Intra-ASEAN

Secure Transactions Framework

ETDA
สพธอ
www.etda.or.th

MINISTRY OF ICT
Smart Thailand

Background

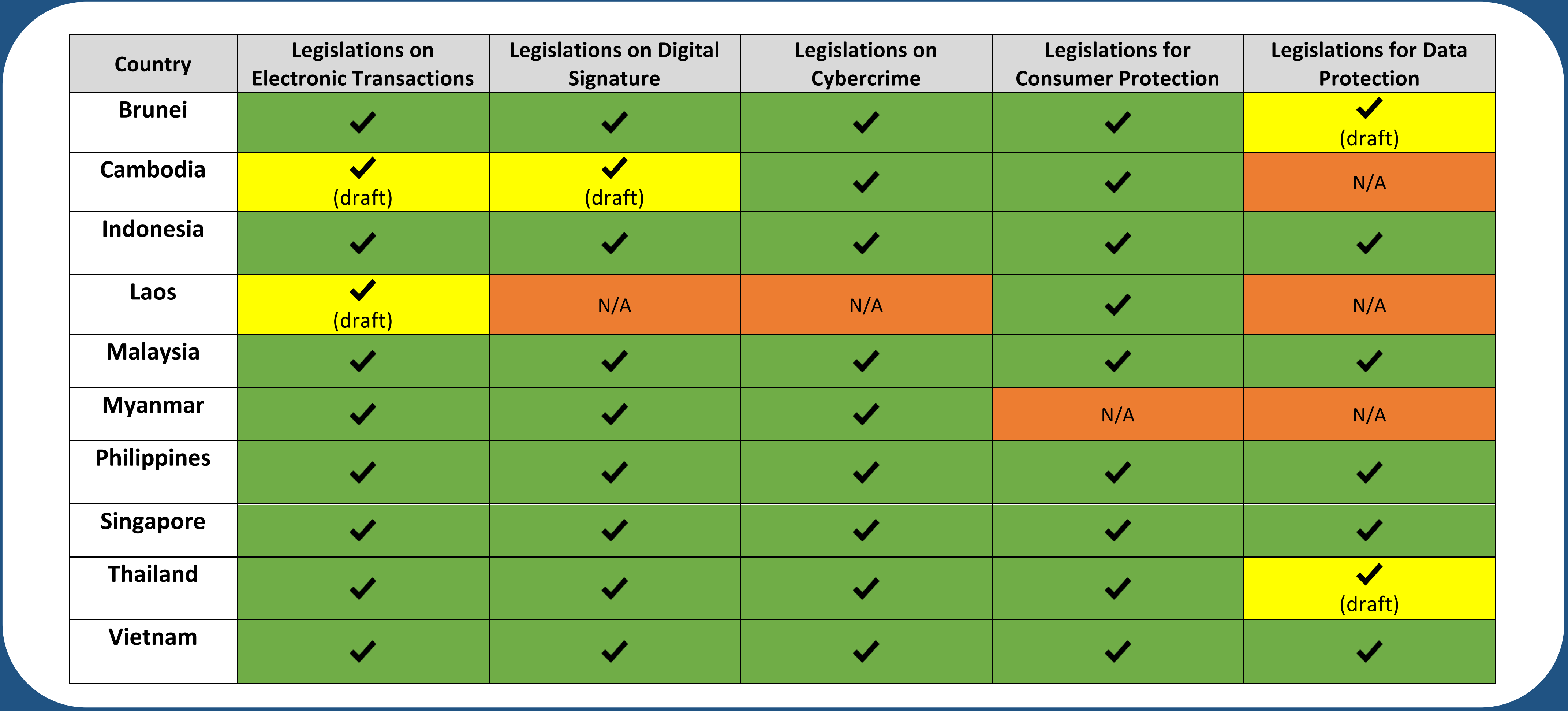
- What is Intra-ASEAN Secure Transactions Framework ?
  - Funded Project by ASEAN ICT
  - Part of the ASEAN ICT Masterplan 2015

Initiative 2.4 " Building Trust and promote secure transaction within ASEAN"

- Objectives

1. Provide **guideline**, technology-neutral framework, and legal consistency in secure transaction approaches across ASEAN member states
2. Increase trust and promote secure and efficient electronic transactions through **proper selection of e-authentication mechanism**
3. **Initiate online identity provider service** and authentication across cross-border systems

