

SAMOA
NATIONAL DIGITAL IDENTIFICATION
REGULATIONS 2025

Arrangement of Provisions

PART 1
PRELIMINARY

1. Short title and commencement
2. Interpretation

PART 2
REGISTRATION

3. Samoa Digital Identification Number
4. Token
5. Physical ID card

PART 3
AUTHENTICATION
FUNCTION

6. Application for registration as a relying party
7. Safeguards and standards for authentication function

8. Online authentication

PART 4
DATA PROTECTION

9. Measures applying to Biometric Database
10. Measures to be implemented by the Registrar General for security, integrity and confidentiality

PART 5
GRIEVANCES

11. Process for grievances

PART 6
OFFENCES

12. Offences
-

PURSUANT to section 59 of the National Digital Identification Act 2024, I, **TUIMALEALIIFANO VAALETOA SUALAUVI II**, Head of State, acting on the advice of Cabinet, **MAKE** the following Regulations:

DATED this 12th day of JUNE 2025.


(Tuimalealiifano Vaaletoa Sualauvi II)
HEAD OF STATE

REGULATIONS

PART 1 PRELIMINARY

1. Short title and commencement-(1) These Regulations may be cited as the National Digital Identification Regulations 2025.

(2) These Regulations commence on a date to be nominated by the Minister.

2. Interpretation-(1) In these Regulations, unless the context otherwise requires:

“*Act*” means the National Digital Identification Act 2024;

“*authentication function*” means the process of a relying party or the Registrar General identifying a registered person or authenticating a registered person’s identity, by using data contained in the NDIDS;

“*IEC*” means the International Electrotechnical Commission; and

“*ISO*” means the International Organization for Standardisation.

(2) Unless the context otherwise requires, a term or expression that is used in these Regulations and defined in the Act has the meaning given to it in the Act.

PART 2 REGISTRATION

3. Samoa Digital Identification Number-(1) A Samoa Digital Identification Number ("SDIN") consists of 10 digits assigned by the Registrar General.

(2) The first 8 digits of the SDIN must be randomly generated.

(3) The last 2 digits of the SDIN, which serve as a 'check sum', must be calculated in accordance with the formula set out in sub-regulation (4).

(4) The formula is:

$$a + b + c + d + e + f + g + h = i$$

where:

a to h are the randomly generated first 8 digits; and
 i is the number that provides the last 2 digits.

(If i is less than 10, the first of the last 2 digits is 0 and the second of the last 2 digits is i .)

4. Token - A token, issued for use in place of an SDIN in online transactions, consists of 16 digits.

5. Physical ID card-(1) A physical ID card issued under the Act expires on the tenth anniversary of the day on which the card was issued.

(2) Despite sub-regulation (1), the Registrar General may, by notice in the Savali, amend the date of expiry of physical ID cards issued under the Act.

(3) The Registrar General must provide, to a holder of a physical ID card (an "existing card"), a replacement physical ID card before the expiry of the existing card.

PART 3

AUTHENTICATION FUNCTION

6. Application for registration as a relying party-(1) An entity eligible to be a relying party may apply to the Registrar General to become registered as a relying party.

(2) In addition to the matters in section 40(1) and (2) of the Act, the entity must provide, with its application, the following information to the Registrar General:

- (a) a detailed description of the current information system and security in use by the entity;
- (b) a list of the entity's proposed authorised users;
- (c) for each proposed authorised user, a copy of the confirmation, oath, or affirmation referred to in Regulation 10 signed by the user;
- (d) a signature for the application by an authorised signatory of the entity; and
- (e) any other information required by the Registrar General.

(3) Within 3 months of the Registrar General receiving an application, the prescribed fee, and any further information required by the Registrar General, the Registrar General must determine the application.

(4) In addition to the requirements in section 41(1) of the Act, a relying party must comply with any requirement by the Registrar General:

- (a) to undergo an assessment of the security of the party's information systems;
- (b) to undergo an assessment of an authorised user's understanding of and competency in relation to cybersecurity and data protection;
- (c) to deliver training, or to facilitate the delivery of training, to authorised users in the use of the authentication function, cybersecurity, and data protection; and
- (d) to provide physical access to the relying party's premises or equipment for a purpose described in paragraphs (a) to (c).

7. Safeguards and standards for authentication function-(1) The Registrar General must ensure that any person who uses the authentication function has received training in the proper use of the function.

(2) The authentication function must incorporate safeguards that effectively protect against unauthorised access and use.

(3) The safeguards must include 1 or more of the following features for authorised users to gain access to the authentication function:

- (a) one-time passwords;
- (b) multi-factor authentication.

