



NATIONAL DIGITAL IDENTIFICATION REGULATIONS 2024

Samoa

PART I PRELIMINARY

1. Short title and commencement
2. Interpretation

PART II REGISTRATION

3. Registration of Eligible Person
4. Samoa Digital identification and Tokens
5. ID Credentials
6. Biometric database

PART III AUTHENTICATION

7. Use of Authentication
8. Relying Parties

PART IV DATA PROTECTION

9. Security, integrity and

10. confidentiality
Oaths by Registrar General and its Employees
11. Oath or affirmation by other person(s)

PART V GRIEVANCES

12. Grievances

PART VI MISCELLANEOUS

13. Fees
14. Offences

Schedules

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

DATED at Apia this day of 2024.

REGULATIONS

PART I PRELIMINARY

1. Short title and commencement – (1) These regulations may be cited as the National Digital Identification Regulations 2024.

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

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

"**the Act**" means the National Digital Identification Act 2024;

"**Eligible Person**" is a person that is eligible to be registered as a registered person;

"**ID Credentials**" means:

- (a) A physical ID card issued by the Bureau that displays the information provided for under this Act;
- (b) A symbol provided by the Bureau that encodes such information in a manner readable by an electronic scanning device; or
- (c) an application installed on a personal communications device such as a mobile phone that contains such information in a form stipulated by the Bureau and readable by another device.

"**Identity database**" includes a system for identification and authentication comprising SDIN and ID credentials;

“Interoperability and integration” means the ability of different computer systems to connect and speak the same frequency, and to exchange and make use of information between the different systems;

“National Digital ID Agency” refers to the division within the Bureau which is responsible for administering the National Digital ID Act 2024 and its relevant regulations, policies and procedures;

“NDIDS” is the National Digital Identification System. It is comprised of the electronic database of the Register of Births, Deaths and Marriages and its associated systems, hereinafter referred to as Civil registration systems

“Registered Person” is a person who has been registered in the NDIDS;

(2) Unless the context otherwise requires, words and expressions in these regulations shall have the same meaning as is given to them in the Act.

PART II REGISTRATION

3. Registration of Eligible Person - (1) Only a citizen or a resident residing in Samoa in accordance the duration of a period for a person to become eligible as a permanent resident shall be a registrable person.

(2) Notwithstanding the registration of eligible persons, only eligible persons 18 years of age and over shall be issued a physical or digital card, or both.

4. The Samoa Digital Identification Number and Tokens - (1) The Samoa Digital Identification Number shall be formulated by the Registrar General by creating 10 digit numbers that are randomly calculated by a system. These calculations shall produce 90,000,000 combinations.

5. Identification Credentials - (1) Subject to section 34 of the Act, the Registrar General may elect to use the QR Code for online transactions and authentication.

(2) The Card Holders shall apply in writing to the Registrar General to activate its QR-Code for online transactions, in which terms and conditions shall apply.

(3) The QR-Code may also be de-activated through the following mechanisms:

- (a) The associated individual's SDIN, or an associated token on or in the ID credential, is deactivated;
- (b) A duplicative physical ID credential was issued in relation to the same individual;
- (c) The Registrar General has reason to believe that the ID credential was lost, stolen, damaged or destroyed, or has been obtained or accessed without permission or tampered with;
- (d) Or any other reason that will go against the objectives of the Act or regulations, or any other relevant law.

(4) The Registrar General will develop a National Implementation Plan, which includes the procedures and processes for QR-Code.

6. Biometric Data – (1) All biometric data collected by the Registrar General shall be encrypted.

(2) The encrypted Biometric Data shall only be searched for authentication purposes.

(3) Biometric Data must be linked to biographic data of any person under the Identification Database through SDIN, or a token number.

PART III AUTHENTICATION

7. Use of Authentication Function of NDIDS – (1) The Registrar General shall have the following powers and responsibilities:

- (a) to administer the authentication function of NDIDS;
- (b) to approve or disapprove any application by a relying party (in accordance with the form in Schedule 1) seeking

the application of authentication and verification services, based on merit;

- (c) to conduct trainings for all users of the authentication function;
- (d) to issue a one time password or a 2 factor authentication, or multiple factor authentication for all users when logging into the authentication function of the NDIDS;
- (e) to ensure that the authentication function is interoperable with other verification systems provided by relying parties, within reason;
- (f) to ensure that the online authentication contains the major components of:
 - (a) QR-Code generator;
 - (b) Authentication application that can capture QR-Code;
 - (c) Backend authentication server or web socket server (cloud);
 - (d) Or any other component that the Registrar General deems fit and appropriate for the objectives of the Act and the Regulations.

(2) The authentication function contains alternatives in verifying registered persons against their enrollment data:

- (a) verifying persons using biographic data;
- (b) verifying persons using SDIN;
- (c) verifying persons by scanning fingerprints.

(3) The fingerprint verification in regulation 7(2)(c) must be utilized in accordance with the international standards as set by the International Organisation Standards and the International Eletrotechnical Commission 19794-2 compliant templates without use of proprietary extended data, or any other relevant international standards, whichever has the priority.

