ELECTRONIC TRANSACTION STANDARD

ETS 11 Part 1-2566

DIGITAL IDENTITY –
PART 1: FRAMEWORK

Electronic Transactions Development Agency

Ministry of Digital Economy and Society

ICS 35.030

ELECTRONIC TRANSACTION STANDARD

DIGITAL IDENTITY – PART 1: FRAMEWORK

ETS 11 Part 1-2566

Electronic Transactions Development Agency

The 9th Tower Grand Rama9 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 persons 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 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 1 - Framework is a document explaining the terminology, processes, risk assessment, and specifications of the assurance levels related to digital identity proofing and authentication to ensure that the understanding of those involved in digital identity proofing and authentication systems is the same.

Table of Contents

Table of Figures

Table Index

Electronic Transactions Standard

Digital Identity – Part 1: Framework

1. Scope

This Standard explains the terminology, processes, risk assessment, and specifications of the assurance levels related to digital identity proofing and authentication to ensure that the understanding of those involved in digital identity proofing and authentication systems is the same.

2. Definitions

The meaning of the terms used in this Standard is as follows.

2.1 "Identity proofing and authentication" means the process of proofing and authenticate the identity of a person. [1]

2.2 "Identity" means the unique characteristics which can indicate or distinguish a person by an attribute or set of attributes related to that person. [2]

Note 1: Examples of attributes related to a person include identification number, name, address, date of birth, email address, mobile phone number, facial image or information identifying a device used by the person.

Note 2: Examples of attributes related to a juristic person include juristic person registration number, name of juristic person, location of the head office, or names of the board members of the juristic person.

2.3 "Identity evidence" means physical documents or electronic data that can be used as evidence in identity proofing.

2.4 "Identity proofing" means the process of collecting and validating information about the identity of a person and verifying the linkage between the person and the information about that identity. [2]

2.5 "Authenticator" means something that is used to bind an identity with a person, which that person possesses and controls for the purpose of authentication, such as a password, biometric data, etc. [2]

2.6 "Authenticator management" means the process of binding the identity of a person who has undergone identity proofing with the authenticator and authenticator management. [2]

2.7 "Authentication" means the process of verifying a person's identity by determining the

validity of the authenticator of that person. [2]

2.8 "Identity provider" (IdP) means an agency that provides services to third parties in relation to identity proofing, the issuance and management of authenticators or authentication. An identity provider (IdP) may outsource some operations to a service provider or an agent of the IdP with the IdP taking responsibility in the same way as if they were themselves the operators.

2.9 "Relying party" (RP) means a person or agency that relies upon the assertion of authentication from an IdP or something used as an authenticator that the subscriber already has, in deciding to provide transaction services or grant access to a system.

2.10 "Authoritative source" (AS) means a source of information that provides information or prepares information rationally, with principles or references so that people or business groups can validate or confirm the information.

Note: Examples of authoritative sources include systems of government agencies to validate information related to identity.

2.11 "Subscriber" means a person who has undergone identity proofing and has received an authenticator to verify their identity.

2.12 "Identity assurance level" (IAL) means the level of security in the identity proofing process of a person.

2.13 "Authentication assurance level" (AAL) means the level of security in the authentication process of a person who possesses an authenticator.

3. Digital Identity Proofing and Authentication

3.1 Overview

Identity comprises the unique characteristics of a person that can indicate or distinguish that person by an attribute or a set of attributes related to that person, while digital identity is an identity recorded in an electronic format which the person can use for electronic transactions. The digital ID of each person must be unique to the context of a particular transaction service, but may not necessarily be unique in every context. However, some kinds of transaction services may not be strict in validating information abput the identity of the subscriber, for example email or online social media services, while for high-risk transaction services, such as financial services, the service provider must know the true identity of the subscriber to be used as a digital ID for electronic transactions.

Identity proofing is the process by which an IdP collects and validates information about the identity of a person and verifies the linkage between the person and the information about that identity. The objective is to ensure that the claimed identity is the real identity of that

person (e.g. the person claiming to be "Somchai" is the real "Somchai" and not another person in disguise). This Standard defines the security of the identity proofing process as a level known as the "identity assurance level (IAL)."

A person who has successfully completed identity proofing will becomes a "subscriber" and receive an authenticator to use in verifying their identity. When a subscriber wants to access the service or conduct an electronic transaction with a relying party (RP), which is a service provider who needs to know information about the identity of the subscriber before deciding to provide the transaction service, the RP will ask the IdP with whom the subscriber has previously undergone identity proofing and from whom the subscriber has received an authenticator, in order to assist in the authentication of the subscriber.

