

ELECTRONIC TRANSACTION STANDARD

ETS 11 Part 2-2566

DIGITAL IDENTITY – PART 2: IDENTITY PROOFING REQUIREMENTS

Electronic Transactions Development Agency
Ministry of Digital Economy and Society

ICS 35.030

Disclaimer: This translation is provided by the Electronic Transactions Development Agency as the competent authority for information purposes only. Whilst the Electronic Transactions Development Agency has made efforts to ensure the accuracy and correctness of the translation, the original Thai text as formally adopted and published shall in all events remain the sole authoritative text having the force of law.

ELECTRONIC TRANSACTION STANDARD

DIGITAL IDENTITY –
PART 2: IDENTITY PROOFING
REQUIREMENTS

ETS 11 Part 2-2566

Electronic Transactions Development Agency

The 9th Tower Grand Rama 9 Building (Tower B) Floor 20-22

33/4 Rama 9 Road, Huai Khwang, Bangkok 10310

Tel: +66 0 2123 1234 Fax: +66 0 2123 1200

Foreword

When entering into various transactions, there needs to be an initial process to prove and authenticate the identity of the person who wishes to enter into the transaction in order to ensure that the person who wishes to enter into the transaction is indeed who they claim to be. There is also today a great increase in transactions and the use of services in digital formats. Service providers have therefore begun to develop digital identity proofing and authentication processes to facilitate access to various services. At the same time, the law on electronic transactions has been revised to enable individuals to prove and authenticate their identity through a digital authentication system. This mechanism can reduce the burden on subscribers to report in person and to submit documents or evidence for identity proofing and authentication. It also helps to reduce the steps that had to be repeated in former processes to prove and authenticate one's identity before entering into a transaction.

However, current identity proofing and authentication processes vary and have different requirements depending on the conditions and needs of each service provider or agency, which in some cases may cause inconsistency or mutual incompatibility. Therefore, the Electronic Transaction Development Agency and related agencies, both government and private sectors, have jointly developed standards for digital identity proofing and authentication, namely the ETDA Recommendation on ICT Standard for Electronic Transactions (ETDA Recommendation), which has been continuously developed and improved as follows.

- Version 1.0: Numbers ETDA Rec. 18-2561, 19-2561 and 20-2561
- Version 2.0: Numbers ETDA Rec. 18-2564, 19-2564 and 20-2564
- Version 3.0: Numbers ETDA Rec. 18-2566, 19-2566 and 20-2566

In this regard, in order to ensure consistency and strengthen the reliability and acceptance of the digital identity proofing and authentication system, and to enable service providers and agencies together to refer to and choose to use digital ID based on a consistent standard and assurance level, the Electronic Transactions Commission therefore approved an upgrade of the standards by revising Recommendation on Standards No. ETDA Rec. 18-2566, 19-2566 and 20-2566 into a set of Electronic Transaction Standards on Digital Identity (No. ETS 11), which consists of:

- Part 1: Framework
- Part 2: Identity Proofing Requirements
- Part 3: Authentication Requirements

Digital Identity Part 2 - Identity Proofing Requirements provides the requirements for identity providers (IdPs) for identity proofing on a person who wishes to use a service or conduct electronic transactions so that IdPs implement the same standards according to the identity assurance level (IAL).

Table of Contents

	Page
1. Scope	1
2. Identity Proofing	1
2.1 Collecting Identity Information	2
2.2 Validating Identity information	2
2.3 Verifying the Linkage Between the Person and the Identity	2
3. Identity Assurance Level: IAL	2
3.1 IAL1	2
3.2 IAL2	3
3.3 IAL3	3
4. Identity Proofing Requirements	3
4.1 Requirements for Collecting Identity Information	3
4.2 Requirements for Validating Identity Information	4
4.3 Requirements for Verifying the Linkage between a person and an Identity	7
4.3.1 Requirements for Biometric Comparison	8
4.4 Summary of the Key Requirements of Identity Proofing according to IAL	8
Appendix A. Infographic on Identity Assurance Levels (IAL)	14
Bibliography	15

Table Index

	Page
Table 1 Requirements for Collecting of Identity Information	4
Table 2 Requirements for Validating Identity Information	4
Table 3 Requirements for Verifying the Linkage between a person and an Identity	7
Table 4 Summary of the Key Requirements of Identity Proofing according to IAL	9

Electronic Transaction Standard

Digital Identity –

Part 2: Identity Proofing Requirements

1. Scope

This Standard is a requirement for identity providers (IdPs) to prove the identity of persons who wish to use services or conduct electronic transactions so that IdPs implement the same standards according to the identity assurance level (IAL).

