THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-8-2-(2)2025

UNJSPF Blockchain-based Digital Identity Solution for Proof-of-Life

Dino Cataldo Dell'Accio and Mirko Montuori
United Nations Joint Staff Pension Fund (UNJSPF), USA

Correspondence: dellaccio@un.org, mirko.montuori@un.org
Received: 6 February 2025 **Accepted**: 18 April 2025 **Published**: 30 July 2025

Abstract
This article presents the insights and experience from a four-year journey of implementing a cutting-edge Digital Identity Solution for Proof-of-Life in the United Nations Joint Staff Pension Fund (UNJSPF). The solution, which leveraged blockchain, biometrics, artificial intelligence (AI), and geo-localisation technologies, has revolutionised the process of verifying pension beneficiaries' existence. The article delves into the challenges faced and addressed during deployment, highlighting how the system has enhanced accountability, security, and efficiency in beneficiary verification. Emphasis is placed on the solution's success in streamlining what was previously a lengthy, error-prone manual process and the critical aspects of trust and assurance, discussing how UNJSPF has worked to ensure the reliability and security of the solution through external audits and certifications, including ISO standards.

Keywords: *Digital Identity Solution, Artificial Intelligence, Blockchain, Distributed Ledger Technology, Geo-localisation, Biometrics, United Nations Joint Staff Pension Fund, United Nations, UNJSPF*

JEL Classifications: *O3 (technological change and the knowledge-based economy)*

1. Introduction

The United Nations Joint Staff Pension Fund (UNJSPF) was established in 1948, by a resolution of the General Assembly, to provide retirement, death, disability, and related benefits for staff upon cessation of their services with the United Nations and the other organisations admitted to membership in the Fund. As an independent interagency entity, the Fund operates under its own Regulations as approved by the General Assembly and, in accordance with its governance structure, is administered by the United Nations Joint Staff Pension Board, which currently consists of 33 members, representing the 25 member organisations.

Historically, the process of verifying the continued eligibility of UNJSPF retirees and beneficiaries, known as the "proof-of-life" verification, has been a significant administrative challenge. Traditionally, this process involved the annual submission of a paper-based Certificate of Entitlement (CE), which required beneficiaries to physically mail the form to the UNJSPF. This method was not only time-consuming and prone to errors but also presented significant logistical challenges, especially for beneficiaries residing in remote or conflict-affected areas [21].

To address these challenges, UNJSPF embarked on a journey to develop a cutting-edge Digital Identity Solution known as the Digital Certificate of Entitlement (DCE). This solution was developed in collaboration with the United Nations International Computing Centre (UNICC), which provided the technical expertise to create a solution that leveraged advanced technologies such as blockchain, biometrics, AI, and geo-localisation in streamlining the proof-of-life verification process. The DCE app allows beneficiaries to provide their proof-of-life through a secure, user-friendly mobile application, significantly enhancing the efficiency, security, and accuracy of the verification process.

The implementation of the DCE represents a significant innovation in the field of digital identity and has set a new standard for how international organisations can leverage technology to improve administrative processes. This article presents the insights and experience gained from the four-year journey of implementing the DCE, highlighting the challenges faced, the solutions developed, its evolution, and the impact of the DCE on the verification process [23].

Enrolment in the Digital Identity Solution is optional and not mandatory. Users enrolled in the digital solution can opt out at any time during each fiscal year. UNJSPF maintains the paper-based process in parallel to the digital one.

2. Methodology

UNJSPF faced a significant challenge in confirming the annual "proof-of-life" for its over 80,000 retirees and beneficiaries residing in over 190 countries. For more than 70 years, this process relied on a manual, paper-based system where

beneficiaries would receive and return a signed Certificate of Entitlement (CE) form via postal services. This traditional method was fraught with issues, including delays, lost forms, and errors, which often resulted in frustration for both the beneficiaries and the Fund, as well as questioning from UN governing and oversight bodies.

2.1 Challenges of the Traditional Process

The manual process required significant resources for physical and logical storage, handling, and verification of the returned forms. It was also environmentally unfriendly due to the extensive use of paper and postal services. Moreover, the process was time-consuming and prone to human error, which could lead to incorrect or incomplete submissions. The reliance on over 190 different postal services worldwide further complicated the process, as delivery times and reliability varied greatly, in addition to having a significant environmental impact.

2.2 Need for Digitalisation

To address these challenges, UNJSPF recognised the need to digitalise the Certificate of Entitlement process. This involved developing a system that could efficiently and securely verify the identity and existence of beneficiaries while also confirming their location and ensuring the integrity of the transaction. The digital solution needed to provide four critical proofs:

(i) Proof of Identity/Authentication, ensuring that the person submitting the DCE is who they claim to be.
(ii) Proof-of-Life, confirming the beneficiary is alive.
(iii) Proof of Transaction, verifying that the submission was made by the beneficiary.
(iv) Proof of Location, confirming the beneficiary's residence, when necessary (i.e., in those instances where beneficiaries elect to receive their benefits in local currency).

2.3 Requirements

UNJSPF faced a complex challenge in transitioning its traditional paper-based Certificate of Entitlement (CE) process to a digital platform. This transformation required careful consideration of several key requirements to ensure alignment with UN strategies, security, reliability, transparency, accountability, and attribution.