1. Law Development for secure e-Transactions

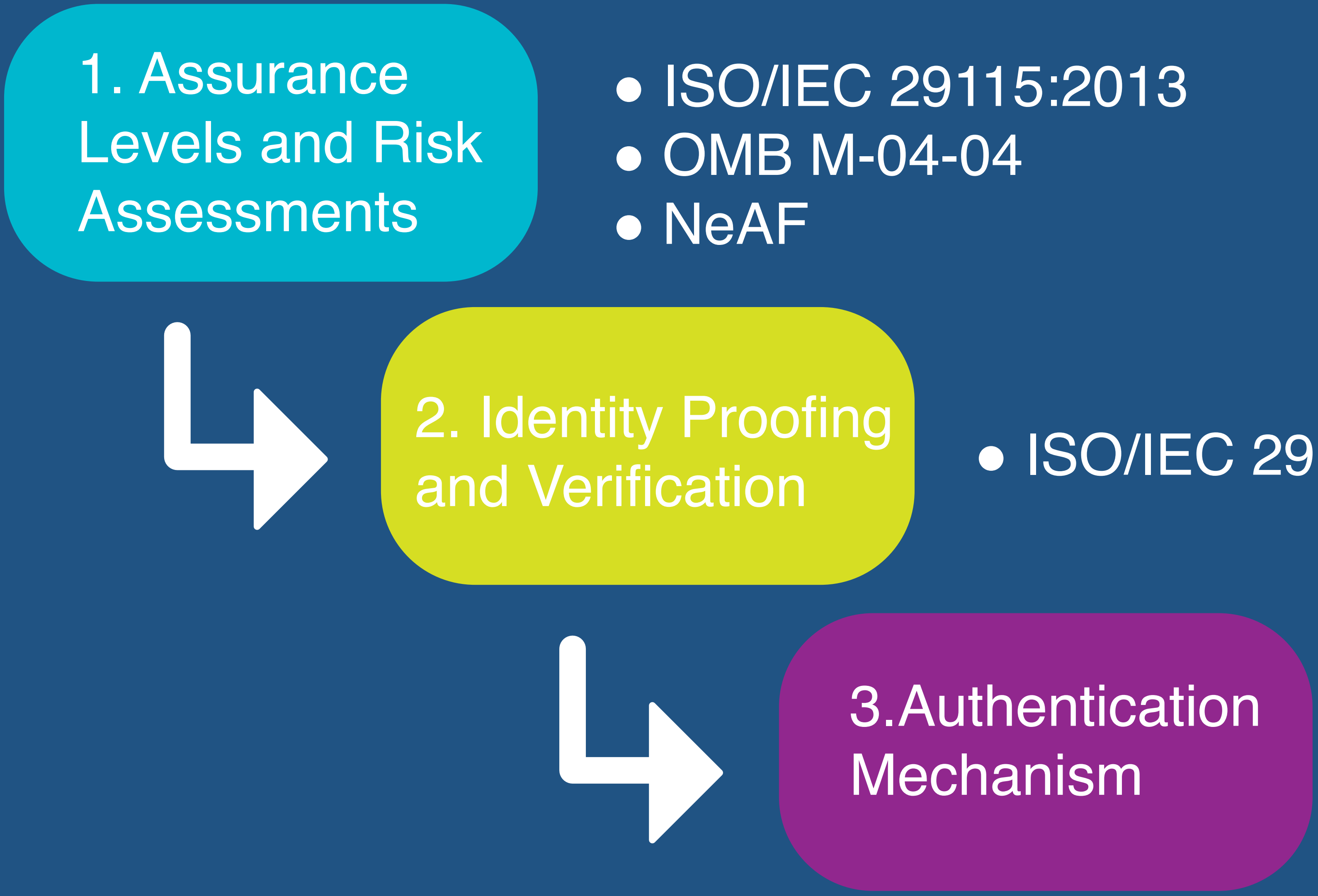


Country	Legislations on Electronic Transactions	Legislations on Digital Signature	Legislations on Cybercrime	Legislations for Consumer Protection	Legislations for Data Protection
Brunei	✓	✓	✓	✓	✓ (draft)
Cambodia	✓ (draft)	✓ (draft)	✓	✓	N/A
Indonesia	✓	✓	✓	✓	✓
Laos	✓ (draft)	N/A	N/A	✓	N/A
Malaysia	✓	✓	✓	✓	✓
Myanmar	✓	✓	✓	N/A	N/A
Philippines	✓	✓	✓	✓	✓
Singapore	✓	✓	✓	✓	✓
Thailand	✓	✓	✓	✓	✓ (draft)
Vietnam	✓	✓	✓	✓	✓

- Legal Framework for secure e-Transactions is almost ready.
- A little reminder: Legal is the supporting framework, but Business Framework or Existing Flow is the main actor.

