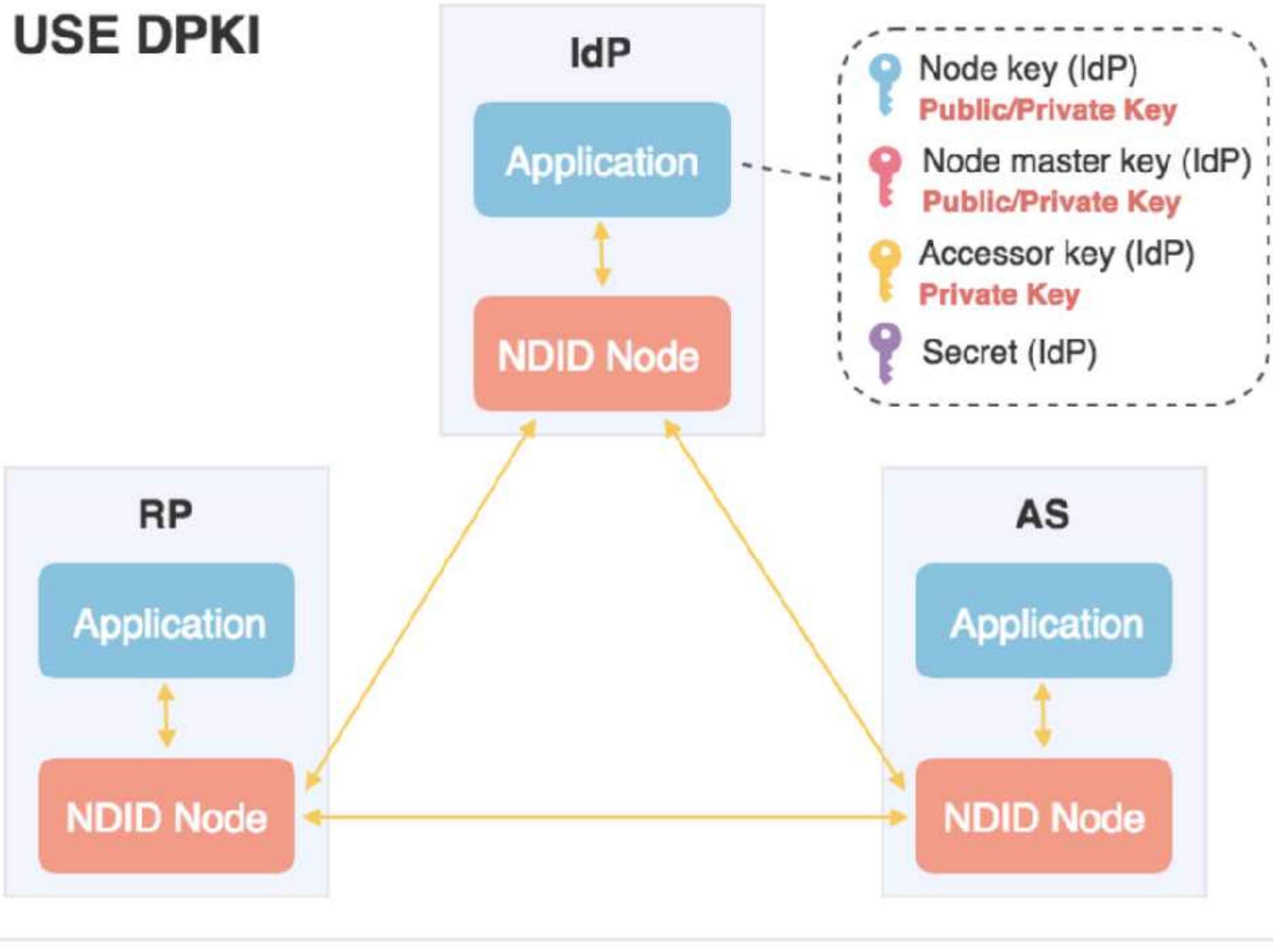
Git : Smart Contract

Tendermint

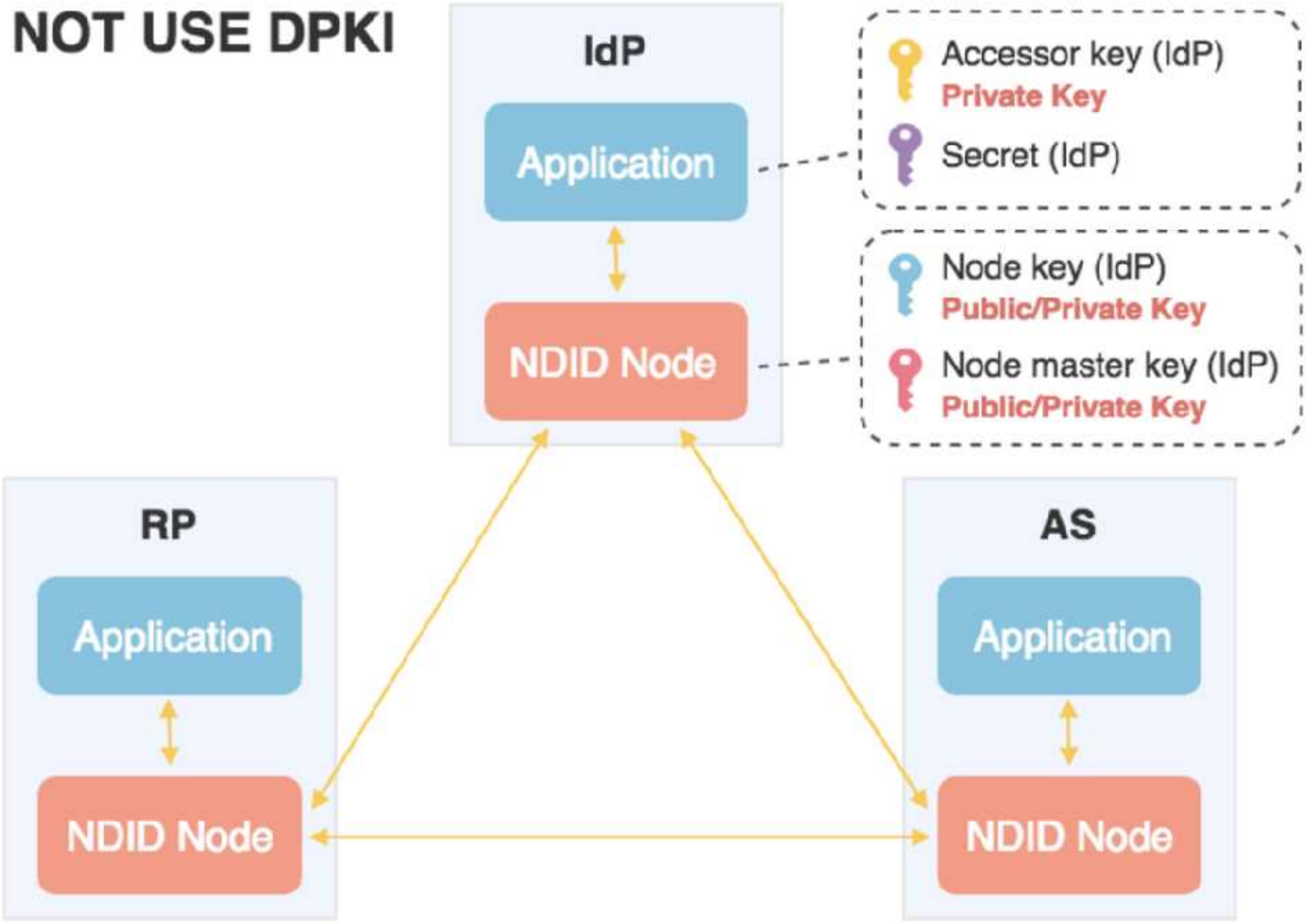
ABCI

App State DB

USE DPKI


IdP
Application
NDID Node
Node key (IdP)
Public/Private Key
Node master key (IdP)
Public/Private Key
Accessor key (IdP)
Private Key
Secret (IdP)
RP
Application
NDID Node
AS
Application
NDID Node

NOT USE DPKI


IdP
Application
NDID Node
Accessor key (IdP)
Private Key
Secret (IdP)
Node key (IdP)
Public/Private Key
Node master key (IdP)
Public/Private Key
RP
Application
NDID Node
AS
Application
NDID Node

System Properties

- Blockchain and distributed messaging.
- Decentralized.
- Distributed.
- No single point of failure.
- No single point of attacking.
- Not control by any single party.