2.4 Alignment with UN Strategies

- 2018 United Nations Secretary-General Strategy on New Technologies: The digitalisation of the CE process needed to align with the Secretary-General's strategy, which emphasises the use of new technologies to accelerate the achievement of UN mandates, particularly the 2030 Agenda. This involved leveraging technologies like AI, blockchain, and biometrics to enhance efficiency and transparency.
- United Nations Secretary-General UN 2.0: The initiative to modernise the UN through innovation and digital solutions also played a crucial role. The UN 2.0 vision aims to strengthen expertise in data, digital innovation, and foresight to better support Member States. By embracing this vision, the UNJSPF could ensure that its digital solutions were forward-thinking and aligned with broader organisational goals.
- Sustainable Development Goals (SDGs): The digitalisation process should contribute to achieving the SDGs, particularly by supporting the achievement of Target 16.9 on legal identity, reducing environmental impact through reduced paper usage, and enhancing access to information for beneficiaries worldwide.

2.5 Security Requirements

To protect sensitive beneficiary data from unauthorised access, modification, or deletion by using robust security measures, including:

- Encryption: Encrypting data both in transit and at rest to prevent unauthorised access.
- Authentication: Implementing strong authentication mechanisms to ensure that only authorised individuals can access and modify data.
- Consensus Mechanisms: Utilising blockchain technology with proven and reliable consensus mechanisms to secure transactions and ensure data integrity.

2.6 Reliability Requirements

Ensuring the reliability of the digital platform was crucial to maintaining beneficiary trust and operational continuity, providing:

- Redundancy: Implementing redundant systems to prevent single points of failure; and
- Fault Tolerance: Designing the system to continue functioning even if some components fail, ensuring minimal downtime and maintaining service availability [6].

2.7 Transparency Requirements

Transparency was essential to build trust among beneficiaries and stakeholders, ensuring:

- Data Immutability: Utilising blockchain or similar technologies to ensure that once recorded, data cannot be altered or deleted, providing a tamper-proof record [8].
- Auditability: Ensuring that all transactions and changes are traceable and can be audited to verify compliance and integrity.

- Traceability: Maintaining a clear history of all actions taken within the system to facilitate accountability.

2.8 Accountability Requirements

To ensure accountability, the system needed to:

- Record Data Chronologically: Store data in a chronological and irreversible manner to maintain a complete and accurate history of transactions.
- Provide Transaction History: Offer a comprehensive record of all transactions, allowing for easy tracking and verification of beneficiary interactions.

2.9 Attribution Requirements

Finally, the system had to support attribution by:

- Linking Data to Identities: Ensuring that all data is linked to the identities of participants, providing proof of their actions and maintaining accountability.
- Proof of Actions: Offering clear evidence of who performed specific actions within the system, enhancing trust and compliance.

3. Key Components of the Solution

The UNJSPF DCE represents a significant advancement in the verification of pension beneficiaries. This chapter explores the key components of the solution, including the roles of the registrar and authentication processes, blockchain integration, and the decision models employed.

The UNJSPF DCE leverages the integration of blockchain, AI, biometrics, and geo-localisation to overcome the limitations of traditional methods.

Blockchain technology offers a decentralised and tamper-proof ledger, ensuring the integrity and immutability of identity data. Transactions on a blockchain are transparent and traceable, enhancing trust and accountability.

AI plays a crucial role in fraud detection by analysing patterns and detecting anomalies, helping to identify and prevent fraudulent activities. AI-driven processes automate identity verification, reducing manual intervention and improving efficiency.

Biometric technologies, such as facial recognition, provide unique and reliable methods of verifying an individual's identity. Advanced biometric systems incorporate liveness detection to prevent spoofing and ensure that the biometric data is captured from a live person.

Geo-localisation technologies enable the verification of a user's location, adding an additional layer of security to the identity verification process. By understanding the user's location, systems can provide context-aware services and detect potential anomalies.

These technological advancements have paved the way for more secure, efficient, and user-friendly digital identity solutions, addressing many of the challenges faced by traditional methods. The UNJSPF Digital Identity Solution leverages these technologies to enhance the proof-of-life verification process, as discussed in the subsequent sections of this article.

4. System Architecture and Design

The UNJSPF DCE is built on a robust and scalable architecture that integrates multiple advanced technologies. At its core, the system employs a blockchain platform to ensure the immutability and transparency of identity data. This decentralised ledger records all transactions related to the proof-of-life verification process, providing a tamper-proof audit trail [4].

The architecture also incorporates AI and biometric technologies to enhance security and accuracy. The AI module, embedded within the facial recognition and biometrics algorithm, is designed to detect and prevent potential "deep fakes" by employing advanced liveness detection techniques [5]. This ensures that the biometric data captured is from a live person, thereby preventing spoofing attempts.

Geo-localisation technology is another critical component of the system architecture. It enables the verification of a user's location, adding an additional layer of security to the identity verification process. By understanding the user's location, the system can also detect potential anomalies [6].