2. Increase trust by proper e-authentication

- Methodology for selecting the proper e-authentication mechanism



1. Assurance Levels and Risk Assessments

- ISO/IEC 29115:2013
- OMB M-04-04
- NeAF

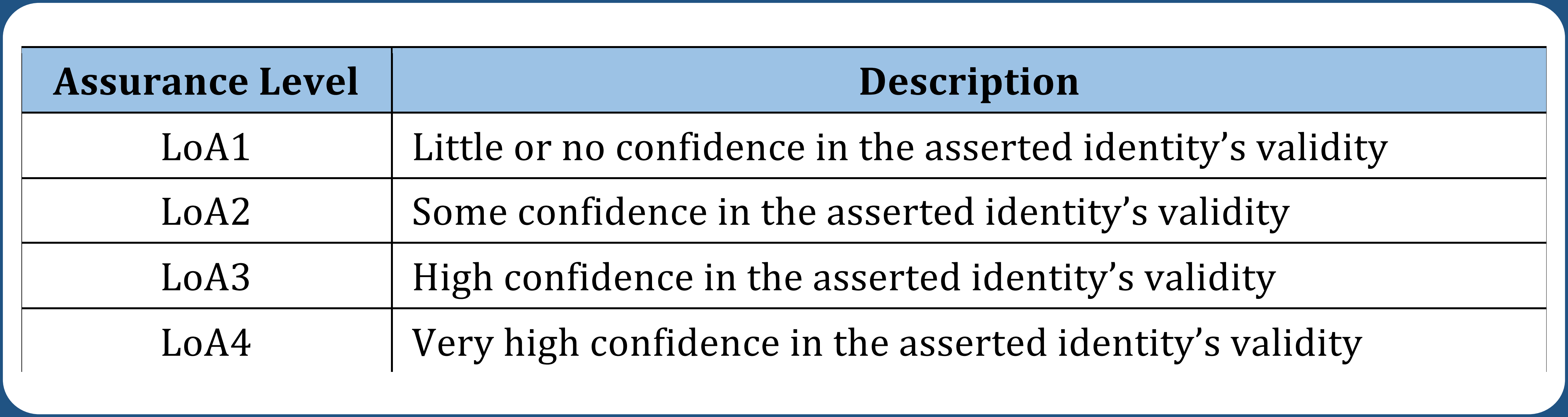
2. Identity Proofing and Verification

- ISO/IEC 29115:2013

3.Authentication Mechanism

- NIST Special Publication 800-63-1

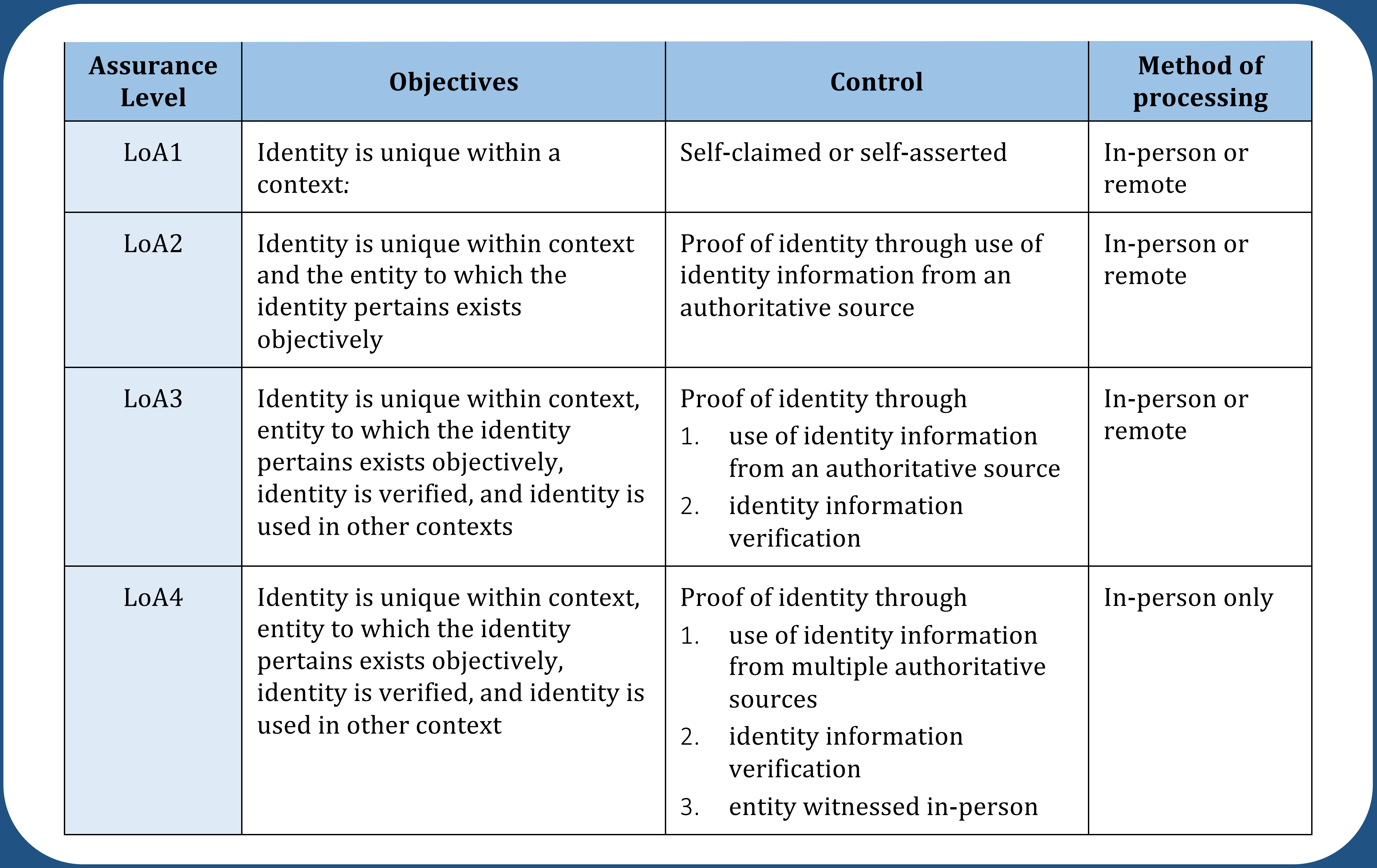
2.1 Level of Assurance



Assurance Level	Description
LoA1	Little or no confidence in the asserted identity’s validity
LoA2	Some confidence in the asserted identity’s validity
LoA3	High confidence in the asserted identity’s validity
LoA4	Very high confidence in the asserted identity’s validity