PART IV DATA PROTECTION

8. Relying Parties – (1) Any person can apply to be a relying party by providing the following information to the Registrar General:

- (a) Write an application (consider putting the template as annexure or schedule to these regulations) for the use of the Authentication Function of the NDIDS;
- (b) The letter to outline – the purpose of the Organization and why the authentication function is needed;
- (c) List of users or potential users;

(2) The Registrar General, after assessing the application on its merits, may or may not approve the request by the relying party.

(3) If approved, the Registrar General to:

- (a) Sign an Agreement for use of services, together with the relying party;
- (b) Conduct relevant trainings for users;
- (c) Conduct assessments and onsite visits to ensure that the services are used in accordance with the Act and the regulations.

(4) The Registrar shall have powers to activate or de-active any account of a relying party based on merit and in accordance with the Act and regulations.

9. Security, Integrity, and Confidentiality (look if we can slot in oaths like in the Statistics Act; also look at confidentiality provisions from Stats Act and other relevant laws etc) of digital personal data – (1) The following are the duties and responsibilities of the Registrar General to ensure that the digital personal data of the people are secure, integral and kept confidential, within reasonable means:

- (a) to ensure that the System Backup is up and running at all times;
- (b) to provide daily backup for backend data (2 hour backup for authentication transactions and user logs);
- (c) shall keep all software up to date to ensure it has the

latest security patches, bug fixes and other updates to protect against new and old cybersecurity threats;

- (d) to provide rules and enforcement for users to keep their passwords and login credentials safe from each other;
- (e) to ensure that the NDIDS Virtual Private Network is a secure encrypted tunnel for personal data to hide personal data from hackers and snoopers;
- (f) to monitor the existing antivirus softwares for protection of personal data from ransomware, spyware, Trojan horses and various known and unknown cyber threats, in present and in future; (make this general and not refer to specific antivirus etc)
- (g) to ensure that the key infrastructure system is functioning at all times;
- (h) All information given to the Registrar General under the Act or regulations shall be used only in accordance with the objectives of the Act and the regulations.

10. Oaths- (1) the Registrar General, its officers or anyone employed by the Registrar General to fulfill the duties and responsibilities for the Act and regulations, must take and subscribe an oath or affirmation before their duties commence. The affirmation shall be signed and be in this format:

“I [Name], solemnly swear/affirm, that I will faithfully and honestly fulfil my duties as an officer of the National ID agency, in conformity with the requirements of the National Digital Identification Act 2024 and its pertinent regulations, and that any information obtained or received by me as an officer of the National Identification agency will:

- (a) During my employment or engagement as an officer, be disclosed by me only in accordance with my official duties; and*
- (b) After that employment or engagement ceases, be disclosed by me only with the express authority of the National ID agency.*

I acknowledge that any act or omission by me in breach of this

[oath/affirmation] may result in disciplinary proceedings in which, if convicted, I may be sentenced to a fine or imprisonment term, or both”.

(2) The oath or affirmation may be administered by any person before whom an affidavit may be sworn under section 14 of the *Oaths, Affidavits and Declarations Act 1963*.

11. Oath or affirmation by other persons - (1) a person who is an employee of the State or who is working in or for an approved organization as an employee or contractor for the National ID Agency may, at the discretion of the Registrar General, be permitted to make an oath or affirmation in the following form (which may be amended as appropriate for particular circumstances):

“I [Name] [solemnly swear/affirm] that I will faithfully and honestly conform to the requirements of the National Digital Identification Act 2024 and its pertinent regulations, and all other relevant laws of Samoa, and that any information obtained or received by me relating to the Act and regulations will be used only for the purposes for which it was made available [or specify the purpose] and will be disclosed by me only with the express authority of the Registrar General.

I acknowledge that I have read and understood my obligations under the Act and the regulations”.

I acknowledge that any act or omission in breach of this [oath/affirmation] may render me subject to criminal proceedings which, if convicted, I may be sentenced to a fine or imprisonment, or both, in Samoa”.

PART V GRIEVANCES

12. Grievances - (1) Subject to the Bureau’s Procedure for grievances, as well as the National Digital Identification System Strategy, an aggrieved party may lodge a complaint with the Assistant Chief Executive Officer of the National Identification Division

(“ACEO”) regarding any grievance arising out of the Act or the regulations.

(2) The ACEO will then receive, register and review its merits and then communicate the status to the aggrieved party. If the matter is resolved, then that will be the conclusion of the matter.

(3) If the matter is not resolved, the ACEO will then forward it to the Registrar General for investigations and review and if not resolved, then the Registrar General shall refer it to the Ombudsman, PSC or Identification Advisory Board for remediation, whichever is the legally appropriate avenue to take.

(4) Should the grievance not be resolved, then the option of Court is available for the aggrieved party.

PART VI MISCELLANEOUS

13. Fees - (1) The Registrar General, with the approval of the National Revenue Board, may issue a list of fees by way of an Order of the Registrar General, from time to time.

14. Offences – (1) A person who commits an offence under these regulations is liable on conviction to a fine not exceeding 150 penalty units or to imprisonment not exceeding seven (7) years, or both.

Schedule 1

Relying Party Application Form

1.	Name of Company, Business	
2.	Name of Shareholders or registered owners	
3.	Name of Ultimate Beneficial Owner(s)	
4.	Type of Business	
5.	Rationale for applying for authentication function	