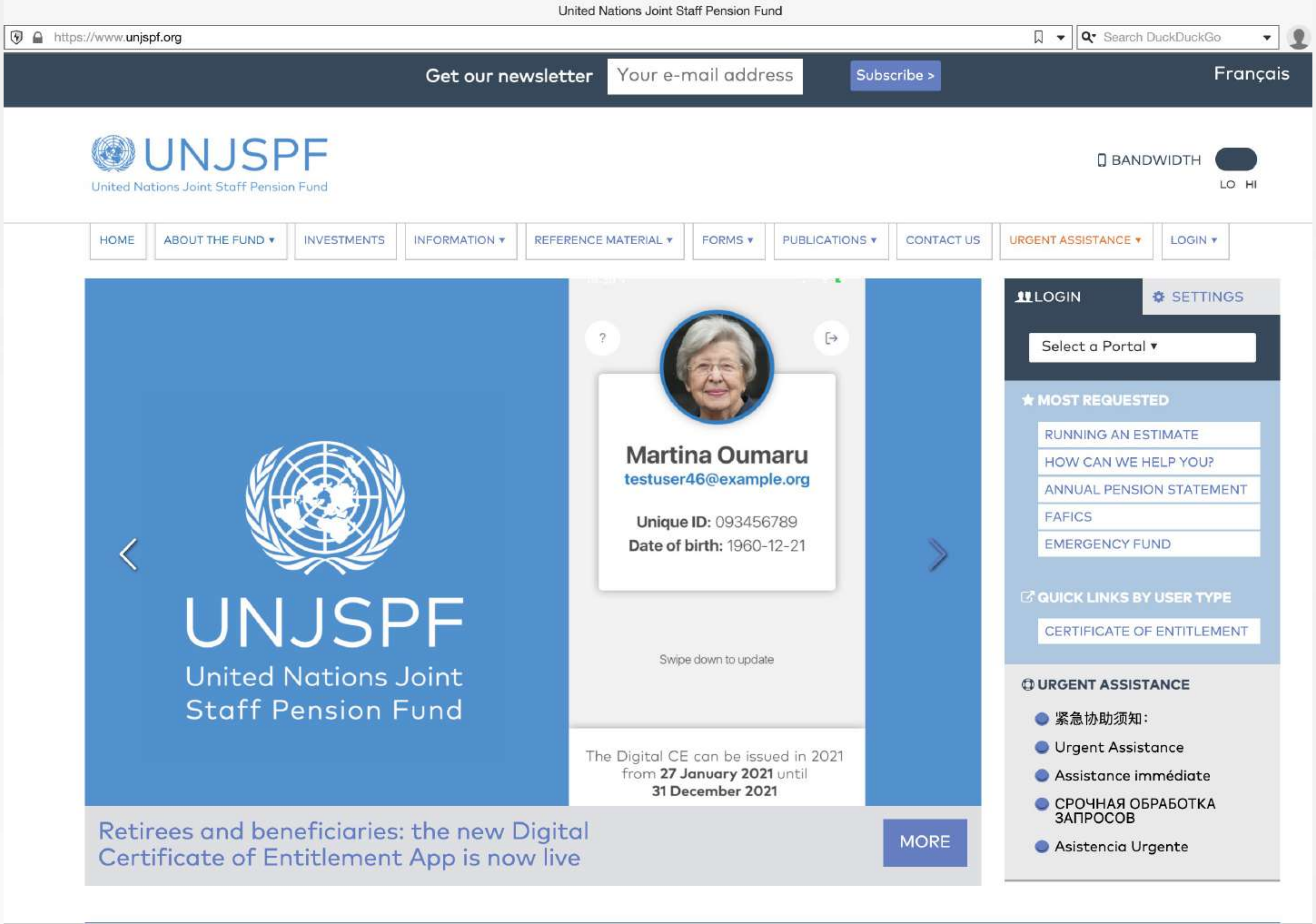
# UNJSPF

United Nations Joint
Staff Pension Fund

Dino Cataldo DELL'ACCIO
Chief Information Officer

# Presentation of the UNJSPF “Digital Certificate of Entitlement Solution”



United Nations Joint Staff Pension Fund

https://www.unjspf.org

Get our newsletter | Your e-mail address | Subscribe > | Français

UNJSPF
United Nations Joint Staff Pension Fund

BANDWIDTH LO HI

HOME | ABOUT THE FUND ▾ | INVESTMENTS | INFORMATION ▾ | REFERENCE MATERIAL ▾ | FORMS ▾ | PUBLICATIONS ▾ | CONTACT US | URGENT ASSISTANCE ▾ | LOGIN ▾

UNJSPF
United Nations Joint Staff Pension Fund

**Martina Oumaru**
testuser46@example.org

**Unique ID:** 093456789
**Date of birth:** 1960-12-21

Swipe down to update

The Digital CE can be issued in 2021 from **27 January 2021** until **31 December 2021**

Retirees and beneficiaries: the new Digital Certificate of Entitlement App is now live

MORE

LOGIN | SETTINGS

Select a Portal ▾

MOST REQUESTED
- RUNNING AN ESTIMATE
- HOW CAN WE HELP YOU?
- ANNUAL PENSION STATEMENT
- FAFICS
- EMERGENCY FUND

QUICK LINKS BY USER TYPE
- CERTIFICATE OF ENTITLEMENT

URGENT ASSISTANCE
- 紧急协助须知：
- Urgent Assistance
- Assistance immédiate
- СРОЧНАЯ ОБРАБОТКА ЗАПРОСОВ
- Asistencia Urgente

# AGENDA

I. Introduction and Background: UNJSPF – UNICC

II. The Business Problem: Challenges and Proofs

III. The Strategic Approach

IV. The Design Approach: Blockchain; Biometrics; Geo-location

V. Gartner Case Study and Industry Recognition

VI. Short Demo Video

I. Referenced Standards and Industry Best Practices

II. Proof of Concept & Pilot Test

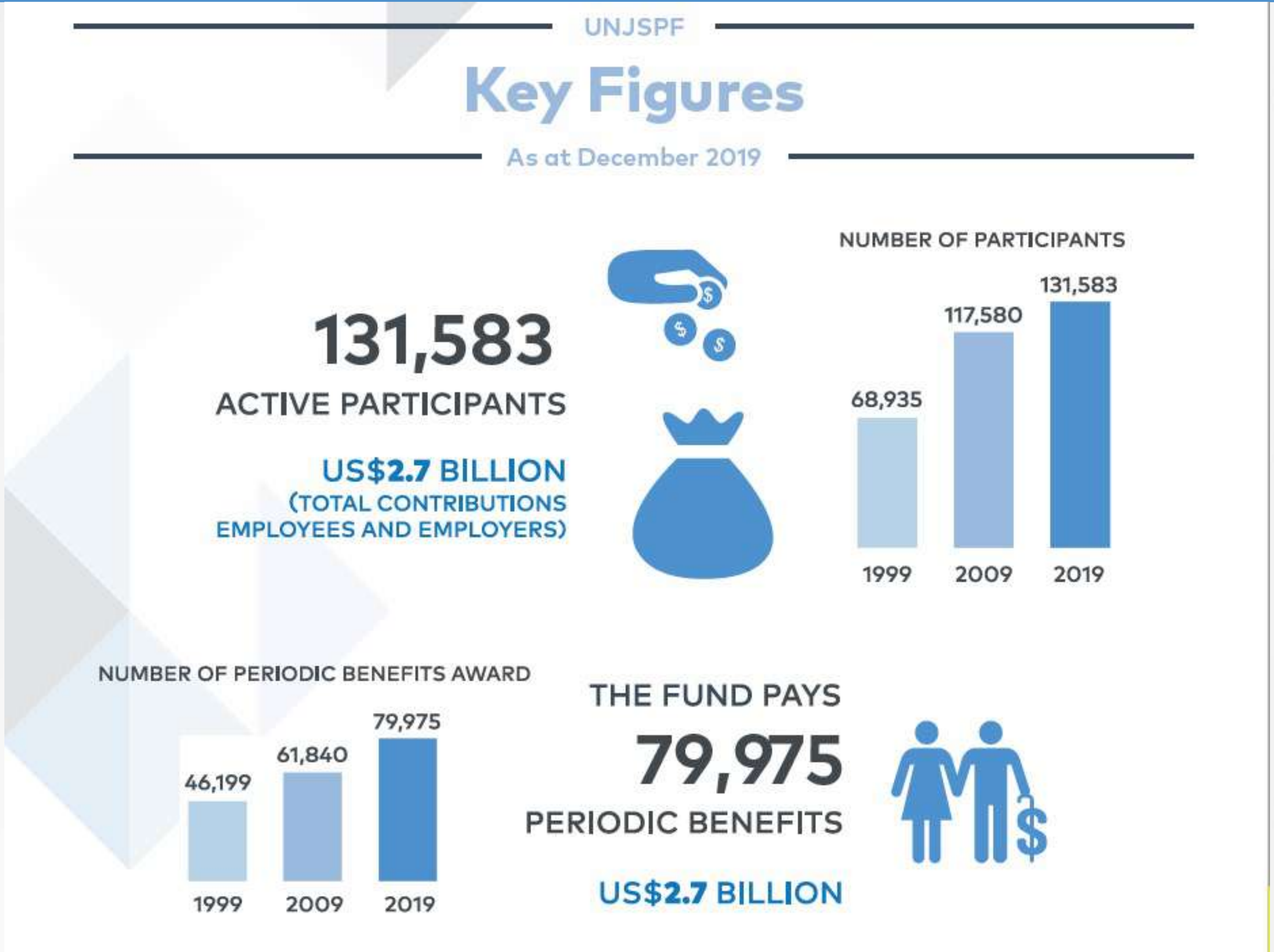
III. Overview of the Step-by-Step Process

IV. Cybersecurity & Privacy Assurance

V. Key Elements of the Underlying Technologies and

VI. Walkthrough

# Introduction to UNJSPF



UNJSPF

## Key Figures

As at December 2019

**131,583**

ACTIVE PARTICIPANTS

**US$2.7 BILLION**
(TOTAL CONTRIBUTIONS
EMPLOYEES AND EMPLOYERS)

NUMBER OF PARTICIPANTS

| 1999 | 2009 | 2019 |
|---|---|---|
| 68,935 | 117,580 | 131,583 |

NUMBER OF PERIODIC BENEFITS AWARD

| 1999 | 2009 | 2019 |
|---|---|---|
| 46,199 | 61,840 | 79,975 |

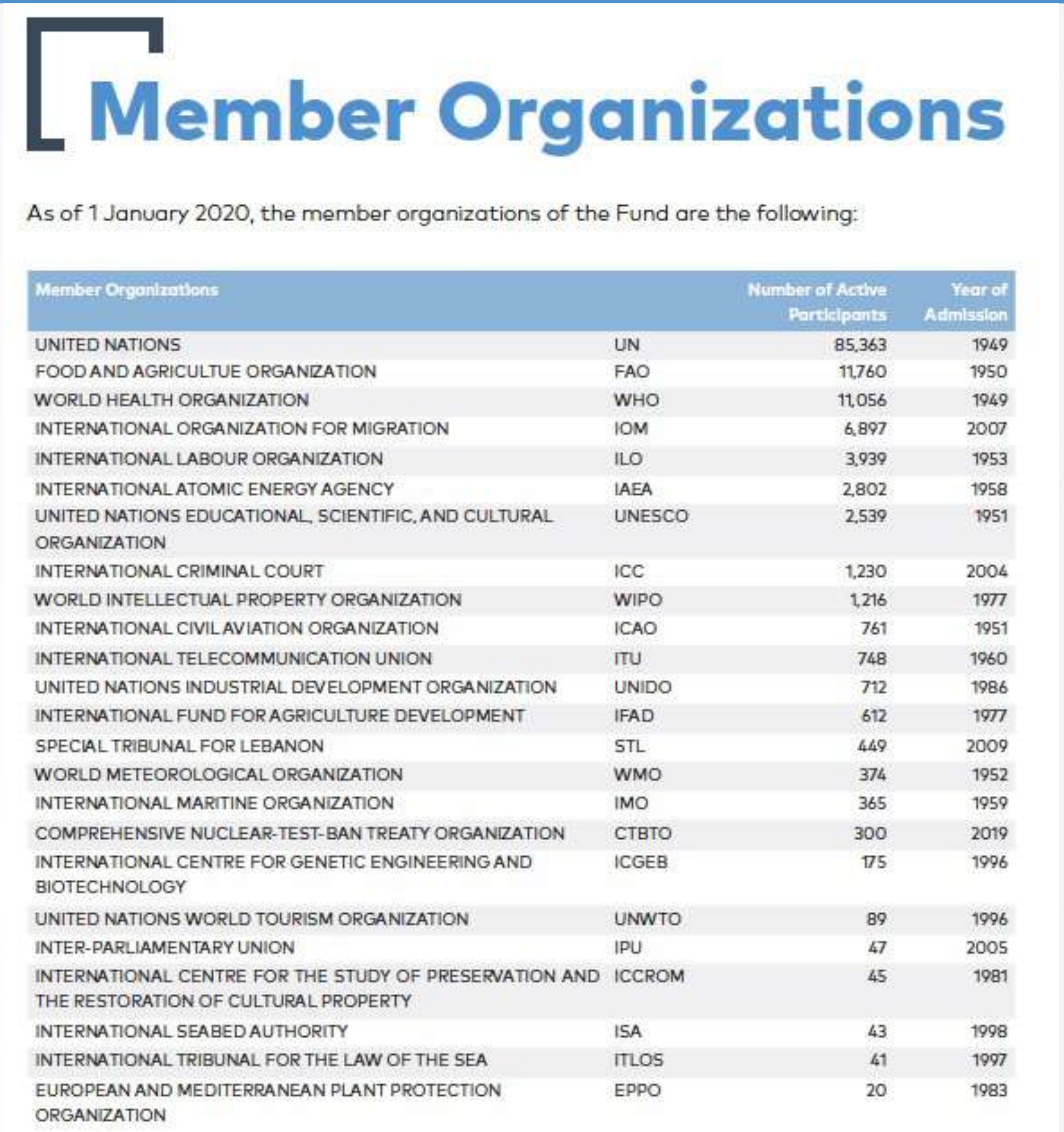
THE FUND PAYS

**79,975**

PERIODIC BENEFITS

**US$2.7 BILLION**

# United Nations Joint Staff Pension Fund



## Member Organizations

As of 1 January 2020, the member organizations of the Fund are the following:

| Member Organizations | | Number of Active Participants | Year of Admission |
|---|---|---|---|
| UNITED NATIONS | UN | 85,363 | 1949 |
| FOOD AND AGRICULTUE ORGANIZATION | FAO | 11,760 | 1950 |
| WORLD HEALTH ORGANIZATION | WHO | 11,056 | 1949 |
| INTERNATIONAL ORGANIZATION FOR MIGRATION | IOM | 6,897 | 2007 |
| INTERNATIONAL LABOUR ORGANIZATION | ILO | 3,939 | 1953 |
| INTERNATIONAL ATOMIC ENERGY AGENCY | IAEA | 2,802 | 1958 |
| UNITED NATIONS EDUCATIONAL, SCIENTIFIC, AND CULTURAL ORGANIZATION | UNESCO | 2,539 | 1951 |
| INTERNATIONAL CRIMINAL COURT | ICC | 1,230 | 2004 |
| WORLD INTELLECTUAL PROPERTY ORGANIZATION | WIPO | 1,216 | 1977 |
| INTERNATIONAL CIVIL AVIATION ORGANIZATION | ICAO | 761 | 1951 |
| INTERNATIONAL TELECOMMUNICATION UNION | ITU | 748 | 1960 |
| UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION | UNIDO | 712 | 1986 |
| INTERNATIONAL FUND FOR AGRICULTURE DEVELOPMENT | IFAD | 612 | 1977 |
| SPECIAL TRIBUNAL FOR LEBANON | STL | 449 | 2009 |
| WORLD METEOROLOGICAL ORGANIZATION | WMO | 374 | 1952 |
| INTERNATIONAL MARITINE ORGANIZATION | IMO | 365 | 1959 |
| COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION | CTBTO | 300 | 2019 |
| INTERNATIONAL CENTRE FOR GENETIC ENGINEERING AND BIOTECHNOLOGY | ICGEB | 175 | 1996 |
| UNITED NATIONS WORLD TOURISM ORGANIZATION | UNWTO | 89 | 1996 |
| INTER-PARLIAMENTARY UNION | IPU | 47 | 2005 |
| INTERNATIONAL CENTRE FOR THE STUDY OF PRESERVATION AND THE RESTORATION OF CULTURAL PROPERTY | ICCROM | 45 | 1981 |
| INTERNATIONAL SEABED AUTHORITY | ISA | 43 | 1998 |
| INTERNATIONAL TRIBUNAL FOR THE LAW OF THE SEA | ITLOS | 41 | 1997 |
| EUROPEAN AND MEDITERRANEAN PLANT PROTECTION ORGANIZATION | EPPO | 20 | 1983 |

# United Nations Joint Staff Pension Fund

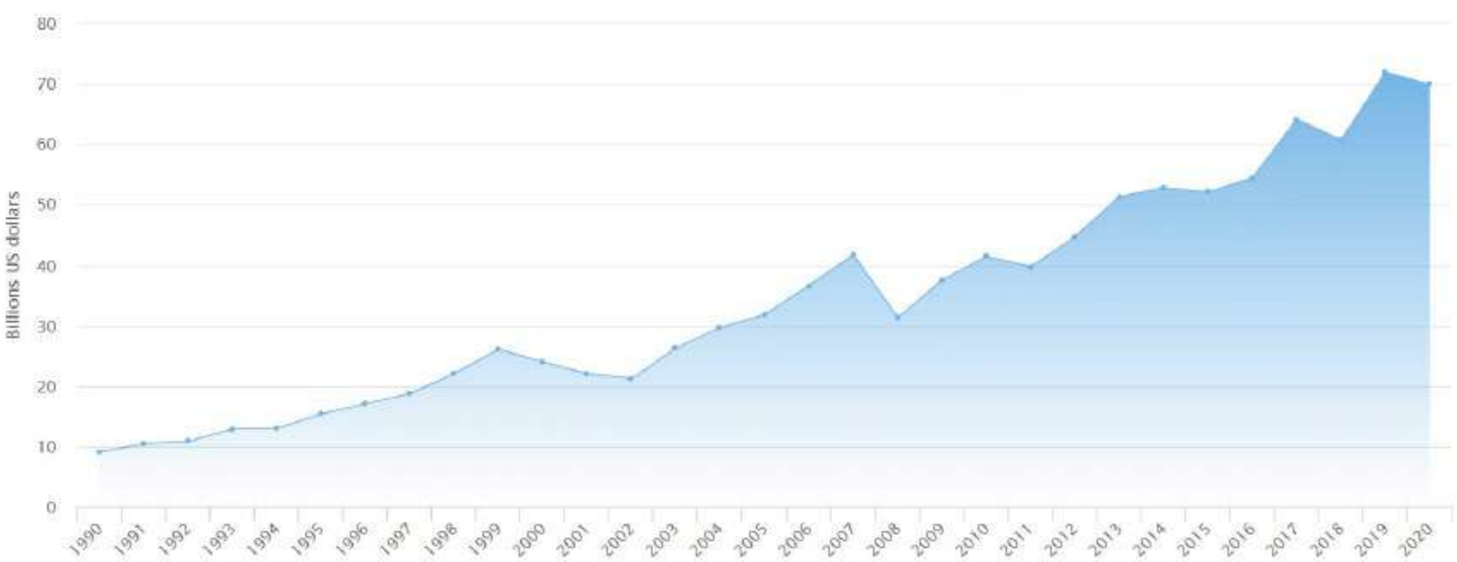
UNJSPF

## Market Value of Assets

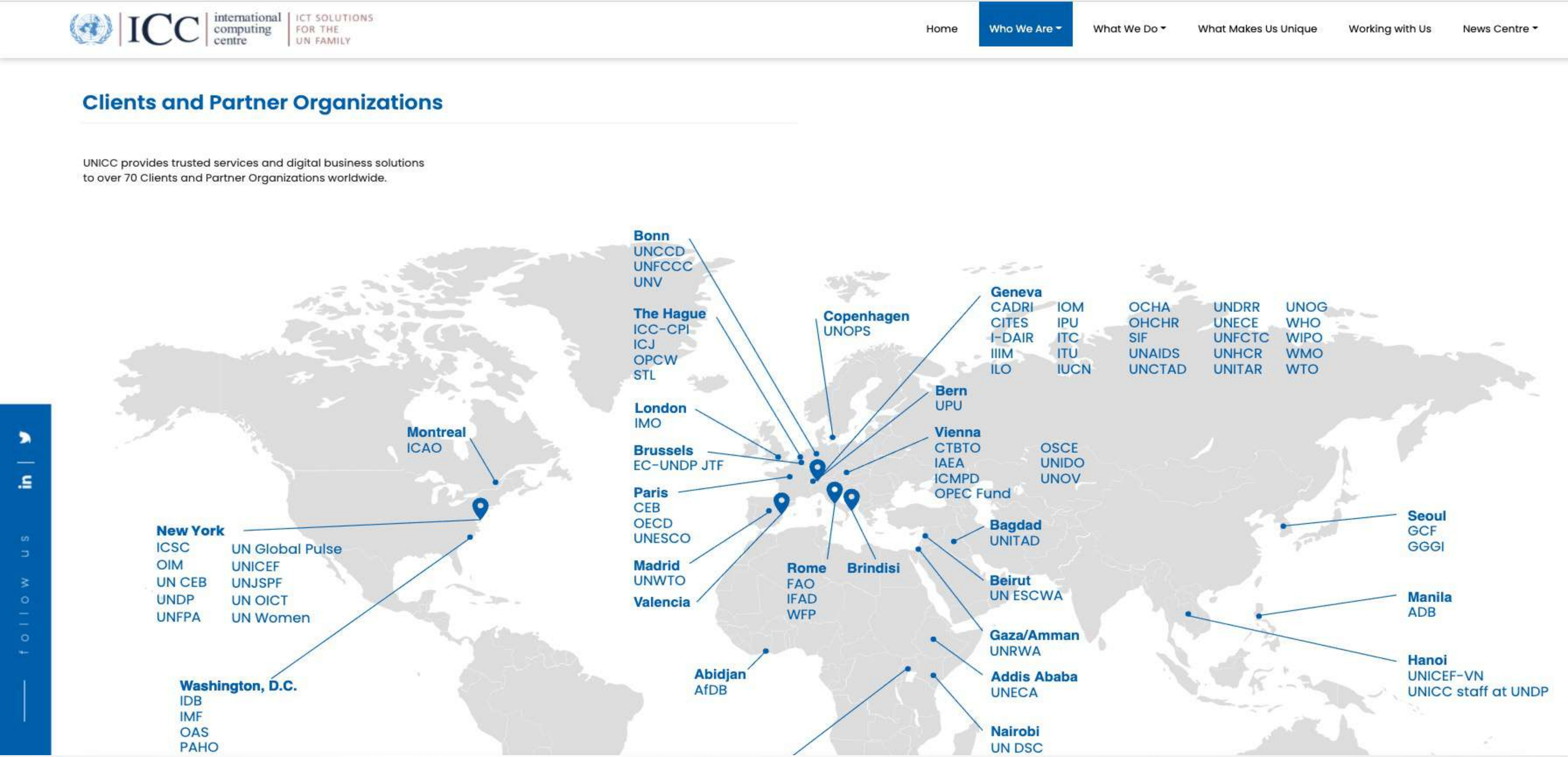
As at 4 September 2020

**US$74.35 billion**

(Billions of USD)



# United Nations International Computing Centre



## Clients and Partner Organizations

UNICC provides trusted services and digital business solutions to over 70 Clients and Partner Organizations worldwide.

**Montreal**
ICAO

**New York**
ICSC
OIM
UN CEB
UNDP
UNFPA
UN Global Pulse
UNICEF
UNJSPF
UN OICT
UN Women

**Washington, D.C.**
IDB
IMF
OAS
PAHO

**Bonn**
UNCCD
UNFCCC
UNV

**The Hague**
ICC-CPI
ICJ
OPCW
STL

**London**
IMO

**Brussels**
EC-UNDP JTF

**Paris**
CEB
OECD
UNESCO

**Madrid**
UNWTO

**Valencia**

**Abidjan**
AfDB

**Copenhagen**
UNOPS

**Rome**
FAO
IFAD
WFP

**Brindisi**

**Geneva**
CADRI
CITES
I-DAIR
IIIM
ILO
IOM
IPU
ITC
ITU
IUCN
OCHA
OHCHR
SIF
UNAIDS
UNCTAD
UNDRR
UNECE
UNFCTC
UNHCR
UNITAR
UNOG
WHO
WIPO
WMO
WTO

**Bern**
UPU

**Vienna**
CTBTO
IAEA
ICMPD
OPEC Fund
OSCE
UNIDO
UNOV

**Bagdad**
UNITAD

**Beirut**
UN ESCWA

**Gaza/Amman**
UNRWA

**Addis Ababa**
UNECA

**Nairobi**
UN DSC

**Seoul**
GCF
GGGI

**Manila**
ADB

**Hanoi**
UNICEF-VN
UNICC staff at UNDP

# Background of the Certificate of Entitlement Process

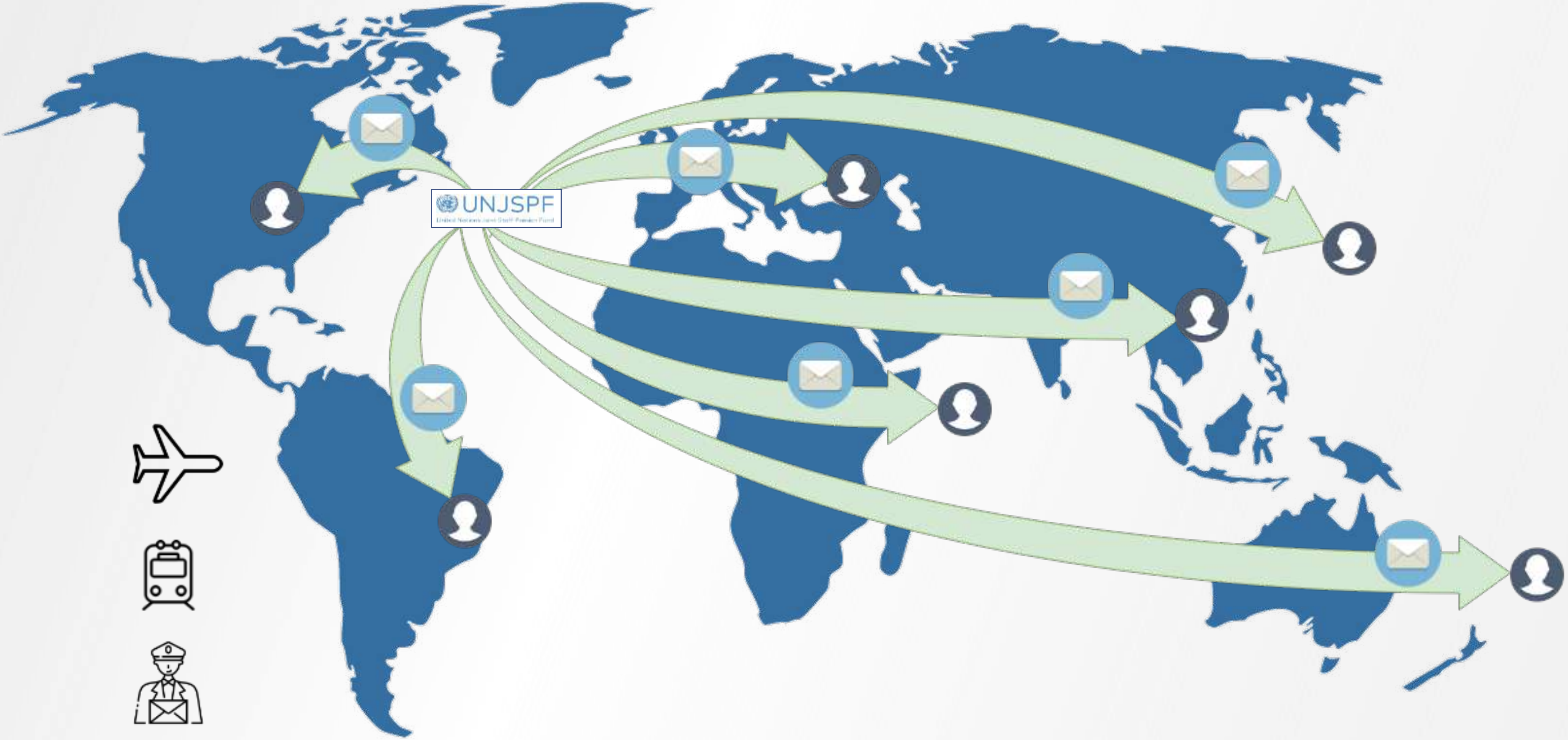
1. Every year, UNJSPF must ensure the reliable and consistent processing of benefit payments

2. This requires an annual verification of over 70 thousand beneficiaries located in more than 190 countries

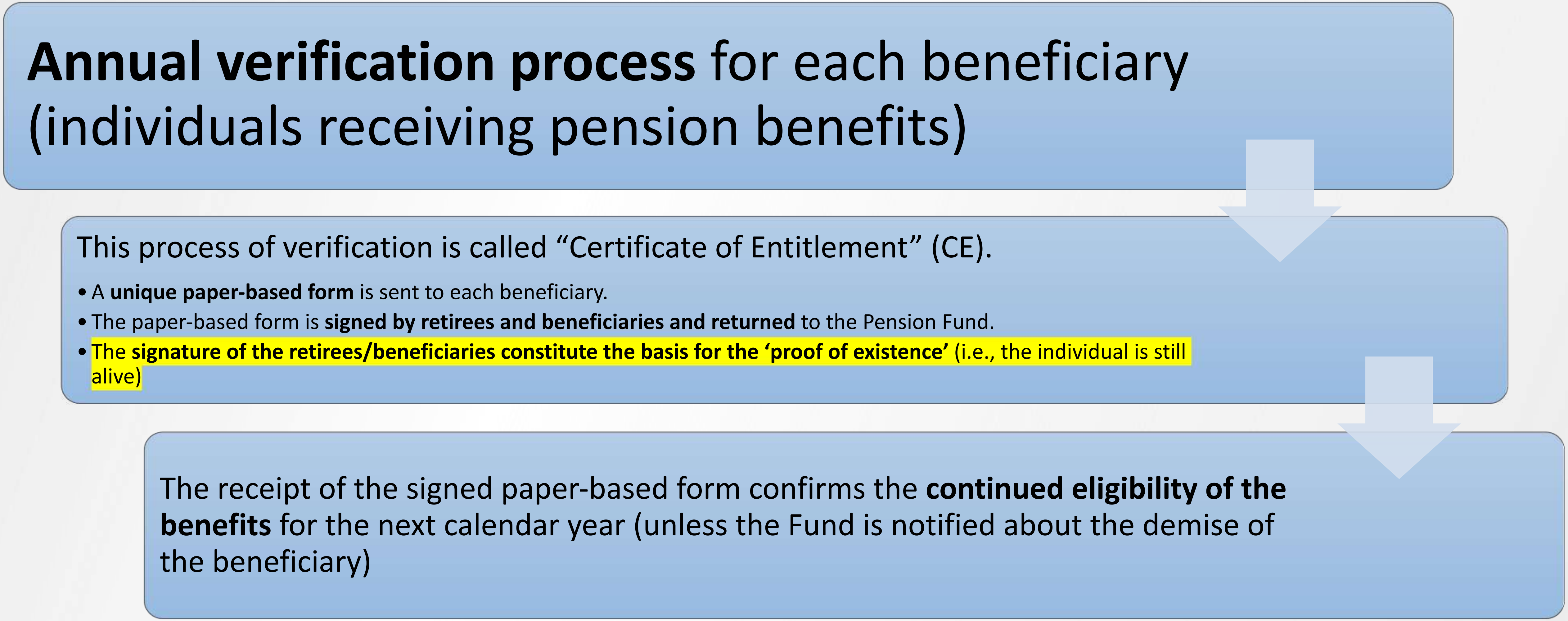
3. To confirm that each beneficiary is still alive

4. For the last 70 years, this confirmation has been conducted through a manual process, using a paper-based form (i.e., Certificate of Entitlement - CE).

