



Mobile Application "Digital Citizen"

Together in the digital era!

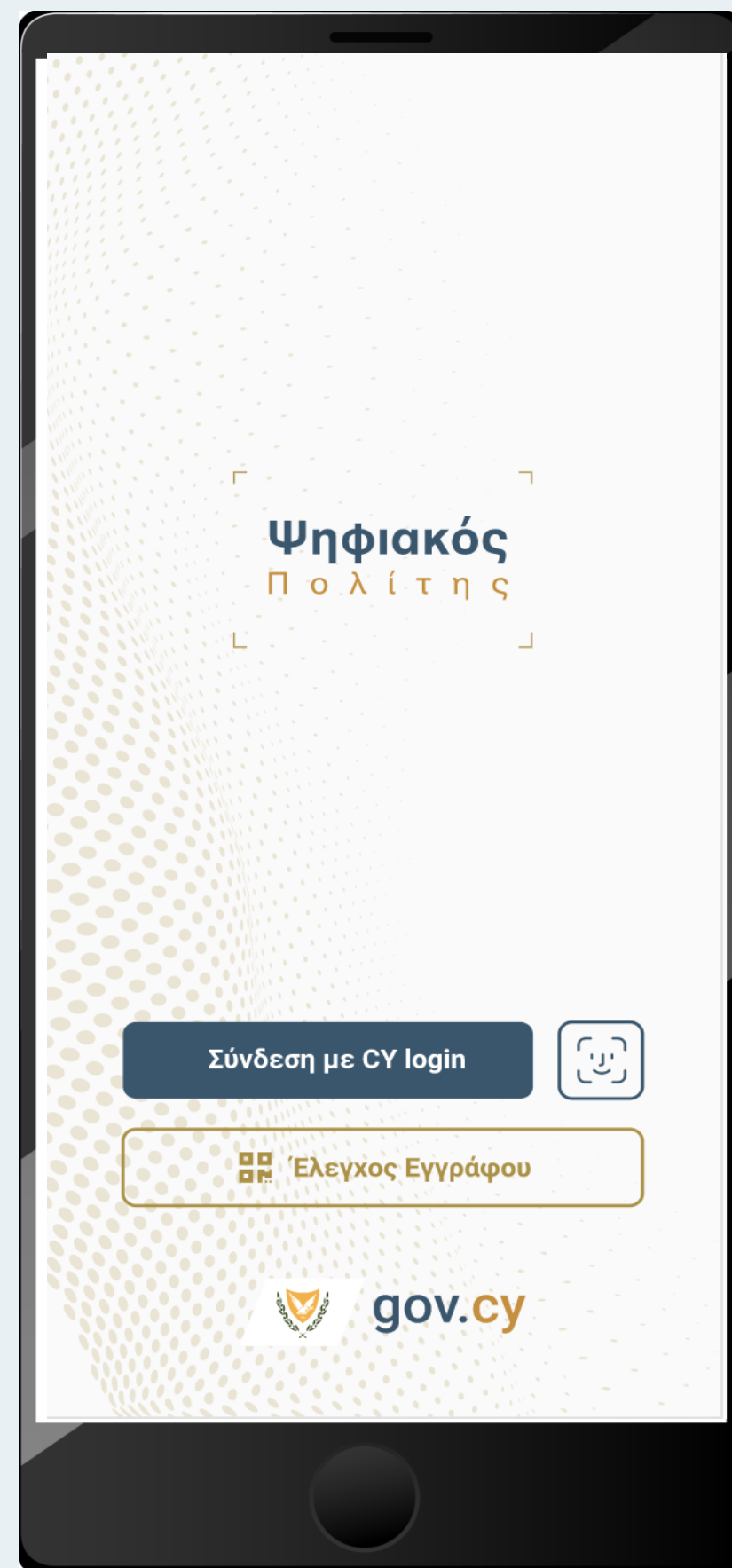


DEPUTY MINISTRY OF RESEARCH, INNOVATION AND DIGITAL POLICY



DEPUTY MINISTRY OF RESEARCH, INNOVATION AND DIGITAL POLICY

What is the "Digital Citizen" mobile application



Digital Citizen mainly consists of a mobile application that allows citizens to register via CY Login and add different types of their documents in digital form. Likewise, it allows the national authorities and private entities to directly validate the authenticity of documents and digitally verify the citizen's details.

