National Digital ID

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

Recap: วัตถุประสงค์ของโครงการ National Digital ID

1

สร้างมาตรฐานการพิสูจน์และการยืนยันตัวตนของประเทศไทย และยกระดับการทำธุรกรรมต่างๆ ให้มีความน่าเชื่อถือมากขึ้น

2

สามารถพิสูจน์และยืนยันตัวตนผ่านช่องทาง Online Self Service ได้

3

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

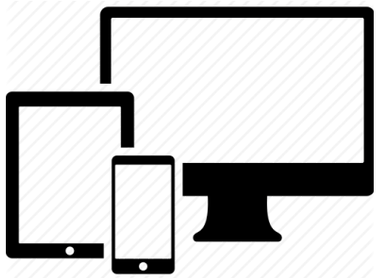
Recap: การยืนยันตัวตนผ่าน Channel and Authentication Method อะไรก็ได้

Face 2 Face

KIOSK

Chat

Call Center



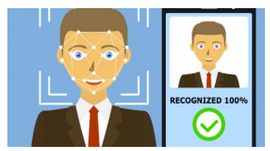
Customer Device

User

ไม่ต้องกรอกเอกสาร และมีเอกสารประกอบ (Full Version)

Citizen ID

Passport

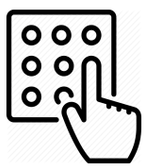


Face Recoanition

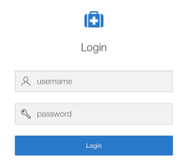
Finger

Mobile / SMS

Card

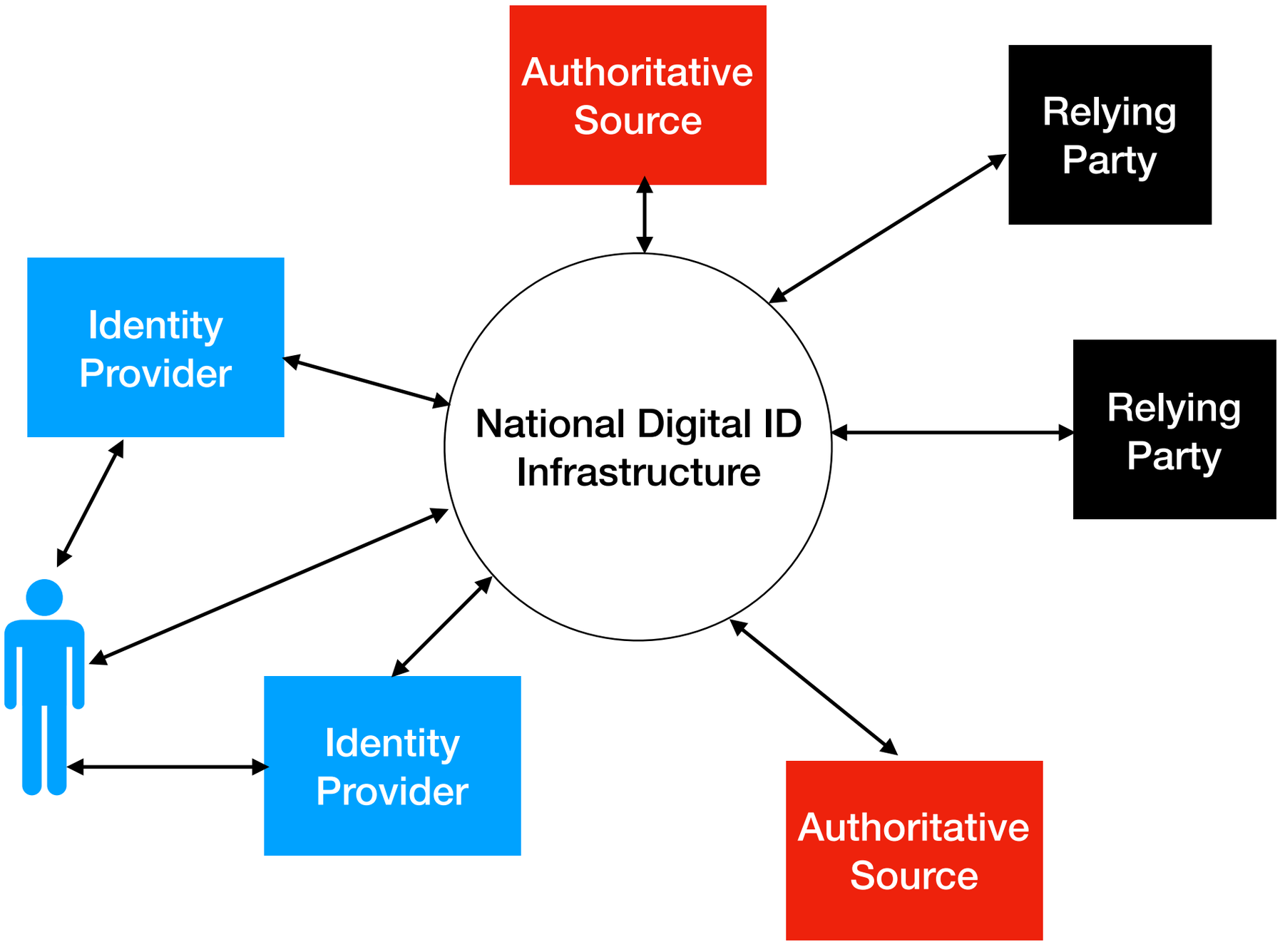


Pin Code



User/ Password

Infrastructure



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.

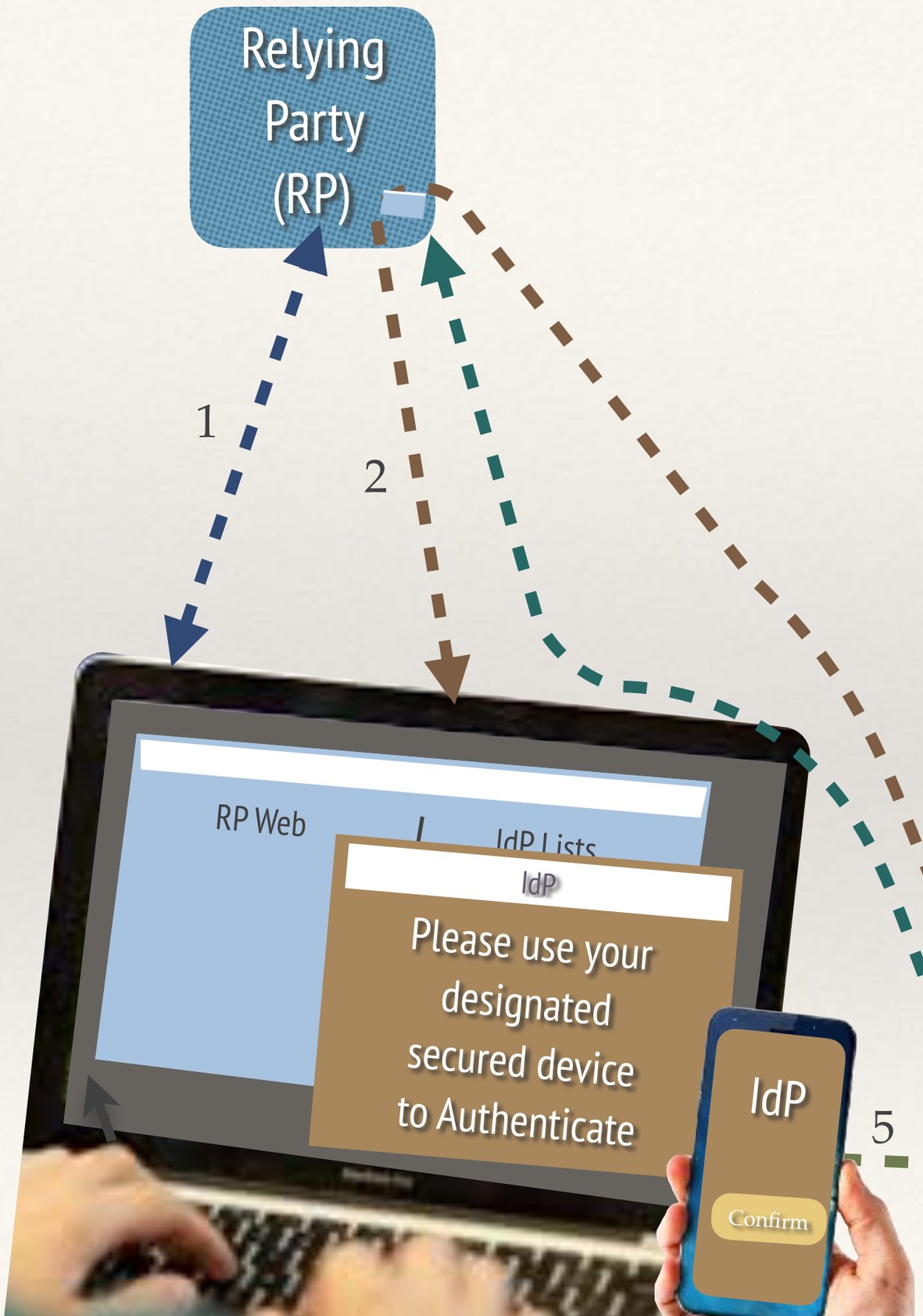
Integrity

- 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.

