UN/CEFACT

Global Trust Registry Project

This deck will be updated as the project progresses.
Versions are split off and saved in the project folder for easier reference to past revisions.

Why do we need a Global Registrar Information Directory?

Global trade is (very) big business, and so is the fraud that it attracts

Scammers no longer just create fake invoices; they create fake companies, fake websites, fake provenance, fake registrations and fake registrars.

They exploit a core weakness: **It is difficult to verify an international company's legal status**.

Example tactics:

1. **Impersonation**: Using a real company's legitimate registration details (like an ABN) to appear trustworthy.
2. **Fabrication**: Registering a new, fake "shell company" for the sole purpose of committing fraud (e.g., GST or supplier fraud).
3. **Infection:** hacking legitimate business systems and injecting crime managed payment endpoints on invoices for major purchases.

Paper documentation makes verification vulnerable.

Unprotected digital documentation makes it worse

Paper based documentation makes verification inefficient and vulnerable. Physical documents can be faked and verification is slow and challenging - knowing what each document should “look like” from every possible location is an impossible task.

Simple digitisation creates a facsimile of the original document (a PDF) and/or represents the document content in human and machine readable forms.

Both enhance the risk of fraud and opportunity for fraudsters to create perfect documents.

AI is exponentially increasing the breadth, depth and frequency of all types of fraud, it makes every fraudster an expert fraudster.

[but AI can’t fake authentic cryptography]

The Systemic Risk:
"Deep fake Registrars"

Today's system relies on fragmented, easy-to-fake verification. **The Threat:**

- **Deepfake Websites**: Scammers create a pixel-perfect copy of a national registrar's website (e.g., companies-house.gov.uk.com instead of .gov.uk). You "verify" a fake company on a fake site.
- **Deepfake Documents**: AI-generated "Certificates of Good Standing" that look perfectly authentic, complete with watermarks and signatures.
- **“Real” digital signatures using fake keys**. Every valuable digital document should be (**needs** to be) cryptographically signed, but who says that is the digital signature of a legitimate organisation?

The Problem: There is no single, global "source of truth" to verify the right registrar to sign the document.

Hence the Global Registrar Information Directory (GRID)

The GRID will reduce socio-economic risks:

- **Detect fake registrar websites**: You would never Google "Bolivian company registrar." You would go to the GRID, find "Bolivia", and get the link.
- **Ghost Companies**: You can check a supplier's registration through their authoritative registrar.
- **Fake Claims**: Fakes fail when ownership of trademarks, land titles, certificates of compliance etc. are verified through trustworthy identifiers of organisations.

TL;DR

GRID and DIA answer two key questions for trade document verification…

Q1: How do you know if an identifier has been issued by a nation state authoritative registrar?

A1: The **Global Registrar Information Directory**

Q2: How do you know that organisation presenting the identifier has the right to present it?

A2: The nation state registrar issued **Digital Identity Anchor**

Project Value Points

1. An authoritative global directory of registrars will add significant value to supply chain transparency
2. A verifiable Digital Identity Anchor (UNTP Spec) will massively multiply this value

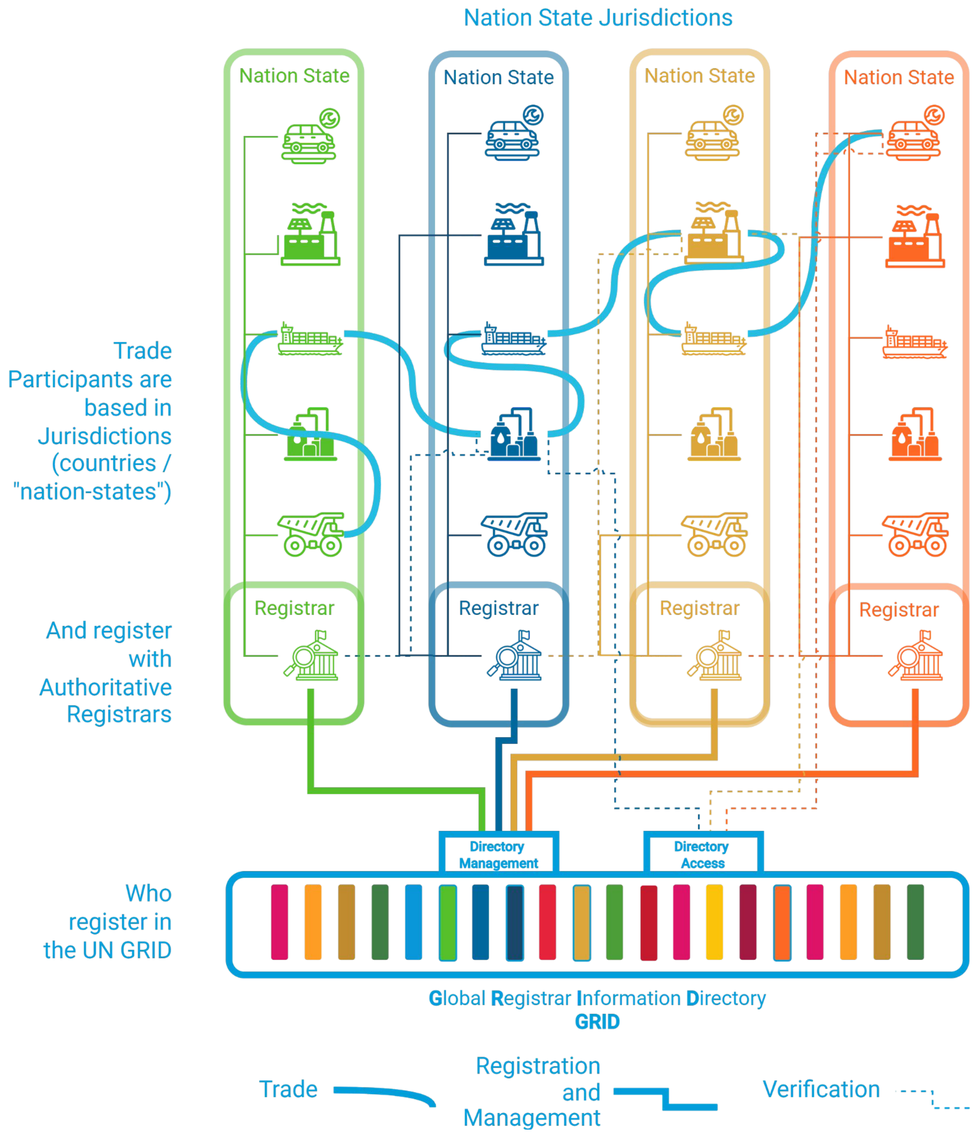
A directory will provide information about the authoritative registrar in participating nation state for eligible registers.

Self-maintained by the Registrars, this means that relying parties can use trustworthy information to tell the difference between authoritative registrars and false registrars and how and what the authoritative registrars register.

Further, by enabling authoritative registrars to issue verifiable digital identifiers (such as the UNTP DIA) we can significantly enhance global supply chain transparency, efficiency and effectiveness

The GRID Logical Model

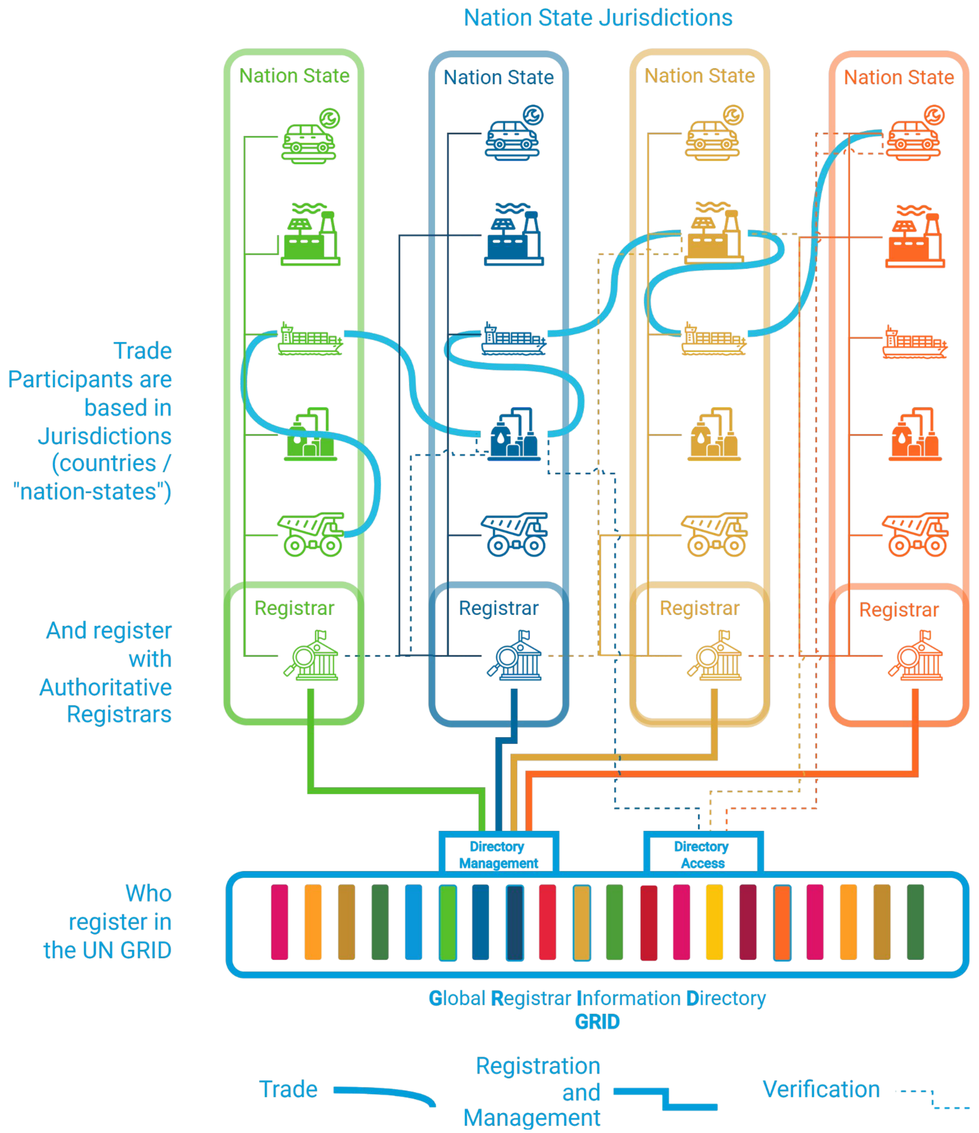
This is the logical model for the Global Trust Registry project



It may look centralised, but this is only a logical representation.

