



Mobile ID

DIGITAL PARTNERS • MOBILE ID

Capability Overview

The citizen-facing layer of a national digital identity programme

DP-CAP-001 • Version 1.2 • August 2026

Prepared for national identity authorities, digital public infrastructure programmes and multilateral development partners.

AT A GLANCE

What it is	A government-issued identity credential held on the citizen's own phone, with the private signing key held on the device.
Architecture	Centralised. Credentials are X.509 certificate-based. Every verification performs a real-time check against the issuing authority's register.
Core functions	Authentication • Payment authorisation • E-consent and digital signature • Identity verification.
What is delivered	A complete end-to-end system: citizen application and control platform, organisation registration and administration portals, support and marketing portals, full backend and frontend.
Who owns what	The State owns the register, the trust anchor and the policy. Digital Partners supplies, integrates and maintains the application layer.
Where we are	Head office in Istanbul, Türkiye. Africa branch registered in Nairobi, Kenya.

1. What Mobile ID is

Most national identity programmes solve two of the three problems well. They build a register, and they build a trust anchor. What they often lack is the third: a way to put a usable, verifiable credential into the citizen's hand and let them present it, consent with it and sign with it.

The distinction is easiest to see as a currency system. The State runs the mint — it decides who exists, what a credential means and which certificates are trustworthy. The relying party runs the till — the bank branch, the ministry portal, the telecom shop that has to accept the credential and check it. Mobile ID is the wallet in between: the thing the citizen actually carries, opens and uses.

Digital Partners does not run the mint and does not run the till. We build, deploy and maintain the wallet, and the portals and interfaces that connect it to both sides.

2. The four core functions

FUNCTION	WHAT IT DOES
Authentication	The citizen proves who they are to a public or private service, with the assertion signed by the key on their device.
Payment authorisation	The citizen approves a payment instruction with a signature that is bound to that specific instruction.
E-consent and digital signature	The citizen signs a document, a consent or a mandate, producing evidence that can be checked afterwards.
Identity verification	A relying party confirms an identity claim against the authority's register in real time, rather than against a stored copy.

In every one of these, the citizen initiates the flow and signs as an individual. Nothing is asserted on the citizen's behalf without an action on their device. This is what allows a transaction to be defended afterwards: the evidence chains back to a key the citizen holds, under a certificate issued by the country's own authority.

3. What is delivered

Mobile ID is not a single application. A national deployment includes:

- **Citizen layer** — the application the citizen installs, and the platform through which they manage their credential, devices and consents.
- **Organisation layer** — registration and administration portals through which banks, ministries, telecoms and other relying parties are onboarded, configured and monitored.
- **Operational layer** — support portals for the authority's helpdesk, and marketing portals for citizen adoption campaigns.
- **Technical layer** — full backend and frontend, with interfaces that can be integrated at whatever level the programme requires — direct to the register, through an interoperability layer or enterprise service bus, or through an SDK embedded in an existing government application.

One consequence worth naming: where an authority captures biometrics and issues a national identity number, the citizen's digital identity can be activated at that moment. They do not have to wait for a physical card to be printed and distributed before they can use their identity.

4. How trust works

- **The key sits with the citizen.** The private key that produces the citizen's signature is generated and held on the citizen's device. Digital Partners never holds it.
- **Certificates chain to the country's anchor.** Credentials are X.509 certificates. Where a country operates a national root that issues natural-person certificates, Mobile ID credentials are issued under that root, so the trust chain terminates at the State's own anchor.

- **Verification is live.** Verification is not an offline check against a cached copy. Each authentication queries the issuing authority's register, so a revoked, suspended or superseded credential fails at the point of use.
- **Evidence, not assertion.** Because the signature is bound to the specific instruction and to a device-held key, a relying party can show what was signed, by whom, and when.

5. Role and boundaries

An identity vendor that will not state its limits is a risk to the programme buying from it. Ours are:

- **We are not a CA.** We do not operate a certification authority and do not seek to become the country's trust anchor.
- **We are not the identity issuer.** We do not decide who exists or what a credential means. The authority does.
- **We are not the data controller.** Citizen data and cryptographic keys sit in government infrastructure. We process only what the deployment contract requires, under the authority's instruction.
- **There is no vendor lock-in.** The platform integrates with existing registers, PKI and interoperability layers. Source code and continuity arrangements are agreed as part of the deployment.
- **Exclusivity binds us, not you.** Where a territory is exclusive, the obligation is on Digital Partners not to licence a competing programme in that territory. It does not bind the State to us.
- **Deployment is sovereign.** Citizen data and cryptographic keys remain in government infrastructure. The government owns its data, its keys and its policy; Digital Partners retains ownership of the platform intellectual property.

6. Where Mobile ID sits

LAYER	OWNER	CONTENT
Legal and policy	State	Electronic transactions and signature law, data protection law, identity policy.
Register	National identity authority	The population or civil register and the identifiers it issues.
Trust	State or licensed authority	National PKI, root and issuing certification authorities, certificate policy.
Application	Digital Partners	Device credential, citizen platform, relying-party portals, verification interfaces.

Where a country has already invested in the first three layers, Mobile ID is additive: it makes that investment reach the citizen. Where the trust layer is not yet issuing natural-person certificates, we say so at the outset and scope accordingly, rather than describing the deployment as sovereign trust when it is not yet.

7. Standards and reference frameworks

- ITU-T X.509 for certificate-based credentials and trust chaining.
- Designed against the World Bank ID4D Ten Principles on Identification for Sustainable Development.
- Data protection aligned to the national data protection law of the deployment country; Digital Partners' own corporate processing is governed by Türkiye's KVKK.
- Certificate policy and practice statements of the deployment country's national PKI, where one is in operation.

8. Who this is for, and the next step

- National identity authorities and ministries building or modernising a citizen digital ID programme.
- Digital public infrastructure programmes looking for a vendor-supported credentialing layer.
- Regional and multilateral development programmes evaluating identity partners for member states.

Engagement models are shaped around the programme's funding position and procurement route, and are discussed once that position is understood. We do not propose a commercial structure before we have mapped the programme.

A briefing is a working session, not a sales presentation. We map what your programme already has — the register, the PKI, the legal basis — and show where Mobile ID would and would not add value. There is no cost and no procurement step attached to it.

Request a briefing: info@digitalpartners.tech

Digital Partners · Sultan Selim Mah. Eski Büyükdere Cad. No: 61, İç Kapı No: 1, Kağıthane 34400, İstanbul, Türkiye · digitalpartners.tech