

ID Wallet & VCs

Architecture, Trust & Rollout Pathways

Implementing ID Wallets and Verifiable Credentials at national scale

ID4Africa - Abidjan
May 15th, 2026

Marie Eichholtzer
Senior Digital Specialist





Wallets are not a new type of digital ID system. They are a new paradigm

“Traditional” Digital ID

Wallet / VC Model



Trust Location

Centralized in a government database. Every verification requires a call to the authoritative source.



Embedded in the credential. The cryptographic proof travels with the data.



Data Flow

Through government back-ends. Citizens are subjects of the system, not holders of their own data.



Directly from holder to verifier. Citizens control what they share, with whom, and when.



Governance

One agency controls everything. Complex, but contained within one institutional boundary.



Distributed across an ecosystem of actors. Requires explicit governance architecture from the start.



Uptake

Central systems become bottlenecks. Cross-border and cross-sector use require custom integration.



Any credential, any compliant verifier, any sector, any border. Interoperability by design, not integration.



Wallets sit on top of what you already have



The Wallet

Cryptographic key store · credential storage
· issuance & presentation protocols
(OID4VC, mdoc) · trust verification logic

The App

User interface · biometric unlock · QR/NFC
presenter · hosts the wallet (Multiple apps can
implement the same wallet protocol)

New



Issuer & Verifier of Verifiable credentials

Issuance portals (ministries, universities) · credential signing service · verifier apps & portals

New



Common Trust Infrastructure

Public Key Infrastructure (PKI) · trust registry (authorized issuers & verifiers) · credential schemas ·
VC formats and protocols · credential status service · identity binding service

Mostly new



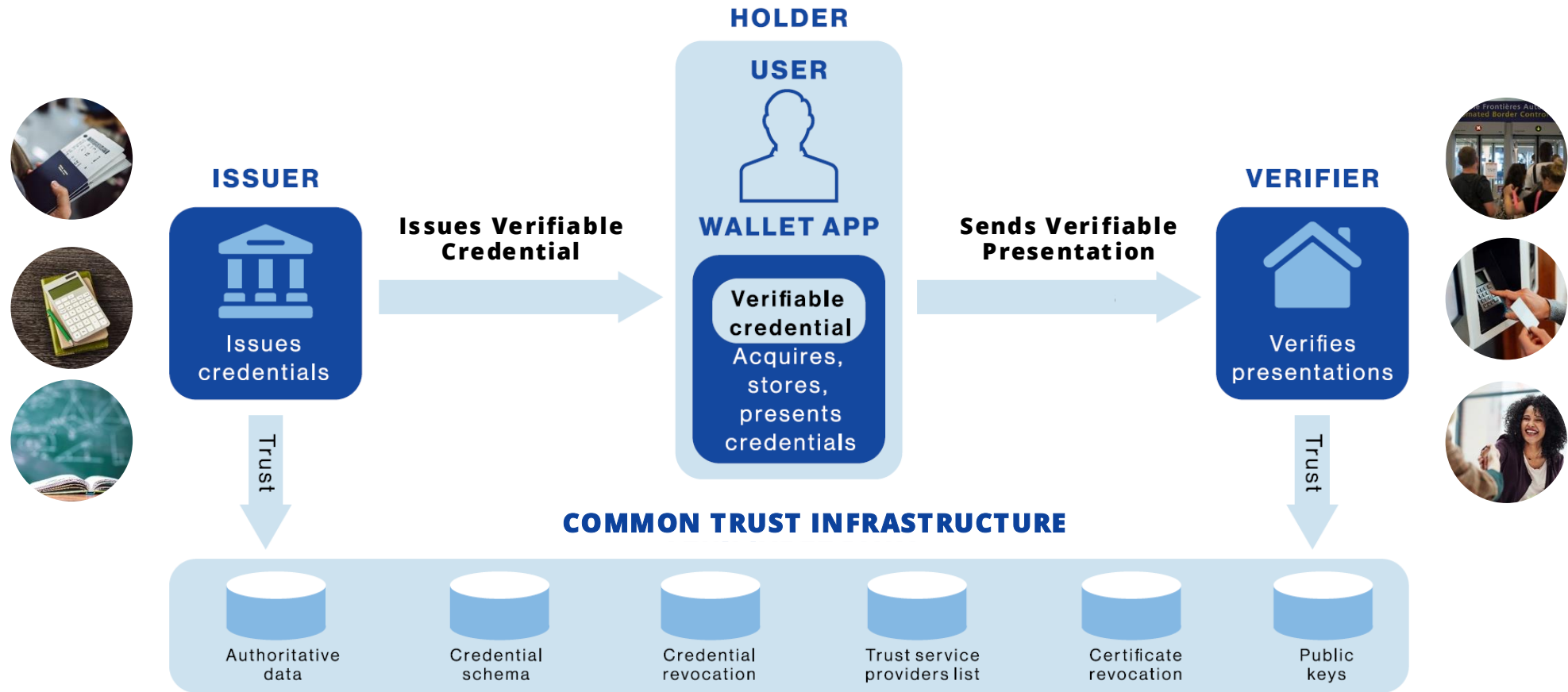
Foundations

Civil registry · National ID systems · Authoritative sources/base registries

You have this



The ID wallet and VC ecosystem





VCs extend trust. They don't create it.