# Paper-Based Certificate of Entitlement: AS-IS Process



# Paper-Based Certificate of Entitlement: Overview of the AS-IS process



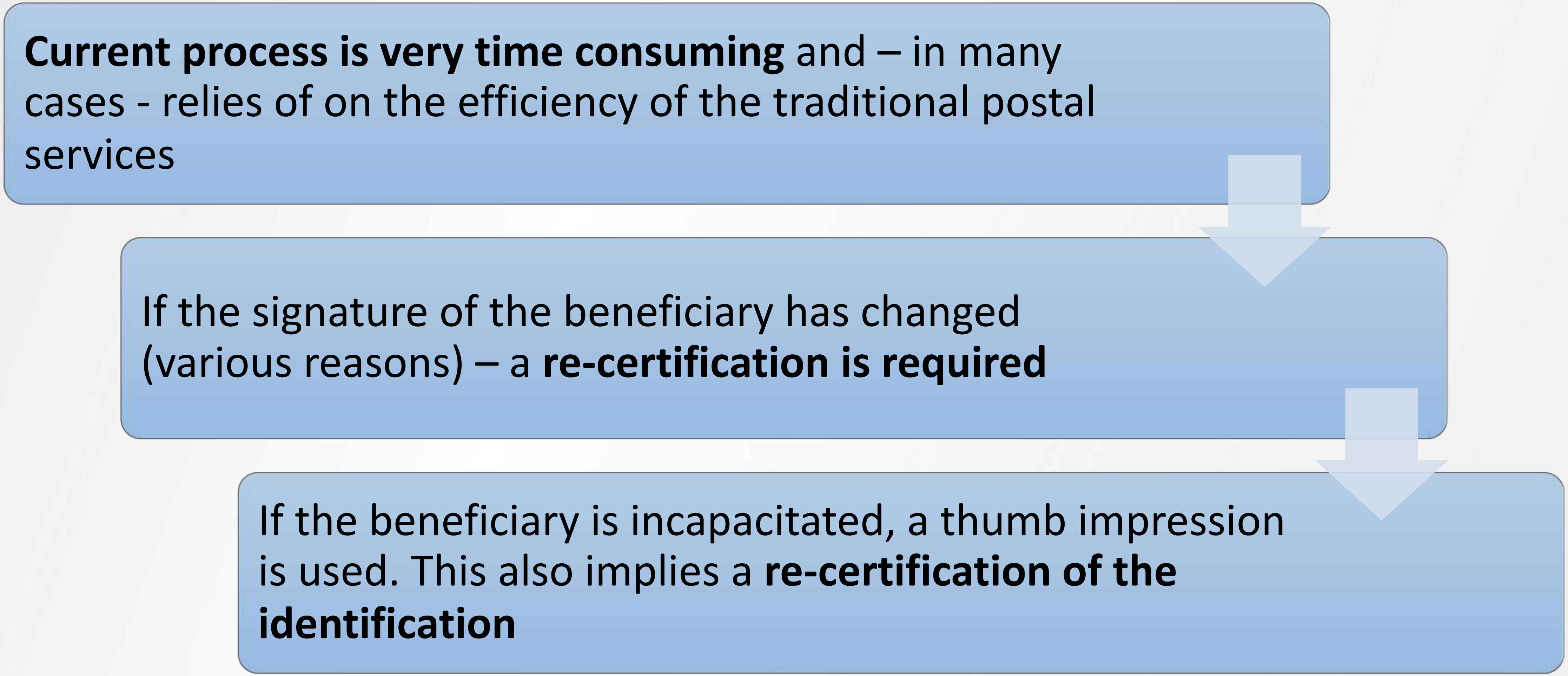
**Annual verification process** for each beneficiary (individuals receiving pension benefits)

This process of verification is called “Certificate of Entitlement” (CE).

- A **unique paper-based form** is sent to each beneficiary.
- The paper-based form is **signed by retirees and beneficiaries and returned** to the Pension Fund.
- The **signature of the retirees/beneficiaries constitute the basis for the ‘proof of existence’** (i.e., the individual is still alive)

The receipt of the signed paper-based form confirms the **continued eligibility of the benefits** for the next calendar year (unless the Fund is notified about the demise of the beneficiary)

# Paper-Based Certificate of Entitlement: Limitations of the AS-IS Process



**Current process is very time consuming** and – in many cases - relies of on the efficiency of the traditional postal services

If the signature of the beneficiary has changed (various reasons) – a **re-certification is required**

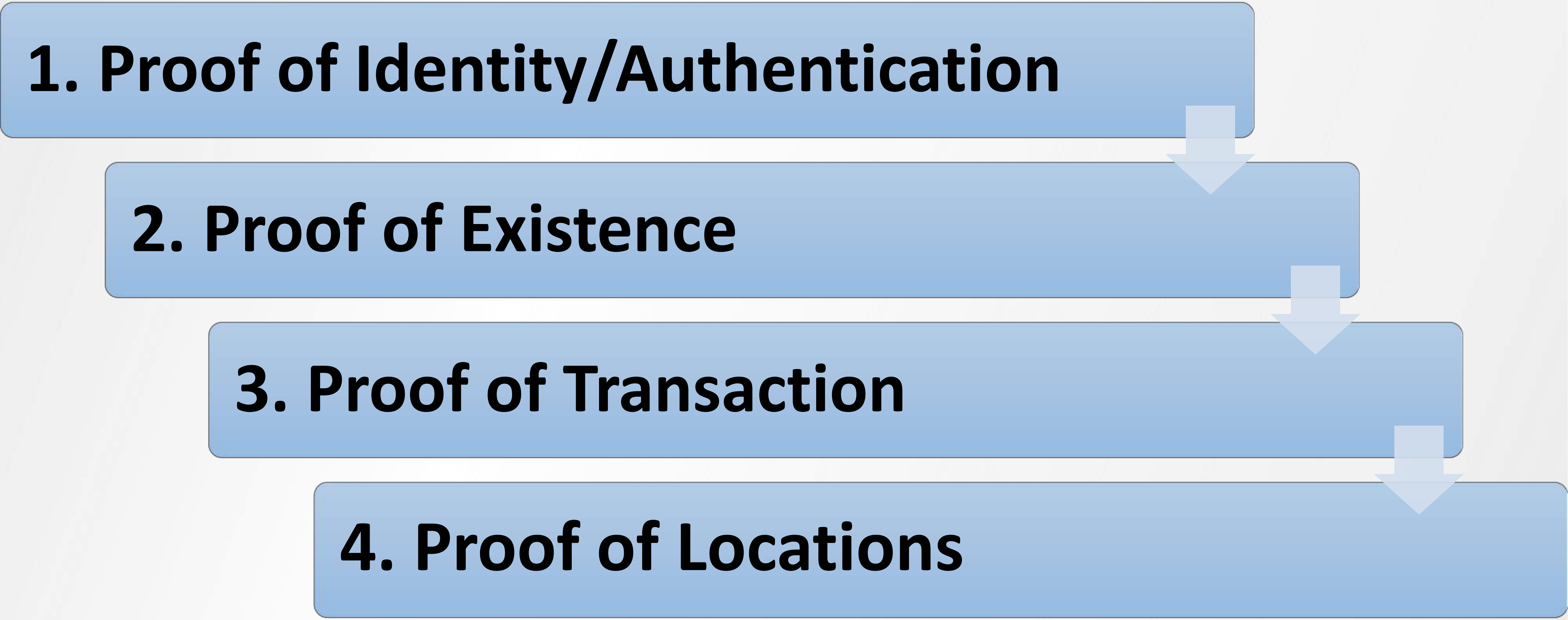
If the beneficiary is incapacitated, a thumb impression is used. This also implies a **re-certification of the identification**

# The Challenge(s)

UNJSPF
GENEVA OFFICE
CERTIFICATE OF ENTITLEMENT 2019
UNJSPF
CTBTO EPPO FAO IAEA ICGEB ICCROM ICAO ICC IFAD ILO IMO IOM IPU ISA ITU ITLOS STL UNESCO UNIDO UN UNWTO WHO WIPO WMO
No photocopy will be provided

- Transform a 70-year-old manual process
- Involving more than 70 thousand UN retirees & beneficiaries
- Residing in more than 190 countries
- Using paper-based forms
- Transmitted through 190 postal services
- Prone to delays + errors + questioning (negative proof)
- Causing – in same cases – suspension of payments

# The Challenge(s): Address & Provide 4 Proofs



1. Proof of Identity/Authentication

2. Proof of Existence

3. Proof of Transaction

4. Proof of Locations

# Digital Certificate of Entitlement: TO-BE/New Process

UNJSPF
United Nations Joint Staff Pension Fund
GPS

# A Digital Transformation Initiative

UNJSPF
GENEVA OFFICE
CERTIFICATE OF ENTITLEMENT 2019
CTBTO EPPO FAO IAEA ICGEB ICCROM ICAO ICC IFAD ILO IMO IOM IPU ISA ITU ITLOS STL UNESCO UNIDO UN UNWTO WHO WIPO WMO
UNJSPF
No photocopy will be provided

Transform

**From:** A manual ‘snail-mail’ Certificate of Entitlement Process

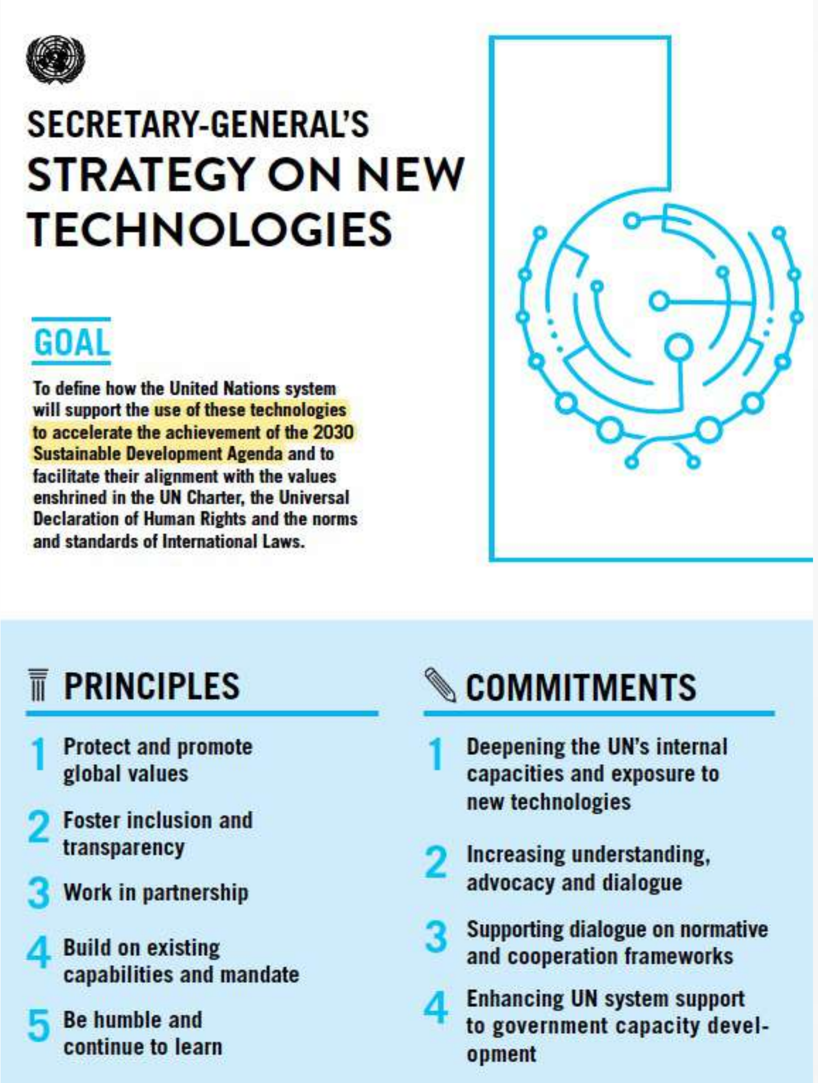
**To:** A Biometric-based solution using Mobile App and Blockchain

# A Digital Transformation Initiative Aligned with the SG Strategy on Innovation Technologies & Sustainable Development Goals

— UN SECRETARY-GENERAL'S —

STRATEGY ON NEW TECHNOLOGIES

SEPTEMBER 2018



SECRETARY-GENERAL'S

STRATEGY ON NEW TECHNOLOGIES

GOAL

To define how the United Nations system will support the use of these technologies to accelerate the achievement of the 2030 Sustainable Development Agenda and to facilitate their alignment with the values enshrined in the UN Charter, the Universal Declaration of Human Rights and the norms and standards of International Laws.

PRINCIPLES

1 Protect and promote global values

2 Foster inclusion and transparency

3 Work in partnership

4 Build on existing capabilities and mandate

5 Be humble and continue to learn

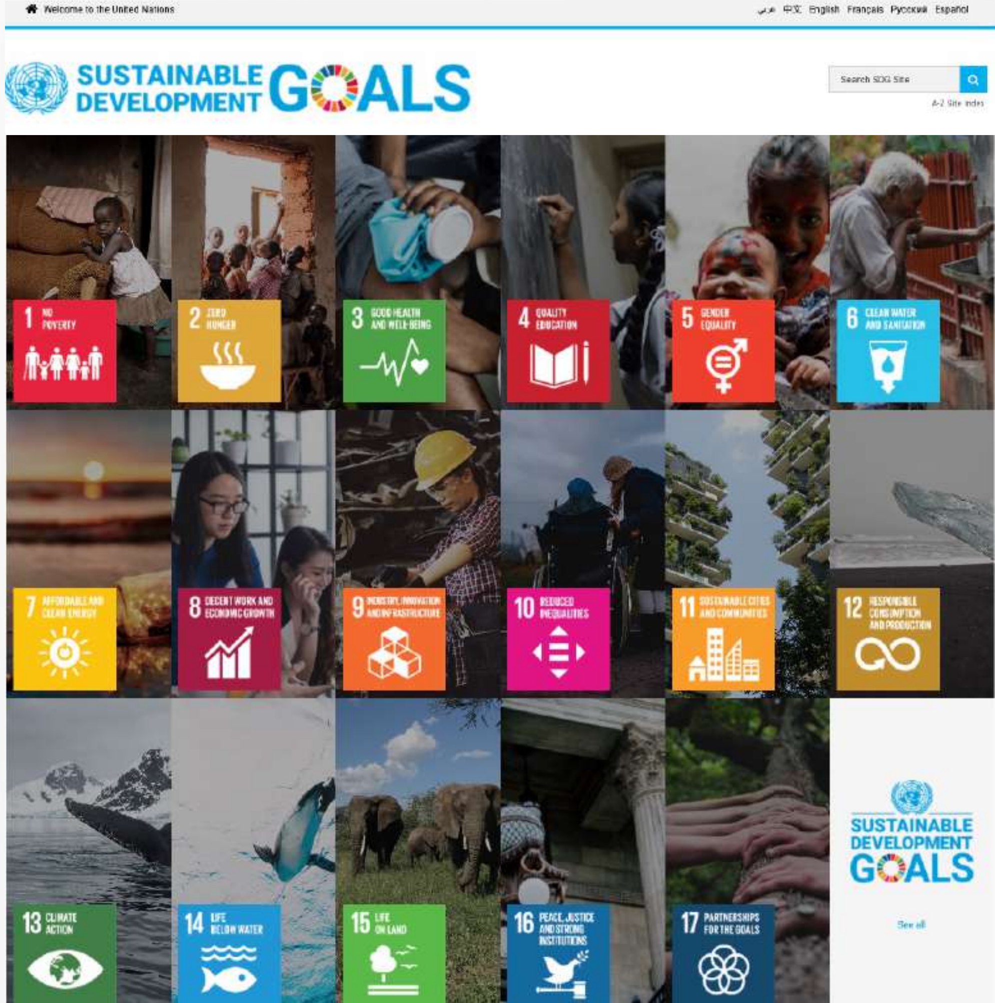
COMMITMENTS

1 Deepening the UN's internal capacities and exposure to new technologies

2 Increasing understanding, advocacy and dialogue

3 Supporting dialogue on normative and cooperation frameworks

4 Enhancing UN system support to government capacity development



Welcome to the United Nations

عربي 中文 English Français Русский Español

SUSTAINABLE DEVELOPMENT GOALS

Search SDG Site

A-Z Site index

1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
SUSTAINABLE DEVELOPMENT GOALS
See all

# A Digital Transformation Initiative - Details

## TRADITIONAL PAPER-BASED PROCESS

### PAPER-BASED PROCESS

The Certificate of Entitlement process is managed with a form transmitted and received through the regular postal mail service

UNJSPF
GENEVA OFFICE
CERTIFICATE OF ENTITLEMENT 2019
UNJSPF
No photocopy will be provided
UNJSPF

## DIGITAL CERTIFICATE OF ENTITLEMENT

### NEW TECHNOLOGIES

Used of innovative technologies, based on:

Smart Phone +

Mobile App +

Biometric Solution +

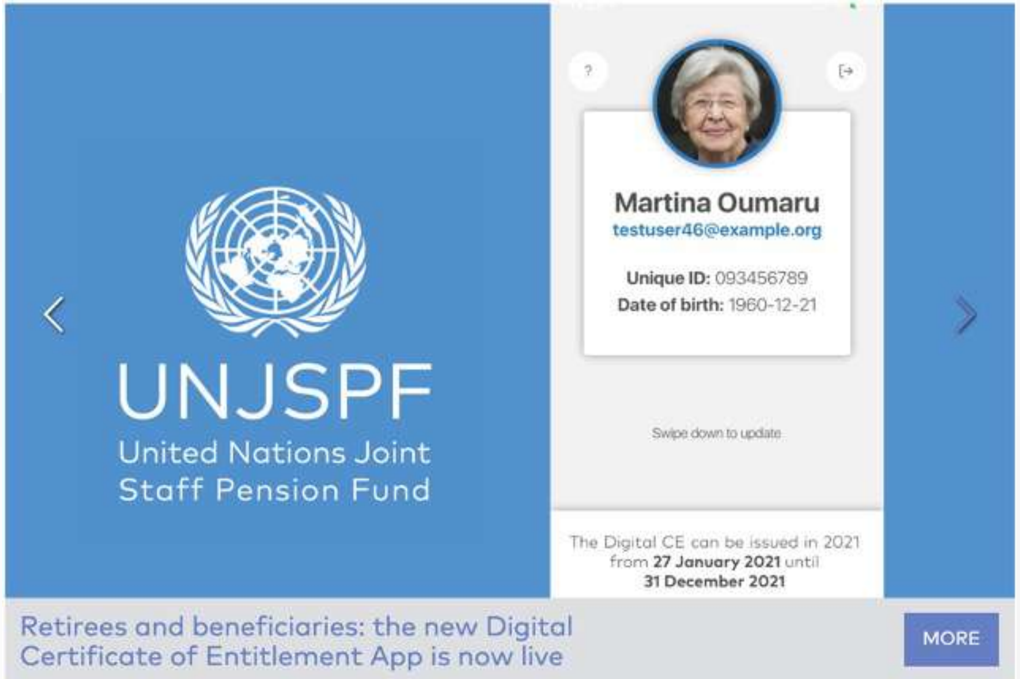
Blockchain

To Provide & Confirm:

- Ease-of-use
- Security
- Trust
- Auditability

# A Digital Transformation Initiative: UNJSPF Digital CE gives input to the UN Digital ID

**The history of computerization at the UN started in 1965** when the Secretariat received its first mainframe computer: An IBM 7044/1401 mainframe computer system.



UNJSPF

United Nations Joint Staff Pension Fund

Martina Oumaru

testuser46@example.org

**Unique ID:** 093456789

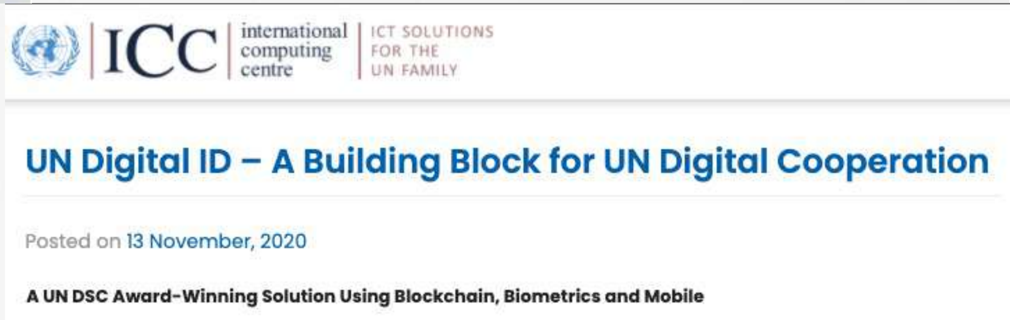
**Date of birth:** 1960-12-21

Swipe down to update

The Digital CE can be issued in 2021 from **27 January 2021** until **31 December 2021**

Retirees and beneficiaries: the new Digital Certificate of Entitlement App is now live

**January 2021: UNJSPF goes live with the Digital CE Solution** and contributes to the the UN wider project for the development of a UN Digital ID



ICC | international computing centre | ICT SOLUTIONS FOR THE UN FAMILY

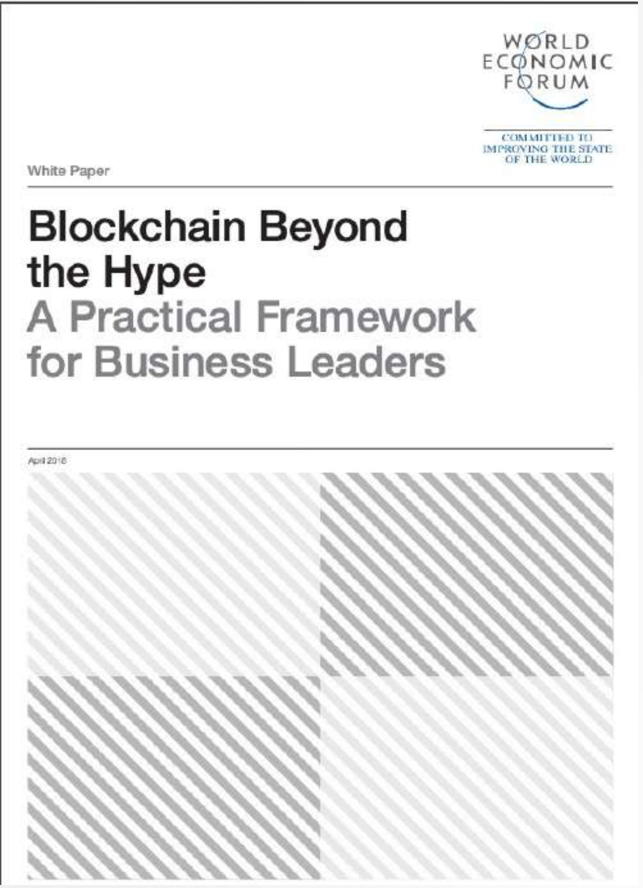
## UN Digital ID – A Building Block for UN Digital Cooperation

Posted on 13 November, 2020

**A UN DSC Award-Winning Solution Using Blockchain, Biometrics and Mobile**

# Blockchain: Example of a Decision Tree

(http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf)



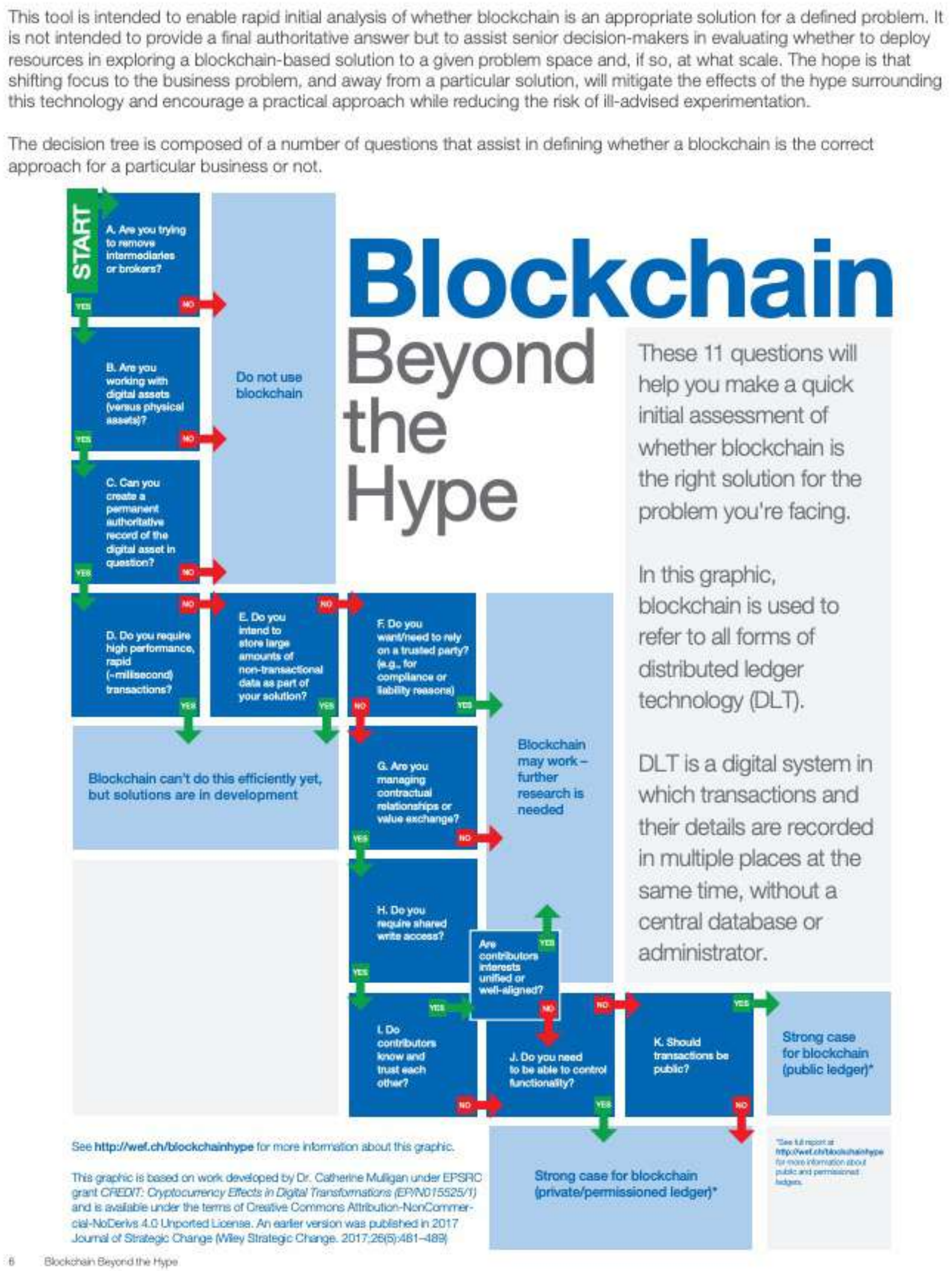
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Blockchain Beyond the Hype
A Practical Framework for Business Leaders

April 2018



This tool is intended to enable rapid initial analysis of whether blockchain is an appropriate solution for a defined problem. It is not intended to provide a final authoritative answer but to assist senior decision-makers in evaluating whether to deploy resources in exploring a blockchain-based solution to a given problem space and, if so, at what scale. The hope is that shifting focus to the business problem, and away from a particular solution, will mitigate the effects of the hype surrounding this technology and encourage a practical approach while reducing the risk of ill-advised experimentation.

The decision tree is composed of a number of questions that assist in defining whether a blockchain is the correct approach for a particular business or not.

START
A. Are you trying to remove intermediaries or brokers?
B. Are you working with digital assets (versus physical assets)?
C. Can you create a permanent authoritative record of the digital asset in question?
D. Do you require high performance, rapid (~millisecond) transactions?
E. Do you intend to store large amounts of non-transactional data as part of your solution?
F. Do you want/need to rely on a trusted party? (e.g., for compliance or liability reasons)
G. Are you managing contractual relationships or value exchange?
H. Do you require shared write access?
Are contributors interests unified or well-aligned?
I. Do contributors know and trust each other?
J. Do you need to be able to control functionality?
K. Should transactions be public?
YES
NO
Do not use blockchain
Blockchain can't do this efficiently yet, but solutions are in development
Blockchain may work – further research is needed
Strong case for blockchain (public ledger)*
Strong case for blockchain (private/permissioned ledger)*

Blockchain Beyond the Hype

These 11 questions will help you make a quick initial assessment of whether blockchain is the right solution for the problem you're facing.

In this graphic, blockchain is used to refer to all forms of distributed ledger technology (DLT).

DLT is a digital system in which transactions and their details are recorded in multiple places at the same time, without a central database or administrator.

See http://wef.ch/blockchainhype for more information about this graphic.

This graphic is based on work developed by Dr. Catherine Mulligan under EPSRC grant *CREDIT: Cryptocurrency Effects in Digital Transformations (EP/N015525/1)* and is available under the terms of Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Unported License. An earlier version was published in 2017 Journal of Strategic Change (Wiley Strategic Change. 2017;26(5):481–489)

*See full report at http://wef.ch/blockchainhype for more information about public and permissioned ledgers.

