

## CONCEPT **Note**

# **Digital Wallet Interoperability Framework with Global Sovereign Nations**

**Case Study:** Interoperability between DigiLocker (India) and the European Union Digital Identity Wallet (EUDI Wallet) Ecosystem

Date: July 29<sup>th</sup>, 2026

## Table of Contents

|                                                                                                        |    |
|--------------------------------------------------------------------------------------------------------|----|
| Executive Summary.....                                                                                 | 4  |
| Background and Rationale .....                                                                         | 4  |
| Strategic Objectives.....                                                                              | 5  |
| Scope .....                                                                                            | 5  |
| Institutional Roles and Trust Anchors.....                                                             | 6  |
| India-Side Institutions.....                                                                           | 6  |
| EU-Side Institutions .....                                                                             | 6  |
| Other Stakeholders.....                                                                                | 6  |
| Interoperability Model.....                                                                            | 6  |
| Core Design Principles .....                                                                           | 7  |
| Fundamental Pillars .....                                                                              | 7  |
| i) Pillar 1: Onboarding and Pre-Travel Access.....                                                     | 7  |
| ii) Pillar 2: Time-Based Access Control and Session Lifecycle.....                                     | 10 |
| iii) Pillar 3: Authentic Document (VC) Issuance Mechanism .....                                        | 11 |
| iv) Pillar 4: Decentralized Presentation and Offline Trust Verification .....                          | 12 |
| v) Pillar 5: Immutable Audit Logging for Legal and Regulatory Monitoring.....                          | 13 |
| High-Level Components .....                                                                            | 14 |
| Phased Integration Roadmap.....                                                                        | 14 |
| Phase 1: Legal and Regulatory Foundation.....                                                          | 14 |
| Phase 2: Proof of Concept — Limited Live Pilot.....                                                    | 14 |
| Phase 3: Full Mutual Recognition and Sectoral Expansion .....                                          | 15 |
| Phase 4: Global Extension .....                                                                        | 15 |
| Technical Standards and Core Components.....                                                           | 15 |
| Core Technical Standards .....                                                                         | 15 |
| Technical Standards Summary .....                                                                      | 16 |
| Security Architecture, Operational Resilience and Extensibility Framework.....                         | 16 |
| Security Architecture: Key Management, Certificate Management, Encryption and Trust Establishment..... | 16 |
| Trust List and DID Registry Distribution: High Availability and Resilience.....                        | 17 |
| ML-Based Threat Model and Risk Mitigation.....                                                         | 17 |
| Non-Functional Requirements (NFRs) .....                                                               | 18 |
| Monitoring, Logging and Alerting for Operational Visibility.....                                       | 18 |
| Credential Revocation and Status Validation.....                                                       | 19 |

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| API and Credential Format Versioning and Backward Compatibility ..... | 19 |
| Offline Verification Support .....                                    | 19 |
| Onboarding Framework for Future Sovereign Wallets.....                | 20 |
| Detailed Cryptographic Handshake and Data Flow Architecture .....     | 20 |
| a. Native Issuance Flow (OpenID4VCI) .....                            | 20 |
| b. Peer-to-Peer Presentation Flow (OpenID4VP) .....                   | 21 |
| Onboarding, Identity Proofing and Aadhaar Considerations .....        | 22 |
| Aadhaar Onboarding Challenge.....                                     | 22 |
| Mitigation Strategies .....                                           | 22 |
| Data Protection, Sovereignty and Residency .....                      | 22 |
| Technical Interoperability Gaps and Mitigation .....                  | 23 |
| Identified Gaps .....                                                 | 23 |
| Mitigation Measures.....                                              | 23 |
| Risk Assessment: Private Wallet Monopoly and Sovereignty .....        | 23 |
| Private Wallet Monopoly Threat.....                                   | 23 |
| DigiLocker–EUDI Counterstrategy .....                                 | 23 |
| Regulatory and Policy Recommendations .....                           | 24 |
| India-Side Measures.....                                              | 24 |
| Aligning Private Wallets to Open Standards.....                       | 24 |
| EU-Side Measures.....                                                 | 24 |
| Use Cases, Benefits, and Impact .....                                 | 24 |
| Primary Use Cases.....                                                | 24 |
| Quantified and Strategic Benefits .....                               | 25 |
| Annexures .....                                                       | 25 |

## Executive Summary

This concept note outlines a framework for interoperability and mutual recognition between India's DigiLocker platform and comparable international digital identity systems, anchored in a sovereign-to-sovereign model of digital trust. It proposes a travel-centric model designed to support international mobility, enable regulated exchange of digital credentials, and ensure privacy-preserving verification across jurisdictions. Rather than requiring an Indian traveler to acquire a foreign wallet, the framework upgrades DigiLocker itself into a W3C Verifiable Credential (VC) native holder wallet, capable of presenting credentials directly and peer-to-peer to any conformant relying party or wallet in the European Union, and, symmetrically, capable of verifying EUDI Wallet-issued credentials presented by EU citizens in India. The model envisions DigiLocker and the European Digital Identity (EUDI) Wallet ecosystem as interoperable public digital infrastructure systems, connected through mutual recognition, open standards, shared trust frameworks, and consent-based data exchange. It also serves as a broader reference model for future collaboration among sovereign digital identity ecosystems across India, the European Union, and other partner jurisdictions.

The proposed model aims to facilitate a secure, privacy-preserving, and legally robust exchange of digital credentials across borders, covering use cases such as travel, education, employment, financial services, healthcare, and public service delivery. It is structured around five core implementation pillars: onboarding and pre-travel intimation, time-bound access controls, authoritative credential issuance into the holder wallet, decentralized peer-to-peer credential presentation, and tamper-evident audit logging. Together, these elements are designed to enable cross-border use of government-issued credentials while avoiding the creation of persistent offshore copies of citizen data, avoiding live tracking of citizens by any gateway, and avoiding dependence on real-time cross-border connectivity at the point of use.

## Background and Rationale

Digital public infrastructure is increasingly becoming central to cross-border mobility, service access, and trust-based verification. India's DigiLocker has emerged as a large-scale government-backed platform for issuance, access, and sharing of digital records, while the EUDI Wallet framework under the revised eIDAS regime is designed to support secure and user-controlled digital identity and credential use across European jurisdictions.

At present, cross-border acceptance of credentials remains fragmented. Students, professionals, travellers, employers, regulators, and service providers often rely on apostille processes, manual attestation, physical document presentation, and repetitive verification workflows. These processes increase cost, delay, and compliance burden.

A structured interoperability model between DigiLocker and the EUDI Wallet can reduce this friction by enabling selective disclosure, offline-verifiable trust, and mutual recognition between public institutions rather than proprietary platforms. Such a model can also strengthen digital sovereignty by preventing excessive dependence on private wallet

ecosystems, and it must be built so that no foreign gateway is technically or legally positioned to record when, where, or to whom an Indian citizen presents a credential.

## Strategic Objectives

- Enable mutual recognition of sovereign digital wallets so that credentials issued in one jurisdiction can be accepted in the other without repetitive attestation or manual verification.
- Establish a standards-based and privacy-preserving mechanism for cross-border exchange of identity, educational, professional, financial, health, and travel-related credentials, without requiring either side's citizens to onboard a second, foreign-issued wallet.
- Protect digital sovereignty through government-anchored trust frameworks, native upgrade of DigiLocker to a W3C VC-compliant wallet, and avoidance of exclusive dependence on private wallet providers or any centralized cross-border gateway.
- Demonstrate a scalable digital public infrastructure interoperability model that may be extended to other partner countries and regions, sequenced correctly so legal recognition precedes live data exchange.