Legal Basis / Acceptance of Digital Citizen Documents



The digital form of the public documents in the Digital Citizen application is equivalent to the corresponding physical document, for any lawful use within the territory of the Republic of Cyprus.



For every document integrated into the Digital Citizen application, appropriate legislation must be put in place so that the digital form of the document has the same legal force as the printed form.

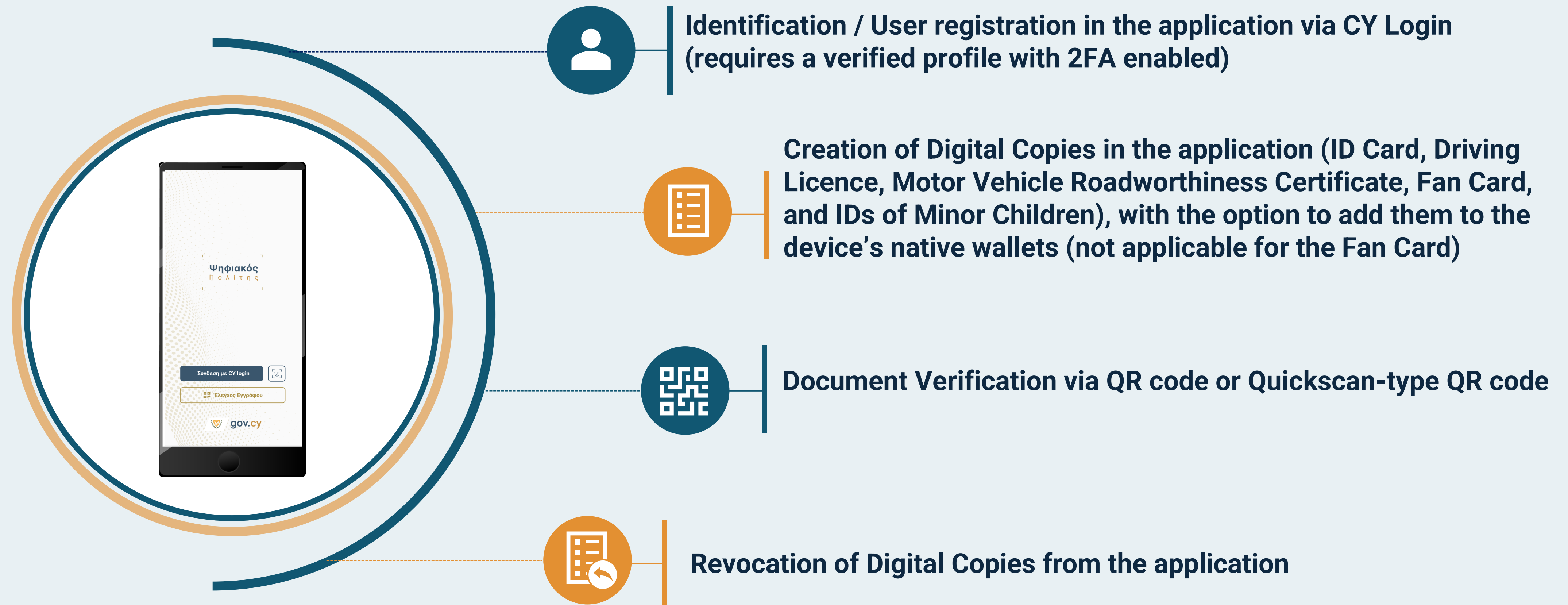


At this stage, the legal regulation has been completed both for the identity card (Decision of the Director-General of the Ministry of Interior) and for the driving licence (Order under section 57A(1) / K.D.P. 381/2024).



Current functions of the Digital Citizen application

Main Functions



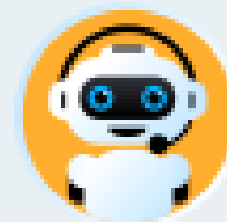
Additional Functions



App accessibility
for ages 14-18



Greek & English versions



Digital Assistant



CY-GR document interoperability
(for Id and driving license only)



DEPUTY MINISTRY OF RESEARCH, INNOVATION AND DIGITAL POLICY

Upcoming features of the application

Sports Event Tickets

Adding sports event tickets (football first division only) to the application, enabling stadium entry using a barcode.

