MOSIP  
Standard Operating Procedures

Al Tariq Sheik

April 30, 2023

**Executive Summary:**

This document outlines SOPs for a Digital Identity system, designed to demonstrate its Minimal Acceptable Functionality for in-person registration with Minimal Supporting Documents. The SOPs cover key processes such as validation, verification, issuing, binding, authentication, and account management throughout its lifecycle. This document begins with an introduction to SOPs before defining the scope of the SOPs in more detail. NIST Information and Authentication Assurance Levels are referenced when designing SOPs.

Contents

|  |  |  |  |
| --- | --- | --- | --- |
| 1.0 | Introduction to Standard Operating Procedures | | 1 |
| 2.0 | Scope (SOPs for MAF and MVP) | | 1 |
| 3.0 | Methodology | | 2 |
|  | 3.1 | Information Assurance Levels | 2 |
|  | 3.2 | Authentication Assurance Levels | 3 |
| 4.0 | SOPs – Design and Documentation | | 3 |
|  | 4.1 | DID SOPs with Reference to IAL | 7 |
|  | 4.2 | SOPs - Documentation | 8 |
| 5.0 | Conclusion | | 9 |
|  | Glossary | | 10 |
|  | Appendix A: NIST Information Assurance Framework | | 12 |
|  | Appendix B: NIST Authentication Assurance Framework | | 13 |
|  | Appendix C: DID System Data Flow Diagram | | 14 |
|  |

1.0 Introduction

Standard Operating Procedures (SOPs) are a set of step-by-step instructions that explain in detail how to execute a function. SOPs typically decompose a function into discrete processes, with each process comprising sequential procedures (the instructions for that process). By following SOPs, administrators promote a standardised manner of working with consistent outcomes per function.

The aim of this work was to design SOPs that accommodate the Minimal Acceptable Functionality (MAF) of a Digital Identity (DID) system. The MAF of a DID system is the set of functions which enable its most basic execution. There are three essential phases in a DID system. Each phase contains a series of functions that must be executed for the MAF. These phases are:

1. **Onboarding** – The registration of an applicant onto the DID system and the validation and verification of an applicant’s claimed identity.
2. **Authentication** – The modules and mechanisms for approving the identity of an applicant or a claimant (a person who claims to possess a registered identity).
3. **DID Lifecycle Management** – The recording of DID account holder data and the maintenance of DID account holder records.

It is intended that the SOPs outlined in this report will be followed to demonstrate an open source DID system that meets the Minimum Viable Product (MVP) requirements. These requirements stipulate that the system should:

1. Comply with data regulations and open-source licenses/policies, demonstrating commitment to legal and ethical standards.
2. Avoid the security risks associated with registering an applicant and storing their data through robust risk management frameworks.
3. Ensure data is available and efficient to access for due diligence, employing redundant storage and efficient access controls.
4. Document compliance with data protection laws and highlight progress in privacy controls through regular audits and control logs.
5. Establish a routine for monitoring service access, utilizing automated tools for real-time alerts on suspicious activities.
6. Ensure software and firmware integrity through digital signatures, checksums, and regular updates.
7. Adopt and document an ISMS framework, supported by a continuous improvement process for security and compliance.
8. Deploy comprehensive preventive controls, including firewalls and intrusion detection systems, and conduct ongoing user/admin education.

The following subsection outlines the scope of SOPs designed for the MAF of a DID system and MVP requirements.

2.0 Scope (SOPs for MAF and MVP)

Administrators of the DID system must be aware of the SOPs for commonly encountered and security-compromising events. For an MVP-DID system, typical events are considered to be the in-person registration of an applicant who: registers with a First Name, Surname, Phone Number, Postal Address and Date of Birth; is over the age of 18; and holds at least two Minimum Supporting Documents (MSDs), such as a birth certificate, driver’s license or passport. During the lifecycle of a DID account, common and security-compromising events include the loss or theft of an authenticator and the unauthorised duplication or use of an authenticator. The administrator should also be knowledgeable of the SOPs to revoke a DID account at the request of the account holder, their Next of Kin, or when an account is found to be fraudulent. Events that are beyond the scope of the SOPs documented in this report are those considered unlikely to occur in the lifecycle of a DID account.

