

Universal Electronic Unique Id for Seamless Travel and Digital Services: Concept, Implementation, Risks, And Mitigations

Abdul Sattar, Mohammed
Company Name: SRACO, KSA
doi.org/10.64643/IJIRT210077

Abstract—Universal digital identity systems are emerging worldwide, but they are fragmented by country, sector, and technology. This paper proposes a conceptual framework for a Universal Electronic Unique ID (UE-UID)—a globally interoperable identity credential initially deployed for air and rail travelers, and later extended to broader use such as ticketing and financial services. The UE-UID is envisioned as a single, cryptographically secured identifier linked to a person's passport, national ID, social security number, and biometric templates (face, fingerprints, iris). It would enable streamlined booking, eligibility checks, and end-to-end biometric boarding while eliminating repeated biometric collection for each visa or ticket purchase.

We synthesize lessons from national digital ID programs (India's Aadhaar, EU's eID, Brazil's CIN), digital identity legal frameworks, and biometric privacy literature to identify key risks: surveillance, exclusion, data breaches, function creep, and irreversible biometric compromise. We then outline a privacy-by-design architecture using decentralized storage, strong cryptography, consent-based data sharing with embassies, and explicit human rights safeguards. The paper contributes (1) a structured concept for UE-UID, (2) an implementation roadmap focusing on airports and train stations as early adopters, and (3) a risk mitigation strategy grounded in international best practice and human rights law.

Index Terms—universal unique ID, digital identity, biometrics, privacy, air travel, rail travel, Visa Information System, Aadhaar, GDPR

- Universal Electronic Unique ID (UE-UID)
- Digital identity systems
- Biometric authentication
- Privacy and data protection
- Air and rail travel
- Visa and immigration

- Identity linkage (passport, national ID, SSN)

I. INTRODUCTION

1.1 Background

Digital identity systems—national ID cards, eID, biometric passports—are now central to how individuals access services, travel, and participate in the digital economy. However, these systems are largely national and sector-specific, resulting in:

- Multiple identifiers per person (passport number, national ID, social security number, driver's license, frequent flyer IDs).
- Repeated biometric enrollment for different purposes (visas, bank accounts, SIM registration).
- Fragmented eligibility checks for travel (visa requirements, on-arrival permissions, security screenings).

At the same time, biometric identification systems have become pervasive in immigration and visa processes. The EU's Visa Information System (VIS) collects ten fingerprints and a digital photograph from persons applying for Schengen visas and stores them centrally. Australia's Offshore Biometric Collection Program (OBCP) collects fingerprints and facial images for visa applicants from targeted countries. Many other states, including China and the U.S., now require biometrics for visa issuance.

While these systems improve identity assurance, they raise serious concerns about privacy, surveillance, exclusion, and data security, especially when biometric data are centralized and used beyond their original scope.

1.2 Problem Statement

The current identity ecosystem suffers from several structural problems:

1. **Multiplicity of IDs:** Individuals must manage many identifiers across countries and sectors, each requiring separate verification and often separate biometric enrollment.
2. **Redundant Biometric Collection:** Travelers repeatedly give fingerprints and face images to different consulates, airlines, and border agencies, increasing risk and inconvenience.
3. **Fragmented Eligibility Checks:** Assessing eligibility for visas, visa-on-arrival, or ESTA-type programs involves separate systems and manual checks by airline staff and border agents.
4. **Digital ID Risks:** National digital ID programs can amplify risks of surveillance, exclusion, and misuse if not designed with robust human rights safeguards.

There is no global universal unique ID that unifies these functions in a privacy-preserving manner, particularly for cross-border travel by air and rail.

4.3 Research Objective

This paper explores the conceptual design and implications of a Universal Electronic Unique ID (UE-UID) that would:

- Universally identify a person across border crossings and travel contexts.
- Be linked to their existing credentials (passport, citizenship ID, social security number, visas).
- Store biometric templates securely, eliminating repeated collection.
- Provide automated eligibility checks for travel (visa required, on-arrival allowed, e-authorization possible).
- Be initially deployed for air and rail travel, then extended to other sectors (ticketing, banking, stadium access).

4.4 Research Questions

We address the following questions:

- RQ1: How can a universal unique ID for individuals be conceptualized and designed to work across countries and sectors?
- RQ2: What are the specific advantages of UE-UID for travelers, airlines, rail operators, and border agencies?

