ELECTRONIC TRANSACTION STANDARD

ETS 11 Part 3-2566

DIGITAL IDENTITY –
PART 3: AUTHENTICATION REQUIREMENTS

Electronic Transactions Development Agency

Ministry of Digital Economy and Society

ICS 35.030

ELECTRONIC TRANSACTION STANDARD

DIGITAL IDENTITY – PART 3: AUTHENTICATION REQUIREMENTS

ETS 11 Part 3-2566

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 authenticatethe 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, 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 3 - Authentication Requirements gives the requirements for identity providers (IdPs) for the management of authenticators and subscriber authentication so that the IdPs implement the same standards according to the Authentication Assurance Level (AAL).

Table of Contents

Page

1. Framework **1**

2. Authentication Assurance Level: AAL **1**

2.1 AAL1 2

2.2 AAL2 2

2.3 AAL3 3

2.4 Summary of the Key Requirements of Authentication according to AAL 4

3. Requirements according to Type of Authenticator **5**

3.1 Memorized Secret 5

3.2 Out-of-Band Device 6

3.3 Single-Factor OTP Device 7

3.4 Multi-Factor OTP Device 8

3.5 Single-Factor Cryptographic Software 9

3.6 Single-Factor Cryptographic Device 9

3.7 Multi-Factor Cryptographic Software 10

3.8 Multi-Factor Cryptographic Device 11

4. General Requirements for Authenticators **12**

4.1 Authenticator Devices (‘Something You Have’ Type) 12

4.2 Limits on the Number of Authentication Failures 12

4.3 Use of Biometrics (Registration only with an Authenticator that is a Device) 13

4.4 Replay Resistance 14

4.5 IdP Impersonation Resistance 14

5. Authenticator Lifecycle Management **15**

5.1 Authenticator Binding 15

5.2 Loss, Theft, Damage, and Replacement 16

5.3 Expiry and Renewal 16

5.4 Revocation 17

Bibliography **19**

Table Index

Page

Table 1 Summary of the Key Requirements of Authentication according to AAL 4

Electronic Transaction Standard

Digital Identity –

Part 3: Authentication Requirements

1. Framework

This Standard is a requirement for identity providers (IdPs) to manage authenticator and subscriber authentication so that IdPs implement the same standards according to the Authentication Assurance Level (AAL).

This Standard is a requirement for agencies that provide third-party identity verification and authentication services. The requirements of this Standard can be applied to identity verification 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.

AALs in this Standard define the types of face-to-face authenticators and authentication protocols by considering their characteristics in preventing cyberattacks that may occur mainly through online channels, such as man-in-the-middle attacks and replay attacks. For this reason, face-to-face authentication whose characteristics and criteria cannot be used to determine AALs through online channels is not within the scope of this Standard. In the event that an IdP wishes to provide face-to-face authentication services, an appropriate authentication method shall be used according to the requirements of the relying party (RP).

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. Authentication Assurance Level: AAL

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

2.1 AAL1

AAL1 provides a certain level of assurance that the person accessing the service is in possession and control of the subscriber's authenticator. AAL1 requires the use of at least single-factor authentication. The fact that the subscriber is in possession and control of the authenticator shall be demonstrated by a secure authentication protocol.

Types of authenticators which can be used

AAL1 authentication shall use a type of authenticator from the following list:

(1) Memorized secret
(2) Out-of-band device
(3) Single-factor OTP device
(4) Single-factor cryptographic software
(5) Single-factor cryptographic device
(6) Other types of authenticators for AAL2 and AAL3

Important requirements

(1) Communication between the subscriber and the IdP shall be through an authenticated protected channel to maintain the confidentiality of the results used for authentication identity and to prevent man-in-the-middle attacks.

2.2 AAL2

AAL2 provides a high level of confidence that the person accessing the service is in possession and control of the authenticator of the subscriber. AAL2 requires authentication with at least 2 different authentication factors. The fact that the subscriber possesses and controls two different authentication factors must be demonstrated by a secure authentication protocol.

Notes Authentication with 2 different authentication factors can be done in 2 ways:

(1) Using 2 different single-factor authenticators, such as entering a password (something you know) and confidential information sent to the subscriber's mobile phone via SMS (something you have) for identity authentication.
(2) Using one multi-factor authenticator, such as a multi-factor OTP device, which will generate a one-time password (OTP). After the subscriber successfully enters his or her PIN or scans his or her fingerprint, the subscriber enters the OTP displayed on his or her device for identity authentication.