This Standard is a requirement for agencies that provide identity proofing and authentication services to third parties. The requirements of this Standard can be applied to identity proofing and authentication services used for the benefit of one's own business. However, there is no intention to block or prohibit the use of other methods to increase the efficiency of identity verification and authentication.

This Standard uses the following forms of terminology to express the characteristics of normative and informative content:

- “shall” is used to identify requirements which must be followed.
- “should” is used to identify recommendations.
- “may” is used to identify permission.

2. Identity Proofing

Identity proofing is the process by which the IdP collects and validates person's identity information and verifies the linkage between the person and the identity information, with the aim of ensuring that the claimed identity is the true identity of that person according to a specified level of assurance. The expected results from identity proofing of persons who wish to have a digital ID for electronic transactions include:

- the ability to distinguish identity that claim to be unique and specific in the context of the transaction service;
- the ability to validate information related to the accuracy, correctness and current validity of the identity information;
- the ability to verify the linkage between the person who is undergoing identity proofing and the information about the claimed identity.

Identity proofing consists of 3 basic processes: [1]

2.1 Collecting Identity Information

Collecting identity information is the process by which the IdP collects identity information from identity evidence in order to distinguish whether the claimed identity is unique and specific within the context of the transaction service.

2.2 Validating Identity information

Identity information validation is the process by which the IdP checks the accuracy, correctness and current validity of information about the identity to prove that the claimed identity information is of the person who actually exists.

2.3 Verifying the Linkage Between the Person and the Identity

Verifying the linkage between the person and the identity is the process by which the IdP verifies the linkage between the person whose identity is being proofed and the claimed identity information to prove that the claimed identity is the true identity of the person whose identity is being proofed.

After the identity proofing is completed, the IdP will link the identity of the person who has passed the identity proofing with the authenticator. Individuals who have passed identity proofing will change their status to subscribers and receive the authenticator for further authentication

3. Identity Assurance Level: IAL

The Identity Assurance Level (IAL) is the level of assurance in the identity proofing process of a person. It is divided into 3 levels as follows:

3.1 IAL1

IAL1 may involve the collecting of identity information, which is self-asserted information. However, IAL1 may involve validating identity information or verifying the linkage between the person and the identity information by other means based on the risk of the transaction service in addition to the methods required at the IAL2 and IAL3 levels, such as:

- Checking a copy or photograph of identity evidence.¹

¹ In the case of a Thai national ID card (smart card), a copy or photo of only the face of the national ID card should be stored according to the recommendation of the Ministry of Interior. [5] A copy or photo of the reverse of the ID card should not be stored because the number on the reverse of the ID card (laser code) is information that may be used for authentication or to conduct transactions in some cases. If there is a leak of this information, it may cause damage to the subscriber.

- Checking the physical characteristics of identity evidence by an official.
- Validating the information of the identity evidence and validating the status of the identity evidence.
- Comparing the face or facial image of a person with the facial image of the identity evidence.
- Verifying the contact details of the person applying to use the service (e.g., phone number, email).

3.2 IAL2

IAL2 requires a request for identity evidence, validation of identity information that the claimed identity information of the person who actually exists, and verification of the linkage between the person whose identity is being proofed and the information about that identity. Identity proofing at the IAL2 can be done either face-to-face or non-face-to-face, such as identity proofing through kiosks or IdP applications.

An IdP that supports IAL2 can send an assertion that contains information about the identity of that person to an RP that requires the same or lower IAL if the consent of the person who owns the information is obtained.

In practice, the IAL2 is divided into 3 sub-levels, namely IAL2.1, IAL2.2 and IAL2.3, depending on consideration of the assurance of the method of validating identity information and the method of verifying the linkage between the person and the identity.