3.0 Methodology

There are four fundamental steps towards designing SOPs that meet the MVP requirements and have the MAF of a DID system:

1. Distil the DID system phases (Onboarding, Authentication and DID Lifecycle Management) into functions and identify the processes associated with each function.
2. Review the scope of SOPs and existing documentation to gather information about stakeholders and the mechanisms of the system.
3. Develop a framework for processes and procedures, and document the framework in a standardised form.
4. Verify and validate the design of SOPs using the NIST Assurance Framework.

3.1 Information Assurance Level

The NIST Information Assurance Level (IAL), Appendix A, corresponds to the degree that an identity, or the attributes of an identity, must be validated and verified by information. Of particular relevance to the DID system’s SOPs are IAL1 and IAL2:

**IAL1** – The self-asserted, personally identifying attributes of an applicant do not require validation or verification.

**IAL2** – The self-asserted, personally identifying attributes of an applicant require validation and verification via identity proofing that is conducted in-person or remotely.

Supporting information may be classified as NOT STRONG, FAIR, STRONG, SUPERIOR. References to IAL are made in the documentation of the SOPs.

3.2 Authentication Assurance Level

The NIST Authentication Assurance Level (AAL), Appendix B, corresponds to the level of authenticator security and the reauthentication practices required to prove that an identity belongs to a claimant.

4.0 SOPs - Design and Documentation

In this section, key aspects of the DID system are discussed. A summary of the Functions, Processes and SOP documentation are provided in Table 1. Readers are advised to refer to Appendix C for the Data Flow diagram of this DID system.

**Phase A – Onboarding**

Identity proofing is a critical process for establishing and verifying an individual's identity, involving the collection, validation, and verification of personal information. The goal is to obtain attributes and evidence that can identify a unique individual within a given population or context. The de-duplication process is crucial for preventing duplicate enrolment by checking the applicant's biographic, biometric, and government-issued attributes against the identity system's database of enrolled individuals and their associated evidence. Identity proofing comprises three main functions: Identity Collection and/or Resolution, Validation, and Verification, each of which is described below.

Identity Proofing consists of the following functions: *Identity Collection and/or Resolution*, *Validation* and *Verification*, each of which are described below:

1. **Function: Collection and/or Resolution**

DID systems commonly include de-duplication processes in their identity proofing framework. This involves verifying biographic attributes (e.g., name, age, gender), biometrics (e.g., fingerprints, iris scans, facial recognition images), and government-issued attributes (e.g., driver's license, passport, taxpayer identification numbers) to prevent duplicate enrolment and ensure the accuracy and reliability of identity information:

**Physical Identity Collection** involves individuals presenting physical documents, such as government-issued ID cards and passports, in person to identity service providers. To ensure document deduplication, a process and criteria must be defined for identifying duplicate identities, and for reviewing and approving the deduplication of identities.

**Biometric Collection** procedures ensure secure and accurate data collection while maintaining the privacy of the applicant's data. By following these steps, a digital identity system can create a reliable and trustworthy biometric database that verifies an individual's identity in various contexts.

1. **Function: Validation**

Validation is the process of confirming that evidence is authentic and accurate by comparing it against a reliable source. This ensures that the information matches with independent and dependable data or records. An example of validation is when an administrator checks physical identity evidence, such as a driver's license or passport, for alterations and verifies that identification numbers follow standard formats, and physical and digital security features are valid and intact. Additionally, the administrator may query relevant sources to confirm that the information matches.