## Scope

1. Sovereign control over trust anchors, issuer accreditation, and legal recognition.
2. User-consented, purpose-bound, and minimal disclosure exchange, executed directly between the citizen's own device and the verifier, with no intermediary able to observe the transaction.
3. Native, standards-based issuance of authoritative records by concrete Sovereign Issuing Authorities directly into the citizen's DigiLocker wallet ahead of travel, rather than either static document replication or real-time cross-border lookups at the point of use.
4. Hardware-backed wallet security on the user's own device (the DigiLocker app itself) at the point of onboarding, issuance, and presentation.
5. Strict time-bounded entitlement for foreign-use access linked to the traveler's lawful stay, enforced through credential-embedded expiry rather than externally triggered device actions.
6. Dual-ended, metadata-only auditability for legal defensibility without movement tracking.
7. Jurisdictions covered: Republic of India and the 27 EU Member States, with an extension path to EUDI-compatible non-EU jurisdictions (e.g., UK, Norway, Switzerland) and selected Global South partner nations.
8. Document and credential categories: identity documents; education credentials; professional and vocational licenses; financial and tax credentials; residence and civil status proofs; health and social protection credentials.
9. Stakeholder groups: Indian and EU students, professionals, tourists, migrants, universities, employers, banks, regulators, hospitals, and government agencies.

## Institutional Roles and Trust Anchors

### India-Side Institutions

1. **MeitY / Government of India:** Policy custodian for DigiLocker, anchor authority for trust, governance, interoperability rules, and international arrangements.
2. **DigiLocker issuer ecosystem:** Registered issuer partners connected to DigiLocker through approved APIs and issuance workflows, progressively upgraded to issue natively signed W3C Verifiable Credentials.
3. **UIDAI:** Foundational identity proofing and tokenized identity assertions, where legally permissible.
4. **MoRTH and transport registries:** Driving license and transport-related records relevant to mobility use cases.
5. **MEA / passport systems:** Passport-linked identity and travel verification support, where permitted.
6. **CBDT and related agencies:** Tax identity and income-linked records relevant for defined compliance or mobility use cases.
7. **Education boards, universities, and other public issuers:** Academic and institutional credentials made available through DigiLocker.

### EU-Side Institutions

1. **European Commission:** Policy authority for eIDAS 2.0 and the EUDI Wallet framework, including third-country trust recognition pathways.
2. **ENISA and related technical bodies:** Trust framework and technical architecture support for trusted issuer and conformity systems.
3. **EU Member State authorities:** National wallet operators, relying parties, and domestic legal recognition authorities.

### Other Stakeholders

1. **Issuers:** Universities, regulators, boards, hospitals, transport authorities, tax agencies, and other accredited entities.
2. **Relying parties:** Universities, employers, banks, hospitals, immigration authorities, embassies, councils, and regulated service providers — including EU-side EUDI Wallet apps, which act as verifiers of DigiLocker-presented credentials rather than as holders of them.
3. **End users:** Indian citizens, NRIs, OCIs, EU citizens, EU residents, and other eligible persons using credentials across borders.

## Interoperability Model

The proposed model treats DigiLocker itself as the sovereign holder wallet for Indian citizens, upgraded to natively support the W3C Verifiable Credentials (VC) data model and SD-JWT credential formats. Rather than an Indian traveler

downloading, onboarding onto, or transferring credentials into a foreign wallet, DigiLocker remains the single holder of the citizen's credentials at all times.

## Core Design Principles

- **DigiLocker as native holder wallet:** DigiLocker is upgraded to issue, store, and present W3C VC / SD-JWT credentials natively. No Indian traveler is required to be issued a foreign EUDI Person Identification Data (PID) attestation, and no traveler downloads or onboards a second wallet abroad — foreign tourists on short-term visas cannot, in any case, be lawfully issued an official EUDI PID under eIDAS 2.0.
- **Peer-to-peer presentation:** Credential presentation moves directly from the citizen's DigiLocker app to the verifier's system using **OpenID4VP**, whether the verifier is a web portal, a border checkpoint terminal, or a local EUDI Wallet instance used purely to scan and validate the presentation. No centralized gateway sits in the credential-presentation path.
- **Offline trust-list verification:** Verifiers (on either side) periodically cache signed Trusted Lists or DID Registries and validate signatures locally, without contacting a live central endpoint at the moment of verification.
- **Native, device-bound cryptography:** Credentials are signed by the authoritative issuer, or by DigiLocker acting as an authorized primary issuance endpoint at the moment of credential creation — never re-signed or re-packaged from legacy formats after the fact — and every presentation is bound to the traveler's own device through a hardware-backed Key Binding JWT (KB-JWT).
- **Offline-first credential lifecycle:** Credentials needed for travel are issued into DigiLocker's local secure storage well ahead of departure. Validity and revocation are enforced through standard exp claims and cryptographic status mechanisms (e.g., Status List 2021) rather than real-time cross-border lookups or externally triggered cache purges.
- **Legally sequenced rollout:** Technical interoperability is built on globally open standards (W3C VC, OpenID4VP, ISO 18013-5) so that no side is asked to certify against the other's proprietary rules, and any live exchange of production personal data is preceded by the applicable bilateral legal recognition (data adequacy, eIDAS Article 14 recognition, Trust List inclusion).

## Fundamental Pillars

### i) Pillar 1: Onboarding and Pre-Travel Access

#### a. Objective

This pillar establishes a lawful, user-consented, and low-friction cross-border onboarding path before departure, so that the destination ecosystem can recognize a pending traveler's DigiLocker-issued credentials without pre-positioning raw citizen data outside India and without requiring the traveler to acquire any new wallet. It functions as a pre-clearance lane: DigiLocker communicates only the minimum signed Registration Intent Credential (a

Verifiable Credential) required so that destination relying parties can later recognize and verify the traveler's presentations.

