INDEPENDENT WORKING PAPER · DIGITAL IDENTITY & PLATFORM GOVERNANCE

When a National ID Is Not Enough

Document admissibility, recovery design, and LinkedIn identity verification barriers for Pakistani users

Muhammad Usman

BS Artificial Intelligence · Superior University Lahore

Abstract

This paper examines why a Pakistani user may be unable to verify or recover a LinkedIn account even while holding a valid national identity document. A desk review of LinkedIn and Persona guidance, Pakistan's identity infrastructure, and international identity-proofing principles shows that the central problem is not accurately described as a blanket refusal to verify Pakistanis. It is a layered *document-admissibility gap*: LinkedIn's optional profile-badge flow relies on a country-supported, near-field communication (NFC) credential and an NFC-capable phone, while the restricted-account recovery flow uses country-dependent document rules and offers a notarized fallback only in specified regions. A Computerized National Identity Card (CNIC) may be legally authoritative in Pakistan yet still be outside a particular private verification workflow. The paper proposes transparent country-by-document matrices, CNIC-compatible validation, non-NFC recovery routes, human review, specific error codes, and public parity testing.

Pakistan · LinkedIn · Digital identity · Platform access · Account recovery

1. A valid identity can still be inadmissible

> The core failure is not always “identity unknown.” It can be “evidence not accepted by this workflow.” That distinction matters because the remedy is different.

Pakistan operates a mature national identity infrastructure through the National Database and Registration Authority (NADRA). Government sources describe national identity cards, biometric systems, the Pak ID app, and e-passport services as parts of the country’s digital public infrastructure.[10–12] Yet a private platform can impose a narrower evidence boundary than the state. LinkedIn’s help material says accepted identity documents vary by country, and its optional Persona badge flow requires a valid NFC-compatible passport or ID plus a mobile device with an NFC reader.[2–5]

Central argument. The Pakistan problem is best understood as an interaction among document format, country configuration, device capability, and recovery governance. It is not enough to ask whether a user has a government ID; one must ask whether the precise verification flow can ingest, authenticate, and escalate that credential.

Research questions

1. How do LinkedIn’s optional profile verification and mandatory account-recovery verification differ?
2. Which points in those workflows can exclude a legitimate Pakistani user?
3. Why is a CNIC’s domestic legal authority not automatically equivalent to platform admissibility?
4. What design changes could preserve fraud resistance while reducing false rejection and recovery dead ends?

Why the distinction is consequential

OPTIONAL TRUST SIGNAL

Profile badge

Failure means the member does not receive an identity badge. LinkedIn states that profile verifications are optional and free; workplace or educational verification may provide other trust signals where supported.[1,6]

ACCESS CONTROL

Restricted-account recovery

Failure can prevent access to a professional profile, contacts, messages, and job-search history. In this setting, identity proofing is not cosmetic; it is the gate to restoration.[4]

Motivating observation

This study was prompted by an unsuccessful attempt by a Pakistani LinkedIn user to verify a restricted account with a Pakistani identity document. That experience is treated as a case motivation, not as statistical proof. The analysis therefore avoids claiming how many Pakistani users are affected or why LinkedIn made a particular design choice.

2. This paper audits the published rules, not the private system

> A careful reading of public documentation can reveal where a process is opaque, but it cannot measure rejection rates or infer discriminatory intent.

Method

The study uses qualitative document analysis. Sources were reviewed as available on 14 October 2026 and grouped into four sets: (1) LinkedIn guidance for profile verifications; (2) LinkedIn guidance for recovering restricted accounts; (3) Persona guidance for end users; and (4) public sources on inclusive identity design and Pakistan's identity infrastructure. Claims were compared across documents to identify differences in scope, required evidence, supported devices, privacy statements, and fallback routes.

Evidence set	What it establishes	What it cannot establish
LinkedIn Help	Published rules, stated data sharing, documented steps and alternatives	Backend configuration, rejection rates, support-agent practice
Persona user guidance	General scan constraints and the customer's role in configuring a flow	LinkedIn's unpublished country-document matrix
Pakistan public sources	Existence of national identity, biometric, digital ID and e-passport infrastructure	Automatic interoperability with a private US platform
NIST and World Bank	Risk-based proofing concepts and inclusion principles	A binding rule for LinkedIn's global product

Three concepts organize the analysis

Legal validity

A state recognizes a credential as evidence of identity or citizenship. This is a legal and institutional property.