1. **Function: Verification**

To confirm that a validated identity belongs to the individual being proofed, several measures can be employed. One approach is to request the applicant to submit a mobile phone video or photo along with additional liveness checks and compare them to the photos on the identity evidence or the photo on record in the database. To confirm that the identity evidence matches the actual applicant, an enrolment code can be sent to the verified phone number linked to the identity. The applicant must then provide the enrolment code to authenticate that they are a real person with access to and control of the verified phone number.

1. **Function: Enrolment and Binding**

Enrolment refers to the process of registering an applicant who has undergone identity-proofing as a subscriber, establishing their identity account. This involves securely binding the subscriber's verified identity attributes to one or more authenticators that are owned and controlled by the subscriber, which is also known as "credentialing". The binding protocol used is designed to ensure a high level of security and reliability.

**Phase B – Authentication**

Defining the types of digital identities to be authenticated and specifying the types of transactions or access granted based on authentication are crucial in identifying the purpose and scope of digital identity authentication. This includes determining the level of assurance needed for authentication, the types of credentials that can be used, and the types of authenticators that are acceptable. By doing so, organizations can ensure that only authorized individuals have access to sensitive information or perform specific transactions, thereby enhancing the security and integrity of digital identity systems.

1. **Function: Knowledge factors - Passwords**

The purpose of establishing guidelines for creating and managing passwords is to ensure a secure and reliable digital identity system. These guidelines are aimed at ensuring that the passwords used in the system are strong, unique, and protected against unauthorized access or theft. By following these procedures, the system can protect the personal and sensitive data of its users, prevent unauthorized access to their accounts, and maintain the integrity of the overall system. Additionally, these procedures enable users to easily manage and reset their passwords without compromising the security of their accounts.

1. **Function: Ownership factors - One Time Passwords**

The use of "something you have" as an authenticator requires clear requirements and procedures to ensure secure and effective usage throughout the digital identity lifecycle. This may include cryptographic keys stored in hardware or software, one-time passwords generated by hardware devices, or software OTP generators installed on digital devices like mobile phones. The aim is to guarantee the secure and accurate identification of the subscriber and to prevent unauthorized access or fraud. The procedures should address the enrolment and revocation processes, as well as the management of the authenticators, to ensure their reliability and effectiveness. By following these guidelines, the digital identity system can provide users with a robust and secure means of authentication.

1. **Function: Influence factors - Fingerprint Biometrics**

To effectively use fingerprint biometrics for digital identity verification, it is crucial to establish clear processes and procedures. These should outline the specific systems and applications that will rely on fingerprint biometrics as a form of identity verification, as well as the process for collecting and storing this biometric data securely. Additionally, guidelines should be established for accessing and using the biometric data, including training for personnel and protocols for handling any potential errors or discrepancies. By implementing these policies and procedures, the digital identity system can ensure the accurate and reliable use of fingerprint biometrics for identity verification, while also safeguarding the privacy and security of users' biometric data.

**Phase C: ID Lifecycle Management**

The purpose of creating an SOP for Identity Lifecycle Management is to provide guidelines for managing events that occur during the subscriber's authenticator lifecycle. These include issuance, binding, and revocation of authenticators and credentials. The aim is to maintain the security and trustworthiness of authenticators, minimise risks of security breaches and unauthorised access to user data. ID lifecycle management involves four stages.

1. **Function: Issuing and recording credentials**

The purpose of establishing guidelines for credential management is to ensure that the administrator can issue, record, and maintain credentials and associated data in the subscriber's identity account throughout the lifecycle of the credential. The subscriber generally possesses the credential, but the administrator or verifier may also possess the credential. The subscriber always possesses the authenticator, which is used to claim identity when interacting with a relying party. These procedures aim to maintain the security and privacy of the subscriber's identity and data, as well as the reliability and trustworthiness of the digital identity system.

1. **Function: Binding**

To establish clear guidelines for the administrator to maintain records of all authenticators associated with each subscriber's identity account throughout the digital ID lifecycle. The administrator should also maintain the necessary information to control authentication attempts. When the administrator issues new credentials that bind a new authenticator to the subscriber's account post-enrolment, the administrator should require the subscriber to authenticate at the assurance level or higher at which the new authenticator will be used. These procedures aim to ensure the security and integrity of the subscriber's identity account and maintain the trustworthiness of the digital identity system.