4.1 Design Patterns, Components, and Macro Processes

The design of the UNJSPF DCE follows several key patterns that ensure its effectiveness and reliability. One of the primary design patterns employed is the use of microservices architecture. This approach allows the system to be modular, with each service responsible for a specific function, such as identity verification, data storage, or user authentication [7, 10, 11]. This modularity enhances the system's scalability and

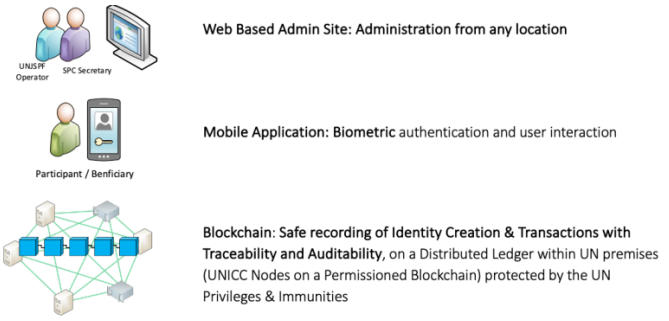
maintainability, allowing for easier updates and integration of new features.

Furthermore, the solution employed a "Decentralised Identifiers Documents (DIDs)" design pattern, which empowers users with full control over their digital identities. A security decision model underpinned this approach, ensuring robust authentication and authorisation mechanisms. This security model incorporated several key elements:

- Identifiers registry: A decentralised registry for storing and managing DIDs.
- Multiple registrations: Allowing users to register multiple identifiers for different contexts.
- Blockchain and account pairing: Ensuring that each digital identity is securely linked to a blockchain account.
- Dual resolution: Providing both on-chain and off-chain resolution mechanisms for DIDs to enhance flexibility and security.

The decision model also emphasised "Authentication and Authorisation," ensuring that only authorised parties can access and verify identity information.

4.2 Components



The solution consists of three primary components:

- Web administrator site: This platform is used for managing the system, monitoring transactions, and overseeing the issuance of digital certificates.
- Mobile application: Users interact with the system through a mobile app, which facilitates enrolment, biometric data capture, and proof-of-life verification.
- Blockchain: The blockchain serves as the backbone for storing and verifying transactions related to digital identities and proof-of-life confirmations. No personal identifiable information is recorded on the blockchain. Indeed, the blockchain captures only the transaction validation data (i.e., root hash), transaction type (i.e., attribute transaction), transaction timestamp (i.e., epoch), and sender public signature (i.e., public key).

4.3 Registrar and Authentication

At the heart of the DCE is the registrar (i.e., UNJSPF or HR Department of UN organisations), which plays a crucial role in managing and verifying the identities of retirees and beneficiaries. The registrar is responsible for enrolling users into the system, ensuring that their biometric data is accurately captured and securely stored on their devices. This process involves the collection of facial recognition data, which is then used for subsequent proof-of-life verifications [21].

Authentication within the DCE is multi-faceted, combining biometric verification with blockchain technology to ensure the highest levels of security and accuracy. When a beneficiary submits their proof-of-life via the DCE app, their biometric data is matched against the stored records (i.e., maintained exclusively on their device). This process is enhanced using AI algorithms that detect and prevent potential synthetically generated images (aka "deep fakes") through advanced liveness detection techniques.

The integration of these technologies ensures that the verification process is both secure and reliable.

4.4 Blockchain Integration

Blockchain technology is a cornerstone of the DCE, providing a decentralised and tamper-proof ledger for recording all transactions related to the proof-of-life verification process. The UNJSPF solution is based on Hyperledger Indy (Distributed Ledger) and Aries (Libraries). The revocation mechanism for the solution is described in the relevant Hyperledger documentation available online [26].

Each transaction, including the submission of biometric data and the verification results, is recorded on the blockchain, ensuring transparency and immutability [19]. This decentralised approach not only enhances security but also builds trust among beneficiaries, as they can be confident that their data is protected from unauthorised alterations.

The blockchain integration also facilitates dual resolution, where both the registrar and the blockchain independently verify the authenticity of the data. This redundancy adds an extra layer of security, ensuring that any discrepancies are quickly identified and addressed [20].

4.5 Rationale for the Adoption of a Blockchain

UNJSPF is an Interagency UN Entity serving 25 UN Member Organisations, with their own governing and oversight bodies. Therefore, the blockchain is used by over 80,000 retirees of 25 UN Member Organisations (i.e., not just a single organisation) to which UNJSPF is accountable for the security, integrity, and transparency of the pension processing.

The rationale behind the use of a blockchain was further justified by the need to prevent/detect any potential instances of "collusion" between UNJSPF employees (i.e., Database Administrators, Payment Officers, etc.) and retirees/beneficiaries. The reasons for rejecting a public blockchain were as follows:

Control and Trust: Manage and operate a controlled environment where UNJSPF can ensure that all participants are trusted entities, reducing the risk of unauthorised access or malicious activities.

Enhanced Privacy and Security: Restrict access to specific participants only. This enhances privacy and security by limiting who can view and interact with the data.

Scalability: Handle a higher volume of transactions more efficiently because only a limited number of nodes need to process and verify transactions.

Regulatory Compliance: Define and comply with specific UN regulatory requirements.