Authentication Flow : Cross Channel

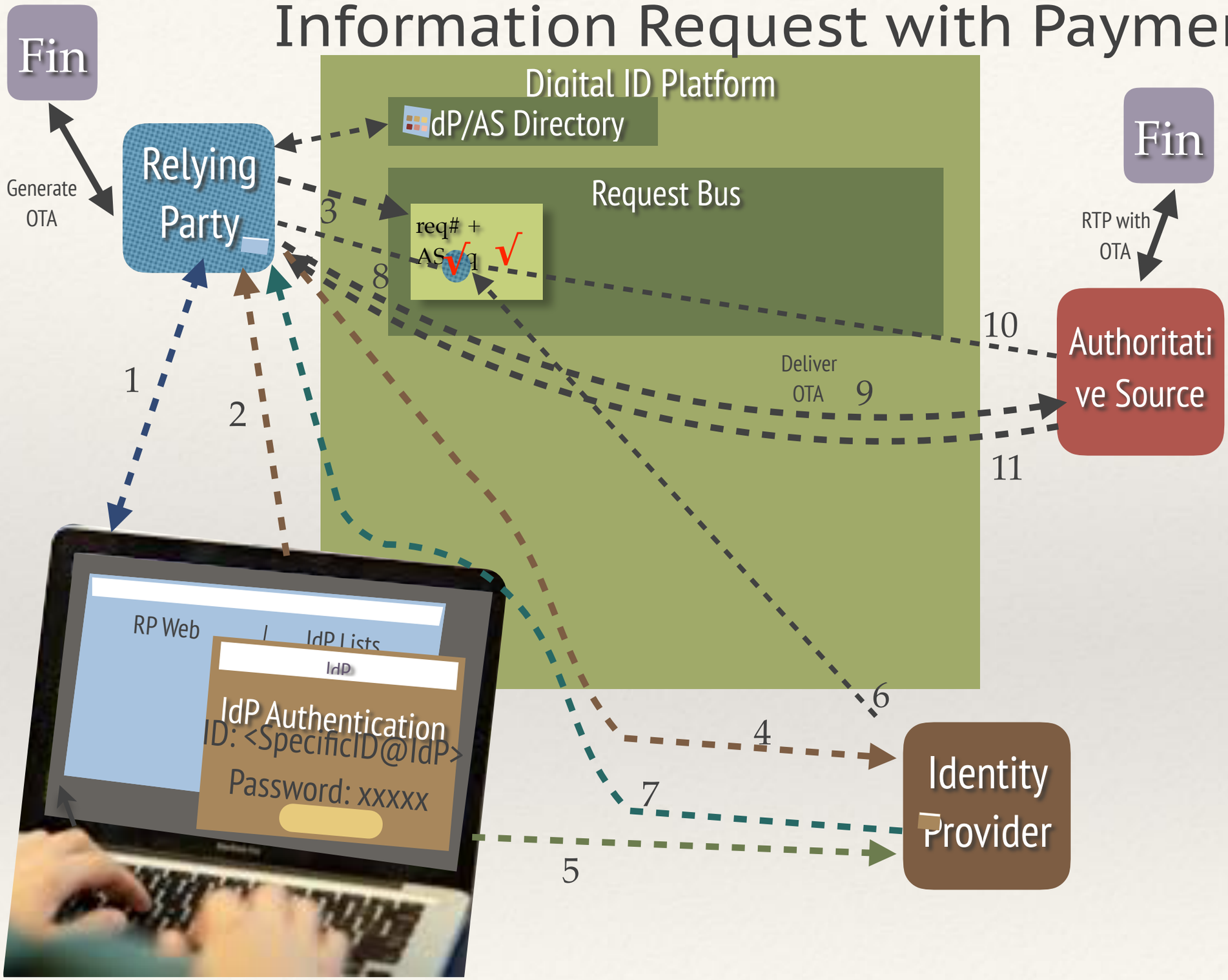


Channels and (applicable) Authentication Methods (AM) may vary from one IdP's to another, giving the variety and choice of preference to consumers. Technology choice is flexible with possibility for new innovative technology, e.g. biometrics, mobile PKI, etc.

Regulating Body (e.g. EDTA) may specify the standard of each Authentication Method (AM) and specify the "level of assurance" of each AM .

IdP determines that the user was enrolled or required to use another channel

Information Request with Payment



ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

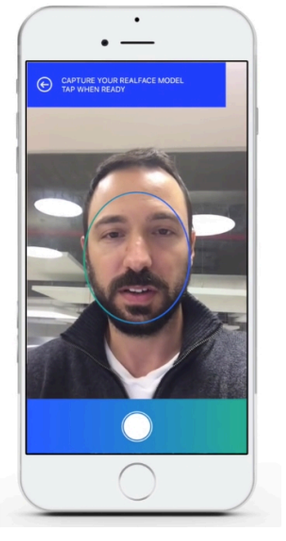
1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อตกลงและเปิดเผยข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ

กำหนด PIAL 2.1

เลือก Selling Agent เพื่อเปิดบัญชี

ยอมรับ Term and Conditions เพื่อเป็น เปิดเผยข้อมูล

กรอกข้อมูลตามบัตรประชาชน(ตรวจสอบ 5 Fields กับกรมการปกครอง) และถ่ายรูปบัตรประชาชน



ตรวจสอบความถูกต้องกับกรมการปกครอง (ถ้าระบบล่ม จะทำยังไง?)

หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อตกลงและเปิดเผยข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ

Direct Debit

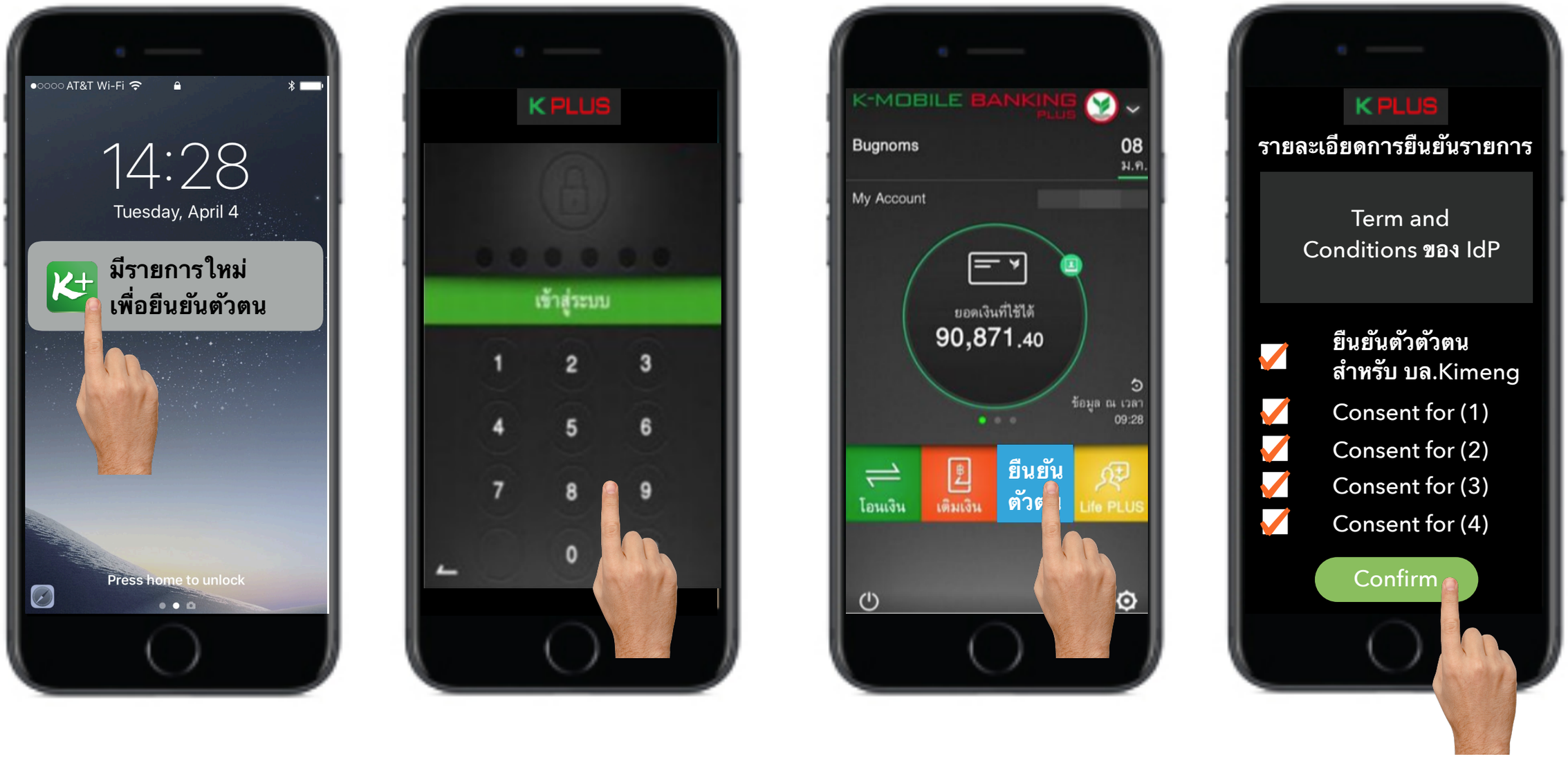
ถูก Auto Fill จากข้อมูลตอนกรอกบัตรประชาชน (ห้ามแก้)

