American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Resilient Digital Identity for Disaster Displaced Populations

Dr. Sameer Khanna

Assistant Professor, Jawaharlal Nehru University (JNU), India

Abstract

Natural hazards, climate-related emergencies, conflict-linked evacuations, and infrastructure failures can abruptly separate individuals from identity documents, home institutions, communications networks, and administrative records. The resulting identity discontinuity can restrict access to emergency relief, health services, temporary accommodation, financial assistance, social protection, telecommunications, and other essential services precisely when displaced populations are most vulnerable. This study develops a Resilient Digital Identity for Disaster-Displaced Populations (RDI-DDP) framework that treats identity as continuity infrastructure rather than as a single credential. The framework combines flexible identity proofing, multi-channel authentication, offline-capable verification, federation, recoverable credentials, privacy-preserving attribute disclosure, interoperable records, accessible redress, and continuity procedures for degraded network environments. Current NIST SP 800-63-4 separates identity proofing, authentication, and federation into distinct assurance dimensions and explicitly incorporates security, privacy, equity, and usability considerations. UNHCR's registration ecosystem provides an operationally relevant example: its PRIMES applications are designed for online and offline operation, while its Biometric Identity Management System can function under weak or unavailable internet connectivity and is intended to preserve continuity of identity across operations.

Because no authentic disaster-displacement dataset was supplied, the quantitative component uses a transparent simulation of 240 hypothetical identity-service scenarios distributed across four resilience architectures. Mean simulated identity-service recovery time declines from 67.73 hours in a paper-dependent architecture to 11.07 hours in a layered resilient model. The simulated association between resilience maturity and recovery time is strongly negative ($r = -0.877$). The findings are methodological illustrations rather than empirical estimates. The paper concludes that resilient identity should provide multiple legitimate pathways to recognition, avoid dependence on a single document, device, biometric, network, or institution, and preserve due process for individuals whose evidence is incomplete, damaged, inaccessible, or legally complex.

Keywords: digital identity; disaster displacement; identity resilience; humanitarian technology; identity proofing; offline verification; federated identity; biometrics; digital public infrastructure; inclusive identity

1. Introduction

Identity becomes operationally critical during disasters because access to assistance frequently depends upon an institution's ability to determine who an individual is, what claims can reasonably be associated with that person, and whether previously established records can still be trusted. Displacement can make these tasks unusually difficult. People may leave homes without passports, civil-registration certificates, identity cards, mobile phones, authentication devices, or other evidence. Administrative offices may be inaccessible, network connectivity may fail, and affected individuals may cross municipal, regional, or

national administrative boundaries. The World Bank has long identified lack of identification as a serious obstacle for people forced from their homes by conflict, persecution, or natural disaster because absence of recognized documentation can increase protection risks and restrict access to services.

The problem is not solved merely by replacing paper cards with digital credentials. A digital identity architecture can itself become fragile when access depends on a particular smartphone, active SIM, cloud connection, centralized database, biometric modality, or authentication mechanism. Disaster resilience therefore requires a more demanding design criterion: identity should remain recoverable and verifiable when normal infrastructure is partially unavailable. UNHCR's identity-management environment illustrates this operational requirement. Its PRIMES applications are designed to work in both online and offline environments, and its BIMS platform is designed to operate under varied infrastructure and connectivity conditions, including weak or absent internet. Such capabilities are directly relevant to populations moving through temporary shelters, field-registration centers, border locations, emergency clinics, and mobile assistance points.

Modern identity assurance also requires separation of several technical questions that are frequently collapsed into a single notion of "verification." NIST SP 800-63-4, finalized in 2025, provides current guidance for digital identity and distinguishes identity proofing and enrollment, authentication and authenticator management, and federation and assertions. This distinction is important in disaster settings. A person may have been strongly proofed before displacement but lose the authenticator they normally use. Another person may possess an authenticator but lack sufficiently accessible evidence for formal proofing. A third may need a relying organization to accept attributes asserted by another trusted institution. Resilience requires these situations to be handled through proportionate recovery mechanisms rather than assuming that failure at one identity layer invalidates the person.