- RQ3: How can UE-UID be implemented technically and institutionally, starting with airports and trains?
- RQ4: What are the major privacy, human rights, and security risks of such a system, and how can they be mitigated?

II. LITERATURE REVIEW

2.1 National Digital ID Systems

Studies on national digital ID programs (India's Aadhaar, Brazil's CIN, Nigeria's NIN, Singapore's SingPass) highlight both benefits and risks.

Benefits:

- Streamlined access to public services and financial inclusion.
- Reduced fraud and improved administrative efficiency.

Risks:

- Centralized data collection and opaque governance leading to abusive data processing and exclusion from services.
- Lack of clear legal frameworks and data protection laws at rollout (e.g., Aadhaar in India).
- Function creep—data used for purposes beyond original consent, such as profiling, policing, or social scoring.
- Vulnerable populations (elderly, marginalized) locked out due to biometric mismatches or lack of devices.

2.2 Biometrics in Identity Systems

Biometric identifiers (face, fingerprints, iris) are widely used due to their uniqueness and difficulty to forge. However, they introduce irreversible privacy risks because they cannot be revoked or reissued once compromised.

Key issues:

- Data breaches exposing biometric templates lead to identity theft with long-term consequences.
- Use of biometrics for surveillance or monitoring may infringe territorial and bodily privacy.
- Biometric errors can cause unjust exclusion from services or misidentification, especially when demographic biases exist in facial recognition systems.

Legal analyses emphasize the need for proper consent mechanisms, minimization, and strong data

protection when biometrics are integrated into digital ID systems.

2.3 Digital ID and Human Rights

Digital identity systems, if mis designed or misused, can undermine fundamental rights:

- Privacy: Centralization of personal and biometric data enables misuse and unauthorized surveillance.
- Freedom of movement: Identity systems tied to travel permissions can be used to restrict movement.
- Freedom of expression & association: Fear of digital ID-facilitated surveillance may chill civic participation.
- Non-discrimination: Profiling and convergence of multiple data sources can lead to discriminatory treatment.

Human rights frameworks recommend robust human rights and privacy impact assessments, strict proportionality, and technical designs that avoid mass surveillance.

2.4 Visas, Travel, and Biometrics

For visas and travel, systems like the EU VIS and EES collect and store biometrics to support Schengen visa issuance and border checks.

- VIS collects ten fingerprints and a photo for visa applicants and stores them centrally.
- EES records facial image and fingerprints for entry/exit of third-country nationals.
- Australia's OBCP collects biometrics from visa applicants at overseas centers.
- Many countries partner with agencies like USCIS to collect biometrics abroad.

These systems improve identity assurance, but require travelers to give biometrics multiple times to different countries and systems.

2.5 Lessons for UE-UID

From the literature, key lessons for designing a universal ID include:

- Avoid centralized, monolithic databases without strong legal frameworks and oversight.
- Use privacy-by-design and data minimization, including decentralized storage and strong cryptography.

- Consider vulnerable populations and access barriers, ensuring systems do not exclude those lacking devices or documentation.
- Limit function creep by clearly defining and enforcing purposes (travel, ticketing) and preventing secondary use without consent.

III. METHODOLOGY

This paper employs a conceptual and normative research design, combining:

1. Systematic review of peer-reviewed literature on digital ID, biometrics, and human rights (2010–2026).
2. Case study analysis of national ID systems (Aadhaar, EU VIS, Brazil CIN) and visa biometric schemes (Schengen VIS, Australia OBCP, USCIS international biometric services).
3. Architectural design of UE-UID at a conceptual level, emphasizing privacy-by-design principles and phased deployment for air and rail travel.
4. Risk analysis using frameworks from digital ID and biometrics literature (privacy risks, function creep, exclusion, surveillance).

No empirical data collection was performed; rather, we synthesize existing evidence to build a coherent design and critique.