4.6 Governance Model

UNJSPF adopted a centralised governance model, where decision-making authority is held by the Senior Management Team of the Fund, to ensure:

- Controlled Access: Only authorised users can participate in the process, ensuring privacy and compliance with UN regulatory requirements.
- Centralised Decision-Making: UNJSPF decides on network rules, membership, and transaction validation.

For the specific "Proof-of-Life" use case, UNJSPF serves as both the issuer and verifier of credentials.

4.7 Addressing Potential Errors or Biometric Breaches

In the event of significant errors, UNJSPF has the authority to roll back the ledger. This is because the Fund implemented a permissioned blockchain to serve its specific requirements.

Potential breaches of biometric data are prevented and minimised by the fact that this data is only stored on the hardware security module of the end-user device. Biometric data is never stored or transmitted outside the user's device.

The UNJSPF approach to handle potential cases of biometric data breaches is to:

- Adhere to international certification standards (i.e., ISO/IEC 27001:2022, ISO/IEC 42001:2023, ISO/IEC 30107-3:2023, NIST Face Recognition Vendor Test);
- Conduct regular risk assessments (i.e., Algorithmic Assessments, Data Privacy Assessments); and
- Ensure continuous monitoring through a dedicated team.

4.8 Comparison with Alternative Options (i.e., Secure Cloud Databases)

One of the most frequent arguments about the use of blockchain centres around the perceived/assumed better or equal level of security and reliability of cloud-based databases. However, there are significant risks associated with relying on secure cloud databases, particularly concerning data manipulation and collusion risks posed by super-user access, as follows:

A. Super-User Access and Data Manipulation:

- Risk of data tampering: Even with robust security measures, cloud databases are typically managed by database administrators (DBAs) who possess super-user privileges. These privileges allow them to access, modify, or delete data without necessarily leaving an audit trail. This creates a significant risk of data tampering, which can be difficult to detect and rectify.
- Lack of accountability: In a cloud database, if a super-user manipulates data, it may be challenging to identify who made the changes, especially if there is no robust logging mechanism in place. This lack of accountability can lead to serious security breaches without clear consequences for the perpetrator.

B. Collusion Risks:

- Insider threats: The presence of DBAs with elevated privileges inherently introduces the risk of collusion. If multiple administrators collude, they can manipulate data or cover their tracks, potentially leading to catastrophic security breaches. This risk is exacerbated by the concentration of power in the hands of a few individuals.
- External influence: Additionally, there is a risk that external entities could influence or coerce DBAs to compromise the system, further increasing the vulnerability of cloud-based databases.

4.9 Ethical Considerations

Regarding the ethical concerns, the solution has been the subject of:

- Independent Ethical Assessment
- Independent Algorithmic Audit
- Independent Privacy Assessment
- NIST Facial Recognition Vendor Test (FRVT)
- Certification in accordance with ISO/IEC 27001:2022 (Information Security)

- Currently being certified in accordance with ISO/IEC 42001:2023 (Artificial Intelligence)
- Currently being tested in accordance with ISO/IEC 30107-3 (Presentation Attack Detection)

5. Self-Sovereign Identity and Verifiable Credentials

The DCE is a pioneering example of how self-sovereign identity (SSI) and verifiable credentials can be effectively implemented to enhance the proof-of-life verification process for pension beneficiaries. This chapter explores the concepts of self-sovereign identity and verifiable credentials and their application within the DCE.

5.1 Concept of Self-sovereign Identity

Self-sovereign identity (SSI) is a paradigm shift in the way digital identities are managed. Unlike traditional identity systems, where control over identity data is held by centralised authorities, SSI empowers individuals to own and control their digital identities. This approach is built on the principles of decentralisation, privacy, and user autonomy [1].

In the context of the DCE, SSI allows retirees and beneficiaries to have full control over their identity data. They can manage their personal information, decide who has access to it, and revoke access when necessary. This level of control not only enhances privacy but also builds trust among users, as they are assured that their data is not being misused or accessed without their consent [2].

5.2 Verifiable Credentials

Verifiable credentials are a key component of SSI. They are digital representations of information that can be cryptographically verified. These credentials can include various types of information, such as identity documents, certificates, and proofs of life. The use of verifiable credentials ensures that the information is authentic and has not been tampered with [3].

Within the DCE, verifiable credentials are used to securely store and transmit proof-of-life data. When a beneficiary submits their proof-of-life through the DCE app, their biometric data is converted into a verifiable credential. This credential is then stored on the blockchain, ensuring its immutability and authenticity. The use of verifiable credentials not only enhances security but also simplifies the verification process, as the credentials can be easily and quickly verified by the UNJSPF [4].