เลือก IdP

หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อตกลงและเปิดเผยข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ



หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อตกลงและเปิดเผยข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ

ยืนยันตัวตนตามระดับ AAL 2.1

AIS dtac truemove H

Something you have (Regular)

ต้อง Login ด้วยเบอร์โทร หรือเครื่องมือถือที่เคยลงทะเบียนเอาไว้

+

Something you know (Encrypt)

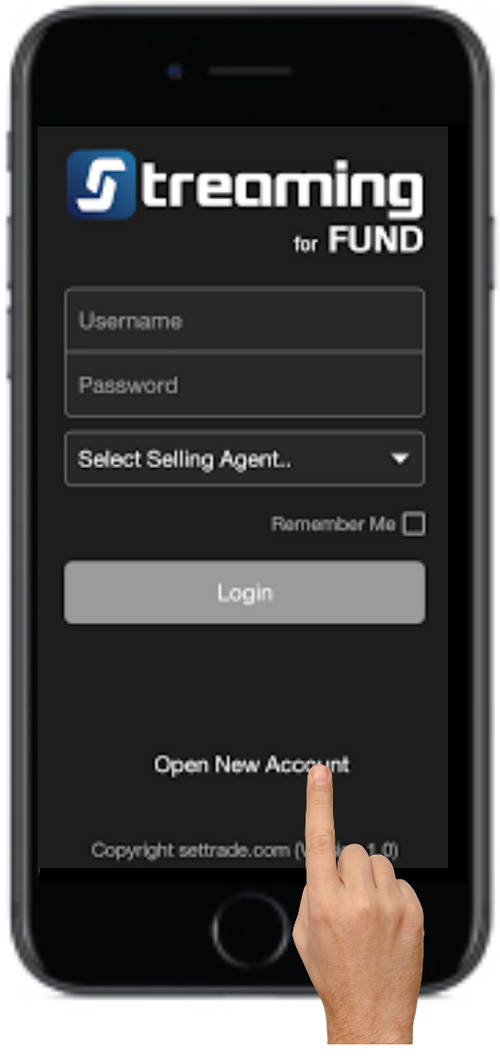
Pin Code ที่ลงทะเบียนกับ IdP

หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อตกลงและเปิดเผยข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ

กลับมาที่ Streaming for Fund



ทำ Asynchronous โดย SET ทำการเก็บ Device No. ของ User ไว้ และเมื่อกลับมาสามารถ ทำรายการต่อได้ทันที

ข้อมูลแบ่งเป็น 3 ส่วน ที่ถูกกรอกข้อมูลในใบสมัคร (ถ้ามี AS เพิ่มขึ้นลูกค้าก็กรอกใบสมัครน้อยลง)

1.ข้อมูลที่มาจาก AS

ไม่มี AS เลย ในระบบ

2.ข้อมูลที่ลูกค้ากรอกเอง

ตามใบสมัครมาตรฐาน

3.เอกสาร (e-Documents)

ตามเอกสารทั่วไปที่ทาง บริษัทหลักทรัพย์ต้องการ

หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

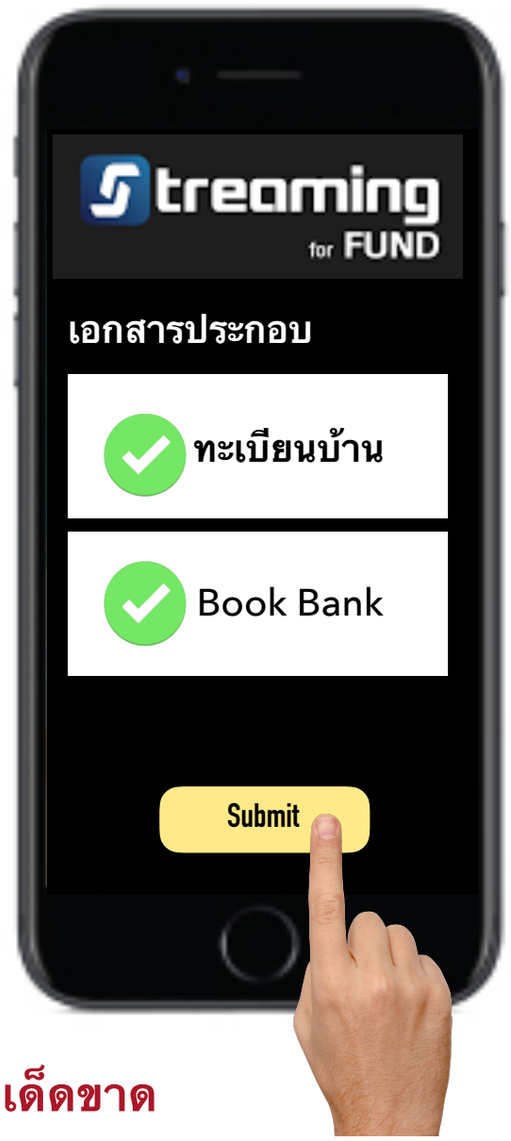
ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อตกลงและเปิดเผยข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ

ถ้าไม่มี AS ลูกค้าก็ทำหน้าที่ถ่ายเอกสาร ตามมาตรฐาน (e-Documents)

ถ่ายรูป ทะเบียนบ้าน

ถ่ายรูป *Book Bank*



หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อ[illegible]ลงและเปิดใช้ข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ

ยืนยันการสมัคร (ทุกอย่างครบ)

1. Citizen ID
2. ชื่อ - นามสกุล
3. วันเกิด
4. เพศ
5. สัญชาติ
6. สถานะสมรส
7. เบอร์ลงทะเบียน
8. เบอร์ติดต่อ
9. Email
10. ข้อมูลคู่สมรส
11. ข้อมูลบุตร
12. ที่อยู่ทะเบียนบ้าน
13. ที่อยู่ที่ติดต่อได้
14. ที่อยู่ที่ทำงาน
15. อาชีพ

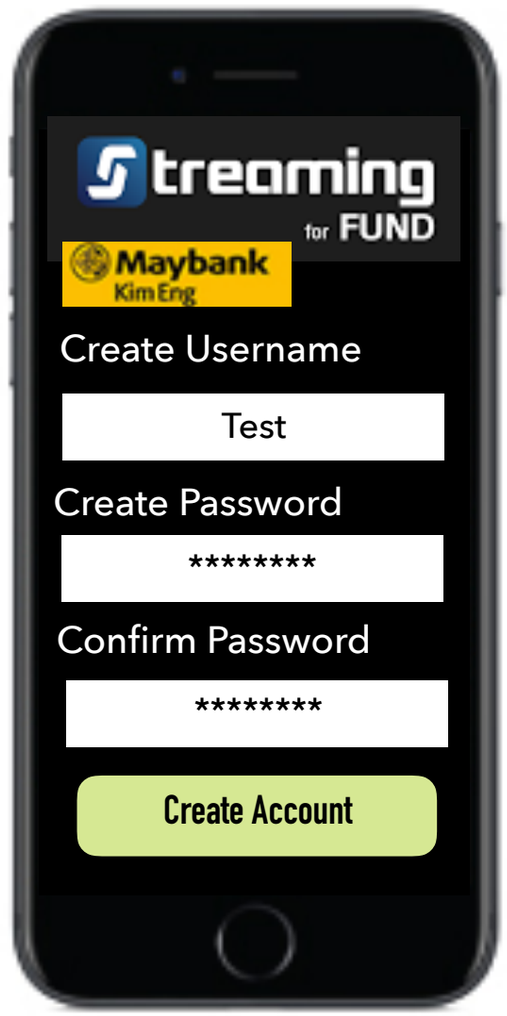
ยืนยันการสมัคร (ทุกอย่างครบ)

16. ประเภทธุรกิจ
17. แหล่งที่มารายได้
18. รายได้
19. ประเมินความเสี่ยง

Term and Conditions การสมัครใช้บริการ

ยืนยันการสมัคร

สร้าง Account



หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อตกลงและเปิดเผยข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ

Maybank Kim Eng

ตรวจสอบข้อมูลตาม กม. กำหนด และตรวจ Fraud

เมื่อข้อมูลทุกอย่าง Verify ถึงจะเปิดบัญชีให้ลูกค้าได้

ทุกอย่างผ่าน ส่งคำขอมาให้ BBL เพื่ออนุมัติการตัดบัญชี (จะผ่าน Finnet?)