1. **Function: Mitigating the Risks Associated with Compromised Authenticators**

The security and integrity of a DID account heavily rely on the bound authenticator. However, in cases of loss, theft, or unauthorized use of the authenticator, the account becomes compromised, risking unauthorized access to sensitive information. To address such risks and maintain trust, administrators must follow clear and comprehensive procedures for handling authenticator breaches, including revocation and investigations. Proactive measures can reduce the likelihood and impact of breaches, thus enhancing the security and trust of the DID system.

1. **Function: Expiration and Renewal**

To ensure the secure and reliable management of authenticators in a digital identity system, it's crucial to establish clear guidelines for the administrator to maintain records of all authenticators associated with each subscriber's identity account throughout its lifecycle. This includes controlling authentication attempts and requiring authentication at an appropriate assurance level when issuing new credentials that bind a new authenticator to the account. By following these procedures, the administrator can ensure the security and integrity of the subscriber's identity account and maintain the trustworthiness of the digital identity system.

1. **Function: Revocation**

The purpose of the standard operating procedure is to provide clear guidelines for the administrator to promptly revoke authenticators when necessary. Authenticators may need to be revoked in various scenarios such as when an identity ceases to exist, when requested by the subscriber, or when the administrator determines that the subscriber no longer meets the eligibility requirements. The procedures will outline the revocation process for each scenario, including the necessary steps and timeline. By following these procedures, the digital identity system can maintain its security and integrity by ensuring that only authorised users have access to the system.

4.1 DID SOPs with Reference to IAL

The MAF was identified functionalities derived from IAL1 and IAL2. During the onboarding phase of the MAF, the following parameters are required, and their definitions are described in Appendix A:

* Presence - In-person and/or Unsupervised Remote
* Resolution - Minimum Attributes necessary, KBV - MAY
* Evidence - Between SUPERIOR, STRONG and FAIR
* Validation - Between SUPERIOR STRONG and FAIR
* Verification - STRONG/NOT STRONG
* Address Confirmation and Subprocess
* Address confirmation - SHALL/SHALL NOT, Address validation through supplied ID - SHOULD/MAY
* Self-asserted address data - SHALL/ SHALL NOT
* Enrolment Code - SHALL - its Validity for 7 days - SHALL
* Biometric Collection - SHALL/SHALL NOT
* Security Control - LOW, MODERATE and HIGH

4.2 SOPs - Documentation

Table 1. List of DID Phases, Functions and Processes.