Types of authenticators which can be used

AAL2 authentication shall use a type of authenticator from the following list:

(1) Multi-factor OTP device
(2) Multi-factor cryptographic software

(3) A memorized secret used in conjunction with an out-of-band device.
(4) A memorized secret used in conjunction with a single-factor OTP device
(5) A memorized secret used in conjunction with single-factor cryptographic software.
(6) Other types of authenticators for level AAL3

Important requirements

(1) Communication between the subscriber and the IdP shall be through an authenticated protected channel to maintain the confidentiality of the results used for authentication identity and to prevent man-in-the-middle attacks.

(2) At least one authenticator shall be able to prevent replay attacks.

(3) When a device such as a mobile phone is used for authentication, unlocking the device (e.g. by using a PIN or biometrics) shall not be considered as one of the authentication factors, as the IdP will not be able to know if the device is locked or if the unlocking process meets the requirements of that kind of authenticator.

2.3 AAL3

The AAL3 provides a very high level of confidence that the person accessing the service is in possession and control of the authenticator of the subscriber. The AAL3 requires authentication with at least 2 different authentication factors, and the authenticator that is used is hardware-based, containing a cryptographic key, and can prevent IdP impersonation.

The fact that the subscriber possesses and controls two different authentication factors must be demonstrated by a secure authentication protocol, and also the fact that the subscriber possesses and controls the cryptographic key must be demonstrated by a cryptographic protocol.

Types of authenticators which can be used

AAL3 authentication shall use a type of authenticator from the following list:

(1) Multi-factor cryptographic device
(2) Single-factor cryptographic device used in conjunction with a memorized secret.
(3) Multi-factor OTP device used in conjunction with a single-factor cryptographic device
(4) Multi-factor OTP device (hardware only) used in conjunction with single-factor cryptographic software
(5) Single-factor OTP device (hardware only) used in conjunction with multi-factor cryptographic software
(6) Single-factor OTP device (hardware only) used in conjunction with single-factor cryptographic software and a memorized secret

Important requirements

(1) Communication between the subscriber and the IdP shall be through an authenticated protected channel to maintain the confidentiality of the results used for authentication identity and to prevent man-in-the-middle attacks.

(2) An authenticator shall be able to prevent replay attacks.

(3) An authenticator shall be able to prevent IdP impersonation

(4) When a device such as a mobile phone is used for authentication, unlocking the device (e.g. by using a PIN or biometrics) shall not be considered as one of the authentication factors, as the IdP will not be able to know if the device is locked or if the unlocking process meets the requirements of that kind of authenticator.

2.4 Summary of the Key Requirements of Authentication according to AAL

The key requirements for each level of authentication can be summarized in Table 1.

Table 1 Summary of the Key Requirements of Authentication according to AAL

Authentication requirements	AAL		
	AAL1	AAL2	AAL3
Types of authenticators that can be used	Type of authenticator from the following options. (1) memorized secret (2) out-of-band device (3) SF OTP device (4) SF crypto software (5) SF crypto device (6) Other types of authenticator at AAL2 and AAL3	Type of authenticator from the following options. (1) MF OTP device (2) MF crypto software (3) memorized secret **+** out-of-band device (4) memorized secret **+** SF OTP device (5) memorized secret **+** SF crypto software (6) Other types of authenticator at AAL3	Type of authenticator from the following options. (1) MF crypto device (2) SF crypto device **+** memorized secret (3) MF OTP device **+** SF crypto device (4) MF OTP device (hardware only) + SF crypto software (5) SF OTP device (hardware only) + MF crypto software (6) SF OTP device (hardware only) + SF cryptosoftware + memorized secret

Authentication requirements	AAL		
	AAL1	AAL2	AAL3
Man-in-the-middle resistance	✓	✓	✓
Replay resistance)		✓	✓
IdP impersonation resistance			✓

Note: SF stands for “single-factor”, MF stands for “multi-factor” and crypto stands for “cryptographic”

3. Requirements according to Type of Authenticator

The types of authenticators that the IdP can issue or register for subscribers to use for authentication according to AAL are as follows.

