consult hyperion

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

A Framework to Compare National Identity Systems for Interoperability: EUDI and Aadhaar

consult hyperion
consulting by fime

Presentation to the ITU Workshop on Trustable and Interoperable Digital Identities for Human and Agentic AI

Gilad Rosner, Consult Hyperion

Date:
March 30, 2026

consult hyperion

EU-IN DIGITAL POLICY DIALOGUE

Global Gateway

Co-funded by the European Union

Federal Ministry for Digital Transformation and Government Modernisation

Implemented by

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

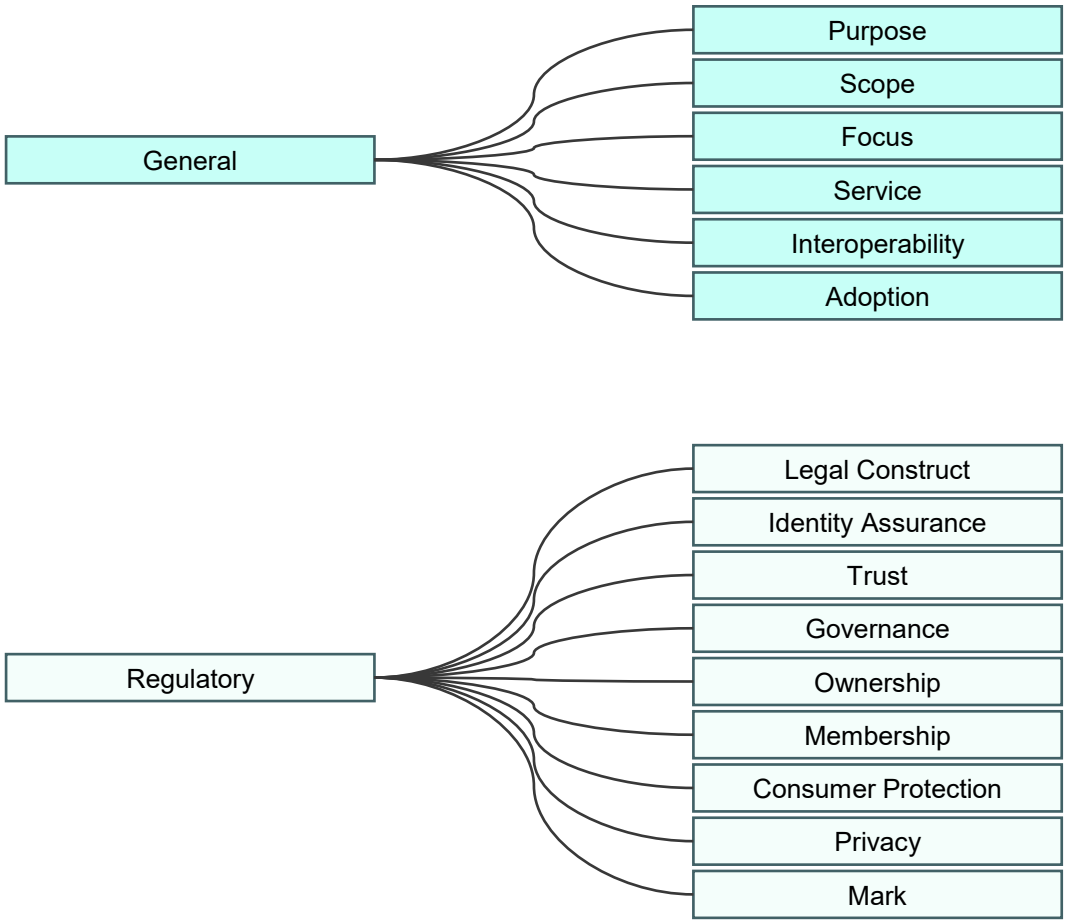
consult hyperion

What do we mean by interoperability?

The ability for the holder of a credential issued in one jurisdiction to present that credential and have it accepted in another jurisdiction.