3.3 IAL3

IAL3 adds to the assurance of IAL2 by requiring additional verification of the existence of identity from authoritative sources in government agencies and the verification of the linkage between the person undergoing identity proofing and the identity information by biometric comparison to prevent impersonation and double registration. Identity proofing at IAL3 must be done face-to-face only.

An IdP that supports IAL3 can send an assertion that contains identity information of that person to an RP that requires the same or lower IAL level if the consent of the person who owns the information is obtained.

4. Identity Proofing Requirements

4.1 Requirements for Collecting Identity Information

The requirements for the collecting identity information according to IAL level can be seen in Table 1

Table 1 Requirements for Collecting of Identity Information

IAL	Requirements for Collecting Identity Information
IAL1	(1) The IdP <u>may</u> collect identity information, which is self-asserted information to be used to determine that the identity is unique and specific.
IAL2	(1) The IdP <u>shall</u> collect at least one piece of identity information from identity evidence to be used to determine that the identity is unique and specific. (2) An IdP that supports IAL2 can send an assertion that contains identity information of that person to an RP that requires the same or lower IAL level if the consent of the person who owns the information is obtained.
IAL3	(1) The IdP <u>shall</u> collect identity information from at least one piece of identity evidence and additionally from authoritative sources in government agencies (in addition to the registration database of the Department of Provincial Administration) to be used to determine that the identity is unique and specific. (2) An IdP that supports IAL3 can send an assertion that contains identity information of that person to an RP that requires the same or lower IAL level if the consent of the person who owns the information is obtained.

4.2 Requirements for Validating Identity Information

The requirements for validating identity information according to IAL can be seen in Table 2.

Table 2 Requirements for Validating Identity Information

IAL	Requirements for Validating Identity Information
IAL1	The IdP does not need to validate identity information.

IAL	Requirements for Validating Identity Information
IAL2.1	<p><u>In the case where a Thai national ID card (smart card) is used as identity evidence</u></p> <ol style="list-style-type: none"> (1) If there is an ID card reader, the IdP <u>shall</u> validate the identity information using the national ID card reader to compare the identity information with the identity information retrieved from the chip in the ID card. (2) If there is no ID card reader, the IdP <u>shall</u> validate the identity information using the information from the authentication result of an IdP who has previously conducted identity proofing of the person at IAL2.3 or higher. Submitting an assertion that contains identity information shall require the person to achieve at least AAL2 authentication. (3) The IdP <u>should</u> verify and confirm the contact details of the person who has applied to use the service, such as verifying the telephone number with the mobile service operator and verifying the contact details through a one-time password. (OTP) sent via SMS or email. <p><u>In the case where a passport is used as identity evidence</u></p> <ol style="list-style-type: none"> (1) The IdP <u>shall</u> validate identity information using near field communication (NFC) technology to compare the identity information with the retrieved identity information from the chip in the passport. (2) The IdP <u>should</u> validate and confirm the contact details of the person who has applied to use the service, such as verifying the telephone number with the mobile service operator and verify the contact details through a one-time password. (OTP) sent via SMS or email.
IAL2.2	<p><u>In the case where a Thai national ID card (smart card) is used as identity evidence</u></p> <ol style="list-style-type: none"> (1) If there is a national ID card reader, the IdP <u>shall</u> validate the identity information using the national ID card reader to compare the identity information with the identity information retrieved from the chip in the national ID card. (2) If there is no national ID card reader, the IdP <u>shall</u> validate the identity information using the information from the authentication result of an IdP who has previously verified the identity of the person at IAL2.3 or higher. Submitting an assertion that contains identity information shall require the person to perform at least AAL2 authentication. (3) The IdP <u>shall</u> validate the status of the ID card with the verification system of a government agency by using the chip number in the case where there is a national ID card reader, or using the number on the reverse of the ID card (laser code) in the case that there is no national ID card reader. (4) The IdP <u>should</u> verify and confirm the contact details of the person who has applied to use the service, such as verifying the telephone number with the mobile service

