

Mobile ID

DIGITAL PARTNERS

Mobile ID

The citizen-facing layer of national digital identity

Government-issued identity, held and controlled by the citizen on their own phone. Built on the State's own trust anchor. Delivered as a complete, sovereign-deployed platform that the government owns and operates.

- **FOUR CORE FUNCTIONS**

Authentication · Payment authorisation · e-Consent & signature · Identity verification

- **SOVEREIGN BY DESIGN**

Data, keys and policy stay with the State. Digital Partners never holds citizen data.

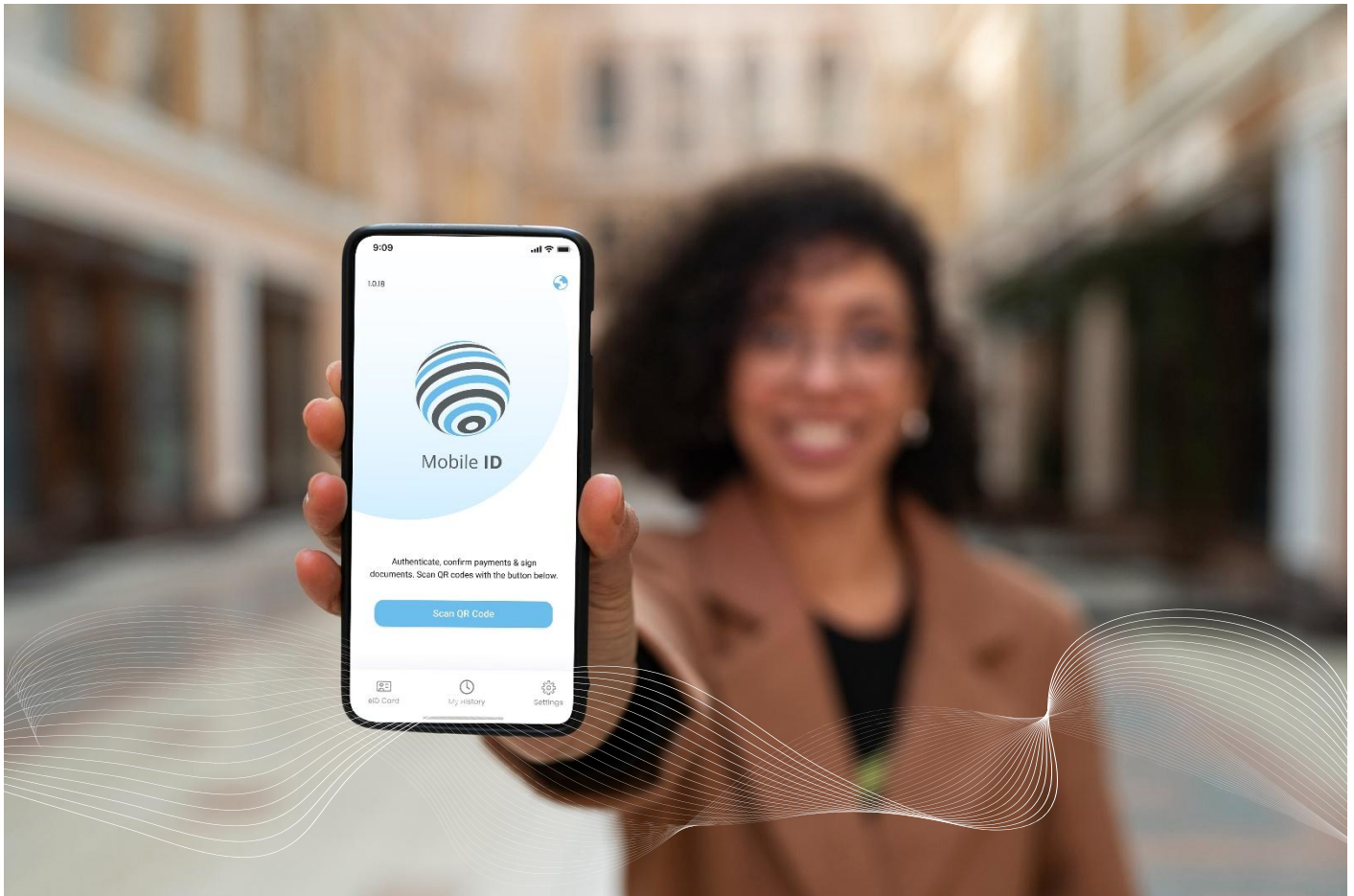
- **LIVE IN PRODUCTION**

Deployed for the Republic of Djibouti.

PRODUCT OVERVIEW

Mobile ID in one view

Mobile ID is the citizen-facing layer of national digital identity: a secure way for citizens to prove their identity, authorise transactions, give consent and verify identity from their mobile phones.