Source: *ISO/IEC 29115: 2013*

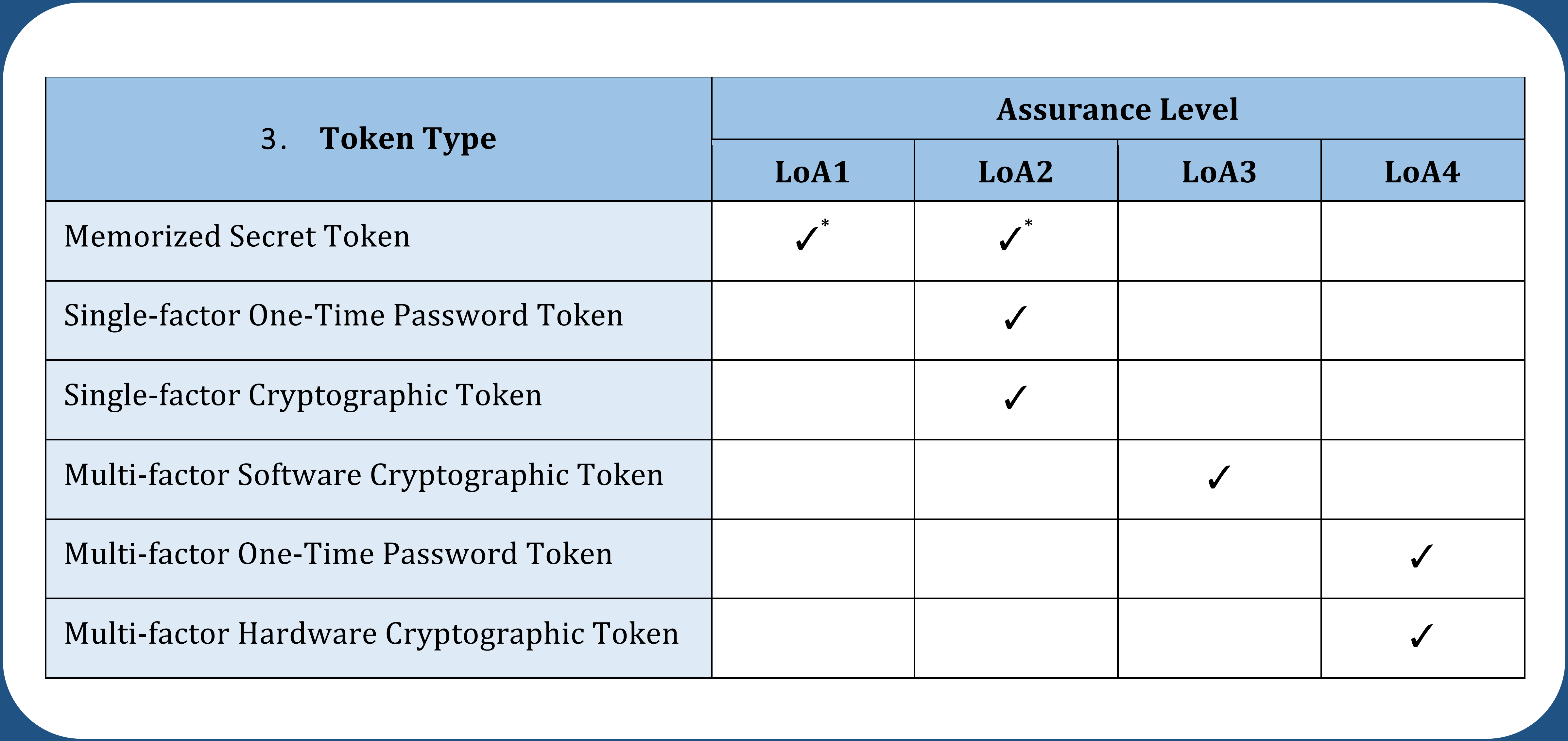
2.2 Approach to Identity Proofing



Assurance Level	Objectives	Control	Method of processing
LoA1	Identity is unique within a context:	Self-claimed or self-asserted	In-person or remote
LoA2	Identity is unique within context and the entity to which the identity pertains exists objectively	Proof of identity through use of identity information from an authoritative source	In-person or remote
LoA3	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through 1. use of identity information from an authoritative source 2. identity information verification	In-person or remote
LoA4	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other context	Proof of identity through 1. use of identity information from multiple authoritative sources 2. identity information verification 3. entity witnessed in-person	In-person only