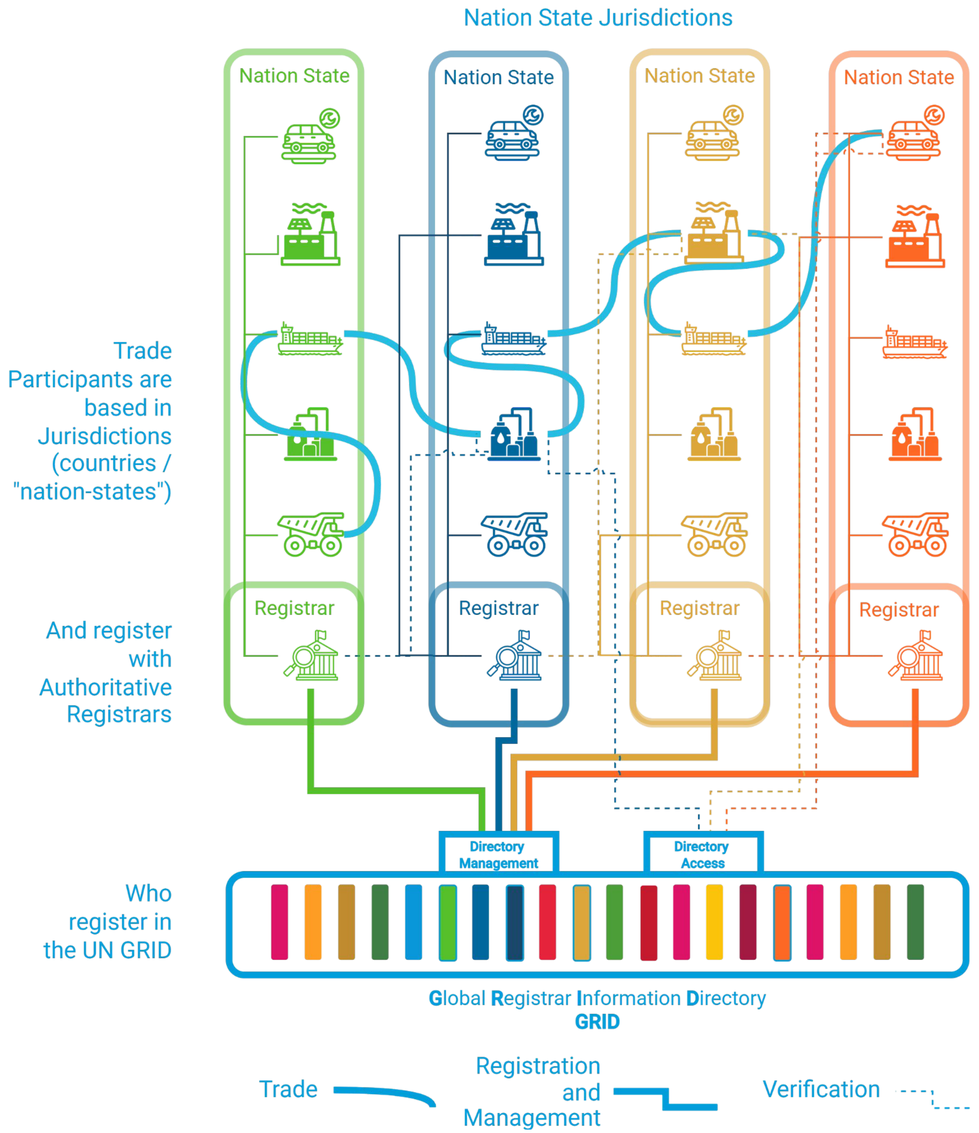
The physical, implementation will be distributed, decentralised, and resilient.

For example, the GRID could issue “Digital Identity Anchors” to Registrars in recognition of their entry in the GRID, enabling chains of provenance through protocols not platforms.



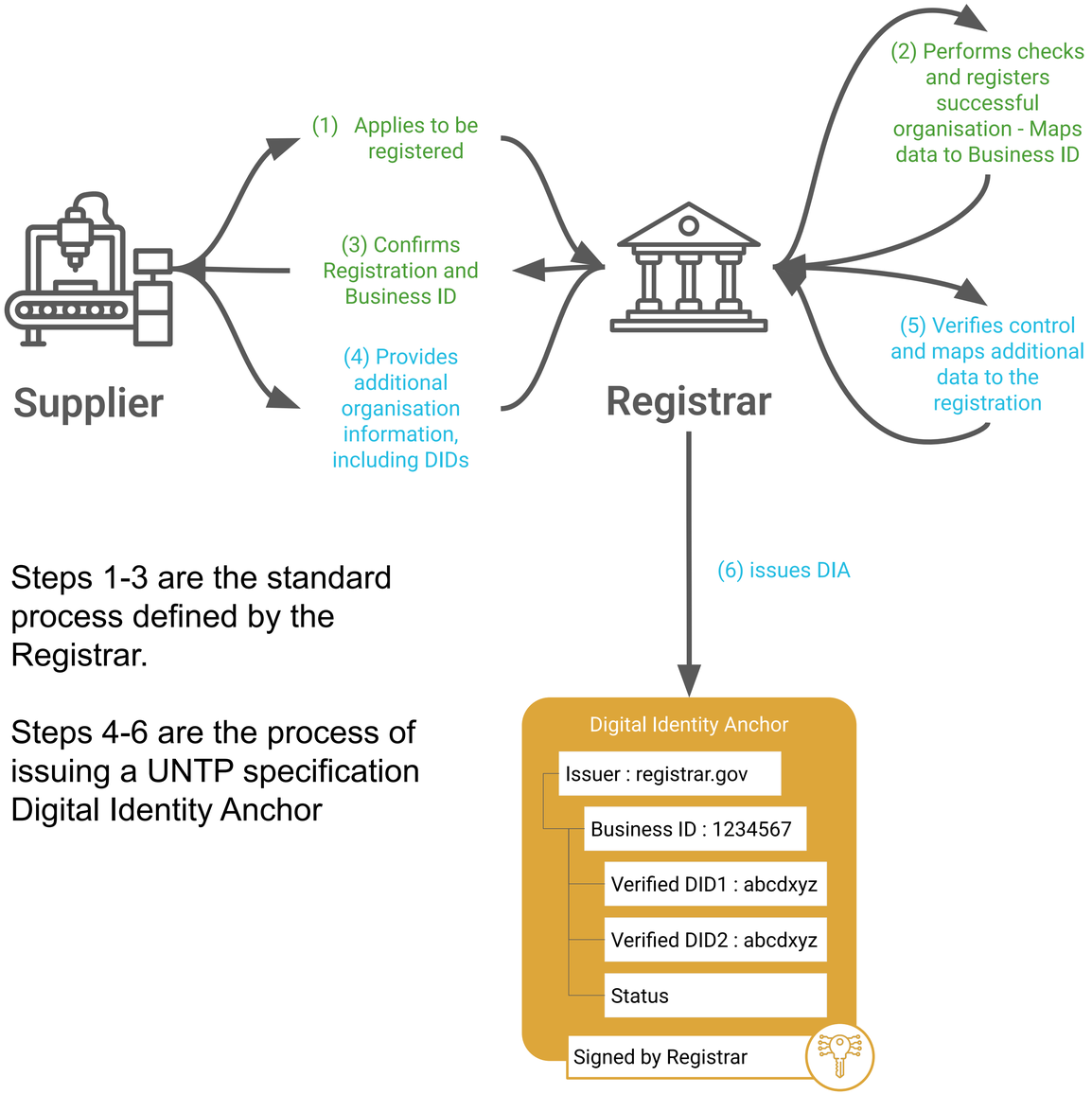
Key principles:

- **Voluntary:** Nation State Registrars choose to apply to the GRID
- **Trustworthy:** the GRID checks eligibility and quality requirements
- **Self-Sustained:** Participants manage their data in the GRID
- **Min scope max value:** The GRID only has data about Registrars and their registers. The Registry data stays the responsibility and control of nation state registrars.