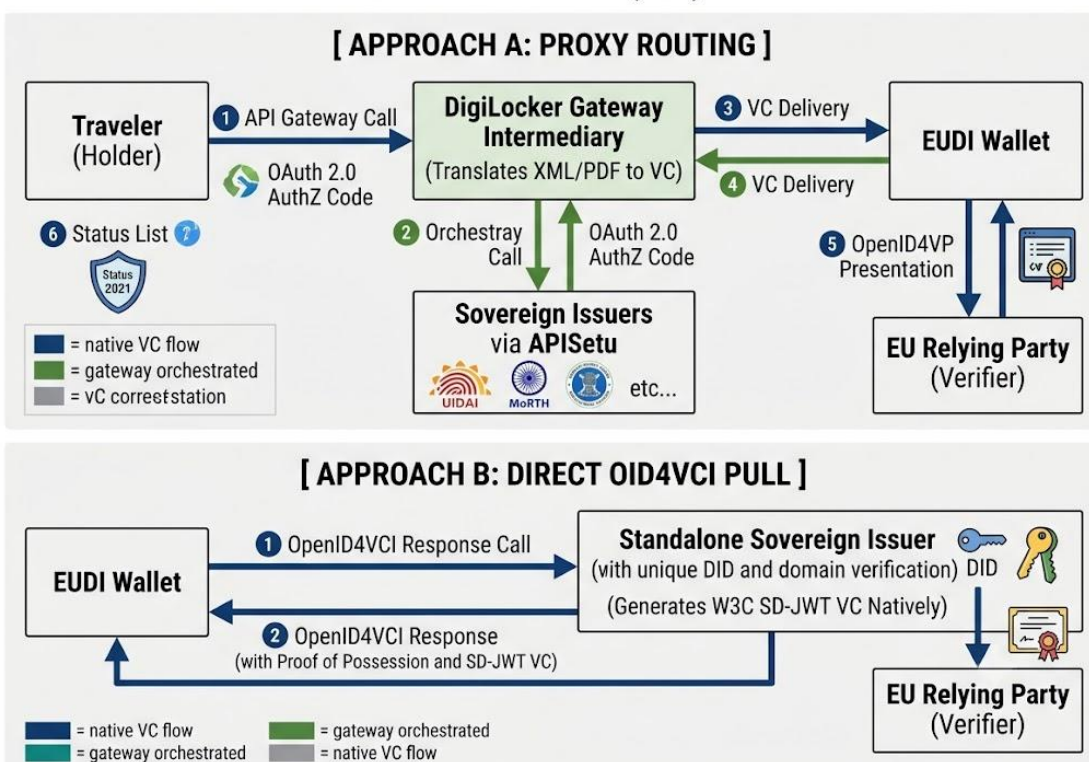
## b. Onboarding

DigiLocker links with the EUDI ecosystem as a mutually recognized sovereign wallet issuer via the partner ecosystem (i.e., APISetu on the India side and the relevant Member State / EU trust infrastructure on the EU side) to establish trust anchors between the two independent networks. This governs trust establishment and the recognition of DigiLocker-issued, W3C-conformant Verifiable Credentials (VCs) and Verifiable Presentations (VPs) by EU relying parties — and, symmetrically, recognition of EUDI Wallet-issued VCs by Indian relying parties. No wallet-to-wallet data routing or translation gateway sits between the two ecosystems; onboarding establishes trust recognition, not a live data channel.

## c. User Journey and Flow Mapping

The traveler opens the “International Travel” section inside DigiLocker itself, signs in using DigiLocker’s native verified channels, and reviews the terms governing cross-border use, retention, and reliance. There is no selection among multiple destination wallets inside DigiLocker — DigiLocker remains the traveler’s single wallet throughout the journey, and the traveler simply declares an intended destination Member State.

## OID4VC AUTHENTIC DOCUMENT (VC) PULL MECHANISMS



### *The Core Flow Execution:*

1. **Initiation:** The traveler, acting as the holder, opens “International Travel” inside DigiLocker.
2. **Consent & Destination Selection:** The user consents to “Outbound Travel Intent to EU” and declares the destination Member State.
3. **Verification:** DigiLocker verifies the traveler using its native login stack (e.g., OTP to verify mobile or email).
4. **Intent Generation:** DigiLocker issues a short-lived Registration Intent Credential (VC) to itself and asynchronously registers the corresponding trust-resolution record with the EUDI federation’s recognition registry.
5. **Recognition:** EU-side relying parties (including local EUDI Wallet instances used as verifiers) are able to recognize and later verify presentations made from that DigiLocker session, based on public trust registries and decentralized status mechanisms — without any wallet ingesting or holding a copy of the traveler’s credentials on the EU side.

### **d. Registration Intent Metadata Packet (Registration Intent Credential VC)**

The registration intent is modeled strictly as a Verifiable Credential (Registration Intent Credential) conforming to the W3C VC Data Model. The credential is signed by DigiLocker (via did:web) to a pseudonymous subject identifier and includes only minimal, policy-conformant claims:

- Origin wallet identifier and corridor/session identifier with access timeframe information.
- Declared destination Member State.
- Pseudonymous traveler correlation identifier generated for the corridor session (e.g., a unique session-bound DigiLocker ID).
- Verified communication handles (hashed or minimal confirmed attributes) represented as signed verification claims.
- Consent receipt identifier and a reference to the underlying digital consent artifact.

The Registration Intent Credential is retained by DigiLocker as the holder; only a trust-resolution record (not the credential itself) is shared with the EUDI recognition registry, allowing any conformant relying party to later verify a DigiLocker-presented VP using standard OpenID4VP verification semantics.

### **e. Asynchronous Signaling Architecture**

Because a traveler may register before departure, while verification only occurs on arrival or at the point of service, signaling remains fundamentally asynchronous and metadata-only. DigiLocker publishes registration-state metadata, cryptographic hashes, or handles — never substantive personal data — to the EU-side recognition registry. No live, synchronous connection is required between DigiLocker and any EU system at the moment a traveler actually presents a credential; verification depends on the offline-cached trust list described in Pillar 4.

#### f. Destination / Post-Arrival Presentation

1. On arrival or at the point of service, the traveler opens DigiLocker on their own device — the same wallet used to onboard in India. No new wallet is downloaded, and no local EUDI Wallet ingests the traveler's credentials.
2. The traveler selects the relevant credential(s) already provisioned into DigiLocker ahead of travel (see Pillar 3) and initiates a Verifiable Presentation.
3. DigiLocker builds a Verifiable Presentation (VP), selectively disclosing only the required claims, and signs it using a hardware-backed Key Binding JWT (KB-JWT) generated on the traveler's own device.
4. The traveler presents the VP directly to the relying party — a web portal, border checkpoint, or a local EUDI Wallet instance acting solely as a verifier/scanner — via OpenID4VP (remote QR/deep link or proximity BLE/NFC).
5. The relying party independently verifies the VP's signature and revocation status against its own offline-cached Trust List / DID registry, with no live query back to India required.

#### g. Key Principles

- **Sovereign-to-Sovereign Trust:** Trust is anchored exclusively in MeitY and the European Commission/ENISA, bypassing commercial gatekeepers.
- **Single Holder Wallet:** DigiLocker remains the sole holder and presenter of the traveler's credentials throughout the journey; no credential is transferred into or duplicated inside a foreign wallet.
- **Privacy-by-Design:** Minimized data payloads achieved via claim-level selective disclosure using SD-JWT VC profiles, and peer-to-peer presentation that leaves no centralized transaction record.
- **Offline-Verifiable Trust:** Relying parties validate assertions using periodically synced, locally cached trust lists rather than live, per-transaction status endpoints.

### ii) Pillar 2: Time-Based Access Control and Session Lifecycle

#### a. Objective

This pillar prevents indefinite foreign reuse of the cross-border corridor and ensures that access rights terminate automatically when the lawful travel period ends — expressed as an intrinsic property of the credential itself, not as an external command that reaches into the traveler's device. The architecture utilizes strict, non-extendable validity windows, modeled as Corridor Lease Credential VCs, linked directly to the authorized stay window (e.g., a 90-day Schengen stay, or a visa-specific duration asserted through lawful travel metadata).

#### b. Time-Based Wallet Access

DigiLocker issues a Corridor Lease Credential natively to itself as part of the traveler's onboarding, containing:

- Corridor session identifier.

- Traveler pseudonymous subject reference.
- Device-bound key reference (the traveler’s own DigiLocker app instance).
- A standard exp claim marking hard expiry, alongside a not-before timestamp.
- Permitted relying-party classes or credential categories.
- A non-extendable flag preventing silent renewal.

Any credential presentation must reference a valid, unexpired Corridor Lease Credential. Enforcement relies on the standard exp claim: verifiers automatically reject an expired credential at the point of verification. DigiLocker additionally marks the corresponding presentation capability as inactive within the app once the lease expires, but no external gateway command purges the device’s local cache — expiry is a property the credential itself carries and that any verifier can check independently, including offline.