Security

- Confidentiality Integrity
- Privacy
- Abuse Prevention

Confidentiality

- Data transmission is encrypted.
- Only intended party can decrypt data.
- Logs do not contain sensitive data.

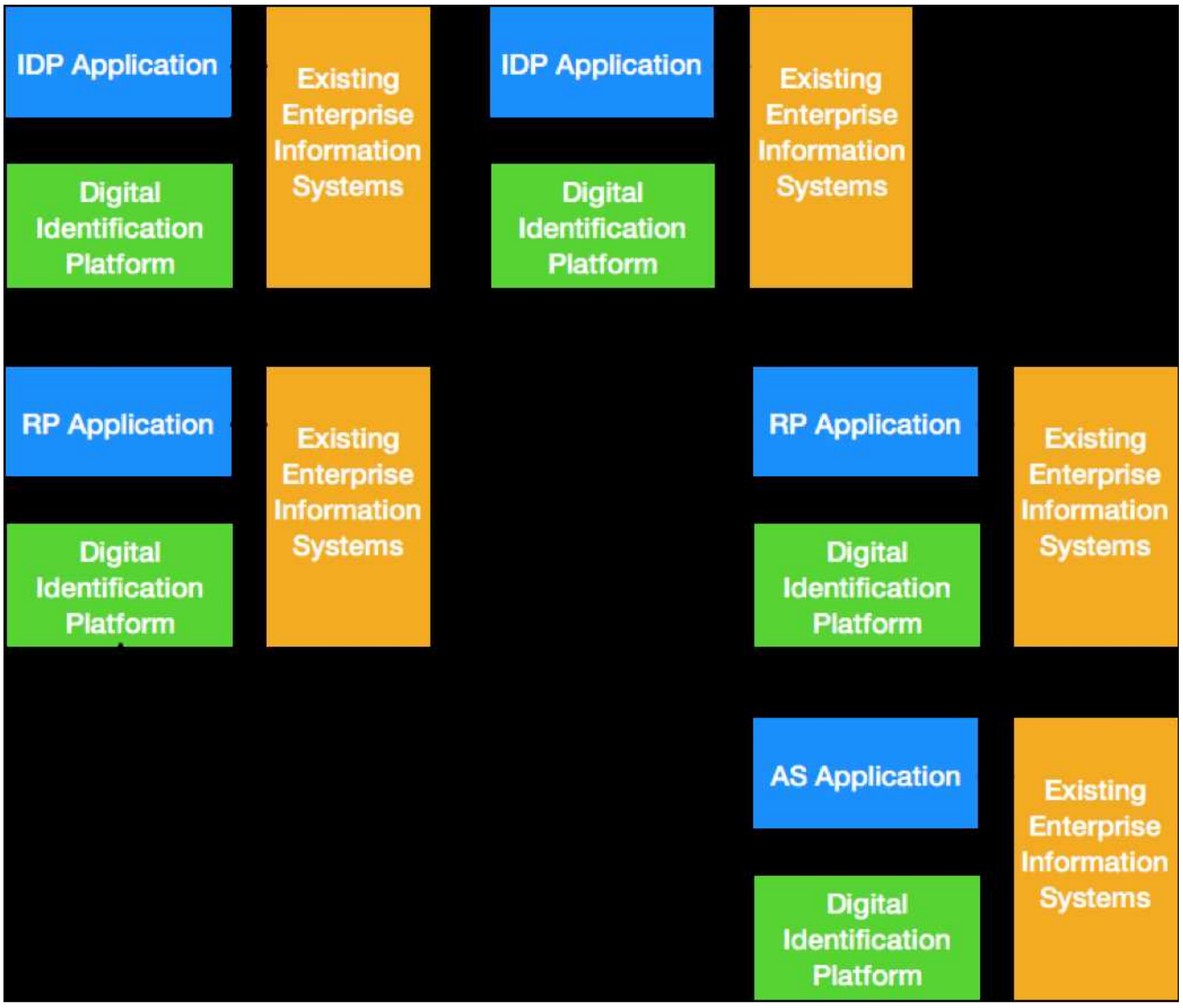
Integrity

- Data transmitted are delivered properly.
- Data stored cannot be tampered.
- Data transmission cannot be tampered.