6 Blockchain Beyond the Hype

A. Are you trying to remove intermediaries or brokers?

B. Are you working with digital assets (versus physical assets)?

C. Can you create a permanent authoritative record of the digital asset in question?

D. Do you require high performance, rapid (~millisecond) transactions?

E. Do you intend to store large amounts of non-transactional data as part of your solution?

F. Do you want/need to rely on a trusted party? (e.g., for compliance or liability reasons)

G. Are you managing contractual relationships or value exchange?

H. Do you require shared write access?

I. Do contributors know and trust each other?

J. Do you need to be able to control functionality?

K. Should transactions be public?

# Blockchain: Used to Provide Proof of Identity & Transaction

Immutable

Independently Auditable

Traceable

Triple-Entry

Distributed Ledger

# Biometrics: Used to Provide Proof of Authentication

**Facial Recognition**

**Stored only on the User’s Device**

**To Authenticate Users**

**Events Recorded on the Blockchain**

# GPS: Used to Provide Proof of Location

GPS

**Global Positioning System**

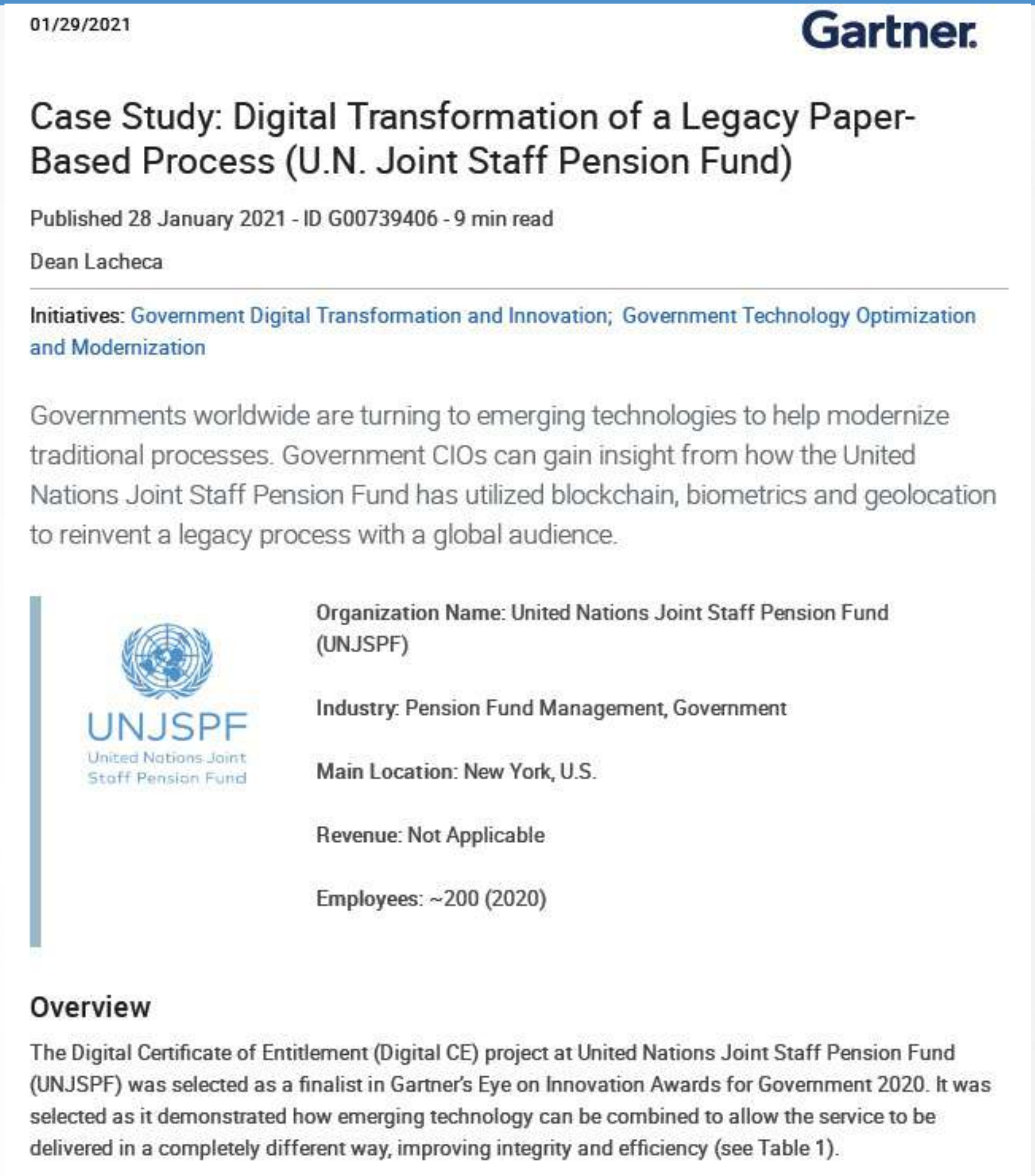
**Of the User's Device**

**Use to Determine & Record Location**

**Required only for specific cases**
**(two-track system)**

# Digital Certificate of Entitlement: Demo Video

# Gartner: UNJSPF Digital CE Finalist and Case Study on "Eye on Innovation Awards for Government"



01/29/2021

Gartner.

## Case Study: Digital Transformation of a Legacy Paper-Based Process (U.N. Joint Staff Pension Fund)

Published 28 January 2021 - ID G00739406 - 9 min read

Dean Lacheca

Initiatives: Government Digital Transformation and Innovation; Government Technology Optimization and Modernization

Governments worldwide are turning to emerging technologies to help modernize traditional processes. Government CIOs can gain insight from how the United Nations Joint Staff Pension Fund has utilized blockchain, biometrics and geolocation to reinvent a legacy process with a global audience.

UNJSPF
United Nations Joint
Staff Pension Fund

Organization Name: United Nations Joint Staff Pension Fund (UNJSPF)

Industry: Pension Fund Management, Government

Main Location: New York, U.S.

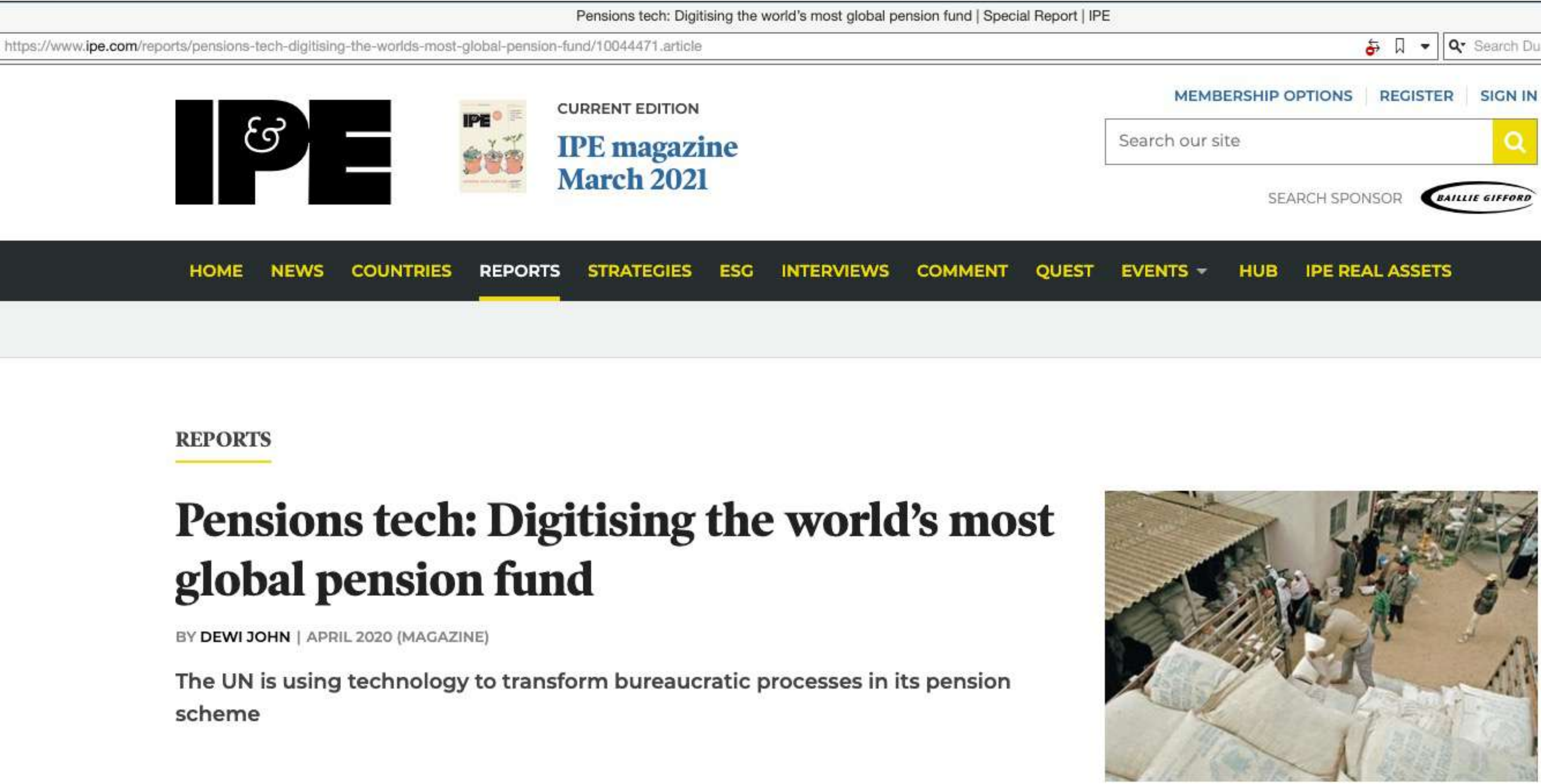
Revenue: Not Applicable

Employees: ~200 (2020)

### Overview

The Digital Certificate of Entitlement (Digital CE) project at United Nations Joint Staff Pension Fund (UNJSPF) was selected as a finalist in Gartner's Eye on Innovation Awards for Government 2020. It was selected as it demonstrated how emerging technology can be combined to allow the service to be delivered in a completely different way, improving integrity and efficiency (see Table 1).

# Investment & Pension Europe: Pensions Tech - Digitising the world's most global pension fund



REPORTS

## Pensions tech: Digitising the world's most global pension fund

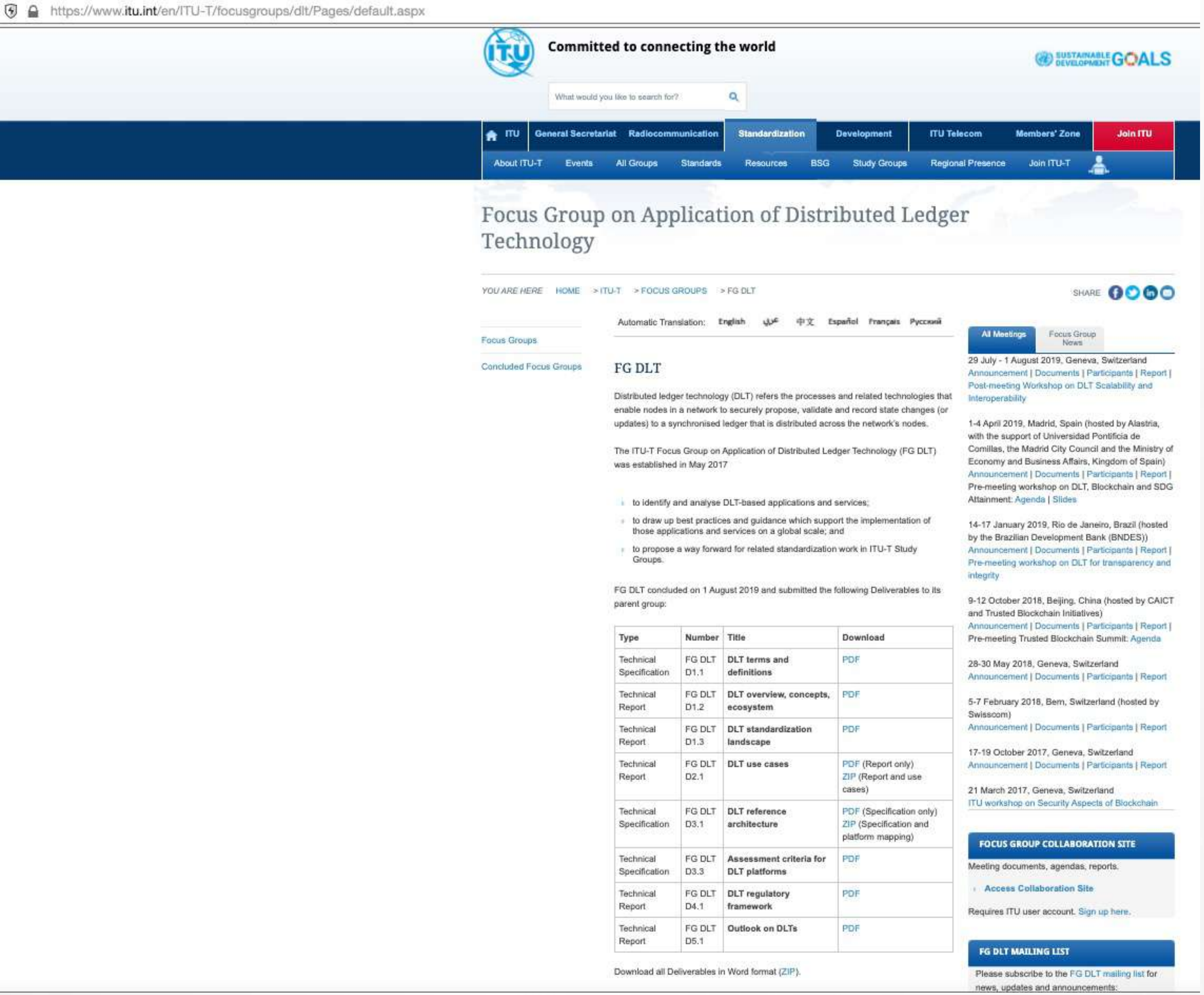
BY DEWI JOHN | APRIL 2020 (MAGAZINE)

The UN is using technology to transform bureaucratic processes in its pension scheme

# UNJSPF Digital Certificate of Entitlement

## Referenced Standards & Best Practices

# UN International Telecommunication Union



Focus Group on Application of Distributed Ledger Technology

YOU ARE HERE HOME > ITU-T > FOCUS GROUPS > FG DLT

## FG DLT

Distributed ledger technology (DLT) refers the processes and related technologies that enable nodes in a network to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes.

The ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT) was established in May 2017

- to identify and analyse DLT-based applications and services;
- to draw up best practices and guidance which support the implementation of those applications and services on a global scale; and
- to propose a way forward for related standardization work in ITU-T Study Groups.

FG DLT concluded on 1 August 2019 and submitted the following Deliverables to its parent group:

| Type | Number | Title | Download |
|---|---|---|---|
| Technical Specification | FG DLT D1.1 | **DLT terms and definitions** | PDF |
| Technical Report | FG DLT D1.2 | **DLT overview, concepts, ecosystem** | PDF |
| Technical Report | FG DLT D1.3 | **DLT standardization landscape** | PDF |
| Technical Report | FG DLT D2.1 | **DLT use cases** | PDF (Report only)<br>ZIP (Report and use cases) |
| Technical Specification | FG DLT D3.1 | **DLT reference architecture** | PDF (Specification only)<br>ZIP (Specification and platform mapping) |
| Technical Specification | FG DLT D3.3 | **Assessment criteria for DLT platforms** | PDF |
| Technical Report | FG DLT D4.1 | **DLT regulatory framework** | PDF |
| Technical Report | FG DLT D5.1 | **Outlook on DLTs** | PDF |

Download all Deliverables in Word format (ZIP).

29 July - 1 August 2019, Geneva, Switzerland
Announcement | Documents | Participants | Report | Post-meeting Workshop on DLT Scalability and Interoperability

1-4 April 2019, Madrid, Spain (hosted by Alastria, with the support of Universidad Pontificia de Comillas, the Madrid City Council and the Ministry of Economy and Business Affairs, Kingdom of Spain)
Announcement | Documents | Participants | Report | Pre-meeting workshop on DLT, Blockchain and SDG Attainment: Agenda | Slides

14-17 January 2019, Rio de Janeiro, Brazil (hosted by the Brazilian Development Bank (BNDES))
Announcement | Documents | Participants | Report | Pre-meeting workshop on DLT for transparency and integrity

9-12 October 2018, Beijing, China (hosted by CAICT and Trusted Blockchain Initiatives)
Announcement | Documents | Participants | Report | Pre-meeting Trusted Blockchain Summit: Agenda

28-30 May 2018, Geneva, Switzerland
Announcement | Documents | Participants | Report

5-7 February 2018, Bern, Switzerland (hosted by Swisscom)
Announcement | Documents | Participants | Report

17-19 October 2017, Geneva, Switzerland
Announcement | Documents | Participants | Report

21 March 2017, Geneva, Switzerland
ITU workshop on Security Aspects of Blockchain

**FOCUS GROUP COLLABORATION SITE**

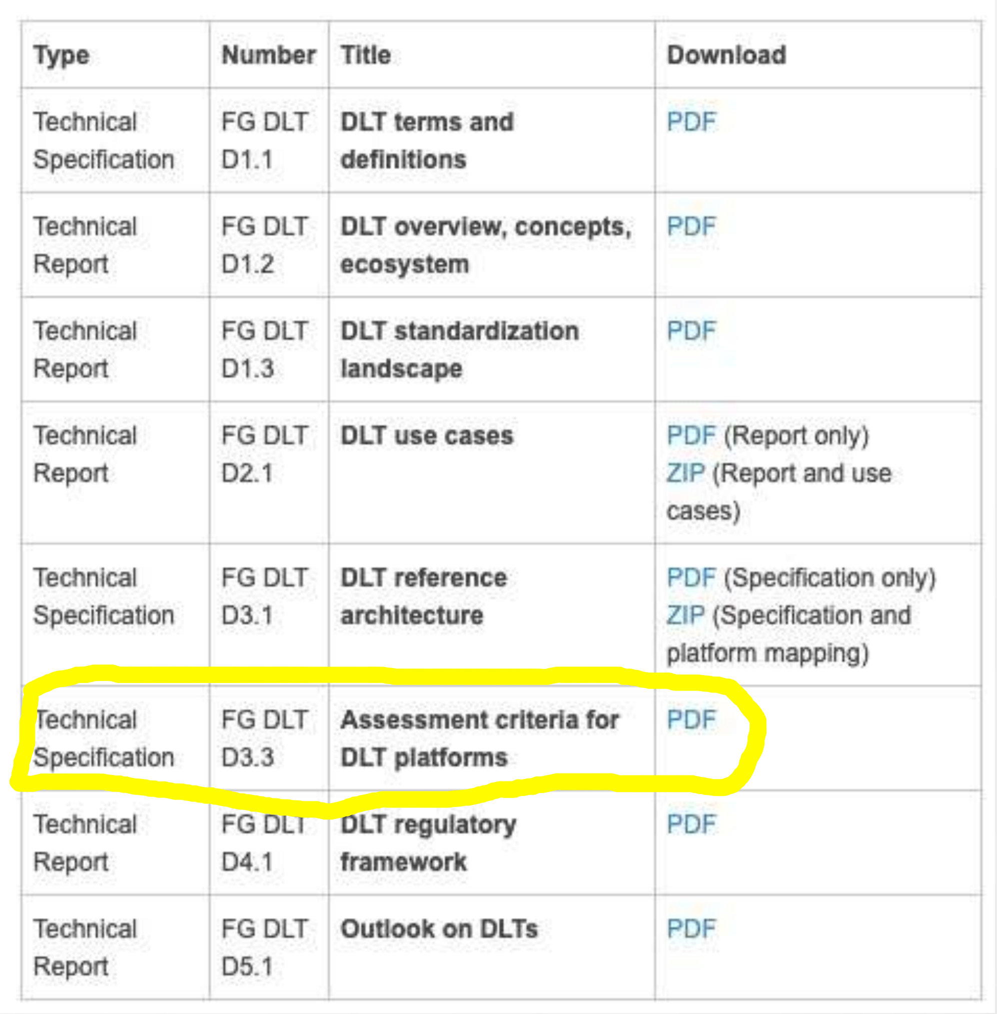
Meeting documents, agendas, reports.

- **Access Collaboration Site**

Requires ITU user account. Sign up here.

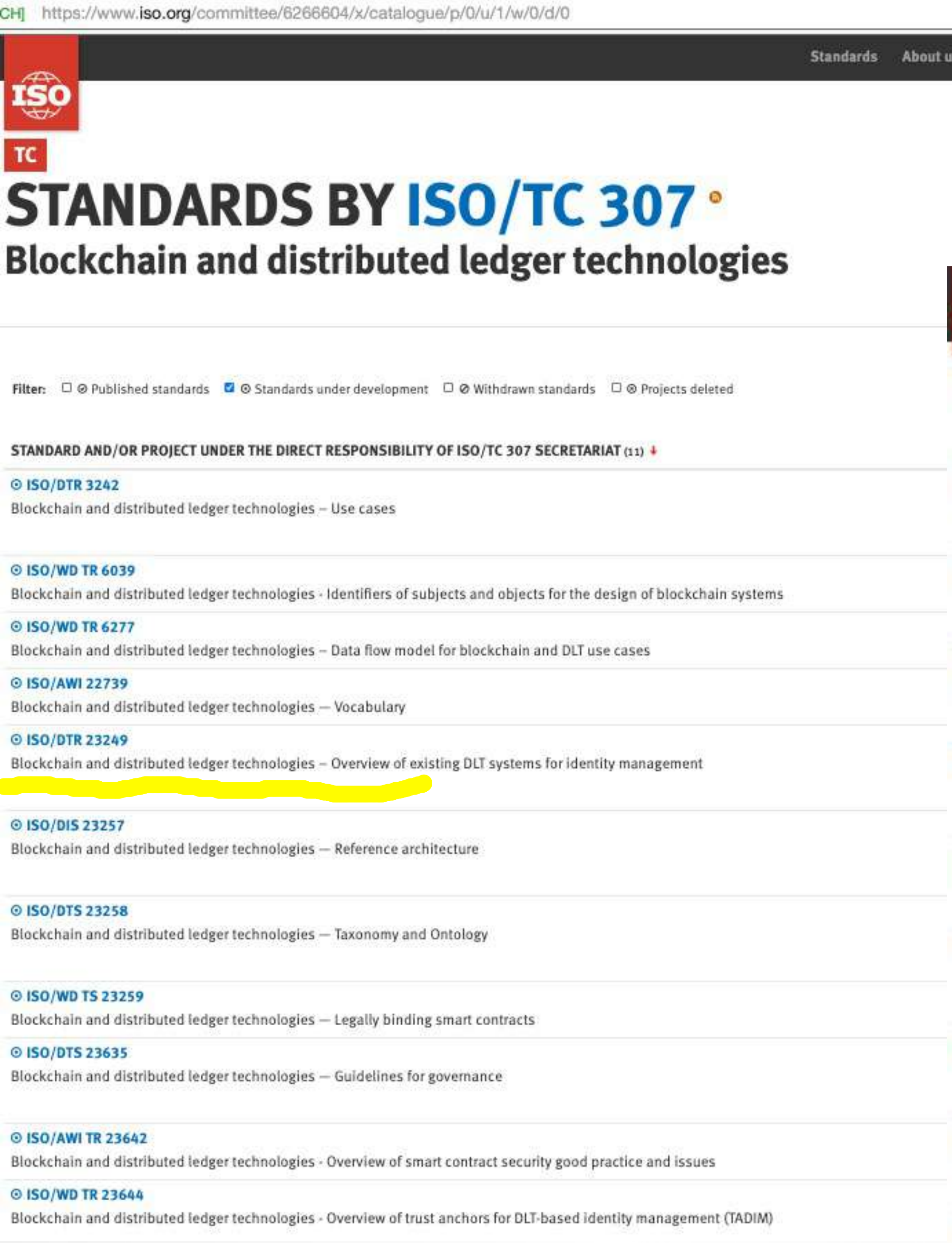
**FG DLT MAILING LIST**

Please subscribe to the FG DLT mailing list for news, updates and announcements:



| Type | Number | Title | Download |
|---|---|---|---|
| Technical Specification | FG DLT D1.1 | **DLT terms and definitions** | PDF |
| Technical Report | FG DLT D1.2 | **DLT overview, concepts, ecosystem** | PDF |
| Technical Report | FG DLT D1.3 | **DLT standardization landscape** | PDF |
| Technical Report | FG DLT D2.1 | **DLT use cases** | PDF (Report only)<br>ZIP (Report and use cases) |
| Technical Specification | FG DLT D3.1 | **DLT reference architecture** | PDF (Specification only)<br>ZIP (Specification and platform mapping) |
| Technical Specification | FG DLT D3.3 | **Assessment criteria for DLT platforms** | PDF |
| Technical Report | FG DLT D4.1 | **DLT regulatory framework** | PDF |
| Technical Report | FG DLT D5.1 | **Outlook on DLTs** | PDF |

# International Organization for Standardization (ISO): DLT and SECURITY


CH] https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0
Standards About us News Taking part Store EN
ISO
TC

## STANDARDS BY ISO/TC 307

### Blockchain and distributed ledger technologies

Filter: □ Published standards ☑ Standards under development □ Withdrawn standards □ Projects deleted

STANDARD AND/OR PROJECT UNDER THE DIRECT RESPONSIBILITY OF ISO/TC 307 SECRETARIAT (11)

**ISO/DTR 3242**
Blockchain and distributed ledger technologies – Use cases

**ISO/WD TR 6039**
Blockchain and distributed ledger technologies - Identifiers of subjects and objects for the design of blockchain systems

**ISO/WD TR 6277**
Blockchain and distributed ledger technologies – Data flow model for blockchain and DLT use cases

**ISO/AWI 22739**
Blockchain and distributed ledger technologies — Vocabulary

**ISO/DTR 23249**
Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management

**ISO/DIS 23257**
Blockchain and distributed ledger technologies — Reference architecture

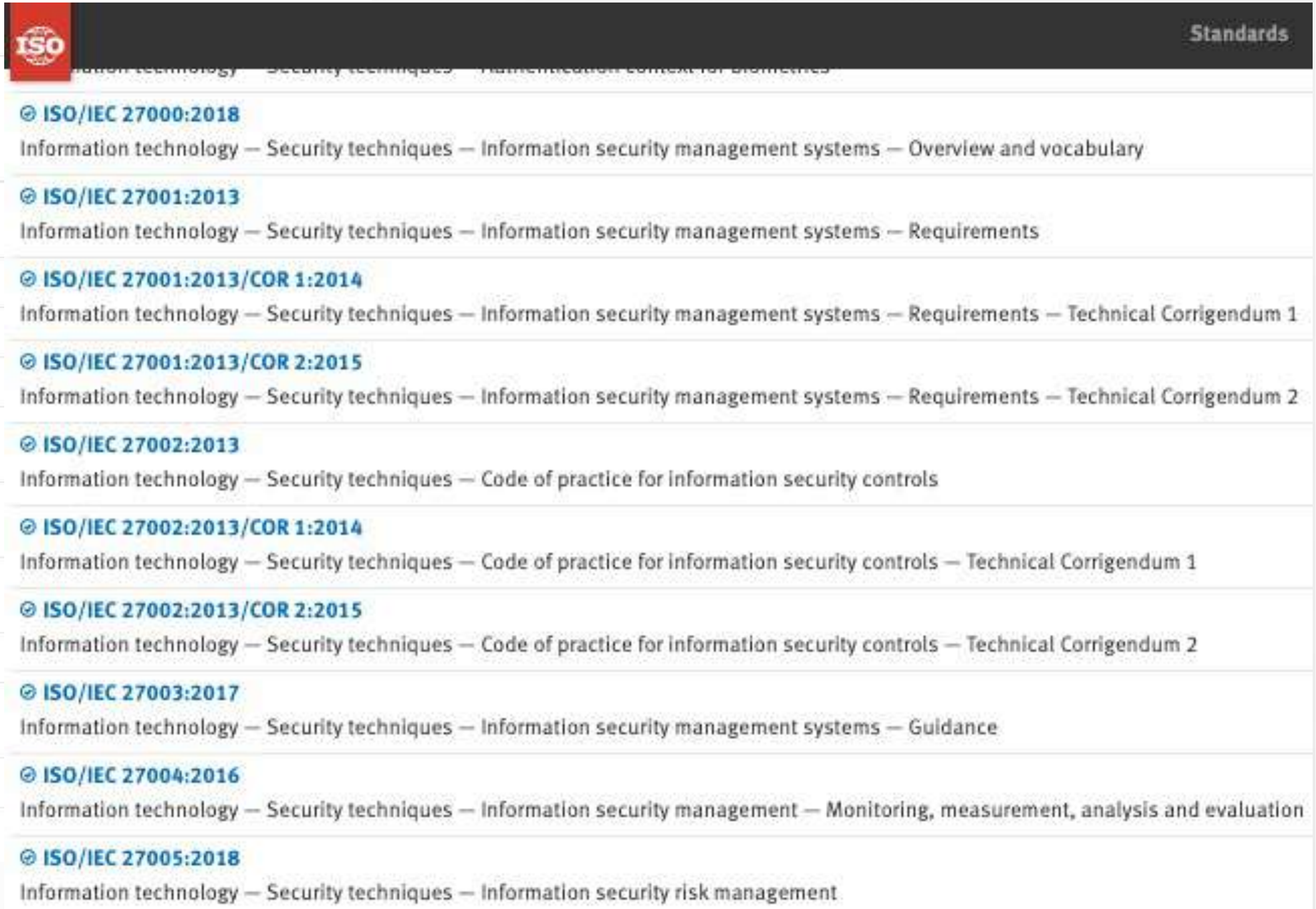
**ISO/DTS 23258**
Blockchain and distributed ledger technologies — Taxonomy and Ontology

**ISO/WD TS 23259**
Blockchain and distributed ledger technologies — Legally binding smart contracts

**ISO/DTS 23635**
Blockchain and distributed ledger technologies — Guidelines for governance

**ISO/AWI TR 23642**
Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues

**ISO/WD TR 23644**
Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management (TADIM)



**ISO/IEC 27000:2018**
Information technology — Security techniques — Information security management systems — Overview and vocabulary

**ISO/IEC 27001:2013**
Information technology — Security techniques — Information security management systems — Requirements

**ISO/IEC 27001:2013/COR 1:2014**
Information technology — Security techniques — Information security management systems — Requirements — Technical Corrigendum 1

**ISO/IEC 27001:2013/COR 2:2015**
Information technology — Security techniques — Information security management systems — Requirements — Technical Corrigendum 2

**ISO/IEC 27002:2013**
Information technology — Security techniques — Code of practice for information security controls

**ISO/IEC 27002:2013/COR 1:2014**
Information technology — Security techniques — Code of practice for information security controls — Technical Corrigendum 1

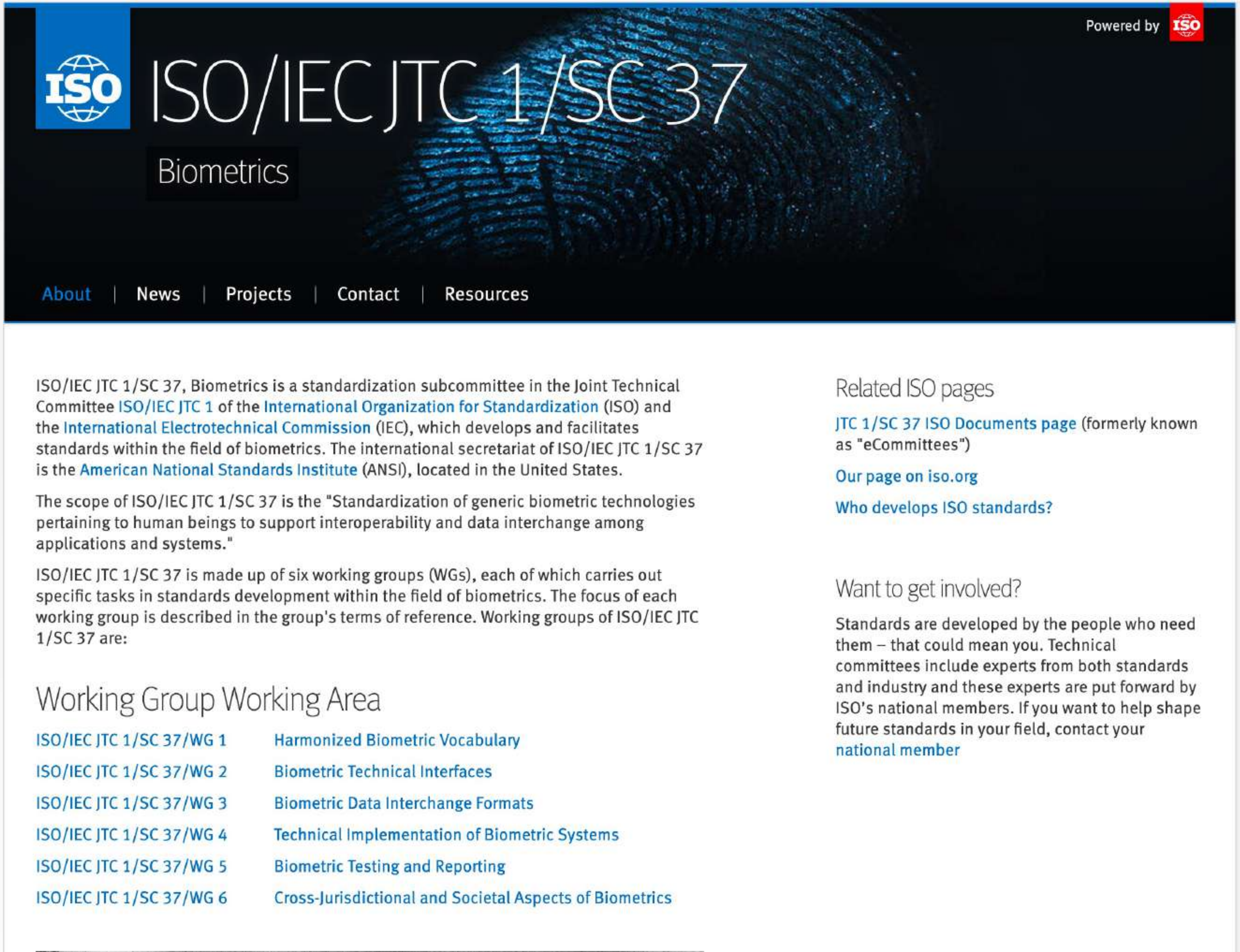
**ISO/IEC 27002:2013/COR 2:2015**
Information technology — Security techniques — Code of practice for information security controls — Technical Corrigendum 2

**ISO/IEC 27003:2017**
Information technology — Security techniques — Information security management systems — Guidance

**ISO/IEC 27004:2016**
Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

**ISO/IEC 27005:2018**
Information technology — Security techniques — Information security risk management

# International Organization for Standardization (ISO): BIOMETRICS



ISO/IEC JTC 1/SC 37, Biometrics is a standardization subcommittee in the Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which develops and facilitates standards within the field of biometrics. The international secretariat of ISO/IEC JTC 1/SC 37 is the American National Standards Institute (ANSI), located in the United States.