(1) Memorized secret
(2) Out-of-band device
(3) Single-factor OTP device
(4) Multi-factor OTP device
(5) Single-factor cryptographic software
(6) Single-factor cryptographic device
(7) Multi-factor cryptographic software
(8) Multi-factor cryptographic device

3.1 Memorized Secret

A memorized secret, commonly known as a password or personal identification number (PIN), is a secret that is memorized by a subscriber. Memorized secrets must be complex at a level that is difficult for to predict.

A memorized secret is a ‘something you know’ authentication factor.

Technical requirements

(1) A personal identification number (PIN) registered with a specific device shall be at least 6 digits long, while the password shall have at least 8 characters.

(2) IdPs should make a blacklist of memorized secrets which subscribers are prevented from choosing, such as passwords that have been attacked in the past, words found in the dictionary, repeated or sequential characters, and easily predictable words.

(3) IdPs should provide instructions for subscribers to choose a memorized secret that is difficult to guess, such as a measurement of password safety.

(4) IdPs shall set a limit on the number of authentication errors as specified in Section 4.2.

3.2 Out-of-Band Device

An out-of-band device is a device that can communicate securely with an IdP through a secondary channel, which is separate from the primary channel used for authentication.

An out-of-band device is a 'something you have' authentication factor.

An out-of-band device can work in one of the following ways.

(1) Subscribers receive secret information from an out-of-band device through a secondary communication channel, and send that secret to the IdP using the primary communication channel. For example, a subscriber receives a 6-digit secret sent to a mobile phone via SMS and enters that secret in the authentication window.

(2) Subscribers receive secret through the primary communication channel and use an out-of-band device to transmit the secret to the IdP through a secondary communication channel. For example, a subscriber sees secret information displayed as a QR code in the authentication window and scans the QR code with a mobile phone to send the secret information to the IdP.

Technical requirements

(1) An out-of-band device shall create a secondary communication channel that is separate from the primary communication channel to receive or transmit the secret to the IdP. Devices at the endpoints used to communicate with the IdP through the primary and secondary communication channels may be the same. The device shall not cause data leakage from one channel to another without the permission of the subscriber.

(2) Methods that cannot demonstrate that the subscriber owns and controls a specific device, such as voice-over-IP (VoIP) or email-based methods, shall not be considered an authentication method with an out-of-band device.

(3) An out-of-band device shall authenticate the device's identity with the IdP by one of the following methods.

(3.1) Create an authenticated protected channel with the IdP using a cryptographic process where the cryptographic key shall be stored in appropriate secure storage, such as keychain storage, trusted platform module (TPM), trusted execution environment (TEE), or secure element (SE).

(3.2) Authenticate the identity of the device through the public telephone network using a SIM card or other method that can identify the device. This method shall only be used if the IdP sends the secret information to an out-of-band device only through the public telephone network.

(4) Authentication of the subscriber shall use one of the following methods.

(4.1) Sending a secret to the IdP via the main communication channel: the IdP shall send randomly generated secret to an out-of-band device and then shall wait for a reply with the secret on the main communication channel.

(4.2) Sending a secret to the IdP via the secondary communication channel: the IdP shall display the randomly generated secret to the subscriber on the main communication channel, and then the IdP shall wait for a response with the secret from the out-of-band device of the subscriber through the secondary communication channel.

(5) Randomly generated secret shall have a length of at least 6 digits.

(6) The IdP shall set a period of time for replying to the secret from the subscriber to not exceed 10 minutes. If the specified period of time is exceeded, the authentication will be considered as invalid.

(7) The IdP shall accept only one reply with the secret from the subscriber during the specified period of time to prevent replay attacks.

(8) The IdP shall set a limit to the number of authentication errors as specified in Section 4.2.

3.3 Single-Factor OTP Device

A single-factor OTP device is a specific piece of hardware or software installed on a device (such as a mobile phone) to generate an OTP. The subscriber will enter the OTP displayed on the device on the authentication window of the IdP to show that he or she really possesses and controls the device.

A single-factor OTP device contains two data values for generating an OTP: (1) a symmetric key, which has a constant value over the life of the device, and (2) a nonce, which will change in value each time the device is used or change in value according to the current time.

A single-factor OTP device is a ‘something you have’ authentication factor.