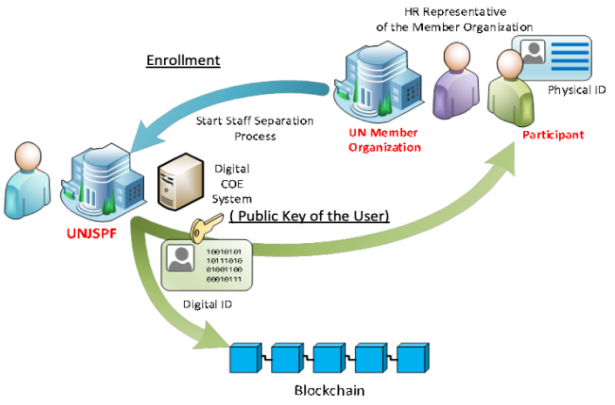
6. Implementation of the DCE

The implementation of SSI and verifiable credentials within the DCE involves several key steps. First, beneficiaries enrol in the system by providing their biometric data, which is then converted into a digital identity. This identity is stored on the blockchain, ensuring its immutability and security. The beneficiaries are then issued verifiable credentials, which they can use to submit their proof-of-life [5].

When a proof-of-life submission is made, the DCE app verifies the biometric data against the stored digital identity.

The verifiable credential is then checked for authenticity and validity. This process is facilitated using AI algorithms, which enhance the accuracy and reliability of the verification [6].

6.1 Enrolment Process

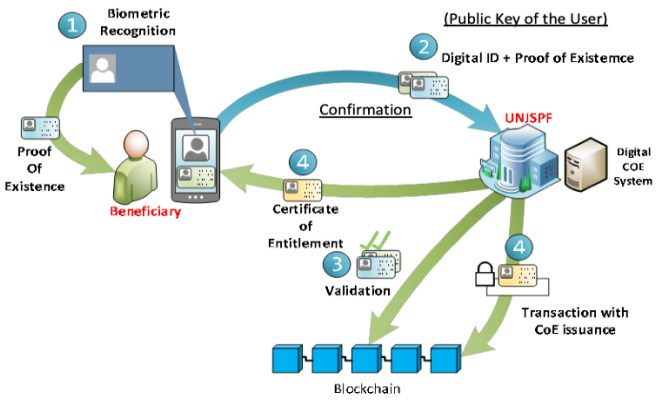


DID Creation

The Enrolment process involves several steps:

1. Identity verification/recording: Users undergo a verification process to confirm their identity.
2. Biometrics data capturing: Biometric data, such as facial recognition, is collected to enhance security and uniqueness.
3. Data acquisition: Relevant personal and identity information is gathered.
4. Digital ID creation: A unique digital ID is created and linked to the user's biometric data, stored exclusively on the hardware secure module of the user's device.

6.2 Issuance of Proof-of-Life Process



CE Issuance

The proof-of-life process is facilitated through:

1. Biometric Recognition: Users are authenticated using their biometric data.
2. Confirmation of Pairing Digital ID + Proof-of-Life: The system verifies that the digital ID is correctly paired with the proof-of-life confirmation.
3. Validation and Transaction Recording on Blockchain: The proof-of-life transaction is validated and recorded on the blockchain to ensure immutability and transparency.
4. Issuance of the Digital Certificate: Upon successful validation, a digital certificate is issued to confirm the user's proof-of-life status.
5. The payload of the "message" processed by the solution is extremely small. Furthermore, the frequency of the process is once per year (i.e., UNJSPF retirees need to confirm that they are still alive only once every 365 days). Therefore, the process does not lead to significant operational and financial overhead or scalability issues.

6.3 Decision Model for Blockchain

The decision to use blockchain technology for the DCE was based on its ability to provide a secure, transparent, and tamper-proof ledger for storing identity data. Blockchain's decentralised nature ensures that no single entity has control over the data, reducing the risk of unauthorised access and manipulation [9, 20]. Additionally, blockchain's transparency allows for easy auditing and verification of transactions, further enhancing trust in the system [19].

Studies have shown that blockchain is an effective solution for identity management, particularly in scenarios where security and trust are paramount. The use of blockchain in the DCE not only addresses these requirements but also provides a scalable and efficient solution for managing the identities of a large number of beneficiaries (i.e., 72,000 retirees, residing in more than 190 countries).

7. Deployment

The deployment of the DCE was a multi-year endeavour that involved meticulous planning, development, and deployment. This chapter outlines the deployment process, the challenges faced, and solutions developed, and the user experience with the DCE app.

7.1 Deployment Process

The deployment of the DCE began with a pilot project in 2021, involving 250 testers from over 40 countries [22].

This initial phase was crucial for identifying potential issues and gathering feedback to refine the solution. The pilot project demonstrated the feasibility of using facial recognition and blockchain technologies for proof-of-life verification, paving the way for a broader rollout.

Following the successful pilot, the DCE was gradually introduced to the wider population of UNJSPF beneficiaries. The deployment process involved several key steps:

1. User Enrolment: Beneficiaries were invited to enrol in the DCE by providing their biometric data through the app. This data was securely stored – exclusively in their devices – and used for subsequent verifications [21].

2. Training and Support: A dedicated support team provided training and assistance to beneficiaries, ensuring they were comfortable using the app. This included step-by-step guides, video tutorials, and a helpdesk for addressing any issues [23].

3. System Integration: The DCE was integrated with existing UNJSPF systems to ensure seamless data flow and interoperability. This involved collaboration with the United Nations International Computing Centre (UNICC) and other technical partners [19].

4. Security and Compliance: The solution underwent rigorous security assessments and compliance checks to ensure it met international standards for data protection and privacy [24].

