|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Changes Made** |
| 1.0 | 16/09/2024 |  |
|  |  |  |
|  |  |  |

*Prepared by the Trustworthy Digital Infrastructure for Identity Systems Team*

*This work was supported, in whole or in part, by the Gates Foundation [INV- 057591]. 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.*

Standard Operating Procedure REQUEST NEW DID PHYSICAL CARD (LOST THEFT DAMAGED)

LM.1.E - WITH RATIONALISATION

**Version Control**

**Guidelines for Maintaining the SOP Version Control Table:**

* **Version**: Assign a new version number for every update. Minor changes can be denoted by incremental changes in decimal (e.g., 1.1, 1.2), while major changes can increment the whole number (e.g., 1.0 to 2.0).
* **Date**: The date when the changes were finalised.
* **Changes Made**: A brief description of the changes or updates made.

Table of Contents

[1. Purpose 3](#_Toc177314825)

[2. Definitions and Abbreviations 3](#_Toc177314826)

[3. Application 3](#_Toc177314827)

[3.1 Ownership and Stakeholders 3](#_Toc177314828)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314829)

[3.1.2 IT and Security Teams 3](#_Toc177314830)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314831)

[3.2 Users and Beneficiaries 3](#_Toc177314832)

[3.2.1 General Public 3](#_Toc177314833)

[3.2.2 Government Agencies 4](#_Toc177314834)

[3.2.3 Private Sector Companies 4](#_Toc177314835)

[4. Prerequisites 4](#_Toc177314836)

[4.1 Assumptions 4](#_Toc177314837)

[4.2 Constraints 4](#_Toc177314838)

[5. Process Flow - Process and Procedures 4](#_Toc177314839)

[5.1. Initiating the Request Process: 4](#_Toc177314840)

[5.2. Reporting and Verification: 4](#_Toc177314841)

[5.3. Visiting the DID Portal or Service Center: 5](#_Toc177314842)

[5.4. Selecting Reason for Requesting New Card: 5](#_Toc177314843)

[5.5. Confirming the Request: 5](#_Toc177314844)

[5.6. Verification by the Administrator: 5](#_Toc177314845)

[5.7. Authentication and Security Checks: 5](#_Toc177314846)

[5.8. Approval and Issuance of New Card: 6](#_Toc177314847)

[5.9. Notification and Logging: 6](#_Toc177314848)

[5.10. Error Handling and Security Measures: 6](#_Toc177314849)

[5.11. Closing the Process: 6](#_Toc177314850)

[6. Visualisation 7](#_Toc177314851)

[7. Rationalisation 8](#_Toc177314852)

[8. References 9](#_Toc177314853)

# 1. Purpose

This SOP outlines the standardized procedure for users to request a new Digital Identity (DID) physical card in case of loss, theft, or damage. It ensures secure and accurate processing through proper verification, documentation, and error handling.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**KR**: Key Revocation

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**AC**: Access Control

**OTP**: One-Time Password

**HTTPS**: Hyper Text Transfer Protocol Secure

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership**: Oversee the physical card request process.
* **Responsibilities**: Ensure secure and compliant issuance of new physical cards.

### 3.1.2 IT and Security Teams

* **Ownership**: Manage technical infrastructure and security protocols.
* **Responsibilities**: Maintain system security, data encryption, and infrastructure.

### 3.1.3 Compliance and Legal Departments

* **Ownership**: Ensure compliance with legal and regulatory standards.
* **Responsibilities**: Oversee compliance checks, documentation, and regulatory adherence.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users**: Individuals requesting new physical cards for their DID accounts.
* **Usage**: Provide updated identity verification for secure account management.

### 3.2.2 Government Agencies

* **Users**: Agencies requiring verified and updated identities for services.
* **Usage**: Utilize verified identity information for secure service delivery.

### 3.2.3 Private Sector Companies

* **Users**: Businesses requiring updated identity verification.
* **Usage**: Use secured identities for compliance and verification purposes.

# 4. Prerequisites

## 4.1 Assumptions

* Subscribers have access to required documents and authentication methods.
* Administrators are trained to handle the physical card request process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The physical card request process may be affected by system downtimes or regulatory changes.
* Secure devices and internet access are required for administrators and users.

# 5. Process Flow - Process and Procedures

## **5.1. Initiating the Request Process:**

* **Claimant/Subscriber Action:**
  + If the claimant is 18 years or older, they can initiate the process by reporting the lost, stolen, or damaged card through a service hotline or the DID portal.
  + If under 18, the process must be initiated by a parent, guardian, or authorized introducer.
  + The claimant provides details about the incident leading to the card's loss, theft, or damage.
* **Output:** A case number is generated for tracking the incident.

## **5.2. Reporting and Verification:**

* **Claimant/Subscriber Action:**
  + The claimant must report the incident to a local police authority if the card is lost or stolen.
  + A police report or a similar document must be obtained as proof of the incident.
* **Output:** A police report or proof of incident document is obtained.

## **5.3. Visiting the DID Portal or Service Center:**

* **Claimant/Subscriber Action:**
  + Claimant visits the DID portal or an offline service center to request a new card.
  + For online requests, the claimant logs into their account using their credentials (password, OTP, memorable secret).
* **Output:** Access to the request form for a new card is granted.

## **5.4. Selecting Reason for Requesting New Card:**

* **Claimant/Subscriber Action:**
  + The claimant selects the reason for the new card request, choosing from lost, stolen, or damaged.
  + The system prompts the claimant to upload the police report or relevant documentation, especially for lost or stolen cards.
* **Output:** Reason for request and supporting documents are submitted.