Technical readability

A workflow can capture and authenticate the credential using its available camera, NFC, barcode, database, or manual-review methods.

Platform admissibility

The service has configured that country and document type as acceptable for the particular purpose.

> **Analytical rule:** legal validity does not guarantee technical readability, and technical readability does not guarantee platform admissibility.

Limitations

- No access was available to LinkedIn's private decision rules, Persona's customer configuration, or support case data.
- No representative survey of Pakistani users was conducted.
- LinkedIn can change country coverage, accepted documents, retention periods, and recovery paths without notice; readers should check the live help pages.
- This is an independent systems and policy analysis, not legal advice and not an allegation of intentional discrimination.

3. “LinkedIn verification” is actually two different systems

Much confusion comes from treating the profile badge and account recovery as one process. LinkedIn itself warns that its Persona troubleshooting page for adding a badge does not apply to recovering a locked or compromised account.[3]

FLOW A · MEMBER STILL HAS ACCESS

Optional identity badge

Supported profile location and eligible issuing country › **NFC-compatible document** photo + chip scan › **Selfie and consent** verification shown on profile

LinkedIn’s Persona guidance describes an app-based sequence: photograph the credential, scan its NFC chip, take a selfie, and consent to sharing selected results. An NFC-capable mobile device is required.[2,3]

FLOW B · MEMBER CANNOT ACCESS THE ACCOUNT

Restricted-account recovery

Login challenge identity must be confirmed › **Country-dependent evidence** ID card, licence, passport or digital ID › **Persona result** LinkedIn decides restoration

The recovery page uses broader language—government ID card, driver’s licence, passport, or digital ID—but immediately qualifies that accepted documents vary by country.[4] The public troubleshooting page recognizes unsupported-country-ID errors.[5]

The two flows differ on consequence, evidence, and fallback

Dimension	Profile badge	Restricted-account recovery
Purpose	Add an optional trust signal	Prove ownership to regain access
Published evidence	Valid NFC-compatible passport or ID in supported countries	Government ID card, driver’s licence, passport, or digital ID; varies by country
Device	Mobile device with NFC reader	Mobile capture required; exact evidence route may vary
Documented alternative	Workplace/education checks may add other profile verifications where eligible	Notarized affidavit publicly offered only for Canada, the European Union, or the United Kingdom
Failure cost	No identity badge	Potential continued lockout

Critical implication: advice to “get an e-passport for the badge” does not, by itself, prove that every restricted-account recovery case will be resolved. The user must first identify which workflow is active.

4. Pakistan has strong identity infrastructure, but interoperability is not automatic

> Pakistan’s identity ecosystem and LinkedIn’s verification stack solve related problems through different institutions, standards, and risk decisions.

Pakistan’s public identity infrastructure is centered on NADRA. Government reporting describes national identity cards, overseas cards, biometric enrollment and authentication, digital ID services, and e-passports as parts of a wider digital public infrastructure.[10–12] NADRA’s privacy notice states that its mobile application may collect facial images and, in supported scenarios, fingerprints for matching against its national database.[9]

The interoperability gap

DOMESTIC AUTHORITY

CNIC / NADRA ecosystem

- Credential is issued under Pakistani law.
- Identity records and biometrics are maintained by a national authority.
- The credential supports domestic public and private services.

PRIVATE PLATFORM

LinkedIn / Persona workflow

- LinkedIn chooses the proofing purpose and customer configuration.
- Persona processes the document and selfie in the defined flow.
- Country, document, device, and chip support determine technical acceptance.

Government-recognized identity
Legitimate within Pakistan

≠

Guaranteed platform acceptance
Requires an implemented verification route

Why an e-passport can work where a CNIC does not

An e-passport provides a standardized, chip-based travel credential designed for machine verification across borders. LinkedIn’s badge guidance explicitly centers an NFC-compatible passport or ID and a phone capable of reading the chip.[2,3] A CNIC may contain secure features and remain the primary domestic identity credential, but that does not demonstrate that LinkedIn’s configured Persona workflow accepts or can authenticate that exact card type.