Technical requirements

(1) An OTP shall be at least 6 digits long.

(2) If the nonce value used to generate the OTP changes according to the current time, the nonce value shall change at least every 2 minutes, and the IdP shall accept OTPs generated from the nonce value only once during a given period of time to prevent replay attacks.

(3) The IdP shall set a limit to the number of authentication errors as specified in Section 4.2.

3.4 Multi-Factor OTP Device

A multi-factor OTP device is a specific piece of hardware or software installed on a device (e.g., a mobile phone) that generates an OTP after the subscriber successfully authenticates their identity using a second authentication factor (e.g., entering a personal identification number (PIN) or scanning a fingerprint). The subscriber will fill in the OTP displayed on the device in the IdP's authentication window to show that he or she actually possesses and controls the device.

Similar to a single-factor OTP device, a multi-factor OTP device contains two data values for generating an OTP: (1) a symmetric key, which has a constant value over the life of the device, and (2) a nonce value, which will change in value each time the device is used or change in value according to the current time.

A multi-factor OTP device is a 'something you have' authentication factor and generates an OTP after the subscriber verifies their authentication using the second authentication factor, which is something you know or something you are.

Technical requirements

(1) Authentication with a multi-factor OTP device shall each time use 2 authentication factors.

(2) The second authentication factor shall be a memorized secret or biometric data.

(3) In the case where the second authentication factor is a memorized secret, the memorized secret shall be at least 6 digits in length or as required in Section 3.1.

(4) In the case where the second authentication factor is biometric data, the use of biometric data shall be as required in Section 4.3.

(5) An OTP shall be at least 6 digits long.

(6) In the case where the nonce value that is used for generating the OTP changed according to the current time, the nonce value shall change at least every 2 minutes, and the IdP shall accept OTP generated from the nonce value only once during a given period of time to prevent replay attacks.

(7) The IdP shall set a limit to the number of authentication errors as specified in Section 4.2.

3.5 Single-Factor Cryptographic Software

Single-factor cryptographic software is a cryptographic key that is stored on a hard disk or other form of storage media.

Authentication with single-factor cryptographic software is done by showing that the subscriber possesses and controls the cryptographic key through a cryptographic protocol. For example, the subscriber digitally signs the nonce value sent from the IdP with the cryptographic key and sends the results to the IdP for verification to show that he or she actually possesses and controls the cryptographic key.

Single-factor cryptographic software is a 'something you have' authentication factor.

Technical requirements

(1) Cryptographic keys shall be stored in appropriate secure storage, such as keychain storage, a trusted platform module (TPM), a trusted execution environment (TEE), or a secure element (SE).

(2) The cryptographic key shall be protected from unauthorized disclosure by using access control, which allows only specific software to access cryptographic keys.

(3) The cryptographic key and the algorithm used shall comply with the minimum requirements of the NIST Standard Special Publication 800-131A Rev. 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths.

3.6 Single-Factor Cryptographic Device

A single-factor cryptographic device is a device that uses a cryptographic key embedded within the device to generate an assertion and send the assertion to an endpoint via a direct connection (e.g. a computer's USB port).

Authentication with a single-factor cryptographic device is achieved by demonstrating that the subscriber possesses and controls the cryptographic device by a cryptographic protocol. For example, the subscriber digitally signs the nonce value sent from the IdP with a cryptographic device and sends the results to the IdP for verification to show that he or she actually possesses and controls the cryptographic device.

The difference between a cryptographic device and cryptographic software is that all software embedded within a cryptographic device is regulated by the IdP or device manufacturer.

A single-factor cryptographic device is a 'something you have' authentication factor.

Technical requirements

(1) The cryptographic key shall not be removed from the cryptographic device.

(2) The encryption key shall be protected from unauthorized disclosure.

(3) A single-factor cryptographic device shall comply with at least FIPS 140-2 Security Requirements for Cryptographic Modules at Level 1.

(4) The cryptographic key and the algorithm used shall comply with the minimum requirements of the NIST Standard Special Publication 800-131A Rev. 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths.

3.7 Multi-Factor Cryptographic Software

Multi-factor cryptographic software is a cryptographic key stored on a hard disk or other form of storage that can be used after the subscriber is successfully authenticated by using a second authentication factor (e.g. entering a personal PIN or scanning a fingerprint).