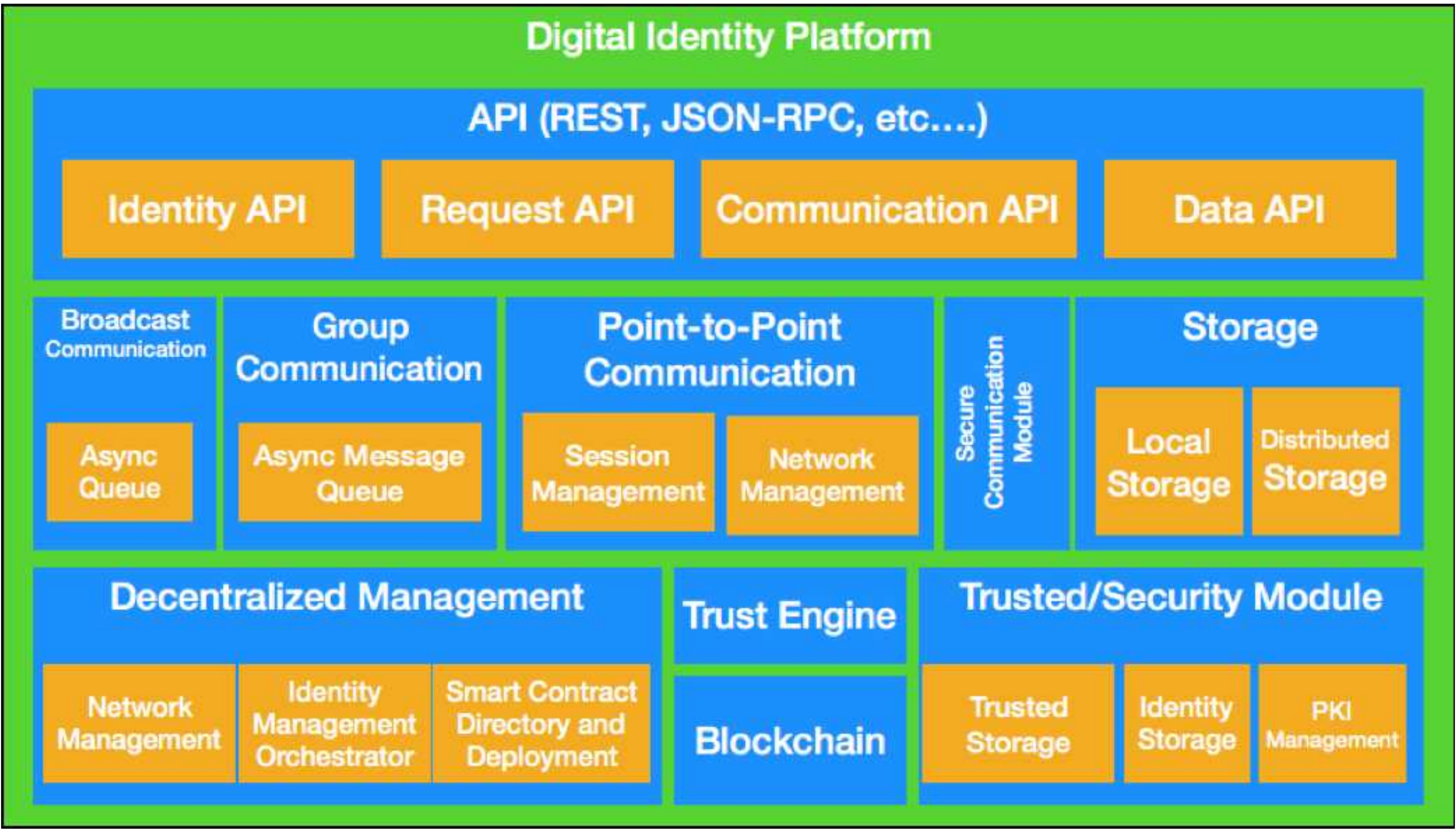
Privacy

- Platform does not store personal information.
- Messages and Requests in the platform may hide source, destination, and/or content from other parties in the ecosystem (minimum 2 out of 3)
- Anonymity: RP, IDP and/or User may hide their identity.
- Anonymized data stored in the platform is resistant to brute force.