> **Evidence boundary.** The public sources reviewed do not provide a definitive, current LinkedIn table naming every Pakistani document accepted for restricted-account recovery. Therefore, this paper does not claim that every CNIC submission is rejected. It finds instead that the published rules are insufficiently granular for a Pakistani user to predict acceptance before entering the process.

Availability is also device-dependent

Even a supported chip document is not sufficient without a compatible mobile device, functioning NFC reader, current app, usable camera, and successful selfie capture. The verification result can therefore depend on both identity evidence and access to specific consumer technology.[3,5]

5. The exclusion risk is produced by a chain of small gates

> A legitimate user can fail before the system ever reaches the substantive question: “Does this person own the account?”

Gate	Failure mode for a Pakistani user	Observable outcome
Country configuration	Issuing country or profile location is not enabled for that flow	Country unavailable or unsupported-country error
Document configuration	CNIC or older machine-readable passport is not among accepted types	Document type absent or rejected
Hardware	Phone lacks NFC, chip cannot be read, or camera capture fails	Scan cannot complete
Data alignment	Profile name differs from credential because of spelling, transliteration, initials, or naming order	Name mismatch or additional check
Biometric capture	Selfie quality, lighting, camera, or matching step fails	Verification remains incomplete
Consent	User does not approve the required sharing from Persona to LinkedIn	Result cannot be attached or used
Escalation	No locally documented non-biometric or human fallback is available	Repeated loop or unresolved lockout

Opacity compounds each technical failure

LinkedIn’s recovery documentation names broad categories of acceptable evidence but qualifies them by country. Its troubleshooting guidance recognizes unsupported-country documents yet does not expose a public, Pakistan-specific recovery matrix in the materials reviewed.[4,5] A user may therefore receive a failure without knowing whether the cause is the country, the document type, capture quality, NFC capability, name alignment, or risk review.

The fallback is geographically uneven

For account recovery, LinkedIn documents a notarized Affidavit of Identity alternative for users located in Canada, the European Union, or the United Kingdom.[4,5] Pakistan is not named in that published fallback. This does not prove that support has no discretion, but it does mean that an equivalent route is not clearly promised to Pakistani users in the reviewed guidance.

Finding 1. The most serious exclusion risk appears when a high-consequence recovery decision relies on a narrow automated evidence route without a clearly documented, geographically equitable appeal path.

Privacy and control are part of accessibility

LinkedIn states that Persona collects the evidence and shares selected results with LinkedIn after consent. For recovery, LinkedIn says it receives the result, identifying attributes, ID type and issuer, and a redacted copy showing the name and portrait, but not biometric data or document numbers; it says recovery data is generally deleted within 14 days after the issue is resolved.[4] A user who declines sharing cannot complete the process.

6. Security and inclusion are not opposites

> The design question is not whether LinkedIn should verify identity. It is whether equal assurance can be reached through more than one evidence path.

Risk-based identity proofing supports evidence diversity

The National Institute of Standards and Technology (NIST) separates identity resolution, evidence validation, and verification that the applicant is connected to the evidence. Its guidance supports multiple proofing techniques and emphasizes reducing false negatives while maintaining the required assurance level.[8] This framework suggests that an NFC passport is one strong route, not the only imaginable route.

1
Resolve
Identify a unique account claimant using minimum necessary attributes and account history.

2
Validate
Confirm that evidence is genuine, current, and issued by a credible authority.

3
Verify
Confirm that the applicant owns the evidence through possession, biometric comparison, or supervised review.

Inclusion principles identify the hidden costs

The World Bank's Identification for Development guidance calls for removing direct and indirect barriers, reducing disparities in technology access, and ensuring that people are not denied associated services because they lack connectivity, devices, or digital literacy.[7] Although those principles primarily address identification systems, they are useful for evaluating private-platform identity gates because the same frictions—cost, travel, hardware, literacy, and administrative burden—shape access.