The scope of ISO/IEC JTC 1/SC 37 is the "Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems."

ISO/IEC JTC 1/SC 37 is made up of six working groups (WGs), each of which carries out specific tasks in standards development within the field of biometrics. The focus of each working group is described in the group's terms of reference. Working groups of ISO/IEC JTC 1/SC 37 are:

| Working Group | Working Area |
|---|---|
| ISO/IEC JTC 1/SC 37/WG 1 | Harmonized Biometric Vocabulary |
| ISO/IEC JTC 1/SC 37/WG 2 | Biometric Technical Interfaces |
| ISO/IEC JTC 1/SC 37/WG 3 | Biometric Data Interchange Formats |
| ISO/IEC JTC 1/SC 37/WG 4 | Technical Implementation of Biometric Systems |
| ISO/IEC JTC 1/SC 37/WG 5 | Biometric Testing and Reporting |
| ISO/IEC JTC 1/SC 37/WG 6 | Cross-Jurisdictional and Societal Aspects of Biometrics |

## Related ISO pages

JTC 1/SC 37 ISO Documents page (formerly known as "eCommittees")

Our page on iso.org

Who develops ISO standards?

## Want to get involved?

Standards are developed by the people who need them – that could mean you. Technical committees include experts from both standards and industry and these experts are put forward by ISO's national members. If you want to help shape future standards in your field, contact your national member

# UNJSPF Digital Certificate of Entitlement

Proof of Concept

# Objectives of the Proof of Concept

## Objective 1

- Explore the adoption of innovative & secure technologies for Digital Identification and Authentication to *automate* the Certificate of Entitlement process

## Objective 2

- Build a Proof of Concept that can *demonstrate the reliable application of new technologies to address existing limitations*
- Prevent the introduction of additional risks that could hamper the flow of entitlements

## Objective 3

- Establish the *technical feasibility* of a service using new technologies

# Key Principles of the Proof of Concept

## Principle 1

- **Privacy and Security**: Biometric information to reside as close to the owner as possible.
- Biometric information stored and accessed securely at all times with clear audit trails

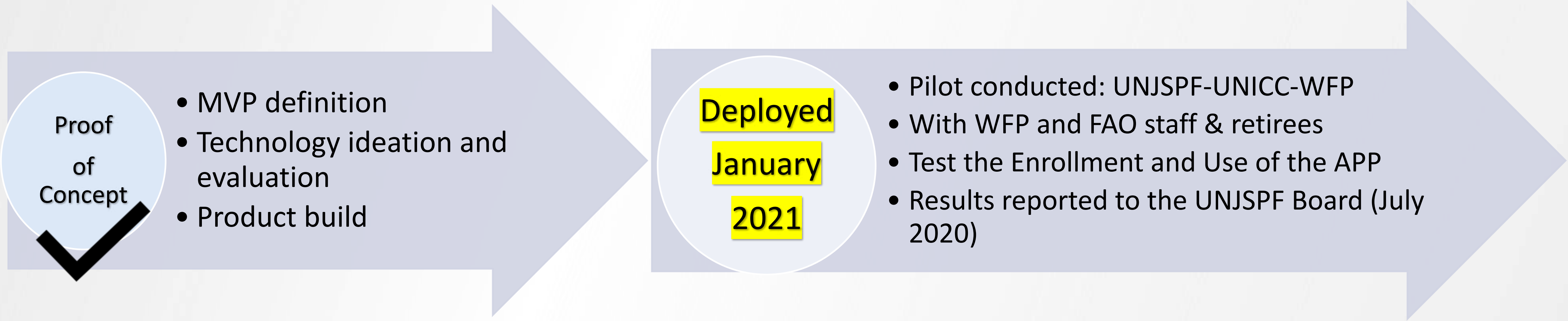
## Principle 2

- **Confidentiality and Integrity** Adoption of *secure* (i.e., private) cloud based technology – especially for storing and processing Biometric information

## Principle 3

- **Flexibility and Scalability** Pilot a solution *that can be used globally* to serve all beneficiaries of the Fund

# The Digital Certificate of Entitlement: The Journey



Proof of Concept ✓

- MVP definition
- Technology ideation and evaluation
- Product build

Deployed January 2021

- Pilot conducted: UNJSPF-UNICC-WFP
- With WFP and FAO staff & retirees
- Test the Enrollment and Use of the APP
- Results reported to the UNJSPF Board (July 2020)

## Technology Highlights

Machine Learning (deep neural network) algorithms to Certify Proof of Existence using Biometric Recognition through a Mobile Phone App

Digital Identity on a Permissioned Blockchain with Immutable & Auditable Records of Transactions

Users in Control of their Identity (including biometric information)

Technology applicable to 'disconnected' smart phone apps

UNJSPF United Nations Joint Staff Pension Fund

WFP United Nations World Food Programme

ICC international computing centre ICT SOLUTIONS FOR THE UN FAMILY

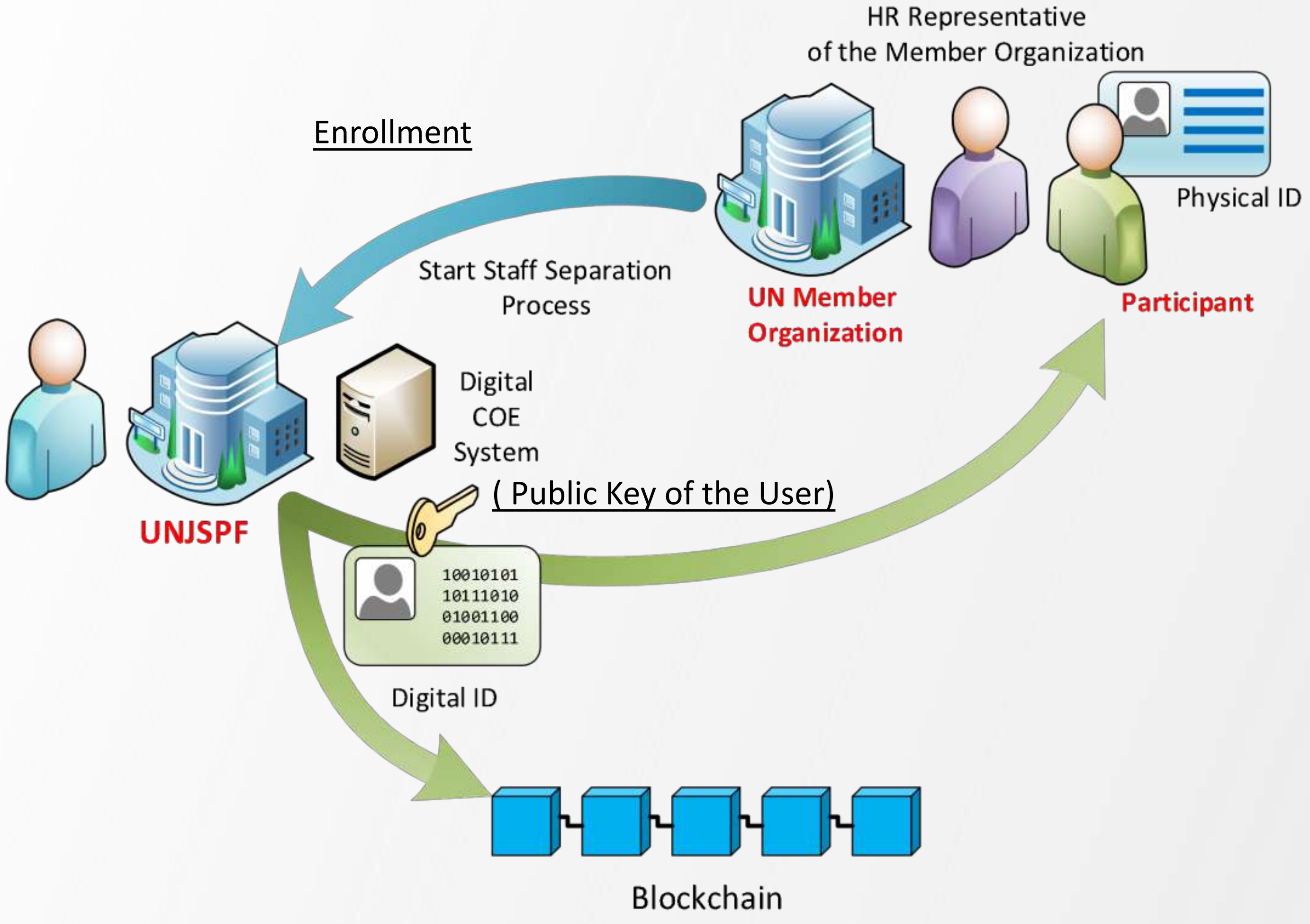
# Conceptual View – Enrollment process

UN Member Organizations

- Identity Verification/Recording
- Capture Biometric Data

UNJSPF

- Data Acquisition
- Digital ID Creation (Decentralized Identifier)



DID Creation

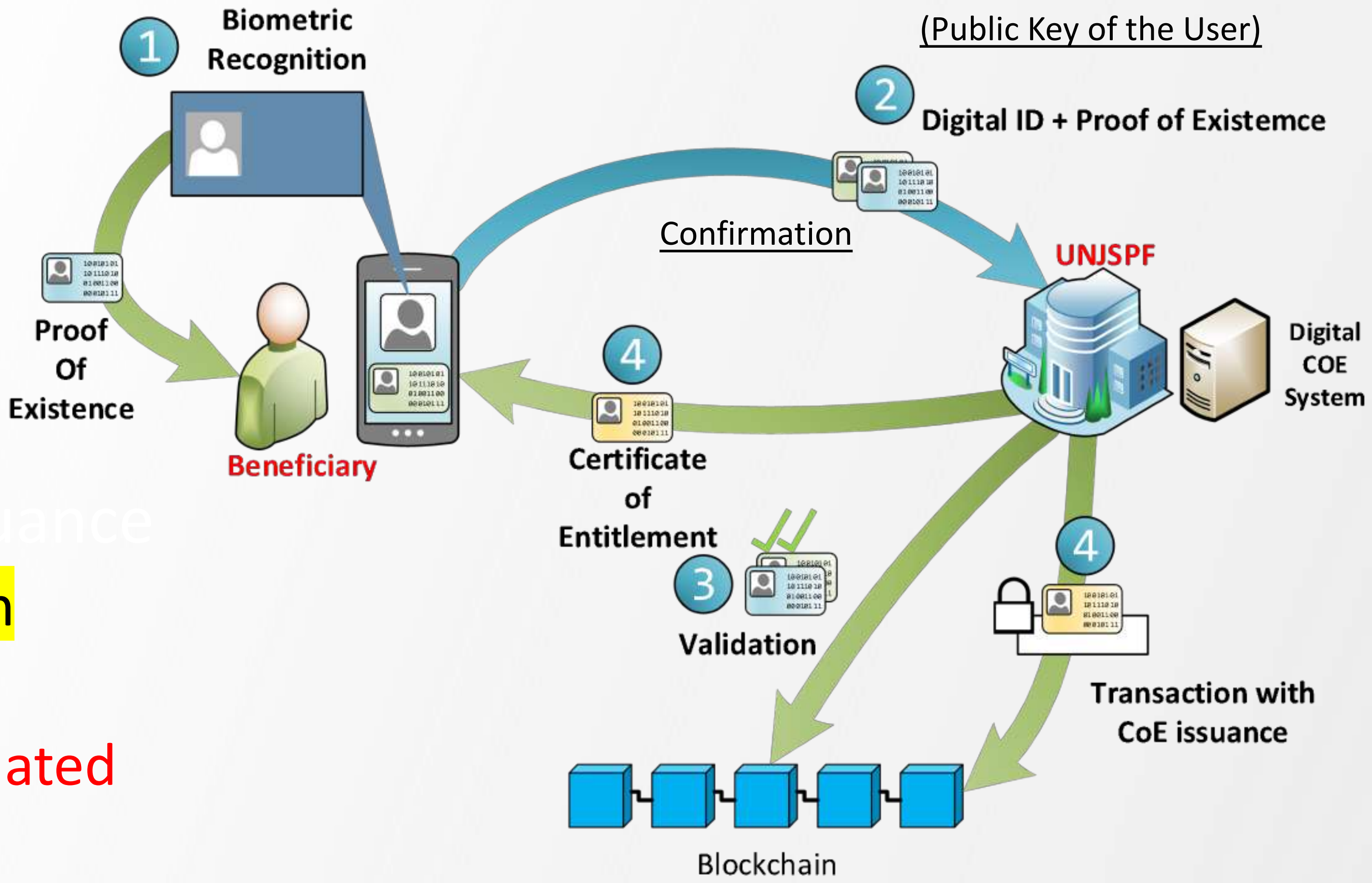
# Conceptual View – Digital Certificate of Entitlement

## Biometric Identity

- Face recognition
- Proof of Existence

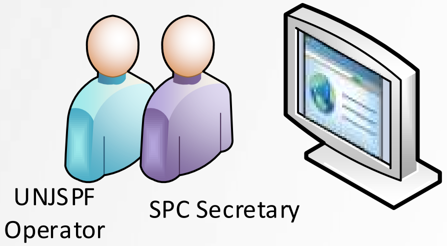
## Digital Certificate of Entitlement issuance

- Transactions stored in the Blockchain
  - Immutable and Tamper Proof
  - Can be Traced, Audited and Validated

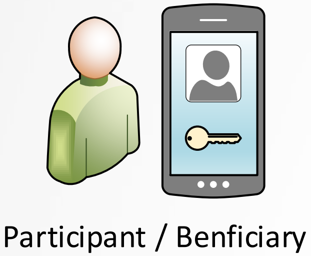


CE Issuance

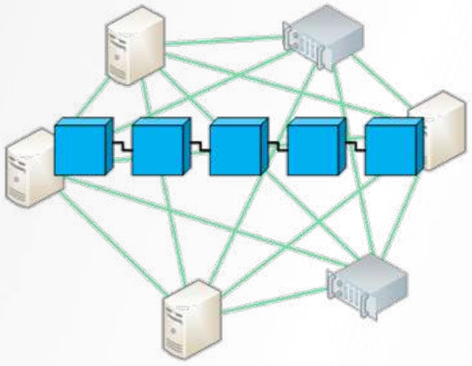
# Conceptual View - Components



Web Based Admin Site: Administration from any location



Mobile Application: Biometric authentication and user interaction



Blockchain: Safe recording of Identity Creation & Transactions with Traceability and Auditability, on a Distributed Ledger within UN premises (UNICC Nodes on a Permissioned Blockchain) protected by the UN Privileges & Immunities

# Components View

### Users Layer

- Beneficiaries use a mobile app to interact with the system
- UNJSPF Representative and Operators use a Web Application to interact with the system

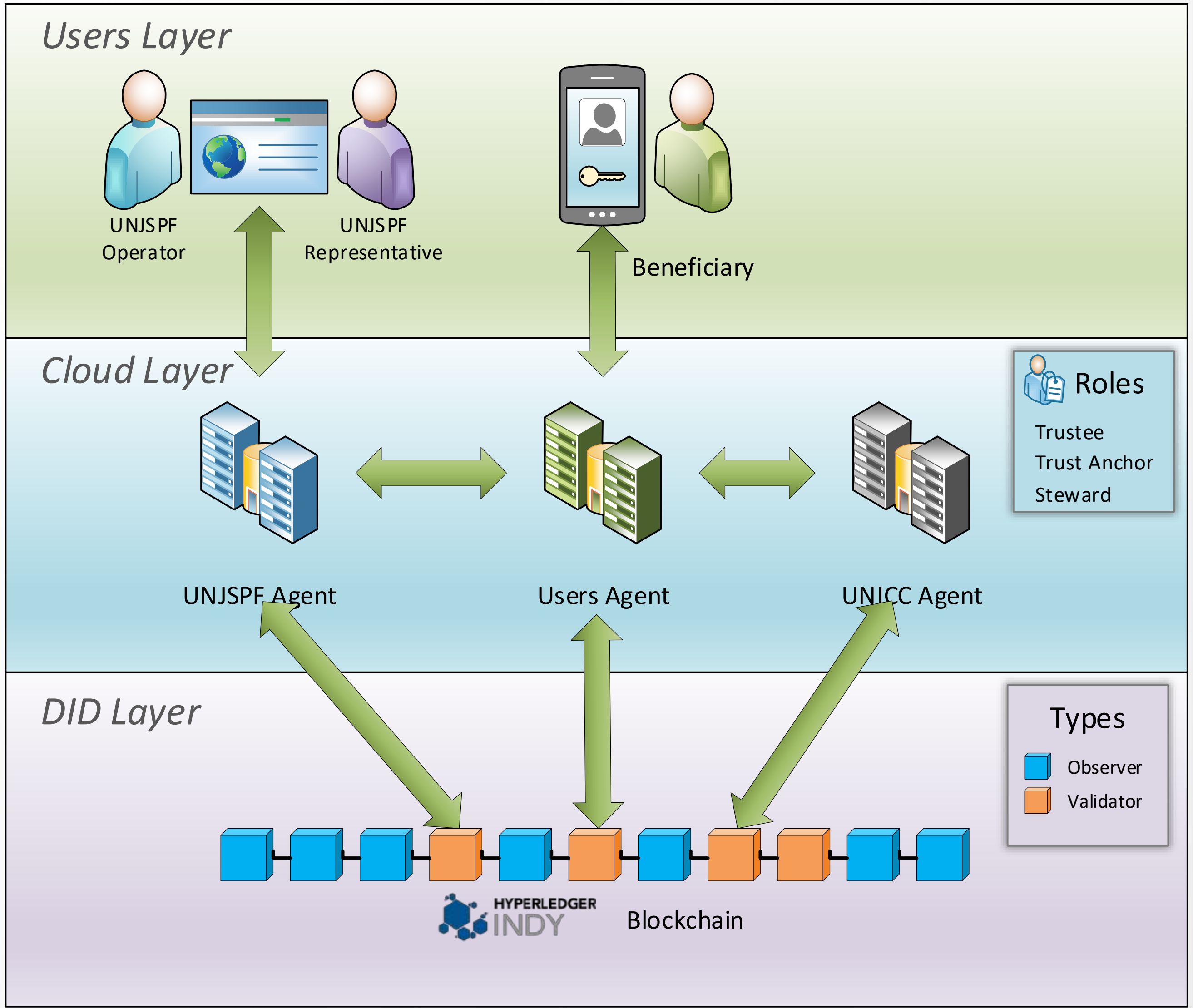
### Cloud Layer

- UNJSPF Agent – Issues *UNJSPF-ID* and *Certificate of Entitlement* credentials. Interacts with UNJSPF users
- Users Agent – Interacts with UNJSPF. Requests and manages user's credentials
- UNICC Agent – Support users in generating their Proof-of-Existence

### DID Layer

- Blockchain nodes append/record transactions

(NO Personal Identifiable Information stored on the Blockchain, whether on clear or encrypted form)



# UNJSPF Digital Certificate of Entitlement

## The Pilot Test

# Pilot Programme Metrics

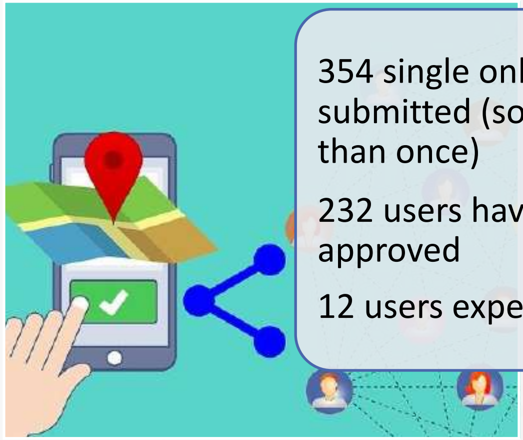
265 Invites sent out on **18/May/2020**

86 Invites sent out on 9/June/2020

## Beneficiaries

- 352 volunteers
- in 70+ countries

## Onboarding



354 single onboardings submitted (some users more than once)

232 users have their onboarding approved

12 users expected to re-onboard

## DCE Issued

**192 DCE issued, for 143 Beneficiaries, from 43 countries**

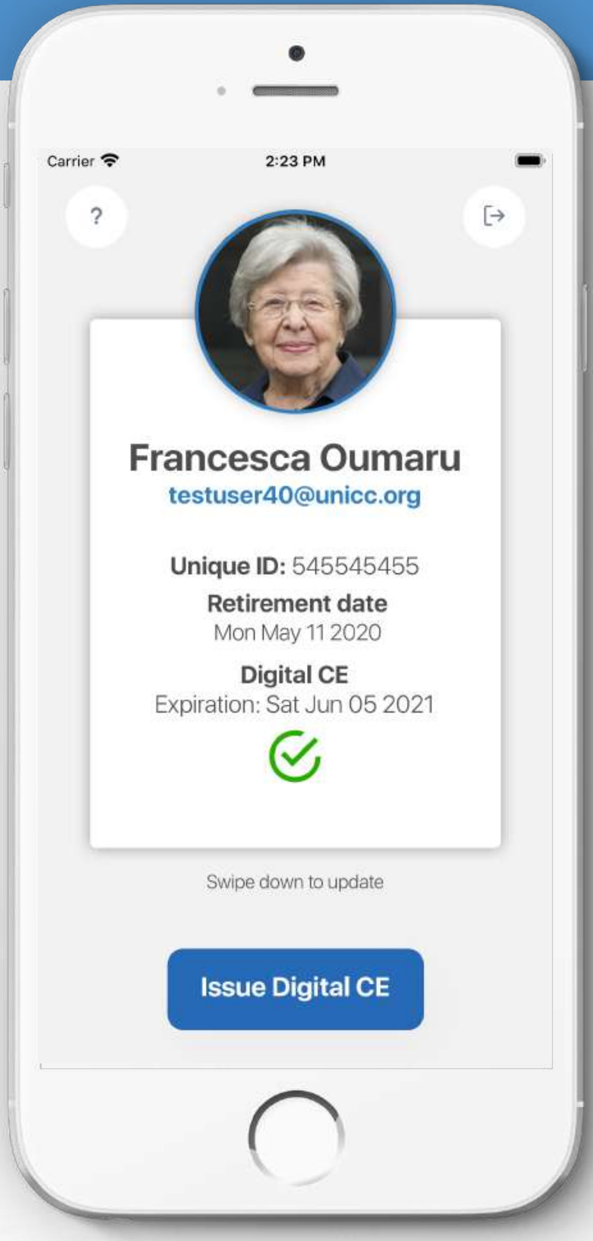
Ethiopia, Guatemala, Vietnam, Italy, Nepal, Bangladesh, Pakistan, Thailand, Indonesia, Japan, Honduras, Sri Lanka, Madagascar, Kenya, USA, Yemen, Indonesia, Germany, Belgium, Ecuador, France, Sweden, Syria, India, UK, Bolivia, Rwanda, Philippines, Australia, Iran, Cambodia, Senegal, Sudan, Ghana, Malta, Portugal, Spain, Ireland, South Africa, Laos, Canada, Uganda, Egypt

# Pilot Programme Metrics

## Digital CE:

- **192 single DCEs were issued**
- **143 beneficiaries issued a DCE once or more, both on Android and iOS**
- **43 countries:**

Ethiopia, Guatemala, Vietnam, Italy, Nepal, Bangladesh, Pakistan, Thailand, Indonesia, Japan, Honduras, Sri Lanka, Madagascar, Kenya, USA, Yemen, Indonesia, Germany, Belgium, Ecuador, France, Sweden, Syria, India, UK, Bolivia, Rwanda, Philippines, Australia, Iran, Cambodia, Senegal, Sudan, Ghana, Malta, Portugal, Spain, Ireland, South Africa, Laos, Canada, Uganda, Egypt



Francesca Oumaru
testuser40@unicc.org

**Unique ID:** 545545455

**Retirement date**
Mon May 11 2020

**Digital CE**
Expiration: Sat Jun 05 2021

✓

Swipe down to update

# Pilot Programme Metrics – Pilot Test Findings & Lessons Learned

## **Security device compatibility**:

1. Android security:

   OS version the device ***shipped*** with >= 7.0

   - Impacted 15 users. Need to use a compatible device
   - Android 7.0 was released on August 2016. Devices shipped earlier than this date will be affected by this issue

## **Network conditions**:

1. The app proved to operate normally regardless to fluctuating network conditions
2. The mean size of the main requests was:
   1. Onboarding submission: ~900 kilobytes
   2. DCE issuance: ~500 bytes