7.2 Challenges and Solutions

The implementation of the DCE was not without its challenges. One of the primary obstacles was ensuring the accuracy and reliability of the biometric verification process. To address this, the team incorporated advanced AI algorithms for liveness detection, which helped prevent spoofing and ensured that the biometric data was captured from a live person [20, 22, 23, 24].

Another challenge was the digital divide, as some beneficiaries had limited access to smartphones or the Internet. To mitigate this, UNJSPF introduced a kiosk mode, allowing beneficiaries to submit their proof-of-life from designated kiosks at various UN duty stations. This ensured that all beneficiaries, regardless of their technological capabilities, could use the DCE.

The transition from a paper-based system to a digital solution also required significant change management efforts. The support team played a crucial role in this, providing continuous assistance and addressing any concerns raised by beneficiaries.

7.3 User Experience

The user experience with the DCE app has been overwhelmingly positive. Beneficiaries have praised the

convenience and ease of use of the app, which allows them to complete their annual proof-of-life from the comfort of their homes. The app's user-friendly interface and clear instructions have made the transition from paper-based forms to digital verification smooth and straightforward.

Screenshots of the DCE app show a clean and intuitive design, with clear prompts guiding users through the verification process. The app also includes features for troubleshooting common issues, such as poor lighting or incorrect positioning during biometric capture.

User ratings and feedback have highlighted the app's reliability and security, with many beneficiaries expressing confidence in the system's ability to protect their personal information. The DCE has not only streamlined the verification process but also enhanced the overall user experience, making it a model for other organisations looking to implement similar solutions.

In conclusion, the implementation of the UNJSPF Digital Identity Solution has been a complex but successful endeavour. Through careful planning, robust technology integration, and continuous user support, the DCE has transformed the proof-of-life verification process, providing a secure, efficient, and user-friendly solution for UNJSPF beneficiaries.

8. Validation and Certification

The DCE has undergone rigorous validation and certification processes to ensure its security, reliability, and compliance with international standards. This chapter explores the measures taken to validate and certify the solution, focusing on ISO/IEC 30107:2023 compliance and ISO/IEC 42001:2023 certification.

8.1 ISO/IEC 30107:2023 Testing

One of the critical components of the DCE is its AI module, which is embedded within the facial recognition and biometrics algorithm. This module is designed to detect and prevent potential "deep fakes" by employing advanced liveness detection techniques. To ensure the effectiveness and reliability of this AI module, UNJSPF sought validation and attestation in accordance with ISO/IEC 30107:2023 [12].

ISO/IEC 30107:2023 is an international standard that specifies requirements for biometric presentation attack detection (PAD). It provides guidelines for evaluating the performance of biometric systems in detecting and preventing presentation attacks, such as spoofing attempts. The AI module within the DCE was subjected to extensive testing to ensure it met the stringent requirements of this standard [13].

The validation process involved a series of tests to assess the AI module's ability to accurately detect liveness and differentiate between genuine biometric data and potential spoofing attempts. The results of these tests demonstrated that the AI module effectively prevents presentation attacks, providing a high level of security and reliability for the DCE [14].

8.2 ISO/IEC 42001:2023 Certification

In addition to validating the AI module, the UNJSPF also sought certification for its AI Management System in accordance with ISO/IEC 42001:2023 [15].

This standard specifies requirements for establishing, implementing, maintaining, and continually improving an AI Management System. It provides a framework for managing the risks associated with AI technologies and ensuring their ethical and responsible use.

The certification process involved a comprehensive assessment of the UNJSPF AI management practices, including the development, deployment, and monitoring of the AI module within the DCE. The assessment focused on several key areas, including data privacy, algorithmic transparency, and ethical considerations [16, 17, 18, 19].

External audits and independent assessments (i.e., cybersecurity, data privacy, and algorithmic audits) have further strengthened the trust and assurance in the DCE. These assessments have confirmed that the solution meets the highest standards of security, privacy, and reliability. The DCE has been featured in the Global Standard Mapping Initiative on Digital Identity by the Global Blockchain Business Council (GBBC), highlighting the due diligence process followed in its design, development, and implementation.

9. Results and Benefits

The introduction of the DCE has revolutionised the proof-of-life verification process for UNJSPF beneficiaries. Prior to the DCE, the verification process was manual, time-consuming, and prone to errors. Beneficiaries were required to submit paper-based Certificates of Entitlement (CE) via postal mail, which often led to delays and logistical challenges, especially for those residing in remote or conflict-affected areas [23].

With the DCE, beneficiaries can now complete their annual proof-of-life through a secure mobile app, using biometric data for verification. This digital approach has significantly streamlined the process, reducing the time and effort required for both beneficiaries and the UNJSPF administration. The use of facial recognition and blockchain technologies ensures that the verification is accurate, secure, and tamper-proof [22].

The DCE has also enhanced the efficiency of the verification process. Automated verification through the app has reduced the administrative burden on the UNJSPF, eliminated printing,

mailing, and archiving of paper-based forms, and allowed staff to focus on more complex tasks. Additionally, the digital ledger provided by blockchain technology offers a transparent and immutable record of all transactions, facilitating easy auditing and compliance [3].