A proportionality test for LinkedIn

Question	Profile badge	Account recovery
What harm is being prevented?	Impersonation and false credibility	Unauthorized takeover and policy evasion
What happens if the user cannot verify?	The badge is not added	The user may remain locked out
How broad should evidence be?	Narrow evidence may be tolerable if clearly optional	Multiple equivalent routes and review are more important
What process protection is needed?	Clear eligibility and privacy explanation	Reason code, appeal, human review, and time-bounded response

Finding 2. A control can be technically secure yet procedurally unfair if legitimate users cannot understand why they failed or reach an equivalent review channel.

Design principle: strengthen identity assurance by combining independent signals—credential authenticity, account history, known-device possession, verified email, selfie comparison, and human review—rather than making a single credential format the sole path.

7. Six findings explain the Pakistan verification gap

7.1 Pakistan is not accurately described as categorically “unverifiable”

Current public guidance and Pakistan-focused implementation material indicate a Persona route for eligible Pakistani users with an NFC-compatible e-passport or ID and suitable phone.[2,3,13] The stronger claim—that LinkedIn rejects all Pakistani accounts—is unsupported.

7.2 CNIC authority and platform acceptance are separate questions

NADRA’s national identity system can be authoritative domestically while a specific LinkedIn/Persona workflow remains unable or unwilling to accept that document format. The gap is one of implemented interoperability and admissibility, not necessarily document legitimacy.

7.3 Public documentation is broader than operational certainty

The recovery page broadly names ID cards, licences, passports, and digital IDs, but says acceptance varies by country. Without a public Pakistan-specific table, users cannot know in advance which credential is supported.[4,5]

7.4 Badge verification and access recovery must not be conflated

An e-passport solution for an optional badge does not automatically describe the recovery route for a restricted account. LinkedIn explicitly separates the relevant troubleshooting guidance.[3]

7.5 Hardware and cost can become hidden eligibility criteria

Requiring an NFC document and NFC-capable phone turns possession of specific technology into a condition of verification. For a voluntary badge this may be an inconvenience; for account recovery it can become an access barrier.

7.6 The weakest point is the absence of an equivalent published fallback

The reviewed recovery guidance documents a notarized alternative only for Canada, the European Union, and the United Kingdom. A Pakistani user whose document route fails is not shown an equivalent local pathway in the same guidance.[4,5]

What the evidence does not show

- It does not show the number or percentage of Pakistani users affected.
- It does not show that LinkedIn intentionally discriminates against Pakistani users.
- It does not show that every CNIC fails or that every e-passport succeeds.
- It does not show that workplace or education verification can restore a restricted account.

> **Research integrity note:** claims circulating online that “99% of Pakistanis lack e-passports” or that “thousands are permanently locked out” were not adopted because this review did not locate a reliable primary dataset supporting them.

8. A better system can preserve assurance without creating a dead end

Recommendation matrix

Priority	Action	Security benefit	Inclusion benefit
1	Publish a live country-by-document-by-purpose matrix	Reduces unsupported submissions and social-engineering confusion	Lets users know the exact evidence needed before they begin
2	Add a CNIC/Smart CNIC route through authoritative validation or trained manual review	Uses a state-issued, identity-bound credential	Recognizes the document most Pakistani adults actually use
3	Offer a non-NFC recovery path with layered evidence	Combines known device, verified email, historical account data, ID image, and selfie	Removes dependence on a chip passport and premium phone
4	Guarantee human review after bounded automated failures	Detects fraud patterns machines may miss	Provides due process for legitimate edge cases
5	Return specific, safe failure reasons	Preserves anti-fraud secrecy while reducing blind retries	Distinguishes country, document, NFC, image, name, and consent problems
6	Report completion and appeal outcomes by country and document type	Reveals abuse concentrations and control performance	Measures parity and identifies systematic false rejection

A tiered recovery architecture

Route A
NFC e-passport + selfie

or

Route B
CNIC + authoritative or manual validation + selfie

or

Route C
Layered account evidence + trained reviewer

Each route should meet the same risk target, but through different combinations of evidence. Route C should be reserved for recovery—not badge issuance—and should require multiple independent signals such as control of a long-standing email address, a recognized device, historic profile attributes, and support review.