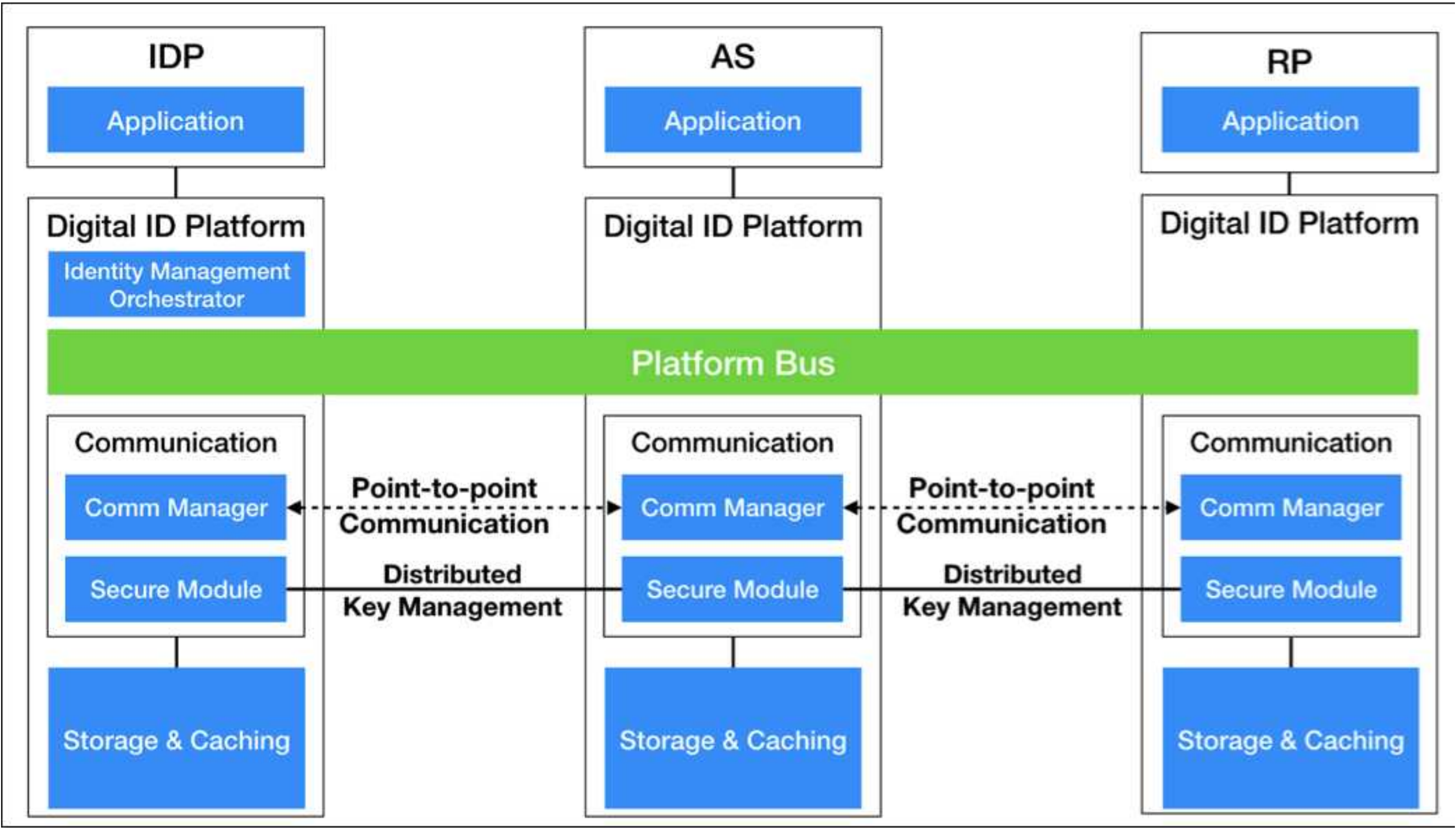
Architecture Design



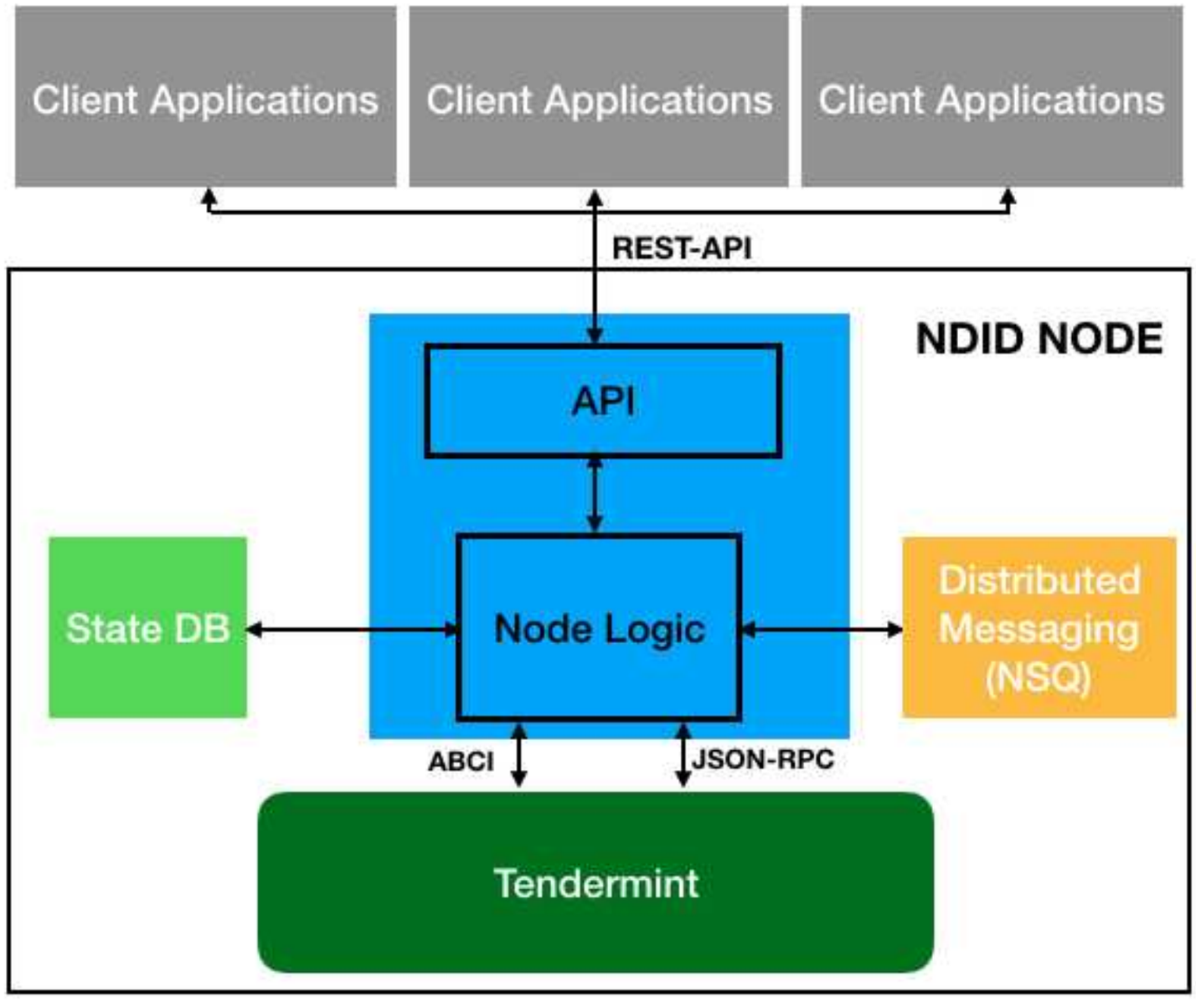
Platform Node Components



Communication Between Nodes



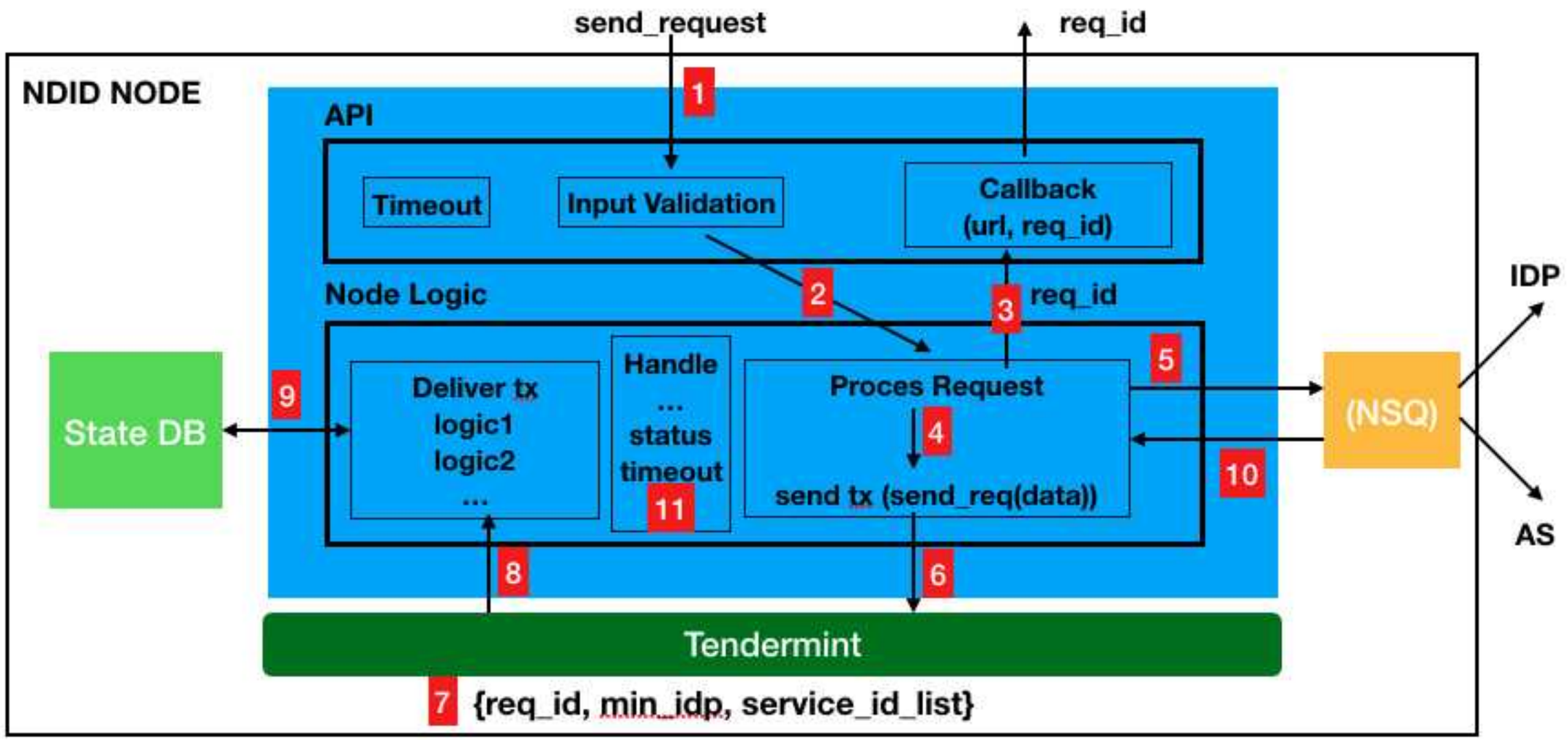
Example NDID Node



Example Request

Send request to {namespace}/{identifier} (async)

{ns, id, request_type, request_message, min_ial, min_aal, min_idp, service_id_list, timeout}



https://ndidplatform.github.io

Secure https://ndidplatform.github.io

NDID platform

Development hub for Thailand National Digital ID platform.

Title	URL
Official site	http://www.digitalid.or.th/
TEDxChiangMai Talk	https://www.youtube.com/watch?v=E8HHNRRIsoo
GitHub organization	https://github.com/ndidplatform
HTTP API schema	https://app.swaggerhub.com/apis/NDID/
Facebook page	https://www.facebook.com/NationalDigitalID/
Whitepaper	https://goo.gl/v4Cfpe
Slack	https://bit.ly/2LMD5W8

Architecture overview

Recommended reading: For newcomers, we highly recommend that you watch the TEDxChiangMai talk which describes the importance and benefits of having a digital ID infrastructure in Thailand, and read the Digital Identity Guideline for Thailand – Overview and Glossary (DRAFT) document to understand the overall process of the Digital ID model.

From the whitepaper:

Useful Links

- https://ndidplatform.github.io/
- https://github.com/ndidplatform
- https://app.swaggerhub.com/search?type=API&owner=NDID