The Alan Turing Institute

Standard Operating Procedures for Digital Identity Systems

September 2024

Executive Summary

Using Standard Operating Procedures (SOPs) when establishing a Digital Identity (DID) system is crucial for ensuring the security, reliability, and trustworthiness of the system. The 51 SOPs developed by the Alan Turing Institute provide clear, structured steps for the onboarding, authentication, and lifecycle management of digital identities and their associated credentials. By adhering to these SOPs, the DID system can effectively safeguard the personal and sensitive data of its users, prevent unauthorised access to accounts, and maintain the overall integrity of the system. This includes 51 SOPs for system implementers and 51 accompanying documents that provide the rationalisation for each SOP. Together, these SOPs provide a comprehensive framework for managing digital identities in a secure and consistent manner, as outlined in this document.

These SOPs are intended to cover scenarios that are typical or likely to occur during the lifecycle of a DID system. They address common events and standard operational processes to ensure smooth and secure management of digital identities. While the SOPs focus on routine and expected scenarios, they may need to be expanded upon further testing and evaluation to include additional events or circumstances that could arise. This ongoing evaluation ensures that the SOPs remain relevant, comprehensive, and capable of addressing the evolving needs and challenges of digital identity management.

All SOPs developed in this work can be accesses via the project's GitHub repository

https://github.com/alan-turing-institute/Standard-Operating-Procedures-for-Digital-Identity-Systems/tree/main

Acknowledgements

This work was supported, in whole or in part, by the Bill & Melinda Gates Foundation [INV-001309]. Under the grant conditions of the Foundation, a Creative Commons Attribution 4.0 Generic License has already been assigned to the Author's Accepted Manuscript.

The Institute is named in honour of Alan Turing, whose pioneering work in theoretical and applied mathematics, engineering and computing is considered to have laid the foundations for modern-day data science and artificial intelligence. It was established in 2015 by five founding universities and became the United Kingdom's (UK) National Institute for Data Science and Artificial Intelligence. Today, Turing brings together academics from 13 of the UK's leading universities and hosts visiting fellows and researchers from many international centres of academic excellence. Turing also liaises with public bodies and is supported by collaborations with influential organisations.

The Alan Turing Institute

Table of Contents

1. Introduction

Standard Operating Procedures (SOPs) are a set of step-by-step instructions that detail how to execute specific functions within a system. SOPs typically break down a function into discrete processes, with each process consisting of sequential procedures (the instructions for that process). By following suitable SOPs, administrators ensure a standardised approach to operations, promoting consistency and reliability in outcomes.

The trustworthy digital infrastructure for Identity Systems team at the Alan Turing Institute has prepared a set of 51 SOPs for use. This collection consists of two versions: 51 SOPs specifically designed for system implementers, and an additional 51 SOPs that include detailed rationalisations for each procedure. This document provides a comprehensive overview of each SOP, detailing their purpose, scope, methodology, and structure. It offers an in-depth understanding of how the SOPs are designed to guide the management of DID system. There are three essential phases in a DID system, each encompassing a series of critical functions that need to be executed. These phases are:

- **Onboarding** – This phase involves the registration of an applicant into the DID system, including the collection, validation, and verification of the applicant's claimed identity. It ensures that new users are securely and efficiently integrated into the system.
- **Authentication** – This phase focuses on the modules and mechanisms used to verify and approve the identity of an applicant or a claimant (a person claiming to possess a registered identity). It employs various methods such as passwords, biometrics, and multi-factor authentication to ensure secure access to the system.
- **DID Lifecycle Management** – This phase deals with the ongoing management of DID account holder data, including updating personal information, handling compromised authenticators, and managing account suspensions or deletions. It ensures the continued security, accuracy, and compliance of the digital identity records throughout their lifecycle.

The SOPs outlined in this report are designed to be followed to maintain a trustworthy DID system. These SOPs ensure that the system:

- Complies with relevant data regulations and policies, safeguarding user information and maintaining legal and regulatory standards.
- Minimises security risks associated with the registration of applicants and the storage of their data, protecting against unauthorised access and data breaches.