|  |  |  |
| --- | --- | --- |
| **Phase** | **Function** | **SOP** |
| Onboarding | The Collection and Resolution of Applicant Registration Data | [A.1](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20A%20-%20Onboarding/A.1%20SOP%20-%20Collection%20%26%20Resolution.pdf) |
| The Validation of an Applicant’s Identity | [A.2](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20A%20-%20Onboarding/A.2%20SOP%20-%20Validation.pdf) |
| The Verification of an Applicant’s Identity | [A.3](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20A%20-%20Onboarding/A.3%20SOP%20-%20Verification.pdf) |
| The Enrolment and Binding of a DID Applicant to the Credentials of a DID Account | [A.4](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20A%20-%20Onboarding/A.4%20SOP%20-%20Enrollment%20and%20Binding.pdf) |
| Authentication | The Creation and Management of a Suitable Authenticator with Knowledge Factor – Passwords | [B.1](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20B%20-%20Authentication/B.1.%20SOP%20-%20Knowledge%20Factor.pdf) |
| The Creation and Management of a Suitable Authenticator with Ownership Factor - OTPs | [B.2](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20B%20-%20Authentication/B.2%20SOP%20-%20Ownership%20Factor.pdf) |
| The Creation and Management of a Suitable Authenticator with Ownership Inherence Factor - Fingerprints | [B.3](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20B%20-%20Authentication/B.3%20SOP%20-%20Inherence%20Factor.pdf) |
| DID Lifecycle Management | The Issuing and Recording of Credentials, Authenticators and Amendments to The Personal Attributes of a DID Subscriber | [C.1](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20C%20-%20ID%20Lifecycle%20Management/C.1%20SOP%20-%20Issuing%20and%20Recording.pdf) |
| The Binding (Credentialing) of Authenticators to the DID Subscriber Account and The Maintenance of Bound-Authenticator Data | [C.2](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20C%20-%20ID%20Lifecycle%20Management/C.2%20SOP%20-%20Binding.pdf) |
| The Handling of Authenticators that have been Compromised by Loss, Theft, Unauthorized Duplication or Unauthorized Usage | [C.3](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20C%20-%20ID%20Lifecycle%20Management/C.3%20SOP%20-%20Compromised%20Authenticator.pdf) |
| The Expiration and Renewal of an Authenticator During the Lifecycle of a DID Account | [C.4](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20C%20-%20ID%20Lifecycle%20Management/C.4%20SOP%20-%20Expiration%20and%20Renewal.pdf) |
| The Revocation (Termination) of a DID Account due to the Death of a Subscriber, at the Request of the Subscriber or if the DID Account is Fraudulent or Ineligible | [C.5](https://livewarwickac.sharepoint.com/sites/SOP/Shared%20Documents/General/Exemplar%20SOPs/Level%202%20Phase%20C%20-%20ID%20Lifecycle%20Management/C.5%20SOP%20-%20Revocation%20(Termination).pdf) |

5.0 Conclusion

Developing SOPs for a DID system is critical to ensuring the security, reliability, and trustworthiness of the system. These procedures provide clear guidelines for the enrolment, authentication, and management of digital identities and their associated credentials and authenticators throughout their lifecycle. By following these procedures, the DID system can protect the personal and sensitive data of its users, prevent unauthorised access to their accounts, and maintain the integrity of the system. The SOPs outlined in this document aim to provide a framework for managing digital identities in a secure and reliable manner.

It should be noted these SOPs are intended to be followed when demonstrating the MAF of a DID system. Consequently, they attempt to cover scenarios that are considered commonplace or certain to occur during the DID lifecycle. Occurrences that were considered rare/unlikely to occur were not considered when designing these SOPs. This was a subjective judgement and upon testing the SOPs, it may be determined that the SOPs should be broadened in terms of the events they address.

**Glossary**

**Digital Identity (DID)** – An online personal identity system.

**Standard Operating Procedure (SOP)** – The functions, processes and procedures that should be followed by Applicants, Subscribers, Claimants and Admin.

**Minimal Acceptable** **Functionality (MAF)** – The most fundamental scenario in which a Digital Identity system should operate.

**Minimum Support Documents (MSD)** – The fundamental documents that can be used to validate and verify an identity, such as birth certificates, driver’s licenses and passports.

**Applicant** – A person who applies for a Digital Identity.

**Subscriber** – An Applicant who has passed validation and verification, and has been enrolled into the online Digital Identity system. Also, a Claimant who has passed authentication. The Digital Identity account holder.

**Claimant** – A person who claims to possess an identity and has not yet passed authentication.

**Admin/Administration** – The staff of the Digital Identity provider, who conducts Onboarding and Identity Lifecycle Management.

**New Subscriber Registration Form** – The form that is completed by an Applicant in-person to register for a Digital Identity.

**Service Provider (SP)** – Also known as Admin/administrator, the SP conducts Onboarding and Identity Lifecycle Management.

**Unique Identity Number (UIN)** – A unique number that is assigned to subscribers and is used to identity a Digital Identity account.

**Password** – A Subscriber-defined code that is known only to the Subscriber, and is used for authentication purposes.

**One Time Password (OTP)** – A password that is generated by Admin and sent to the Subscriber via phone, email or post, which is used for authentication purposes.