Bangkok Bank ธนาคารกรุงเทพ

RP Role

BBL's Node

ตรวจสอบ Consent และการยืนยันตัวตน

เมื่อผ่าน ก็ดำเนินสมัครการตัดบัญชีอัตโนมัติให้ลูกค้า

Digital ID Platform

หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อตกลงและเปิดเผยข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ

SET
ตลาดหลักทรัพย์แห่งประเทศไทย

ใบสมัครในรูปแบบ XML ให้ บล.กิมเอ็ง และ BBL

Maybank Kim Eng

ตรวจสอบข้อมูลตาม กม. กำหนด และตรวจ Fraud

เมื่อข้อมูลทุกอย่าง Verify ถึงจะเปิดบัญชีให้ลูกค้าได้

ทุกอย่างผ่าน ส่งคำขอมาให้ BBL เพื่ออนุมัติการตัดบัญชี (จะผ่าน Finnet?)

Bangkok Bank ธนาคารกรุงเทพ RP Role

BBL's Node

ตรวจสอบ Consent และการยืนยันตัวตน

เมื่อผ่าน ก็ดำเนินสมัครการตัดบัญชีอัตโนมัติให้ลูกค้า

Digital ID Platform

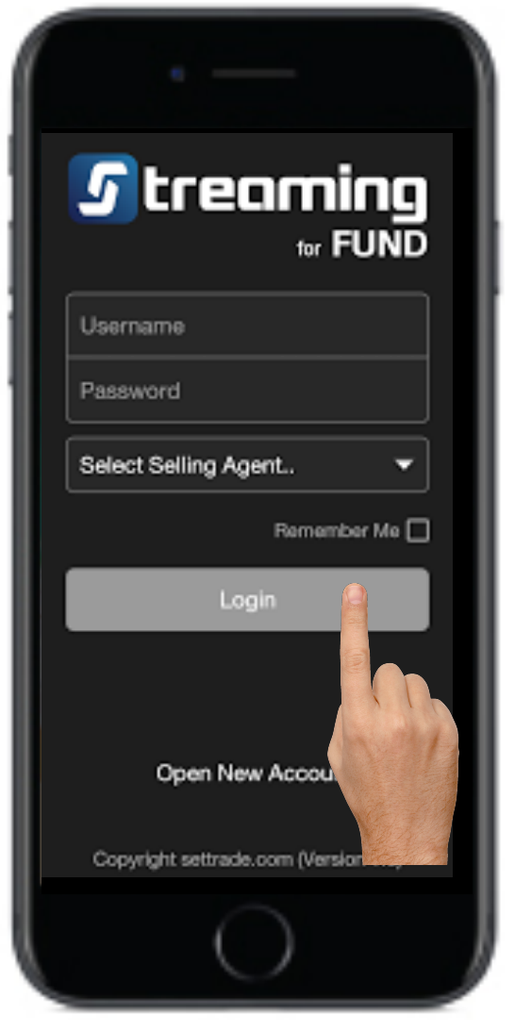
หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

ตัวอย่าง User Journey การเปิดบัญชีกองทุนโดยใช้ 2nd Tier IdP

1. ลูกค้าแสดงเจตนาเปิดบัญชีกับ บล. และยินยอมตามข้อตกลงและเปิดเผยข้อมูล
2. Verify ข้อมูลกับ DOPA
3. เลือกหักบัญชีธนาคาร (RP)
4. เลือก IdP เพื่อยืนยันตัวตน
5. ยืนยันตัวตนตามระดับ IAL ที่ช่อง IdP
6. กรอกข้อมูลตามใบสมัคร
7. แนบเอกสารที่ RP ต้องการ
8. สร้าง Account
9. ระบบหลังบ้าน
10. เข้าใช้บริการ

Streaming for Fund แจ้งเตือนเมื่อเปิดบัญชีเสร็จ

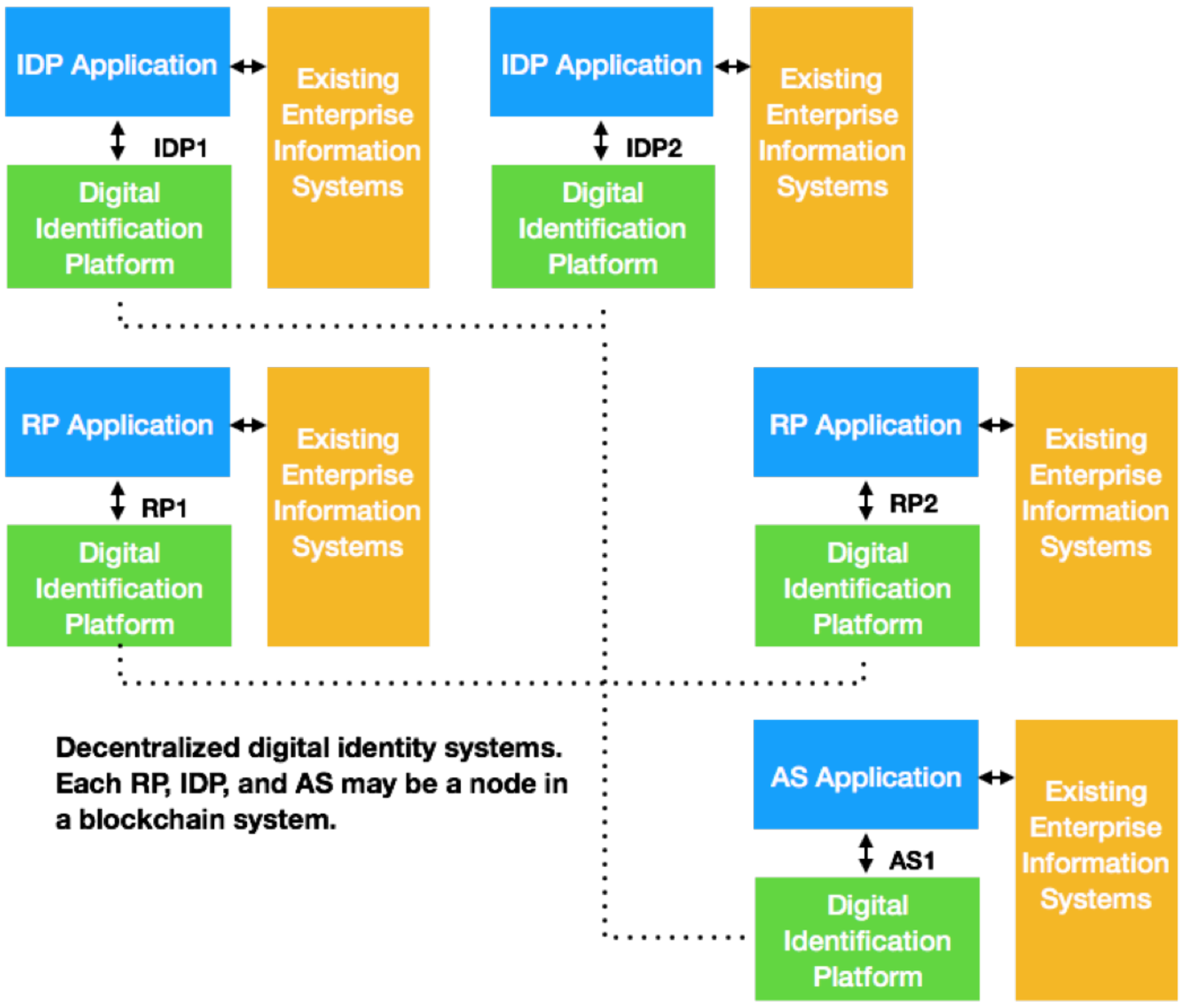
Login ด้วยรหัสที่ Create เอาไว้เมื่อตอนเปิดบัญชี