Source: *ISO/IEC 29115:2013*

2.3 Mechanisms

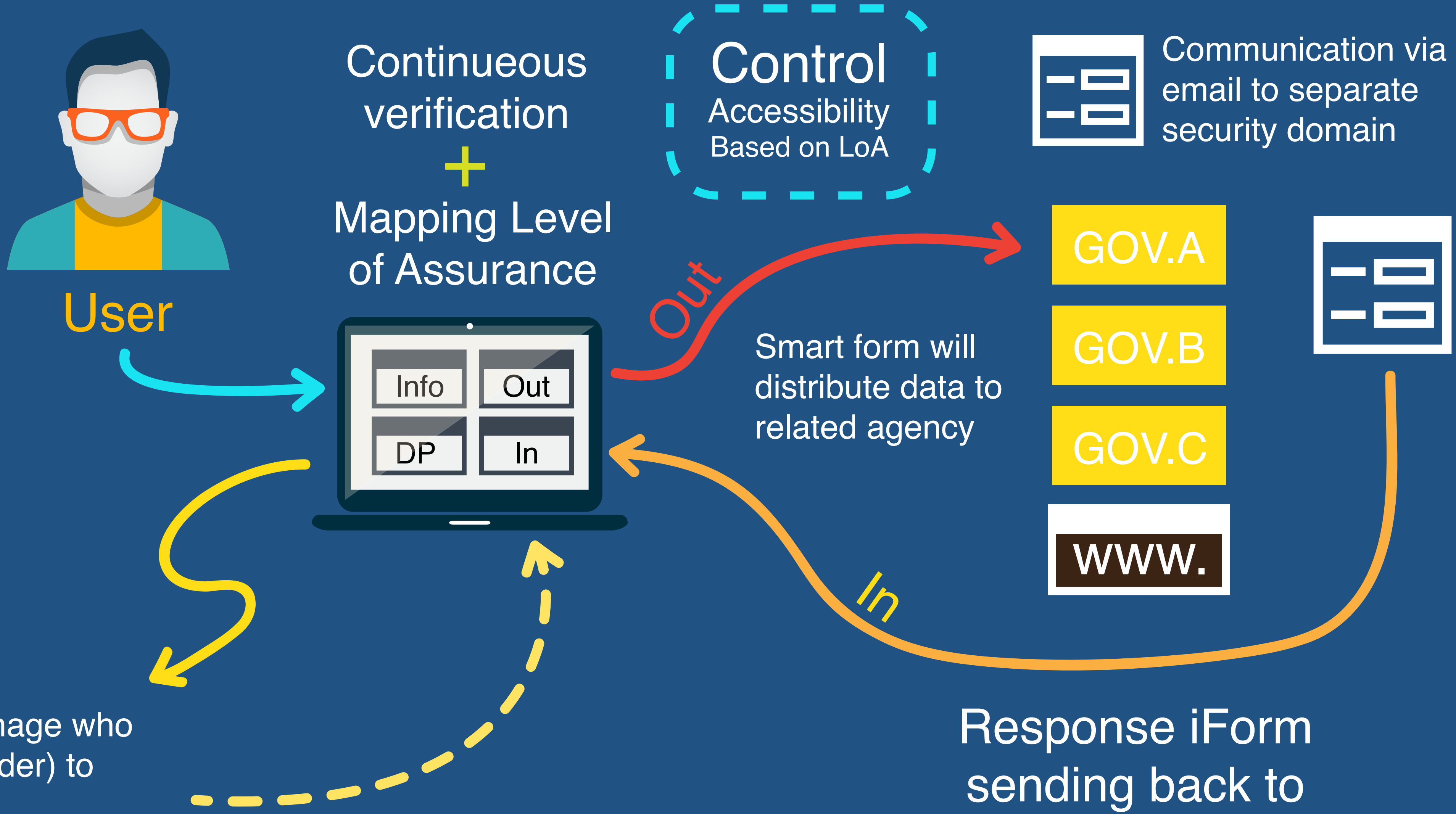


3. **Token Type**	**Assurance Level**			
	LoA1	**LoA2**	**LoA3**	**LoA4**
Memorized Secret Token	✓*	✓*		
Single-factor One-Time Password Token		✓		
Single-factor Cryptographic Token		✓		
Multi-factor Software Cryptographic Token			✓	
Multi-factor One-Time Password Token				✓
Multi-factor Hardware Cryptographic Token				✓

Source: *NIST Special Publication SP-800-63-1*

3. Initiating online identity provider

National Contact Information System



Info

User can Register And Upgrade Level of Assurance by providing more information (Authoritative of Corroborative)