Government-issued identity is held and controlled by the citizen. The platform is deployed on government infrastructure and bound to the State's own trust anchor.

Authentication Sign a challenge with the private key on the citizen's device.	Payment authorisation Sign transaction details so the approval is bound to the amount, payee and moment.
e-Consent & digital signature Give attributable consent or sign as a named individual under the national root.	Identity verification Verify identity attributes against the national register in real time, with consent.

WHAT MOBILE ID IS

Three layers. One clear boundary.

Most national identity programmes already own the hard part: a register of citizens, a national identity number, captured biometrics, and increasingly a national public key infrastructure. What is usually missing is the last mile — a secure way for a citizen to prove that identity from their own phone, to any service, in real time.

Mobile ID is that last mile. It is not a new identity, a new register or a new root of trust. It is the application layer that sits on top of what the State already has.

THE STATE

Sovereign trust layer

National register · national identity number · biometrics · national PKI root and certificate policy. Owns all data, all keys and all policy.

DIGITAL PARTNERS

Citizen-facing application layer

The Mobile ID platform: citizen app, organisation and administration portals, APIs and backend. Installed on government infrastructure and bound to the national root.

THE CITIZEN

Holds the key

A private signing key generated on the citizen's own device, certified under the national root. Every transaction is initiated and signed by the citizen, as an individual.

The analogy we use. Think of a national currency. The central bank owns the mint and decides what a legitimate note looks like. A bank issues wallets and card readers so the money can actually be used in shops. Mobile ID is the wallet and the reader — never the mint.

WHY THIS MATTERS TO A GOVERNMENT

Because the trust anchor stays yours, Mobile ID adds capability without adding dependency. Change supplier, change policy, revoke a credential — the root, the register and the citizen data are untouched, because they were never ours to begin with.

WHAT IT DOES

Four core functions

Every Mobile ID deployment ships with the same four citizen functions. Each is exposed to relying parties — ministries, banks, telecoms, utilities, employers — through a single organisation onboarding process and a common API.

1 Authentication

The citizen proves who they are to a public or private service by signing a challenge with the key on their device. No shared passwords, no one-time codes sent by SMS.

Example. A citizen logs in to the tax portal by scanning a QR code with Mobile ID and confirming with a fingerprint. The portal receives a signed, certificate-backed assertion — not a password.

2 Payment authorisation

The citizen approves a specific transaction by signing its details. The signature is bound to the amount, the payee and the moment — so it cannot be replayed or altered.

Example. A bank shows a transfer for approval inside its own app. The citizen confirms in Mobile ID; the bank receives a signature it can keep as evidence, tied to the customer's national identity.

3 e-Consent and digital signature

The citizen gives legally attributable consent, or signs a document, as a named individual under the national root. Consent is explicit, recorded and revocable.

Example. A hospital requests consent to share records with a specialist. The citizen sees exactly what is being shared and with whom, and signs — or declines — on the phone.

4 Identity verification

A relying party verifies a citizen's identity attributes — name, national number, date of birth, photograph — against the national register in real time, with the citizen's consent.

Example. A mobile operator activates a SIM at a kiosk. The citizen presents a QR code; the operator's verifier confirms the identity against the register in seconds, with no photocopy of a card.

COMMON THREAD

In all four, the citizen initiates the flow and signs as an individual. Control stays with the citizen; evidence stays with the relying party; the root stays with the State.

WHO RELIES ON IT

Government	Tax, social protection, civil registration, e-government portals, elections administration
Financial services	Account opening (eKYC), transaction approval, loan and remittance consent
Telecoms and utilities	SIM registration, contract signature, account access
Health and education	Record-sharing consent, enrolment, results and certificate access
Employers and landlords	Right-to-work checks, tenancy and contract signature

HOW IT WORKS

From enrolment to everyday use

ACTIVATION — THE CITIZEN'S IDENTITY GOES LIVE

1 Authority enrolls

The national authority captures biometrics and issues the national identity number, exactly as today.

2 Citizen activates

The citizen installs Mobile ID and activates it against their record — on the spot, with no wait for a physical card.

3 Key on device

A private key is generated inside the phone's secure hardware and never leaves it.

4 Certified under the root

A certificate for that key is issued under the State's national PKI. The citizen now signs as themselves.

This is why Mobile ID is also a distribution remedy: a citizen who has been enrolled but is still waiting for a card can use their identity the same day.

VERIFICATION — A SERVICE CHECKS THE CITIZEN

1 Citizen initiates

The citizen opens Mobile ID and chooses to present. Nothing is shared until they do.

2 QR presented

A time-bound, single-use QR code is shown to the verifier, or scanned from the service.

3 Citizen consents

The citizen sees exactly which attributes are requested and approves or declines each one.