Authentication is the process of verifying the identity of a person by validating that person's authenticator, with the objective of ensuring that the person accessing the service actually possesses and controls the authenticator (e.g., the person who is accessing the service is the real "Somchai" who entered the correct password). This Standard specifies the level of security of the authentication process, known as the "authentication assurance level (AAL)".

When a subscriber is able to authenticate with the IdP that he or she actually possesses and controls the authenticator according to the specified protocol, the IdP will send the result of the identity authentication (assertion) to the RP for use in deciding to provide transaction services or grant access to the system. The assertion may consist of the result of validating the authenticator and information about the identity of the subscriber, such as identification number, name, date of birth, email address, mobile phone number, or other attributes collected in the identity proofing process, depending on the policy of the IdP, the requirements of the RP, and the consent to disclosure of the owner of the information.

3.2 Relationships among Relevant Parties

The relationships among those involved in identity proofing and identity authentication are shown as a diagram in Figure 1, where the left side of the figure is the identity proofing process and the right side is the authentication process.

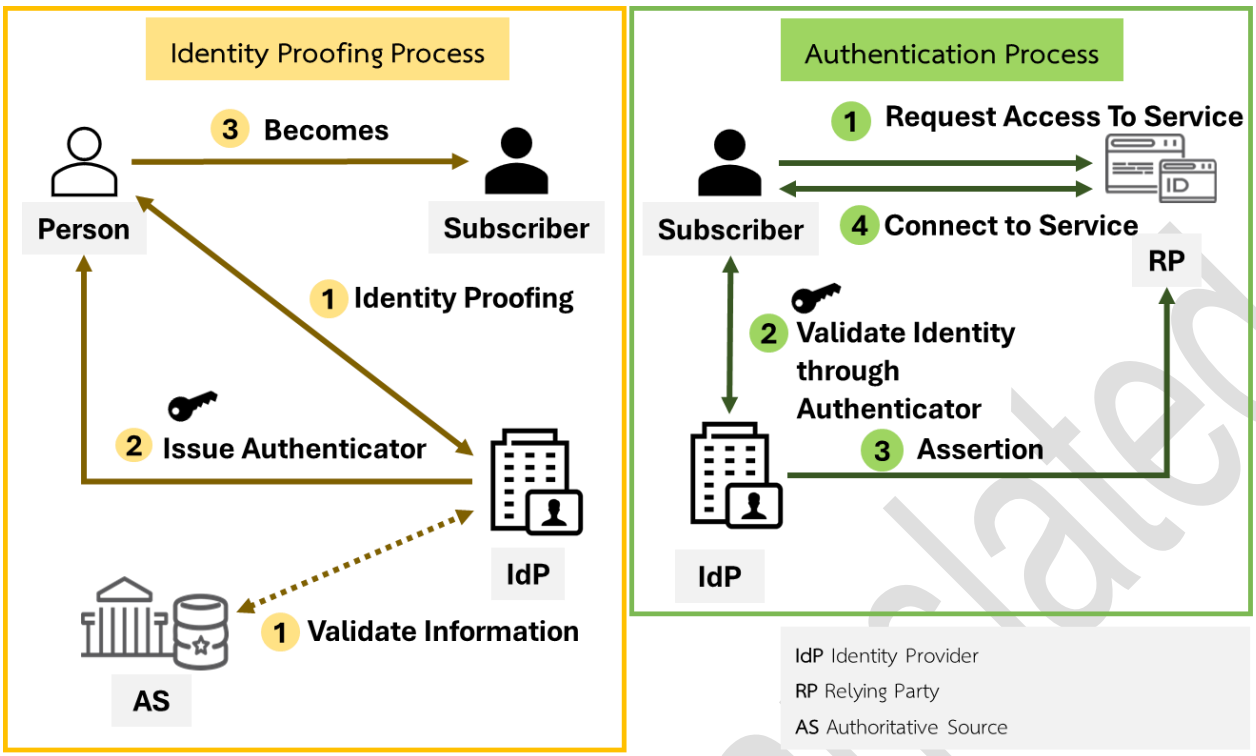

Figure 1 Relationships among those involved in identity proofing and identity authentication

The identity proofing process has the following general steps:

(1) A person wishing to have a digital ID for electronic transactions presents herself/himself to an IdP. The IdP will verify the identity of the person according to the specified IAL level, which may be done through validating identity evidence and information about the identity with an AS, as well as verifying the linkage between the person and that identity.