IAL	Requirements for Validating Identity Information
	<p>operator and verifying the contact details through a one-time password. (OTP) sent via SMS or email.</p> <p><u>In the case where a passport is used as identity evidence</u></p> <ol style="list-style-type: none"> (1) The IdP <u>shall</u> validate identity information using near field communication (NFC) technology to compare identity information with the retrieved identity information from the chip in the passport. (2) The IdP <u>shall</u> validate the status of the passport with authoritative sources, or validate other official identification documents issued by the Thai government or an agency of the state of the citizen (e.g. work permit, driver's license) or validate the status of the national ID card with the verification system of a government agency by using the number on the reverse of the national ID card (laser code). (3) The IdP <u>should</u> verify and confirm the contact details of the person who has applied to use the service, such as verifying the telephone number with the mobile service operator and verifying the contact details through a one-time password. (OTP) sent via SMS or email.
IAL2.3	<p><u>In the case where a Thai national ID card (smart card) is used as identity evidence</u></p> <ol style="list-style-type: none"> (1) If there is a national ID card reader, the IdP <u>shall</u> validate the identity information using the national ID card reader to compare the identity information with the identity information retrieved from the chip in the national ID card, and validate the status of the national ID card with the verification system of a government agency. (2) If there is no national ID card reader, the IdP <u>shall</u> validate the identity information on the national ID card and validate the status of the national ID card with the verification system of a government agency by using the number on the reverse of the ID card (laser code). In this case, the IdP <u>shall</u> conduct a biometric comparison by using the digital face verification service of only the Ministry of Interior. (3) The IdP <u>should</u> verify and confirm the contact details of the person who has applied to use the service, such as verifying the telephone number with the mobile service operator and verifying the contact details through a one-time password. (OTP) sent via SMS or email. <p><u>In the case where a passport is used as identity evidence</u></p> <p>The requirements are the same as for IAL2.2.</p>
IAL3	<p><u>In the case where a Thai national ID card (smart card) is used as identity evidence</u></p> <ol style="list-style-type: none"> (1) The IdP <u>shall</u> validate the identity information using the national ID card reader to compare the identity information with the identity information retrieved from the chip in the national ID card, and validate the status of the national ID card with the verification system of a government agency

IAL	Requirements for Validating Identity Information
	<p>(2) The IdP <u>shall</u> validate the existence of an identity from at least one authoritative source in a government agency in addition to the registration database of the Department of Provincial Administration.</p> <p>(3) The IdP <u>should</u> verify and confirm the contact details of the person who has applied to use the service, such as verifying the telephone number with the mobile service operator and verifying the contact details through a one-time password. (OTP) sent via SMS or email.</p>

4.3 Requirements for Verifying the Linkage between a person and an Identity

The requirements for verifying the linkage between a person and an identity according to IAL can be seen in Table 3.

Table 3 Requirements for Verifying the Linkage between a person and an Identity

IAL	Requirements for Verifying the Linkage between a person and an Identity
IAL1	The IdP does not need to verify the linkage between a person and an identity.
IAL2.1	<p>(1) Face-to-face or non-face-to-face identity proofing.</p> <p>(2) The IdP <u>shall</u> have an official conduct a visual comparison of a person's face or facial image with the facial image retrieved from the chip in the identity evidence of a government agency or the facial image from an IdP who has previously proofed the identity of the person at IAL2.3 or higher. Submission of a facial image shall require the person to perform at least AAL2 authentication.</p> <p>(3) In the case of non-face-to-face identity proofing, the IdP <u>shall</u> record the facial image of the person to prevent denial of identity verification or to be used for repeated identity proofing.</p>
IAL2.2	The requirements are the same as for IAL2.1
IAL2.3	<p>(1) Face-to-face or non face-to-face identity proofing.</p> <p>(2) The IdP <u>shall</u> use biometric comparison by using one of the following methods.</p> <p>(2.1) The IdP uses biometric technology to compare a person's facial image or fingerprints with the biometric data retrieved from a chip in the identity evidence of a government agency.</p> <p>(2.2) The IdP uses the face verification service of the Ministry of Interior to compare the facial image of a person with the biometric database.</p> <p>(3) In the case of non face-to-face identity proofing the IdP <u>shall</u> record a biometric sample of the person to prevent denial of identity or to be used for repeated identity proofing.</p>