Digital Identity Anchors

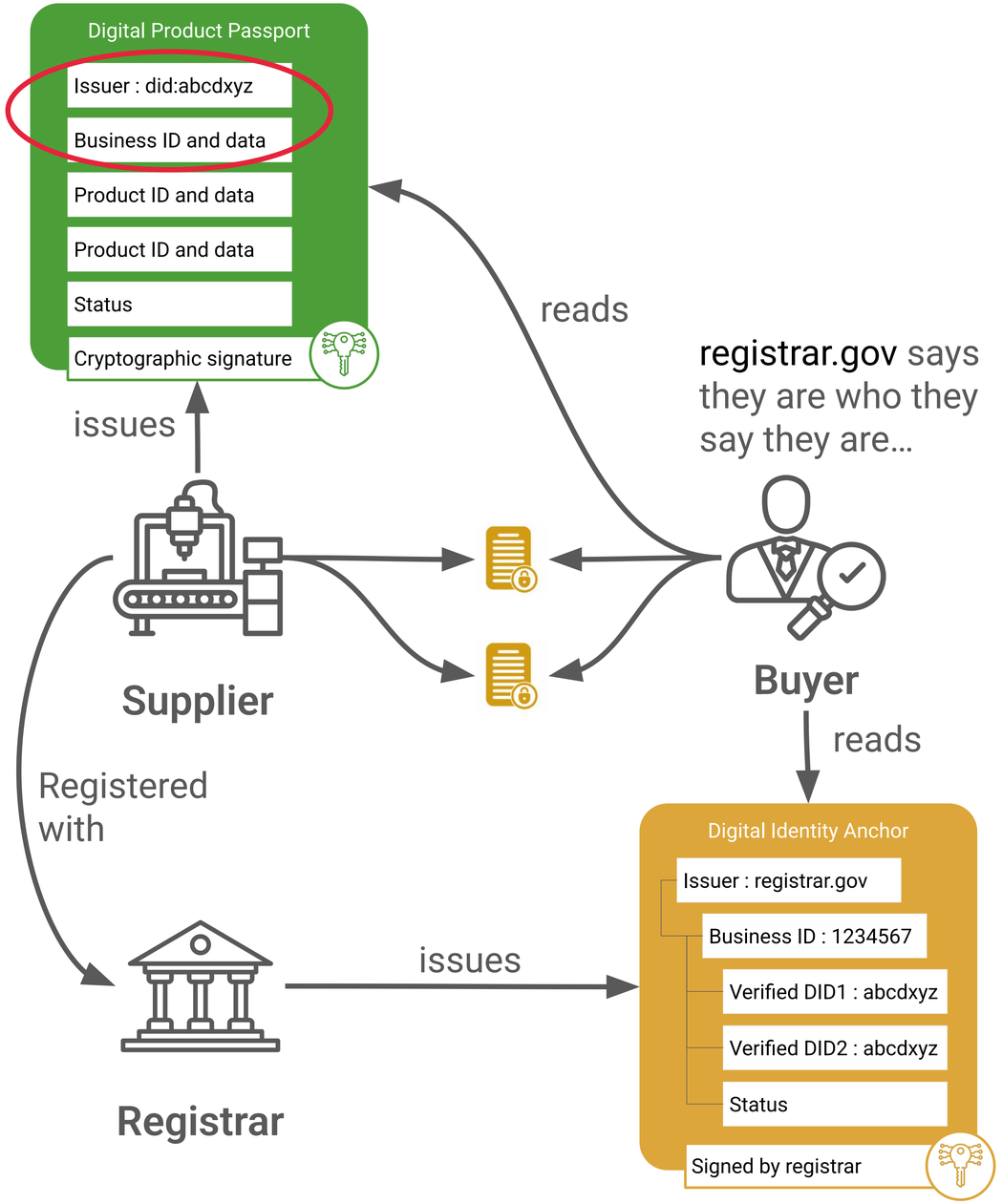
A DIA is issued by an authoritative registar and maps the Business ID to a business name and one or more decentralised identifiers (DIDs)



Steps 1-3 are the standard process defined by the Registrar.

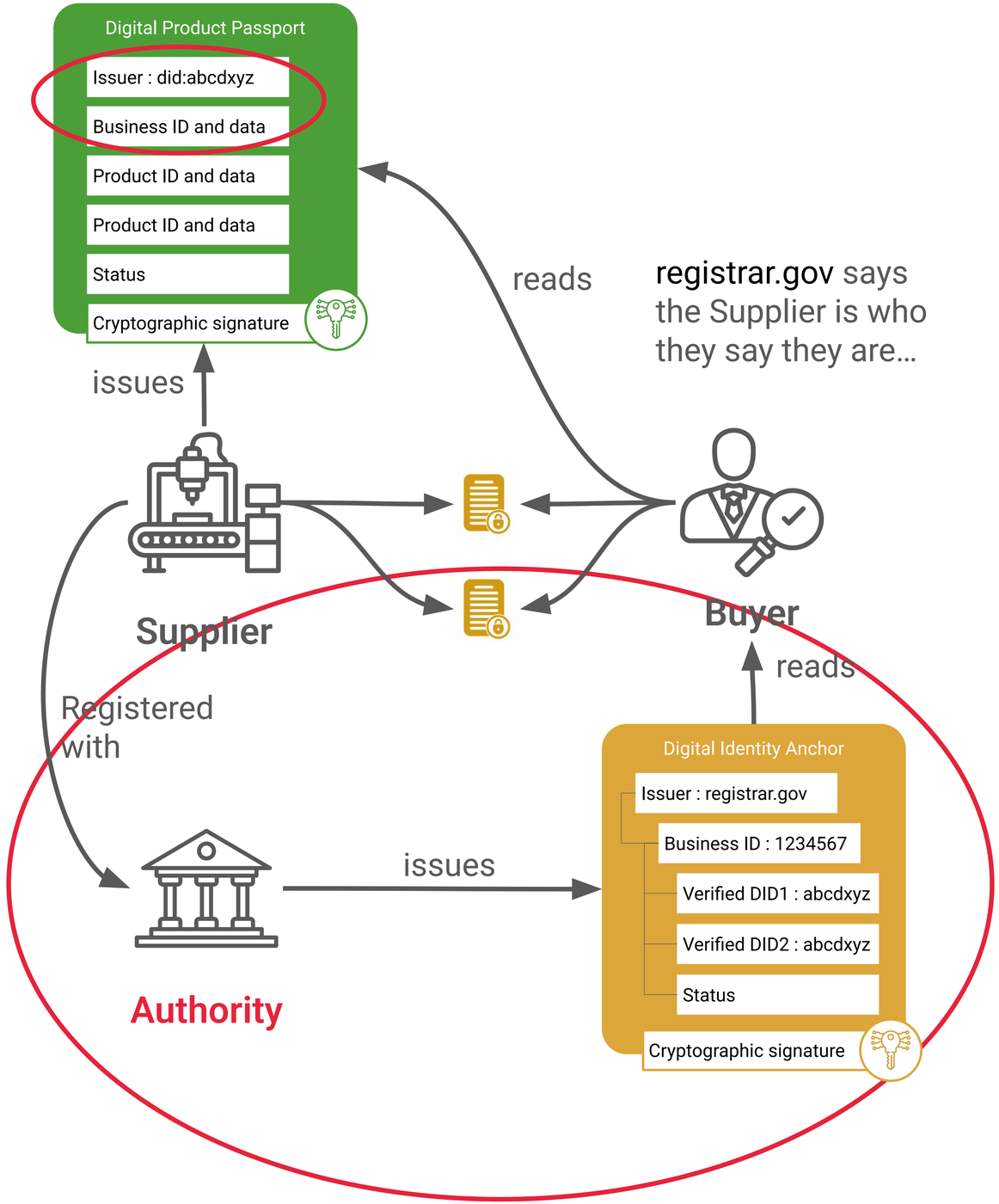
Steps 4-6 are the process of issuing a UNTP specification Digital Identity Anchor

The Digital Identity Anchor enables the **Buyer** to verify that the **Supplier** Business ID and DID are registered with the **Authority**



In summary…

Buyers need more than verifiable **Supplier** claims, they need evidence from **Authoritative Registries**



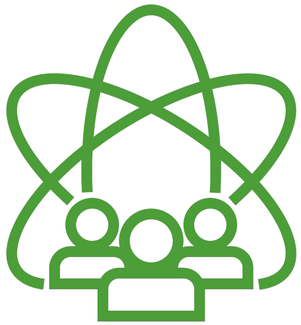
Ways of Working and IPR

The GRID and DIA are the deliverables of the UN/CEFACT “Global Trust Registry” Project

The GTR Project has three core focus areas:

1. Recommendations for the GRID to be ready for the 2026 UN/CEFACT Plenary
2. Updates and Implementation Guides for the UNTP Digital Identity Anchor (DIA) specification
3. Curated/Executed Pilots to test 1 & 2.

The GTR Project follows the UN/CEFACT Open Development Process



The following principles should be followed by all members of the project:

1. To welcome participation by anyone designated as an expert by a Head of Delegation to UN/CEFACT.
2. To encourage global input.
3. To work collaboratively and effectively.
4. To not incorporate specific hardware and/or proprietary software requirements into their processes or deliverables, or the implementation thereof.
5. To understand and agree to be subject to the UN/CEFACT Intellectual Property Rights (IPR) Policy.
6. To understand and agree to be subject to the UN/CEFACT Code of Conduct.