### c. Non-Extendability and Renewal

A corridor lease cannot be silently extended by user action, background API traffic, or local wallet refreshes. Any extension mandates a fresh sovereign authorization cycle: a new DigiLocker travel-intent declaration and a renewed issuance event under a current legal basis. This strict lifecycle ensures the credential never becomes permanent, standing entitlement beyond the lawful stay.

## iii) Pillar 3: Authentic Document (VC) Issuance Mechanism

### a. Objective

The framework enforces authoritative, pre-travel issuance of Verifiable Credentials directly into the traveler’s DigiLocker wallet, in place of either ad hoc real-time lookups at the border or indefinite static document replication. Following initial consent, specified credentials are issued into DigiLocker’s secure on-device storage ahead of travel, and are queryable and presentable on demand, thereafter, including in offline or low-connectivity conditions.

### b. Trigger Path Inside DigiLocker

When a traveler requests a credential inside DigiLocker ahead of travel:

1. The traveler selects the required credential type (e.g., driving license, educational proof, civil status) within DigiLocker.
2. DigiLocker verifies that the traveler’s Corridor Lease Credential is active and within policy scope.
3. The request is generated — including requested schema type, single-use nonce, and cryptographic proof-of-possession tied to the traveler’s own device key.

### c. Native Issuance Flow

The Sovereign Issuing Authority (e.g., UIDAI, MoRTH, NHA, MEA, a university, or a professional regulator), connected via APISetu, either issues the credential as a natively signed W3C-conformant Verifiable Credential (SD-JWT VC) directly, or — where an issuer

has not yet completed its own native upgrade — DigiLocker acts as an authorized primary issuance endpoint on the issuer’s behalf, signing the credential at the moment of creation under its own did:web identifier with the issuer’s explicit delegation. In both cases, the credential is created once, natively, in VC form, and stored directly in DigiLocker’s secure on-device storage; no legacy XML or PDF-A record is stripped of its original signature and re-wrapped after the fact, and no EUDI Wallet or other foreign application is involved in retrieving or holding this credential — DigiLocker itself is both the recipient and the sole holder of the issued credential.

#### **iv) Pillar 4: Decentralized Presentation and Offline Trust Verification**

##### **a. Objective**

Once credentials reside securely inside DigiLocker, they must be seamlessly presentable across web portals, remote application tracks, and physical in-person checkpoints — without exposing excessive user data, without requiring a live connection back to India, and without the credential ever leaving DigiLocker for another wallet.

##### **b. SD-JWT VC for Web and Portal Verification**

SD-JWT VC serves as the canonical profile of the W3C VC Data Model, transforming standard claims into selectively disclosable elements from the point of native issuance. When presenting via OpenID4VP, DigiLocker discloses only purpose-bound attributes (e.g., an “age over 18” status or a “degree awarded” flag) while cryptographically blinding all adjacent, unnecessary identity fields. This satisfies rigorous privacy-by-design requirements globally.

##### **c. Offline Trust List Verification**

Relying parties on either side — web portals, border checkpoints, or a local EUDI Wallet instance used purely as a verifier — periodically download and cache the signed Trusted List (or DID Registry) of recognized issuers and validate a presented VP’s signature and issuer status locally using that cached list. No relying party is required to ping a live Trust Registry endpoint at the moment of verification; trust lists are refreshed on a defined periodic cycle, and revocation is checked against a cryptographic status mechanism (e.g., Status List 2021) rather than a synchronous, per-transaction registry call. This preserves anti-tracking guarantees under eIDAS 2.0 and privacy-by-design principles under the DPDP Act, since no gateway or registry operator can observe when, where, or to whom a citizen presents a credential.

##### **d. Peer-to-Peer Presentation, No Cross-Wallet Transfer**

Presentation of a DigiLocker-issued credential to a European relying party — and, symmetrically, presentation of an EUDI Wallet-issued credential to an Indian relying party — moves directly between the citizen’s own device and the verifier’s system via OpenID4VP. Credentials are never transferred into, duplicated inside, or co-held by a second wallet application; the original issuer’s signature and provenance are preserved

end-to-end, and any relying party can execute standard validation rules directly against the holder's presentation.

## v) Pillar 5: Immutable Audit Logging for Legal and Regulatory Monitoring

### a. Objective

Cross-border interoperability requires durable, legally defensible evidence of explicit user consent and processing integrity without creating a centralized tracking instrument. The architecture strictly adheres to both India's Digital Personal Data Protection (DPDP) framework and the EU's privacy expectations by eliminating the ingestion of raw identity trails at any central point.

### b. Dual-Ended Localized Logging Model

Rather than assembling a single multi-jurisdictional database, the architecture enforces synchronized, localized append-only log stores at both ends:

- **India-Side Log:** Maintained natively by DigiLocker and the respective Indian Sovereign Issuing Authorities, recording issuance and presentation events initiated from the traveler's own device.
- **EU-Side Log:** Maintained independently by each relying party or Member State wallet-verifier operator, recording verification events performed locally.

### c. Technical Logging Hooks

- **Transaction Event Hooks:** Recorded at the point of issuance (within DigiLocker or at the Sovereign Issuer) and at the point of verification (within the relying party or verifying EUDI Wallet instance) never at a shared intermediary.
- **Cryptographic Records:** Each side store hashes of its own native OpenID4VCI issuance events and OpenID4VP presentation exchanges, together with the relevant did:web signatures, independently of the other side.
- **Consent Validation:** Linked to decentralized consent receipts signed by DigiLocker under the traveler's own session key, and, on the EU side, to the relying party's own consent record.

### d. Immutability and Legal Evidence

Logs on both sides are strictly metadata-only. They contain trusted timestamps, transaction event types, pseudonymous corridor session identifiers, authority codes, success/failure states, and cryptographic hashes of the envelopes. Raw personal data, document contents, and location tracks are completely redacted at the point of ingestion.

Immutability is achieved via append-only architecture, cryptographic chaining of entries, and hardware security module (HSM) log sealing, providing a tamper-evident, shared evidence schema for regulatory audit or judicial review without data exposure risks.

## High-Level Components

| Standard                          | Purpose                                                  | Applicability                                                |
|-----------------------------------|----------------------------------------------------------|--------------------------------------------------------------|
| W3C Verifiable Credentials (VC)   | Credential data model                                    | Both sides                                                   |
| OpenID4VP / OpenID4VCI            | Peer-to-peer credential issuance & presentation protocol | Both sides                                                   |
| SD-JWT (Selective Disclosure JWT) | Privacy-preserving attribute sharing                     | EUDI / DigiLocker                                            |
| DID (Decentralised Identifiers)   | Issuer & wallet identification                           | Offline-cached trust registry                                |
| Status List 2021                  | Cryptographic revocation and status checking             | Both sides                                                   |
| eIDAS Trust Lists                 | Qualified trust service provider recognition             | EU + India crosswalk, synced periodically and cached offline |

## Phased Integration Roadmap

The roadmap is sequenced so that legal mutual recognition is secured before any live, production exchange of personal credentials takes place. Technical conformance work and sandbox testing may proceed in parallel with legal negotiations, but no production pilot involving real user data is launched ahead of the applicable bilateral recognition.

### Phase 1: Legal and Regulatory Foundation

- Negotiate and conclude the bilateral legal basis for exchange: an India–EU data transfer arrangement with protections comparable to GDPR adequacy decisions and DPDP requirements, and formal steps toward eIDAS Article 14 recognition of MeitY/CCA as an equivalent trust framework.
- Align technical standards (W3C VC, OpenID4VCI/OpenID4VP, SD-JWT, DIDs, ISO 18013-5) between the two ecosystems, and complete conformity assessment of DigiLocker’s native VC issuance capability.
- Conduct sandbox-only technical conformance testing with synthetic data — no live citizen data is exchanged at this stage.

