IOTA

Interoperable Digital Identity for Tax Administrations.

mDoc, ISO standards, and cross-border trust.

Jesse Dyer • Product Director
FAST ENTERPRISES

INTRA-EUROPEAN ORGANISATION
OF TAX ADMINISTRATIONS

• AGENDA

Identity that works across borders, channels, and agencies.

01

Why identity matters

Where identity shows up in the taxpayer journey, what is changing underneath it, and the lessons from real implementations.

02

The standards that make it work

ISO 18013-5 and 18013-7, OpenID4VP, and the W3C Digital Credentials API — how privacy by design, strong security, and offline verification fit into a single interoperable stack.

03

Cross-border trust

How trust lists, eIDAS 2.0, and the EUDI Wallet let verifiers trust issuers they have never met — and what that means for a tax administration.

PART ONE

Why identity matters in modern tax administration.

Identity is no longer single field on a form. It is the foundation of every secure interaction a taxpayer has with government.

FAST

Identity touches every step of the taxpayer journey.

THE TAXPAYER JOURNEY

01
Registration

Who is this person or business? Are they who they claim to be?

02
Filing

The right taxpayer is signing, submitting, and attesting to the return.

03
Payments

Money moves on behalf of the right account, with the right authorisation.

04
Compliance & Audit

Access to sensitive records whare are all tied to verified identity.

WITH EVERY CHANNEL

Online portal

Self-service login, e-filing, account management.

In-person service

Field offices, kiosks, appointments or whenever an ID is checked at a counter.

Representation & delegation

Accountants, agents, family members acting on a taxpayer's behalf.

A modern identity approach must serve every stage of the journey on every channel it runs through.

Identity programmes succeed when they start with real use cases, not the technology.

OBSERVATION 1

Start with the use case, not the credential.

The agencies that have moved fastest picked a few high-value moments, such as first-time registration, high-risk filing, in-person taxpayer service and designed an identity strategy around them.

OBSERVATION 2

Plan for channels that don't exist yet.

In-person kiosks, web portals, mobile apps, third-party agents. The credential must work across them all — which means choosing standards that anticipate this from day one.

OBSERVATION 3

Integration is the hidden cost.

Every custom identity integration is a liability: another vendor to manage, another contract to renew, another line of code to patch. Open standards turn N×M integrations into N+M.

From national silos to interoperable ecosystems.

YESTERDAY

One Country. One Solution. One Vendor.

- ✗ Credentials only valid at home
- ✗ Custom integrations for every agency
- ✗ Lock-in and limited or controlled use

TODAY

Open standards. Many issuers. Many verifiers.

- ✓ Credentials that travel across borders
- ✓ Readers can support many issuers
- ✓ Reuse across tax, banking, and more...

NOT ONE STANDARD – A FAMILY

Three bodies of work, one interoperable stack.

PROXIMITY

ISO/IEC

18013-5 • 18013-7 • 23220

Originated in-person with NFC, BLE, and QR codes to present identity documents with mDoc. Now extending online with more flexibility.

INTERNET

OpenID Foundation

OpenID4VP • OpenID4VCI

Originated on the web using OAuth-based issuance and presentation across credential formats. Included in ISO/IEC standards.

BROWSER

W3C

Digital Credentials API

A protocol-agnostic pipe allowing browsers to use it to carry ISO/IEC or OpenID requests between web servicers and the wallet.

No single body owns "digital identity." Each solves a different problem. Together they let a credential cross borders, channels, and vendors.

PART TWO

mDoc and the ISO standards.

A short tour of ISO/IEC 18013-5 and 18013-7. Exploring what they are, how they work, and why verification does not require contacting the issuer during use.