Source: UN/CEFACT Open Development Process:
https://unece.org/sites/default/files/2023-12/ECE_TRADE_C_CEFACT_2016_17E_ODP.pdf

Objectives and Approach

Project Objectives

The GTR project will

1. Make recommendations and propose governance and operational requirements for a global registrar directory for the 2026 UN/CEFACT Plenary
2. Review and if necessary propose changes to the UNTP specification of a “Digital Identity Anchor”
3. Curate pilots to test/prove the recommendations and to develop guidelines for implementations.

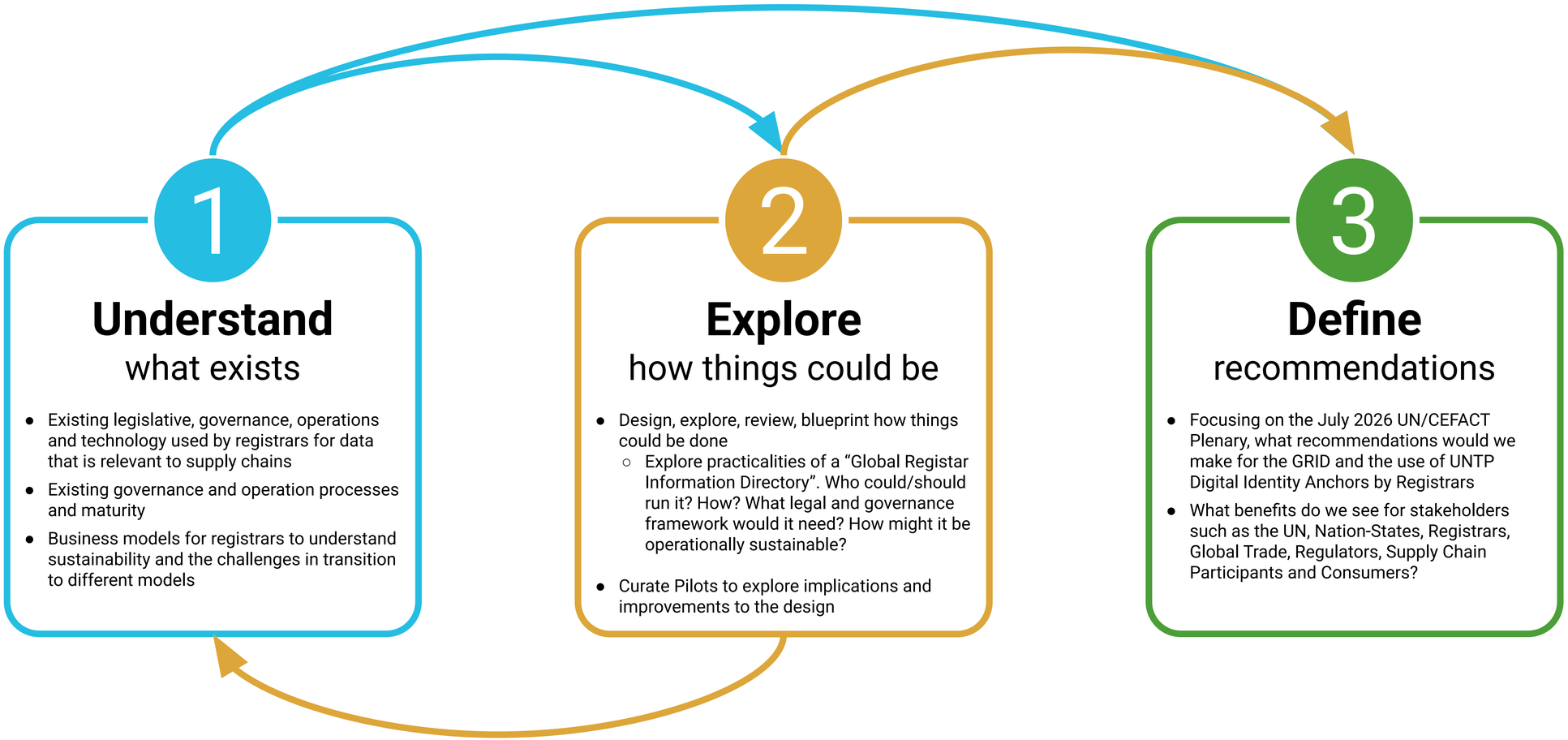
The name for the directory system is the “**G**lobal **R**egistrar **I**nformation **D**irectory” (**GRID**).

The project name “Global Trust Registry” caused some confusion when the initial call for participation was announced. Hence we produced a few “will and won’t” statements to help clarify the scope and intent of the project.The GTR project…

- ☑️ **Will** seek to recognise the government registries that exist, understand their legal and governance framework, what they issue, and if and how they make that digitally accessible and verifiable
- ☑️ **Will** propose a governance framework for the UN CEFACT Registrar recognition process
- ☑️ **Will** seek to define a data model and verification process for Registrar identifiers that enables trustworthiness and interoperability
- ☑️ **Will** develop implementation pilots and guidance
- ☑️ **Will** support key SDGs, including SDG 9 Innovation and resilient infrastructure, SDG 12: Supply chain transparency and SDG 16 : Peace, justice and strong institutions.

- ⛔ **Will not** seek to create [yet another] central register of all things
- ⛔ **Will not** issue secondary credentials nor issue credentials on behalf of registrars
- ⛔ **Will not** disrupt existing business models of nation state registrars
- ⛔ **Will not** dictate to nation states what they do, nor how they should do it

The project has three connected areas of work



Project tools and spaces

Too maximise collaboration, communication and free public access, we will use a combination of tools

Key required capabilities of the toolset are:

- Enable production of our deliverables - mostly documents
- Enable asynchronous comments and collaboration
- Provide history, revision and version control
- Are familiar and/or easy to learn
- Are free to use for contributors

First draft / working copies / discussion documents will use Google tools (Docs, Slides, Sheets, Meet, Groups, Calendar etc.) since we can make those freely available.

These project artefacts are in this folder:
https://drive.google.com/drive/folders/15SAuJW8ee_Lj_SNtHUKh2-e12RsEzAtu

UNICC GitLab repo
Mature / ready for initial public viewing content will be placed on the project UNICC GitLab repo here:
GitLab link: https://opensource.unicc.org/un/unece/uncefact/gtr
Website (auto produced from GitLab content): https://un.opensource.unicc.org/unece/uncefact/gtr/

Communication
Group email: https://groups.io/g/UNCEFACTGlobalTrustRegistry
Slack channel: Slack Channel: https://uncefact.slack.com/archives/C0904NU8SN6

Meetings
Project meetings are held biweekly online using google meet. Details are in the project calendar here:
Project Calendar (with meeting date/times/details and past meeting minutes):
https://calendar.google.com/calendar/embed?src=c_0f1b7a519c6ffaa8e9e50417e3688e37f485a6af1792ab0fcd9141b50ba3366c%40group.calendar.google.com

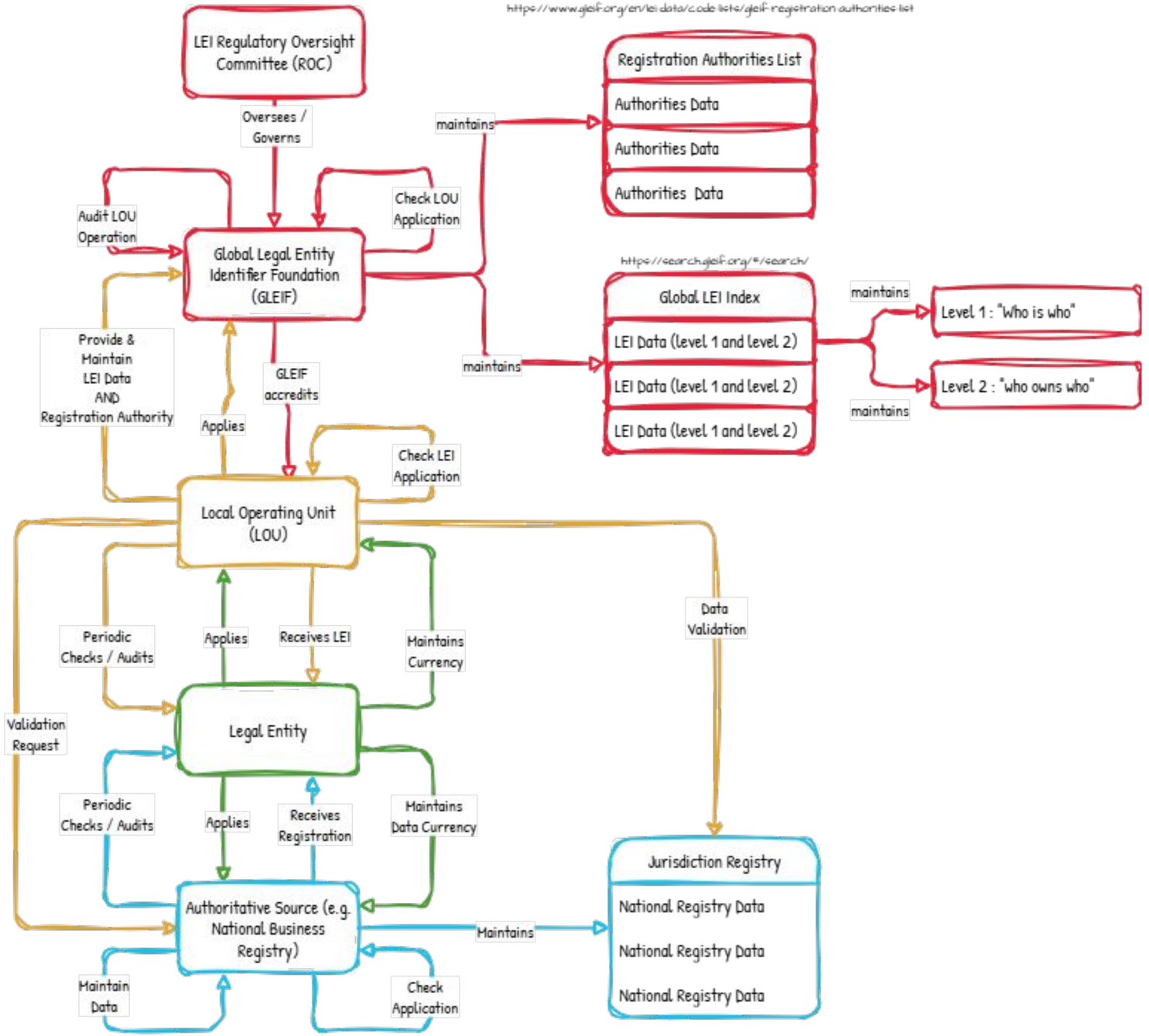
Public address in iCal format:
https://calendar.google.com/calendar/ical/c_0f1b7a519c6ffaa8e9e50417e3688e37f485a6af1792ab0fcd9141b50ba3366c%40group.calendar.google.com/public/basic.ics