### Phase 2: Proof of Concept — Limited Live Pilot

- Once the Phase 1 legal basis is in place, launch a limited live pilot scoped to education credentials (degree certificates, transcripts, English proficiency certificates) issued natively via DigiLocker and verified by three pilot EU Member States and 10–15 pilot institutions.

- Include India's DID Registry entries in the relevant EUDI Trusted Issuer List for the pilot scope and confirm both sides can perform offline trust-list verification in production conditions.

### Phase 3: Full Mutual Recognition and Sectoral Expansion

- Expand to professional qualifications, driving licenses and core identity attributes, on the basis of the legal recognition already secured.
- Achieve mutual recognition of all major DigiLocker document categories and corresponding EUDI Wallet credentials, and onboard at least 10 additional EU Member States.
- Publish open APIs and reference implementation toolkits for relying parties and issuers.

### Phase 4: Global Extension

- Extend the framework to EUDI-compatible third countries (e.g., UK, Norway, Switzerland), applying the same legal-recognition-before-live-pilot sequencing.
- Offer a reference model and technical toolkit to Global South nations to interoperate with DigiLocker and EUDI using open standards.

## Technical Standards and Core Components

### Core Technical Standards

The DigiLocker–EUDI interoperability model adopts the global OID4VC (OpenID for Verifiable Credentials) framework as its foundational architecture, utilizing the following specifications to ensure secure, standards-compliant cross-border operations:

- **W3C Verifiable Credentials (VC) Data Model v2.x:** Serves as the canonical abstraction and credential data model for all cross-border exchanges.
- **OpenID4VCI (OpenID for Verifiable Credential Issuance):** The protocol governing how DigiLocker natively receives Verifiable Credentials from Sovereign Issuing Authorities ahead of travel.
- **OpenID4VP (OpenID for Verifiable Presentations):** The standard presentation protocol used by DigiLocker to securely transmit Verifiable Presentations (VPs) containing disclosed attributes directly to relying parties, online or in person.
- **SD-JWT (Selective Disclosure JWT):** The primary token profile for W3C VCs, allowing privacy-preserving, claim-level attribute sharing.
- **Decentralized Identifiers (DID):** Used for cryptographic identity verification of issuers and DigiLocker (leveraging did:web for domain-verified endpoint resolution), resolved by relying parties from a periodically synced, locally cached trust list.

## Technical Standards Summary

| Component             | Model                                                                                                                                                                                                        |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Credential Format     | Natively issued in W3C VC / SD-JWT form at the point of creation by the Sovereign Issuing Authority, or by DigiLocker as an authorized primary issuance endpoint. No post hoc translation of legacy formats. |
| Issuance Protocol     | OpenID4VCI, issuing directly into DigiLocker's on-device secure storage ahead of travel.                                                                                                                     |
| Presentation Protocol | OpenID4VP, peer-to-peer from DigiLocker directly to the relying party (remote QR/deep link or proximity BLE/NFC) no intermediary gateway.                                                                    |
| Trust Resolution      | Decentralized trust lists (eIDAS Trust Lists / India DID Registry) synced periodically and cached locally by each relying party for offline verification.                                                    |
| Status Checking       | Status List 2021 / OCSP-compatible status mechanism, checked by the verifier against a periodically refreshed cache; expiry enforced via the credential's own exp claim.                                     |

## Security Architecture, Operational Resilience and Extensibility Framework

To strengthen the technical robustness, operational resilience and long-term extensibility of the DigiLocker–EUDI interoperability framework, this section defines the underlying security architecture, trust-list distribution resilience design, threat model, non-functional requirements, operational monitoring approach, credential lifecycle management, versioning strategy, offline verification support, and a pathway for onboarding future sovereign wallets.

### Security Architecture: Key Management, Certificate Management, Encryption and Trust Establishment

The interoperability model between DigiLocker and the EUDI Wallet rests on an explicitly defined security architecture rather than implicit trust between participating systems.

- **Key management:** Each issuer connected through APISetu maintains its own PKI key chain, generating and rotating signing keys within hardware security modules (HSM); DigiLocker validates issuer signatures against published public keys rather than custodial issuer private keys, and DigiLocker's own did:web signing key is likewise HSM-protected when it acts as an authorized issuance endpoint.
- **Certificate management:** X.509 certificates for issuer signing endpoints and DigiLocker's own signing infrastructure are issued and renewed through a defined certificate authority hierarchy, with automated expiry monitoring and renewal well ahead of expiry to avoid service disruption.

- **Encryption:** All data in transit during issuance (DigiLocker to issuer, over APISetu) and during presentation (DigiLocker directly to a relying party) uses mutually authenticated TLS 1.3; any trust-list or registry data synced between MeitY and EU authorities is likewise encrypted in transit, and metadata retained for audit purposes is protected using envelope encryption with keys managed independently of the encrypted data store.
- **Trust establishment:** Trust between DigiLocker and EUDI systems is established through Decentralized Identifiers (DIDs). eIDAS maintains its own DID registry, whereas DigiLocker does not; DigiLocker instead leverages did:web, which is compliant with the standards and allows issuer identity to be resolved directly from a hosted, domain-verified endpoint, then cached by relying parties for offline use.
- **Device hardware binding:** At the moment of presentation, DigiLocker signs a Key Binding JWT (KB-JWT) using a hardware-backed private key stored in the traveler's device Secure Element/StrongBox, cryptographically binding the presentation to that specific device and preventing spoofing or replay.
- **Challenges:** OpenID4VCI and OpenID4VP are recognized standards; each issuer must maintain its own PKI key chain and produce outputs aligned with W3C standards. A dedicated development team must manage VC lifecycle operations such as issuance, revocation, expiration and key rotation, and DigiLocker's own upgrade to a native VC-issuing and VC-holding wallet is itself a significant engineering undertaking.

### Trust List and DID Registry Distribution: High Availability and Resilience

- **High availability:** The periodic Trust List / DID Registry publication and synchronization service (used by relying parties to build their offline verification caches) should be deployed as a stateless, horizontally scalable service across at least two availability zones within India, with active-active load balancing so that a zone failure does not interrupt scheduled trust-list distribution.
- **Failover:** Automated health checks should detect degraded distribution nodes and reroute traffic within seconds. Because this service distributes only public, non-personal trust-list data on a periodic batch cycle rather than routing live credential exchanges, a temporary outage delays trust-list refresh but does not interrupt any traveler's ability to present or verify a credential already cached offline.
- **Disaster recovery:** A geographically separate disaster recovery site should maintain warm-standby infrastructure with a target Recovery Time Objective (RTO) of under 15 minutes for the trust-list distribution service and a Recovery Point Objective (RPO) of near-zero for the (non-personal) trust-list data itself.
- Regular DR drills and chaos-engineering exercises should validate failover readiness ahead of go-live and at defined intervals thereafter.

### ML-Based Threat Model and Risk Mitigation

A structured threat model, supported by machine-learning-based anomaly detection, should be maintained to identify and mitigate risks specific to a cross-border credential exchange corridor.