The DCE has also contributed to significant efficiency gains for the UNJSPF. The automated verification process has reduced the administrative workload, allowing staff to focus on more strategic tasks. The transparent and immutable record provided by blockchain technology has facilitated easy auditing and compliance, further enhancing the trust and accountability of the verification process.

In conclusion, the UNJSPF Digital Identity Solution has transformed the proof-of-life verification process, delivering a secure, efficient, and user-friendly solution for pension beneficiaries. Through rigorous validation, certification, and continuous improvement, the DCE has set a new benchmark for digital identity solutions in the pension sector.

10. Evolution

The successful implementation of the UNJSPF DCE served as a pivotal catalyst for the United Nations Chief Executive Board (CEB) to launch the comprehensive "United Nations Digital Identity Solution." The DCE's innovative use of blockchain, biometrics, and global positioning technologies to verify the identity and existence of UNJSPF beneficiaries worldwide provided a model for broader UN digital transformation initiatives.

10.1 Leveraging Success for Broader UN Initiatives

The UNJSPF DCE's success in streamlining the proof-of-life process for UNJSPF beneficiaries demonstrated the potential of digital technologies to enhance efficiency, security, and user experience across the UN system. This achievement caught the attention of the High-Level Committee on Management (HLCM), which recognised the value of extending similar digital identity solutions to other UN organisations. The HLCM endorsement led to the development of the UN Digital ID, a system-wide identity solution aimed at providing a universal digital identity for UN staff from onboarding to retirement.

10.2 Alignment with UN Digital Transformation Goals

The UN Digital ID initiative aligns with the UN's broader digital transformation goals, including the Secretary-General's UN 2.0 vision, which emphasises leveraging technology to enhance organisational efficiency and effectiveness. By adopting a similar technological approach to the DCE, the UN Digital ID aims to reduce data fragmentation, enhance interoperability between UN agencies, and provide real-time verified data for decision-making. This initiative also supports the Sustainable Development Goals (SDGs) by promoting digital inclusion and reducing administrative costs.

10.3 Governance and Implementation

The governance structure for the UN Digital ID involves a collaborative approach, with an Executive Steering Committee overseeing the project's strategic direction and implementation. The phased implementation plan includes piloting the solution with select organisations before scaling it across the UN system, ensuring that lessons learned from the DCE are incorporated to enhance the overall effectiveness of the UN Digital ID. In summary, the UNJSPF DCE has not only modernised the proof-of-life process for its beneficiaries but has also inspired a broader digital transformation within the United Nations. By adopting similar technologies and approaches, the UN Digital ID initiative aims to create a unified digital identity framework that enhances efficiency, security, and collaboration across the UN system.

11. Conclusion

The implementation of the DCE has addressed several long-standing challenges associated with the proof-of-life verification process. By leveraging advanced technologies such as blockchain, AI, biometrics, and geo-localisation, the DCE has significantly enhanced the efficiency, security, and accuracy of the verification process.

The transition from a manual, paper-based system to a digital solution has streamlined the verification process, reducing the time and effort required for both beneficiaries and the UNJSPF administration. The use of facial recognition and blockchain technologies has ensured that the verification is accurate, secure, and tamper-proof, providing a high level of trust and assurance for all stakeholders.

The DCE has also demonstrated the importance of rigorous validation and certification processes. By adhering to international standards such as ISO/IEC 30107:2023 and ISO/IEC 42001:2023, the UNJSPF has ensured that the solution meets the highest standards of security, privacy, and ethical AI management. External audits and independent assessments have further strengthened the trust and reliability of the DCE.

The positive feedback from beneficiaries highlights the success of the DCE in enhancing the user experience. The app's user-friendly interface, combined with robust support and training, has made the transition to digital verification smooth and straightforward for beneficiaries.

Looking ahead, there are several potential enhancements and broader applications for the DCE. One area of focus is the continuous improvement of the AI algorithms used for biometric verification. Advances in AI and machine learning can further enhance the accuracy and reliability of the

verification process, ensuring that the DCE remains at the forefront of digital identity solutions.

Another potential enhancement is the expansion of the DCE to include additional verification methods, such as voice recognition or multi-modal biometrics. This would provide beneficiaries with more options for completing their proof-of-life, further enhancing the flexibility and accessibility of the solution.

A significant ongoing development is the introduction of a kiosk mode for the DCE. This feature is designed to support beneficiaries and retirees, particularly those in countries with connectivity issues or limited access to technology. The kiosk mode will allow beneficiaries to submit their proof-of-life from designated kiosks at various duty stations [23].

This initiative aims to bridge the digital divide and ensure that all beneficiaries, regardless of their technological capabilities, can use the DCE effectively.

The principles and technologies underpinning the DCE can also be applied to other areas within the UNJSPF and beyond. For example, the use of blockchain and verifiable credentials can be extended to other administrative processes, such as pension disbursements or identity verification for other services. The success of the DCE serves as a model for other organisations looking to implement similar digital identity solutions.