Automatic Document Refresh

Updating documents that have expired in the citizen's application by automatically fetching their new issued document.

Non Cypriots' Documents

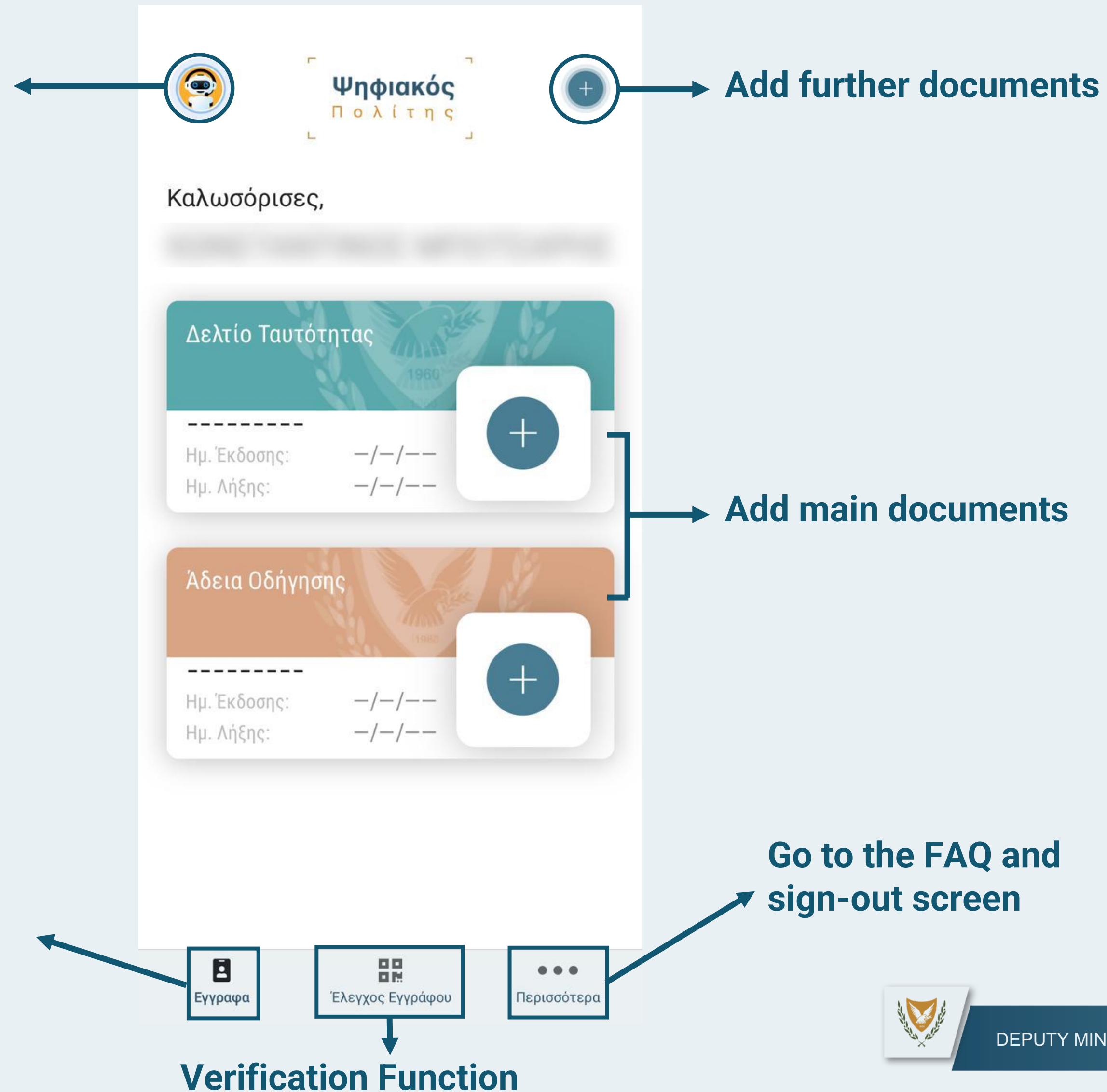
Issuance of electronic copies of non-Cypriot nationals' documents (registration/residence permit) in the application.