- Reduces the likelihood of downtime caused by procedural failures or inconsistencies, thereby ensuring the system's reliability and availability.
- Guarantees that data is accessible and efficiently retrievable for due diligence, supporting transparency and accountability in the management of digital identities.

By implementing these SOPs, the DID system can achieve a high level of security, reliability, and user trust, facilitating efficient and secure management of digital identities.

2. Scope

2.1. In Scope

The SOPs for the DID system are designed to establish a secure, reliable, and standardised process for managing digital identities. The scope includes procedures for onboarding new users, authenticating their identities, and managing the lifecycle of digital identities. These SOPs ensure compliance with regulatory standards, protect user data, and maintain the integrity and trustworthiness of the DID system. The SOPs cover the following key areas:

- **Onboarding**: To facilitate the registration and enrolment of new users into the DID system, ensuring that all necessary information is collected, validated, and verified.
- **Authentication**: To authenticate users securely and reliably, using various factors (knowledge, ownership, inherence) to verify their identities and grant access to the DID system.
- **DID Lifecycle Management**: To manage digital identities throughout their lifecycle, including updates, handling compromised authenticators, account suspensions, and deletions.

2.2. Out of Scope

Events and scenarios that are considered rare or unlikely to occur within the DID system's lifecycle, such as unusual forms of identity fraud or complex legal disputes over digital identity ownership, are not covered by these SOPs. Additionally, the SOPs do not address issues that fall outside the standard regulatory compliance and data protection frameworks for digital identity systems.

3. Methodology

A DID system is designed to ensure a secure, efficient, and standardised approach to managing digital identities. The overall methodology for developing these SOPs was structured to cover all critical phases of the DID system, including onboarding, authentication, and lifecycle management to enable appropriate deployment in an auditable and consistent

way. The development methodology involved a rigorous process to ensure that the procedures meet industry standards. This ensures that the DID system complies with applicable data protection regulations and open-source policies. This process was structured with four fundamental steps:

1. **Decomposing the DID System Phases:** The first step was to break down the core phases of the DID system into distinct functions. These phases include Onboarding, Authentication, and Digital Identity Lifecycle Management. Each phase was examined to identify the specific processes associated with it, ensuring comprehensive coverage of the DID system's operational requirements.

2. **Reviewing Scope and Existing Documentation:** To build a foundation for the SOPs, an in-depth review of the system's scope and existing documentation was conducted. This included gathering information about stakeholders, understanding the mechanisms of the system, and identifying relevant standards and good practices. For example, standards such as NIST Digital Identity Guidelines, ISO 27001 for secure data handling, and eIDAS for identity proofing were considered to align the SOPs with recognised best practices.

3. **Developing Rationalisation:** A rationalisation was then developed to standardise processes and procedures. This provides a structured approach for documenting each SOP in a consistent and standardised format. It ensures clarity and ease of use for system implementers, covering aspects such as application initiation, document submission, biometric checks, data encryption, and validation.

4. **Verification and Validation:** The final step involved verifying and validating the SOPs using established frameworks like the NIST Assurance Framework and standards. This step ensures that each SOP meets the required assurance levels in comparison with other ID systems, providing confidence in the security and integrity of the DID system.

The SOPs cover various critical steps such as initiating online applications, document submission, terms acceptance with liveness checks, encryption and secure processing of personal data, and validation of identity information. They incorporate measures aligned with standards like NIST Digital Identity, ISO 27001, and GDPR for data protection, ensuring that the procedures are both secure and compliant with industry standards.

By following this structured methodology, the SOPs are designed to offer a comprehensive framework for securely managing digital identities throughout their lifecycle. They not only

guide system implementers through best practices but also provide rationalisation for each step, ensuring that the DID system is reliable, and in line with international standards and good practices.

4. Overview of the SOPs

In this section, key aspects of the DID system are discussed. A summary of the functions respective to each phase are discussed below Tables 1, 2, and 3. Further visualisation can be referred from Appendices A, B and C.