In conclusion, the UNJSPF Digital Identity Solution has set a new benchmark for proof-of-life verification in the pension sector. Through the innovative use of advanced technologies and a commitment to rigorous validation and certification, the DCE has transformed the verification process, providing a secure, efficient, and user-friendly solution for beneficiaries. The insights and experiences gained from this project will continue to guide future enhancements and applications, ensuring that the UNJSPF remains a leader in digital identity solutions [25].

Competing Interests:
N/A: The authors are permanent staff members of UNJSPF.

Ethical Approval:
Not applicable.

Author's Contribution:
The two authors contributed equally to the manuscript.

Funding:
None declared.

Acknowledgement:
Not applicable.

References:

[1] "A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity," *Business & Information Systems Engineering*, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s12599-023-00830-x.

[2] "Digital identity: An approach to its nature, concept, and functionalities," *International Journal of Law and Information Technology*, 2023. [Online]. Available: https://academic.oup.com/ijlit/article/32/1/eaae019/7760180.

[3] "Investigating identity management and authentication solutions using blockchain," *SSRN Electronic Journal*, 2023. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4922025.

[4] "Blockchain-based biometric identity management," *Cluster Computing*, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s10586-023-04180-x.

[5] "A blockchain-based biometric protection and authentication mechanism," in *Advances in Intelligent Systems and Computing*, Springer, Singapore, 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-99-2680-0_25.

[6] "Combining blockchain and biometrics: A survey on technical aspects and applications," *arXiv*, 2023. [Online]. Available: https://arxiv.org/html/2302.10883v2.

[7] "Microservices architecture: Aligning principles, practices, and culture," *Apress*, 2023. [Online]. Available: https://link.springer.com/book/10.1007/978-1-4842-6538-7.

[8] *Secure Multi-Party Computation*. Springer, 2023. [Online]. Available: https://link.springer.com/book/10.1007/978-3-030-66665-1.

[9] *Blockchain Technology: Principles and Applications*. Springer, 2023. [Online]. Available: https://link.springer.com/book/10.1007/978-3-030-66665-1.

[10] *AI and Deep Learning for Biometrics*. Springer, 2023. [Online]. Available: https://link.springer.com/book/10.1007/978-3-030-66665-1.

[11] *Geo-localization Technologies and Applications*. Springer, 2023. [Online]. Available: https://link.springer.com/book/10.1007/978-3-030-66665-1.

[12] *ISO/IEC 30107-3:2023 - Information Technology — Biometric Presentation Attack Detection — Part 3: Testing and Reporting*. ISO, 2023. [Online]. Available: https://www.iso.org/standard/67381.html.

[13] "Biometric presentation attack detection: A review," *International Journal of Information Security*, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s10207-023-00512-4.

[14] "Liveness detection in biometrics: An overview," in *Advances in Intelligent Systems and Computing*, Springer, Singapore, 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-66665-1_5.

[15] *ISO/IEC 42001:2023 - Artificial Intelligence — Management System*. ISO, 2023. [Online]. Available: https://www.iso.org/standard/81228.html.

[16] *AI Governance and Risk Management: A Framework*. AI & Society, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s00146-023-01345-6.

[17] *Ethical AI: Principles and Practices*. Springer, 2023. [Online]. Available: https://link.springer.com/book/10.1007/978-3-030-66665-1.

[18] "External audits and independent assessments in AI," *International Journal of Information Security*, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s10207-023-00512-4.

[19] *Global Blockchain Business Council features the UNJSPF Digital Identity* Solution. UNJSPF, 2023. [Online]. Available: https://www.unjspf.org/newsroom/global-blockchain-business-council-features-the-unjspf-digital-identity-solution/.

[20] *Blockchain Central at UNGA: closing "The Digital Divide" for UNJSPF* Retirees *and Beneficiaries*. UNJSPF, 2023. [Online]. Available: https://www.unjspf.org/newsroom/blockchain-central-at-unga-closing-the-digital-divide-for-unjspf-retirees-and-beneficiaries/.

[21] *Digital Certificate of Entitlement (DCE) - UNJSPF*. UNJSPF, 2023. [Online]. Available: https://www.unjspf.org/for-clients/digital-certificate-of-entitlement/.

[22] *Facial Recognition and Blockchain to Replace Gradually Paper - UNJSPF*. UNJSPF, 2023. [Online]. Available: https://www.unjspf.org/newsroom/facial-recognition-and-blockchain-to-replace-paper-un-pension-fund-enters-digital-age/.

[23] "An innovative option to secure pension benefits - UN Today," *UN Today*, 2023. [Online]. Available: https://untoday.org/an-innovative-option-to-secure-pension-benefits/.

[24] *UNJSPF Showcases its Digital Identity Solution at WSIS High-level Meeting*. UNJSPF, 2023. [Online]. Available: https://www.unjspf.org/newsroom/unjspf-showcases-its-digital-identity-solution-at-wsis-high-level-meeting/.

[25] *UNJSPF Leads the Way on Emerging Technologies*. UNJSPF, 2023. [Online]. Available: https://www.unjspf.org/newsroom/unjspf-leads-the-way-on-emerging-technologies/.

[26] *Revocation Mechanism for the UNJSPF Digital Identity Solution*. [Online]. Available: https://github.com/decentralized-identity/aries-rfcs/tree/main/features/0183-revocation-notification.