Authentication with multi-factor cryptographic software achieved by showing that the subscriber possesses and controls the cryptographic key through a cryptographic protocol. For example, the subscriber digitally signs the nonce value sent from the IdP with the cryptographic key and sends the result to the IdP for verification to show that he or she actually possesses and controls the cryptographic key.

Multi-factor cryptographic software is a 'something you have' authentication factor and will be available after the subscriber is authenticated using a second authentication factor, which is of the 'something you know' or 'something you are' type.

Technical requirements

(1) Each multi-factor cryptographic software authentication shall use both authentication factors.

(2) The second authentication factor shall be a memorized secret or biometric data.

(3) In the case where the second authentication factor is a memorized secret, the memorized secret shall be at least 6 digits in length, or as defined in Section 3.1, and there shall be a limit on the number of consecutive authentication failures as defined in Section 4.2.

(4) In the case where the second authentication factor is biometric information, the use of biometric information shall be as specified in Section 4.3.

(5) Cryptographic keys should be stored in appropriate secure storage, such as keychain storage, a trusted platform module (TPM), a trusted execution environment (TEE), or a secure element (SE).

(6) The cryptographic key shall be protected from unauthorized disclosure using access control, which allows only specific software to access the cryptographic key.

(7) The cryptographic key and the algorithm used shall comply with the minimum requirements of the NIST Standard Special Publication 800-131A Rev. 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths.

3.8 Multi-Factor Cryptographic Device

A multi-factor cryptographic device is a device that uses a cryptographic key embedded within the device to generate an assertion and send the assertion to an endpoint via a direct connection (e.g. a computer's USB port). The cryptographic key will be available after the subscriber has successfully been authenticated using a second authentication factor (e.g. entering a PIN or scanning a fingerprint).

Authentication by a multi-factor cryptographic device is achieved by demonstrating that the subscriber possesses and controls the cryptographic device using a cryptographic protocol. For example, the subscriber digitally signs the nonce value sent from the IdP with the cryptographic device and sends the result to the IdP for verification to show that he or she actually possesses and controls the cryptographic device.

The difference between a cryptographic device and cryptographic software is that all software embedded within a cryptographic device is regulated by the IdP or device manufacturer.

A multi-factor cryptographic device is a ‘something you have’ authentication factor and will be available after the subscriber is authenticated using the second authentication factor, which is of the ‘something you know’ or ‘something you are’ type.

Technical requirements

(1) Each authentication with a multi-factor cryptographic device shall use both authentication factors.

(2) The second authentication factor shall be a memorized secret or biometric information.

(3) In the case where the second authentication factor is a memorized secret, the memorized secret shall be at least 6 digits in length, or as specified in Section 3.1, and there shall be a limit on the number of consecutive authentication failures as specified in Section 4.2.

(4) In the case where the second authentication factor is biometric information, the use of biometric information shall be as specified in Section 4.3.

(5) The cryptographic key shall not be removed from the cryptographic device.

(6) The cryptographic key shall be protected from unauthorized disclosure

(7) The multi-factor cryptographic device shall comply with FIPS 140-2 Security Requirements for Cryptographic Modules to at least Level 2.

(8) The cryptographic key and the algorithm used shall comply with the minimum requirements of the NIST Standard Special Publication 800-131A Rev. 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths.

4. General Requirements for Authenticators

4.1 Authenticator Devices ('Something You Have' Type)

The IdP shall provide recommendations to the subscriber on ways to protect the authenticator from being lost or stolen and shall have a mechanism to revoke or suspend the use of the authenticator immediately after being notified by the subscriber that the authenticator has been lost or stolen.

4.2 Limits on the Number of Authentication Failures

In the case where the type of authenticator requires the IdP to set a limit on the number of authentication failures, the IdP shall have a process to protect against online guessing attack, such as random guessing of a memorized secret. The IdP must limit the number of consecutive authentication failures by a subscriber (for example no more than 100 times). If the specified number is exceeded, the IdP should suspend the authentication of the subscriber.

To reduce the chance of attacks that will cause subscribers to be suspended due to consecutive authentication errors in excess of the specified number, the IdP may choose the following methods.

(1) The subscriber is required to pass a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) before authentication.