4.1. Onboarding Phase

This phase outlines the procedures for registering a new user in the DID system, focusing on different application methods and the collection of necessary identification data. Further details on each SOP can be referred from Table 1:

- **Online and Offline Applications**: Users can initiate their applications online or offline. There are provisions for self-initiated applications, as well as applications made by parents, guardians, or introducers.
    - **Online Application**: Includes self-initiated, by parent/guardian, and by introducer.
    - **Offline Application**: Similar categories as online but involves physical interactions.
- **Pre-Registration and Appointment Booking**: Users can book appointments for offline biometric collection, ensuring a structured and manageable registration process.
- **Validation and Verification**:
    - **Validation**: Involves checking proof of identity, proof of address, and proof of relationship.
    - **Verification**: Ensures that the provided documents and relationships are genuine and accurate.
- **Biometric Data Collection**: Procedures for collecting biometric data (facial, fingerprint, and iris) from applicants, ensuring accurate and secure data handling.
- **Account Creation and Activation**: Once validation and verification are complete, a new digital ID account is created, authenticators are bound, and credentials are delivered to the user, who then activates their account.

Table 1: Description of functions in the Onboarding Phase

Onboarding Function	Process	Description	SOP Number
Initial Steps	Register New Account	The first step in the onboarding process, where a new account is registered in the DID system, initiating the user's digital identity creation.	OB.1.1.A
	Initiating an Online Application	Users begin their online registration by entering their personal details into the DID system, starting the onboarding process.	OB.1.1.B
Online Application	Self-Initiated Application	Users initiate the registration process online independently, entering their personal details directly into the DID system.	OB.1.2.A
	Application by Parent/Guardian	A parent or guardian can start the online registration process on behalf of a minor or dependent, providing their details and required documents.	OB.1.2.B
	Application by Introducer	A trusted individual or entity (introducer) initiates the online application process for a user, facilitating their registration into the DID system.	OB.1.2.C
Offline Application	Self-Initiated Application	Users visit a physical registration center to start the registration process, providing their details and documents in person.	OB.1.3.A
	Application by Parent/Guardian	A parent or guardian initiates the offline registration process at a registration center on behalf of a minor or dependent.	OB.1.3.B
	Application by Introducer	An introducer initiates the offline application at a registration center,	OB.1.3.C

		providing initial support for the user's registration.	
Pre-Registration & Appointment	Pre-Registration & Appointment Booking	Users can pre-register and schedule appointments for offline biometric data collection, ensuring an organised and efficient registration process.	OB.1.3.D
Biometric Data Collection	Offline Biometric Collection	Collection of biometric data (e.g., facial, fingerprint, iris) from users at registration centers, which is crucial for verifying the identity and preventing fraud.	OB.1.3.E
	Offline Biometric Collection Consent	Explicit consent is obtained from users before collecting their biometric data, ensuring compliance with privacy standards and building trust.	OB.1.4.A
	Facial Data Collection	Collection of facial recognition data during the onboarding process to be used for future biometric authentication.	OB.1.4.B
	Fingerprint Data Collection	Collection of fingerprint data to create a unique biometric signature for the user, enhancing security and identification accuracy.	OB.1.4.C
	Iris Data Collection	Collection of iris scan data, providing a highly secure biometric method due to the uniqueness of iris patterns.	OB.1.4.D
Validation	Proof-of-Identity Validation	Administrators validate proof-of-identity documents (e.g., national ID, passport) to ensure they are genuine and accurate, as part of the registration process.	OB.2.A

	Proof-of-Address Validation	Validation of proof-of-address documents to confirm the user's current residence, ensuring that the provided information is accurate and verifiable.	OB.2.A
	Proof-of-Relationship Validation	In cases where applications are initiated by others (e.g., parent/guardian), the relationship is validated to confirm the legitimacy of the application.	OB.2.B
Verification	Proof-of-Identity Verification	Verification processes to further confirm the identity of the user by cross-checking the provided documents with existing records.	OB.3.A
	Proof-of-Address Verification	Verification of the user's address information, ensuring that it matches official records and is validated through reliable sources.	OB.3.B
	Verifying Relationship in Proof-of-Relationship	Verification of the claimed relationship (e.g., parent-child) to ensure that applications made by others on behalf of the user are legitimate.	OB.3.C
Account Creation	Creating New Digital ID Account	After successful validation and verification, a new digital identity account is created, providing the user with a unique digital identity within the system.	OB.4.A
Authenticator Binding	Binding Authenticators to User Identification Number	Securely binding authenticators (e.g., passwords, OTPs, biometric data) to the user's unique identification number, enabling secure access to the digital identity.	OB.4.B