## **5.5. Confirming the Request:**

* **Claimant/Subscriber Action:**
  + The claimant reviews the request details and confirms the request for a new physical card.
  + A confirmation receipt is generated and provided to the claimant for record-keeping.
* **Output**: A confirmation receipt is generated and sent to the claimant.

## **5.6. Verification by the Administrator:**

* **Administrator Action:**
  + The administrator receives the request and verifies the details, including the claimant's UIN and supporting documents.
  + If the request and documents are valid, the process moves forward; otherwise, errors are flagged for further review.
* **Output:** Verification status (approved/rejected) is determined and recorded.

## **5.7. Authentication and Security Checks:**

* **System Action:**
  + The claimant’s authentication details are masked and encrypted for secure processing.
  + Multiple security checks are performed to ensure the authenticity of the request and to prevent fraudulent activity.
* **Output:** Security check results are logged, and the system status is updated.

## **5.8. Approval and Issuance of New Card:**

* **System and Administrator Action:**
  + Upon successful verification, the request is approved.
  + The administrator issues a new DID physical card to the claimant.
  + The new card details are updated in the system, and old card authentication is deactivated to prevent misuse.
* **Output:** New card details are issued, and the claimant is notified of the issuance.

## **5.9. Notification and Logging:**

* **System Action:**
  + Notifications are sent to the claimant’s registered contact details (email/SMS) to inform them of the new card issuance.
  + All actions and processes are logged for audit and tracking purposes, ensuring compliance and transparency.
* **Output:** Notifications sent to the claimant; process details are logged.

## **5.10. Error Handling and Security Measures:**

* **System Action:**
  + If any issues arise, such as failed authentication or document verification, the system triggers error handling protocols.
  + If errors cannot be resolved within a specific number of attempts, the claimant’s account may be temporarily locked to prevent unauthorized access.
* **Output:** Error notifications are generated, and account status is updated as needed.

## **5.11. Closing the Process:**

* **System Action:**
  + Once the new card is issued and all processes are complete, the system logs the final status.
  + The process is terminated, and the account status is updated to reflect the issuance of the new card.
* **Output:** Final process status is logged, and the account reflects the new card issuance.

# 6. Visualisation

A diagram of a computer

Description automatically generated

Please refer to the [GitHub](https://github.com/alan-turing-institute/Standard-Operating-Procedures-for-Digital-Identity-Systems) repository for further information.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LM.1.E REQUEST NEW DID PHYSICAL CARD (LOST THEFT DAMAGED)** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | User initiates request online | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Account Authentication | User logs in using password and OTP | Authentication Server | Two-Factor Authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Report Loss/Theft/Damage | User selects reason for new card request | User Device, Web Server | Secure data entry | ISO 27001 Data Protection, eIDAS Electronic Identification |
| 4 | Fill Request Form | User fills and submits request form online | User Device, Web Server, Database Server | Data Input Validation | ISO 27001 Data Integrity, GDPR Compliance for Personal Data Handling |
| 5 | Confirm Personal Information | User confirms personal information for verification | User Device, Web Server, Database Server | Confirmation protocol | ISO 27001 User Access Management, NIST SP 800-63 Identity Verification |
| 6 | Authenticate Request | Backend system authenticates the request | Server, Private Network | Authentication checks, Logging | ISO 27001 Authentication Controls, Aadhaar Secure Authentication Practices |
| 7 | Request Verification | System processes request and verifies identity | Server | Data verification, Secure processing | ISO 27001 Cryptography, FATF Digital Identity Guidelines |
| 8 | Notification of Request Approval | User receives notification of request approval | User Device, Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 9 | Encrypt and Mask Personal Data | Personal data encrypted and masked for production | Production System | Encryption, Masking | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 10 | Produce New Physical Card | New digital ID card is produced and personalized | Card Production Facility | Secure production controls | ISO 27001 Physical Security, eIDAS Trust Services |
| 11 | Ship New Card | New card is shipped to user | Shipping System | Secure packaging and mailing | ISO 27001 Communications Security, eIDAS Trust Services |
| 12 | Log Process | Log details of the entire process | Security System | Audit trails, logging | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 13 | End Process | Process completion | Server | Secure session termination | ISO 27001 Information Security Management |
| 14 | Terminate Process if Multiple Failures | Lock user account if multiple authentication failures | Authentication System | Account lockout, Error handling | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |

# 8. References

1. NIST. Digital Identity Guidelines: Age Verification Guidance. Available at: [https://pages.nist.gov/800-63-3/].
2. eIDAS. Identity Proofing Requirements. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\_.2014.257.01.0073.01.ENG].
3. ISO. 27001, Secure System Access Control. Available at: [https://www.iso.org/standard/27001].
4. Aadhaar. Account Creation and Management. Available at: [https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar/aadhaar-enrolment.html].
5. SingPass. Account Creation and Management. Available at: [https://www.singpass.gov.sg/home/ui/assets/pdf/Singpass\_Registration\_Guide.pdf].
6. FATF. Digital Identity Guidance: Authentication Mechanisms. Available at: [https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html].
7. Estonia ID. Data Protection Practices. Available at: [https://toolbox.estonia.ee/asset-page/252494-e-estonia-guide-full-brochure].
8. Emirates ID. Available at: [https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id].