How might GTR work with other ecosystems?

GLEIF CASE STUDY

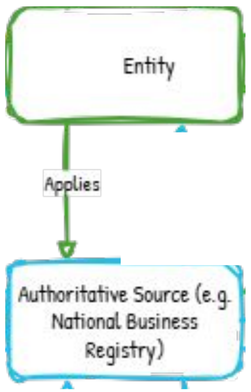
This is a representation of the GLEIF LEI Issuance and Maintenance Model

That's a lot to take in, the next few slides build the picture up step by step…

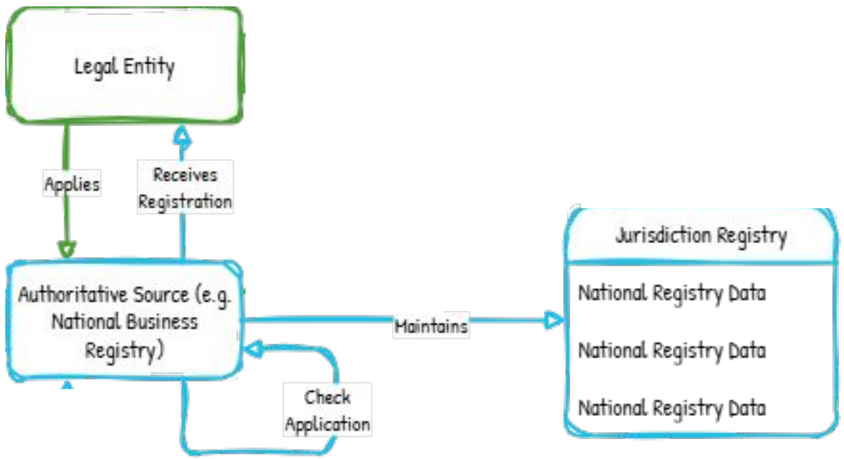


Entities apply to be registered in their jurisdiction with an authoritative register.

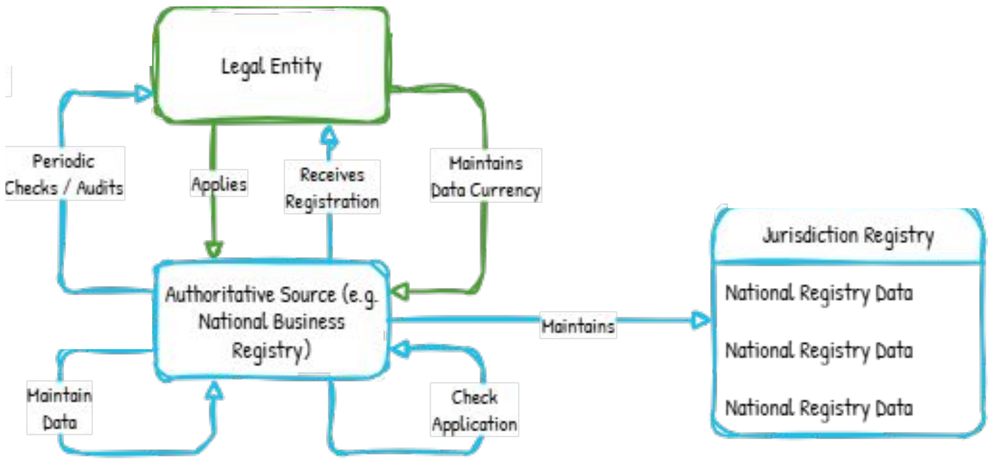
This is the normal/standard practise. Having a legal registration is a precondition for GLEIF LEI issuance



The jurisdiction Authoritative Registrar decides if the entity is eligible and then issues an identifier and records information in their register

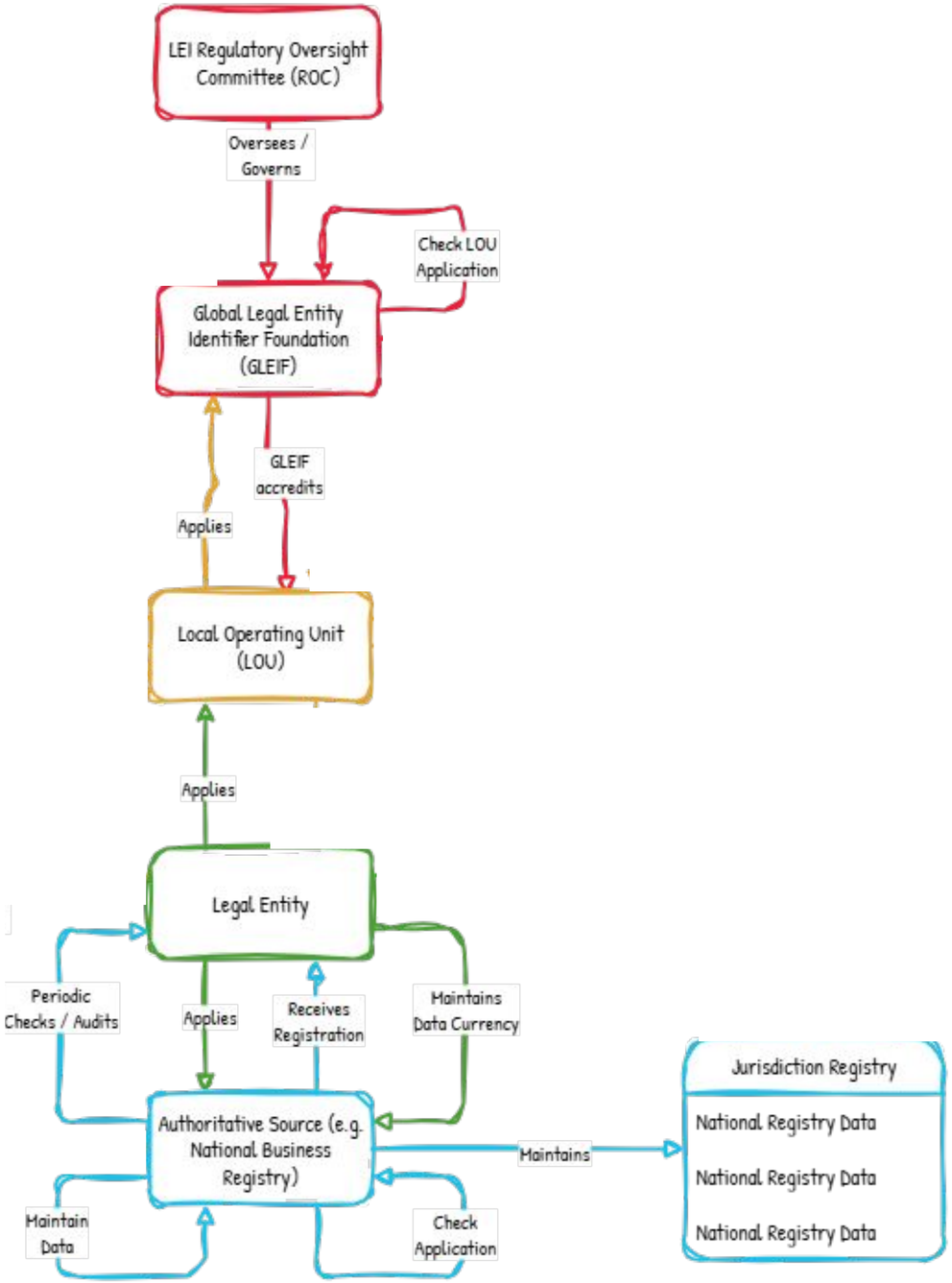


The Authoritative Registrar and the Entity then maintain currency of the registered data as required by the jurisdiction laws