(2) The subscriber is required to wait for a period of time after an incorrect authentication, and the delay will increase each time the subscriber submits a consecutive authentication error (e.g. from 30 seconds to 1 hour according to the number of authentication failures).

(3) Only authentication from the IP address from which the subscriber has already been successfully authenticated is accepted.

When a subscriber successfully authenticates their identity, the IdP should disregard previous authentication errors of the subscriber that come from the same IP address.

4.3 Use of Biometrics (Registration only with an Authenticator that is a Device)

The use of biometrics such as facial images, fingerprints, and irises in authentication is considered a 'something you are' type of authentication factor. Authenticators that can support the use of biometrics for multi-factor authentication consist of multi-factor OTP devices, multi-factor cryptographic software, and multi-factor cryptographic devices.

The use of biometrics in authentication is still limited due to the following reasons. [1]

(1) The use of biometrics has a false match rate (FMR), which creates uncertainty whether the person authenticating their identity is the real subscriber or may have been attacked by using a false facial image or fingerprints (spoofing attack).

(2) Biometric comparison is based on probability while other types of authentication factors are deterministic comparisons that clearly show if the data is the same or not.

(3) Methods of revoking biometric data are still limited with regard to availability and test standards.

(4) Biometrics are not considered confidential data because attackers can steal a person's biometrics by searching for online data or taking photos of a person with a phone camera (in the case of a face), deceiving a person into touching an object with their hands (in the case of fingerprints), or high-resolution photography (in the case of irises).

For these reasons, the use of biometrics in authentication carries the following requirements:

(1) Biometrics shall be used as a co-factor of multi-factor authentication and registered for use only in conjunction with an authenticator device (of the 'something you have' type) because if the subscriber is detected to be fake or suspected of abuse, the IdP can revoke the authenticator device instead of revoking biometric data, which is limited.

(2) Biometric data comparisons can be performed on the subscriber's device or on the IdP's system. If the biometric data comparison is performed on the IdP's system, the biometric data shall be transmitted between the sensor and the IdP through an authenticated protected channel.

(3) The accuracy of biometric data comparison shall have a false match rate (FMR) not exceeding 0.01% and a false non-match rate (FNMR) not exceeding 3%. [2]

(4) IdPs 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 that are consistent with or comparable to international standards such as ISO/IEC 30107 Information technology – Biometric presentation attack detection or FIDO Biometrics Requirements.

(5) The IdP may limit the number of consecutive biometric authentication failures (e.g. no more than 10 times). If the specified number is exceeded, the IdP may choose to use the following methods.

(5.1) Require a delay in the period of time before the subscriber attempts authentication again and the delay will increase each time the subscriber makes a consecutive authentication error (e.g. increases from 30 seconds to 1 hour according to the number of authentication errors).

(5.2) Suspend the biometric authentication of the subscriber and offer to the subscriber authentication with another type of authenticator (if any).

4.4 Replay Resistance

The authentication process can protect against replay attacks. If previous assertions are saved and replayed, authentication cannot be achieved. Replay resistance is an additional operation in an authenticated protected channel communication because the results used for authentication can be stolen by bad actors before they are sent by the protected channel.

An authenticator that uses a nonce value to prove the freshness of the results used for authentication has the property of protecting against replay attacks because the IdP can immediately detect that the result that does not have the appropriate nonce value and is a result used for a previous authentication and resubmitted.

Authenticators which have replay resistance properties include out-of-band devices, OTP devices, cryptographic software and cryptographic devices, while memorized secrets do not have replay resistance properties because the memorized secret is reused for each authentication.

4.5 IdP Impersonation Resistance

An IdP impersonation attack, also known as a phishing attack, tricks subscribers into verifying their identity on a fake IdP website.

An authentication process that protects against IdP impersonation shall create an authenticated protected channel with the IdP and shall connect the channel identifier of the authenticated protected channel with the result used for authentication by using the subscriber's private key to digitally sign the two data. The IdP shall then verify the digital signature with a corresponding public key to verify the identity of the subscriber. In this way

the fake IdP will not be able to apply the digital signature to verify the identity of the real IdP because the channel has a different channel identifier.