(2) If identity proofing is successful, the IdP will issue or register the authenticator and bind the identity of the person who has undergone identity proofing to that authenticator. The IdP is responsible for maintaining information about the identity, information about the binding of the identity with the authenticator, and the status of the authenticator throughout the lifetime of the authenticator.

(3) The person who has undergone identity proofing will become a subscriber and is responsible for securing his or her own authenticator.

The authentication process, which occurs when a subscriber wants to access the service or conduct an electronic transaction with an RP, has the following general steps:

(1) The subscriber requests access to the service or a transaction with RP using a digital ID with IAL and AAL levels corresponding to the RP's requirements.

(2) The RP redirects or advises the subscriber to authenticate their identity with the IdP with whom the subscriber has previously undergone identity proofing and has the

subscriber verify their identity with the IdP that he or she possesses and controls of the authenticator according to the specified protocol or AAL level.

(3) The IdP checks the validity and status of the authenticator then sends an assertion to the RP. The RP can use the data from the assertion in deciding to provide transaction services or grant access to the system to the subscriber.

(4) The RP connects with the subscriber to provide transaction services or access to the system.

The RP and IdP may be the same entity (in the case where the IdP issues the authenticator for use within the organization's business) or different entities (in the case where the IdP issues authenticators to provide services to third parties).

3.3 Authenticators

An authenticator is something used to bind an identity to a person, which that person possesses and controls in order to authenticate with an IdP. Every authenticator has at least one authentication factor. Authentication factors are divided into 3 types as follows:

(1) 'Something you know' is information that only the subscriber knows, such as password and PIN.

(2) 'Something you have' is an item that only the subscriber possesses, such as cryptographic key, out-of-band devices, and OTP device.

(3) 'Something you are' is the biometric data of the subscriber, such as facial image and fingerprint.

Authenticators may consist of only one authentication factor (single-factor authentication) or more than one authentication factor (multi-factor authentication). The security of the authentication system will depend on the number of authentication factors and the ability to prevent attacks on the authentication system. However, IdP or RP may use other information, such as location information or identification information for a device used by the person, to enhance the security of the authentication system. However, this information will not be considered as a authentication factor.

In 'non face-to-face' authentication, the subscriber must demonstrate that he or she possesses and controls the authenticator that is registered with the IdP to verify that he or she is the owner of the claimed identity because the authenticator will contain secret that only real subscribers can use for authentication. The secret information in the authenticator can be asymmetric keys or shared secret.

In the case where the secret is asymmetric keys consisting of a private key and a public key that are associated with each other, the subscriber will use the private key in the authenticator to verify his or her identity, while the IdP will use the public key associated

with the private key to verify that the subscriber possesses and controls the authenticator that has the private key. (Public keys are generally in the form of a public key certificate.)

When the secret is a shared secret, the secret in the authenticator may be symmetric keys or memorized secrets, with the difference that the symmetric keys are randomly selected from a system then stored in hardware or software that is controlled by the subscriber, while memorized secrets are the secrets that the subscriber must remember. Generally, encryption keys, whether they are symmetric keys or private keys, tend to have a longer character length than memorized secrets and therefore, have a complexity that is difficult to predict by attackers.

Note: Although identity evidence such as a national ID card or driver's license (something you have), which does not contain a secret in electronic form, can be used in face-to-face identity authentication with a person (such as a security guard), it cannot be used in non face-to-face identity authentication because a computer system does not have the information to validate or verify the identity of the subscriber.

Multi-factor authentication, in which more than one authentication factor is used, can be done in two ways:

(1) Using more than one authentication factor to directly authenticate one's identity with an IdP. For example, a subscriber must enter both a password (something you know) and secret sent to the subscriber's mobile phone via SMS (something you have) to verify his or her identity with the IdP.

(2) Using certain authentication factors to protect a secret before authentication with an IdP, such as the use of fingerprints (something you are). To protect the private key (something you have) on the mobile phone, subscribers must scan his or her fingerprints to enable the cryptographic software in the mobile phone to retrieve the private key for authentication with the IdP.

3.4 Assertion

If the authentication is successful, an IdP will send the authentication result (assertion) to a RP. The assertion may consist of the result of authenticator validation and information about the identity of the subscriber. The IdP may send the assertion directly to the RP through a protected channel to maintain the integrity of the assertion, or may send the assertion to the RP through the subscriber. The IdP must arrange a method to maintain the integrity of assertion to prevent alteration.

Whether the RP trusts the assertion depends on the source, the time of creation and the current status of the assertion, including the policies of the RP and IdP related to the reliability of identity proofing and authentication. In addition, the RP must verify the source (IdP) and

maintenance of the integrity of the assertion to ensure that the assertion is not altered during transmission from the IdP before the RP can use the assertion for further decisions.