# Pilot Programme Metrics – Pilot Test findings & Lessons Learned

**Biometric process findings:**

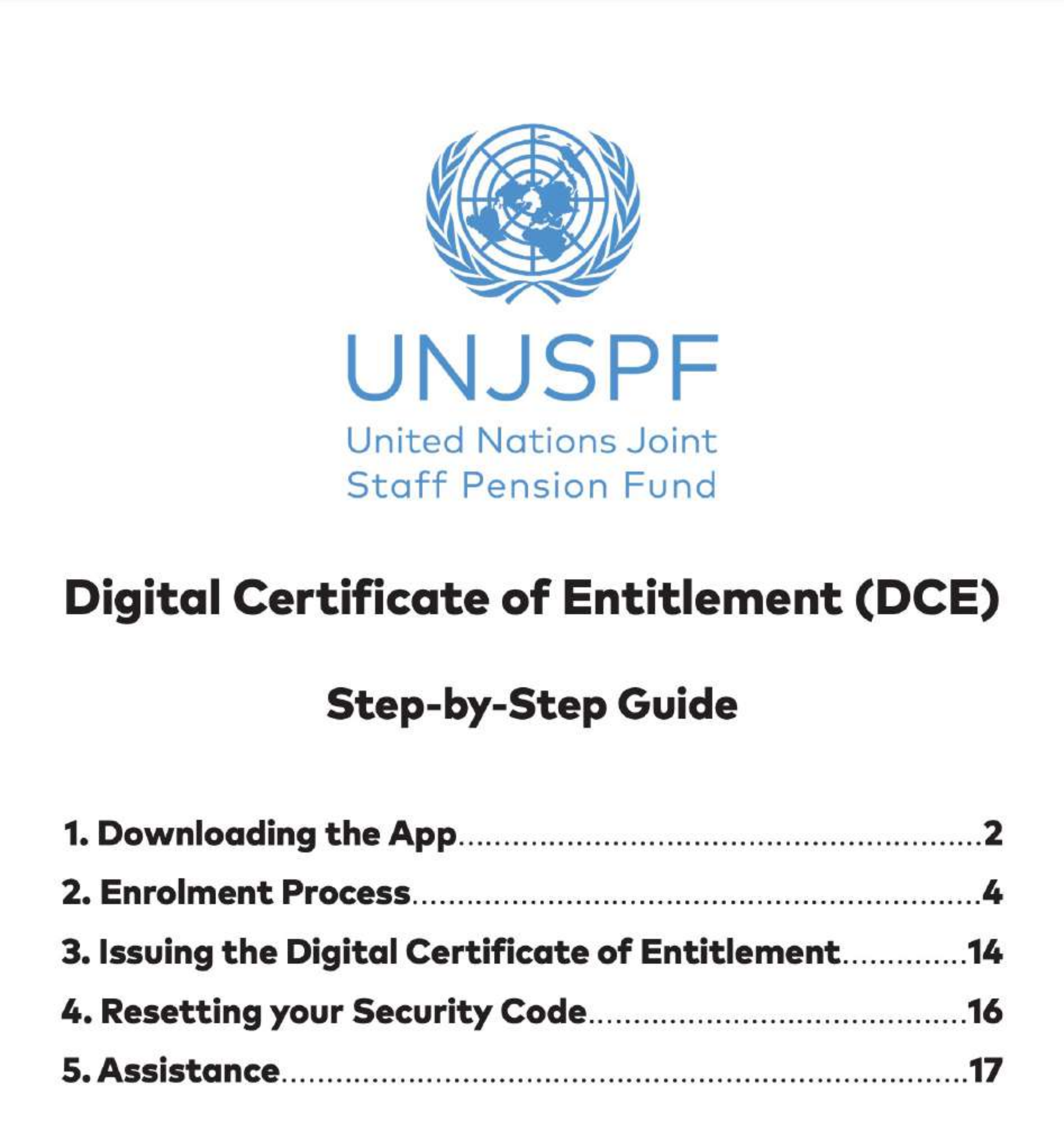
1. Recognition process, lower-end Android devices processor presented compatibility issues:
   - Impacted 14 additional users
   - Those users with an incompatible device as specified in the device security requirements were also affected
   - The list of devices which resulted to be incompatible included:
     - Motorola Moto E5, G5s Plus, E4
     - BlackBerry Z10
     - HUAWEI Y5, Y6
     - Nokia 1
     - Samsung Galaxy A10, J4+, J8
2. The quality of the face capture process impacted the further biometric validation
3. Face capture conditions for 26 users led to adjustments and/or additional on-screen guidance for:
   1. Face detection
   2. Eyes detection (glasses): used for image stabilization
   3. Expression detection
   4. Resiliency to changing light conditions

**Alternative tools and implementation were identified to address all cases**

# UNJSPF Digital Certificate of Entitlement

## Step-by-Step Process

# The UNJSPF Digital CE: Step-by-Step Process



UNJSPF

United Nations Joint
Staff Pension Fund

## Digital Certificate of Entitlement (DCE)

### Step-by-Step Guide

# UNJSPF Digital Certificate of Entitlement

## Cybersecurity & Privacy Assurance

# ITU Standards Referenced to Provide Assurance on Cybersecurity

International Telecommunication Union

**ITU-T Technical Specification**

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

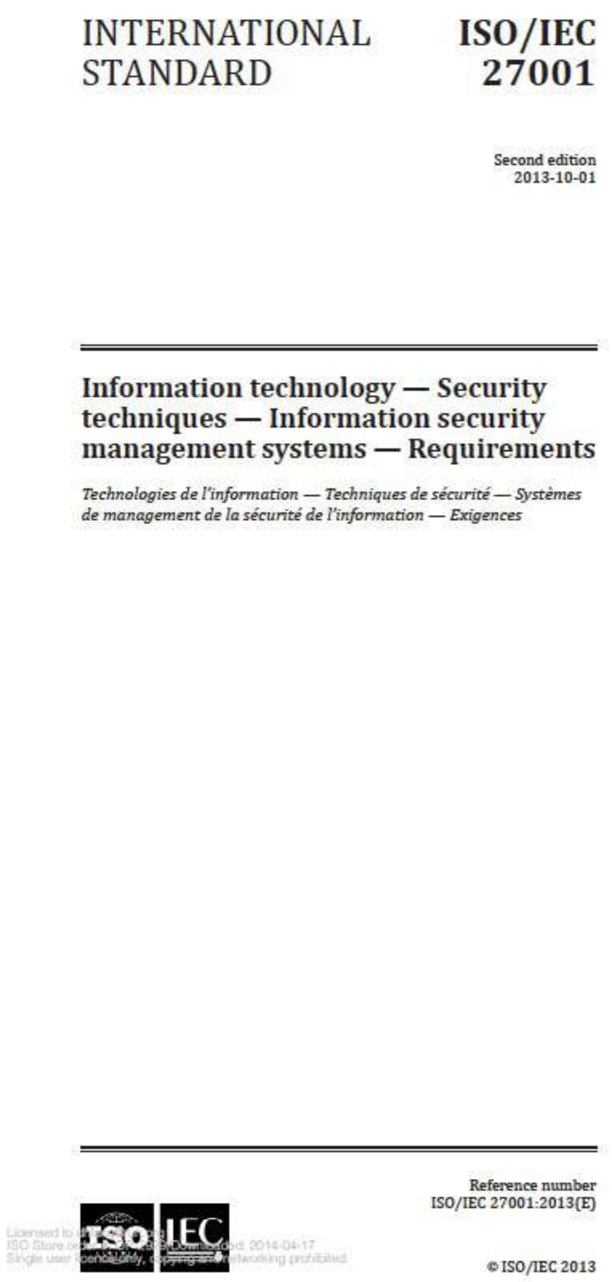
(1 AUG 2019)

ITU-T Focus Group on Application of
Distributed Ledger Technology
(FG DLT)

**Technical Specification FG DLT D3.3**

**Assessment criteria for distributed ledger technology platforms**

# ISO Standards Referenced to Provide Assurance on Cybersecurity



INTERNATIONAL STANDARD

ISO/IEC 27001

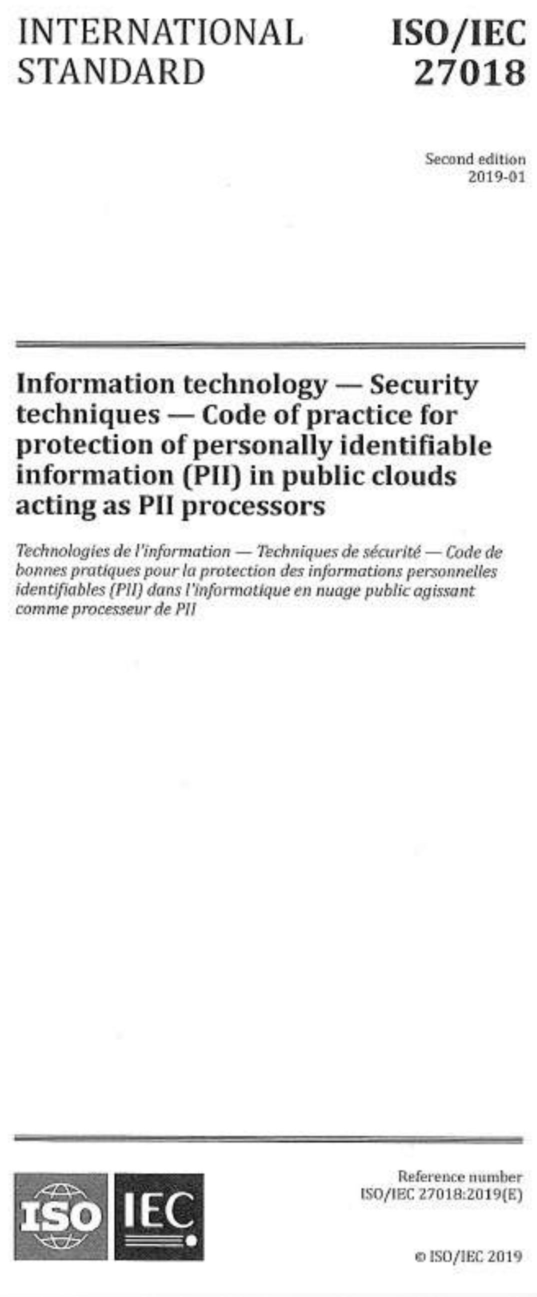
Second edition
2013-10-01

**Information technology — Security techniques — Information security management systems — Requirements**

*Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013



INTERNATIONAL STANDARD

ISO/IEC 27018

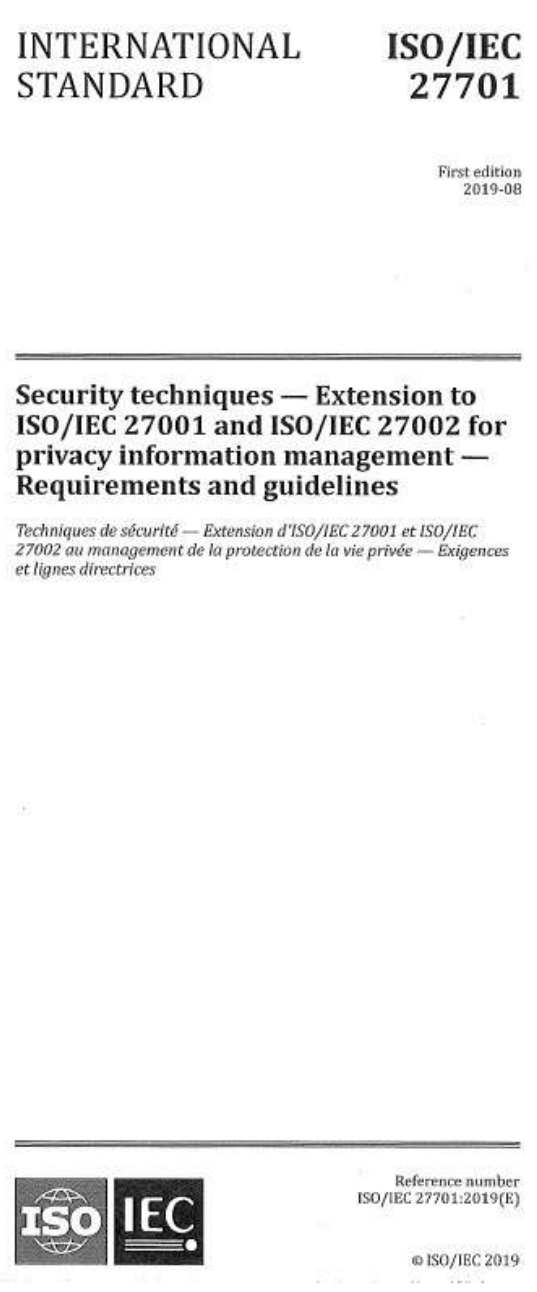
Second edition
2019-01

**Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**

*Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*

Reference number
ISO/IEC 27018:2019(E)

© ISO/IEC 2019



INTERNATIONAL STANDARD

ISO/IEC 27701

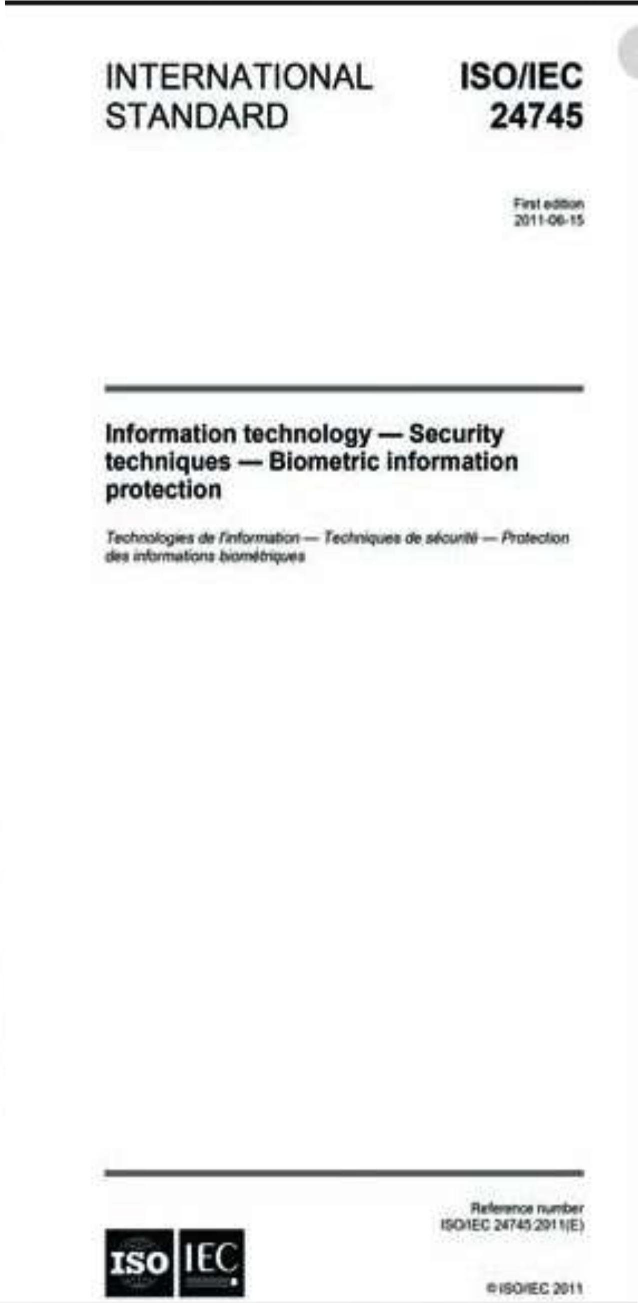
First edition
2019-08

**Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices*

Reference number
ISO/IEC 27701:2019(E)

© ISO/IEC 2019



INTERNATIONAL STANDARD

ISO/IEC 24745

First edition
2011-06-15

**Information technology — Security techniques — Biometric information protection**

*Technologies de l'information — Techniques de sécurité — Protection des informations biométriques*

Reference number
ISO/IEC 24745:2011(E)

© ISO/IEC 2011

# Cybersecurity Assurance – Control Domains

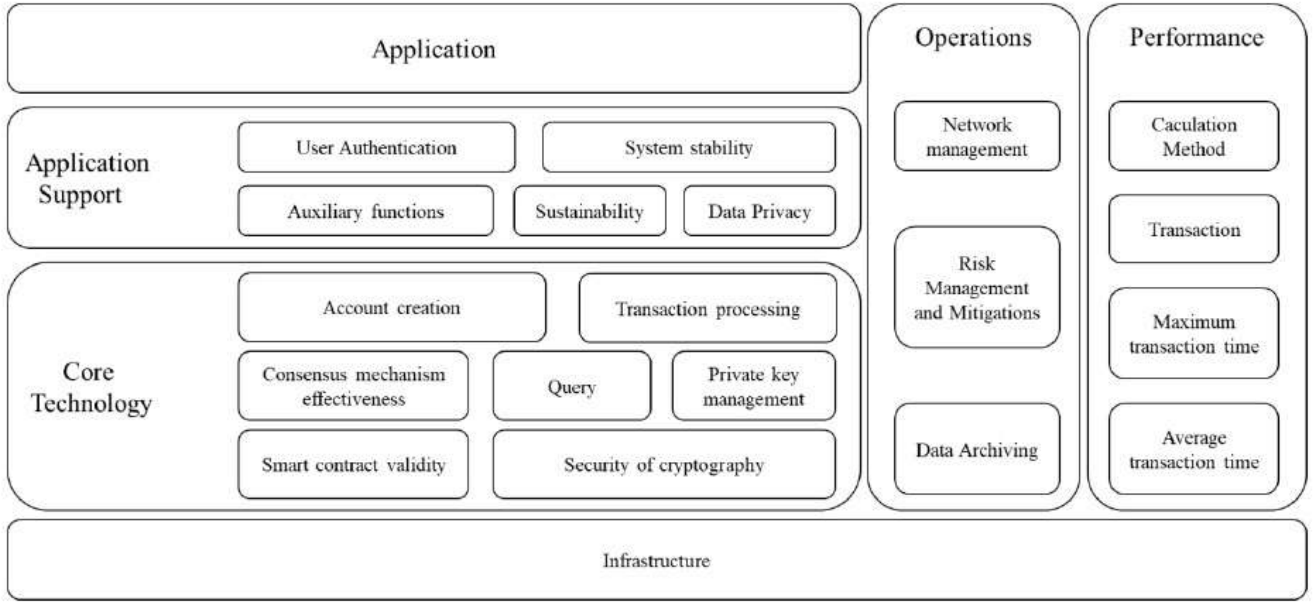
1. High Level Solution

2. Front-End Solution Components

3. Back-End Solution Components

4. Network Security

5. External System Integration



Application

Operations

Performance

Application Support

User Authentication

System stability

Auxiliary functions

Sustainability

Data Privacy

Core Technology

Account creation

Transaction processing

Consensus mechanism effectiveness

Query

Private key management

Smart contract validity

Security of cryptography

Network management

Risk Management and Mitigations

Data Archiving

Caculation Method

Transaction

Maximum transaction time

Average transaction time

Infrastructure

**ITU-T** **Technical Specification**

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(1 AUG 2019)

6. Business Network Integration

7. Non-Technical Threats

8. Pace of Change

9. Web 3.0 vs Traditional Development

10. Smart Contracts (N/A)

11. Futureproofing

What if I lose my phone?

And how do I mitigate such disasters before they happen?

Daniel Hardman
Chief Architect, Evernym
Secretary, Sovrin Foundation Technical Governance Board
March 2019

sovrin
identity for all

https://sovrin.org/wp-content/uploads/2019/03/What-if-someone-steals-my-phone-110319.pdf

# Digital Identity Privacy Assurance – Control Domains

## I. Policy: Formulation, Supporting Principles and Documentation

1. Use Case: i.e., Identity Management
2. Rationale: Requirements & Resources
3. Biometric Modality: i.e., Facial Recognition
4. Legal Norms & Ethical Principles
5. Human Rights Due Diligence
6. Data Provenance, Protection & Privacy Rights
7. Data Stewardship, Minimisation & Purpose Limitation: i.e., Self Sovereign Identity
8. Stakeholder Consultation
9. Security Verification & Business Cont.

11. Risk Assessment
12. Financial Planning; System Procurement, Testing and Standards
13. Network Connectivity

## II. Data Collection: Enrolment & Integrity Biometric Data

14. How biometric data is collected
15. Legality of Data Collection & Consent
16. Data Management & Quality
17. Presentation Attack Detection
18. Exception Handling

## III. Data Processing & Output Management

19. Operating Parameters
20. System Security
21. Performance Mgmt & Testing Protocols

## IV. Organisational Issues

22. Managing & Deploying
23. Operating in extreme conditions
24. Oversight
25. Innovation and emerging tech
26. Service Delivery

# UNJSPF Digital Certificate of Entitlement

## The Underlying Technology

## Hyperledger Indy Blockchain

# Hyperledger Indy: 10 Selection Criteria

1. Supports digital ”assets”

2. Enables the Creation of a Permanent Ledger

3. Supports Private and Secure Identity Verification (BUT On-Chain Transactions Include Only Public Data)

4. Employs industry-standard cryptography and best practices in key management

5. Adopts the approach and principles of privacy-by-design (prevents correlation by allowing identify owner to own multiple DIDs)

6. Business logic contains cryptographic mechanisms verify credentials

7. Not required to deliver fast processing performance

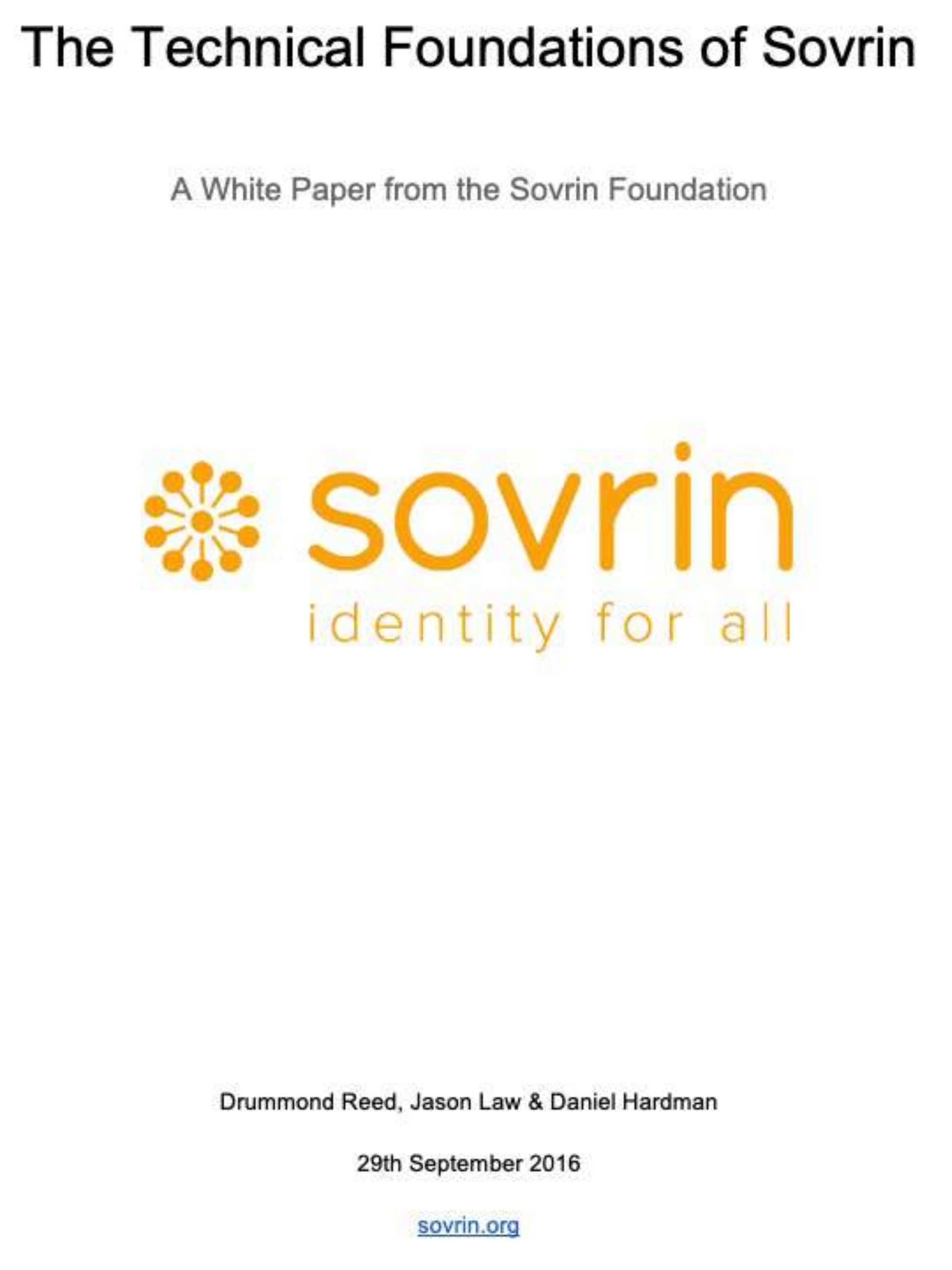
8. Not required to store large amount of data

9. Full traceability and auditability of transactions

10. Consensus Protocol (i.e., Plenum) => An Implementation of the Redundant Byzantine Fault Tolerance

# Sovrin Foundation

https://www.evernym.com/wp-content/uploads/2017/07/The-Technical-Foundations-of-Sovrin.pdf



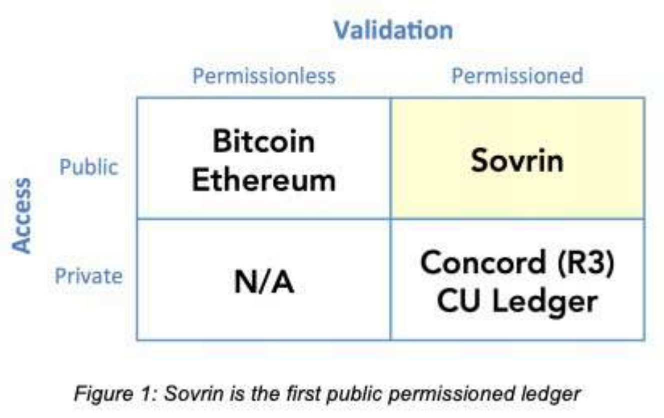
# The Technical Foundations of Sovrin

A White Paper from the Sovrin Foundation

Drummond Reed, Jason Law & Daniel Hardman

29th September 2016

sovrin.org



| | | Validation | |
|---|---|---|---|
| | | Permissionless | Permissioned |
| Access | Public | Bitcoin<br>Ethereum | Sovrin |
| | Private | N/A | Concord (R3)<br>CU Ledger |

*Figure 1: Sovrin is the first public permissioned ledger*

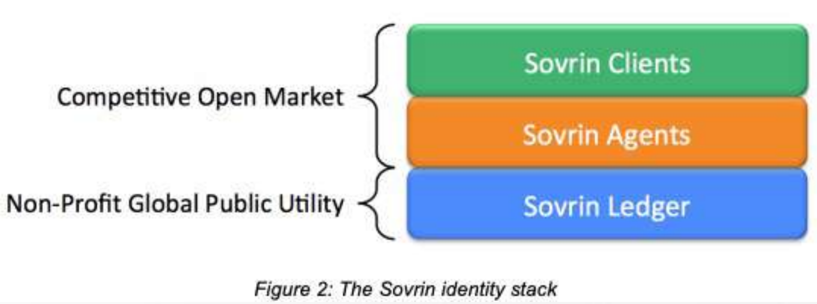
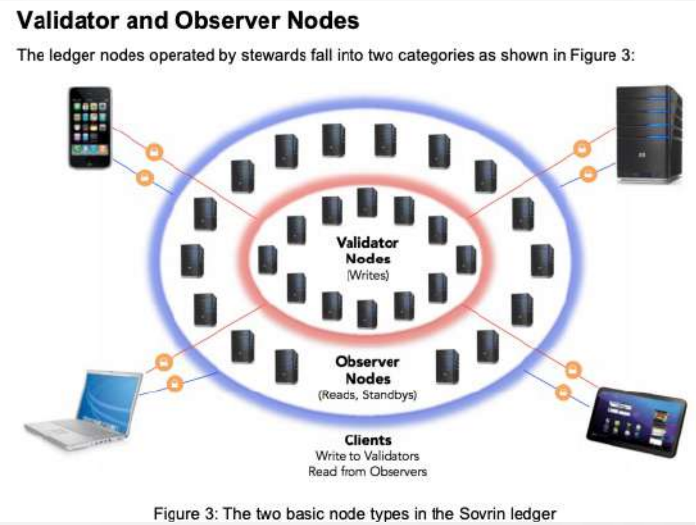


*Figure 2: The Sovrin identity stack*



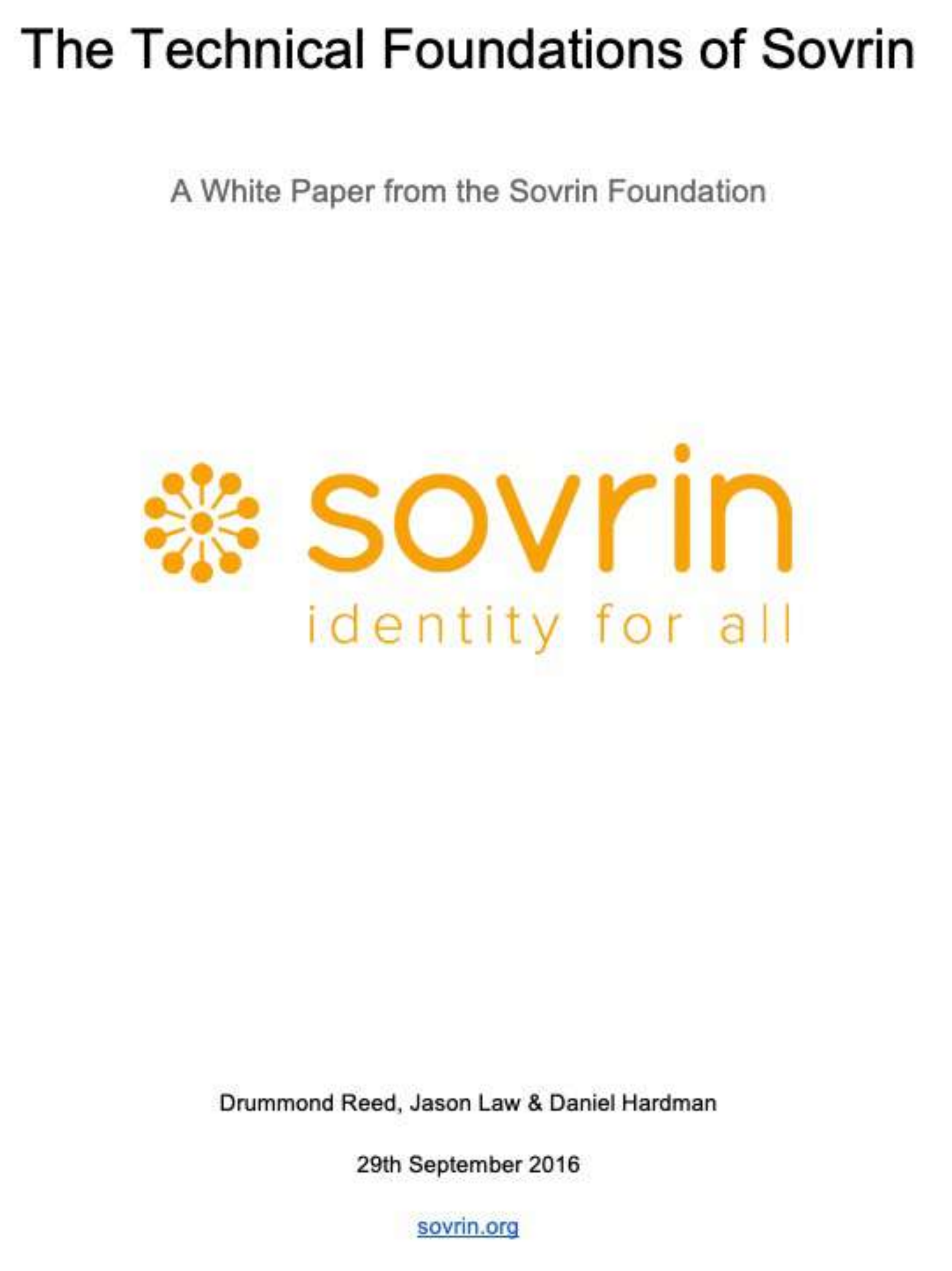
### Validator and Observer Nodes

The ledger nodes operated by stewards fall into two categories as shown in Figure 3:

Figure 3: The two basic node types in the Sovrin ledger

# Sovrin Foundation

https://www.evernym.com/wp-content/uploads/2017/07/The-Technical-Foundations-of-Sovrin.pdf



## The Technical Foundations of Sovrin

A White Paper from the Sovrin Foundation

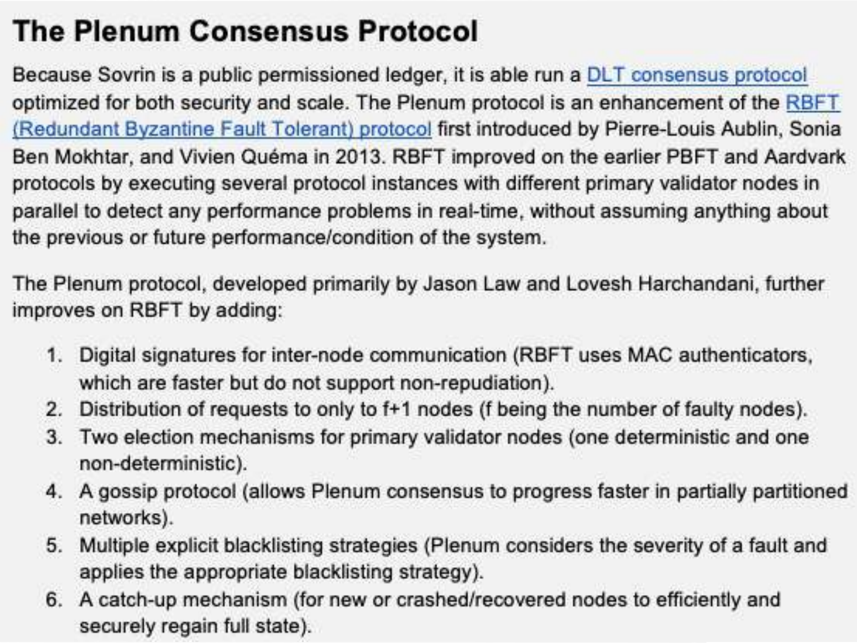
sovrin

identity for all

Drummond Reed, Jason Law & Daniel Hardman

29th September 2016

sovrin.org

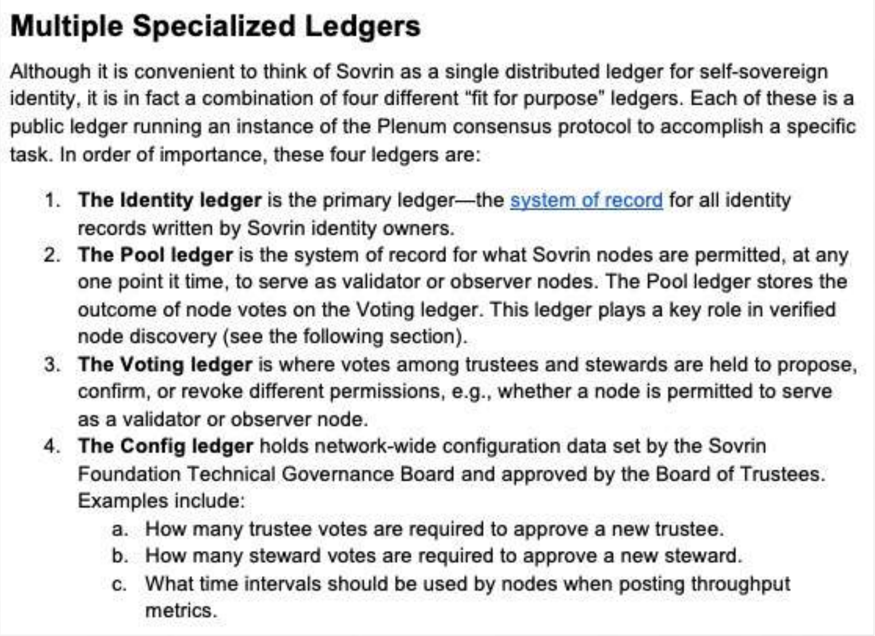


### The Plenum Consensus Protocol

Because Sovrin is a public permissioned ledger, it is able run a DLT consensus protocol optimized for both security and scale. The Plenum protocol is an enhancement of the RBFT (Redundant Byzantine Fault Tolerant) protocol first introduced by Pierre-Louis Aublin, Sonia Ben Mokhtar, and Vivien Quéma in 2013. RBFT improved on the earlier PBFT and Aardvark protocols by executing several protocol instances with different primary validator nodes in parallel to detect any performance problems in real-time, without assuming anything about the previous or future performance/condition of the system.