Credential Delivery & Activation	Delivery of Digital ID & FTP Credentials	Credentials (e.g., usernames, passwords) are securely delivered to the user, ensuring they can access and manage their digital identity.	OB.4.C
	Activation of Digital ID Account	Users activate their digital ID account using the provided credentials, completing the onboarding process and enabling them to use their digital identity securely.	OB.4.D

4.2. Authentication Phase

This phase describes the authentication mechanisms to verify and authorise users in the DID system. Further details on each SOP can be referred from Table 2:

- **Knowledge Factors:** Involves creating strong, memorable secrets like passwords and PINs, which users will use for authentication.
- **Password-Based Authentication:** Users create and use passwords for securing their accounts.
- **PIN-Based Authentication:** Personal Identification Numbers are used for additional security.
- **Ownership Factors:** Involves using One-Time Passwords (OTPs) and tokens as part of the authentication process.
- **One-Time Passwords:** Generated for multi-user authentication scenarios to enhance security.
- **Token-Based Authentication:** Uses tokens (shared codes) for secure authentication.
- **Inherence Factors (Biometrics):** Uses biometric data (fingerprints, iris, facial recognition) for authentication, requiring obtaining explicit consent from users before collecting biometric data.

Table 2: Description of functions in the Authentication Phase

Authentication Function	**Process**	**Description**	**SOP Number**
Knowledge Factors	Creation of Strong Passwords	Users create strong, unique passwords as a part of their digital identity security, ensuring robust	AU.1.A

		protection against unauthorised access.	
	Password-Based Authentication	Users authenticate themselves by entering their passwords, which are securely stored and managed within the DID system.	AU.1.B
	Creation of Memorable Secrets	Users set up memorable secrets (e.g., security questions or phrases) to add an extra layer of security beyond passwords.	AU.1.C
	Memorable Secret-Based Authentication	Authentication process using memorable secrets, which serve as backup or supplementary methods to passwords for securing accounts.	AU.1.D
	Creation of Personal Identification Number (PIN)	Users create a PIN, which serves as a quick and secure method of authentication, useful especially for mobile devices or quick access scenarios.	AU.1.E
	PIN-Based Authentication	Users enter their PINs to authenticate their identity, adding a simple yet effective security layer to their accounts.	AU.1.F
Ownership Factors	Generation of One-Time Password (OTP)	One-time passwords are generated for secure, time-sensitive authentication. These are used once and expire shortly after being issued.	AU.2.A
	Creation of Multi-User One-Time Password	Procedures for creating OTPs that can be used by multiple users in scenarios requiring shared access or authentication.	AU.2.B
	OTP-Based Authentication	Authentication using OTPs, which are sent to a user's registered device. This method ensures that even if	AU.2.C

		other credentials are compromised, unauthorised access is prevented.	
	Generation of Tokens	Tokens (shared codes) are created for use in authentication, providing an additional security layer by requiring possession of the token.	AU.2.D
	Token-Based Authentication	Using tokens for authentication, requiring the user to have a specific token or device, enhancing security through multi-factor authentication.	AU.2.E
Inherence Factors (Biometrics)	Biometric Authentication (Fingerprint Data)	Authentication using fingerprint data ensures that the person accessing the account is the legitimate owner by verifying their unique biometric signature.	AU.3.B
	Biometric Authentication (Iris Data)	Uses iris scans for authentication, providing a high level of security due to the uniqueness of each individual's iris patterns.	AU.3.C
	Biometric Authentication (Facial Data)	Facial recognition is used for authentication, verifying a user's identity through unique facial features.	AU.3.D
	Obtaining Claimant Consent for Biometric Use	Explicit consent is obtained from users before collecting and using biometric data, ensuring compliance with privacy regulations and building user trust.	AU.3.A

