



Mobile ID

DIGITAL PARTNERS

TECHNICAL ARCHITECTURE OVERVIEW

Mobile ID

How the platform is built, where the trust sits, and where the boundaries are

A description of the Mobile ID platform for the technical teams of national identity authorities, their PKI and interoperability partners, and relying parties preparing to integrate. It covers the four-layer stack, platform components, the trust and key architecture, the core APIs, the principal flows, integration points and security controls.

- **CENTRALISED, PKI-BASED**

Citizen credentials are X.509 certificates issued under the national root; every check is confirmed live against the register.

- **CITIZEN HOLDS THE KEY**

Private keys are generated on the citizen's device and never leave it. Digital Partners holds no citizen key and no CA key.

- **SOVEREIGN DEPLOYMENT**

The whole platform runs on government infrastructure. Digital Partners' build environment is entirely separate.

DP-ARC-001 · Version 1.0 · September 2026

www.digitalpartners.tech

ARCHITECTURE AT A GLANCE

Mobile ID within the national identity stack

Mobile ID sits between the State’s identity and trust infrastructure and the citizen’s device. The State remains the authoritative source for identity and trust, while Mobile ID provides the application and integration layer through which citizens and approved relying parties interact.



The State owns the identity system and trust anchor. The citizen’s device holds the private signing key, while the Mobile ID platform connects the two through defined, controlled interfaces.

Sovereign trust layer National identity register, identity number, biometric enrolment and national PKI form the State’s authoritative trust foundation.	National interoperability layer The government service bus or interoperability gateway connects Mobile ID and relying parties to authoritative national services.
Mobile ID platform layer Backend services, portals, verification capability and relying-party APIs provide the application and integration layer.	Citizen device layer The citizen’s smartphone holds the Mobile ID app, certificate and device-bound private key used to approve and sign requests.

PURPOSE AND SCOPE

What this document describes

This overview explains how Mobile ID is built and how it fits into a national digital identity programme. It is written for technical readers: the identity authority's engineering and security teams, the operator of the national PKI, the interoperability or e-government service bus team, and the integration teams of relying parties. It is deliberately descriptive rather than promotional: it describes the platform as deployed today.

It does not replace a deployment-specific solution architecture. Every national deployment is mapped to the country's own register, PKI and interoperability layer, and that mapping is documented separately during the discovery phase.

DESIGN PRINCIPLES

The State is the root of trust

Mobile ID does not operate a certification authority and does not issue identity. Citizen certificates are issued under the State's national PKI, and identity attributes come from the State's register.

The citizen holds the key

Every citizen has a private signing key generated on their own device. Signatures are attributable to one person on one device. No party, including Digital Partners, can sign on a citizen's behalf.

Live confirmation, not cached copies

Every authentication and verification is confirmed in real time against the national register. Revocation is immediate. No identity data sits on the device to be copied or misused.

Citizen-initiated, consent-bound

Every flow starts with the citizen. A relying party can request, but nothing is released until the citizen approves each requested attribute.

Sovereign infrastructure

The platform is installed on the government's infrastructure and bound to the national PKI. Citizen data never leaves the country and never reaches Digital Partners.

Complete and open at every layer

Mobile ID is the whole stack (app, portals, backend, APIs) and each layer exposes documented interfaces, so it can be delivered whole or integrated into what already exists.

ARCHITECTURE

The four-layer stack

Mobile ID sits at layer 3. Layers 1 and 2 are the State's, and Mobile ID consumes them through defined interfaces; layer 4 is the citizen's own device. The boundary between layers 1 and 3 is the most important line in the architecture: the platform never holds a CA key, never holds a citizen key, and never becomes an authoritative source of identity data.

4	Citizen device layer Owned by: Citizen	Mobile ID app on the citizen's smartphone (iOS and Android). Holds the device-bound private key and the citizen's certificate; presents QR codes; captures consent and biometric confirmation.
3	Mobile ID platform layer Owned by: Digital Partners (software) · Authority (operation)	Backend services, citizen and organisation registration, consent and signature services, verification services, administration, support and marketing portals, relying-party APIs and verifier capability.
2	National interoperability layer Owned by: State	The e-government service bus or interoperability gateway through which relying parties and the platform reach the national register and other authoritative sources.
1	Sovereign trust layer Owned by: State	National identity register, national identity number, biometric enrolment, national PKI root and certificate policy. The single source of truth for identity and the anchor for all certificates.