(4) The authentication function may authenticate the identity of a registered person using 1 or more of the following:

- (a) verification of the SDIN provided by the person;
- (b) verification of the biographic data provided by the person;
- (c) verification of scans of the person's fingerprint;
- (d) verification of e-signature by the person.

(5) The process for verifying fingerprints and e-signatures used in the authentication function must comply with the latest relevant ISO and IEC standards for template compliance.

8. Online authentication-(1) The Registrar General must ensure that the authentication function is available online to relying parties.

(2) The authentication function must, as far as is practicable, be designed for interoperability with verification systems used by relying parties.

(3) The authentication function must contain the following components:

- (a) a QR code generator;
- (b) an authentication app to capture QR code; and
- (c) a server that is based on cloud that is a backend authentication server or web socket server.

PART 4 DATA PROTECTION

9. Measures applying to Biometric Database-(1) The measures that apply to data held in the Biometric Database and to any link between the data and a relevant SDIN or token in accordance with section 38(3) are:

- (a) all biometric data must be encrypted to prevent unauthorised access;

- (b) an individual's biometric data must be linked to their biographical information only through a unique identifier such as their SDIN or token; and
- (c) biometric data must be used only for the purpose of authentication using the authentication function.

10. Measures to be implemented by the Registrar General for security, integrity and confidentiality-(1) The measures in sub-regulation (2), to ensure the security, integrity and confidentiality of personal data held in connection with the Act, must be implemented by the Registrar General in accordance with section 46.

(2) The measures that must be implemented are:

- (a) a system back up is operational at all times;
- (b) authentication transactions and user logs are backed up at least once in every two-hour period;
- (c) all access and transaction logs are transferred to archive files at least once in every two-year period;
- (d) the NDIDS virtual private network operates as a secure, encrypted channel;
- (e) a public key infrastructure system operates at all times to manage public/private key pairs and digital certificates for the purposes of the authentication function;
- (f) all software is kept updated and all security patches, bug fixes, and other updates are applied promptly;
- (g) antivirus measures for protecting personal data against cyber threats are in place and kept current;
- (h) mechanisms are in place to ensure authorised users keep their login credentials secure;
- (i) security measures and standards set by the Ministry of Communications and Information Technology or the Office of the Regulator that are relevant to the NDIDS are applied; and
- (j) before a person is granted access to data held in connection with the Act, the person confirms in writing that they understand -

- i. the requirements of the Act in relation to the confidentiality and protection of data; and
- ii. that unauthorised disclosure of personal data is an offence under the Act.

(3) In place of a written confirmation described in sub-regulation (2)(j), the Registrar General may require a person to make an oath or affirmation to the same effect.

PART 5 GRIEVANCES

11. Process for grievances-(1) In accordance with section 53, a person who has a grievance in connection with the Act or these regulations (a "complainant") may lodge the grievance in writing with the Registrar General by delivering it to the Bureau.

(2) After a grievance is lodged, the Registrar General must:

- (a) review and investigate the grievance; and
- (b) notify the complainant that the grievance has been received and that it is being investigated.

(3) After investigating the grievance, the Registrar General must:

- (a) take any steps reasonably necessary to resolve the grievance; and
- (b) notify the complainant of the steps that the Registrar General has taken (or that the Registrar General had decided not to take any steps in relation to the grievance, if that is the case).

(4) The Registrar General must:

- (a) provide the complainant with an opportunity to comment on any proposed resolution (including if the Registrar General proposes not to take any steps in relation to the grievance); and
- (b) provide the complainant with an explanation for any steps taken to resolve the grievance (or an explanation as to why the Registrar General intends to take no steps in relation to the grievance).

(5) If the complainant is not satisfied with the steps taken by the Registrar General to resolve the grievance, the complainant may seek a review of the grievance by the National Identity Advisory Board by delivering it to the Chairperson.

(6) The National Identity Advisory Board must deal with the grievance in accordance with sub-regulations (2) to (4) and those provisions apply as if each reference to the Registrar General were a reference to the board.

(7) If the Registrar General is the subject of a grievance, the National Identity Advisory Board must deal with the grievance in accordance with this regulation in place of the Registrar General.

(8) If the complainant commences proceedings in a court in respect of the grievance, the process under this Regulation must be suspended until those proceedings are at an end.

(9) Nothing in this Regulation limits:

- (a) Part 3 of the Ombudsman (Komesina o Sulufaiga) Act 2013; or
- (b) regulations made under section 55 of the Public Service Act 2004.

PART 6 OFFENCES

12. Offences - A person who contravenes a provision of these Regulations commits an offence and is liable on conviction to a fine not exceeding 50 penalty units or to imprisonment not exceeding 12 months, or both.