Inclusiveness is equally important. The World Bank's ID4D guidance emphasizes non-exclusion and non-discrimination and warns that foundational identity systems can become exclusionary when eligibility rules or proof requirements prevent vulnerable residents from being recognized. Its 2026 guidance on statelessness-sensitive identity systems further argues that digital modernization can reinforce existing exclusion when people lacking conventional evidence are left outside interoperable databases or automated eligibility processes. The report recommends context-sensitive enrollment, accessible due process, grievance mechanisms, legal support, and attention to people whose nationality or documentation status is uncertain. These principles are particularly relevant after disasters, when previously documented people may temporarily resemble "undocumented" populations because their evidence is lost, inaccessible, or disconnected from functioning registries.

The present study develops a resilience-centered identity model for disaster-displaced populations. The central proposition is that identity continuity depends upon redundancy across evidence, authenticators, verification channels, institutions, and recovery procedures. Because no real participant or emergency-management dataset was supplied, the quantitative component is explicitly simulation-based. A synthetic dataset of 240 hypothetical identity-service scenarios is used to compare paper-dependent, centralized digital, offline-capable federated, and layered resilient identity architectures. The purpose is not to claim real disaster outcomes but to establish a transparent methodological framework that can subsequently be validated through field studies involving emergency authorities, civil registries, humanitarian organizations, and displaced populations.

2. Objectives of the Study

2.1 To Develop a Resilient Identity Continuity Model

The first objective is to develop an identity architecture capable of preserving recognition and service access despite loss of documents, devices, connectivity, or local administrative infrastructure. The

proposed model integrates flexible proofing, recoverable authenticators, offline-capable validation, federation, secure synchronization, minimal attribute disclosure, and post-disaster credential recovery. These components correspond conceptually with NIST's separation of identity proofing, authentication, and federation and with UNHCR's operational use of interoperable and offline-capable registration systems.

2.2 To Evaluate Identity-Service Recovery Across Resilience Architectures

The second objective is to use simulation to compare identity-service recovery time across four progressively resilient identity architectures. The analysis tests the proposition that systems with redundant verification channels and offline continuity can restore access to identity-dependent services more quickly than systems relying on a single physical credential or continuously available centralized infrastructure.

2.3 To Identify Inclusion, Privacy, and Governance Requirements

The third objective is to identify governance safeguards required when digital identity is deployed for disaster response. These include non-discrimination, proportional identity proofing, privacy protection, data minimization, accessible appeals, credential revocation and reissuance, cross-agency interoperability, purpose limitation, and protection against treating uncertain identity evidence as evidence of illegitimacy. World Bank and UNDP guidance emphasizes that digital identity can support disaster response and service access, but that privacy, security, inclusion, and rights protection must be built into identity systems.

3. Review of Literature

3.1 Identity Loss, Displacement, and Service Exclusion

Displacement can convert administrative identity into a protection issue. The World Bank's Identification in the Context of Forced Displacement explains that lack of identity documentation can obstruct protection and access to services for people displaced by conflict, persecution, or natural disaster. The practical consequences arise because formal systems frequently use identity documentation as the gateway to benefits, civil status processes, financial participation, communications services, education, health care, and other rights or services.

UNHCR similarly treats registration and identity management as integral to protection. Its current guidance describes registration, documentation, case management, assistance, and identity verification as connected operational processes. UNHCR documentation can demonstrate identity and refugee status and may reduce protection risks when individuals interact with official authorities. This evidence demonstrates why post-disaster identity cannot be evaluated merely as an information-technology problem. A failure to establish or recover identity can affect substantive access to safety and assistance.

Recent World Bank guidance broadens the issue further by examining statelessness-sensitive identity systems. The 2020 report warns that people without recognized identity evidence can be excluded from essential services and that digital transformation can intensify inequality when automated and interoperable systems reproduce existing documentation gaps. Although disaster displacement and statelessness are distinct conditions, the underlying design lesson is transferable: an identity system should not assume that absence of conventional documentation means absence of a legitimate identity claim.

The World Bank's ID4D principles therefore emphasize inclusion by design, people-centered implementation, protection of data, and non-discrimination. In disaster settings, this implies that alternative evidence, assisted proofing, trusted institutional attestations, family or community

relationships, previously established records, and graded assurance mechanisms may be required when standard documentation cannot reasonably be produced.