- **Replay attacks:** Reuse of a captured presentation, token, or request. Mitigated through single-use nonces, proof-of-possession binding via KB-JWT, and short validity windows on all corridor tokens.
- **Compromised devices:** A traveler's own DigiLocker device is jailbroken, rooted, or otherwise compromised. Mitigated through device attestation checks at onboarding, issuance and presentation time, hardware-backed key storage requirements, and ML-based anomaly scoring on device and behavioural signals to flag high-risk sessions for step-up verification.
- **Unauthorized access / credential stuffing:** Attempts to impersonate a traveler or brute-force corridor sessions. Mitigated through rate limiting, adaptive authentication, and anomaly-detection models trained on request velocity, geolocation drift, and login patterns.
- **Man-in-the-middle interception:** Interception of data in transit, mitigated through mutual TLS, certificate pinning and end-to-end signed payload validation.
- **Insider or issuer-side compromise:** Compromise at the issuer or operator level, mitigated through least-privilege access, the immutable audit logging defined under Pillar 5, and periodic conformity assessment of issuers.

ML-based monitoring should operate on metadata-only signals consistent with the framework's privacy-by-design principles, flagging anomalies for human review rather than acting autonomously on citizen data.

## Non-Functional Requirements (NFRs)

- **Scalability:** DigiLocker's native VC issuance and presentation capability should be designed to support Phase 2 pilot-scale concurrent usage, scaling horizontally to accommodate growth through Phases 3–4 without architectural redesign.
- **Performance / response time:** Credential issuance into DigiLocker (a pre-travel, ahead-of-time operation) should target a 95th-percentile completion time of under 2 seconds under normal load; credential presentation at the point of use is a local, on-device operation and is not dependent on network response time.
- **Availability:** The trust-list distribution service and DigiLocker's issuance infrastructure should target 99.9% uptime, consistent with benchmarks for critical government digital infrastructure.
- **Throughput:** The system should be load-tested to sustain peak travel-season volumes, such as visa season and academic admission cycles, without degradation.

These figures are illustrative targets to be refined jointly by MeitY/NeGD and EU technical counterparts during detailed design.

## Monitoring, Logging and Alerting for Operational Visibility

- A centralized, jurisdiction-respecting monitoring layer should track trust-list distribution health, issuance-service latency, error rates and certificate expiry across both India-side and EU-side components.

- Operational logging should extend the metadata-only, privacy-preserving model already defined for audit logging under Pillar 5, adding system performance, capacity and error-condition log distinct from the legal-evidence audit trail.
- Alerting thresholds should be defined for anomalous failure rates, latency spikes, certificate-expiry windows, and threat-model indicators, with defined incident-response runbooks and escalation paths across both India-side and EU-side operations teams.
- Dashboards should be made available to designated government operators without exposing individual traveler-identifiable data.

## Credential Revocation and Status Validation

A formal revocation and status-validation mechanism should be defined so relying parties can always confirm a credential's current state — expired, revoked, or suspended — rather than relying only on a point-in-time issuance signature.

- The Revocation Registry (Status List 2021 / OCSP-compatible mechanism) should support three distinct states with clear semantics: expiry (time-based, automatic via the credential's own exp claim), revocation (issuer-initiated, permanent) and suspension (issuer-initiated, reversible pending review).
- Status checks should be performed by the verifier against its own periodically refreshed cached status list, with defined cache-validity windows so that verification remains possible in degraded-connectivity or fully offline conditions.

## API and Credential Format Versioning and Backward Compatibility

- DigiLocker's native issuance and presentation interfaces should be explicitly versioned (e.g., /v1/, /v2/) with a defined deprecation policy giving relying parties and issuers adequate notice before a version is retired.
- Credential formats (W3C VC, SD-JWT) should carry schema-version identifiers so that consuming relying parties can gracefully handle newer credential fields without breaking on older client implementations.
- New attributes or credential types should be additive wherever possible, with breaking changes limited to major version boundaries and announced through the India-EU technical working group.

## Offline Verification Support

- Credentials support offline verification by design, using locally cached issuer public keys and trust-list snapshots, enabling both remote (OpenID4VP over QR/deep link) and proximity-based verification (BLE/NFC, ISO 18013-7) to function in limited-connectivity scenarios such as border checkpoints or remote areas.
- Offline verification relies on short validity windows and periodically refreshed trust-list snapshots so that a revoked or expired credential cannot be indefinitely presented offline; relying parties are required to sync trust-list and revocation-status data at defined intervals, and the credential's own exp claim provides a hard backstop even if a sync is missed.

## Onboarding Framework for Future Sovereign Wallets

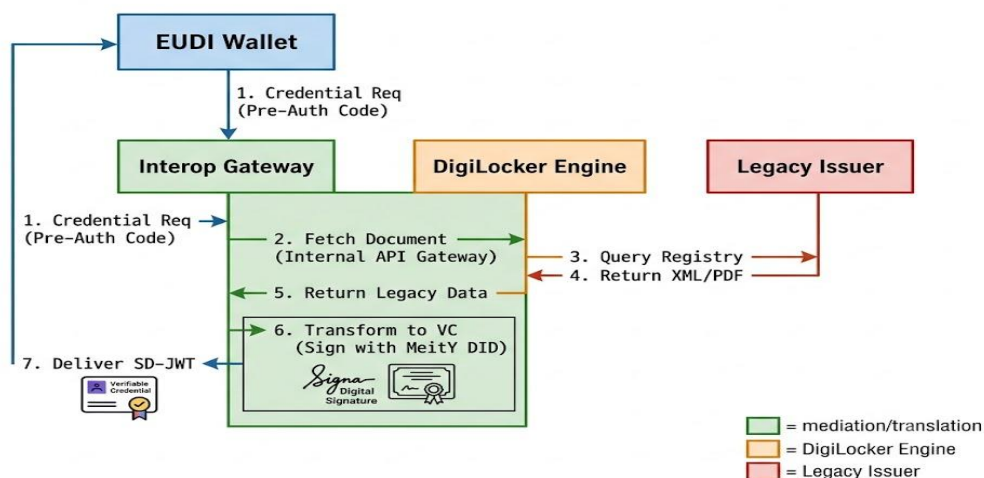
- Onboarding a new sovereign wallet ecosystem beyond the EUDI Wallet should require only: conformance to the shared standards stack (W3C VC, OpenID4VCI/OpenID4VP, SD-JWT, DIDs); a bilateral trust-recognition arrangement between the respective government authorities; and registration in the shared trust registry / trusted-issuer list — with no requirement to certify against a proprietary standard set by either side.
- Support for W3C VC Data Model v2.x (credentials and presentations), including at least one agreed VC profile (JWT/SD-JWT) and the common status mechanism (e.g., Status List 2021), so that new wallets can interoperate with DigiLocker and EUDI without custom per-issuer integrations.
- Since DigiLocker itself is upgraded to natively hold and present VCs, and issuers connected via APISetu issue natively or through DigiLocker as an authorized issuance endpoint, no additional translation layer is required to expose credentials to a newly recognized foreign wallet ecosystem — recognition, not integration, is the primary onboarding task.
- A lightweight onboarding playbook and reference conformance test suite should be published so that new sovereign wallets, including those covered under the Phase 4 Global South extension, can self-certify against the shared open standards with minimal bespoke engineering effort.

## Detailed Cryptographic Handshake and Data Flow Architecture

### a. Native Issuance Flow (OpenID4VCI)

In this model, the Sovereign Issuing Authority issues credentials directly and natively into DigiLocker's secure on-device storage, ahead of travel.