If the assertion is transmitted through a public network, the IdP must have a method to maintain the confidentiality of the personal data of the subscriber which is contained in the assertion to ensure that only the designated RP can access the data.

3.5 Federated Identity Digital ID

A federated identity digital ID is a usage of a digital ID where the subscriber can allow an IdP to send the assertion related to the subscriber to an RP in a different system or different agency, and an RP may rely on assertions from more than one IdP. IdPs and RPs can be connected and exchange data with each other through a network or central system that provides technical facilitation in the connections and system configuration of IdPs, RPs and other related parties.

There are several benefits to using a federated identity digital ID, such as:

(1) The convenience for the subscriber is increased. The subscriber can verify their identity with a particular IdP and use the authenticator received from that IdP to authenticate his or her identity to access the service or conduct electronic transactions with multiple RPs.

(2) The costs to the RP in developing the technological infrastructure (e.g. managing user accounts and authenticators) and the burden on subscribers to own or maintain different authenticators for each RP are reduced, because RPs in the same group can all rely on the same authenticators or information about the identity of subscribers.

(3) It enables an agency to focus its operations directly on its core mission instead of conducting identity proofing and authentication operations.

4. Determining the Assurance Level

4.1 Overview

The risks associated with identity proofing and authentication according to this Standard are divided into two aspects: the risk of identity proofing failure (e.g. a person who comes to proof his or her identity impersonates the identity of another person or uses false identity evidence) and the risk of authentication failure (e.g. the person who presents an authenticator is not in fact the owner of the authenticator). The potential consequences of the failure of the identity proofing and authentication are that providing transaction services or granting access to the system to the wrong person.

As a result, service providers must assess the risks of identity proofing failure and authentication failure so that they can determine the appropriate assurance level for each transaction service and determine the processes and technologies to be used according to each assurance level.

4.2 Assurance Levels

Service providers should define assurance levels of identity proofing and authentication for each transaction service according to the transaction service's risk. This Standard divides assurance levels into 2 aspects as follows:

(1) Identity Assurance Level (IAL)

The identity assurance level is the level of security in the identity proofing process of a person. Determining the appropriate IAL level helps to reduce the chance of identity proofing failure. There are three IAL levels: IAL1 (lowest assurance), IAL2 and IAL3 (highest assurance).

Details comply with Electronic Transaction Standards, Digital Identity Verification – Volume 2, Identity Proofing Requirements.

(2) Authentication Assurance Level (AAL)

The authentication assurance level is the level of security in the authentication process of a person. Determining the appropriate AAL helps to reduce the chance of authentication failure. There are three AALs: AAL1 (lowest assurance), AAL2 and AAL3 (highest assurance).

Details comply with Electronic Transaction Standards, Digital Identity Verification – Volume 3, Identity Authentication Requirements.

4.3 Risk Assessment to Determine Assurance Level

A risk assessment to determine the IAL and AAL appropriate to each transaction service consists of two steps: (1) assessing the potential level of impact and (2) the association of the potential level of impact with the assurance level, as in following details.

(1) Step 1: Assessing the Possible Level of Impact

The assessment of potential impact is the consideration of the potential impact of identity proofing failure (for determining the IAL level) and the potential impact of authentication failure (for determining the AAL level).

Service providers should assess the risks and potential impacts of transaction services by considering the potential in accordance with the criteria of the regulatory agency for each type of transaction service, the risk management policy of the service

provider itself and the context in which the transaction service is used. However, service providers may consider the following 6 impact categories.

- Inconvenience and damage to reputation
- Financial loss
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

The assessment of the potential level of impact shall use a method of considering each aspect of the possible level of impact when a failure occurs, following Table 1.

Table 1 Criteria for evaluating the possible level of impact when a failure occurs

Impact Category	Possible level of impact when a failure occurs		
	Low	Moderate	High
Inconvenience and damage to reputation	Inconvenience and damage to reputation is short-term and limited.	Inconvenience and damage to reputation is severe short-term or moderate and long-term.	Inconvenience and damage to reputation is long term or impacts many persons.
Financial loss	Financial loss is insignificant.	Financial loss is severe.	Financial loss is very severe.
Damage to agency programs or public interests	Damage to agency program or public interest is limited.	Damage to agency program or public interest is severe.	Damage to agency program or public interest is very severe.
Unauthorized release of sensitive information	The release of confidential personal or commercial information to unauthorized parties has a low impact.	The release of confidential personal or commercial information to unauthorized parties. has a moderate impact.	The release of confidential personal or commercial information to unauthorized parties has a high impact.
Personal safety	Minor injuries, not requiring medical treatment.	Moderate risk of minor injury or limited risk of injury requiring medical treatment.	There is a risk of serious injury or death.