FAST

• DEFINITION

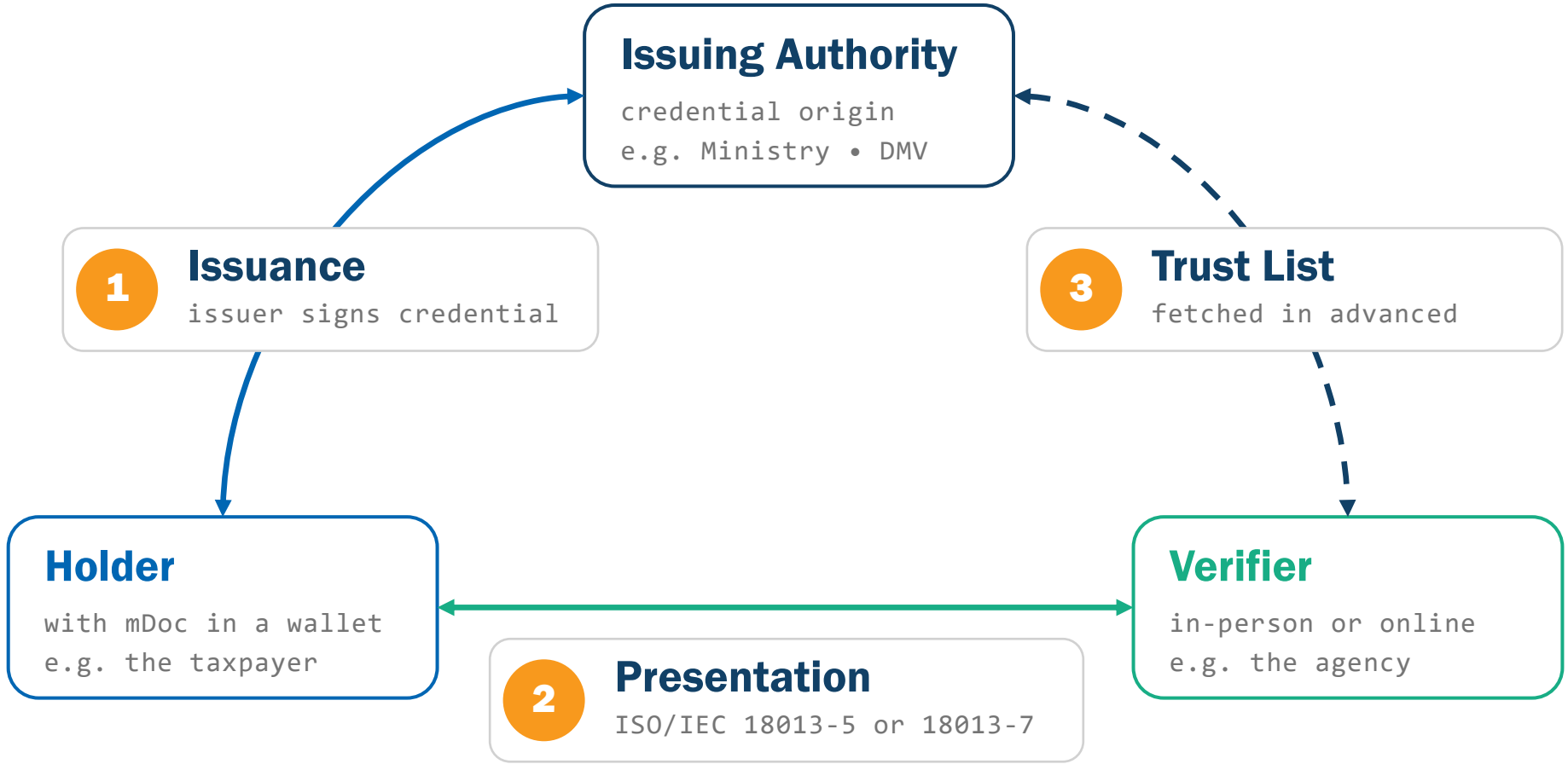
mDoc is a digital credential format your mobile device can securely store and present, signed by the issuer.

Designed first for mobile driver's license **(mDL)** under **ISO/IEC 18013-5**, but the underlying container is generic by design.

The same format now carries the **EU Digital Identity Wallet**, national **Photo ID** schemes, and other attested data including age, residence, tax identifiers.

It works **in person** and **online** through a browser.

A Holder, an Issuer, and a Verifier.



Verification without a call to the issuer

BEFORE

Verifier connects to issuer for every transaction.

✗ Breaks if the network is down

✗ Issuers can track every verification

✗ Issuers must scale to respond to verifiers

NOW

Verifier checks for a signature it can validate that it already trusts.