4.3. ID Lifecycle Management

This phase focuses on managing the lifecycle of DID accounts, ensuring that accounts are updated, maintained, and deactivated properly. Further information can be referred from Table 3:

- **Updating Information**: Includes procedures for updating both online and offline personally identifiable information (PII) and biometric data.
    - **Online/Offline PII Updates**: Ensures users can update their information securely.
    - **Biometric Data Updates**: Maintains up-to-date biometric data to ensure continued accuracy in authentication.
- **Handling Compromised Authenticators**: Procedures for reporting and managing compromised authenticators to prevent unauthorised access.
    - **Reporting Compromised Authenticators**: Processes for identifying and responding to cases where authentication mechanisms have been compromised.
- **Account Suspension and Deletion**:
    - **Temporary Suspension**: Accounts may be suspended temporarily due to fraud, ineligibility, or government orders.
    - **Permanent Deletion**: Accounts can be permanently deleted by user choice or upon the user's death.
- **Expiry and Renewal**: Procedures for the expiration and renewal of authenticators, ensuring they remain effective and secure throughout their lifecycle.

Table 3: Description of functions in the ID Lifecycle Management Phase

Lifecycle Management Function	**Process**	**Description**	**SOP Number**
Updating Information	Updating Online Personally Identifiable Information (PII)	Procedures for users to update their personal details (e.g., name, address) online, ensuring that the DID system maintains accurate and current user data.	LM.1.A

	Updating Offline PII	Similar to online updates, this allows users to update their personal information through offline means, accommodating users who may not have online access.	LM.1.B
	Updating Online Biometric Data	Users can update their biometric information (e.g., facial recognition data, fingerprints) online to keep their authentication methods accurate and secure.	LM.1.C
	Updating Offline Biometric Data	Users provide updated biometric data at a physical location, ensuring that all biometric records are current and accurate for future use.	LM.1.D
	Request New DID Physical Card (Lost/Theft/Damage)	Procedures for requesting a new physical DID card in cases of loss, theft, or damage, ensuring continued secure access to the digital identity.	LM.1.E
Handling Compromised Authenticators	Reporting Online Compromised Authenticators	Procedures for reporting compromised authenticators (e.g., passwords, OTP devices) online, allowing for quick action to secure accounts against unauthoris ed access.	LM.3.A
	Reporting Offline Compromised Authenticators	Similar reporting procedures are available for users who need to report compromised authenticators through offline means, ensuring comprehensive security coverage.	LM.3.B

Account Management	Temporary Account Suspension	Accounts can be temporarily suspended in response to issues such as suspected fraud, ineligibility, or by government order, preventing unauthorised access during investigations.	LM.5.A
	Permanent Account Deletion (By Choice)	Users have the option to permanently delete their digital identity accounts, ensuring their right to privacy and the removal of personal data from the DID system.	LM.5.B
	Permanent Account Deletion (Upon Death)	Accounts are deleted upon the user's death, a necessary step in lifecycle management to protect data and prevent misuse by unauthorised parties.	LM.5.C
Authenticator Management	Expiry and Renewal of Authenticators	Authenticators such as passwords, OTPs, and tokens have defined expiration periods. These processes manage the renewal of these authenticators to maintain ongoing security.	LM.4.B
	Expiry and Renewal of DID Account	Procedures for managing the expiration and renewal of DID accounts, ensuring that inactive accounts are reviewed and reactivated or deactivated as necessary.	LM.4.A

5. Structure of the SOPs

Each SOP features the following components:

5.1. Definition of Purpose and Scope

- Each SOP begins with a clear definition of its purpose, outlining the specific objectives it aims to achieve. For instance, the SOP for registering a new account details the steps from the initial visit to the DID portal to the successful creation of a new user account.
- The scope of each SOP is defined to ensure it covers relevant processes, stakeholders, and regulatory compliance requirements. This includes identifying ownership and responsibilities, target users, and potential beneficiaries such as the general public, government agencies, and private sector companies.