3.2 Digital Identity Assurance, Offline Operation, and Federation

NIST SP 800-63-4 provides a useful analytical structure because it treats digital identity assurance as several related but distinct functions. SP 800-63A-4 focuses on identity proofing and enrollment, through which evidence is evaluated to establish an identity at an appropriate assurance level. SP 800-63B-4 addresses authentication and authenticator management, covering the mechanisms through which a claimant demonstrates control of an authenticator associated with a previously established identity. SP 800-63C-4 addresses federation and assertions, enabling separately administered relying parties to accept authentication and attribute assertions from credential or identity providers.

This separation is highly relevant to disaster recovery because each layer can fail independently. Loss of a phone should not automatically erase the previously established identity. Temporary inability to reach the original credential service provider should not always prevent a trusted emergency service from accepting a verifiable assertion. Similarly, a replacement authenticator should not necessarily require the displaced person to repeat the entire original proofing process when suitable recovery evidence exists.

UNHCR's PRIMES architecture provides practical evidence that humanitarian identity operations must support multiple tools and operating conditions. PRIMES integrates registration, identity management, case management, administrative access, interoperability, and digital services. Its applications are designed for online and offline operation and interoperability with government and partner systems. BIMS maintains a centralized biometric identity record while supporting operations with weak or nonexistent connectivity, and UNHCR states that the system is intended to preserve continuity of identity across locations and over time.

3.3 Privacy, Inclusion, and Human-Centered Identity Resilience

Digital identity can improve continuity, but it can also intensify surveillance, exclusion, security, and data-protection risks. The World Bank's ID4D Practitioner's Guide identifies exclusion, privacy and security violations, vendor lock-in, and unsuitable technology choices among the principal risks of identity systems. The inclusion problem is especially significant when technology becomes mandatory but users lack devices, network access, biometric compatibility, literacy, or conventional evidence.

UNDP has argued that digital legal identity and civil-registration data can assist disaster preparedness, displacement response, and targeted support, while emphasizing that sensitive data should be protected through layered access and restricted to authorized use. The same source notes that identity information may assist authorities in identifying displaced or vulnerable populations and coordinating disaster-related assistance. These benefits create a strong justification for resilient digital identity, but also increase the consequences of unauthorized access because identity records may include highly sensitive information.

Biometrics illustrate this tension clearly. UNHCR uses biometrics for identity verification and BIMS can record fingerprints and irises as part of identity management. Biometrics can support continuity when people lose physical credentials, but they should not be treated as universally available or infallible. The resilience principle proposed in this study therefore avoids “biometric-only” architecture. Biometrics can constitute one high-value verification channel alongside previously issued credentials, cryptographic evidence, trusted records, assisted recovery, and human review.

The literature reveals a broader gap. Digital-identity standards provide detailed assurance requirements, and humanitarian registration systems demonstrate field-oriented identity technologies, but disaster resilience requires these insights to be integrated explicitly around continuity under failure.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

The present study addresses this gap by evaluating identity architecture according to how effectively it can maintain or recover service access when evidence, connectivity, devices, and institutional availability are degraded simultaneously.

4. Research Methodology

4.1 Research Design and Simulation Scope

The study adopts a simulation-based quantitative design supported by identity standards and humanitarian identity guidance. No displaced person was recruited, no government identity record was processed, and no emergency-relief database was accessed. The analysis is therefore a methodological demonstration rather than an empirical claim about actual disaster-affected populations.

A synthetic dataset of 240 hypothetical identity-recovery scenarios was created. Sixty scenarios were assigned to each of four identity architectures: Paper-Dependent, Centralized Digital, Offline-Capable Federated, and Layered Resilient Identity.

The Paper-Dependent condition represents environments in which access depends mainly upon physical documents and manual institutional confirmation. The Centralized Digital condition represents systems that maintain digital records but require reliable connectivity to a central service. The Offline-Capable Federated condition adds offline verification and trusted interoperability across participating institutions.

4.2 Proposed Measurement Instrument

A future empirical study should combine technical performance measures with the experiences of displaced users, emergency workers, registration personnel, health providers, civil-registry staff, and other service operators. The following five-item questionnaire is proposed as an initial screening instrument.