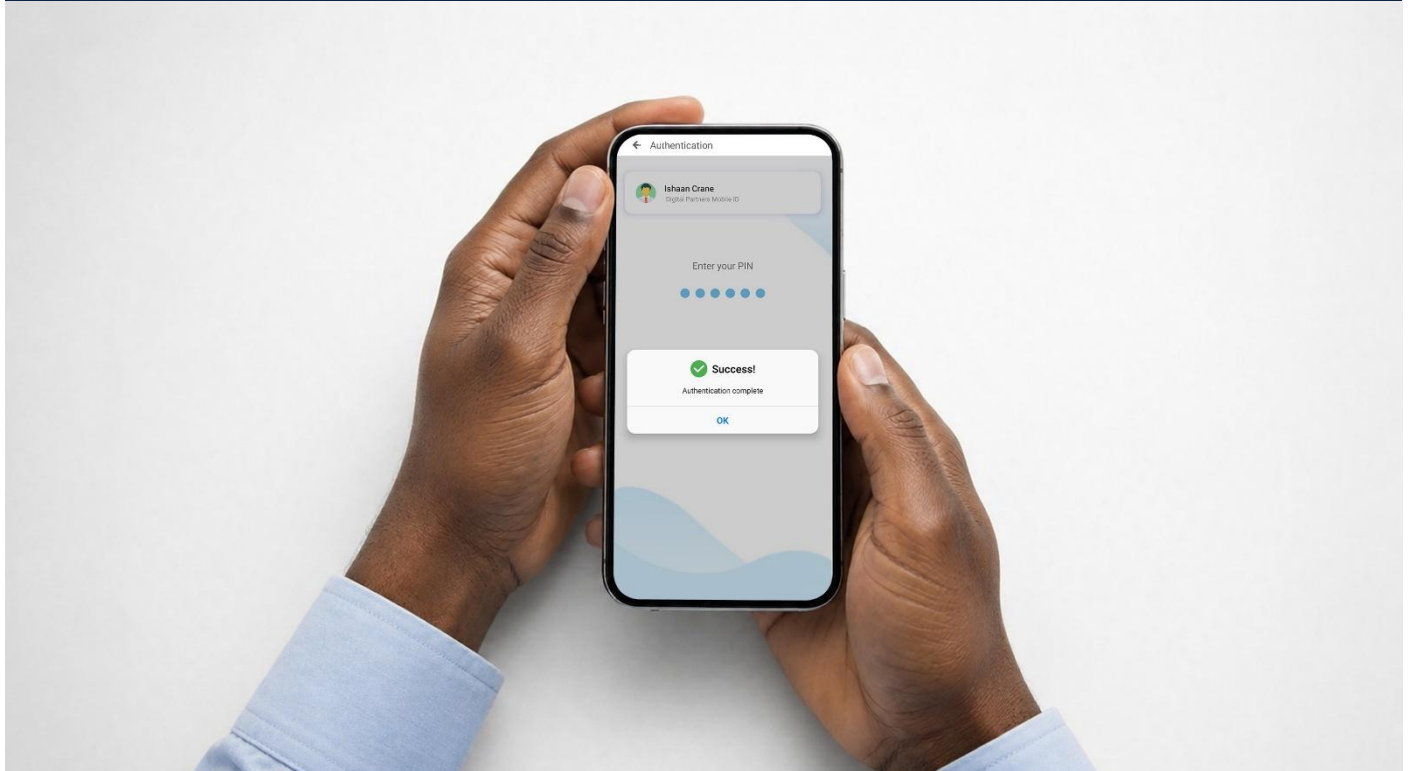
4 Validated live

The relying party validates the signature under the national root and confirms the record against the register in real time.

Verification is by QR code. Because every check is confirmed live against the register, a revoked or suspended identity fails immediately — there is no stale copy on the device to be misused.

A REAL EXAMPLE

A citizen enrolled on Monday walks into a bank on Tuesday to open an account. They have no card. They present Mobile ID; the bank verifies name, national number and photograph against the register, and receives the citizen's signed consent to the account terms. The account is open before they leave.



WHAT YOU RECEIVE

A complete system, not just an app

A citizen app on its own does not make a national programme. Mobile ID is delivered as the full stack needed to run one — every portal, every API and every backend service — installed on the government's own infrastructure.

Citizen application

Registration, activation and day-to-day control. The citizen sees every request, every consent and every signature they have given, and can revoke access.

Organisation portal

Where ministries, banks, operators and other relying parties register, are approved by the Authority, join the interoperability layer and integrate the four functions.

Administration and support portals

The Authority's operational view: relying-party approvals, policy settings, audit, support case handling, and service-desk tooling for citizens.

Marketing and communications portal

Managed content for citizen awareness, onboarding guidance and service announcements — run by the Authority, in its own name.