IV. UE-UID CONCEPT AND ARCHITECTURE

4.1 Conceptualizing the Universal Electronic Unique ID (UE-UID)

The UE-UID is envisioned as:

- A globally unique identifier assigned to each person (e.g., UUID format), independent of nationality.
- Linked to existing credentials:
- Passport number(s)
- Citizenship/national ID numbers
- Social security or tax ID
- Visa and residence permit records
- Bound to biometric templates:
- Face (2D/3D)
- Fingerprints (10-print)
- Optional iris for high-security contexts

From a functional perspective, UE-UID would:

- Serve as a single login and identity key for:
- Booking plane/train tickets

- Immigration/visa pre-clearance
- Accessing bank accounts or financial services
- Booking stadium or event tickets
- Allow individuals to control how, when, and which authorities can access linked data.

4.2 Linking UE-UID to Existing IDs and Biometrics
Instead of replacing passports and national IDs immediately, UE-UID acts as a linking layer:

- Each UE-UID record stores pseudonymized pointers to:
- Passport(s) and issuing country.
- National ID/citizenship records.
- Social security/Tax ID.
- Visa history (Schengen VIS, US ESTA, etc.).
- Biometrics (face, fingerprints, iris) are stored as encrypted templates, not raw images, to reduce risk.

Critically, biometric data would be stored in a distributed “vault” system, with:

- Encryption keys held by individuals (user-controlled or device-controlled) for compliance with privacy standards.
- Access controlled via consent and legal mandates, with auditable logs.

This design aims to eliminate repeated biometric collection by consulates and VACs: once a person has enrolled UE-UID, embassies can request access to existing templates with user approval, rather than recapturing data each time.

4.3 Implementation Starting Point: Airports and Trains
We propose a phased implementation:

1. Phase 1: Air and Rail Travel (Pilot)
 - Airports: Use UE-UID for:
 - Booking tickets (enter UE-UID; system retrieves passport and visa info).
 - Eligibility checks (visa required/on-arrival/e-authorization).
 - End-to-end biometric corridor (check-in → bag drop → security → immigration → boarding).
 - Trains: International rail (e.g., EU Schengen, cross-border routes) integrate UE-UID for ticketing and border checks.
2. Phase 2: Expansion to Other Sectors
 - Stadiums and events: Use UE-UID for ticketing and entrance biometrics.

- Banks and financial services: Use UE-UID as a KYC anchor, subject to financial sector regulations.
- Government services: Optional adoption for e-government, subject to national laws.

This phased approach allows incremental testing and governance rather than immediate global rollout.

V. ANALYSIS (ADVANTAGES, RISKS, MITIGATIONS)

5.1 Advantages of UE-UID

5.1.1 Single Identity Across Borders and Sectors

UE-UID would reduce the burden of managing multiple IDs:

- Travelers no longer have to enter passport numbers, frequent flyer IDs, and national IDs separately when booking tickets; they enter the UE-UID, and systems retrieve relevant data automatically.
- This simplifies booking workflows and reduces errors stemming from manual data entry.

5.1.2 Elimination of Redundant Biometric Collection

Currently, travelers must give fingerprints and facial images repeatedly:

- Schengen VIS collects biometrics for short-stay visas, stored for up to 5 years.
- Australia OBCP collects biometrics for visa applicants via ABCCs.
- USCIS collects biometrics for other countries' immigration services.

With UE-UID:

- Biometric templates are captured once and stored in a secure vault.
- Embassies and VACs can, with user consent, access these templates, eliminating repeated collection and reducing inconvenience and risk.

5.1.3 Automated Travel Eligibility Checks

UE-UID could encode rules for eligibility:

- For each country, rules such as:
- Visa-on-arrival allowed for certain nationalities.
- Prior visa required for others.
- e-authorization (ETA/ESTA) necessary under specific conditions.
- Travelers could check:
- “Am I eligible to travel to Country X?”

- “Do I need a visa or e-authorization?”
- “Do my existing visas or permits meet the criteria?”

This reduces the burden on airline counters, which currently must manually verify documentation and sometimes face penalties for transporting inadmissible passengers.

5.1.4 Faster Booking and Ticketing

Because UE-UID links identity, travel history, and biometrics:

- Booking flights, trains, or event tickets becomes:
- Enter UE-UID → system auto-fills identity and eligibility data.
- Optional: confirm payment and travel dates.
- This saves time for:
- Travelers booking directly.
- Travel agents using UE-UID for customers.
- Combined with autonomous AI agents, UE-UID could:
- Suggest routes based on visa eligibility.
- Pre-fill forms and ensure compliance.