Table 1: Proposed Questionnaire for Disaster-Resilient Digital Identity

Item	Proposed Questionnaire Statement	Primary Construct
Q1	I can prove or recover my identity even if my primary physical identity document has been lost or damaged.	Identity recoverability
Q2	Essential identity-dependent services remain accessible when mobile networks or internet connectivity are unavailable or unreliable.	Offline continuity
Q3	I can use more than one secure method to authenticate or recover access if my usual phone, SIM, credential, or authenticator is unavailable.	Authentication resilience
Q4	Only the minimum identity information necessary for a particular relief or public-service transaction is disclosed.	Privacy and data minimization
Q5	I can obtain human assistance and appeal an identity decision when automated or document-based verification fails.	Due process and inclusion

Source: Proposed by the author for future empirical validation. These questions were not administered to actual displaced persons.

The instrument should be tested for content validity, reliability, construct validity, linguistic accessibility, measurement invariance, and usability across people with different literacy levels, disabilities, languages, and technology experience. Self-reported confidence should also be supplemented by observed recovery outcomes because perceived accessibility may differ from actual system performance.

4.3 Synthetic Variables, Statistical Analysis, and Ethical Position

The primary synthetic outcome was Identity-Service Recovery Time, measured in hours from initial verification failure or displacement-related identity interruption to restoration of sufficient identity assurance for a defined essential service.

Randomized values were generated around distinct architecture-specific recovery distributions. The simulation produced mean recovery times of 67.73 hours for Paper-Dependent systems, 37.49 hours for Centralized Digital systems, 23.69 hours for Offline-Capable Federated systems, and 11.07 hours for Layered Resilient Identity systems.

The ethical position of the study is particularly important because disaster-displaced populations may experience heightened vulnerability. Actual research should minimize collection of sensitive data, avoid linking participation to eligibility for relief, provide accessible informed consent, prevent disclosure of immigration or protection-sensitive information, implement strict access controls, and preserve human review when identity systems produce uncertain or adverse outcomes. The World Bank's current statelessness-sensitive guidance emphasizes accessible redress, context-sensitive enrollment, and protection against exclusion, while ID4D guidance emphasizes privacy, security, and non-discrimination.

5. Analysis

5.1 Recovery Performance Across Identity Architectures

The synthetic analysis identifies a progressive reduction in service-recovery time as resilience capabilities increase.

Paper-Dependent scenarios produced the longest average recovery time at 67.73 hours, with a standard deviation of 13.69 hours. Centralized Digital systems reduced the mean to 37.49 hours, demonstrating the benefit of previously digitized identity records but retaining substantial dependence on central connectivity.

Table 2: Simulated Identity-Service Recovery Outcomes

Identity Architecture	Simulated n	Mean Recovery Time	Median Recovery Time	SD	Illustrative Successful Verification Rate
Paper-Dependent	60	67.73 h	69.57 h	13.69	61.8%
Centralized Digital	60	37.49 h	36.15 h	12.41	76.4%
Offline-Capable Federated	60	23.69 h	23.31 h	7.22	87.6%
Layered Resilient Identity	60	11.07 h	12.08 h	5.56	95.1%

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Source: Author-generated synthetic dataset; total simulated n = 240. Verification percentages are illustrative simulation parameters and do not represent measured disaster-response outcomes.

The difference between the least and most resilient conditions is 56.66 hours in mean recovery time. The layered architecture therefore restores simulated identity-dependent service access approximately five to six times faster than the paper-dependent model. This should not be interpreted as an empirical performance estimate; its purpose is to illustrate the expected direction and magnitude of an operationally meaningful resilience effect.