**Fingerprints** – A biometric dataset obtained from the fingerprint of a Subscriber, which is used for authentication purposes.

**Public Records Portal (PLP)** – A database that may contain driving license records, passport records, etc. that can be used by Admin to validate and verify an Applicant.

**Onboarding** – The overarching function which begins with an applicant registering for an Digital identity in-person, and ends with the online binding of their personal attributes to authenticators.

**Validation** – The process in which Admin ascertain if the Applicant possesses the identity that they claim.

**Verification** – The process in which Admin ascertain if the personal attributes of the Applicant are corroborated by more than one supporting document.

**Enrolment** – The process in which an Applicant becomes an online account holder, a Subscriber.

**Binding** – The process in which Admin commit an authenticator to a Digital Identity account.

**Credentialing** – The process of binding the identity of a subscriber to authenticators.

**Identity Lifecycle Management** – The overarching function undertaken primarily by Admin to maintain Digital Identity account data for security and due diligence.

**Subscriber Identity Account (SIA)** – The unique Digital Identity account belonging to a Subscriber, in which all data (current, upcoming and historic) are contained.

**Subscribers Digital Identity System (SDIS)** - The location within the Digital Identity system in which logs of Subscriber actions are made.

**Revocation** – The process in which a Digital Identity account is removed.

**Appendix A: NIST Information Assurance Framework**

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **IAL1** | **IAL2** | **IAL3** |
| Presence | No requirements | In-person and unsupervised remote | In-person and supervised remote |
| Resolution | No requirements | -The minimum attributes necessary to accomplish identity resolution  - Knowledge-based verification (KBV) may be used | Same as IAL2 |
| Evidence | No identity evidence is collected | - One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, OR  - Two pieces of STRONG evidence, OR  - One piece of STRONG evidence plus two pieces of FAIR evidence. | -Two pieces of SUPERIOR evidence, OR  - One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, OR  - Two piece of STRONG evidence plus one piece of FAIR evidence. |
| Validation | No validation | Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented. | Same as IAL2 |
| Verification | No verification | Verified by a process that is able to achieve a strength of STRONG | Verification by a process that is able to achieve a strength of SUPERIOR |
| Address Confirmation | No requirements for address confirmation required | Enrolment code sent to any address of record. Notification sent by means difference from enrolment code. | Required. Notification of proofing to postal address. |
| Biometric Collection | No | Optional | Mandatory |
| Security Controls | N/A | - SP 800-53  - Moderate Baseline (or equivalent federal or industry standard) | - SP 800-53  - High Baseline (or equivalent federal or industry standard) |

**Appendix B: NIST Authentication Assurance Framework**

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **AAL1** | **AAL2** | **AAL3** |
| Permitted Authenticator Types | Memorised Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device | MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorised Secret plus:   * Look-Up Secret * Out-of-Band * SF OTP Device * SF Crypto Software * SF Crypto Device | MF Crypto Device; SF Crypto Device plus Memorised Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorised Secret. |
| FIPS Verification | Level 1 (Government agency verifiers) | Level 1 (Government agency authenticators and verifiers) | Level 2 overall (MF authenticators)  Level 1 overall (Verifiers and SF Crypto Devices)  Level 3 physical security (all authenticators) |
| Reauthentication | 30 days | 12 hours or 30 minutes inactivity; MAY use one authentication factor | 12 hours or 15 minutes inactivity; SHALL use both authentication factors |
| Security Controls | - SP 800-53 Low  - Baseline (or equivalent) | - SP 800-53 Moderate  - Baseline (or equivalent) | - SP 800-53 High  - Baseline (or equivalent) |
| MitM Resistance | Required | Required | Required |
| Verifier-Impersonation Resistance | Not required | Not required | Required |

**Appendix C: DID System Data Flow Diagram**

**Diagram

Description automatically generated**

*Figure 1: The Data Flow Diagram of a DID System based on MAF.*