Continueous verification
+
Mapping Level of Assurance

Control

Accessibility
Based on LoA

Communication via email to separate security domain

Smart form will distribute data to related agency

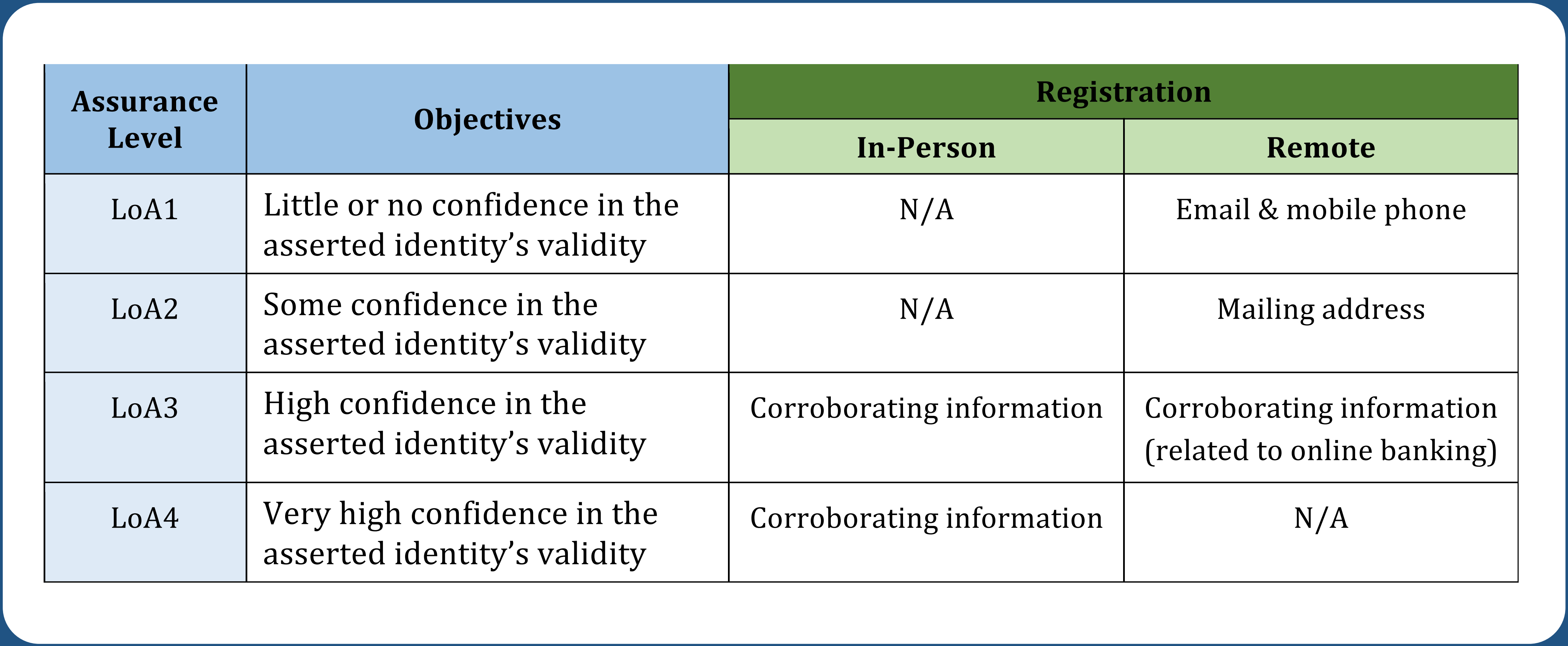
DP

User can manage who (service provider) to share what information with

Response iForm sending back to requester's Inbox

3. Initiating online identity provider

Mapping with the Framework

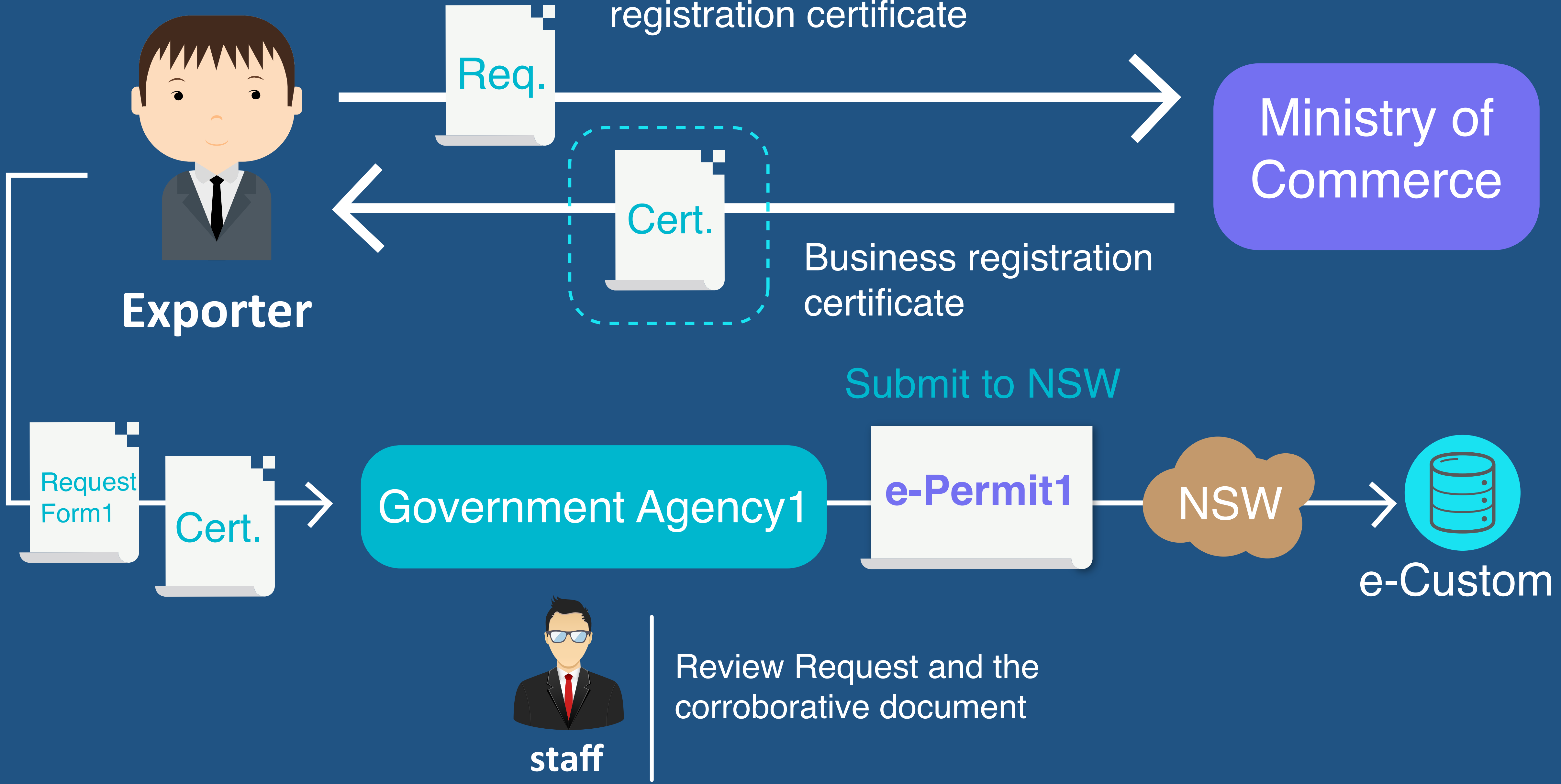


Assurance Level	Objectives	Registration	
		In-Person	Remote
LoA1	Little or no confidence in the asserted identity's validity	N/A	Email & mobile phone
LoA2	Some confidence in the asserted identity's validity	N/A	Mailing address
LoA3	High confidence in the asserted identity's validity	Corroborating information	Corroborating information (related to online banking)
LoA4	Very high confidence in the asserted identity's validity	Corroborating information	N/A