✓ Works fully offline

✓ Issuers cannot see the verification

✓ Fewer central dependencies to operate

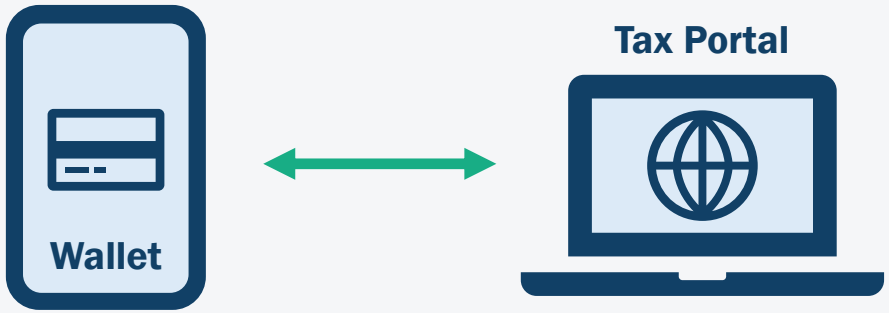
The issuers' public keys are held by the verifier, acquired through a trust list.
A deliberate choice in ISO/IEC 18013-5

The same mDoc works in person and online.

ISO/IEC 18013-5

In person

The phone and the reader talk directly, engaging over with an NFC tap or a QR scan and then transmit data encrypted between devices.



ISO/IEC 18013-7

Online

The same credential is presented from a mobile device through, encrypted through the browser to backend web servers of an online tax portal, for example.

Share the answer, not the whole document.

VERIFIER ASKS

“Confirm this person’s identity.”

given_name + family_name	✓ shared
date_of_birth	✓ shared
portrait	✓ shared
resident_address	– withheld –
driving_privileges	– withheld –

Only ask for what is required to identify

Confirming who a taxpayer is rarely needs all attributes from their credential.

The taxpayer sees and consents

Each request is approved in the wallet. The taxpayer sees which identity fields are being shared, and with whom.

Aligned with GDPR

Data minimization and purpose limitation are built into the protocol, not bolted on.