IAL	Requirements for Verifying the Linkage between a person and an Identity
IAL3	<p>(1) Face-to-face identity proofing only.</p> <p>(2) The IdP <u>shall</u> use biometric comparison by using one of the following methods.</p> <p>(2.1) The IdP uses biometric technology to compare a person's facial image or fingerprints with the biometric data retrieved from a chip in the identity evidence of a government agency.</p> <p>(2.2) The IdP uses the face verification service of the Ministry of Interior to compare the facial image of a person with the biometric database.</p> <p>(3) The IdP <u>shall</u> record a biometric sample of the person to prevent denial of identity or to be used for repeated proofing.</p>

4.3.1 Requirements for Biometric Comparison

- (1) Biometric comparison shall be conducted in a one-to-one comparison between the biometric data of the person presenting and the biometric data from an identity evidence database or from a government agency, and not in a one-to-many comparison with a database containing biometric data of more than one person.
- (2) The accuracy of biometric comparison must not exceed a false match rate (FMR) of 0.01% and a false non-match rate (FNMR) not more than 3%. [2]
- (3) In the case of non face-to-face identity proofing, the IdP shall have a presentation attack detection technology such as liveness detection to help prevent spoofing attacks. IdPs can consider testing the capabilities of biometric spoofing detection technologies consistent or comparable to international standards such as ISO/IEC 30107 Information technology – Biometric presentation attack detection or FIDO Biometrics Requirements.

4.4 Summary of the Key Requirements of Identity Proofing according to IAL

The key requirements of identity proofing according to IAL are summarized in Table 4.

Table 4 Summary of the Key Requirements of Identity Proofing according to IAL

Identity Proofing Requirements	Non-face-to-face identity proofing					Face-to-face identity proofing				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
Collecting Identity Information										
Collect identity information, which is self-asserted information to be used to determine that the identity is unique and specific.	✓ (may)					✓ (may)				
Collect at least one piece of identity information from identity evidence to be used to determine that the identity is unique and specific.		✓ (shall)	✓ (shall)	✓ (shall)			✓ (shall)	✓ (shall)	✓ (shall)	
Collect identity information from at least one piece of identity evidence and additionally from authoritative sources in government agencies (in addition to the registration database of the Department of Provincial Administration) to be used to determine that the identity is unique and specific.										✓ (shall)
Validating of Identity Information										
<u>In the case where a Thai national ID card (smart card) is used</u> – <u>If there is a national ID card reader</u> , validate the identity information using the national ID card reader to compare the identity information with the identity information retrieved from the chip in the national ID card. – <u>If there is no national ID card reader</u> , validate the identity information using the information from the authentication result of an IdP who has previously verified the identity of the person at IAL2.3 or higher. Submitting assertion that		✓ (shall)	✓ (shall)				✓ (shall)	✓ (shall)		

ETS 11 Part 2-2566

Identity Proofing Requirements	Non-face-to-face identity proofing					Face-to-face identity proofing				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
contain identity information shall requires the person to perform at least AAL2 authentication.										
<u>In the case where a Thai national ID card (smart card) is used</u> – Validate the status of the ID card with the verification system of a government agency by using the chip number in the case where there is a national ID card reader, or using the number on the reverse of the ID card (laser code) in the case that there is no national ID card reader.			✓ (shall)					✓ (shall)		
<u>In the case where a Thai national ID card (smart card) is used</u> – <u>If there is a national ID card reader</u> , validate the identity information using the national ID card reader to compare the identity information with the identity information retrieved from the chip in the national ID card, and validate the status of the national ID card with the verification system of a government agency. – <u>If there is no national ID card reader</u> , validate the identity information on the national ID card and validate the status of the national ID card with the verification system of a government agency by using the number on the reverse of the ID card (laser code). In this case, the IdP <u>shall</u> conduct a biometric comparison by using the digital face verification service of only the Ministry of Interior.				✓ (shall)					✓ (shall)	

Identity Proofing Requirements	Non-face-to-face identity proofing					Face-to-face identity proofing				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
<u>In the case where a Thai national ID card (smart card) is used.</u> – Validate the identity information using a national ID card reader to compare the identity information with the identity information retrieved from the chip in the national ID card, and validate the status of the national ID card with the verification system of a government agency. – Validate the existence of an identity from at least one authoritative source in a government agency in addition to the registration database of the Department of Provincial Administration.										✓ (shall)
<u>In the case where a passport is used.</u> – validate identity information using the near field communication (NFC) technology to compare the identity information with the identity information retrieved from the chip in the passport.		✓ (shall)	✓ (shall)	✓ (shall)			✓ (shall)	✓ (shall)	✓ (shall)	
<u>In the case where a passport is used</u> – Validate the status of the passport with authoritative sources, or validate other official identification documents issued by the Thai government or an agency of the state of the citizen (e.g. work permit, driver's license) or validate the status of the national ID card with the verification			✓ (shall)	✓ (shall)				✓ (shall)	✓ (shall)	