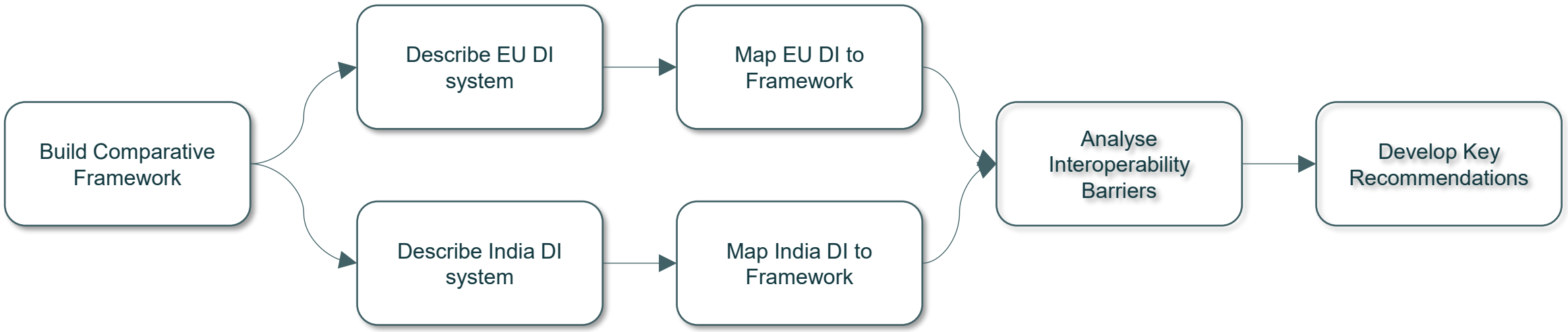
consult hyperion

Comparative Framework



consult hyperion

Methodology for Interoperability Feasibility Study



consult hyperion

Technical Focus – mapping the EU System

Category	Approach	Notes
Architecture	Federated	Leverages decentralised technology but is a network of member state operated (or outsourced) infrastructure – trust lists, wallets.
Data Security	Signed Data RP access certificates	Verifiable credential based RPs need certificate to request presentation from wallet.
Data Transmission	Store and Forward	Wallet based – credentials held in wallet.
Standards	Data: mdoc, sd-jwt Interface: OIDF, ISO 18013-5 Security: EUCC, Fitcem, ETSI	Leveraging multiple protocols to address different use cases – online issuance, online presentation, proximity presentation. Profiles used to restrict the use of standards. Security (and certification) requirements focused on wallet components – WSCD, WSCA, Wallet Instance. For RPs and Issuers, security requirements are aligned with NIS2 Directive. Requirements on “qualified” issuers are more stringent.
Transaction types	All	Credential presentation, authentication, digital signing
Type of Security	Hardware	Focus on strong protection of cryptographic keys especially for the wallet and “qualified” issuers.

consult hyperion

Technical Focus – mapping the India System

Category	Approach	Notes
Architecture	Centralised	National infrastructure. Verifiable Credentials increase portability for Aadhaar ID. DigiLocker PDFs also highly portable but solving slightly different problem to credentials.
Data Security	Combination of signed and unsigned data.	DigiLocker documents are signed by issuer. VCs issued by DigiLocker itself. In Aadhaar and DigiLocker (PDFs), presentation relies on user authentication, rather than the cryptographic holder binding used in verifiable credentials.
Data Transmission	End-to-end	Aadhaar authentication is end-to-end going back to central infrastructure DigiLocker PDFs are in effect end-to-end (for "issued" documents). Storage location (repository) is choice of issuer and can be viewed as issuer infrastructure. Verifiable credentials move towards a store-and-forward model.
Standards	Data: XML based, VCs Interface: Proprietary APIs Security: Session based	Aadhaar and DigiLocker are essentially proprietary systems – although operating on a huge scale. VCs do align with international standards.
Transaction Types	Identification and authentication Credential presentation eSign services support signing	Aadhaar supports identification and authentication DigiLocker PDFs provide digital versions of paper documents VCs enable credential presentation with selective disclosure.
Type of Security	Assume signing keys protected by HSMs. Biometric authentication.	Strong emphasis on biometric authentication. Unclear how private keys in DigiLocker and Aadhaar App protected.