The upcoming features will be available prior to the award of the Contract

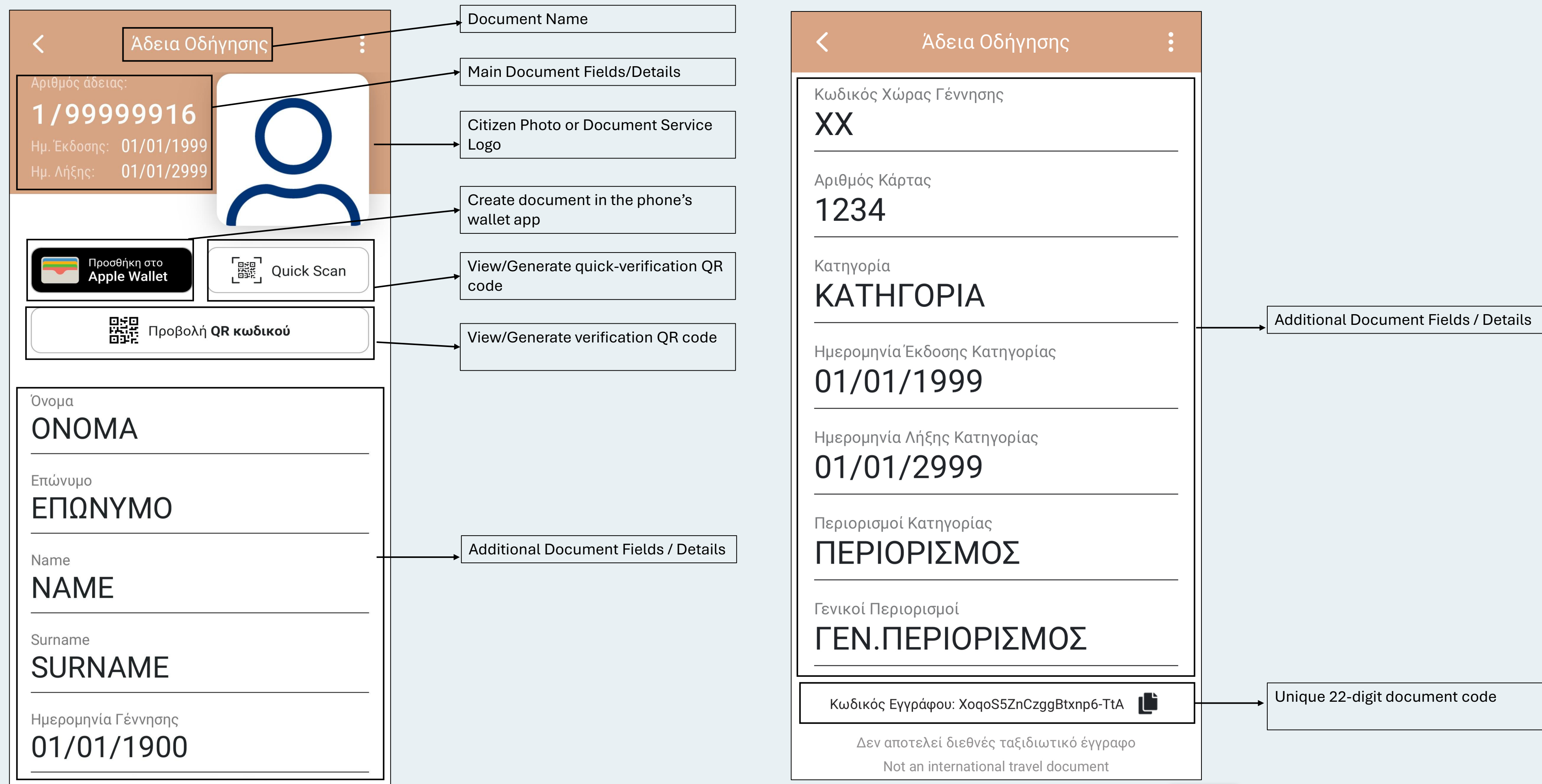


The Digital Citizen home document list screen

Digital Assistant Function



Anatomy of a document in Digital Citizen



Technical Architecture of the “Digital Citizen” Solution



4 core architectural components: mobile application (iOS/Android) + mobile backend, FLEX Gateway (API Gateway & core backend APIs), digital document verification service/website (for public sector only), and citizen support platform.