NCIS Key Feature: Perform online identity regular check

Pilot Project
B2G e-Filing for exporter

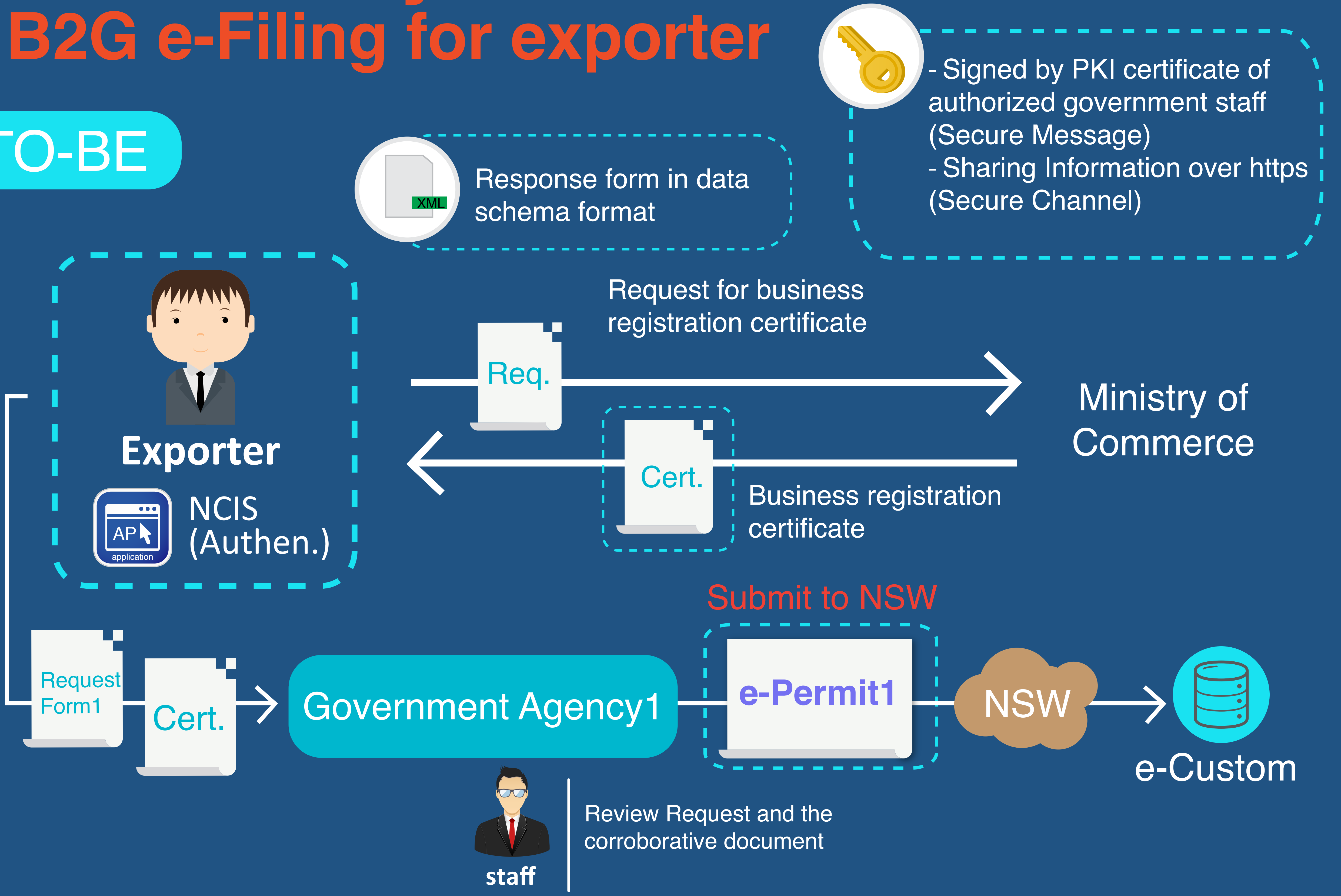
AS-IS


Request for business registration certificate
Req.
Ministry of Commerce
Cert.
Business registration certificate
Exporter
Submit to NSW
Request Form1
Cert.
Government Agency1
e-Permit1
NSW
e-Custom
staff
Review Request and the corroborative document

Pilot Project

B2G e-Filing for exporter

TO-BE



- Signed by PKI certificate of authorized government staff (Secure Message)
- Sharing Information over https (Secure Channel)