#### HARD-BOUND INTEGRATION APPROACH (GATEWAY-ORCHESTRATED)

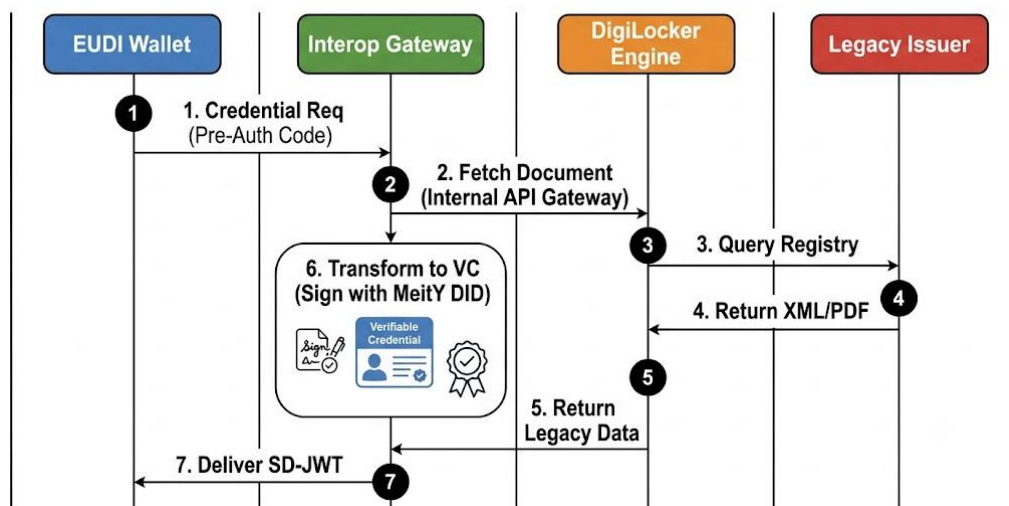


1. **Credential Offer:** The Sovereign Issuing Authority (e.g., UIDAI, MoRTH, NHA, MEA, a university, or a professional regulator) operating a native or DigiLocker-mediated OID4VCI endpoint presents a credential offer containing its Decentralized Identifier (did:web:issuer.gov.in) and supported credential types to DigiLocker.
2. **Token & Proof of Possession Request:** DigiLocker requests an access token from the issuer's OAuth 2.0 authorization server, providing a cryptographic proof of possession (a JWT signed with the traveler's own device's hardware-backed private key, binding the future credential to that physical device).
3. **Native VC Issuance:** The Sovereign Issuing Authority verifies the proof of possession, signs the payload using its own HSM-backed private key (or, where the issuer has delegated this function, DigiLocker signs on the issuer's behalf as an authorized primary issuance endpoint), and issues a native SD-JWT VC directly into DigiLocker's secure storage. No legacy XML/PDF-A record is created, translated, or re-signed as part of this process.

## b. Peer-to-Peer Presentation Flow (OpenID4VP)

In this model, DigiLocker presents credentials directly to the relying party — a web portal, border checkpoint, or a local EUDI Wallet instance used purely as a verifier — with no gateway or foreign wallet holding a copy of the credential.

### COMPLETE OID4VC APPROACH (NATIVE WALLET-TO-WALLET)



1. **Presentation Request:** When encountering an EU relying party (e.g., a university portal, employer, or border checkpoint — including a local EUDI Wallet app used as a verifier), the verifier transmits an OpenID4VP request specifying the required attributes and a unique, single-use nonce, directly to the traveler's device.
2. **Selective Presentation:** DigiLocker parses the request, applies local disclosure rules under user consent, evaluates the active Consent Credential and Corridor Lease Credential, and builds a Verifiable Presentation (VP) containing only the selectively disclosed salts/claims from the original SD-JWT VC. DigiLocker signs the VP wrapper using the traveler's hardware-backed device key (KB-JWT).

3. **Decentralized Verification:** The relying party receives the VP directly from the traveler's device, independently extracts the issuer's signature, resolves the issuer's public key from its own periodically synced, locally cached DID registry (did:web), and checks the credential's exp claim and cryptographic revocation state against its own cached Status List 2021 snapshot — with no data passing back through any central intermediary and no live query to a registry in India at the moment of verification.

## Onboarding, Identity Proofing and Aadhaar Considerations

### Aadhaar Onboarding Challenge

- DigiLocker uses Aadhaar-based eKYC as the primary onboarding mechanism.
- EU citizens do not have Aadhaar, and Aadhaar biometric sharing abroad is prohibited by law; GDPR treats biometric data as special category.
- NRIs/OCIs may lack current Aadhaar linkage.

### Mitigation Strategies

Alternative onboarding:

- For EU citizens: a “Credential Verification Only” flow without full DigiLocker account creation, used only to verify a DigiLocker-presented credential.
- For NRIs/OCIs: use OCI card, Indian passport, or NRI PAN as identity proof.
- Tokenization and virtual IDs: use Aadhaar Virtual IDs and tokenized identifiers; never share raw Aadhaar numbers cross-border.
- No biometric export: ensure no biometric data leaves India; only tokenized or derived identifiers are used.
- Privacy-by-design: enforce minimization, purpose limitation, and explicit consent for cross-border Aadhaar-linked exchanges.

## Data Protection, Sovereignty and Residency

- No Indian citizen's Aadhaar or sensitive personal data is stored on EU servers beyond what is strictly necessary and consented, and none is stored by default since presentation is peer-to-peer, and no EU-side wallet holds a copy of the credential.
- No EU citizen's personal data is stored in India without explicit consent and compliance with GDPR cross-border transfer requirements.
- The interoperability model is designed for zero-knowledge-friendly interactions, transferring proofs or verifiable claims directly between citizen and verifier rather than routing full datasets through any intermediary.
- A joint Data Processing Agreement between MeitY and the European Commission will define roles, purposes, retention, security measures, and data subject rights.
- Consent records and audit trails will be maintained locally on both sides for all cross-border exchanges.

## Technical Interoperability Gaps and Mitigation

### Identified Gaps

- Native VC/SD-JWT issuance capability does not yet exist across all DigiLocker-connected issuers.
- Different revocation mechanisms and status checking approaches.
- Absence of a DID-based issuer registry in India; evolving EUDI ARF.
- Language and script differences between Indian languages and Latin-based EU systems.

### Mitigation Measures

- Prioritize upgrading high-volume DigiLocker issuers to native W3C VC / SD-JWT issuance, with DigiLocker acting as an authorized primary issuance endpoint for issuers not yet upgraded, rather than building a permanent post hoc translation layer.
- Adopt Status List 2021 and OCSP-compatible mechanisms for revocation, checked against periodically cached snapshots.
- Create a government DID registry for India and federate with EU trusted issuer lists, synced on a periodic, non-live basis.
- Use modular architecture to adapt as EUDI ARF matures.
- Implement Unicode normalization and transliteration where acceptable while preserving original language text.

## Risk Assessment: Private Wallet Monopoly and Sovereignty

### Private Wallet Monopoly Threat

- Without sovereign wallet interoperability, private platforms (Apple Wallet, Google Wallet, Microsoft Entra, Meta, payment-network-based identity, commercial KYC platforms) may become de facto identity monopolies.
- Risks include sovereignty loss, vendor lock-in, digital exclusion, surveillance, fragmentation, and democratic concerns.

### DigiLocker–EUDI Counterstrategy

1. Creates a government-to-government trust pathway that bypasses commercial gatekeepers.
2. Uses open standards (W3C VC, OpenID4VP, SD-JWT, DIDs) to avoid vendor lock-in on either side.
3. Demonstrates that sovereign wallets can be interoperable at scale without either side onboarding a foreign wallet, providing a model for G20 and UN-level norms.
4. Allows compliant private wallets to integrate as verifiers of sovereign credentials, provided they respect sovereign trust and data-use rules — without being handed custody of the underlying credential.