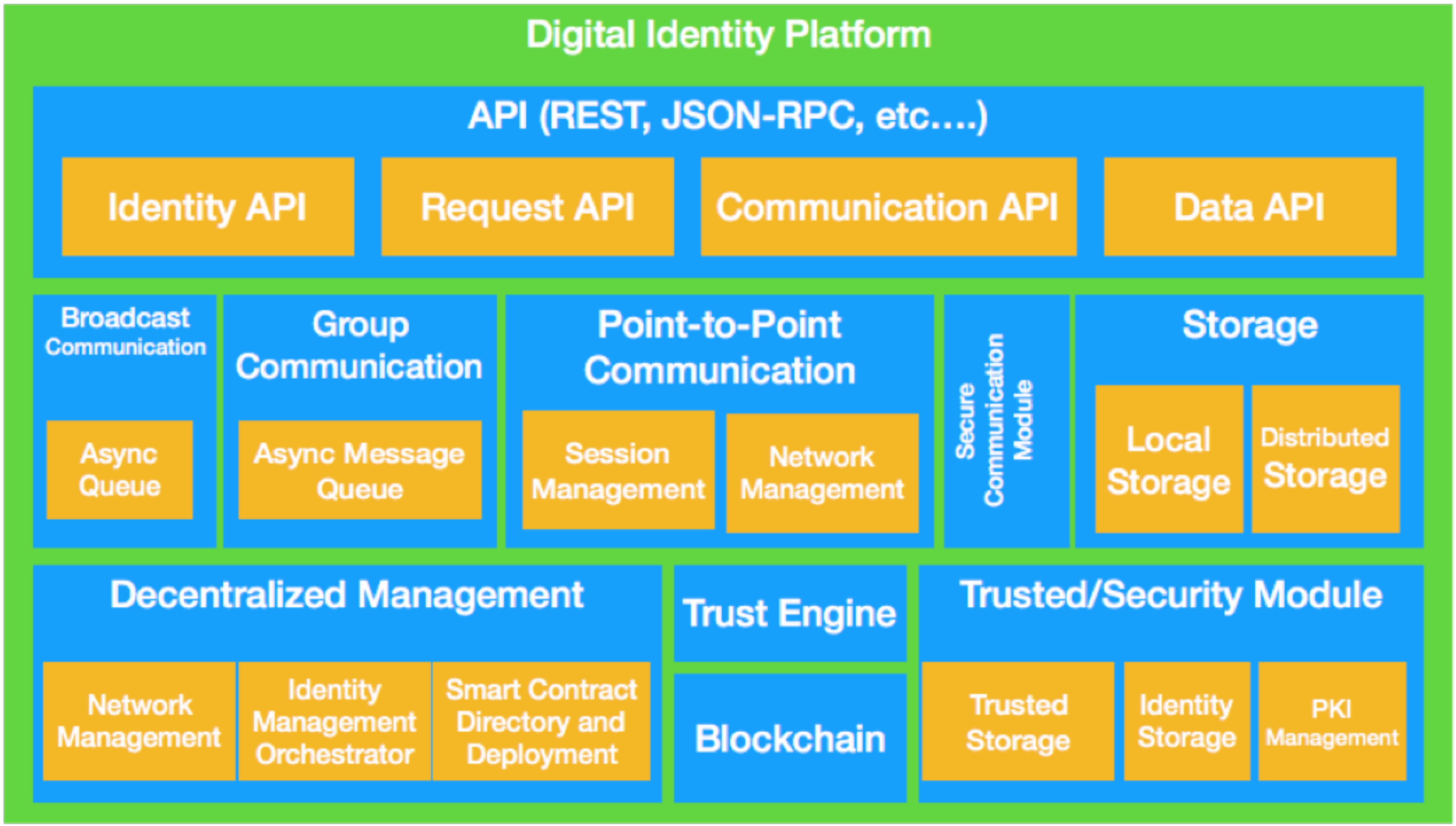
เข้าใช้งาน ซื้อขาย และชำระเงินตามกระบวนการปกติ

หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

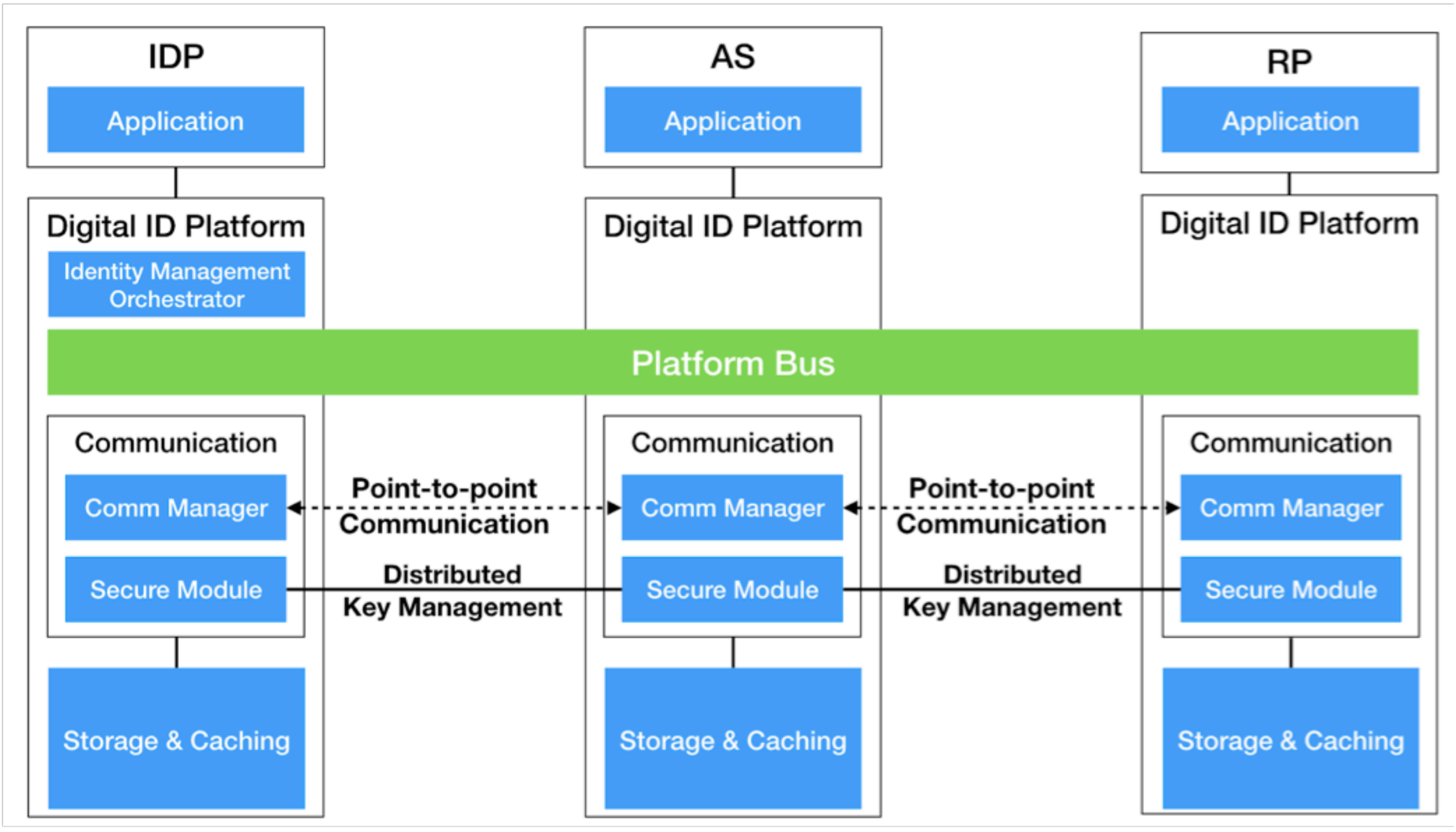
Architecture Design



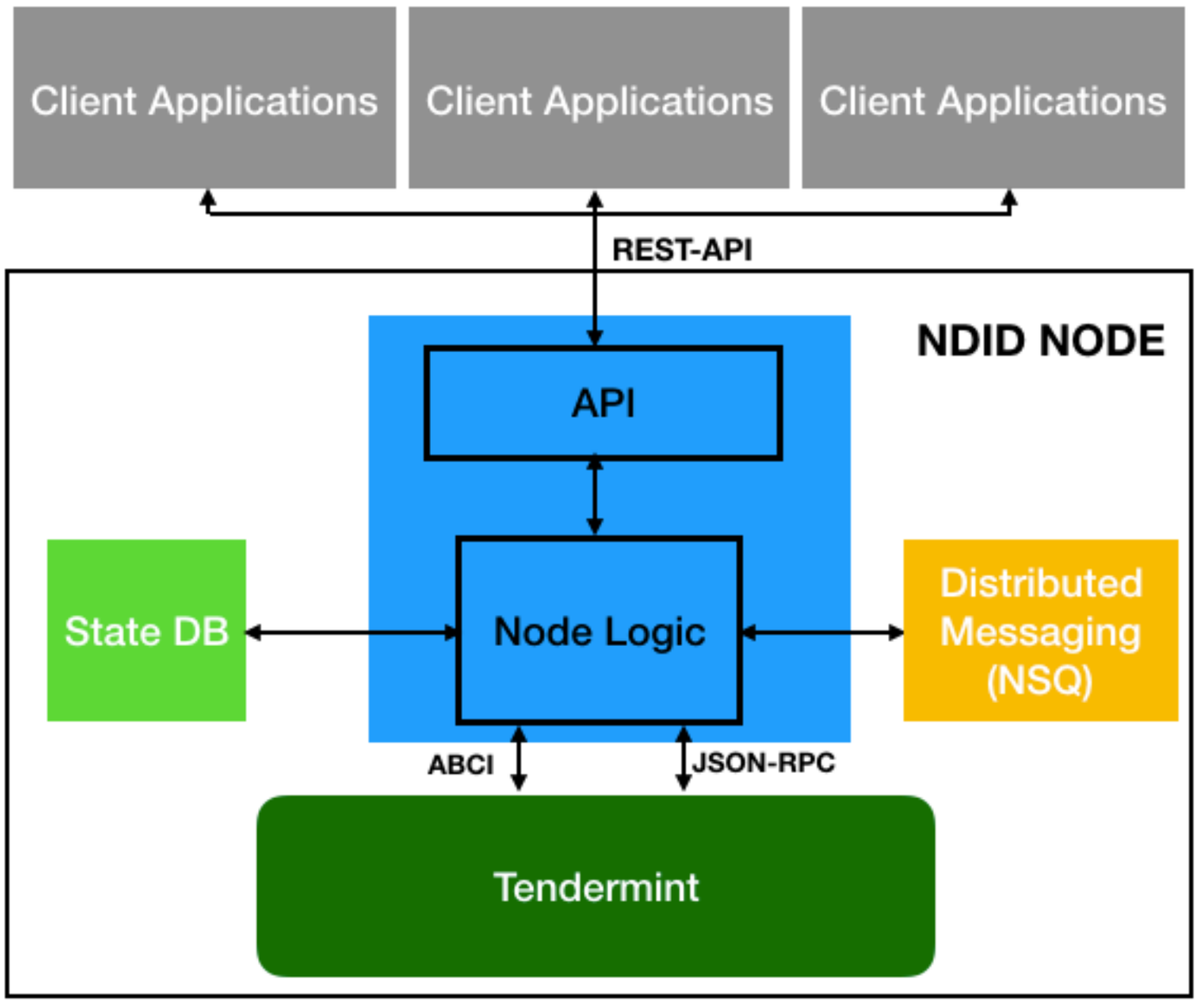
Platform Node Components



Communication Between Nodes



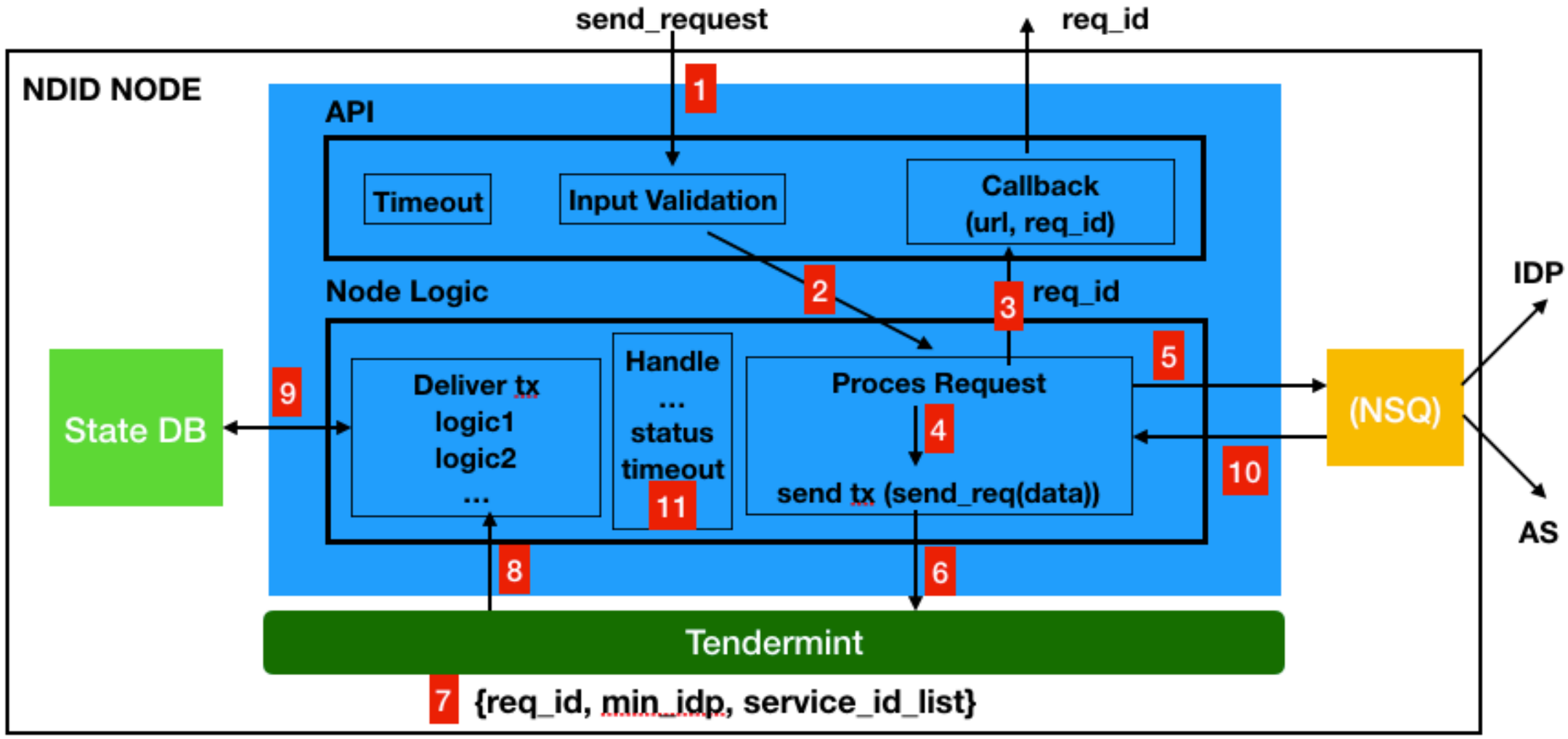
Example NDID Node

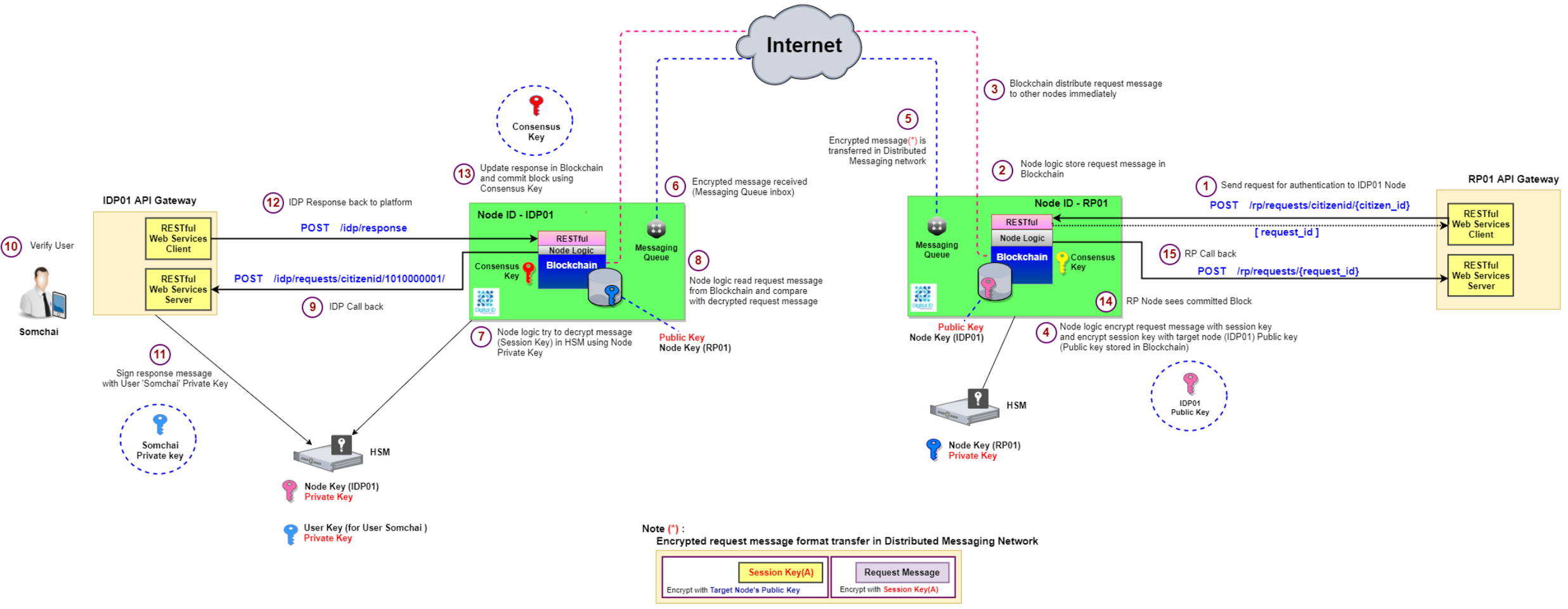


Example Request

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

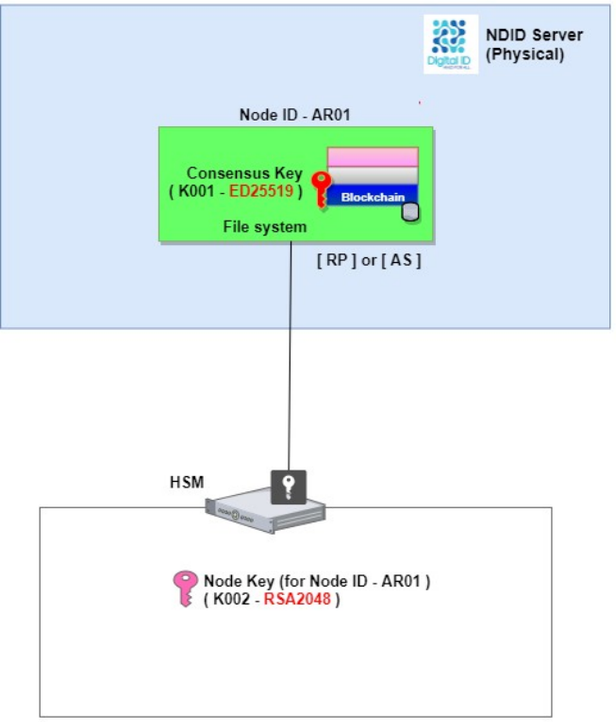
{ns, id, request_type, request_message, min_ial, min_aal, min_idp, service_id_list, timeout}