Authenticators which do not have IdP impersonation resistance properties include memorized secrets, out-of-band devices, and OTP devices because these authenticators allow subscribers themselves to enter the results of idP authentication. Entering the authentication results when the subscriber has no connection with the results of the session that is being verified enables a fake IdP to forward the results to the real IdP and successfully verify the identity of the subscriber.

5. Authenticator Lifecycle Management

The IdP is responsible for binding the identity of the subscriber with the authenticator and managing the authenticator. Authenticator lifecycle management consists of a number of processes, depending on the type of authenticator:

(1) Authenticator binding
(2) Loss, theft, damage, and replacement
(3) Expiry and renewal
(4) Revocation

5.1 Authenticator Binding

Authenticator binding is the creation of a link between the authenticator and the subscriber's account so that the authenticator can be used to authenticate the subscriber's account. The IdP can link the authenticator to the subscriber's account by issuing a new authenticator to the subscriber or registering the authenticator that the subscriber already has.

Requirements for Authenticator Binding

(1) The IdP shall retain all information on the authenticator related to the identity of the subscriber throughout the lifetime of the digital ID.

(2) The stored information shall contain the date and time of the authenticator binding to the subscriber's account and should contain information about the device used in the authenticator binding, such as the IP address or device identification number.

(3) The IdP shall retain the information necessary for limiting the number of authentication failures as specified in Section 4.2.

(4) The IdP shall verify that the type of authenticator complies with requirements at each AAL level.

(5) In the case where the IdP allows the binding to the subscriber's account of an additional authenticator or an authenticator that the subscriber already has, the IdP

shall require authentication of the subscriber at the current AAL (or a higher AAL) before adding a new authenticator.

(6) When adding a new authenticator, the IdP should send a notification to the subscriber through a channel independent of the channel to which the authenticator is linked (e.g. transmission to the subscriber's email).

5.2 Loss, Theft, Damage, and Replacement

An authenticator that is lost, stolen or damaged is considered to be an authenticator used for impersonation by attackers. Therefore, the IdP should have appropriate practices in the event that the authenticator is lost, stolen or damaged, as well as for the issuance of a replacement authenticator.

(1) The IdP should suspend, revoke, or terminate the use of an authenticator immediately after detecting that the authenticator is lost, stolen or damaged.

(2) The IdP should have the subscriber authenticated with a substitute authenticator or other means before accepting notification of loss, theft, or damage of the authenticator to ensure that the notification is from the real subscriber.

(3) The substitute authenticator shall be a memorized secret or a device authenticator.

Requirements for Replacement

(1) If all authenticators are lost, stolen or damaged, the IdP shall re-authenticate the identity of the subscriber by all measures. However, the IdP may choose partial re-authentication by an examination of the connection between the subscriber and the evidence of identity that the subscriber has provided to the IdP in a previous authentication.

(2) When issuing a replacement authenticator, the IdP should send a notification to the subscriber.

5.3 Expiry and Renewal

The IdP may issue to the subscriber an authenticator with a specified period of use, and an expired authenticator cannot be used for authentication. The IdP should have appropriate procedures in the case where the authenticator expires, including the issuance of a new authenticator (renewal).

Requirements for Expiry

(1) An expired authenticator shall not be used for authentication.

(2) In the case of authentication using an expired authenticator, the IdP should notify the subscriber that the authentication is fail because the authenticator is expired.

Requirements for Renewal

(1) The IdP should bind a new authenticator in a reasonable period of time before the original authenticator expires.

(2) Once a subscriber can use a new authenticator, the IdP may immediately revoke the original authenticator.