The Plenum protocol, developed primarily by Jason Law and Lovesh Harchandani, further improves on RBFT by adding:

1. Digital signatures for inter-node communication (RBFT uses MAC authenticators, which are faster but do not support non-repudiation).
2. Distribution of requests to only to f+1 nodes (f being the number of faulty nodes).
3. Two election mechanisms for primary validator nodes (one deterministic and one non-deterministic).
4. A gossip protocol (allows Plenum consensus to progress faster in partially partitioned networks).
5. Multiple explicit blacklisting strategies (Plenum considers the severity of a fault and applies the appropriate blacklisting strategy).
6. A catch-up mechanism (for new or crashed/recovered nodes to efficiently and securely regain full state).



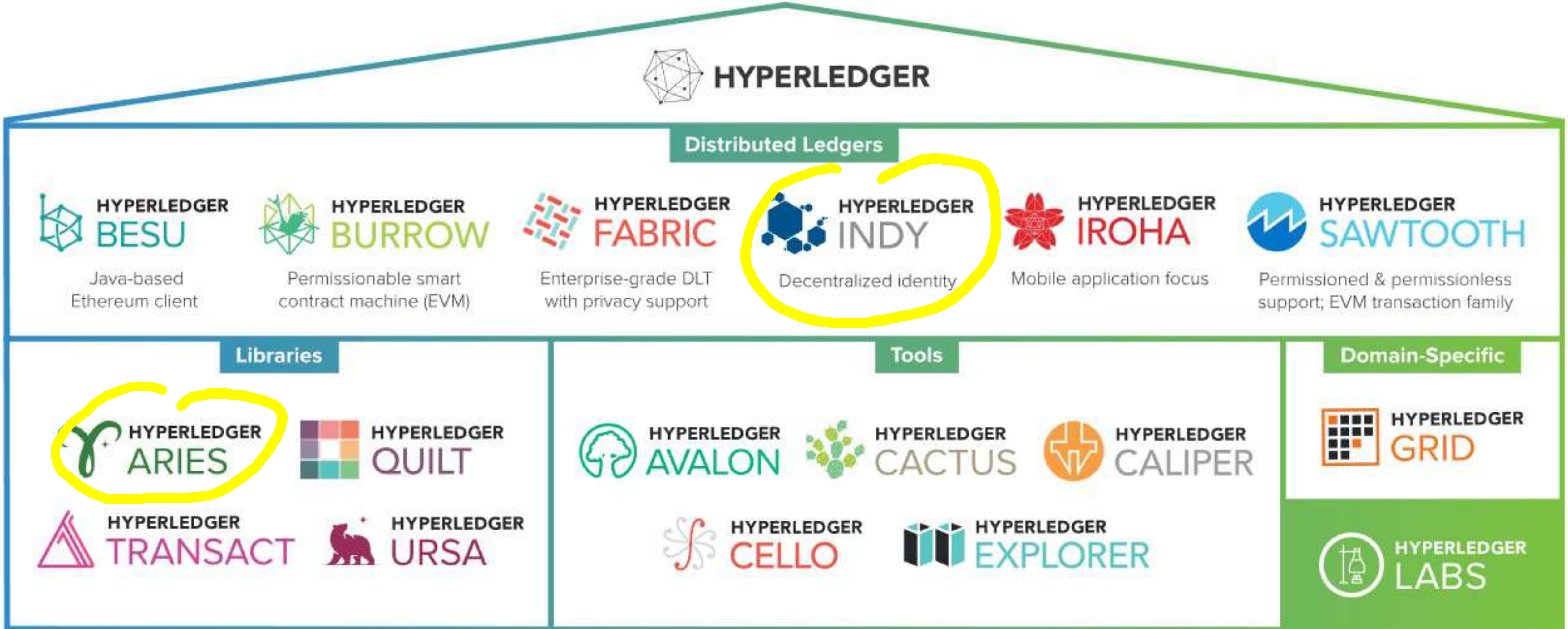
### Multiple Specialized Ledgers

Although it is convenient to think of Sovrin as a single distributed ledger for self-sovereign identity, it is in fact a combination of four different “fit for purpose” ledgers. Each of these is a public ledger running an instance of the Plenum consensus protocol to accomplish a specific task. In order of importance, these four ledgers are:

1. **The Identity ledger** is the primary ledger—the system of record for all identity records written by Sovrin identity owners.
2. **The Pool ledger** is the system of record for what Sovrin nodes are permitted, at any one point it time, to serve as validator or observer nodes. The Pool ledger stores the outcome of node votes on the Voting ledger. This ledger plays a key role in verified node discovery (see the following section).
3. **The Voting ledger** is where votes among trustees and stewards are held to propose, confirm, or revoke different permissions, e.g., whether a node is permitted to serve as a validator or observer node.
4. **The Config ledger** holds network-wide configuration data set by the Sovrin Foundation Technical Governance Board and approved by the Board of Trustees. Examples include:
   a. How many trustee votes are required to approve a new trustee.
   b. How many steward votes are required to approve a new steward.
   c. What time intervals should be used by nodes when posting throughput metrics.

# UNJSPF - UNICC - Hyperledger

**UNICC** is an Associate Member of Hyperledger and the Linux Foundation



HYPERLEDGER

## Distributed Ledgers

- HYPERLEDGER BESU — Java-based Ethereum client
- HYPERLEDGER BURROW — Permissionable smart contract machine (EVM)
- HYPERLEDGER FABRIC — Enterprise-grade DLT with privacy support
- HYPERLEDGER INDY — Decentralized identity
- HYPERLEDGER IROHA — Mobile application focus
- HYPERLEDGER SAWTOOTH — Permissioned & permissionless support; EVM transaction family

## Libraries

- HYPERLEDGER ARIES
- HYPERLEDGER QUILT
- HYPERLEDGER TRANSACT
- HYPERLEDGER URSA

## Tools

- HYPERLEDGER AVALON
- HYPERLEDGER CACTUS
- HYPERLEDGER CALIPER
- HYPERLEDGER CELLO
- HYPERLEDGER EXPLORER

## Domain-Specific

- HYPERLEDGER GRID

HYPERLEDGER LABS

# Hyperledger Indy Framework & Aries Libraries

HYPERLEDGER INDY

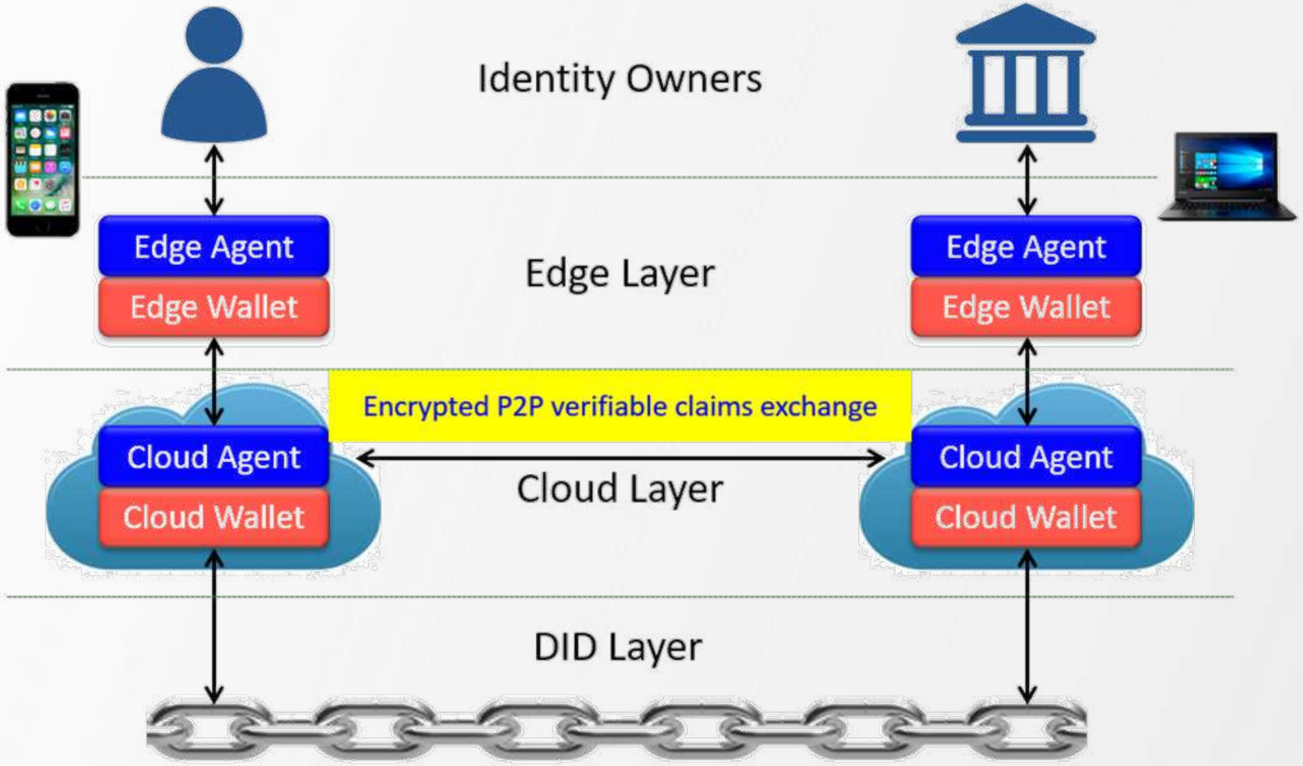
Donated to Hyperledger by the Sovrin Foundation

Digital ID and Verifiable Credentials Store

Elements

- Agent
- Wallet
- Blockchain

HYPERLEDGER ARIES

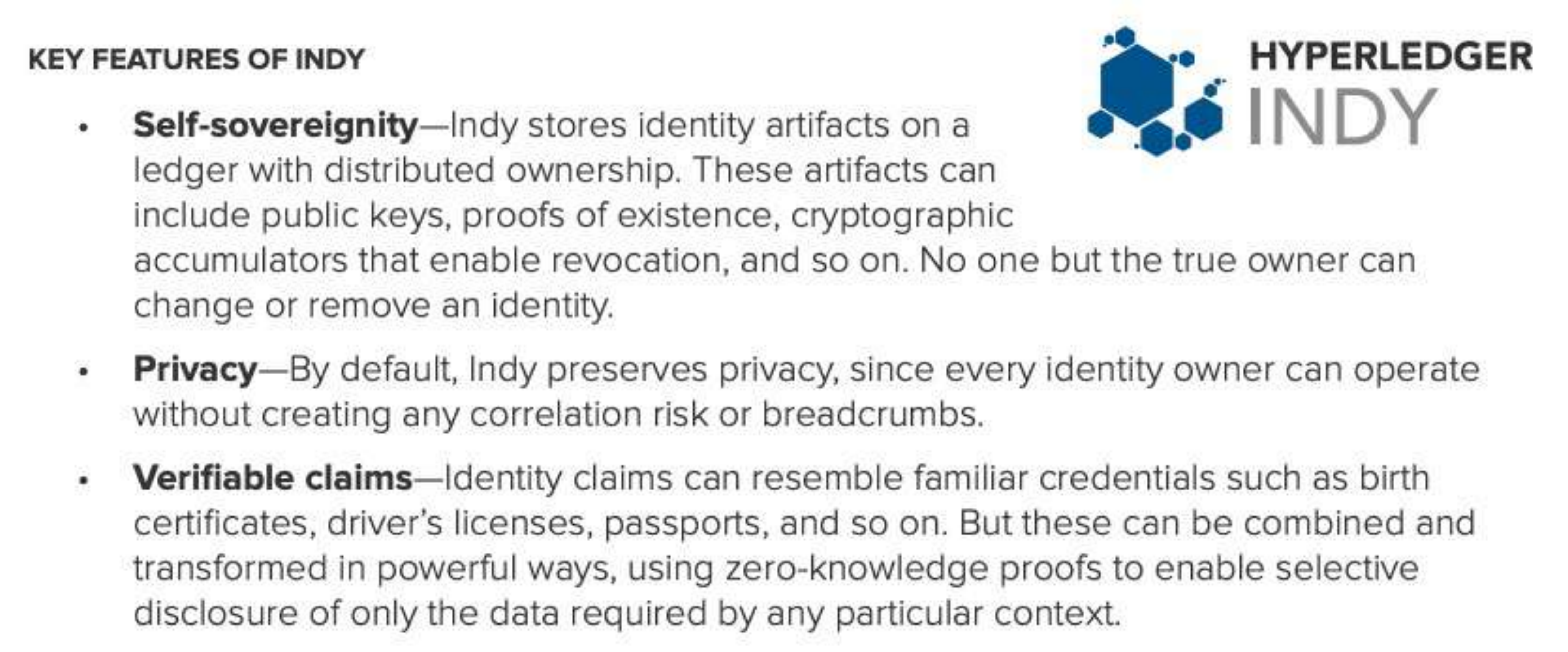


Licensed under CC by 4.0

https://indyscan.io/txs/SOVRIN_MAINNET/domain

# Hyperledger Indy

(https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf)



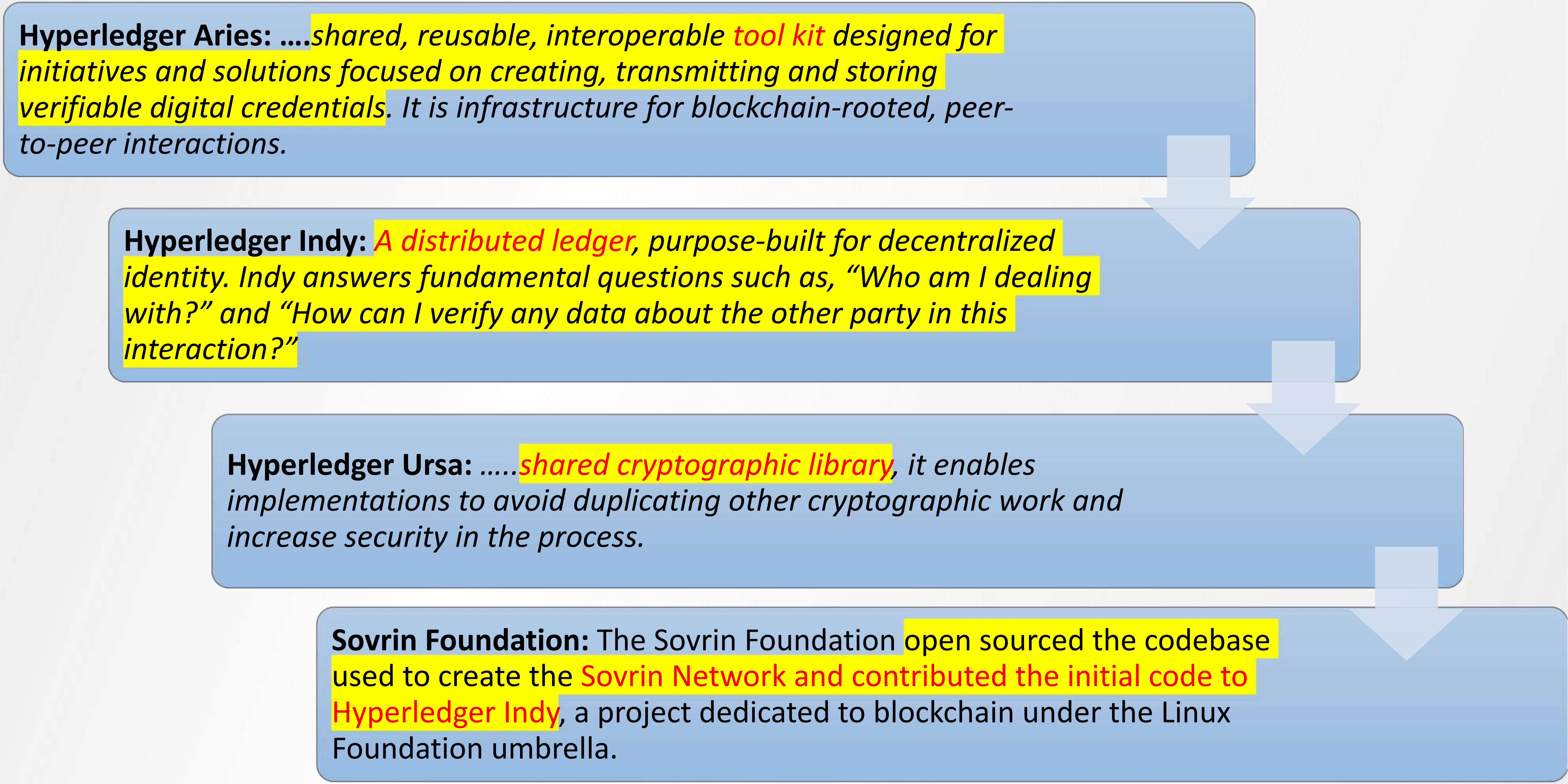
HYPERLEDGER INDY

KEY FEATURES OF INDY

- **Self-sovereignity**—Indy stores identity artifacts on a ledger with distributed ownership. These artifacts can include public keys, proofs of existence, cryptographic accumulators that enable revocation, and so on. No one but the true owner can change or remove an identity.
- **Privacy**—By default, Indy preserves privacy, since every identity owner can operate without creating any correlation risk or breadcrumbs.
- **Verifiable claims**—Identity claims can resemble familiar credentials such as birth certificates, driver's licenses, passports, and so on. But these can be combined and transformed in powerful ways, using zero-knowledge proofs to enable selective disclosure of only the data required by any particular context.

# Sovrin/Hyperledger: Key Components

www.hyperledger.org - https://sovrin.org/faqs/



**Hyperledger Aries:** ….*shared, reusable, interoperable tool kit designed for initiatives and solutions focused on creating, transmitting and storing verifiable digital credentials. It is infrastructure for blockchain-rooted, peer-to-peer interactions.*

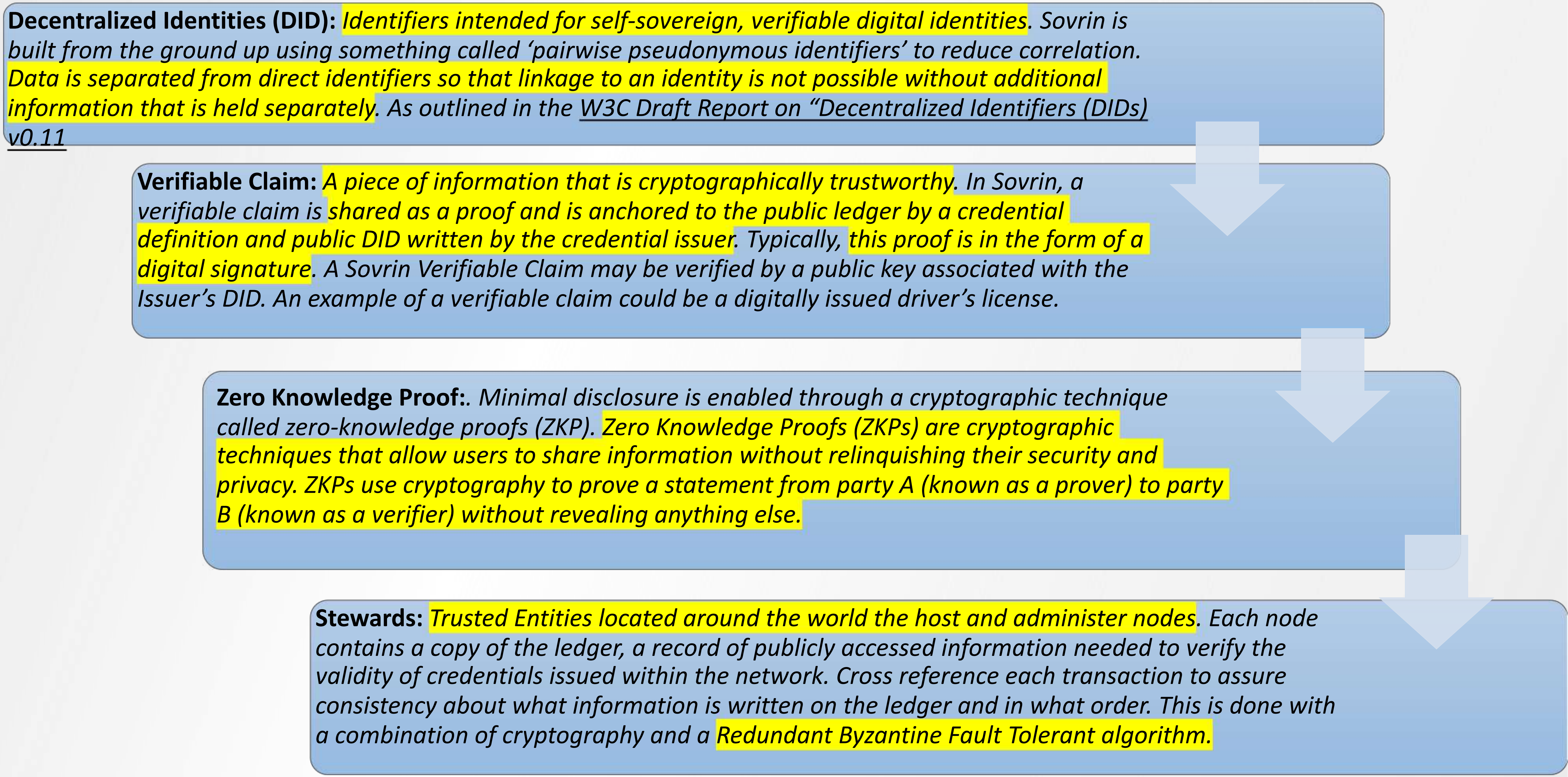
**Hyperledger Indy:** *A distributed ledger, purpose-built for decentralized identity. Indy answers fundamental questions such as, “Who am I dealing with?” and “How can I verify any data about the other party in this interaction?”*

**Hyperledger Ursa:** …..*shared cryptographic library, it enables implementations to avoid duplicating other cryptographic work and increase security in the process.*

**Sovrin Foundation:** The Sovrin Foundation open sourced the codebase used to create the Sovrin Network and contributed the initial code to Hyperledger Indy, a project dedicated to blockchain under the Linux Foundation umbrella.

# Key Definitions

www.hyperledger.org - https://sovrin.org/faqs/



**Decentralized Identities (DID):** *Identifiers intended for self-sovereign, verifiable digital identities. Sovrin is built from the ground up using something called 'pairwise pseudonymous identifiers' to reduce correlation. Data is separated from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. As outlined in the W3C Draft Report on "Decentralized Identifiers (DIDs) v0.11*

**Verifiable Claim:** *A piece of information that is cryptographically trustworthy. In Sovrin, a verifiable claim is shared as a proof and is anchored to the public ledger by a credential definition and public DID written by the credential issuer. Typically, this proof is in the form of a digital signature. A Sovrin Verifiable Claim may be verified by a public key associated with the Issuer's DID. An example of a verifiable claim could be a digitally issued driver's license.*

**Zero Knowledge Proof:**. *Minimal disclosure is enabled through a cryptographic technique called zero-knowledge proofs (ZKP). Zero Knowledge Proofs (ZKPs) are cryptographic techniques that allow users to share information without relinquishing their security and privacy. ZKPs use cryptography to prove a statement from party A (known as a prover) to party B (known as a verifier) without revealing anything else.*

**Stewards:** *Trusted Entities located around the world the host and administer nodes. Each node contains a copy of the ledger, a record of publicly accessed information needed to verify the validity of credentials issued within the network. Cross reference each transaction to assure consistency about what information is written on the ledger and in what order. This is done with a combination of cryptography and a Redundant Byzantine Fault Tolerant algorithm.*

# Hyperledger Indy: Key Definitions

**DID**: A globally-unique identifier for an entity or individual owner that is not managed by a centralized authority but can be registered with the distributed ledger (https://w3c-ccg.github.io/did-spec/#dfn-dlt), the technology's decentralized network, and resolvable on the ledger without requiring any centralized authority.

To maintain privacy, an entity or identity owner can own multiple DIDs. The DID in Indy has the following characters:

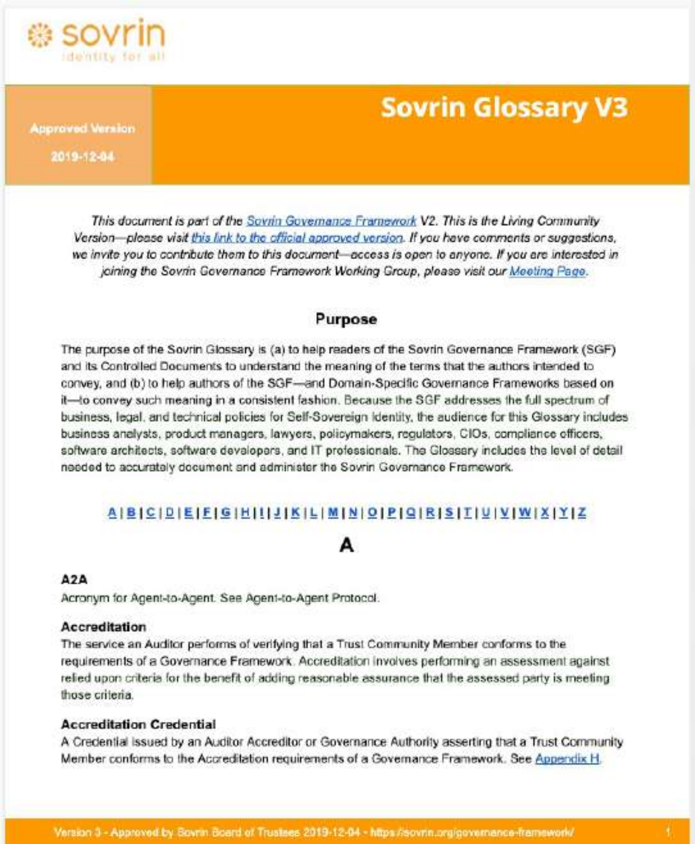
- Persistency
- Globally resolvable
- Cryptographically verifiable
- Decentralized

Hyperledger Indy => 2 two types of DID

- **Verinym:** Unique identifier of a legal identity or identity owner.

- **Pseudonym:** Used to maintain the privacy of a digital relationship or connection between participants. If the pseudonym is used to maintain only one digital relationship, it is also called a **pairwise identifier**, which maintains secure connections between two participants.