HOW THE LAYERS INTERACT

- **Layer 4 → 3.** The app talks only to the Mobile ID backend, over TLS, using the device-bound key to sign every request that carries a decision (activation, consent, authorisation, signature).
- **Layer 3 → 2 → 1.** The backend reaches the register and the PKI through the national interoperability layer. It reads identity attributes for verification and submits certificate signing requests for issuance; it never writes to the register.
- **Relying parties → 3.** Relying parties integrate only with the Mobile ID APIs. They never see the citizen's key, and receive identity attributes only as signed, consented responses.
- **Verifiers → 3.** Verification at a counter or kiosk is a relying-party call in which the presented QR code is the transaction reference; the answer comes from the platform, not from the phone.

PLATFORM COMPONENTS

What is delivered at layer 3

The platform is delivered as a complete system. Each component below is installed on the Authority's infrastructure and operated under the Authority's control, with Digital Partners providing maintenance and support.

COMPONENT	FUNCTION	PRIMARY USERS
Citizen application	Registration and activation; key generation and certificate enrolment; presentation of QR codes; consent, authorisation and signature confirmation; history of every request and revocation of standing consents.	Citizens
Organisation portal	Registration of relying parties; approval workflow by the Authority; API credential issuance; selection of permitted functions and attributes; integration documentation and sandbox access.	Relying parties; Authority approvers
Administration portal	Platform configuration and policy (which attributes exist, which may be requested, fees where applicable); relying-party lifecycle; certificate lifecycle oversight; audit and reporting.	Authority operations
Support portal	Citizen and relying-party case handling; device loss and re-activation; suspension and reinstatement; service-desk tooling.	Authority support staff
Marketing & communications portal	Managed content for citizen awareness, onboarding guidance and service announcements, published in the Authority's name.	Authority communications
Backend services	Identity, consent, signature and verification services; certificate enrolment and status; audit logging; connectors to the register, PKI and interoperability layer; the five relying-party APIs (section 5).	All of the above, via APIs
Verifier capability	Verification of a presented QR code by relying-party staff or systems at a counter, kiosk or within a partner application.	Relying-party front line

DEPLOYMENT TOPOLOGY

National deployment (production)

All components run on infrastructure the Authority owns or contracts. Data, logs and backups stay in country; certificates are issued under the national root. Support access for Digital Partners is granted and controlled by the Authority.

Digital Partners build environment

Development and testing run on Digital Partners' own, entirely separate infrastructure with its own certificates. Nothing from it — no key, certificate or data — carries into a national deployment.

Authority sandbox

A non-production instance on the Authority's infrastructure, with the Authority's test certificates, for relying-party integration testing before production access.

Environment separation

Production and sandbox are separate installations with separate credentials. Promotion to production follows Authority approval in the organisation portal.

TRUST AND KEY ARCHITECTURE

Where every key lives

The architecture is built around a single rule: the key that proves a citizen's identity is created and kept by that citizen, and the authority that vouches for it is the State. The table sets out every key and certificate in the system, who holds it and who may use it.

KEY OR CERTIFICATE	HELD BY	ISSUED BY	USED FOR
National root and issuing CA keys	State (national PKI operator, in its HSM)	State	Signing citizen certificates and status. Never held or accessed by the platform.
Citizen private key	Citizen (device secure hardware, non-exportable)	n/a — generated on device	Signing challenges, authorisations, consents and documents. Never leaves the device.
Citizen certificate (X.509)	Citizen device; public copy in the platform	State's issuing CA, on a CSR via the platform	Binding the public key to the national identity number under the national certificate policy.
Platform TLS certificates	Platform (Authority infrastructure)	State PKI or a public CA, per Authority policy	Protecting all API and app traffic in transit.
Relying-party API credentials	Relying party	Platform, on Authority approval	Authenticating relying-party systems to the APIs; scoped to permitted functions and attributes.