5.4 Revocation

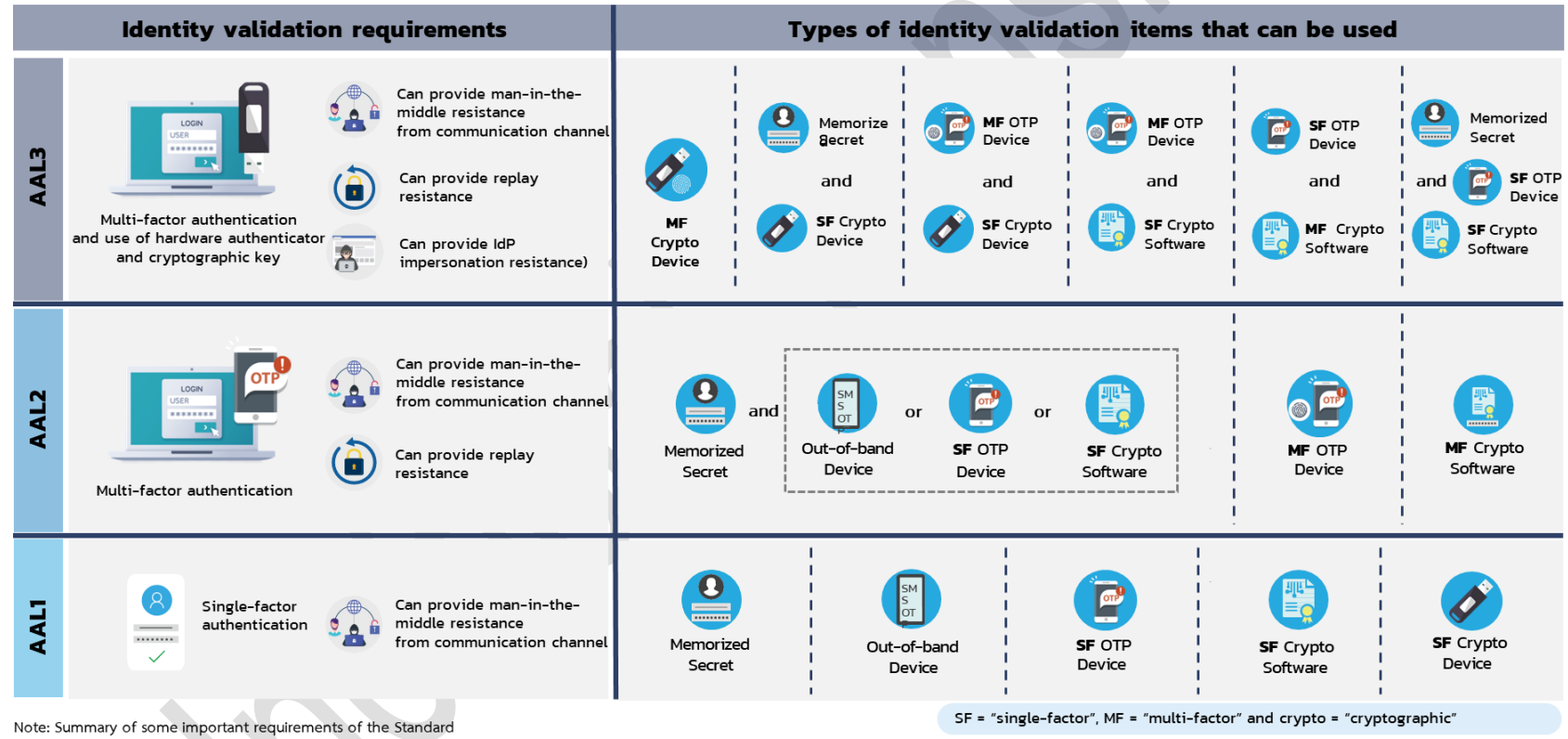
Revocation or termination of the authenticator is the removal of the link between the authenticator and the subscriber's account.

Requirements for Revocation

(1) The IdP shall immediately revoke the authenticator when the following cases become known:
   (1.1) When the digital ID or account of the subscriber ends, such as at the death of the subscriber or the detection of the subscriber's identity as a counterfeit;
   (1.2) When the subscriber requests to revoke the authenticator;
   (1.3) When the IdP determines that the subscriber's qualifications do not meet the criteria.

Appendix A. Infographic on Authentication Assurance Levels (AAL)

Infographic of the Authentication Assurance Levels (AAL) summarizing some of the key requirements from the Standard to present data that can be easily understood.



Bibliography

[1] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management", June 2017.

[2] Digital Transformation Agency, Australian Government, "Trusted Digital Identity Framework (TDIF): 05 - Role Requirements", Release 4.7, June 2022.

[3] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-131A Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths", March 2019.

[4] National Institute of Standards and Technology, U.S. Department of Commerce, "FIPS 140-2, Security Requirements for Cryptographic Modules", May 2001.

[5] International Organization for Standardization, "ISO/IEC 30107-3:2017 Information technology – Biometric presentation attack detection – Part 3: Testing and reporting", September 2017.