## Regulatory and Policy Recommendations

### India-Side Measures

1. Amend DigiLocker Rules 2016 to add an “International Credential Exchange” provision.
2. Issue a notification under Section 69B designating EUDI Wallet issuers as recognized foreign issuers for Indian relying parties.
3. Issue DPDP standards for Adequacy Equivalent treatment of the EU as a data-sharing destination, subject to reciprocity.

### Aligning Private Wallets to Open Standards

1. Require any private wallet or platform participating as a verifier of DigiLocker-issued credentials to conform to the shared open standards (W3C VC, OpenID4VP, SD-JWT) — rather than mandating certification under an India-specific “DigiLocker standard,” which India cannot lawfully impose on wallets operating under foreign law.
2. Prohibit commercial use or profiling based on government-issued credential data.
3. Require non-discriminatory treatment of DigiLocker-issued credentials.
4. Establish a Centre of Excellence for Digital Identity Interoperability at NeGD/DIC.

### EU-Side Measures

1. Publish an eIDAS 2.0 Implementing Act under Article 14 recognizing MeitY/CCA as an equivalent third-country trust framework.
2. Adopt domestic regulations in each Member State allowing the use of DigiLocker-issued credentials for defined services.
3. Include India’s DID Registry entries in the EUDI Trusted Issuer List after conformity assessment.
4. Conclude an India–EU bilateral data transfer arrangement with protections comparable to GDPR adequacy decisions and DPDP requirements.

## Use Cases, Benefits, and Impact

### Primary Use Cases

- Indian students in EU: instant verification of degrees, mark sheets and language certificates, presented directly from DigiLocker.
- Indian professionals in EU: recognition of professional credentials for licensing and employment.
- Visa and tourism: digital presentation of income tax returns, bank statements, and property proof for Schengen visas.
- EU citizens in India: EUDI Wallet credentials verified directly by Indian universities, employers, and RTOs.

- NRI banking and finance: remote onboarding with EU banks and fintechs using DigiLocker PAN, tokenized Aadhaar and income proof.
- Healthcare portability: ABHA-linked DigiLocker health records verified by EU hospitals for emergency treatment and insurance.
- Employer background checks: EU employers verify Indian candidates' credentials directly from DigiLocker.

## Quantified and Strategic Benefits

- Around 150,000 Indian students in EU annually currently face 3–6-week verification delays.
- Around 1.5 million Schengen visa applications from India each year involve costly attestations.
- Apostille and attestation costs of ₹2,000–₹5,000 per document could translate to ₹500–₹1,000 crore in annual savings when replaced with digital verification.
- EU businesses verifying tens of thousands of Indian credentials annually can move from weeks to near real-time verification.
- Strategic benefits for India include digital sovereignty, diplomatic leverage, Global South leadership, economic gains, and citizen empowerment.

## Annexures

### A.1 Sovereign / Government-Issued Wallets (Priority Interoperability Targets)

| Wallet Name       | Country / Region                 | Technology Stack                                                |
|-------------------|----------------------------------|-----------------------------------------------------------------|
| EUDI Wallet       | European Union (27 states)       | eIDAS 2.0 mandated; ARF v1.4; ISO 18013-5; OpenID4VP            |
| DigiLocker        | India                            | MeitY; Aadhaar-linked; 70+ Cr users; DigiLocker XML             |
| BankID            | Norway, Sweden, Denmark, Finland | Bank-issued national eID; 8M+ users; FIDO2 + OpenID Connect     |
| FranceConnect+    | France                           | National identity broker; eIDAS High LoA; OpenID Connect        |
| Ausweis App 2.0   | Germany                          | National eID card app; eIDAS High; PACE + PACE-CAM protocol     |
| GOV.UK One Login  | United Kingdom                   | DCMS managed; post-Brexit non-EU; OpenID Connect; evolving      |
| ItsMe             | Belgium                          | Govt-endorsed private wallet; eIDAS Substantial; OpenID Connect |
| MyID / Smart-ID   | Estonia, Latvia, Lithuania       | E-Residency based; eIDAS High; X-Road interoperability          |
| Austria Mobile ID | Austria                          | MobileConnect based; eIDAS High; deep integration with services |

| Wallet Name          | Country / Region      | Technology Stack                                               |
|----------------------|-----------------------|----------------------------------------------------------------|
| Singpass             | Singapore             | NDI framework; MyInfo integration; OpenID Connect; ASEAN model |
| Digital ID           | Australia             | Digital ID Act 2024; TDIF framework; Aadhaar-equivalent vision |
| Digital Identity     | UAE                   | UAE Pass; Federal ICA; 100+ services; expanding GCC            |
| Aadhar e-KYC         | India (alt)           | UIDAI managed; biometric + OTP; used for DigiLocker onboarding |
| BHIM / eRUPEE Wallet | India (payment layer) | RBI; linked to UPI; could be extended to credential wallet     |
| National Digital ID  | Thailand              | DOPA; OpenID; ASEAN Digital Economy Framework                  |

## A.2 Global Multilateral Frameworks Enabling Wallet Interoperability

| Framework                                    | Scope & Relevance                                                                     |
|----------------------------------------------|---------------------------------------------------------------------------------------|
| HCCH e-APP                                   | Hague Conference e-Apostille; 79 countries; electronic public document authentication |
| ICAO Digital Travel Credential (DTC)         | UN aviation body; ePassport extension; biographic data on mobile                      |
| ISO/IEC 18013-5 (mDL)                        | Global mobile driving licence standard; adopted by EUDI, AAMVA (USA), India VAHAN     |
| W3C Verifiable Credentials                   | Open web standard for credential data model; adopted across all major wallets         |
| OpenID Foundation EUDI Profile               | Standard presentation protocol across EUDI-compatible systems                         |
| ASEAN Digital Economy Framework (DEFA)       | ASEAN digital credential framework — potential expansion beyond EU                    |
| Commonwealth Digital Connectivity Initiative | UK-India-Canada-Australia digital identity alignment (post-CPTPP)                     |
| G20 Digital Economy Task Force               | India-chaired G20 2023 established                                                    |

## A.3 Private Wallet/Platform

| Private Wallet / Platform | Risk Profile                                                                                                                                            |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apple Wallet (USA)        | iOS-integrated; 1.2 Bn+ users; driver's licence in 17 US states; expanding to EU ID cards. Apple controls cryptographic keys and attestation framework. |
| Google Wallet (USA)       | Android-integrated; 2.5 Bn devices; expanding to government ID, transit, event tickets. No sovereign oversight of credential storage.                   |

| <b>Private Wallet / Platform</b> | <b>Risk Profile</b>                                                                                                                                  |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Entra Verified ID      | Enterprise identity; W3C VC compliant; targeting corporate credential issuance globally. Risk of employer-side lock-in.                              |
| Amazon One (Biometric)           | Palm-scan based identity, expanding from payments to access control. No government oversight; biometric data on commercial servers.                  |
| WhatsApp / Meta Identity         | Not yet launched but Meta has 3 Bn users; potential to embed identity into messaging creating unregulated identity infrastructure.                   |
| WeChat (China)                   | Tencent-operated; de-facto national ID for 1.2 Bn users in China; expanding internationally; state-linked but not sovereign in the democratic sense. |
| Mastercard / Visa Identity       | Payment network-based identity; partnering with governments for eKYC; risk of financial identity dependency.                                         |
| Trulioo / Jumio / Onfido         | Commercial KYC platforms; becoming de-facto identity verifiers for banks and fintechs; no public accountability.                                     |