Response form in data schema format

Request for business registration certificate

Business registration certificate

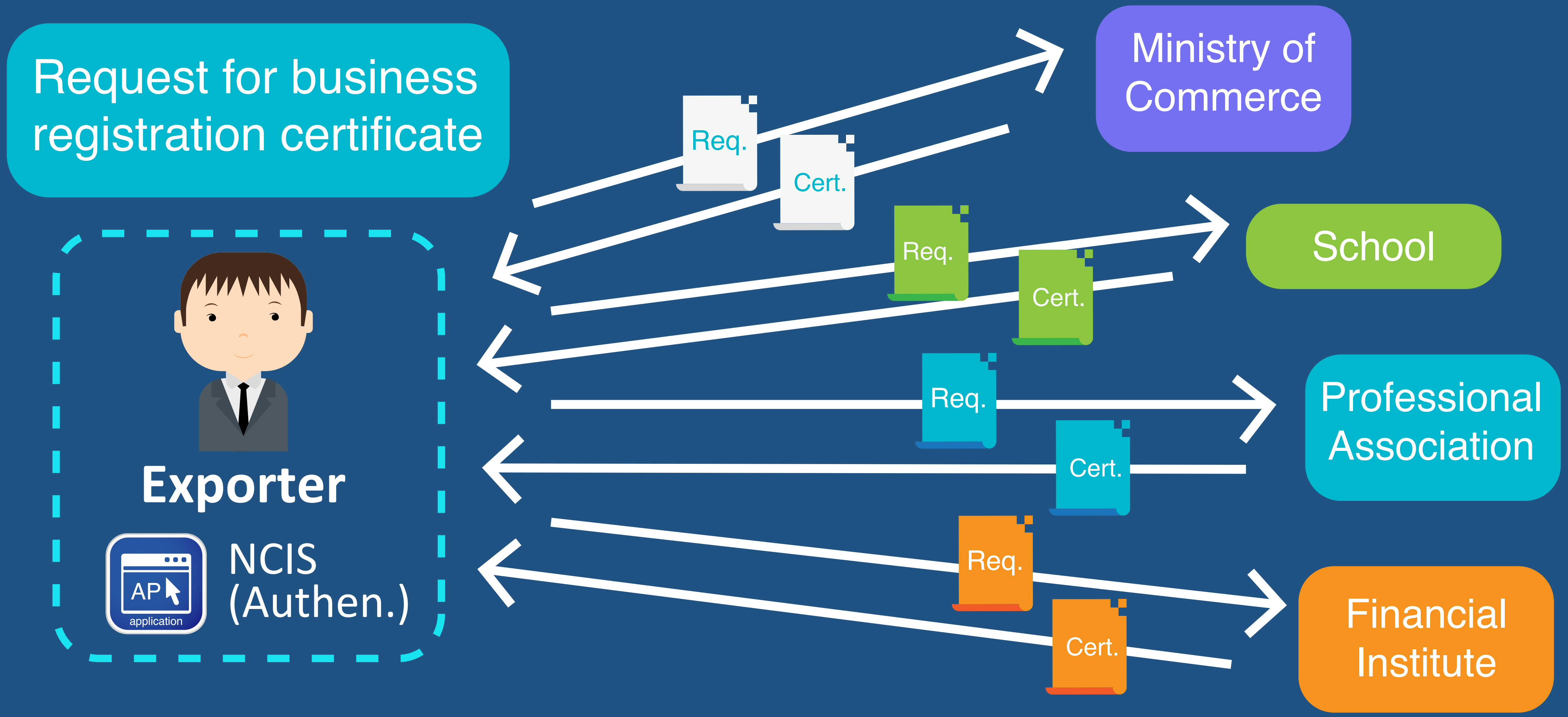
Submit to NSW

Review Request and the corroborative document

TO Authenticate

We also care the 'function' of that identity

- It's not only we want to know he is Mr. John.
- But we also want to know what Mr. John can do.



Request for business registration certificate

Exporter

NCIS (Authen.)

How PKI

can help complete the jigsaw

- Maintain the liability chain
- Keep integrity of data
- Non-repudiation
- Not only human to server but also server to server

Recommendations

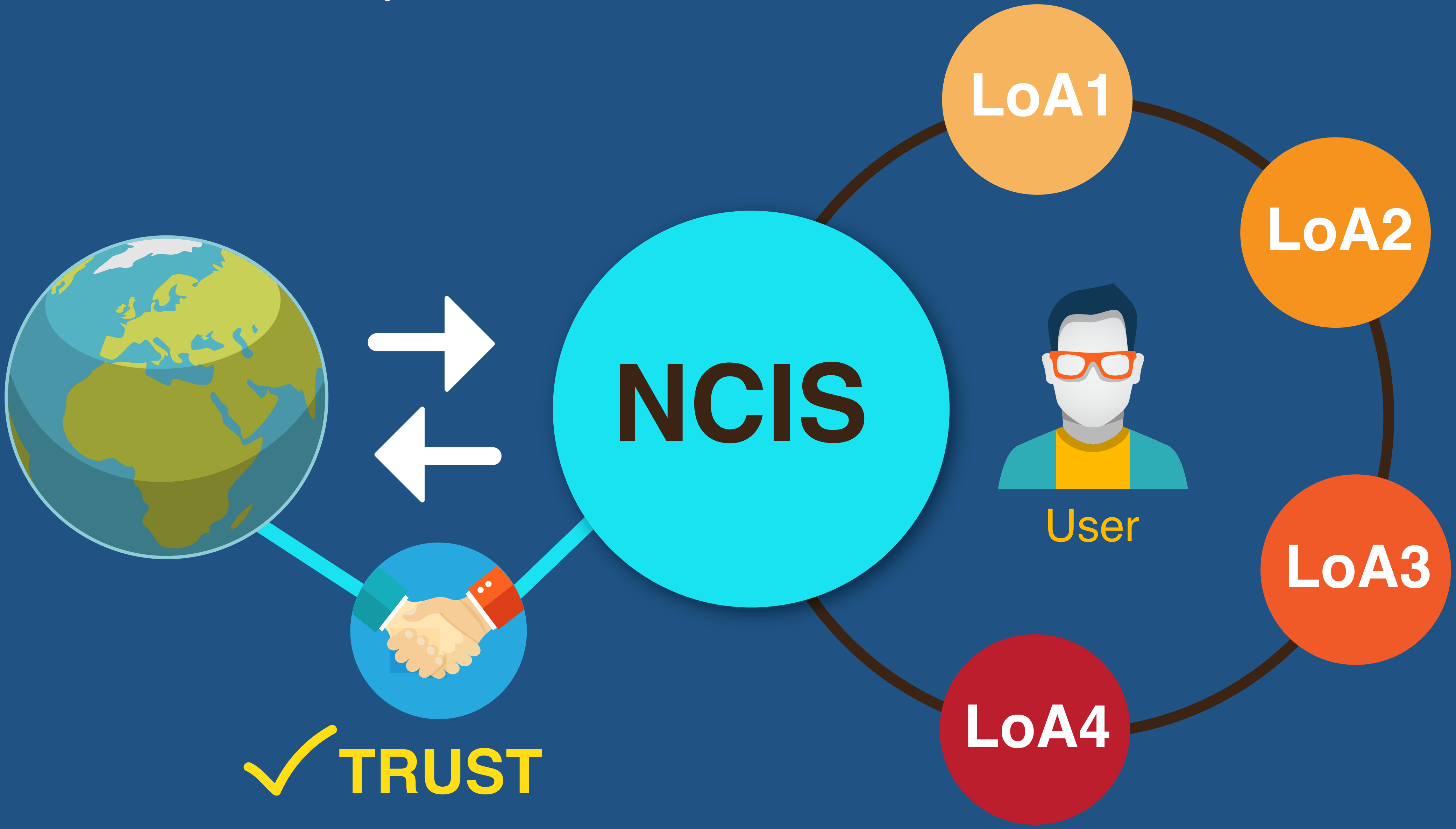
- ASEAN should adopt the risk-based approach to define the Level of Assurance required for each application.

- ASEAN should define identity proofing and verification for each LoA based on ISO29115:2013.

- Credential management should include the Corroborative Information and Authoritative Information.

Summary

1. Guideline, framework, and legal consistency in secure transaction approaches across ASEAN member states
2. Increase trust and promote secure and efficient electronic transactions
3. Initiate online identity provider service and authentication across cross-border systems



THANK YOU

www.etda.or.th