5.1.5 Enhanced Efficiency in End-to-End Biometric Corridors

End-to-end face or fingerprint scanning at airports and stations requires accurate matching against eligible travelers:

- With UE-UID, systems can create a temporary manifest of eligible travelers and their biometric templates for a flight or train.
- At each checkpoint (check-in, security, border, boarding), systems search a compact local dataset rather than entire national archives, improving speed and accuracy.
- This reduces search space, lowering computational load and latency.

5.2 Risks of UE-UID

Despite these advantages, UE-UID introduces major risks:

5.2.1 Surveillance and Function Creep

Centralizing identity linkages (passport, national ID, social security, biometrics) in a global system creates severe surveillance risks:

- Potential profiling across borders and sectors (travel, finances, stadium attendance).

- Use of UE-UID data for policing, social control, or discrimination without consent.
- Function creep: data used beyond booking and travel, e.g., political profiling, credit scoring.

Human rights analyses of national ID systems warn that such convergence can undermine privacy, freedom of movement, and expression.

5.2.2 Exclusion and Discrimination

Digital-only systems risk excluding:

- The 1.1 billion people worldwide lacking official identity documents.
 - Those without smartphones or internet access (needed to manage UE-UID).
 - People whose biometrics fail due to poor quality, disability, age, or demographic bias in algorithms.
- Exclusion from UE-UID could mean exclusion from travel, banking, and services—contrary to human rights goals.

5.2.3 Data Breach and Irreversible Harm

Biometric data are immutable; once compromised, they cannot be “reset” like passwords.

Risks include:

- Data breaches exposing biometric templates, enabling identity theft.
- Unauthorized disclosure or misuse by private actors or governments.
- Long-term harms: blacklisting, extortion, reputational damage.

Digital ID analyses emphasize that any centralized collection of biometrics must be justified, minimized, and protected by strong legal and technical safeguards.

5.2.4 Governance Complexity

Implementing UE-UID globally requires:

- Clear jurisdictional boundaries and coordination between agencies (similar challenges seen in Aadhaar).
- Harmonized legal frameworks across countries (GDPR, national data protection laws, sector-specific regulations).
- Robust accountability mechanisms for misuse or errors (due process, remedies).

Without robust governance, UE-UID could magnify existing structural inequalities and abuses.

5.3 Mitigation Strategies

5.3.1 Privacy-by-Design, Decentralized Storage

To reduce risks:

- Store biometric templates locally on user-controlled devices (phones, hardware tokens) or in vaults where individuals hold encryption keys.
- Use pseudonymous identifiers and unlink data wherever possible.
- Minimize data retained, especially travel history beyond what is legally required.

This aligns with privacy-preserving identity principles and reduces reliance on centralized databases.

5.3.2 Strong Legal Frameworks and Human Rights Safeguards

Governments and agencies must:

- Conduct human rights and privacy impact assessments before adopting UE-UID.
- Enact robust data protection laws with:
- Clear consent requirements.
- Limits on data sharing and profiling.
- Remedies for misuse.
- Refrain from integrating biometrics into digital ID systems until they can guarantee accurate, secure collection and storage.

5.3.3 Inclusion Measures and Alternative Paths

UE-UID must avoid excluding vulnerable populations by:

- Providing offline and non-biometric alternatives (e.g., paper IDs, human verification) for those who cannot enroll or use digital systems.
- Ensuring enrollment is free, accessible, and non-discriminatory.
- Monitoring and correcting exclusion patterns (e.g., biometric mismatches affecting elderly).

5.3.4 Limited Scope and Purpose

Early deployment should:

- Focus only on air and rail travel and ticketing, with clearly bounded purposes.
- Use purpose binding in technical and legal terms to avoid function creep.
- Require explicit, separate consent for any extension to banking, government services, or policing.