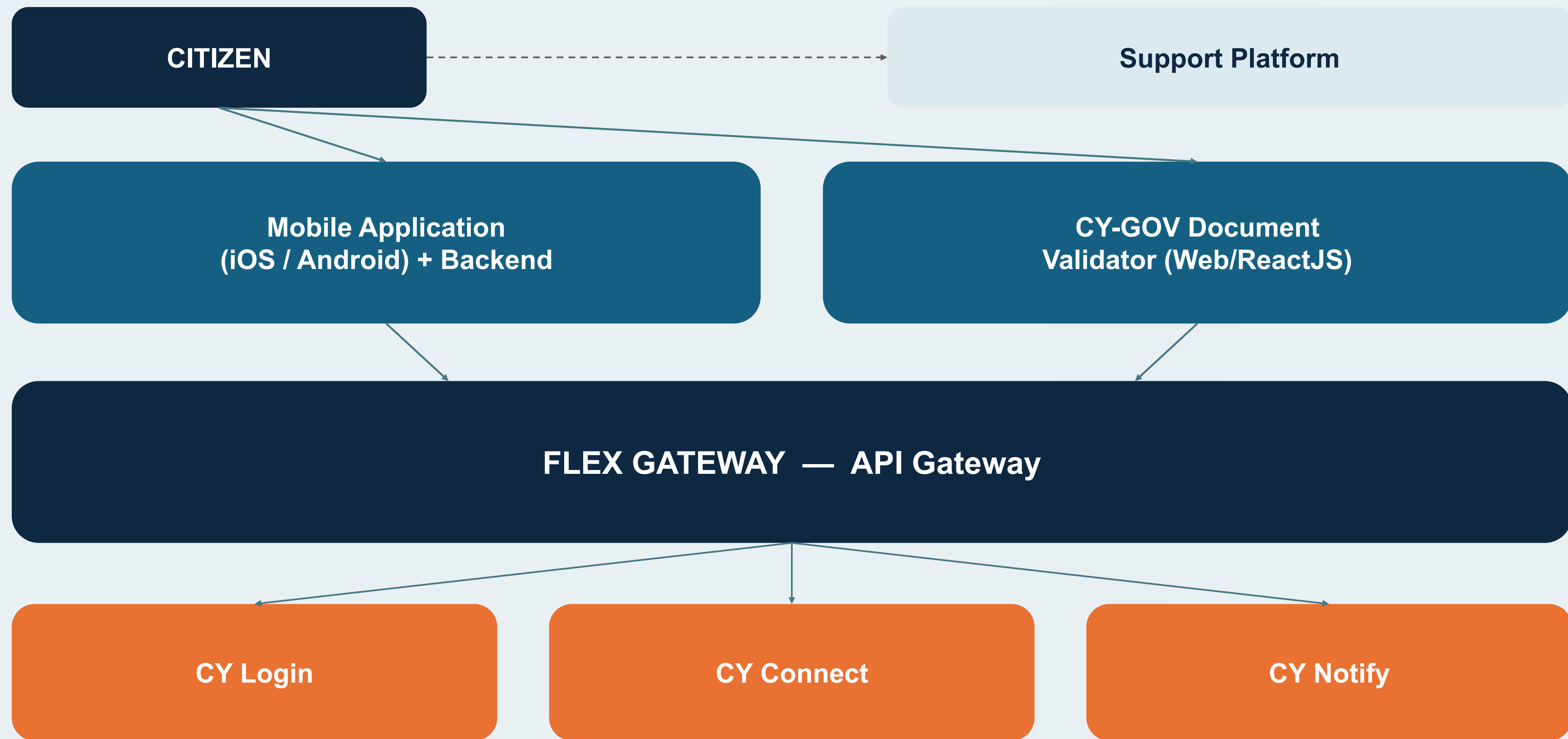
Microservices on Microsoft Azure: cloud-native design with containerized microservices on Azure PaaS services, for high availability, elasticity and cost-effectiveness.



Integration with the gov.cy ecosystem: CY Login (OpenID Connect, citizen authentication), CY Connect (retrieval of data from source database) and CY Notify (SMS OTP / notifications).