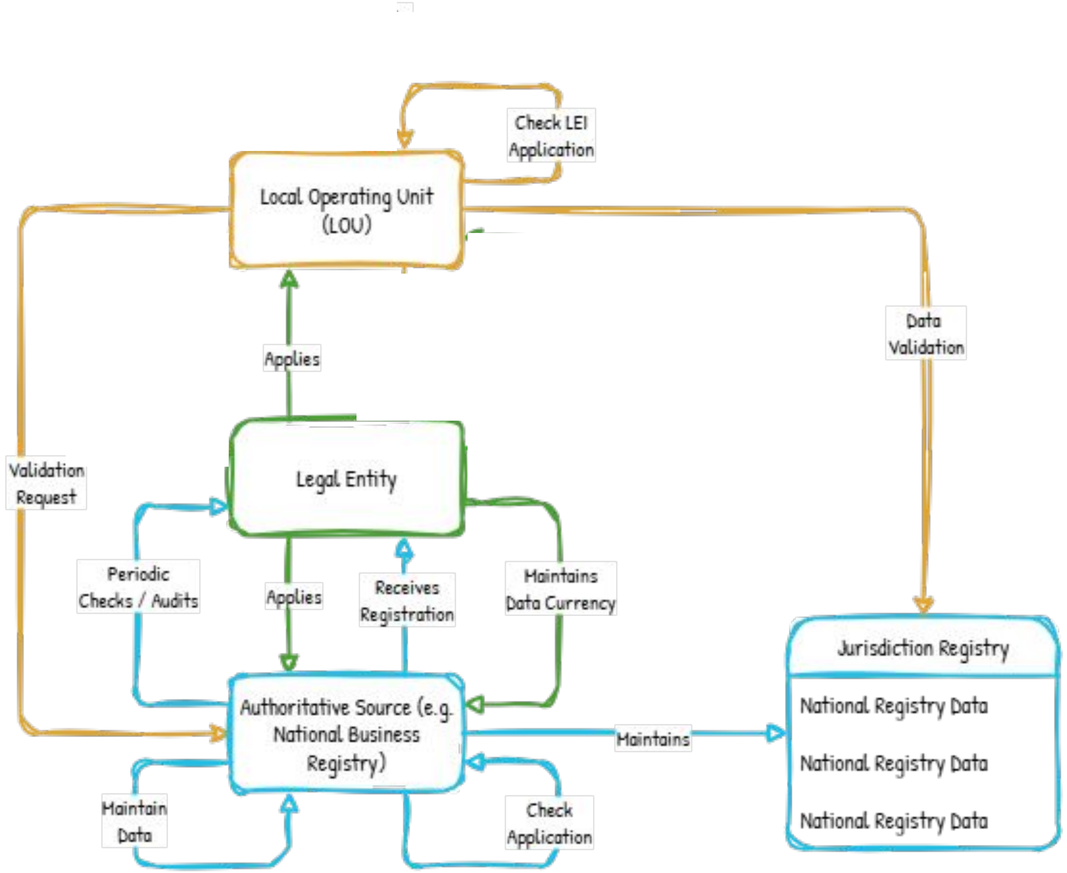
Legal Entity the decides to apply for (or is required to have) a GLEIF LEI, they choose an “Local Operating Unit” - an organisation certified by GLEIF to issue LEIs in their jurisdiction.

GLEIF itself is overseen by the ROC, which i
overseen by the FSB and G20 (FSB and G20
not shown in the diagram)



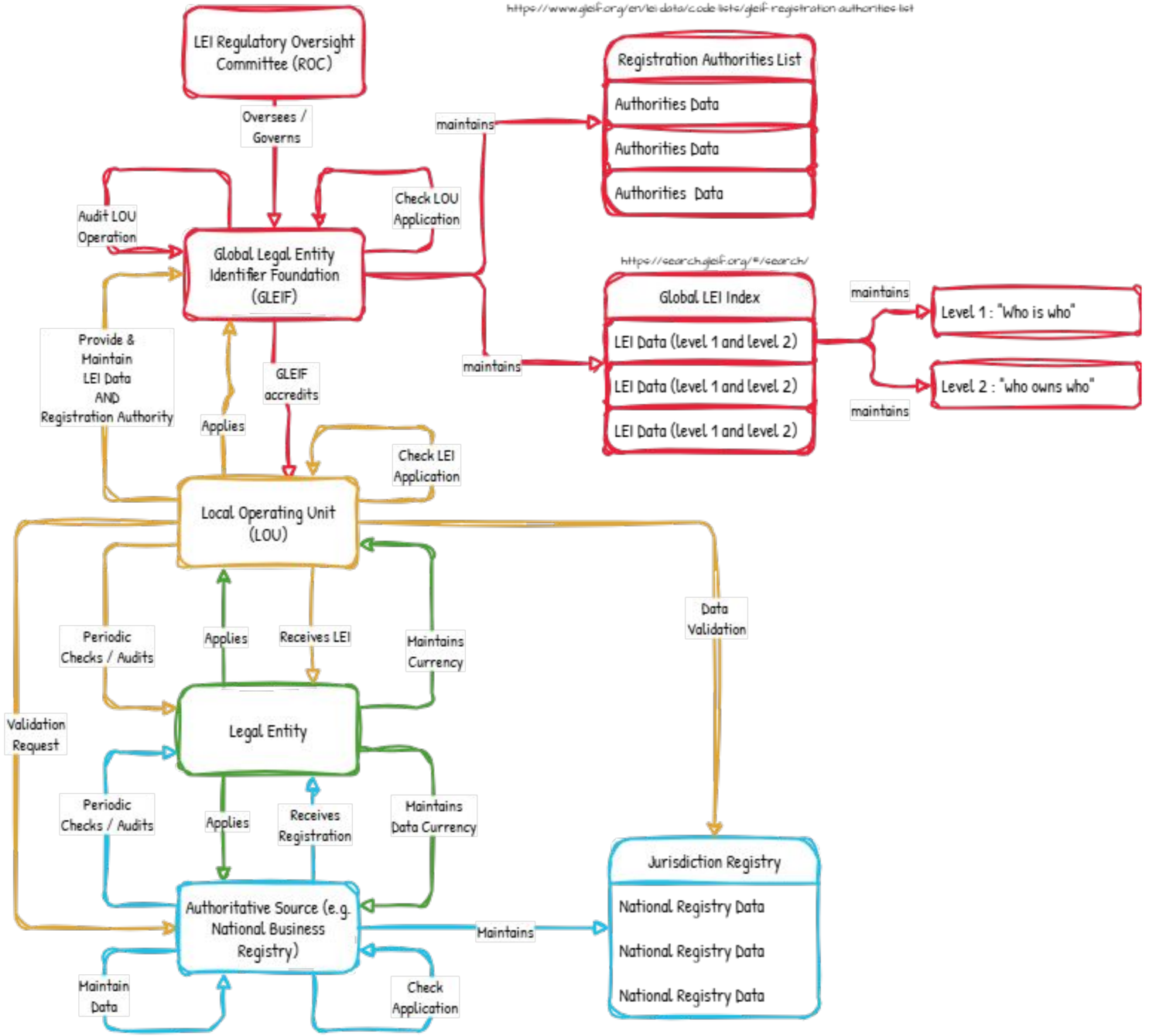
Focusing narrowly again…

The LOU checks the application and verifies that the entity is legal registered with a Registered Authority

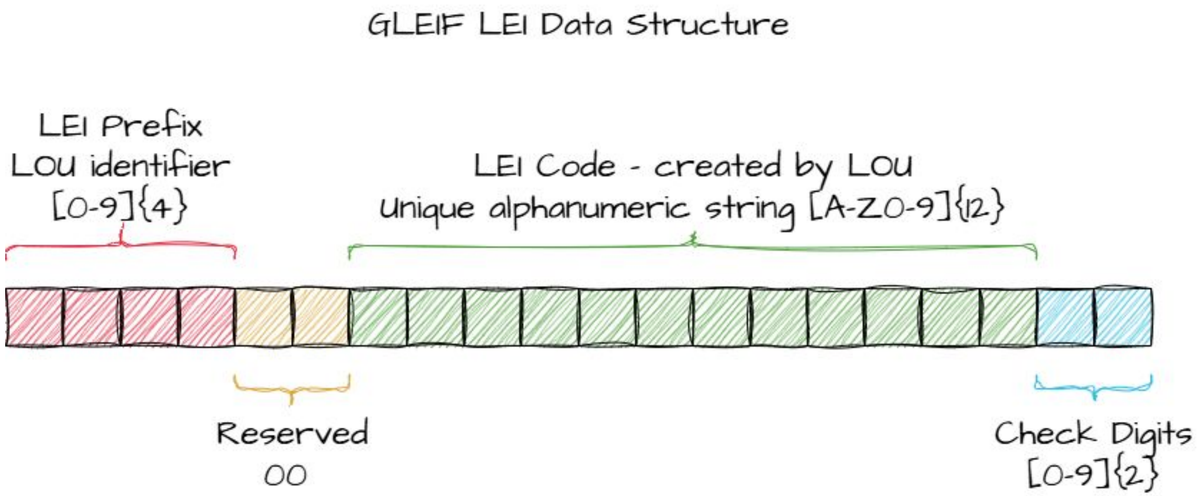


If the checks pass, then the Legal Entity is issued an LEI by the LOU, and the LOU passes the details to GLEIF.

Maintenance of data is a **legal** responsibility of the Entity and Registrar and an **operational** requirement of the LOU and GLEIF



GLEIF LEI structure



Example: 529900VEJFORC0614826

5299 - LEI Prefix, issuing LOU
00 - Reserved
VEJFORC0614B - LEI Code no "embedded intelligence"
26 - Check Digits - calculated from the first 18 digits of the LEI

This is interesting, and vLEIs are (technically and functionally) even more interesting.