Governance safeguards

- **Purpose separation:** do not silently reuse a badge-verification result for unrelated enforcement decisions.
- **Data minimization:** collect only what the selected route needs and publish retention rules for both LinkedIn and its vendor.
- **Contestability:** permit a user to challenge a result and submit corrected evidence.
- **Accessibility:** support low-bandwidth capture, clear instructions, and language-appropriate help.
- **Change transparency:** date-stamp the supported-document matrix and archive material changes.

Finding 3. The appropriate policy response is evidence diversity, not weaker verification. Equivalent assurance can be achieved without making one document format the only doorway.

9. A Pakistani user should diagnose the exact flow before retrying

> Repeatedly submitting the same document without identifying the failure stage can make the process more confusing and may not produce a different result.

Step 1 · Identify the purpose

Adding a badge?

You still control the account and want an optional verification on your profile. Use the profile-verification guidance and check NFC-document eligibility.

Recovering access?

The account is restricted or inaccessible. Use the recovery guidance. Do not assume badge instructions are the same.

Step 2 · Record the exact failure

- Country not listed or “unsupported country ID”
- Document type missing
- Camera or image-quality failure
- NFC chip not detected
- Name mismatch
- Selfie failure
- Consent or data-sharing not completed
- Submission accepted but no decision

Step 3 · Make one controlled retry

Use the current LinkedIn app, a supported mobile device, the original unexpired document, good lighting, all document edges visible, the correct issuing country, and a profile name that accurately corresponds to the credential. For an NFC route, confirm that both the credential and phone support NFC and remove a thick phone case if scanning fails.[3,5,14]

Step 4 · Escalate with a concise evidence trail

When the error persists, record the date, flow, country selected, document type, error wording, device model, app version, and whether NFC capture started. Do not include a full ID number in a public post. Ask support to identify whether the barrier is country support, document support, capture failure, name matching, or another review.

> **Safety note:** submit identity documents only through the official LinkedIn/Persona flow or an authenticated support case. Do not email a CNIC or passport to an address found in a social-media post, and do not pay anyone offering a “verified account.”

Step 5 · Use alternative profile trust signals only where they fit

LinkedIn may offer workplace email or educational verification for supported organizations. These can add profile credibility but should not be represented as a guaranteed substitute for restricted-account recovery.[1,6]

10. The remedy is a recoverable system, not a weaker one

> Identity verification becomes equitable when legitimate users can reach the required assurance through transparent, proportionate, and contestable routes.

This review finds that the difficulties reported by Pakistani users are better framed as a verification-architecture problem than as a simple nationality ban. LinkedIn's profile-badge flow is documented around NFC-compatible credentials and mobile hardware. Its account-recovery flow uses broader categories of government evidence, but accepted documents vary by country and the reviewed guidance does not expose a definitive Pakistan-specific matrix. A valid CNIC can therefore be authoritative in Pakistan yet remain inadmissible or unreadable within a particular private workflow.

The greatest concern arises when an automated evidence boundary controls recovery of a restricted professional account. In that setting, unclear errors and geographically limited fallbacks can transform a fraud-control measure into a procedural dead end. Security remains essential, but it should be pursued through equivalent assurance paths: NFC passport, CNIC-compatible validation, layered account evidence, and trained human review.

Research agenda

1. **Outcome audit.** Measure completion, false-rejection, escalation, and restoration rates for Pakistani users by document type and device class.
2. **Document test suite.** Evaluate Pakistani CNIC, Smart CNIC, NICOP, machine-readable passport, and e-passport samples under controlled, consented conditions.
3. **User study.** Interview students, job seekers, freelancers, recruiters, and diaspora users about the professional cost of failed recovery.
4. **Comparative policy study.** Compare LinkedIn's Pakistan route with platforms that accept Pakistani national identity documents through other vendors or manual review.
5. **Privacy review.** Map the data lifecycle across LinkedIn, Persona, subprocessors, and support channels for both successful and failed attempts.