CERTIFICATE LIFECYCLE

1	Activation	The verified citizen activates the app; it generates a key pair on the device and a CSR carrying the public key and national identity number.
2	Issuance	The platform submits the CSR to the State's issuing CA; the CA issues under the national policy; the platform returns the certificate to the device.
3	Use	Every signed transaction carries the certificate reference; signature and status are validated against the national PKI through the platform.
4	Renewal	Before expiry the app generates a new key pair and the cycle repeats. The old key is destroyed on the device.
5	Revocation	On device loss, suspension or request, the Authority revokes at the CA and the platform marks the identity inactive. Subsequent checks fail immediately.

THE CUSTODY BOUNDARY

Digital Partners never holds a national CA key or a citizen private key, in any environment. The platform submits requests to the State's CA and stores public certificates; it cannot issue and cannot sign as a citizen. Where a national PKI does not yet issue natural-person certificates, the deployment is positioned at that stage with a migration path designed in — the platform never substitutes its own root for the State's.

CORE APIS

The five relying-party interfaces

Relying parties integrate through REST APIs exposed by the platform. Each API follows the same pattern: the relying party creates a request; the platform notifies the citizen; the citizen approves in the app by signing with the device key; the relying party receives a signed, verifiable result. Access to each API and to each attribute is granted per relying party in the organisation portal.

API	RELYING PARTY SENDS	CITIZEN SEES AND APPROVES	RELYING PARTY RECEIVES
Onboarding	Reference of the citizen to be linked (e.g. national identity number) and the account to be created.	Request to link their Mobile ID to the relying party's service.	Confirmation of the link, signed by the citizen, with the consented attributes.
Client authentication	A login challenge bound to a session, and the attributes required.	Which service is asking, and which attributes will be released.	The signed challenge, certificate reference and status result — a verified login without a password.
Payment authorisation	Transaction details: amount, currency, payee, reference, time window.	The exact transaction, presented for approval.	A signature over the transaction details, usable as non-repudiable evidence.
e-Consent signature	The document or consent statement (or its hash) and the attributes to bind.	The document or statement, and what will be shared with whom.	A citizen signature over the document hash, with certificate reference and timestamp.
Digital ID verification	A presented QR code (or a verification request) and the attributes to be confirmed.	Which attributes are requested; approval or denial of each.	The consented attributes, confirmed live against the national register, with the platform's signed response.

COMMON CHARACTERISTICS

- **Time-bound.** Every request carries an expiry. QR codes are single-use and short-lived; an expired or reused code is rejected.
- **Attribute-scoped.** A relying party can only request the attributes the Authority has permitted it, and the citizen may decline any of them individually.
- **Evidence-producing.** Every approval returns a signature the relying party can store and later validate independently against the national PKI.
- **Auditable.** Every request, approval, denial and expiry is logged on the platform, visible to the Authority and, for their own history, to the citizen.
- **Sandbox-first.** Every API is available in the Authority sandbox with test identities before production credentials are issued.

PRINCIPAL FLOWS

Activation, verification, onboarding

6.1 Citizen activation

1	Authority	Enrols the citizen: captures biometrics and issues the national identity number in the register. This step is unchanged by Mobile ID.
2	Citizen	Installs the app from the public app store. Attends the designated activation point, or completes remote activation where the Authority's policy permits, and is verified against the register.
3	App	Generates a key pair in the device's secure hardware. Builds a certificate signing request with the public key and national identity number and sends it to the platform.
4	Platform	Submits the CSR to the State's issuing CA through the agreed interface; receives the certificate; binds it to the citizen record; returns it to the device.
5	Citizen	Sets biometric or PIN confirmation for signing. Mobile ID is live – the same day as enrolment, with no dependency on a physical card.

6.2 Verification at a service point

1	Citizen	Opens the app and chooses to present. The app requests a single-use, time-bound QR code from the platform and displays it.
2	Verifier	Scans the code with the verifier capability or the relying party's own integrated application. The code is only a reference; it contains no identity data.
3	Platform	Sends the citizen a request naming the relying party and the attributes sought.
4	Citizen	Approves or declines each attribute and confirms with biometric or PIN; the app signs the approval with the device key.
5	Platform	Validates the signature and certificate status against the national PKI, confirms the attributes live against the register, and returns a signed response to the verifier.