Backend and APIs

The full server-side platform, integration APIs for relying parties, and connectors to the national register and the national PKI.

Verifier capability

Verification for relying-party staff and services, so a check can be made at a counter, a kiosk or inside a partner app.

INTEGRATES AT ANY LEVEL

Deployments differ. Some governments have a register and no device layer; some have a national PKI already issuing certificates; some have an existing citizen app that needs a signing and assurance capability added. Mobile ID can be delivered as the whole platform, or its functions can be integrated into what already exists. The four functions and the trust boundary are the same in every case.

EXAMPLE

Where a national programme already has a live citizen app, Mobile ID's signing and verification functions can be added inside it as a component — nothing is replaced, and citizens keep the app they know.

OWNERSHIP AND BOUNDARIES

Sovereign by design

The commercial and technical position is the same one: the State owns the identity system; Digital Partners supplies the application layer and the services around it. We think a supplier should say plainly what it is and what it is not.

DIGITAL PARTNERS IS

- + The provider of the citizen-facing application layer
- + The developer and owner of the Mobile ID platform IP
- + The implementation, maintenance and support partner
- + Contractually bound by exclusivity — we do not license competing programmes in your territory

DIGITAL PARTNERS IS NOT

- A certification authority — the national root is yours
- An identity issuer — the register and the number are yours
- A data controller — we never hold citizen data or keys
- A lock-in — the State is not bound to us; only we are bound to the State

WHO OWNS WHAT

Citizen data, register, national number	The State
Root keys, certificate policy, issuance rules	The State
Policy: who may rely, what may be shared, at what fee	The State
Mobile ID platform software and IP	Digital Partners
Deployment, integration, operation and support services	Digital Partners

STANDARDS WE BUILD TO

World Bank ID4D Principles on identification: inclusion, sovereignty, no vendor lock-in.	FATF Digital ID Identity assurance aligned to global AML expectations.	ITU-T X.509 Certificate-based trust, issued under the State's own national PKI.	Data protection KVKK compliant, GDPR aligned, citizen data resident in country.
--	--	---	---

WORKING WITH YOUR NATIONAL PKI

Not every country's PKI is at the same stage, and what Mobile ID can honestly claim depends on it. We assess this openly at the start of every engagement, and position the deployment accordingly.

1 Announced PKI planned, not yet issuing. Deploy on interim trust, with migration to the national root designed in.	2 Government only Root live for government systems. Integrate now; citizen certificates follow when policy allows.	3 Organisations Root issues to organisations. Relying-party trust is national; citizens next.	4 Citizens Root issues to citizens. Citizen keys certified directly under the sovereign root.
---	--	---	---

TRUST AND SECURITY

Evidence, not assurance

Security claims in this field are easy to make. We prefer to describe the mechanisms and let your own engineers judge them. Everything below is in the product as deployed today.

Key held by the citizen

Each citizen's private key is generated inside the phone's secure hardware and cannot be exported. Signatures are therefore attributable to one person and one device — the basis for non-repudiation.

Certified under the national root

Citizen certificates follow the ITU-T X.509 standard and are issued under the State's own PKI and certificate policy. Trust chains to the government, not to a vendor.

Real-time validation

Every authentication and verification is confirmed live against the national register. Revocation takes effect immediately; nothing stale lives on the device.

Time-bound, single-use presentation

Verification QR codes expire quickly and cannot be reused. A screenshot of a code is worthless a minute later.

Minimal disclosure by consent

The citizen sees each attribute a relying party asks for and approves them individually. Consent is recorded and can be withdrawn.

Sovereign deployment

The platform runs on government infrastructure. Digital Partners' own build environment is entirely separate and no build-environment certificate carries into a deployment.

WHAT WE DO NOT CLAIM

Mobile ID does not read the chip in a physical card, and it is not an offline credential: it is designed around live confirmation with the register. We do not present ourselves as a trust service provider. Where a country's national PKI is still maturing, we say so, and we describe what can be claimed at each stage rather than assuming the strongest case.

Honest positioning is, in our experience, what a national programme remembers a supplier for.

PROVEN IN DEPLOYMENT

Republic of Djibouti

Mobile ID is deployed for the Republic of Djibouti as the citizen-facing layer above the State's own register and trust anchor, with relying parties onboarded through the Mobile ID organisation portal. The Authority holds the root and controls the data; Digital Partners delivered and supports the platform.

REQUEST A BRIEFING

Start with a working session

We do not begin with a demonstration. We begin with a discovery session on what your programme already holds — register, identity number, biometrics, PKI — and produce a written programme map showing exactly where Mobile ID fits, what it would claim, and what it would not.

DIGITAL PARTNERS

Sultan Selim Mah. Eski Büyükdere Cad.
No: 61, Levent / İstanbul, Türkiye.
www.digitalpartners.tech