ADDITIONAL DEFINITIONS =>
https://docs.google.com/document/d/1gflz5TT0cNp2kxGMLFXr19x1uoZsruUe_0glHst2fZ8/edit



sovrin
identity for all

Approved Version
2019-12-04

## Sovrin Glossary V3

*This document is part of the Sovrin Governance Framework V2. This is the Living Community Version—please visit this link to the official approved version. If you have comments or suggestions, we invite you to contribute them to this document—access is open to anyone. If you are interested in joining the Sovrin Governance Framework Working Group, please visit our Meeting Page.*

### Purpose

The purpose of the Sovrin Glossary is (a) to help readers of the Sovrin Governance Framework (SGF) and its Controlled Documents to understand the meaning of the terms that the authors intended to convey, and (b) to help authors of the SGF—and Domain-Specific Governance Frameworks based on it—to convey such meaning in a consistent fashion. Because the SGF addresses the full spectrum of business, legal, and technical policies for Self-Sovereign Identity, the audience for this Glossary includes business analysts, product managers, lawyers, policymakers, regulators, CIOs, compliance officers, software architects, software developers, and IT professionals. The Glossary includes the level of detail needed to accurately document and administer the Sovrin Governance Framework.

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

### A

**A2A**
Acronym for Agent-to-Agent. See Agent-to-Agent Protocol.

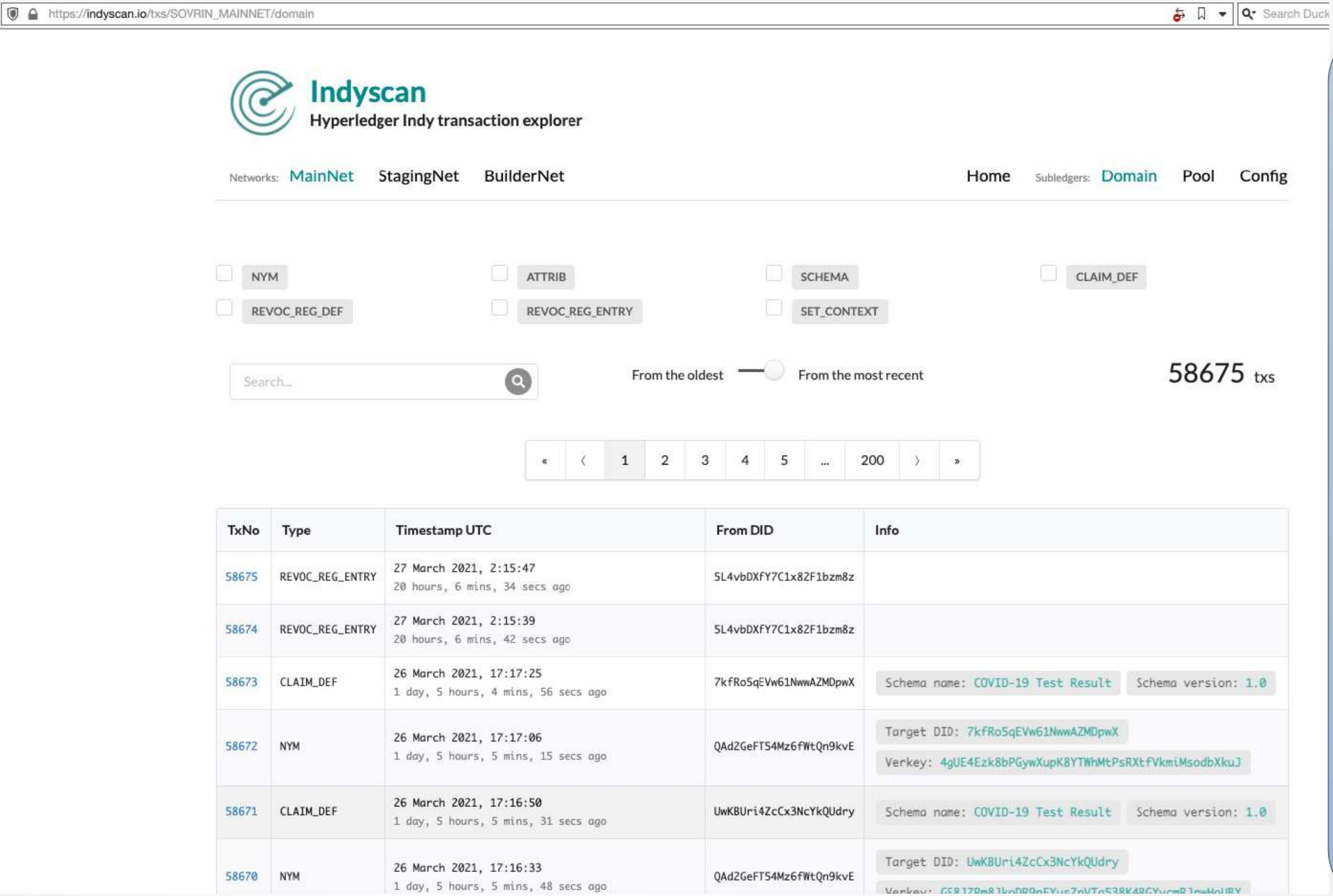
**Accreditation**
The service an Auditor performs of verifying that a Trust Community Member conforms to the requirements of a Governance Framework. Accreditation involves performing an assessment against relied upon criteria for the benefit of adding reasonable assurance that the assessed party is meeting those criteria.

**Accreditation Credential**
A Credential issued by an Auditor Accreditor or Governance Authority asserting that a Trust Community Member conforms to the Accreditation requirements of a Governance Framework. See Appendix H.

Version 3 - Approved by Sovrin Board of Trustees 2019-12-04 - https://sovrin.org/governance-framework/ 1

# Hyperledger Indyscan.io

https://indyscan.io/txs/SOVRIN_MAINNET/domain



https://indyscan.io/txs/SOVRIN_MAINNET/domain

Indyscan

Hyperledger Indy transaction explorer

Networks: MainNet StagingNet BuilderNet

Home Subledgers: Domain Pool Config

□ NYM □ ATTRIB □ SCHEMA □ CLAIM_DEF

□ REVOC_REG_DEF □ REVOC_REG_ENTRY □ SET_CONTEXT

Search...

From the oldest ○ From the most recent

58675 txs

« ‹ 1 2 3 4 5 ... 200 › »

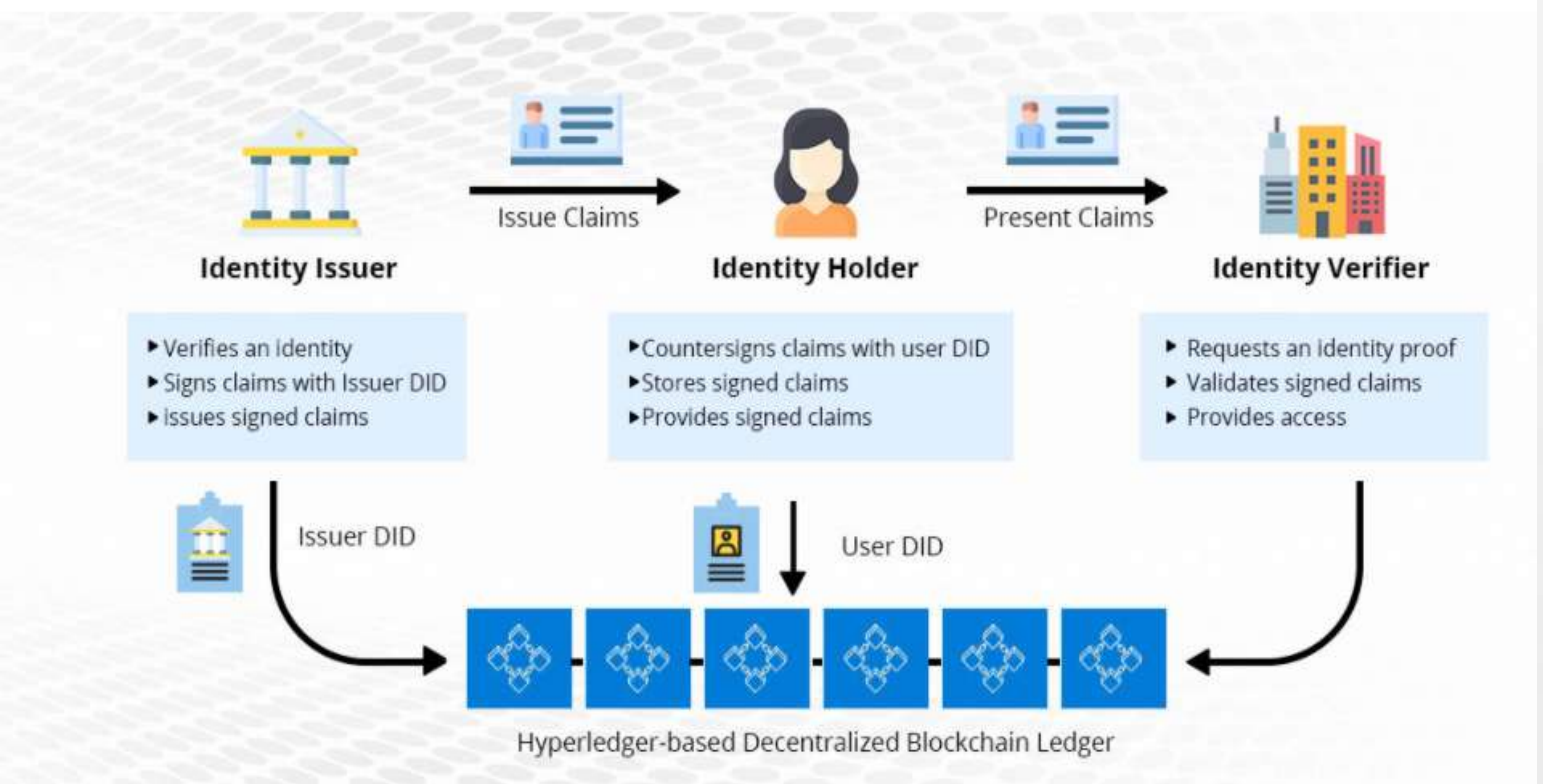
| TxNo | Type | Timestamp UTC | From DID | Info |
|---|---|---|---|---|
| 58675 | REVOC_REG_ENTRY | 27 March 2021, 2:15:47<br>20 hours, 6 mins, 34 secs ago | 5L4vbDXfY7C1x82F1bzm8z | |
| 58674 | REVOC_REG_ENTRY | 27 March 2021, 2:15:39<br>20 hours, 6 mins, 42 secs ago | 5L4vbDXfY7C1x82F1bzm8z | |
| 58673 | CLAIM_DEF | 26 March 2021, 17:17:25<br>1 day, 5 hours, 4 mins, 56 secs ago | 7kfRo5qEVw61NwwAZMDpwX | Schema name: COVID-19 Test Result<br>Schema version: 1.0 |
| 58672 | NYM | 26 March 2021, 17:17:06<br>1 day, 5 hours, 5 mins, 15 secs ago | QAd2GeFT54Mz6fWtQn9kvE | Target DID: 7kfRo5qEVw61NwwAZMDpwX<br>Verkey: 4gUE4Ezk8bPGywXupK8YTWhMtPsRXtfVkmiMsodbXkuJ |
| 58671 | CLAIM_DEF | 26 March 2021, 17:16:50<br>1 day, 5 hours, 5 mins, 31 secs ago | UwKBUri4ZcCx3NcYkQUdry | Schema name: COVID-19 Test Result<br>Schema version: 1.0 |
| 58670 | NYM | 26 March 2021, 17:16:33<br>1 day, 5 hours, 5 mins, 48 secs ago | QAd2GeFT54Mz6fWtQn9kvE | Target DID: UwKBUri4ZcCx3NcYkQUdry<br>Verkey: GF8JZRm8JkoDR9nFYusZnVTq538K4RGYxcmRJrwHoURY |

**BROWSING DETAILS** => SOVRIN Production MainNet

- **NO QUERIES** but YOU CAN DOWNLOAD THE LEDGER
- **3 LEDGERS:**
  - 1. DOMAIN TRANSACTIONS:
    - DIDs
    - Credential Schemas
    - Credential Definitions
  - 2. POOL = Tracks All the Nodes the Verify (Consensus) and Write on the Ledger
  - 3. CONFIG = Tracks Upgrades and Changes to the algorithm; New Nodes; etc.
- **ATTRIB** = Transactions written by Stewards to ensure the ledger is operating as expected
- **NYM** = DIDs
- **SCHEMA** = Defined by the Issuers
- **CLAIM_DEF** = Credential Definitions (linked to schemas)

# The Blockchain Platform: Key Components of Hyperledger Indy

(from Hyperledger.org)



**Identity Issuer**

- Verifies an identity
- Signs claims with Issuer DID
- issues signed claims

**Identity Holder**

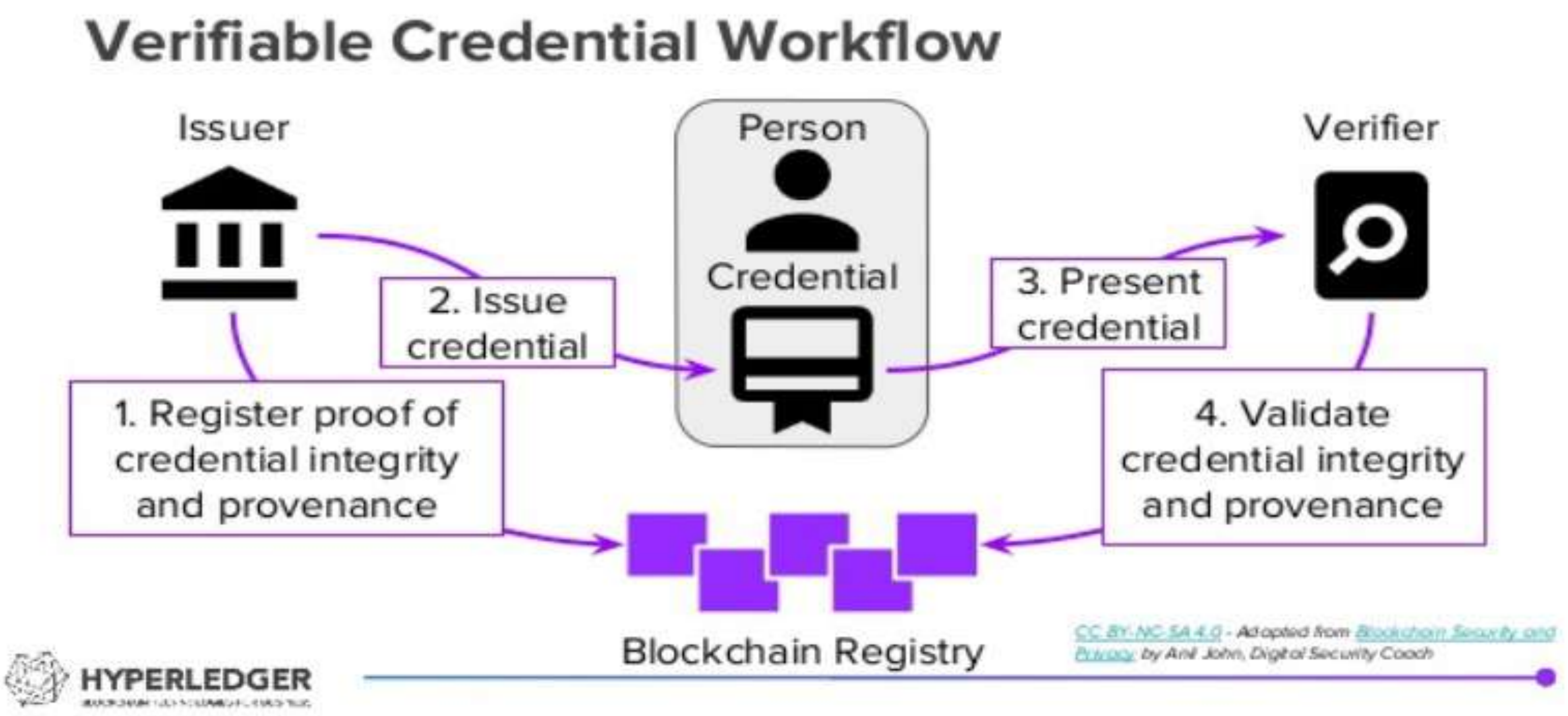
- Countersigns claims with user DID
- Stores signed claims
- Provides signed claims

**Identity Verifier**

- Requests an identity proof
- Validates signed claims
- Provides access

Hyperledger-based Decentralized Blockchain Ledger

# Verifiable Credentials



## Verifiable Credential Workflow

Issuer

Person

Credential

Verifier

2. Issue credential

3. Present credential

1. Register proof of credential integrity and provenance

4. Validate credential integrity and provenance

Blockchain Registry

CC BY-NC-SA 4.0 - Adopted from Blockchain Security and Privacy by Anil John, Digital Security Coach

HYPERLEDGER

# UNJSPF Digital Certificate of Entitlement

Walkthrough

# Basic Terms and Concepts: Agents – Wallets - Blockchain

**Hyperledger Indy and Aries**

Support the creation and storage of Digital Identifiers and Verifiable Credentials

**Elements**

Agent

A piece of software that interacts with the blockchain and users

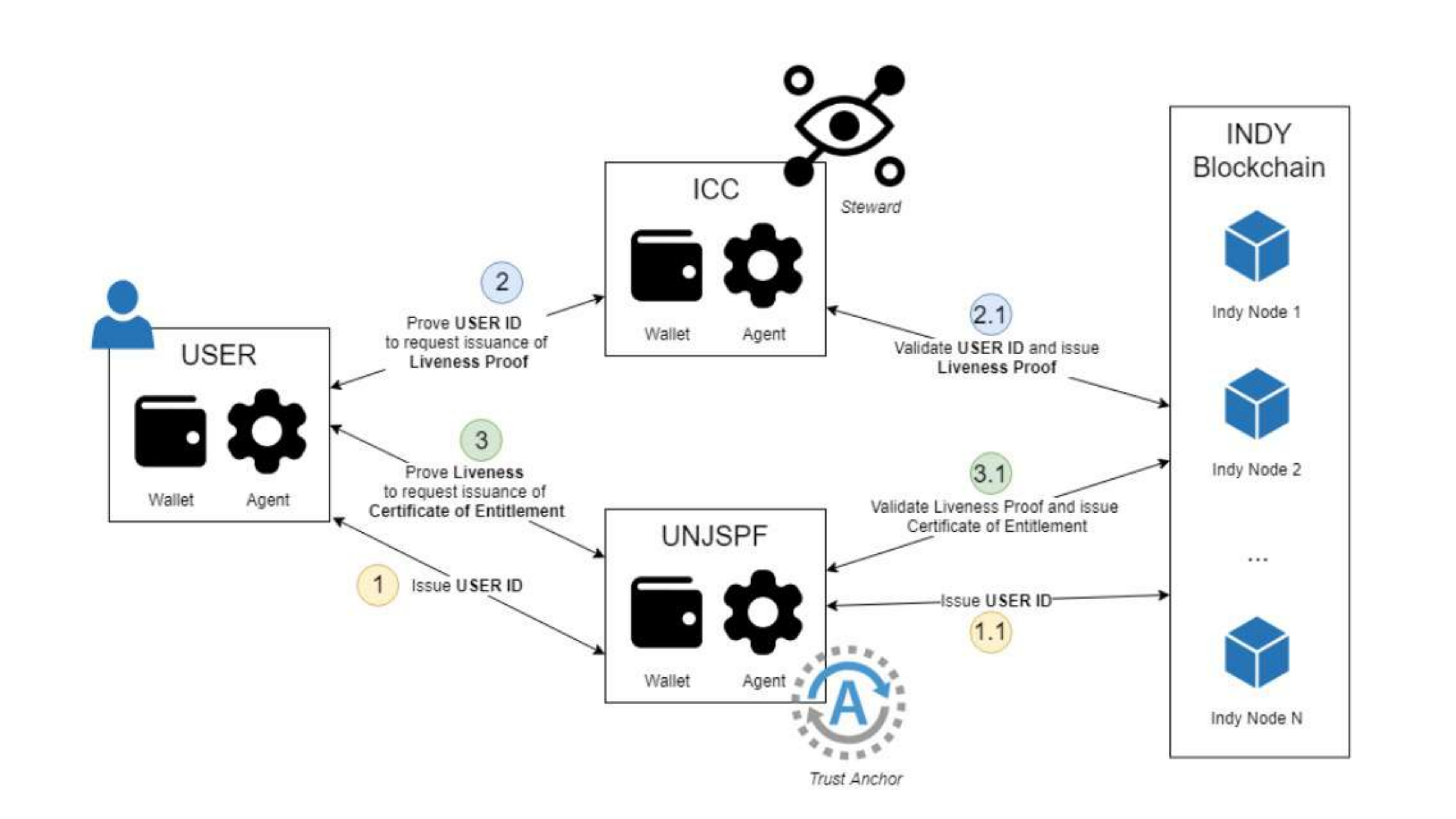
Wallet

A piece of software that safeguards private keys

Blockchain

A distributed ledger, purpose-built for decentralized identity

# Basic Terms and Concepts: Actors and Main Relationships


ICC
Wallet
Agent
Steward
INDY Blockchain
Indy Node 1
Indy Node 2
...
Indy Node N
USER
Wallet
Agent
2
Prove USER ID to request issuance of Liveness Proof
2.1
Validate USER ID and issue Liveness Proof
3
Prove Liveness to request issuance of Certificate of Entitlement
3.1
Validate Liveness Proof and issue Certificate of Entitlement
UNJSPF
Wallet
Agent
1
Issue USER ID
Issue USER ID
1.1
Trust Anchor

# Basic Terms and Concepts: Steward – Onboarding and Trust Anchor

**Steward**

The **Steward** can onboard new actors in the system and assign role to them.

**In the Digital CE process, the Steward (UNICC):**

**Onboards UNJSPF**

Onboarding involves creating a pairwise-unique identity (DID) between two parties. **Pairwise-unique identity** is a pair of DIDs, each owned by one party. This pair of DID is unique because it is only used for communication between these two parties. Each DID is created with a signing key, a verifying key (Verkey), and a DID. Signing key is the private key, kept as secret and stored in wallet. Both the Verkey and DID are public information and are recorded to the ledger for public access.

The pairwise-unique DID is not used for interacting with the ledger. They need another DID (called Verinym) that can identify themselves in the ledger and a role of Trust Anchor.

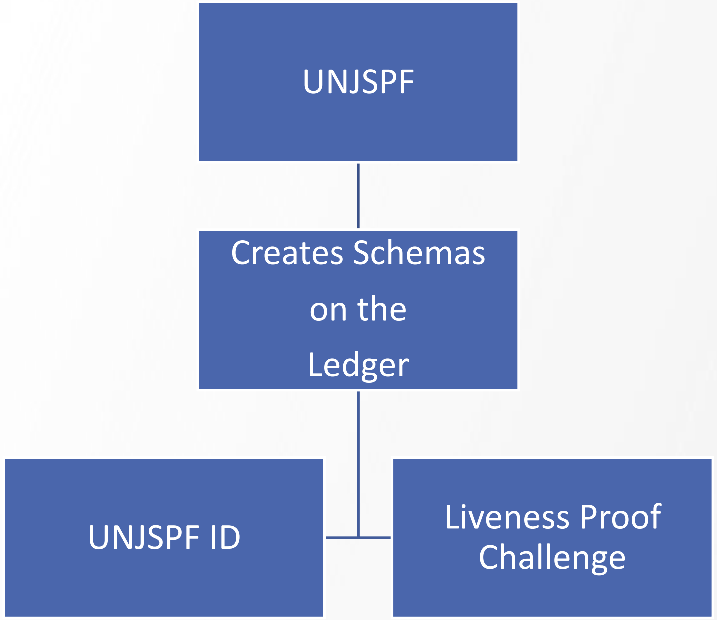
**Grants UNJSPF a Verinym and the Trust Anchor Role**

The Steward will record the DID and Verkey of UNJSPF on the ledger and sets its the role as Trust Anchor.

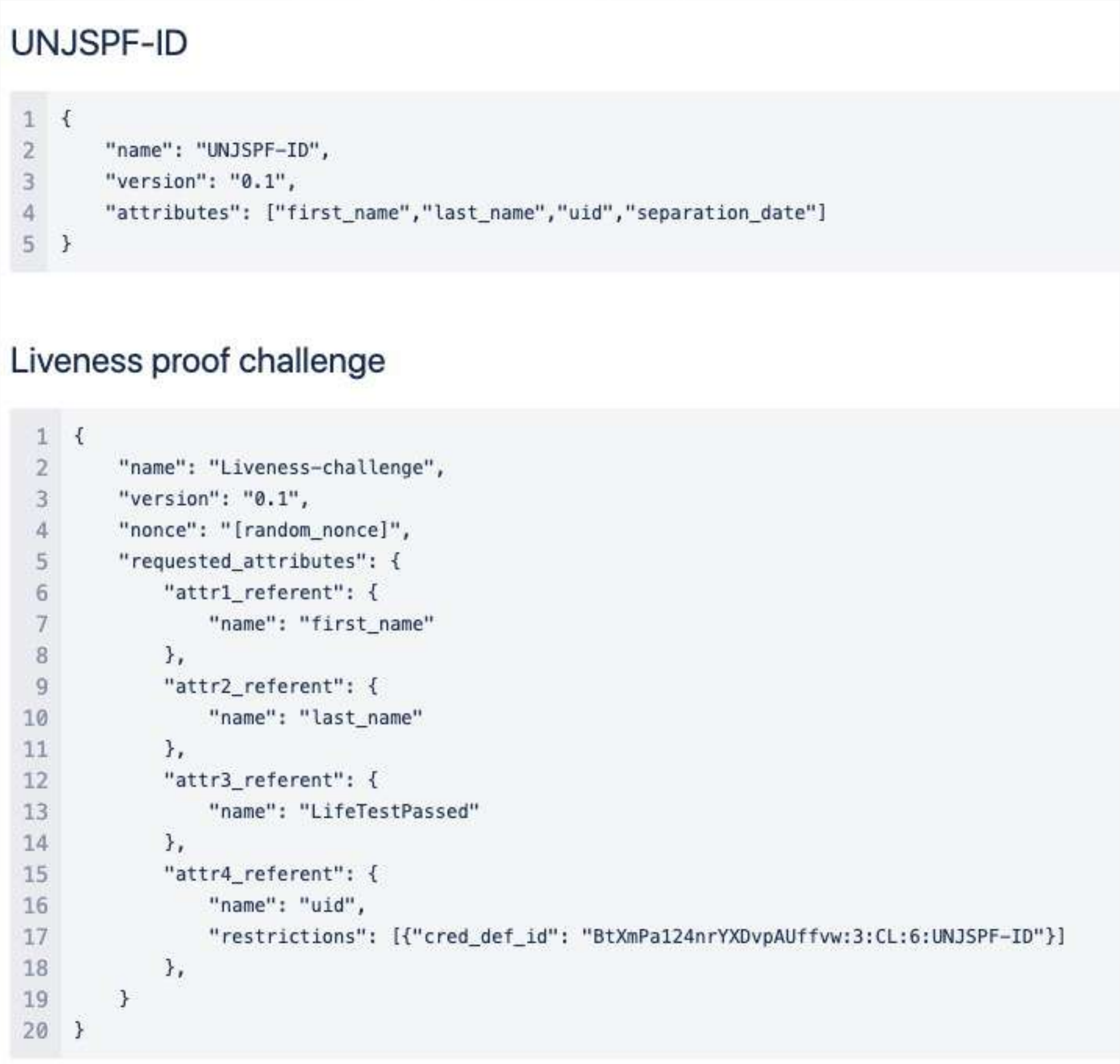
From now on, UNJSPF is fully functioning, with a DID representing itself and its role of Trust Anchor.

# Implementation Step 1: UNJSPF creates two “Schemas” on the Blockchain

UNJSPF creates and issues the ”UNJSPF ID” and “Liveness Proof Challenge” schemas and records them on the ledger. Schemas are visible by everyone.



# Implementation Step 1: UNJSPF creates two “Schemas”



## UNJSPF-ID

```
{
    "name": "UNJSPF-ID",
    "version": "0.1",
    "attributes": ["first_name","last_name","uid","separation_date"]
}
```

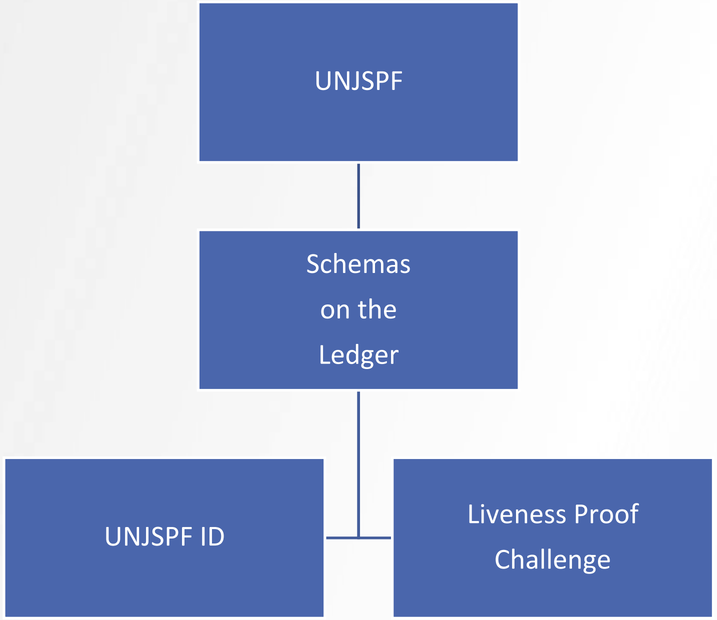
## Liveness proof challenge

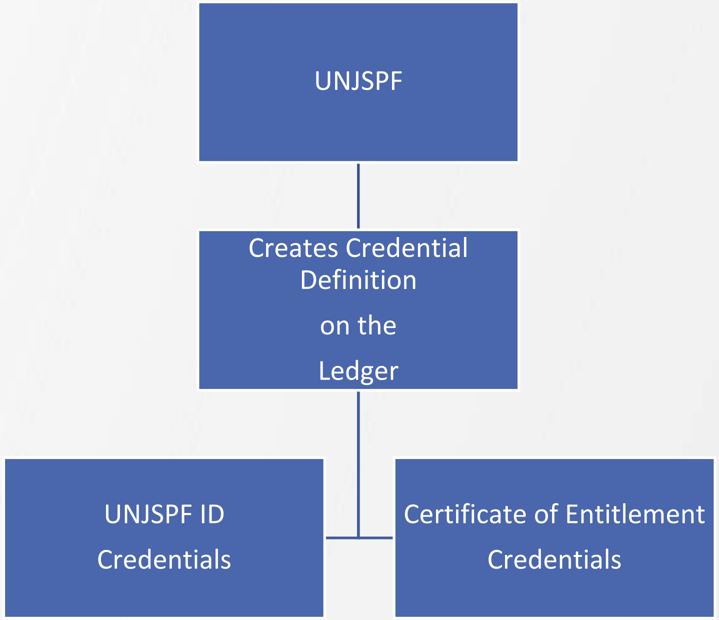
```
{
    "name": "Liveness-challenge",
    "version": "0.1",
    "nonce": "[random_nonce]",
    "requested_attributes": {
        "attr1_referent": {
            "name": "first_name"
        },
        "attr2_referent": {
            "name": "last_name"
        },
        "attr3_referent": {
            "name": "LifeTestPassed"
        },
        "attr4_referent": {
            "name": "uid",
            "restrictions": [{"cred_def_id": "BtXmPa124nrYXDvpAUffvw:3:CL:6:UNJSPF-ID"}]
        },
    }
}
```

# Implementation Step 2: UNJSPF creates the "Credential Definitions on the Blockchain"

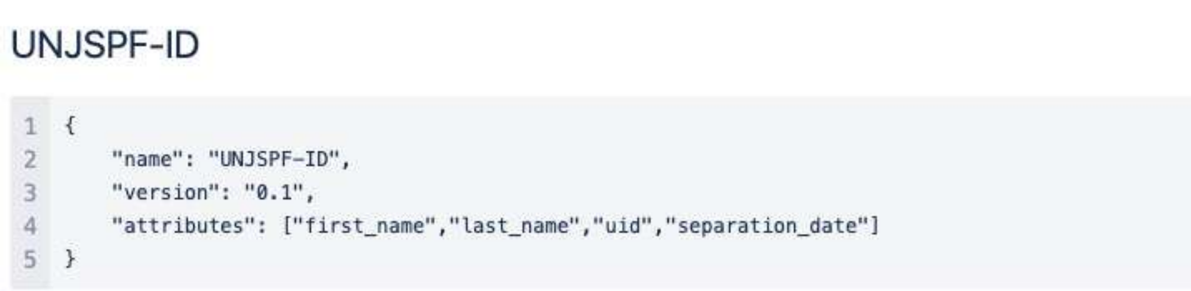
Credentials are defined in accordance with the corresponding schema defined in Step 1, plus the identifying information about the issuer of the "Credential Definitions".