5.2 Relationship Between Resilience Maturity and Recovery Time

The Pearson correlation between the four-level resilience index and identity-service recovery time was:

$r = -0.877$

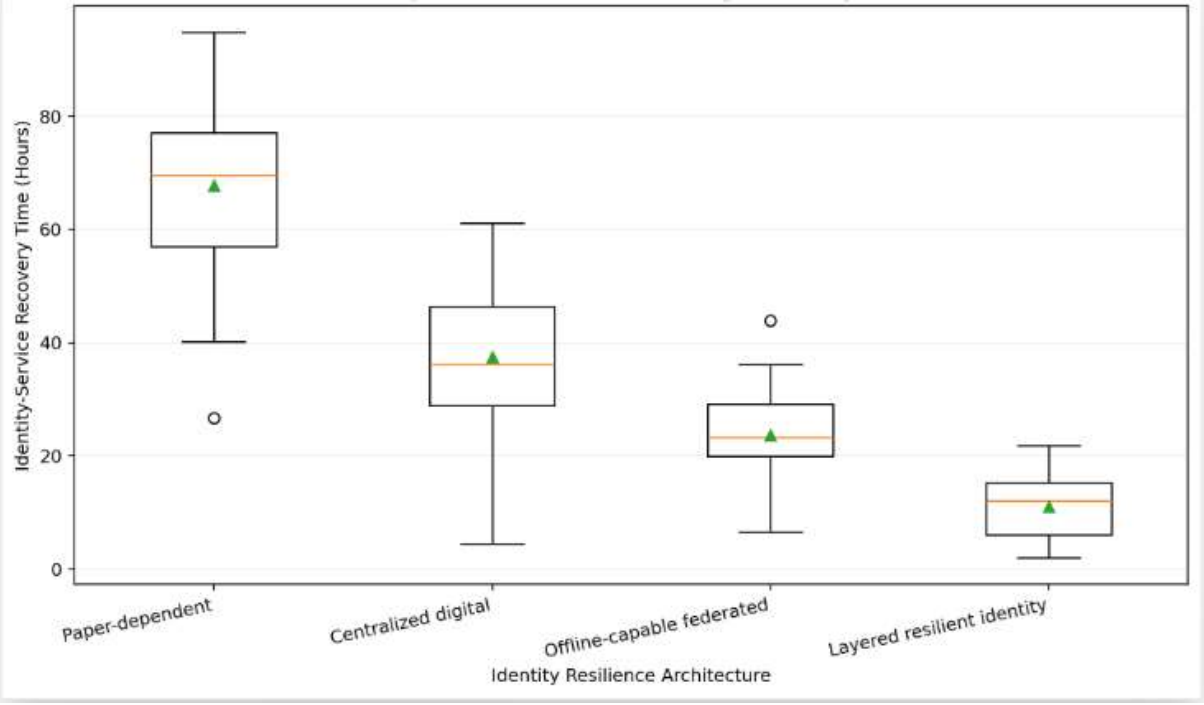
The strong negative relationship indicates that higher identity-resilience maturity corresponds to shorter recovery time in the synthetic dataset.

A simple linear representation of the simulated relationship generated a slope of approximately −18.38 hours per resilience tier. In methodological terms, the model illustrates how future empirical studies could evaluate whether additional redundancy and interoperability produce measurable improvements in service continuity.

The decrease is not assumed to arise from a single technology. Rather, resilience accumulates from multiple design choices: alternative proofing routes, secure credential replacement, cached or offline verification, portable signed assertions, federation, synchronized records, authorized emergency access, and human escalation.

5.3 Distribution of Identity-Service Recovery Time

Graph 1: Simulated Recovery-Time Distribution Across Digital Identity Resilience Models



Source: Author-generated synthetic analysis.

Interpretation: The box plot shows that recovery time declines not only in average value but also in dispersion as identity architecture becomes more resilient. Paper-dependent and centralized systems show substantially longer and more variable recovery periods, whereas the layered model clusters around relatively short restoration times.

Key Finding: Resilience is reflected in both speed and predictability. A disaster identity architecture is operationally stronger when affected people can regain service access quickly and when recovery performance remains consistent despite disruption.

The analytical implication is that identity systems should be evaluated through continuity metrics rather than enrollment volume alone. A system may perform well under normal conditions yet remain fragile if it cannot support people who lose a credential, move outside the issuing jurisdiction, experience network failure, or require human review.

6. Discussion

6.1 Identity Resilience Requires Redundancy Rather Than a Single "Perfect" Credential

The central implication of the study is that disaster resilience cannot be achieved by making one identity credential increasingly sophisticated. A highly secure digital credential still fails operationally if the device containing it is lost, the user cannot unlock it, connectivity is unavailable, or the verifying service cannot contact the issuing system. Resilience therefore requires controlled redundancy.