“Digital Citizen” Architecture



gov.cy ecosystem · Microservices on Microsoft Azure



Roles and Components involved in the architecture

- **Citizen:** The person who uses the "Digital Citizen" smart mobile application to add and share digital documents.
- **CY-GOV Wallet:** The "Digital Citizen" smart mobile application.
- **Mobile Backend:** The backend of the "Digital Citizen" smart mobile application, which is responsible for sending push notifications during document sharing with the two-factor security mechanism.
- **FLEX Gateway:** The application's custom-developed API Gateway, responsible for processing requests originating from the "Digital Citizen" smart mobile application, validating each request, collecting data from the external systems and services it connects to, sending OTPs for enhanced security, and storing device and document data.
- **CY Login:** Government identification and authentication service (Identity Provider, Identity Management), which uses the OpenIDC standard. Citizens are identified using their CY-Login credentials.
- **CY Connect:** The service that manages requests for retrieving data from the source database for the creation of the digital document, providing an interconnection between the "Digital Citizen" application and Cyprus's civil identity registry and the Department of Road Transport, enabling the retrieval of data from the citizen's physical document. (The interconnection with the Cyprus Sports Organisation's Fan Card registry takes place outside CY-Connect)
- **CY Notify:** The notification service/mechanism to citizens' mobile phones provided by the Cypriot government.
- **Swift Datastore:** Uses the Azure Cache for Redis service to temporarily store the OTPs used when adding digital documents, as well as the pairing codes used when sharing documents. This enables a longer time-period validity of the OTPs.
- **Doc DB:** Uses the Azure Cosmos DB for MongoDB service to store and retrieve data relating to the citizen's device and the digital documents that have been added to the application.
- **CY-GOV Document Validator Page:** A page built with React.JS, used to check the validity of a digital document using the document's QR code or unique 22-digit document code, available only on computers with access to the government network.
- **Support:** The application's support platform, for raising queries to be investigated by the support team.



Mobile Application – Technical Overview



Two native code bases: separate implementations for iOS (Swift) and Android (Kotlin), with full functional parity and a shared release plan.



Secure citizen authentication: sign-in via CY Login (OpenIDC, PKCE) with strong authentication (OTP via SMS/Authenticator) and fast re-login (Quick Login) with biometrics or PIN.



Document issuance & protection: digital documents are delivered from the FLEX Gateway end-to-end encrypted for the citizen and digitally signed, so the app can verify each document is authentic and unaltered before storing it.