5.2. Application: Stakeholder Identification and Ownership

- The SOPs specify the roles and responsibilities of key stakeholders, including Digital Identity Service Providers (DISPs), IT and security teams, and compliance and legal departments. Each stakeholder group is responsible for maintaining, updating, and ensuring compliance with the SOPs.
- Collaboration among these stakeholders is emphasised to enhance system functionality, security, and adherence to regulatory standards.

5.3. Prerequisites and Assumptions

- Before executing the SOPs, certain prerequisites must be met. These include system requirements, technical setups, and interdependencies with other SOPs (e.g., those related to system maintenance and security protocols).
- Assumptions are made about the users' basic understanding of navigating digital forms and the operational status of technological infrastructure. Constraints, such as system downtime or regulatory changes, are also identified to manage expectations and plan for contingencies.

5.4. Detailed Process Flows and Procedures

- Each SOP includes a detailed, step-by-step process flow, starting from the initiation of an action to its successful completion or error handling. This ensures that each task is clearly defined, with specific actions, expected outputs, and integrated security measures at each step.
- Process steps cover actions such as applicant registration, document submission, liveness checks, and system processing. Security measures, such as encryption and

biometric checks, are incorporated to ensure data protection and compliance with standards like ISO 27001 and NIST guidelines.

- The SOPs also provide protocols for handling exceptions and errors, ensuring that any issues encountered during a process are managed effectively. For instance, if an error occurs during biometric verification, the system provides clear guidance to the user and implements security protocols to address the situation.
- Limits on retry attempts and clear communication of error messages help manage user expectations and maintain the integrity of the process. These protocols are essential for preserving the security and reliability of the DID system while guiding users toward resolution in the event of an error.
- Notifications and logging are integral to each process. Actions, whether successful or failed, are logged, and users are notified of outcomes through secure channels such as email or phone notifications. This ensures transparency and accountability in the registration process.
- Logging supports audit trails and compliance checks, providing a record of all actions within the DID system. For example, details of an online application process, including document submission and liveness checks, are securely logged for future reference and compliance purposes.

5.5. Visualisation:

- Visual elements, such as flowcharts and diagrams, are included in each SOP to provide a clear representation of the process flow. These visualisations help to simplify complex procedures, making it easier for stakeholders to understand and follow the outlined steps.

- The use of visual aids supports effective communication of the process, highlighting key stages and decision points within the SOP, thus enhancing overall comprehension and implementation.

5.6. Rationalisation and Compliance:

- Robust security measures are incorporated throughout the SOPs to protect user data and prevent unauthorised access. These measures include encryption, two-factor authentication, SSL/TLS protocols, and the use of intrusion detection and prevention systems.

- The SOPs ensure compliance with international standards and regulations (e.g., NIST, eIDAS, ISO 27001) to minimise legal risks and build trust with users and regulatory bodies.

- Each SOP includes a section on rationalisation, offering a detailed explanation for each step and decision within the process. This rationale helps stakeholders understand the importance and necessity of each procedure, ensuring clarity and reinforcing compliance.
- The rationalisation outlines how each step aligns with regulatory requirements, best practices, and security standards. For instance, it explains why specific security measures like encryption or biometric checks are crucial for maintaining the system's integrity.