We will be interested in the technical approach taken by GLEIF for LEIs and vLEIs in the future.

But not what we need to focus on at the moment.

This discussion is focused on the legal / authoritative meaning of LEIs and how they, and GLEIF might interact with GTR.

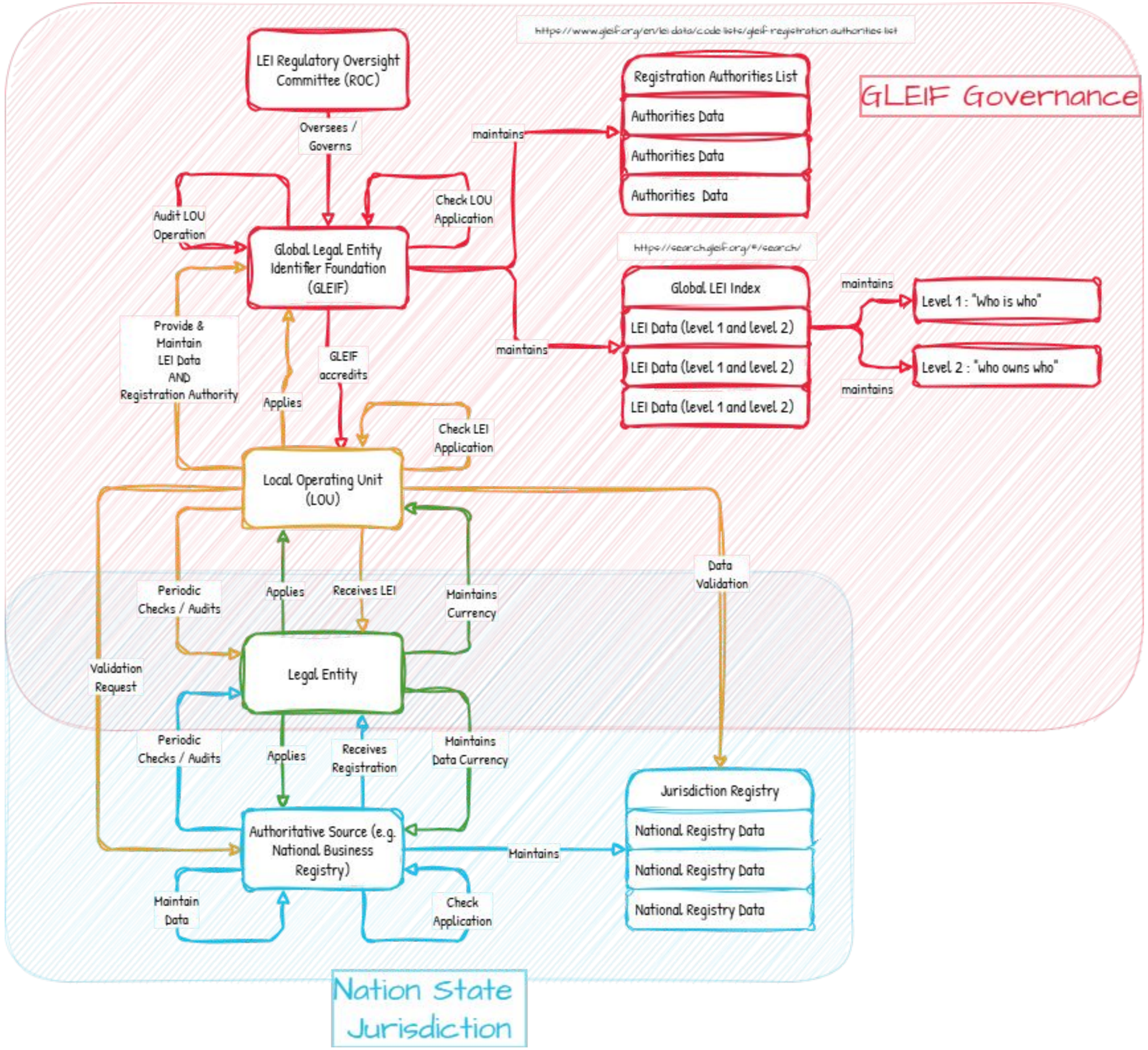
The relative footprints of legal scope and GLEIF governance scope.

The Entity must comply with the legal requirements of the jurisdiction and needs to comply with the governance requirements of GLEIF.

These are not equal.

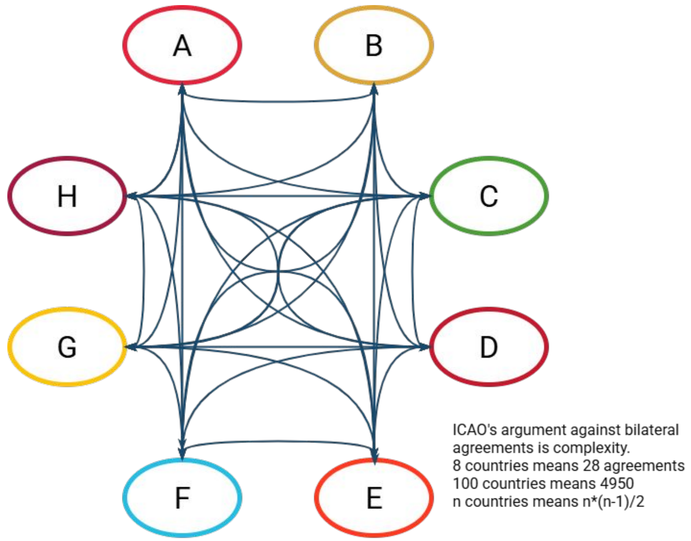
If they lose the legal registration that their LEI is based on, they will also lose their LEI (it will be invalid and flagged by GLEIF).

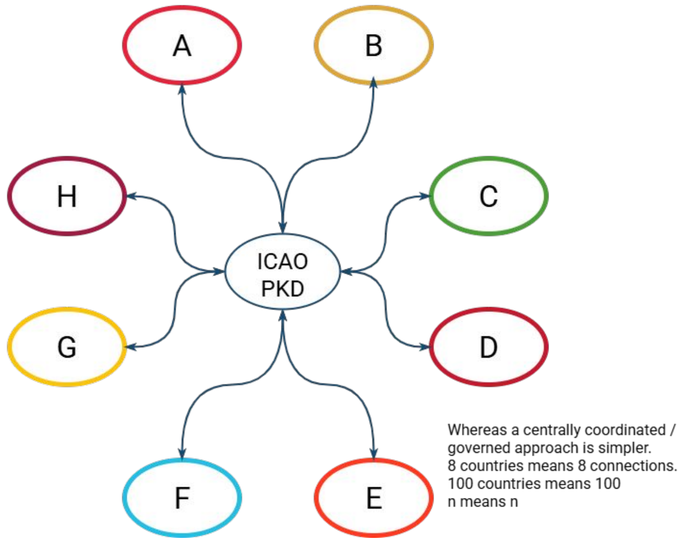
However, if they choose not to renew their LEI there is no impact on their legal registration.



Case Study:

ICAO PKD





ICAO is the International Civil Aircraft Organisation and a UN Agency.

The ICAO Public Key Directory (PKD), established in 2007, is a centralized system for securely exchanging cryptographic information to authenticate electronic Machine Readable Travel Documents (eMRTDs) like ePassports [1].

It was created to address the complexity of bilateral key exchanges, offering a single, trusted platform.

The PKD operates under a robust governance structure overseen by the ICAO Council and managed by a PKD Board and given authority by a 12 page MoU [2]

It is a self-sustaining, funded by its participants. The fee structure designed to encourage growth and adoption.

The system's technical architecture is designed to be secure, resilient, and geographically redundant. The PKD system itself is secure, but overall integrity relies upon the administrative processes of identity verification preceding passport issuance.

The PKD is evolving into a "Trust-as-a-Service" platform for the broader travel ecosystem.