Trust comes from your authoritative sources.

VCs make that trust portable.

If the information in underlying registries are weak, no VCs implementation will fix that.





How to make credentials verifiable?

Information from base registries needs to be coupled with elements of the common trust infrastructure.



Trust registry / List

The authoritative, signed list of authorized issuers, verifiers, and wallet providers, together with their public keys. Tells the verifier whose signatures to trust.



Status and Revocation

Mechanisms to invalidate a credential (holder no longer eligible, wrong data) or an issuer's signing key (compromised). Tells the verifier the credential is still valid today.

Attribute	Definition	Range
familyName	The family name of the person.	LangString
givenName	The given name of the person.	LangString
hasClaim	A claim of the person.	Claim

Schemas and vocabularies

The published structure and meaning of credentials: what fields they contain, what types, what they signify. Let's verifiers in different systems read the same fields the same way.



The Wallet & VCs are the visible part. The Trust Framework is the much bigger part

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam



EM IPSUM

m dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam

B



A

LOREM IPSUM

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam



The Wallet, the App and the VCs

Trust framework

- Strategy
- Technology (Architecture, standards, protocols, security)
- Scheme rules (policies, procedures, roles)
- Compliance
- Agreements and liabilities



You're not building this alone

ROLE	WHAT THEY DO	EXAMPLE
Root of trust for identity	Issue the foundational ID credential. Authoritative source of identity attributes other issuers query before signing.	ID agency, Ministry of Home affairs
Scheme Owner	Define vision, rules, convene	Ministry of Digital Transformation or other Ministry
Supervisory body	Enforce compliance, sanctions	Ministry of Digital Transformation, National Cybersecurity Agency, etc..
Cybersecurity authority	Set & monitor security	National Cybersecurity Agency
Accreditation body	Accredit auditors	National accreditation councils
Conformity assessment body (auditors)	Audit scheme participants	Certified audit firms Specialized digital consultancies
Standards body	Adapt international standards	National standards institutes



Most of you have some of the building blocks already



National ID system?



The authoritative source of identity attributes. Does it have the assurance level you need for the use cases you're targeting?



National PKI already exists?



Your cryptographic trust foundation. Is it fit for issuing credentials at the scale?



Mobile government app already deployed?



Does it have the reach and architecture to host a credential layer?



E-transactions or e-signature law in force?



Is it sufficient legal basis for ID credential validity ?



Digitized registries?



What is the data quality ? Do they expose APIs?



Pick 2-3 use cases that create momentum

The right starting point creates momentum, onboards first issuers and verifiers, and keeps the architecture open for what comes next.

	National Digital ID Credential	Education & Professional Certificate	Cross-Border Trade
VALUE	Anchor credential for KYC, service access, border crossing. Highest adoption leverage.	Diploma fraud is a real and costly problem	Customs clearance from days to minutes. Enables AfCFTA.
VERIFIERS	Banks, government services, border officers	Employers, licensing boards, foreign universities	Customs authorities, port operators, trade finance banks, foreign buyers
CONSTRAINTS	Must work offline if only form of NID. Must work on feature phones. Low-literacy UX essential.	Must be long-lived (20+ years). Must work cross-border . Depends on digitized university registry.	Requires cross-border interoperability



The verifier problem

A credential is worthless until someone accepts it.

Issuance is a one-time push. Verification can happen daily.

Verifier onboarding is harder than issuance. It requires hardware, training, integration, and incentives.





Standards and protocols must be chosen deliberately

The right format and protocol depend on your use case, connectivity context, and cross-border projects.



Credential format

What a credential looks like (data structure and encoding)

W3C VC (JWT-VC / JSON-LD)

Open web standard. Semantic interoperability and linked data.
Strong global ecosystem.

SD-JWT VC

Selective disclosure built in. Growing global adoption (EUDI).

mdoc (ISO 18013-5)

Offline-first, NFC/QR proximity.

+ AnonCreds (Hyperledger / SSI, native ZKP)



Exchange Protocol

How credentials move between actors (issuance, presentation, transport)

**OpenID Foundation standards:
dominant in national programs**

OID4VCI

Issuance: issuer pushes credential into wallet

OID4VP

Presentation: wallet presents credential to verifier

+ DIDComm (SSI stacks)



Privacy by design

VCs are more privacy-preserving than centralized verification by default. But not all privacy properties come automatically.