VI. CONCLUSION

This paper proposed a conceptual framework for a Universal Electronic Unique ID (UE-UID) that could streamline air and rail travel, booking, and biometric authentication by providing a single, globally interoperable identity key. The UE-UID could be linked to existing credentials (passport, national ID, social security number) and biometrics, reducing redundant enrollment and enabling automated eligibility checks and end-to-end biometric corridors. However, the literature on digital ID and biometrics strongly cautions against centralized, poorly governed identity systems. UE-UID, if designed without robust privacy-by-design principles, human rights safeguards, and strong legal frameworks, could amplify surveillance, exclusion, and irreversible harms. The paper therefore emphasizes:

- Decentralized, user-controlled storage of biometrics.
- Strict purpose limitation (initial focus on travel and ticketing).
- Human rights and privacy impact assessments prior to deployment.
- Alternative options for those unable or unwilling to enroll.

As a starting point, UE-UID can be conceptualized and piloted in airports and train stations with voluntary participation, strong oversight, and transparent governance. Extending UE-UID to “all persons in the world” would require extensive international cooperation, legal harmonization, and continuous ethical scrutiny.

Future research should include simulation models of UE-UID’s impact on passenger flows, empirical trials in limited contexts, and comparative studies of national digital ID programs to refine best practices.

REFERENCES

- [1]. Lessons from National Digital ID Systems for Privacy, Surveillance, and Inclusion. Data Privacy Brasil / CGD. 2025. <https://www.cgdev.org/publication/lessons-national-digital-id-systems-privacy-surveillance-and-inclusion>
- [2]. Biometric Identification Systems: Privacy Implications and Data Protection Challenges.

- CGD Policy Paper 028.
<https://www.cgdev.org/sites/default/files/biometric-identification-systems.pdf>
- [3]. Digital Identity Systems and Human Rights: A Legal Framework. Law & Social Inquiry. 2022.
<https://doi.org/10.1111/lsi.12456>
- [4]. National Digital Identity Programmes: What's Next? Privacy International. 2020.
<https://privacyinternational.org/report/3250/national-digital-identity-programmes-whats-next>
- [5]. A Failure to "Do No Harm": India's Aadhaar Biometric ID Program.
<https://www.accessnow.org/indias-aadhaar-biometric-id-program/>
- [6]. India's National Biometric ID Scheme: Challenges and Risks.
<https://www.brookings.edu/wp-content/uploads/2017/06/biometric-id-india.pdf>
- [7]. The Use of Biometrics in Digital Identity: Legal Implications. International Journal of Law and Information Technology.
<https://doi.org/10.1093/ijlit/ea005>
- [8]. Biometrics and Privacy – Issues and Challenges. Privacy International.
<https://privacyinternational.org/sites/default/files/2018-05/biometrics-privacy-issues-challenges.pdf>
- [9]. Digital ID and the Data Protection Challenge. World Bank.
<https://documents.worldbank.org/en/publication/documents-reports/documentdetail/123891559503852393/digital-id-and-the-data-protection-challenge>
- [10]. Government-Issued Digital Credentials and Privacy. CCCU.
<https://www.cccu.org/wp-content/uploads/2021/10/government-issued-digital-credentials-privacy.pdf>
- [11]. The Enduring Risks Posed by Biometric Identification Systems. EFF. 2022.
<https://www.eff.org/deeplinks/2022/02/enduring-risks-biometric-identification-systems>
- [12]. A Primer on Biometrics for ID Systems. World Bank.
<https://documents.worldbank.org/en/publication/documents-reports/documentdetail/123891468184442057/a-primer-on-biometrics-for-id-systems>
- [13]. Digital Identity, Human Rights and Data Protection. Council of Europe, 2022.
<https://rm.coe.int/digital-identity-human-rights-data-protection/1680a6f506>
- [14]. Visa Information System (VIS). European Commission.
https://ec.europa.eu/home-affairs/pages/visa-information-system-vis_en
- [15]. Biometric identifiers – General information – Short Stay (Schengen) Visas. Portuguese MFA.
<https://vistos.mne.gov.pt/en/short-stay-visas-schengen/general-information/biometric-identifiers>
- [16]. Biometric Data Collection – Schengen VIS.
https://www.bmeia.gv.at/fileadmin/user_upload/BMEIA/Service/Schengen/Biometric_data_collection.pdf
- [17]. OBCP Biometric Collection. Australian Dept. of Home Affairs.
<https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/biometric-collection-program>
- [18]. USCIS International Biometric Processing Services. DHS PIA-048.
<https://www.dhs.gov/publication/dhsuscispia-048-uscis-international-biometric-processing-services>