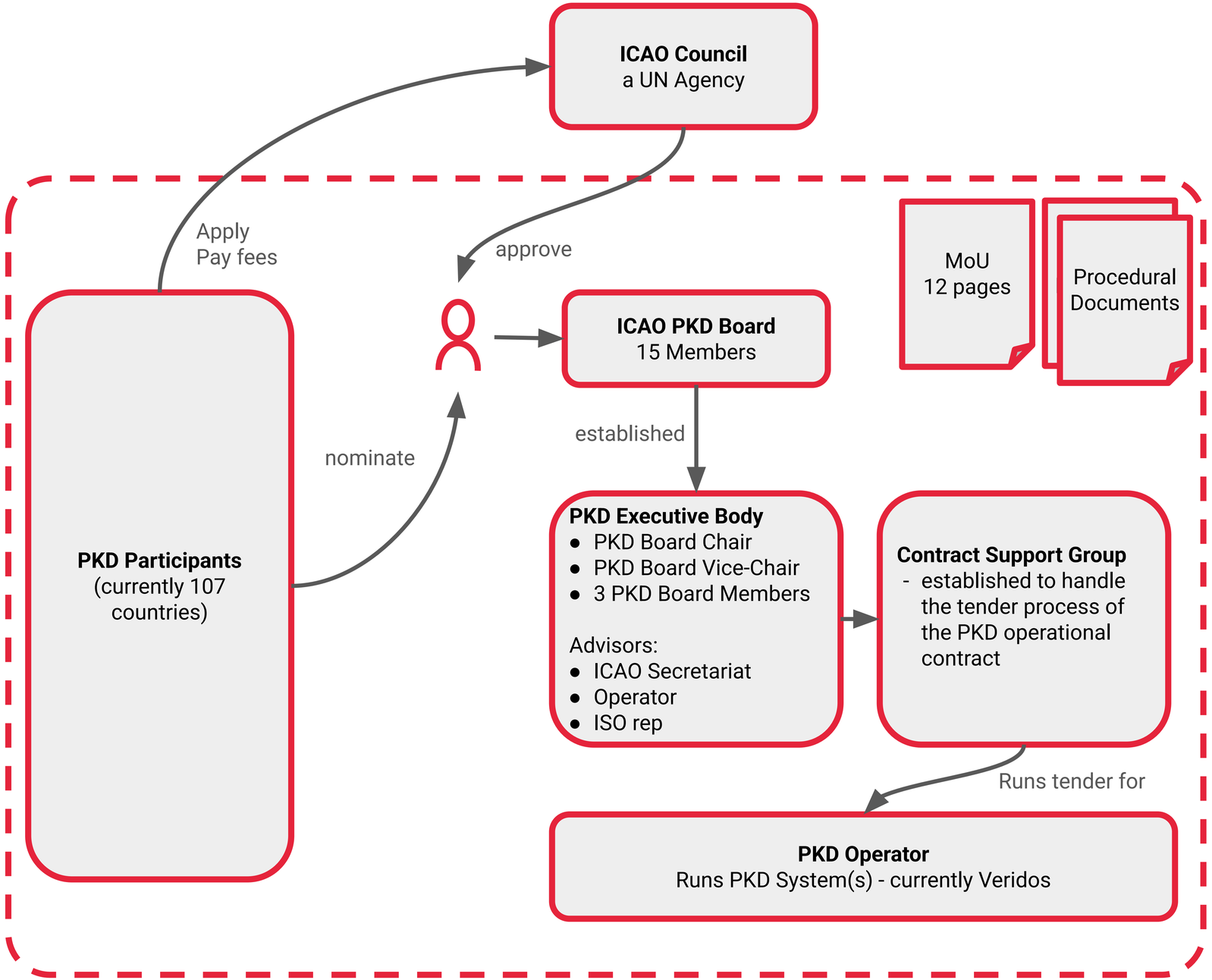
Sources:

1. https://docs.google.com/document/d/1XPhg_MRpgeFb1J8uTNangXG6xq8kjivMlUx-F-BbQf4/edit?usp=sharing

2 https://www.icao.int/sites/default/files/2025-06/MoU-FINAL.Version-8-dated-1-January-2016.pdf

ICAO PKD Governance and Operation

[ICAO is based in Montreal, Canada]



ICAO PKD Fees

- Self-sustaining financial model (funded by fees paid by participants)
- Transparent process of fee calculation based on operating costs and numbers of participants
- One-time registration fee (currently US $15,900)
- Annual Fee:
  - ICAO Portion (effective participants) - US $6,595
  - ICAO Operator Portion (active participants) - US $14,200

So something like US$20k/year per country - that seems very good value!

Case Study:

UN/CEFACT LOCODE

The UN/LOCODE system is a critical standard for global trade provided by UN/CEFACT.

It provides unique five-character codes for over 103,000 locations (e.g. “AUMEL” refers the port of Melbourne). The aim of LOCODE is to eliminate ambiguity in location names for supply chain transactions and shipping destinations. Not all transport destinations are in LOCODE. For example, Melbourne Airport doesn’t have a LOCODE designation (but does have IATA and ICAO designations, “MEL” and “YMML” respectively).

The system's governance has evolved to a decentralized network of National Focal Points (NFPs) and an Advisory Group due to the growth in data volume.

However, it relies on a legacy IT infrastructure, leading to inefficiencies and data quality challenges [2].

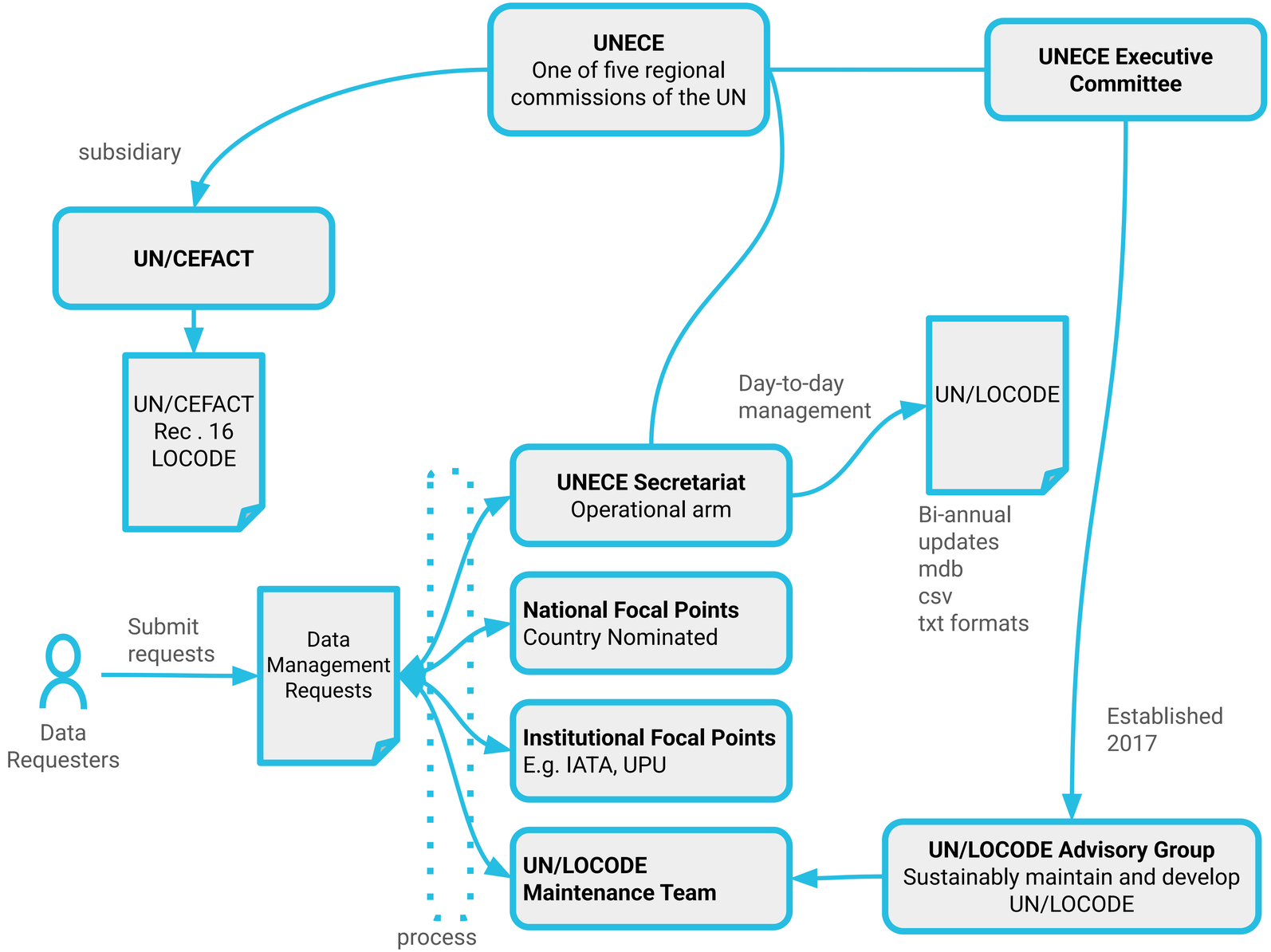
While the official UN/LOCODE is free, a commercial ecosystem offers value-added services with validated, corrected, and API-accessible data for a subscription fee, creating a "freemium" model.

Sources:

1 https://docs.google.com/document/d/1f0QN9D8hPRlgaTwnU75hB2eeTD8dK3jLQyfn1LA0d1U/edit?usp=sharing
2 https://unece.org/sites/default/files/2025-07/ECE_TRADE_C_CEFACT_2025_9E-REV1.pdf

UN/CEFACT LOCODE Governance and Operation

It’s complicated!



UN/CEFACT LOCODE Fees

- LOCODE list is freely available
- Update Requests are free to submit
- Participation is open and free
- Many parties and system rely on and build on LOCODE

However…

A commercial market for LOCODE based services has been established to address shortcomings in the official offering, namely data quality and real-time access. Commercial offerings add:

- Data validation and correction
- Regular updates (more frequent than twice per year)
- API access

A rising concern is that LOCODE needs to be sustainably supported to remain relevant. See https://unece.org/sites/default/files/2025-07/ECE_TRADE_C_CEFACT_2025_9E-REV1.pdf

Observations and ideas from the case studies

ICAO PKD and UN/LOCODE illustrate complementary UN patterns for governance. For GTR, we should not replicate either exclusively.

A hybrid governance approach is advisable: UN-anchored policy and oversight to ensure legitimacy and transparency, combined with structured, distributed participation by Member States and/or designated registrars for scalability and local legitimacy.

Technical operations may be internal or UN-procured under published SLAs.

The specific UN anchoring (e.g., UN/CEFACT under UNECE, the UNECE Secretariat, or a joint UN mechanism) should be determined through Member State consultation.

The Governance text should remain principle-based and technology-neutral at this stage.

The service must be self-sustaining with minimal cost and maximal value and a transparent fee structure that encourages efficiency and use.