MECHANISM	WHAT IT DOES	WHAT IT REQUIRES
Selective disclosure	Holder shares only the fields the verifier needs (e.g. date of birth, not address)	SD-JWT VC or mdoc; verifier apps designed for minimum data
Derived attributes	Wallet answers a question without revealing the underlying data: "over 18: yes" without the date of birth	Schema design at issuance; verifier policies that ask the question, not the field
Holder consent	The user approves each presentation. They see what is being requested and from whom.	Wallet UX designed for informed consent; legal recognition of holder choice
Unlinkability & Pseudonymization	Two verifiers receiving credentials from the same person cannot collude to track them across services	Unique copies, batch issuance; ZKP; Pairwise Binding; policy ban on shared identifiers across verifiers
Unobservability	The issuer is not involved in the transaction at the time of presentation, ensuring it doesn't know where you are using it.	Transaction happens only between the phone and the verifier



Inclusion is non-negotiable

Design for the full spectrum: Even as our societies digitalize, “hybrid” services will remain the norm.

Smartphone

Native wallet app. NFC, QR, online presentation.

Feature phone

USSD-based retrieval. SMS-OTP binding. Cloud wallet.

No device • paper credential

Printed VC with signed QR. Verifier scans. Fully cryptographic.

Benin – C'est moi Verifiable credential printed on a card with QR code

- W3C VC standard
- Verifiable offline
- Photo embedded for visual check
- No device needed from holder





Phased rollout approach

Education sector

Phase A

Verifiable Documents (No wallet needed)

Universities issue **digitally signed diplomas with a verifiable QR code, printed or shared as a PDF.** Can still include physical security features.

Any employer can scan the QR to confirm authenticity instantly.

What you need:

- A digitized credential registry
- Solution to sign/verify documents (e.g. PKI)
- No national wallet ecosystem required.

Value delivered:

- Eliminates diploma fraud
- Works for populations without smartphones

Verifies the document, not the person

Phase B

Holder-Controlled Credentials (Basic wallet)

Graduates **store their credentials in a simple government app** or a third-party wallet (e.g., a university app, google/apple wallets). They can share credentials digitally with employers.

What you need:

- Phase A
- a wallet solution (can be sector-specific at this stage)
- legal recognition of electronic credentials (no more paper)

Value delivered:

- Students control their data
- Can be shared remotely

Authenticate holder on top of the document verification.

Phase C

Full Ecosystem Integration (National wallet)

Education credentials are **part of a national wallet where a graduate's diploma sits alongside their national ID,** professional license, and bank account, all interoperable.

What you need:

- Phases A and B
- A national trust framework with a designated scheme owner

Value delivered:

- VC linked to ID)
- Maximum portability across sectors
- Potential for cross border recognition



How to avoid lock-in?

DIMENSION	WHAT GETS YOU STUCK	HOW TO AVOID IT?
Architecture	Proprietary software, closed interfaces, vendor-specific formats, non-standard encryption, source code controlled by vendor	Mandate the use of Open Standards. Modular architecture. Government-controlled HSMs and signing keys.
Procurement & contracts	No IP clauses. No exit management. No source code escrow. Long-tail maintenance contracts. Data formats not specified.	IP ownership specified up front. Exit and transition clauses. Source code escrow. Open data format requirements. Clear licensing terms.
Implementation capacity	All customization done by one integrator. Operational knowledge concentrated.	Build government capacity to maintain. Avoid private forks.



Five things to take home

01 Let your use cases drive the design

Determine your interoperability level, your trust framework needs, and your infrastructure complexity.

02 Be iterative

Trust framework, infrastructure, and ecosystem all scale in phases.

03 VCs extend trust. They don't create it.

Trust comes from your authoritative sources. Weak registries = no wallet will fix that.

04 Design against lock-in from day one

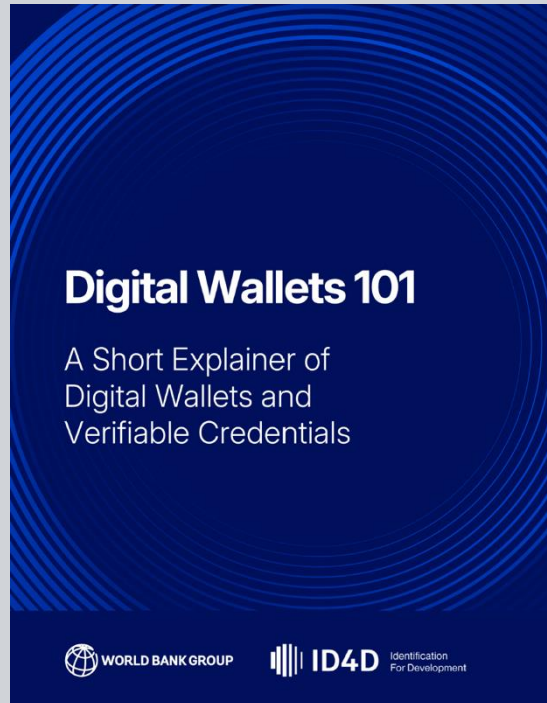
Open standards. Modular architecture. Exit clauses. IP ownership. Government as root of trust.

05 Inclusion and privacy: by design, not by default

Both must be specified in procurement, scheme rules, and law.



The ID4D Digital Wallet Policy Note Series



**Now
Available on
<https://id4d.worldbank.org>**

+ Upcoming | Digital Wallets: Trust Frameworks and Implementation