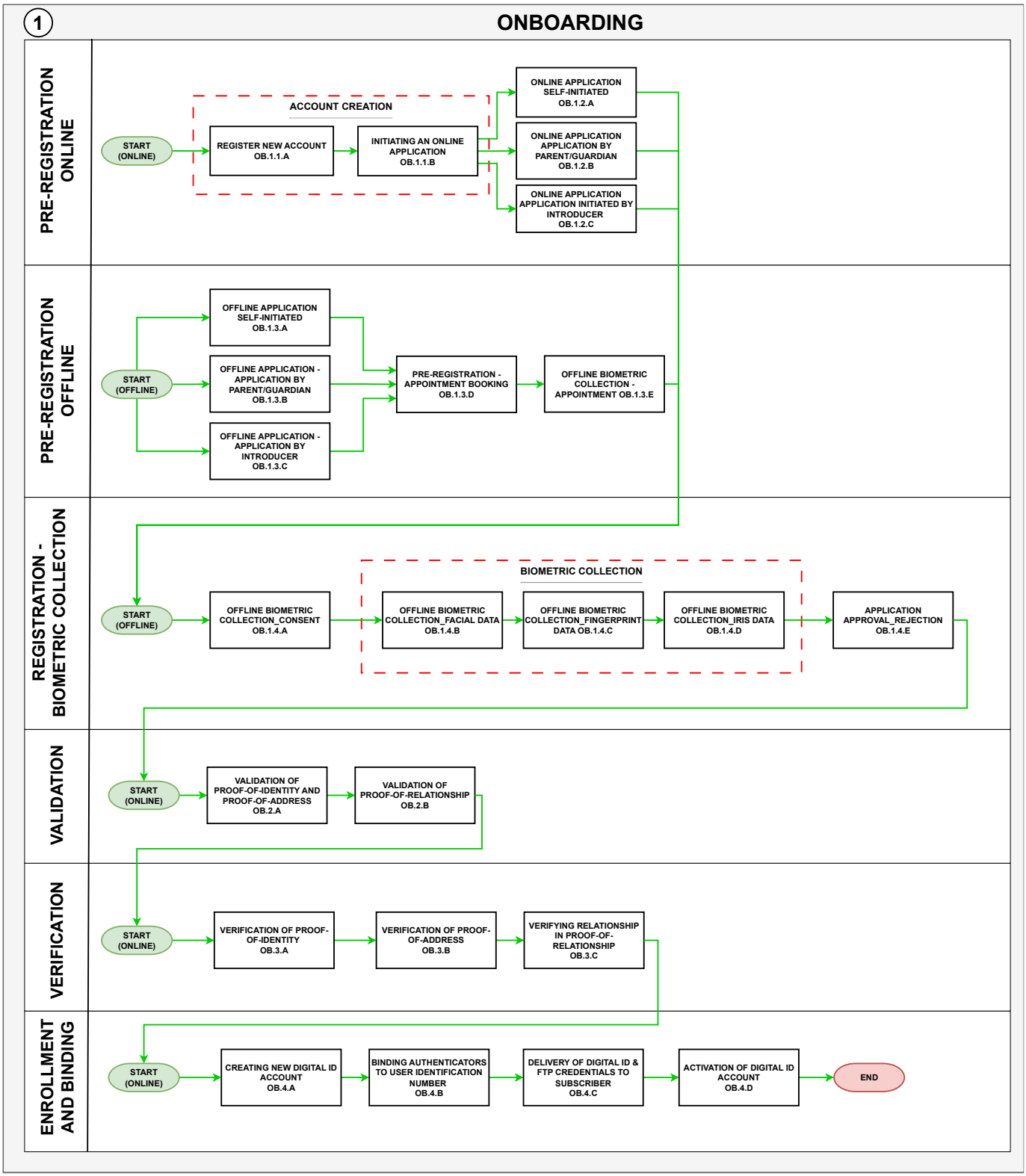
5.7. References

- The SOPs conclude with references to relevant standards, guidelines, and best practices, such as NIST Digital Identity Guidelines, ISO 27001, and eIDAS regulations. This ensures that the SOPs are grounded in recognised frameworks and provide a solid foundation for the DID system's operations