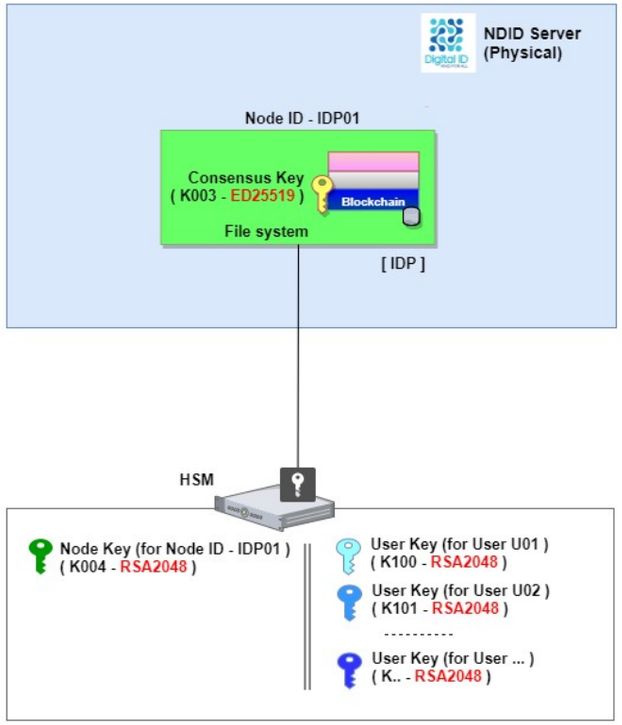


Note (*) :
Encrypted request message format transfer in Distributed Messaging Network

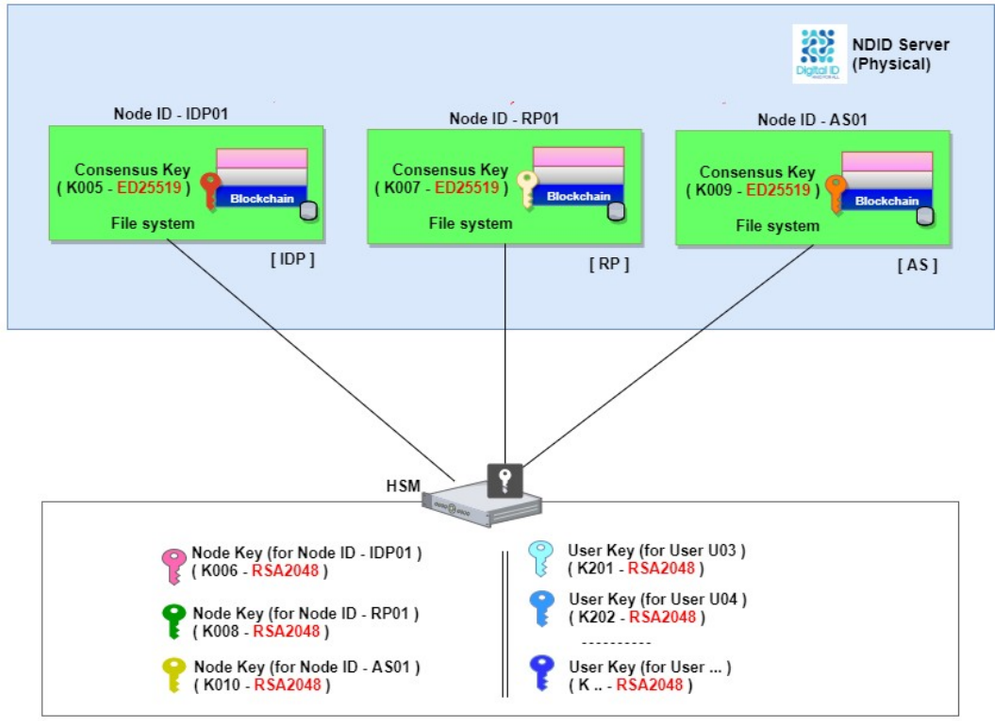
Case 1 : RP x 1 or AS x 1 [2 Keys]



Case 2 : IDP x 1 [2 + N Keys]



Case 3 : IDP x 1, RP x 1 and AS x 1 [(3 x 2) + N Keys]