NIST's current Digital Identity Guidelines support this conceptual distinction by separating proofing, authentication, and federation into different assurance processes. The recovery architecture proposed here extends that logic into disaster operations. Previously established proofing evidence should remain meaningful after loss of an authenticator; alternative authenticators should be recoverable without unnecessarily restarting identity establishment; and federation can allow trusted organizations to recognize authenticated claims across administrative boundaries.

UNHCR's operational systems demonstrate that identity continuity can be designed for difficult connectivity environments. PRIMES applications support online and offline operation, BIMS functions with weak or unavailable connectivity, and Verify Plus provides digitally signed document verification. These capabilities illustrate the value of layered evidence and portable verification rather than dependence on a single always-online portal.

A resilient public architecture could similarly provide several paths to recognition. One person may present a signed digital credential, another may be matched to an existing registry, another may use an offline-verifiable token, and another may require assisted evidence review. The security objective is not to reduce assurance indiscriminately; it is to make assurance recoverable through proportionate and auditable pathways.

6.2 Inclusion and Due Process Must Remain Functional During Emergency Verification

Disaster conditions create strong pressure for fast automation, but emergency efficiency should not remove due process. A person who cannot satisfy a standard identity check may have lost documents, devices, family contacts, or access to their issuing authority. Automatic rejection can therefore transform technical failure into exclusion from essential services.

The World Bank's 2020 statelessness-sensitive identity guidance is particularly relevant because it recommends enrollment processes that do not mechanically require proof of nationality, accessible appeals, legal assistance, consultation with affected communities, and context-sensitive implementation. While a disaster-displaced citizen is not necessarily stateless, the design problem is similar whenever expected evidence is absent. Systems should distinguish "identity not yet sufficiently established" from "person is fraudulent."

Non-exclusion also requires channel diversity. Smartphone-only recovery can exclude people whose device was destroyed, whose battery is unavailable, who cannot replace a SIM, or who lack digital literacy. Biometric-only recovery can also be problematic when a modality cannot be captured reliably or when biometric processing is inappropriate for the transaction. A resilient identity system should therefore permit secure alternatives.

Human review is a core resilience mechanism rather than an exception indicating technological failure. Complex identity cases involve contextual information, previous records, family relationships, institutional attestations, damaged evidence, and legal status questions that may not be safely reduced to automated matching. Accessible escalation should therefore be built into the service model from the beginning.

6.3 Privacy-Preserving Continuity Is Essential for Trust and Long-Term Safety

Identity systems used during disasters can accumulate highly sensitive information because emergency response may involve location, household composition, vulnerability status, health needs, financial assistance, shelter placement, and contact information. UNDP has highlighted the potential value of digital identity and foundational registry data during disasters while also emphasizing layered access controls and privacy protection.

Resilience should consequently not be interpreted as unlimited data replication. Replicating complete identity databases across every emergency node could improve availability while greatly increasing exposure. A stronger architecture would combine resilient availability with selective disclosure, encrypted synchronization, role-based access, audit logs, purpose limitation, and retention controls.

Federation is valuable in this respect because a relying organization may not require a complete identity record. In many transactions, the service may only need confirmation of a limited attribute or eligibility status. NIST SP 800-63C-4 provides the conceptual basis for identity providers to assert authentication and subscriber attributes to separately administered relying parties. A disaster-response architecture can use this principle to minimize disclosure while preserving interoperability.

Long-term trust also depends on post-disaster governance. Temporary credentials need expiration or transition rules, emergency privileges require revocation, duplicate records should be reconciled, and individuals should be able to correct inaccurate information. Data collected under emergency authority should not automatically become a permanent basis for unrelated surveillance or decision-making. Resilient identity is therefore a governance capability as much as a technical system.

7. Conclusion

Disasters expose a structural weakness in identity systems that perform well only under normal administrative conditions. Physical documents may be lost, authentication devices destroyed, telecommunications disrupted, registries inaccessible, and individuals displaced beyond the institutions that originally issued or recognized their credentials. In such conditions, identity becomes part of continuity infrastructure because access to assistance and essential services can depend upon the ability to re-establish trustworthy identity relationships. The World Bank, UNHCR, NIST, and UNDP provide complementary evidence that identity systems must address inclusion, proofing, authentication, interoperability, privacy, offline operation, and disaster-related service continuity.