6.3 Relying-party onboarding

1	Relying party	Registers in the organisation portal: legal identity, service description, requested functions and attributes, technical contacts.
2	Authority	Reviews and approves the application against its own policy; sets permitted functions, attributes and any fees.
3	Platform	Issues sandbox credentials. The relying party integrates and tests against test identities.
4	Authority	Approves promotion to production. Production credentials are issued; the relying party appears to citizens as an approved service.

INTEGRATION POINTS

What the platform connects to

The platform depends on four external interfaces, all on the State's side of the boundary. The exact protocols are agreed per deployment during discovery; the table records what each interface is for and what the platform needs from it.

INTERFACE	PURPOSE	PLATFORM NEEDS	PLATFORM NEVER DOES
National identity register	Confirm a citizen's identity attributes at activation and at every verification.	Read access to agreed attributes by national identity number, via the interoperability layer.	Write to the register or hold a copy of it.
National PKI (issuing CA, CRL/OCSP)	Issue citizen certificates; check certificate status.	A CSR submission interface conforming to the CA's certificate policy and practice statement; a status endpoint.	Hold a CA key, act as a registration authority beyond what the Authority delegates, or issue under its own root.
Interoperability layer / service bus	Route platform calls to the register and other authoritative sources under national governance.	Membership as a registered service, with the routing and authentication the layer mandates.	Bypass the layer to reach the register directly.
Relying-party systems	Deliver the five core functions into public and private services.	A registered, approved relying party with API credentials and, where used, a callback endpoint.	Expose citizen keys or unconsented attributes.

DATA RESIDENCY AND AUDIT

Data held by the platform

Citizen record link (national identity number and certificate reference), consents given, transaction evidence (signatures and hashes, not documents), audit logs. All resident in country on Authority infrastructure.

Data not held by the platform

Citizen private keys, biometric templates, the register itself, documents signed (only their hashes), and any copy of identity data outside the country.

Audit

Every API request, citizen decision, certificate event and administrative action is logged with time, actor and outcome. Logs are the Authority's and are available to it in full.

Legal basis

The Authority is the data controller; Digital Partners acts as processor only to the extent of support access the Authority grants, under the Authority's instructions and controls.

SECURITY CONTROLS

Mechanisms, and their limits

Everything in this section is in the platform as deployed. The final panel records what the platform does not do, so that no reader has to discover a limit during procurement.

Device-bound keys

Private keys are generated in and never leave the phone's secure hardware. Signing requires the citizen's biometric or PIN confirmation on the device.

Certificate-based signatures

All citizen decisions are X.509-based signatures validated against the national PKI, with status checked at every use.

Single-device binding

A Mobile ID is bound to one device. A new device requires re-activation; the previous certificate is revoked.

Transport protection

All app and API traffic runs over TLS. Relying parties authenticate to the API with scoped credentials issued on Authority approval.

Single-use, time-bound codes

QR codes and requests expire quickly and cannot be replayed. A captured code is useless after its window.

Consent enforcement

Attribute release is enforced by the platform per relying party and per request, not left to the relying party's integration.

Live status

Every check confirms certificate status and register status in real time. Suspension or revocation takes effect immediately.

Environment separation

Production, sandbox and the Digital Partners build environment are separate installations with separate certificates and credentials.

WHAT THE SOLUTION DOES NOT DO

It does not read the chip in a physical card, and it does not offer offline verification: every check requires connectivity to the platform. It does not operate a certification authority, and Digital Partners does not present itself as a trust service provider. It does not implement decentralised or holder-only verification models; credentials are X.509 certificates, and verification is centralised by design. Where a national PKI does not yet issue natural-person certificates, the deployment is positioned at that stage and a migration path is designed in.

From overview to deployment architecture

This document describes the platform in general. The deployment architecture for a specific country is produced during discovery, and records the mapping to that country's register, PKI, interoperability layer and policy, together with the environment design, interface specifications and security assessment.

DISCOVERY COVER

- Register and national identity number: attributes, access route, governance
- National PKI: certificate policy, issuance interface, status service, maturity stage
- Interoperability layer: membership, routing, authentication
- Infrastructure: hosting, environments, residency and backup
- Relying-party landscape and phasing
- Security assessment and acceptance criteria

DIGITAL PARTNERS

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

© 2026 Digital Partners. All rights reserved.