Testable hypothesis for future work

H1: A multi-route recovery design that accepts both chip-based travel credentials and locally authoritative national IDs, with human review after bounded automated failure, will reduce legitimate-user abandonment without materially increasing successful fraudulent recovery.

Final position

The credibility of a professional network depends not only on detecting impostors but also on avoiding the exclusion of genuine members. A platform that operates globally should publish what evidence it accepts locally, explain failures at a useful level, and provide a meaningful appeal when automation cannot decide.

Suggested citation: Usman, M. (2026). *When a National ID Is Not Enough: Document Admissibility, Recovery Design, and LinkedIn Identity Verification Barriers for Pakistani Users.* Independent working paper, version 1.0.

References

1. LinkedIn. “Verifications on your LinkedIn profile.” LinkedIn Help. Accessed 14 October 2026. https://www.linkedin.com/help/linkedin/answer/a1359065?hcppcid=search
2. LinkedIn. “Identity verification via Persona.” LinkedIn Help. Accessed 14 October 2026. https://www.linkedin.com/help/linkedin/answer/a1631613
3. LinkedIn. “Troubleshoot identity verification by Persona.” LinkedIn Help. Accessed 14 October 2026. https://www.linkedin.com/help/linkedin/answer/a1631614?trk=li_fb_global_gco_care_facebook_social&linkId=100000417702789
4. LinkedIn. “Verify your identity to recover account access.” LinkedIn Help. Accessed 14 October 2026. https://www.linkedin.com/help/linkedin/answer/a1342692
5. LinkedIn. “ID verification troubleshooting tips.” LinkedIn Help. Accessed 14 October 2026. https://www.linkedin.com/help/linkedin/answer/a1617196?hcppcid=search&trk=li_fb_global_gco_care_facebook_social&linkId=100000291911398
6. LinkedIn. “Workplace verification with your work email.” LinkedIn Help. Accessed 14 October 2026. https://www.linkedin.com/help/linkedin/answer/a1423367
7. World Bank, Identification for Development. “Pillar 1: Inclusion.” Accessed 14 October 2026. https://id4d.worldbank.org/guide/pillar-1-inclusion
8. National Institute of Standards and Technology. *Digital Identity Guidelines: Enrollment and Identity Proofing*, NIST SP 800-63A. https://doi.org/10.6028/NIST.SP.800-63a
9. National Database and Registration Authority. “Privacy Policy.” Pak Identity. Accessed 14 October 2026. https://id.nadra.gov.pk/privacy-policy/
10. Press Information Department, Government of Pakistan. “NADRA Participates in TRUSTECH 2023 Exhibition in Paris.” 29 November 2023. https://pid.gov.pk/site/press_detail/24042
11. Press Information Department, Government of Pakistan. “NADRA Participates in TRUSTECH 2024 Exhibition, Paris.” 3 December 2024. https://pid.gov.pk/site/press_detail/27310
12. Press Information Department, Government of Pakistan. “Strict Measures Will Be Introduced to Curb Beggary and Illegal Immigration.” 10 April 2025. https://pid.gov.pk/site/press_detail/28549
13. Tech Updates Pakistan. “How to Verify Your LinkedIn Profile in Pakistan Using an NFC-Enabled e-Passport.” Accessed 14 October 2026. https://techupdates.pk/blog/how-to-verify-your-linkedin-profile-in-pakistan-using-an-nfc-enabled-e-passport
14. Persona. “Can I use a photo of my ID?” Persona Help Center. Accessed 14 October 2026. https://help.withpersona.com/articles/gyFutFQ7Gxc2I46Ein6QAM/

Source hierarchy

LinkedIn Help pages are treated as the primary source for LinkedIn’s published rules. Pakistan government and NADRA pages establish the national identity context. NIST and World Bank sources provide analytical standards rather than binding requirements. The Pakistan-focused implementation guide is used only as secondary evidence that an NFC e-passport route has been observed; it does not override LinkedIn’s live documentation.

Author declaration

This paper is independent and was not commissioned, endorsed, or reviewed by LinkedIn, Persona, NADRA, or Superior University Lahore. No personal identity-document numbers, account identifiers, or biometric data were collected or reproduced.