Impact Category	Possible level of impact when a failure occurs		
	Low	Moderate	High
Civil or criminal violations	The violation of the law is minor, not subject to enforcement efforts.	The violation of the law risks being subject to enforcement efforts.	The violation of the law has a high risk of being subject to enforcement efforts.

(2) Step 2: Association of Possible Levels of Impact with Assurance Levels

The results of the assessment of the possible level of impact of identity proofing failure and authentication failure from step 1 are linked to the IAL and AAL assurance levels, respectively. The appropriate IAL and AAL assurance levels are the levels that cover all possible impacts, as shown in Table 2.

Table 2 Possible impact level and required assurance level

Impact Category	Required Assurance Level		
	1	2	3
Inconvenience and damage to reputation	Low	Moderate	HIgh
Financial loss	Low	Moderate	HIgh
Damage to agency programs or public interests	N/A	Low/Moderate	HIgh
Unauthorized release of sensitive information	N/A	Low/Moderate	HIgh
Personal safety	N/A	Low	Moderate/HIgh
Civil or criminal violations	N/A	Low/Moderate	HIgh

4.4 Example of determining the level of assurance

An example of determining IAL and AAL of an RP has the following steps

(1) Determining the IAL

(1.1) Step 1: Assess the level of possible impact of identity proofing failure in the following example of assessment results.

Impact Category	Level of Impact
Inconvenience and damage to reputation	Low
Financial loss	Low
Harm to agency programs or public interests	N/A
Unauthorized release of sensitive information	N/A
Personal safety	N/A
Civil or criminal violations	N/A

(1.2) Step 2: Link the results of possible impact level to assurance level.

Impact Category	Required Assurance Level		
	1	2	3
Inconvenience and damage to reputation	Low	Moderate	HIgh
Financial loss	Low	Moderate	HIgh
Damage to agency programs or public interests	N/A	Low/Moderate	HIgh
Unauthorized release of sensitive information	N/A	Low/Moderate	HIgh
Personal safety	N/A	Low	Moderate/HIgh
Civil or criminal violations	N/A	Low/Moderate	HIgh

By connecting the level of possible impact (from Step 1) with the assurance level, it is found that the assurance level covering all possible effects is level 1. Therefore, the appropriate IAL in this example is level IAL1.

(2) Determing the AAL

(2.1) Step 1: Assess the level of possible impact of authetntication failure in the following example of assessment results.

Impact Category	Level of Impact
Inconvenience and damage to reputation	Low
Financial loss	Low
Damage to agency programs or public interests	Low
Unauthorized release of sensitive information	Moderate
Personal safety	N/A

Impact Category	Level of Impact
Civil or criminal violations	Low

(2.2) Step 2: Link the results of possible impact level to the assurance level.

Impact Category	Required Assurance Level		
	1	2	3
Inconvenience and damage to reputation	Low	Moderate	HIgh
Financial loss	Low	Moderate	HIgh
Harm to agency programs or public interests	N/A	Low/Moderate	HIgh
Unauthorized release of sensitive information	N/A	Low/Moderate	HIgh
Personal safety	N/A	Low	Moderate/HIgh
Civil or criminal violations	N/A	Low/Moderate	HIgh

By connecting the level of possible impact (from Step 1) with the assurance level, it is found that the assurance level covering all possible effects is level 2. Therefore, the appropriate AAL in this example is AAL2.

Appendix A. Acronym

Acronym	Description
IdP	identity provider
RP	relying party
AS	authoritative source
IAL	identity assurance level
AAL	authentication assurance level
PIN	personal identification number
OTP	one-time password
FMR	false match rate
FNMR	false non-match rate

Bibliography

[1] Electronic Transactions Act B.E. 2544 (Revised Edition).

[2] Royal Decree on Supervision of Service Businesses Relating to Digital Identification and Authentication Systems that are Subject to Licensing B.E. 2565.

[3] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-63-3, Digital Identity Guidelines", June 2017.

[4] International Organization for Standardization, "ISO/IEC 29115:2013 Information technology – Security techniques – Entity authentication assurance framework", April 2013.

[5] Digital Transformation Agency, Australian Government, "Trusted Digital Identity Framework (TDIF): 01 - Glossary of Abbreviations and Terms", Release 4.6, March 2022.