In the Digital CE implementation, UNJSPF is both the issuer of the Schema and of the Credentials ("UNJSPF ID" and "Proof of Existence Challenge"), which are recorded on the ledger.



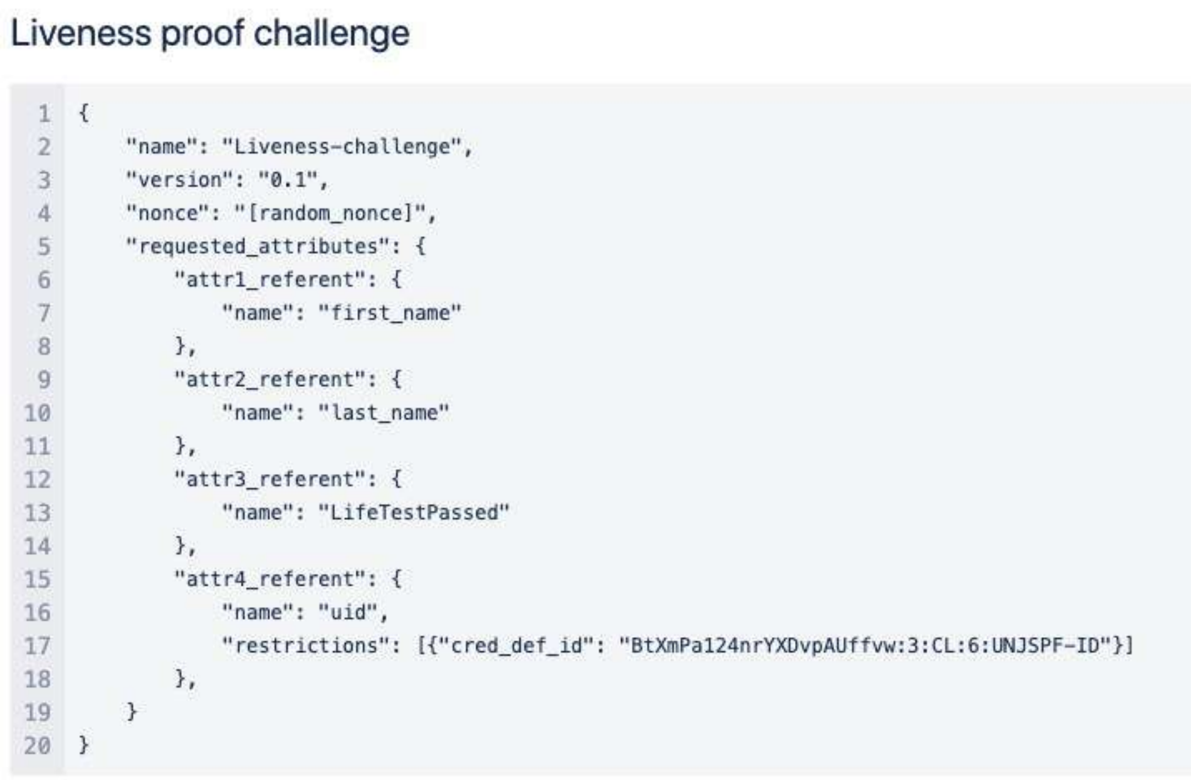

UNJSPF
Creates Credential Definition on the Ledger
UNJSPF ID Credentials
Certificate of Entitlement Credentials

# Implementation Step 2: Relationship between Schemas & Credentials



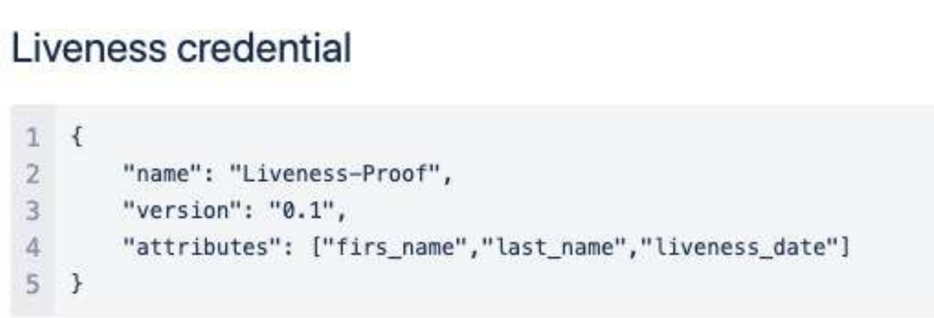
## UNJSPF-ID

```
{
    "name": "UNJSPF-ID",
    "version": "0.1",
    "attributes": ["first_name","last_name","uid","separation_date"]
}
```



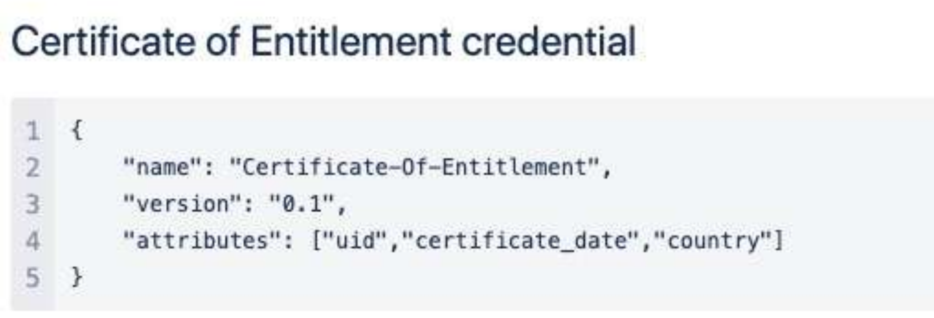
## Liveness proof challenge

```
{
    "name": "Liveness-challenge",
    "version": "0.1",
    "nonce": "[random_nonce]",
    "requested_attributes": {
        "attr1_referent": {
            "name": "first_name"
        },
        "attr2_referent": {
            "name": "last_name"
        },
        "attr3_referent": {
            "name": "LifeTestPassed"
        },
        "attr4_referent": {
            "name": "uid",
            "restrictions": [{"cred_def_id": "BtXmPa124nrYXDvpAUffvw:3:CL:6:UNJSPF-ID"}]
        },
    }
}
```



## Liveness credential

```
{
    "name": "Liveness-Proof",
    "version": "0.1",
    "attributes": ["firs_name","last_name","liveness_date"]
}
```



## Certificate of Entitlement credential

```
{
    "name": "Certificate-Of-Entitlement",
    "version": "0.1",
    "attributes": ["uid","certificate_date","country"]
}
```

# Implementation Step 3: Onboarding - The User obtains an ID from UNJSPF regarding his/her UNJSPF ID

**Detailed steps of the Onboarding process (which it is witnessed and attested by a UNJSPF Representative/Call Center Agent)**

- A connection is established between UNJSPF and the User.

- UNJSPF creates and sends a **UNJSPF Offer** to the User.

- The User (through its Agent/App on the smartphone):
    - Retrieves the "UNJSPF Credential Definition" from the ledger:
    - Creates a **Credential Request;** and
    - Sends the request to UNJSPF.

- UNJSPF issues the **Credential** for the User. The **Credential** contains the values of items listed in the "UNJSPF ID Credential Definition" (and UNJSPF Credential ID Schema), plus the required proof that the User can submit at a later stage in case of a verification (i.e., an independent audit entity).

- The User receives the **Credential** and stores it in his/her wallet (i.e., the Agent/App on the smartphone).

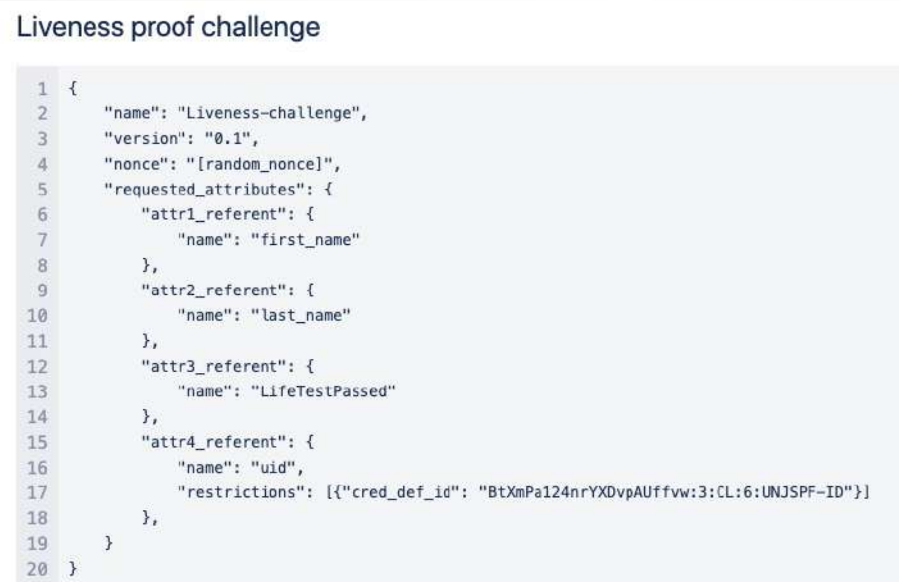
# Implementation Step 4: Users generate the “Proof of Existence” using the credential definitions already stored in their wallets (i.e., smartphones)

**Detailed steps:**

- A connection is established between the User (smartphone/Digital CE App) and UNJSPF (Digital CE System)

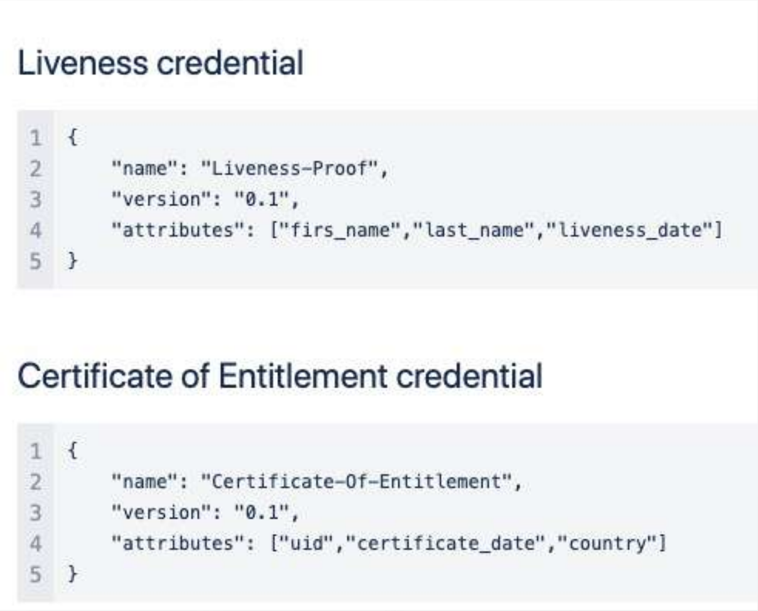
- UNJSPF creates a **“Proof of Existence”** offer for the year.

- Within a year, Users create a ”**Proof of Existence”** using the relevant credential definition already stored in their wallet (on their smartphone/Digital CE App). The proof will contain the relevant data originally defined in the schema “Proof of Existence Challenge”, as follows:



Liveness proof challenge

```
{
    "name": "Liveness-challenge",
    "version": "0.1",
    "nonce": "[random_nonce]",
    "requested_attributes": {
        "attr1_referent": {
            "name": "first_name"
        },
        "attr2_referent": {
            "name": "last_name"
        },
        "attr3_referent": {
            "name": "LifeTestPassed"
        },
        "attr4_referent": {
            "name": "uid",
            "restrictions": [{"cred_def_id": "BtXmPa124nrYXDvpAUffvw:3:CL:6:UNJSPF-ID"}]
        },
    }
}
```



Liveness credential

```
{
    "name": "Liveness-Proof",
    "version": "0.1",
    "attributes": ["firs_name","last_name","liveness_date"]
}
```

Certificate of Entitlement credential

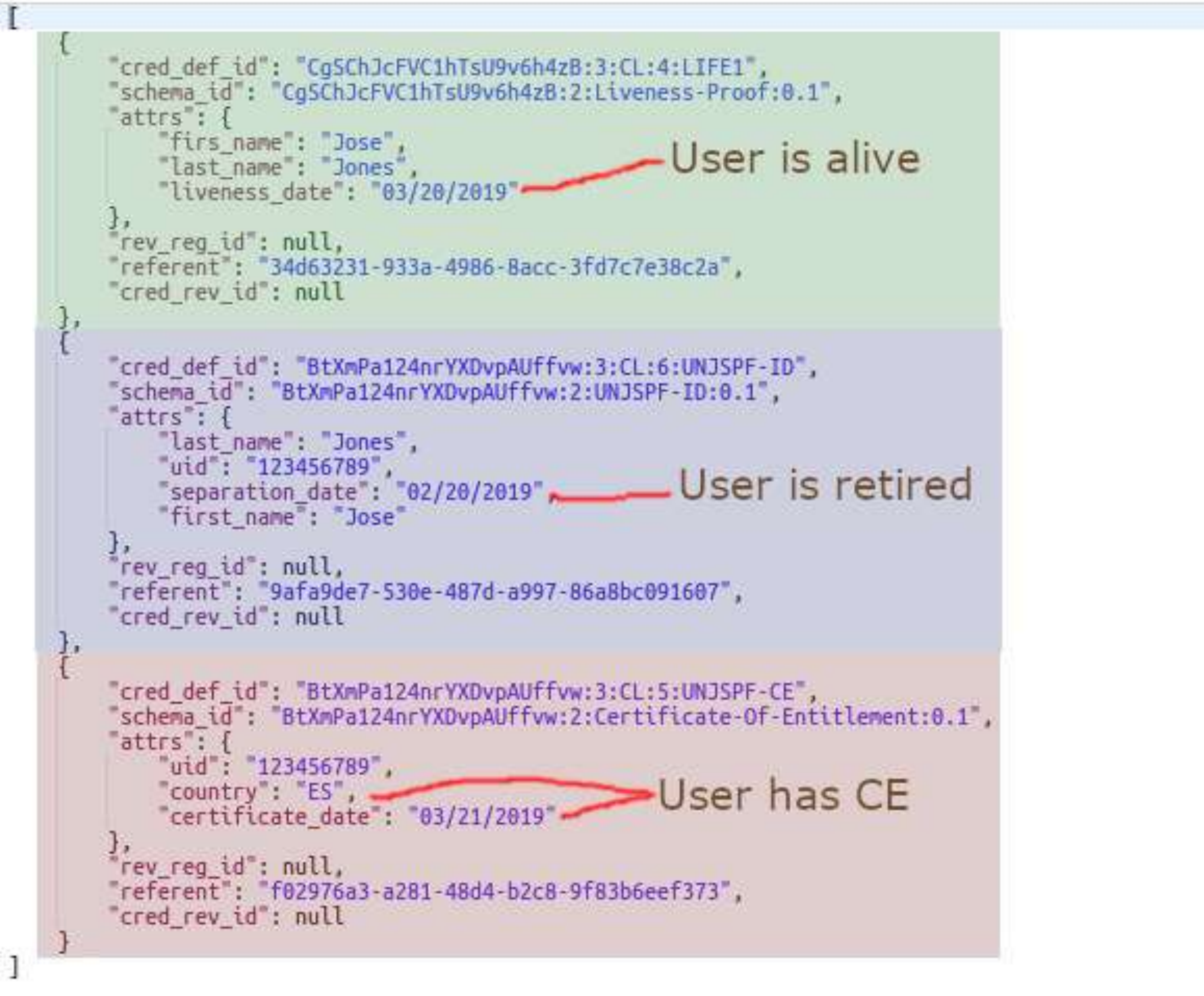
```
{
    "name": "Certificate-Of-Entitlement",
    "version": "0.1",
    "attributes": ["uid","certificate_date","country"]
}
```

# Transactions on the Digital CE system and User’s Wallet (i.e., Smartphone/Digital CE App)

🟩 Proof of Existence Credential

🟦 UNJSPF Credential Data

🟧 Certificate of Entitlement Credential



```
[
  {
      "cred_def_id": "CgSChJcFVC1hTsU9v6h4zB:3:CL:4:LIFE1",
      "schema_id": "CgSChJcFVC1hTsU9v6h4zB:2:Liveness-Proof:0.1",
      "attrs": {
          "firs_name": "Jose",
          "last_name": "Jones",
          "liveness_date": "03/20/2019"
      },
      "rev_reg_id": null,
      "referent": "34d63231-933a-4986-8acc-3fd7c7e38c2a",
      "cred_rev_id": null
  },
  {
      "cred_def_id": "BtXmPa124nrYXDvpAUffvw:3:CL:6:UNJSPF-ID",
      "schema_id": "BtXmPa124nrYXDvpAUffvw:2:UNJSPF-ID:0.1",
      "attrs": {
          "last_name": "Jones",
          "uid": "123456789",
          "separation_date": "02/20/2019",
          "first_name": "Jose"
      },
      "rev_reg_id": null,
      "referent": "9afa9de7-530e-487d-a997-86a8bc091607",
      "cred_rev_id": null
  },
  {
      "cred_def_id": "BtXmPa124nrYXDvpAUffvw:3:CL:5:UNJSPF-CE",
      "schema_id": "BtXmPa124nrYXDvpAUffvw:2:Certificate-Of-Entitlement:0.1",
      "attrs": {
          "uid": "123456789",
          "country": "ES",
          "certificate_date": "03/21/2019"
      },
      "rev_reg_id": null,
      "referent": "f02976a3-a281-48d4-b2c8-9f83b6eef373",
      "cred_rev_id": null
  }
]
```

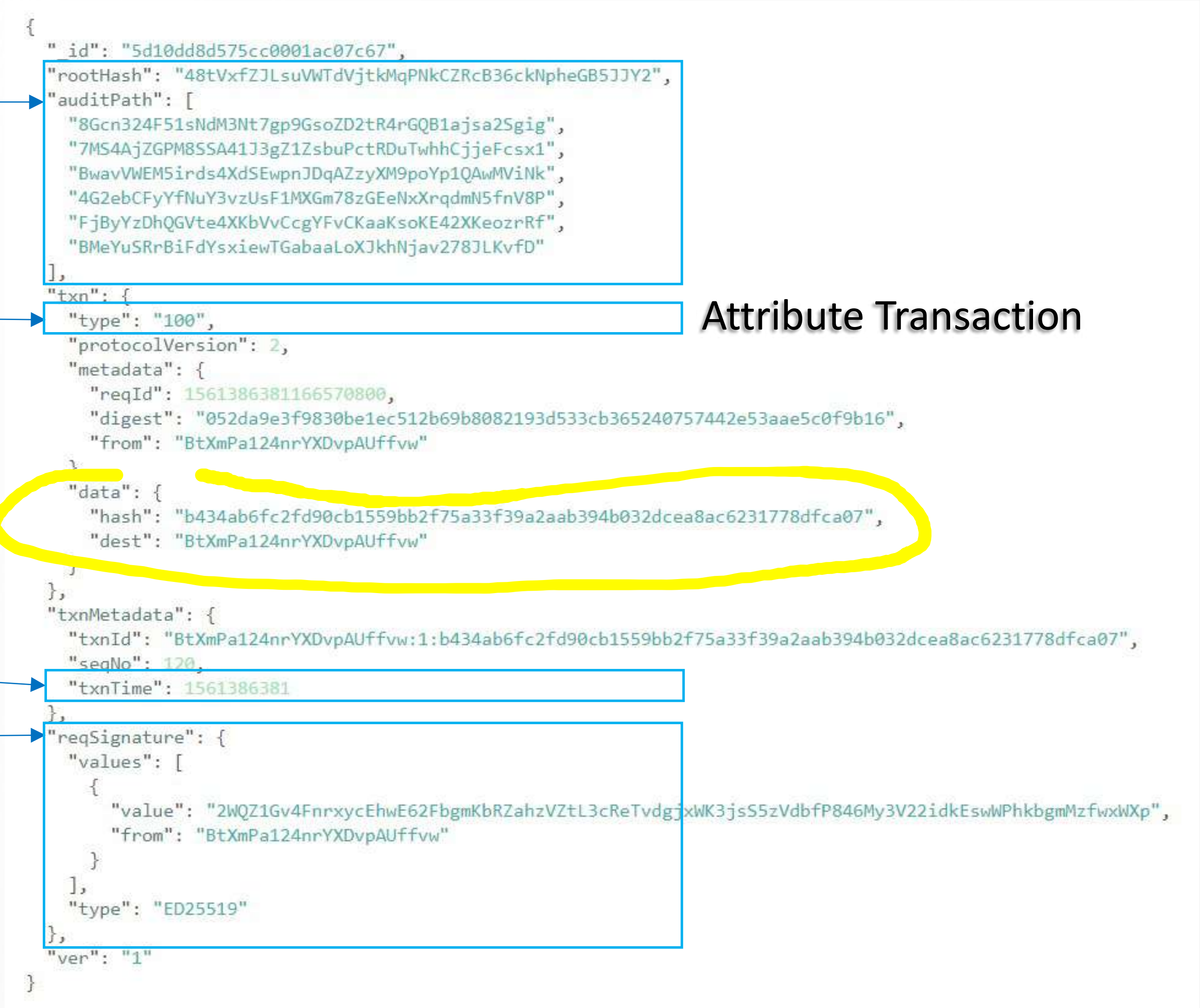
User is alive

User is retired

User has CE

# Transactions on the Blockchain

- Transaction validation
- Transaction type
- Transaction timestamp (epoch)
- Sender’s digital signature



Attribute Transaction

```
{
  "_id": "5d10dd8d575cc0001ac07c67",
  "rootHash": "48tVxfZJLsuVWTdVjtkMqPNkCZRcB36ckNpheGB5JJY2",
  "auditPath": [
    "8Gcn324F51sNdM3Nt7gp9GsoZD2tR4rGQB1ajsa2Sgig",
    "7MS4AjZGPM8SSA41J3gZ1ZsbuPctRDuTwhhCjjeFcsx1",
    "BwavVWEM5irds4XdSEwpnJDqAZzyXM9poYp1QAwMViNk",
    "4G2ebCFyYfNuY3vzUsF1MXGm78zGEeNxXrqdmN5fnV8P",
    "FjByYzDhQGVte4XKbVvCcgYFvCKaaKsoKE42XKeozrRf",
    "BMeYuSRrBiFdYsxiewTGabaaLoXJkhNjav278JLKvfD"
  ],
  "txn": {
    "type": "100",
    "protocolVersion": 2,
    "metadata": {
      "reqId": 1561386381166570800,
      "digest": "052da9e3f9830be1ec512b69b8082193d533cb365240757442e53aae5c0f9b16",
      "from": "BtXmPa124nrYXDvpAUffvw"
    },
    "data": {
      "hash": "b434ab6fc2fd90cb1559bb2f75a33f39a2aab394b032dcea8ac6231778dfca07",
      "dest": "BtXmPa124nrYXDvpAUffvw"
    }
  },
  "txnMetadata": {
    "txnId": "BtXmPa124nrYXDvpAUffvw:1:b434ab6fc2fd90cb1559bb2f75a33f39a2aab394b032dcea8ac6231778dfca07",
    "seqNo": 120,
    "txnTime": 1561386381
  },
  "reqSignature": {
    "values": [
      {
        "value": "2WQZ1Gv4FnrxycEhwE62FbgmKbRZahzVZtL3cReTvdgjxWK3jsS5zVdbfP846My3V22idkEswWPhkbgmMzfwxWXp",
        "from": "BtXmPa124nrYXDvpAUffvw"
      }
    ],
    "type": "ED25519"
  },
  "ver": "1"
}
```

# What IS recorded on the Blockchain?

- **All Decentralized Identifier (DID)** and corresponding verifying key (Verkey – public keys)
- **Schemas**, which define the structure of items referred by both credential definitions and credentials
- **Credential Definition**, which is built on top of a schema, **plus the issuer’s information for proof creation**

All these items are publicly accessible, providing transparency about the organization (UNJSPF), its Users, and the Process.

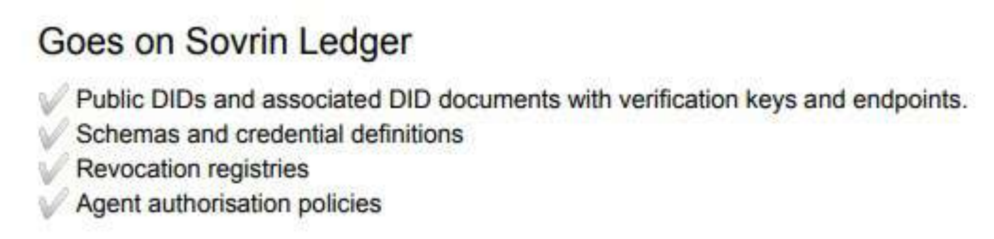
**The detailed recorded in the ledger serve as a “tamper-proof” source of trust for any subsequent audits and/or verifications.**

Sovrin: What Goes on the Ledger?

A white paper from Evernym in cooperation with the Sovrin Foundation.
An overview of what’s on the Sovrin distributed ledger and why.

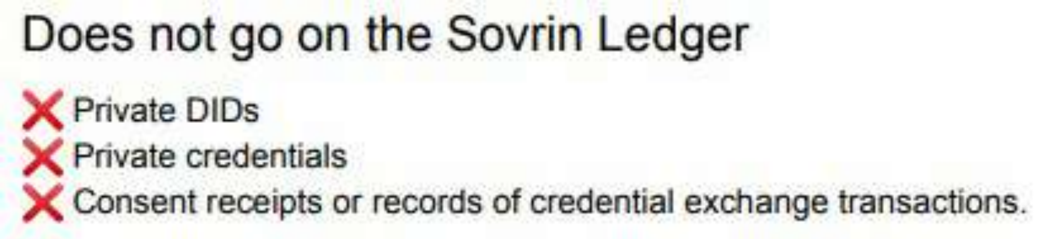
Andrew Tobin, Evernym
Updated September 2018
Originally written April 2017

evernym.com
sovrin.org



Goes on Sovrin Ledger

✓ Public DIDs and associated DID documents with verification keys and endpoints.
✓ Schemas and credential definitions
✓ Revocation registries
✓ Agent authorisation policies



Does not go on the Sovrin Ledger

✗ Private DIDs
✗ Private credentials
✗ Consent receipts or records of credential exchange transactions.

https://sovrin.org/wp-content/uploads/2018/10/What-Goes-On-The-Ledger.pdf

# What IS NOT recorded on the Blockchain?

**Personally Identifiable Information (PII) are NOT stored in the Ledger**

- PII are never exposed in the ledger (not even in an encrypted form) and, therefore, not readily accessible by anyone.

- This data is communicated via peer connections between the Users and UNJSPF. These connections are secured, through authenticated encryption, and information shared between are only known by the two parties.

- No PII is disclosed to the public.

- Information publicly accessible (in the Blockchain) provides trust on the proof.

# UNJSPF Digital Certificate of Entitlement

## Underlying Technology

## The Biometric Solution

# Biometrics & Facial Recognition: Project Requirements

- Provide a mechanism to authenticate users and prove their existence

- Takes into account the “aging” process to prevent the need of recurrent onboardings

- Delivers a consistent experience and performance on the most used iOS and Android platforms

- Works efficiently in “not state-of-the-art” smartphones

- Relies as little as possible on network connectivity, to avoid limitations in areas with challenging ICT infrastructures

# Biometrics & Facial Recognition: The Challenge

## AVAILABLE TECHNOLOGY AND ITS LIMITATIONS

- Modern smartphones include biometric-based authentication mechanisms. Typically a fingerprint scanner or face recognition to unlock the device and provide to additional functionalities

- Both Android and iOS development software development libraries expose very limited functionalities of the inner biometrics working mechanisms

- The app shall not have access to extended biometrical information. The camera content - nor the face features of the user - can be checked through the exposed SDK APIs. Therefore, the biometric solution already available on the devices does not meet the requirements of the project, since it would not allow the app to validate the user identity

- iOS Face ID uses an infrared set of beams to scan the user's face in 3D. Android devices, instead, use more limited mechanisms. Also, they are not present in older and/or low-range devices

- The most popular cloud providers have been providing face recognition services, such as AWS Rekognition and Azure Face services. These methods have been discarded because they require an open connection to the Internet during the whole validation process

# Biometrics & Facial Recognition: The Solution

- Using modern smartphone capabilities and state-of-the-art libraries, the biometric test has been designed to be performed locally on the device

- The solution adopted keeps the biometric information as close as possible to the user

- Nonetheless, building a solution that could work consistently with older smartphones – on both platforms – presented significant challenges

- The mobile app was developed using React Native, based on React. This approach provided a common UI and codebase written in Javascript for both Android and iOS

- The platform native code, written in Java and Kotlin for Android, and Objective-C and Swift for iOS, is used during the biometric process. This allowed to maximize the device performance

# Q & A