The simulation developed in this study illustrates the potential operational effect of resilience-oriented design. Across 240 hypothetical scenarios, mean identity-service recovery time declined from 67.73 hours in a paper-dependent environment to 11.07 hours in a layered resilient identity architecture. The simulated correlation between resilience maturity and recovery time was −0.877. These results are not measurements from actual displaced populations and should not be interpreted as population

estimates. Their contribution is methodological: they demonstrate that disaster identity systems can be evaluated in terms of restoration time, verification success, failure variability, and continuity rather than only enrollment coverage.

The proposed RDI-DDP framework therefore recommends redundancy across several identity dimensions. Strong identity proofing should be preserved where it has already occurred, authentication should remain recoverable when an authenticator is lost, federation should enable trustworthy cross-agency assertions, offline verification should reduce dependence on continuous connectivity, and human review should remain available when standard evidence cannot be produced. No individual should be expected to maintain continuous possession of one document, device, biometric capability, or network connection throughout a disaster.

Future empirical research should validate the framework in collaboration with disaster-management authorities, civil registries, humanitarian organizations, service providers, and displaced communities. Field studies should measure recovery time, false rejection, duplicate identity creation, fraud detection, offline verification reliability, privacy outcomes, user comprehension, appeal success, and service accessibility across different demographic and disability groups. Comparative studies should also examine centralized, federated, wallet-based, biometric-assisted, and hybrid identity architectures under simulated infrastructure outages. The goal of resilient digital identity should ultimately be straightforward: a disaster may interrupt infrastructure, but it should not erase a person's practical ability to be recognized, protected, and served.

References

1. Gelb, A., & Metz, A. D. (2018). *Identification Revolution: Can Digital ID Be Harnessed for Development?* Center for Global Development.
2. World Bank. (2017). *Principles on Identification for Sustainable Development: Toward the Digital Age*. World Bank Group.
3. World Bank. (2019). *ID4D Global Dataset 2019: Global Identification Challenge*. World Bank.
4. World Bank. (2021). *Principles on Identification for Sustainable Development: Toward the Digital Age—Second Edition*. World Bank Group.
5. Gelb, A., & Clark, J. (2013). Identification for development: The biometrics revolution. *Center for Global Development Working Paper, 315*, 1–39.
6. Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review, 30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002
7. Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access, 7*, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2939271
8. Allen, C. (2016). *The Path to Self-Sovereign Identity*. Life With Alacrity.
9. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, 180–184. https://doi.org/10.1109/SPW.2015.27
10. World Food Programme. (2018). *Building Blocks: Blockchain for Zero Hunger*. United Nations World Food Programme.
11. UNHCR. (2018). *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*. United Nations High Commissioner for Refugees.

12. UNHCR. (2020). *UNHCR Policy on the Processing of Biometric Data of Persons of Concern to UNHCR*. United Nations High Commissioner for Refugees.
13. Jacobsen, K. L. (2017). On humanitarian refugee biometrics and new forms of identification. *Ethics and Information Technology, 19*, 3–13. https://doi.org/10.1007/s10676-016-9414-y
14. Madianou, M. (2019). Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises. *Social Media + Society*, *5*(3), 1–13. https://doi.org/10.1177/2056305119863146
15. Latonero, M., Poole, D., & Berens, J. (2019). *Refugee Connectivity: A Survey of Mobile Phones, Privacy, and Data Protection*. Data & Society Research Institute.
16. Gillespie, M., Ampofo, L., Cheesman, M., Faith, B., Iliadou, E., Issa, A., Osseiran, S., & Skleparis, D. (2016). Mapping refugee media journeys: Smartphones and social media networks. *Research Report*. Open University.
17. International Organization for Migration. (2019). *IOM Data Protection Principles*. International Organization for Migration.
18. World Bank. (2018). *ID4D Practitioner's Guide: Identification for Development*. World Bank Group.
19. UNDP. (2019). *Digital Strategy 2020–2025: Digitalization for Development*. United Nations Development Programme.
20. World Economic Forum. (2018). *Identity in a Digital World: A New Chapter in the Social Contract*. World Economic Forum.