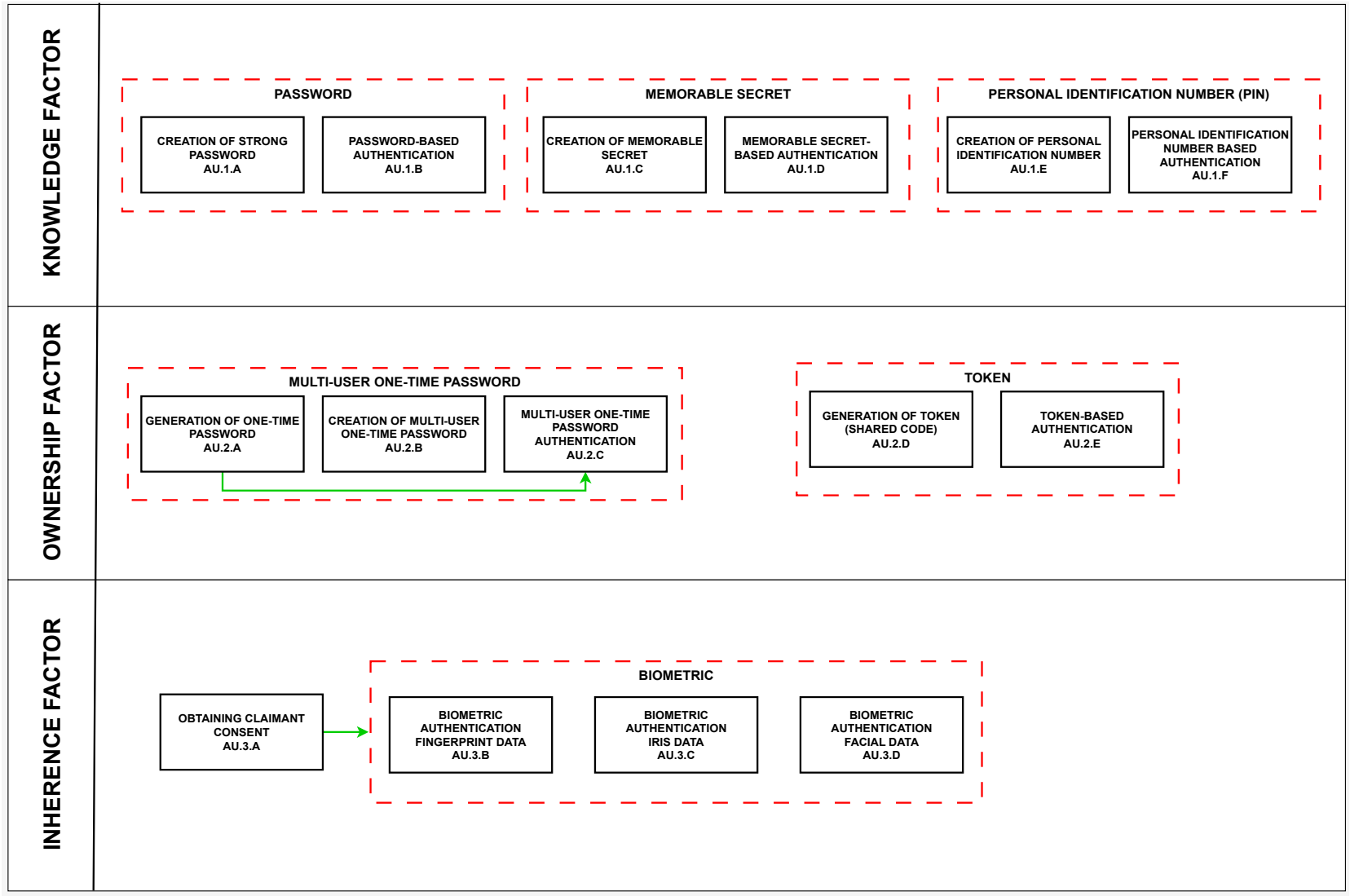
6. Conclusion

In conclusion, the 51 SOP developed for the DID system offer a comprehensive framework for managing digital identities securely and reliably. By incorporating industry standards, best practices, and comprehensive process flows, these SOPs ensure that the DID system remains secure and compliant. They provide clear guidelines for all phases of digital identity management, from onboarding to authentication and lifecycle management, contributing to the overall trustworthiness of the system.

Appendix A: DID System - Overview of Onboarding Phase



Appendix B: DID System - Overview of Authentication Phase



Appendix C: DID System - Overview of ID Lifecycle Management Phase