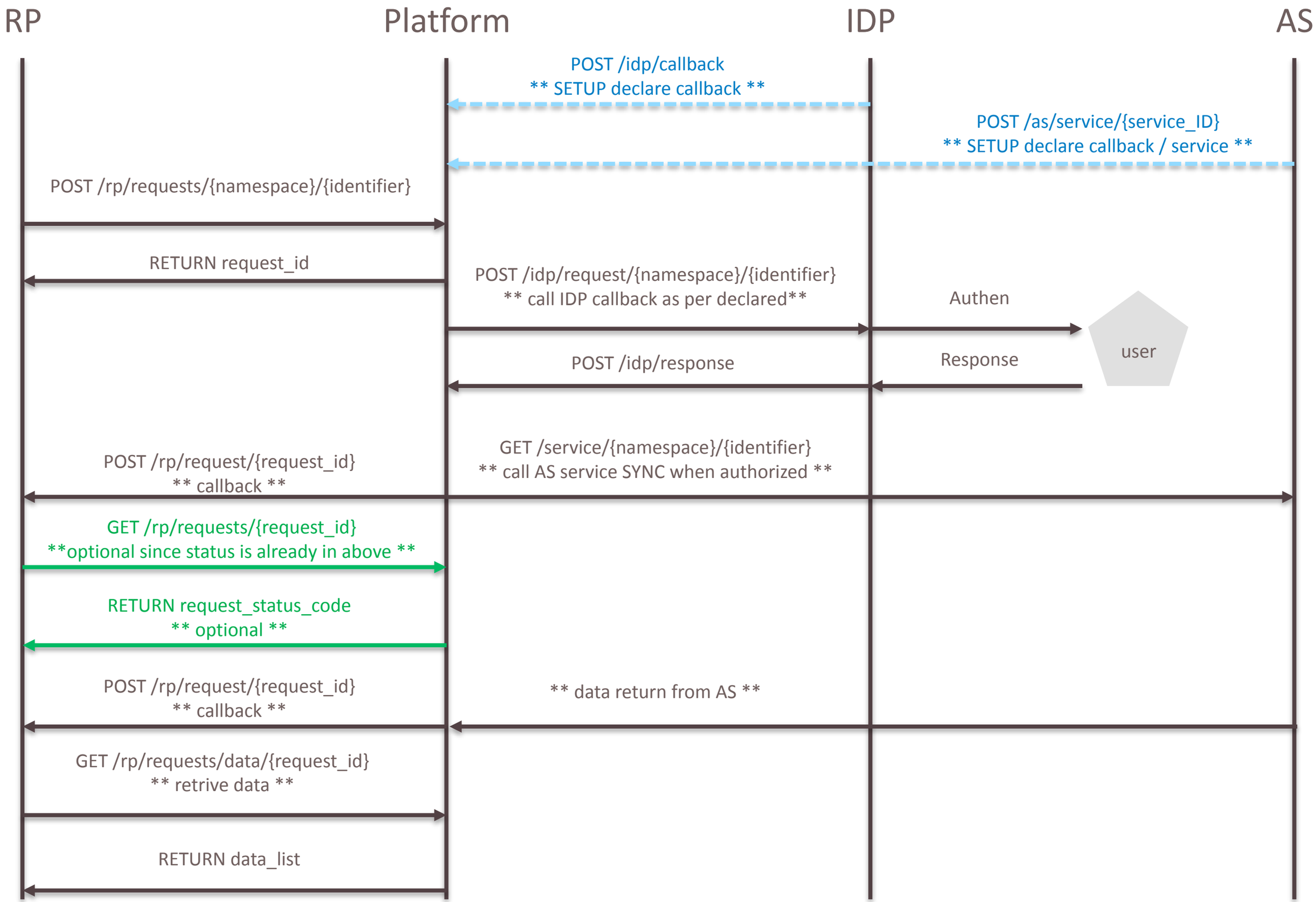
Key Type

1. Consensus Key - Use by Tendermint when commit block

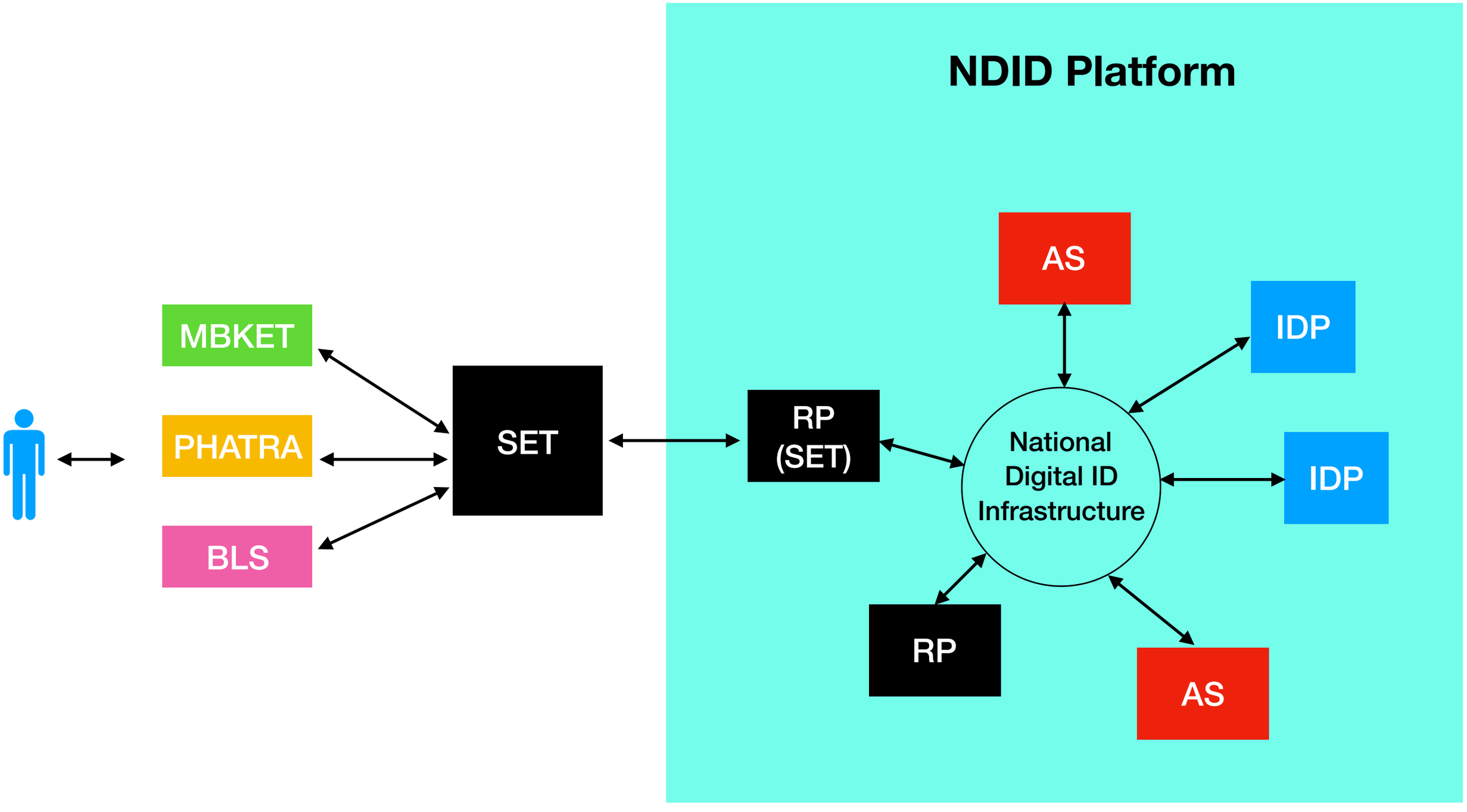
2. Node Key - Private key use for the node to sign transaction before send to target nodes and Public key use by other party to encrypt transaction before send to this node (In point-to-point messaging communication)

3. User Key - Private key use for sign request/response transaction

API 1.0


RP
Platform
IDP
AS
POST /idp/callback
** SETUP declare callback **
POST /as/service/{service_ID}
** SETUP declare callback / service **
POST /rp/requests/{namespace}/{identifier}
RETURN request_id
POST /idp/request/{namespace}/{identifier}
** call IDP callback as per declared**
Authen
user
Response
POST /idp/response
GET /service/{namespace}/{identifier}
** call AS service SYNC when authorized **
POST /rp/request/{request_id}
** callback **
GET /rp/requests/{request_id}
**optional since status is already in above **
RETURN request_status_code
** optional **
POST /rp/request/{request_id}
** callback **
** data return from AS **
GET /rp/requests/data/{request_id}
** retrive data **
RETURN data_list

Using Proxy


NDID Platform
AS
IDP
MBKET
PHATRA
BLS
SET
RP
(SET)
National
Digital ID
Infrastructure
IDP
RP
AS

What got stored on blockchain ?

- Proofs used by recipient of the data to verify truthfulness of the data.

- Proofs ensure that RP cannot be lied to by IDP or AS even in the case that they’re compromise, thus providing secure and trusted infrastructure.

- Claims and Attestation (a confirmation). Signature and hash of data.

No sensitive data on blockchain

- A request for user consent to get bank statements.

```
request_id: 'ef6f4c9c-818b-42b8-8904-3d97c4c520f6'
min_idp: 1
min_aal: 1
min_ial: 2
timeout: 259200
data_request_list: [{
  service_id: 'bank_statement',
  as_id_list: ['AS1', ‘AS2’],
  count: 1,
  request_params_hash: hash({ format: 'pdf' })]
},...
message_hash: hash('Please allow...')
```

Sensitive data transmitted via private channel

- RP to IDP, RP does not need to know IDPs.

```
namespace: 'citizenid'
identifier: '01234567890123'
data_request_list: [{
service_id: 'bank_statement',
as_id_list: ['AS1', 'AS2'],
count: 1,
request_params: { format: 'pdf' }
]
},...
request_message: 'Please allow...'
min_ial: 2
min_aal: 1
min_idp: 1
timeout: 259200
request_id: 'ef6f4c9c-818b-42b8-8904-3d97c4c520f6'
```

Demo

re7eal Merge pull request #1 from ndidplatform/add-docker ··· Latest commit `4d03b3e` 4 days ago

as/example1	fix link service, ial	4 days ago
docker	update latest code and add as node configuration	8 days ago
idp/example1	handle when idp response failed	4 days ago
rp/example1	check idp count	5 days ago
README.md	update readme	14 days ago

README.md

Run in Docker

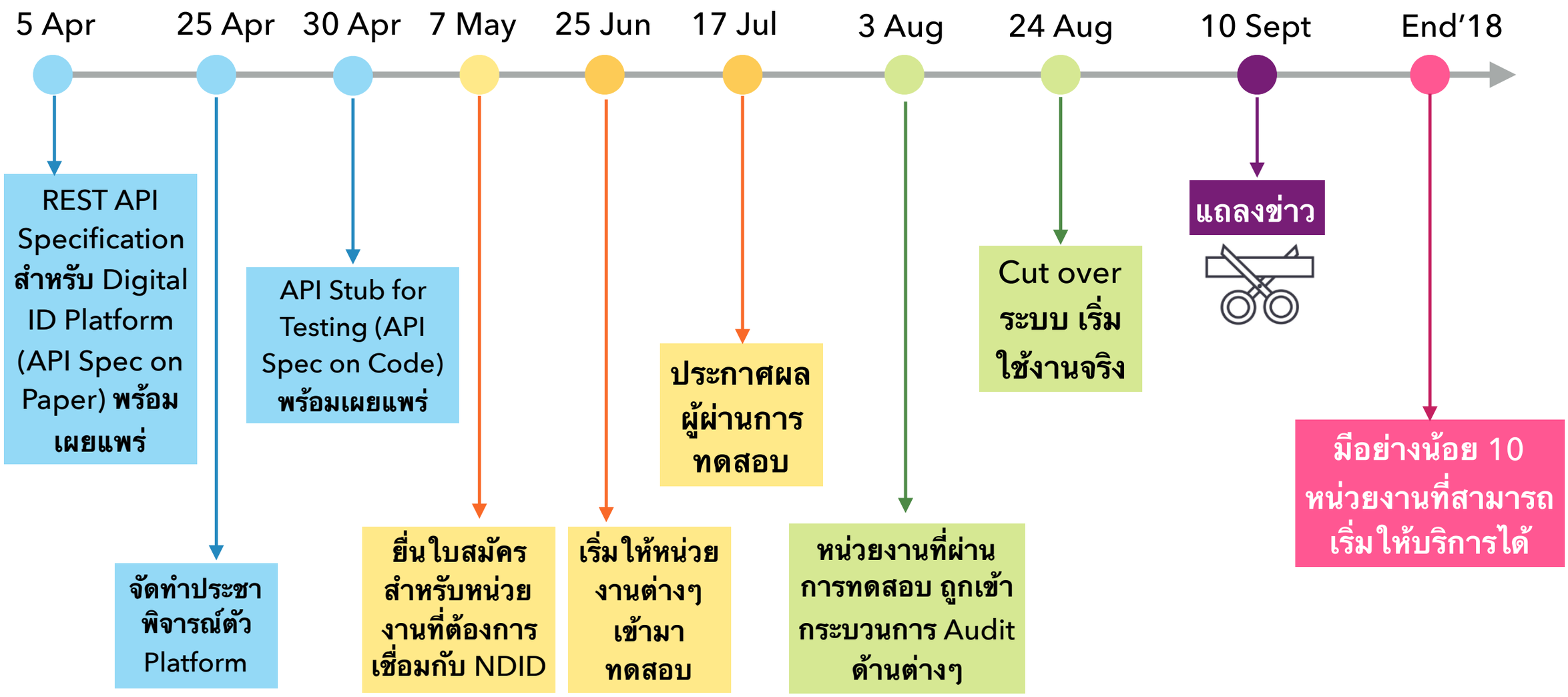
Required

- Docker CE Install docker
- docker-compose Install docker-compose
- git

```
cd docker
./build-container.sh
docker-compose up
```

Then you can run idp-example at port 8001 and rp-example at port 8002

Timeline (ฝั่ง NDID)



Useful Links

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