consult hyperion

Regulatory Focus – mapping the EU system

Category	Approach	Notes
Legal Construct	Framework	Legal framework that establishes roles, obligations, and requirements for identity schemes, wallets, and trust services without prescribing a single implementation, but requires certain technologies, protocols and standards to be used to ensure interoperability and secure interactions.
Identity Assurance	Defined Levels of Assurance	Clearly defines and standardises assurance levels that participants can/must use to create tiered categories for trust in identity information and credentials.
Trust	Mutual Recognition	Trust between different actors is accomplished through a framework that enables mutual recognition (legally and technically) across actors and jurisdictions.
Trust	Participation governed by independent certifications	Different elements undergo independent assessments and certification, which prove to the different actors that a device, process or organization is compliant with the governing framework and can therefore participate.
Governance	Scheme-of-Schemes	Member States operate individual identity schemes and wallet implementations, each governed nationally but aligned to EU-level rules.

consult hyperion

Regulatory Focus – mapping the EU system

Category	Approach	Notes
Ownership	Mixed Public Utility / Non-Profit Consortium / Commercial	National ID schemes, EUDI wallets and foundational registries are typically owned and operated by public authorities, functioning in practice as public utilities. Wallet providers, credential issuers, and trust service providers may be commercial or non-profit , provided they follow regulatory requirements.
Membership	Open Membership	Follows an open membership model, subject to qualification requirements.
Consumer Protection	Recovery Processes Exist	Providers implement technical solutions for users to restore wallet units from backups, and ecosystem participants must provide recovery and data correction pathways.
Consumer Protection	Civil Actions are Permitted	Users can bring actions in civil courts based on established liability regime.
Consumer Protection	Inclusion and Accessibility are prioritized	eIDAS requires adherence to established EU law on inclusion and accessibility for user-facing system components.

consult hyperion

Regulatory Focus – mapping the EU system

Category	Approach	Notes
Privacy	Consent is mainly a functional concept	Consent manifests in the EUDI ecosystem as a functional step at different times within various actions and contexts.
Privacy	Unlinkability is required	The EUDI ecosystem facilitates unlinkability in certain transactions.
Privacy	Biometrics are stored in a decentralized manner	Biometric data is typically stored and processed locally on the user's hardware.
Privacy	Selective Disclosure is available	Users can selectively disclose identity attributes.
Mark	Trust Mark	The EU digital identity ecosystem supports the use of trust marks. Trust is communicated through framework-level indicators linked to compliance with EU requirements. Trust marks are used to signal that wallets, credential issuers, or trust services meet defined regulatory and assurance standards. Recognition is intended to be consistent across Member States, supporting cross-border reliance.

Regulatory Focus – mapping the India system

Category	Approach	Notes
Legal Construct	System	Aadhaar and DigiLocker are founded on a system-based legal construct, governed by specific Indian legislation to provide a national identity infrastructure for India.
Identity Assurance	Relies on authoritative sources	The Aadhaar ecosystem does not define or communicate standardised assurance levels. Confidence in identity is inferred from the strength of the authentication method and the institutional controls governing the system.
Trust	Unitary Statutory Authority	A single authority (UIDAI) sets rules and expectations for the ecosystem that all parties must abide by. Trust is effectively mooted as all participants are required to accept the processes and data of one another.
Trust	Participation governed by bilateral agreements	Aadhaar actors enter into Agreements or Memoranda of Understanding with one another to enable participation in the ecosystem.
Governance	Scheme and Service	Aadhaar operates as a single national scheme, governed through statute, regulations, and administrative rules. Participation by service providers and relying parties is governed through registration, certification, and contractual arrangements. Supporting services (e.g. DigiLocker) operate as within the broader scheme, governed under aligned but distinct operational rules.

consult hyperion

Regulatory Focus – mapping the India system

Category	Approach	Notes
Ownership	Public Utility	Central government ownership and operation of Aadhaar and Digilocker, functioning as a regulated monopoly.
Membership	Closed Membership	Membership is explicitly controlled, with defined categories of participants and limited entry points.
Consumer Protection	Recovery Processes Exist	Key ecosystem participants provide recovery and data correction pathways, mainly via contact centers and forms.
Consumer Protection	Civil Actions are Not Permitted	Users cannot bring actions in civil courts. No liability regime exists.
Consumer Protection	Inclusion and Accessibility are Not Prioritized	With the exception of requiring alternative means of authentication Aadhaar and related services do not require inclusion and/or accessibility features.