Identity Proofing Requirements	Non-face-to-face identity proofing					Face-to-face identity proofing				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
system of a government agency by using the number on the reverse of the national ID card (laser code).										
Verify and confirm the contact details of the person who has applied to use the service, such as verifying the telephone number with the mobile service operator and verifying the contact details through a one-time password. (OTP) sent via SMS or email.		✓ (should)	✓ (should)	✓ (should)			✓ (should)	✓ (should)	✓ (should)	✓ (should)
Verifying the Linkage between a Person and an Identity										
Have an official conduct a visual comparison of a person's face or facial image with the facial image retrieved from the chip in the identity evidence of a government agency or the facial image from an IdP who has previously proofed the identity of the person at IAL2.3 or higher. Submission of a facial image shall require the person to perform at least AAL2 authentication.		✓ (shall)	✓ (shall)				✓ (shall)	✓ (shall)		
Use biometric comparison by using one of the following methods. – The IdP uses biometric technology to compare a person's facial image or fingerprints with the biometric data retrieved from a chip in the identity evidence of a government agency. – The IdP uses the face verification service of the Ministry of Interior to compare the facial image of a person with the biometric database.				✓ (shall)					✓ (shall)	✓ (shall)

Identity Proofing Requirements	Non-face-to-face identity proofing					Face-to-face identity proofing				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
Have a presentation attack detection technology such as liveness detection to help prevent spoofing attacks.				✓ (shall)						
Record the facial image or a biometric sample of the person to prevent denial of identity verification or to be used for repeated identity proofing.		✓ (shall)	✓ (shall)	✓ (shall)			✓ (may)	✓ (may)	✓ (may)	✓ (shall)

Appendix A. Infographic on Identity Assurance Levels (IAL)

Infographic of the Identity Assurance Levels (IAL) summarizing some of the key requirements from the standard to present information that can be easily understood.

Identity Assurance Level: IAL

Requirements for entities that provide identity proofing and validation services to third parties

Also applicable to agencies that proof and validate identities for use in their own businesses



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม



Identity Validation					Validating the Connection between the Person and the Identity		
IAL3	Using ID Card				Check and confirm contact channels e.g. phone number, email	Face-to-face only	Biometric Comparison
	Validate Information and Card Status (Use Chip Number) and Validate the identity from an additional government source						
IAL2	IAL2.3	In the case of using an ID card with a card reader	In the case of using an ID card without a card reader	In the case of using a passport	Face-to-face or Non-face-to-face	Biometric Comparison	
	IAL2.2	Validate Information and Card Status (Use Chip Number)	Validate Information and Card Status (Use Laser Code) and FVS	Validate Information Using NFC and ID Card Status (Use Laser Code) or Other Official Identification Documents			
	IAL2.1	Validate Information	Validate using information from IdP who has used IAL2.3 or higher	Validate Information Using NFC			
	IAL1	Identity information may be collected without the need to validate identity information or validate the connection between a person and an identity					

Note: Summary of some important requirements of the Standard

See more details about the Electronic Transaction Standards on Digital Identity – Part 2 Identity Proofing Requirements (ETS 11 Part 2-2566)

Bibliography

- [1] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing", June 2017.
- [2] Digital Transformation Agency, Australian Government, "Trusted Digital Identity Framework (TDIF): 05 - Role Requirements", Release 4.7, June 2022.
- [3] International Organization for Standardization, "ISO/IEC 29115:2013 Information technology – Security techniques – Entity authentication assurance framework", April 2013.
- [4] International Organization for Standardization, "ISO/IEC 30107-3:2017 Information technology – Biometric presentation attack detection – Part 3: Testing and reporting", September 2017.
- [5] Ministry of Interior Document No. M.I. 0309.2/W 6857 dated March 22, 2013, regarding the photocopying of Thai national ID cards (smart card).