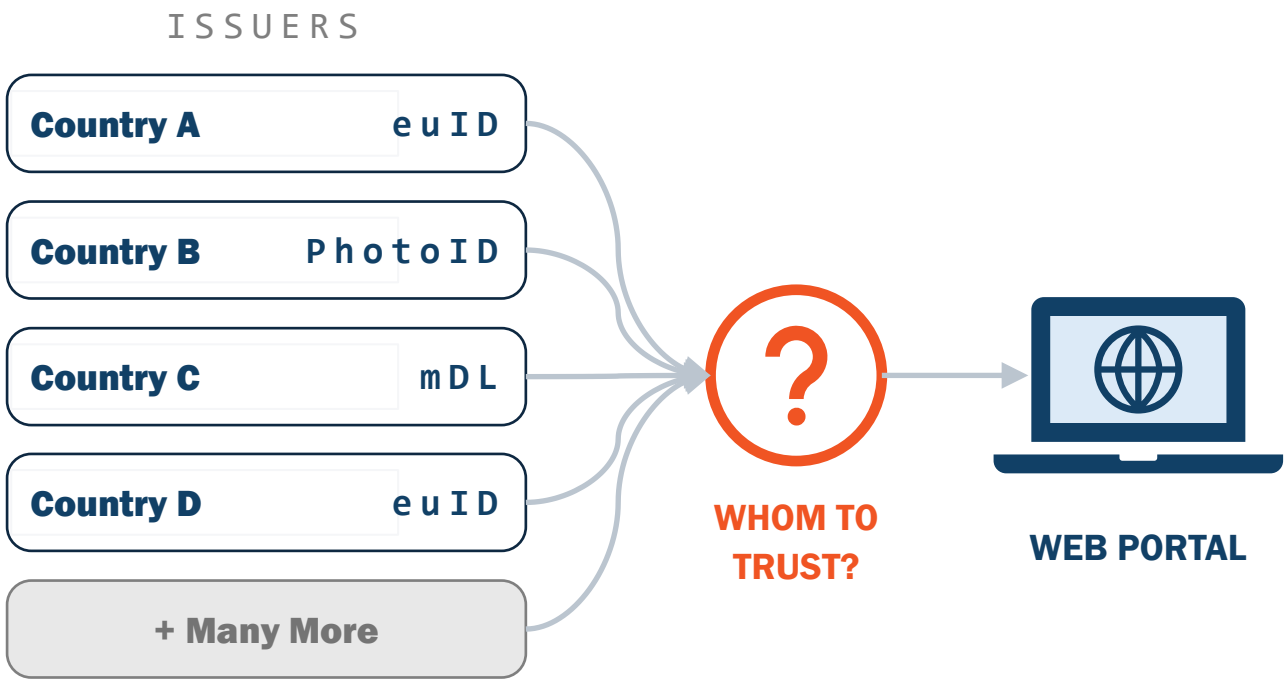
PART THREE

Cross-border trust.

The standards tell us *how* to verify. Trust lists tell us *whom* to trust.

FAST

A verifier in one country has never met an issuer from another.



Every issuer issues its own credentials, signed with its own keys.

A verifier cannot negotiate bilaterally with every issuer in the world nor should it have to.

What's needed is a **shared, signed registry** that answers a single question: *whom does this verifier trust, and how do they know?*

• THE SOLUTION

A signed registry answers the question: whom does this verifier trust?

NORTH AMERICA

AAMVA DTS

The Digital Trust Service publishes a signed **VICAL**. A U.S. tax agency trusts it, and through it, every state DMV on the list.

EUROPE

eIDAS LOTL

Each Member State publishes a Trusted List. The Commission signs a List of Trusted Lists aggregating them. One root, every Member State reachable.

AUSTRALIA

AUSTROADS DTS

A signed **VICAL** for Australian and New Zealand issuing authorities. Same contract as AAMVA: one list, many trusted issuers.

The verifier does not pick whom to trust issuer-by-issuer. It trusts the list, and the list does the work.

*Trust lists are the answer different regions have converged on. They all work the same way: an **operator** publishes a **cryptographically signed list** of issuers a verifier has agreed to accept.*

HOW A VERIFIER USES IT

Fetched in advance. Used offline at presentation.

ONLINE · FROM TRUST LIST — OFFLINE

STEP 1

Fetch the trust list

From AAMVA DTS, an eIDAS TSL, or an equivalent operator.

STEP 2

Verify the trust list

The list itself is signed by the trust operator.

STEP 3

Store the issuer keys

Every trusted Issuer's public key, ready locally.

AT PRESENTATION

Verify trusted mDocs

Offline. Instant. No live call to any Issuer.

What this means in practice

A tax portal can verify a credential it has never seen before, from an Issuer it has never spoken to — on the first presentation. The trust relationship was established in advance, operator-to-operator, not issuer-by-issuer.

The same pieces, under the European roof.

THE REGULATION

eIDAS 2.0

Requires every Member State to offer citizens a **European Digital Identity Wallet by 2026** — accepted across all public and large private services.

THE PRODUCT

EUDI Wallet

Built on **ISO 18013, OpenID4VP, and** eIDAS Trust Lists. The same standards stack we've been describing.

ISO 18013 is not an alternative to eIDAS 2.0 — it is one of the foundations eIDAS builds on.

For a tax administration, this is the unlock: align with the standards, and the same code paths support EU citizens presenting their wallet, AAMVA-conformant mobile IDs from North America, and national schemes across the globe.

Five lessons to carry home.

01 **Start with the use case, not the technology.**
Registration, filing, refunds — pick a real moment and design identity around it. The standard is a means, not the goal.

02 **Use standards to reduce integration risk.**
ISO 18013, OpenID4VP, and the W3C DC API turn N×M custom integrations into N+M. That is where the real cost savings live.

03 **Plan for in-person and online from day one.**
The same credential must work in person and in a browser. ISO/IEC 18013-7 was built on the same foundation as 18013-5.

04 **Build privacy and security in from the start.**
Selective disclosure, offline verification, and signed trust lists are not features to add later. They are part of the contract the standard makes with the document holder.

05 **Use standards collectively, not individually.**
ISO, W3C, and OpenID each solve a different problem. They are designed to compose — and it's the combination that makes a complete, interoperable solution. No single standard does it all.