consult hyperion

Regulatory Focus – mapping the India system

Category	Approach	Notes
Privacy	Consent is mainly a legal concept	Consent manifests in Aadhaar as a statutory requirement and user consent is incorporated procedurally in certain transaction flows.
Privacy	Unlinkability is required	The Aadhaar ecosystem facilitates unlinkability via temporary virtual ID numbers that alias the Aadhaar number.
Privacy	Biometrics are stored centrally	Scans of fingerprints, irises, and facial images are stored centrally in the CIDR.
Privacy	Selective Disclosure is not available	UIDAI requires some data minimization, but user-driven selective disclosure is not available.
Mark	Acceptance Mark	India's digital identity ecosystem primarily relies on acceptance marks. Trust is conveyed through service-level branding and recognition, rather than a formal trust framework mark. Acceptance is implied through association with government-operated or government-recognised services.

consult hyperion

Commercial Focus – mapping the EU system

Category	Approach	Notes
Model	Publicly funded core Free to individuals Commercial value-added services	Basic services (focus of short-term roadmap) can be assumed to be provided as public utilities.
Fees	Fees determined at national level. Fees for RPs Fees for QTSP services	Defining fees at member state level will add complexity to the EU system and could result in interoperability issues with the EU.
Liability Models	Liability for QTSP established under eIDAS 1.0 (e.g. negligence) For EUDIW member states are required to publish liability regimes.	Defining liability regime at member state level could result in interoperability issues with the EU.

consult hyperion

Commercial Focus – mapping the India System

Category	Approach	Notes
Model	Publicly funded systems Free to individuals Aadhaar fees for participants (e.g. relying parties)	Both Aadhaar and DigiLocker are provided as public utilities. Some premium services (DigiLocker)
Fees	Licence and transaction fees for Aadhaar participants.	TBC
Liability Models	Criminal penalties for unauthorised access and breaching data sharing prohibitions. Civil penalties for failing to comply with Aadhaar Act. For DigiLocker, documents are treated as equivalent to paper with similar liabilities	Very strong rules around Aadhaar. Civil penalties make it easier for UIDAI to fine companies without requiring full criminal trial. DigiLocker liabilities similar to paper documents: • Documents are by definition legally valid (cannot be denied) • User can be liable under Indian Penal Code for uploading forgeries • Accuracy of documents sits with issuer, as with paper documents • DigiLocker (the government) could be liable in event of a data breach.

consult hyperion

Thank you

Digital Identity @ Fime

We are your trusted partner enabling you to realise the opportunities and benefits of digital identity.

- We are **independent** and able to provide impartial advice and support.
- We have **global** coverage of digital identity initiatives including eIDAS, mDL / mDoc, Bank ID, eKYC and Biometrics.
- As global leaders in digital payments, we are uniquely positioned to provide support on the **intersection** of payments and identity.
- We are actively involved in the development of the **technical standards** and **governance frameworks** underpinning digital identity.
- We are experts in key identity technologies such as **mobile wallets**, **cryptography, digital credentials** and **biometrics**.

Consulting

- Strategy, Go to market
- Scheme governance
- Specifications and standards
- Vendor selection
- Technical architecture
- Implementation and QA support

Services

- Testing and certification
- mDL / mDL compliance testing
- Biometric testing (FIDO, NIST, MOSIP)
- docAuth testing (FIDO)

Platforms

- Digital Identity Test Suite – QA and conformance test platform
- ISO 18013-5
- ISO 18013-7

consult hyperion

Discover more about how Consult Hyperion can help your business.

Email
gilad.rosner@chyp.com

Address
Fime Headquarters
118, rue de Rivoli
75001 Paris – France

Making innovation possible.
Making the world work.

Consulting | Test Platforms | Testing Services