1

Sign in with CY Login

OpenIDC (PKCE) + 2FA with OTP via SMS / Authenticator

2

Quick Login

Biometrics or PIN, after the first sign-in

3

Digital Document Creation

OTP via SMS · call to the FLEX Gateway with an Access Token

4

Document Validation

QR Code or Quick Scan · real-time citizen consent

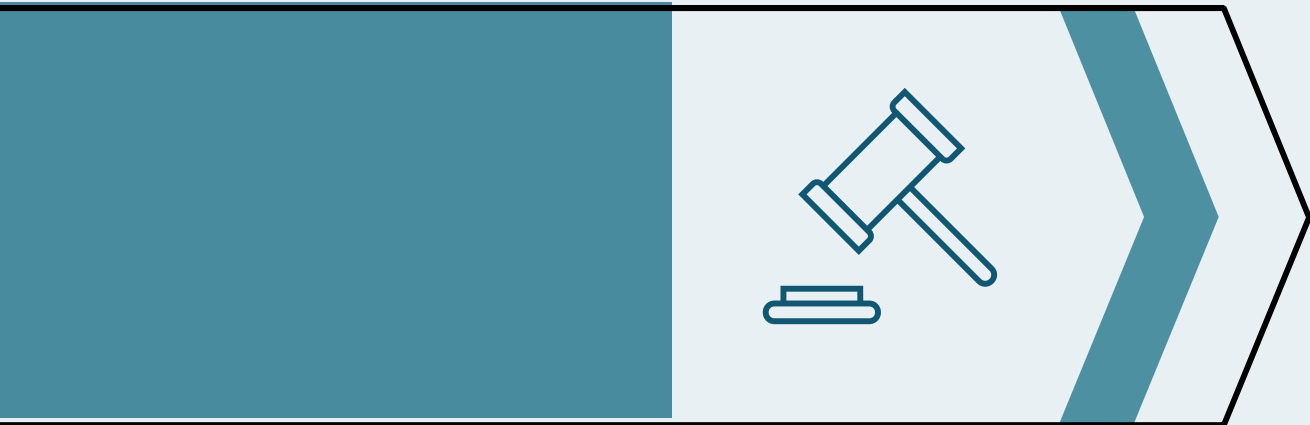




FLEX Gateway – The Application’s API Gateway



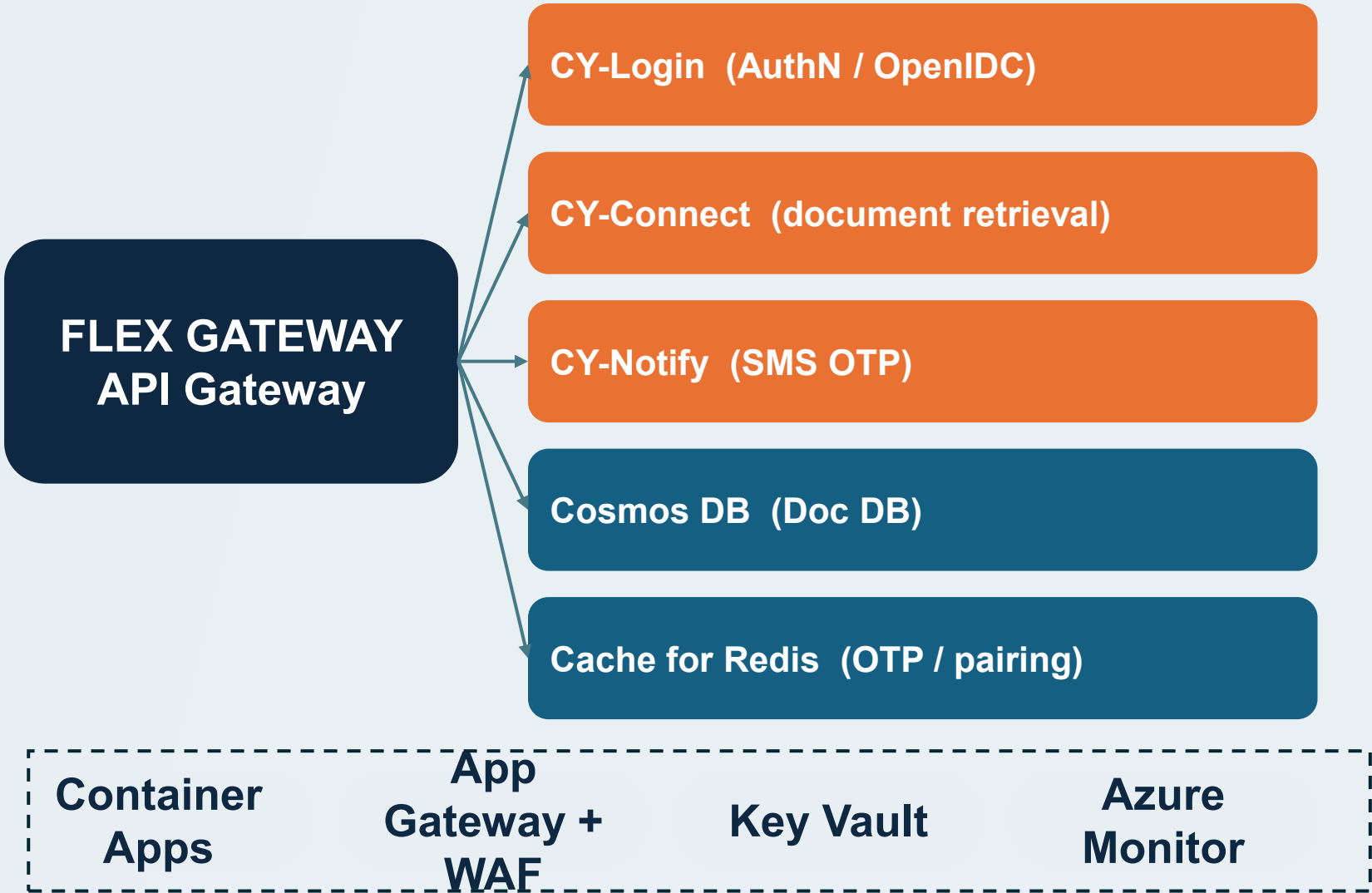
Central request-processing role: validates every request from the mobile application, authorizes via CY Login (OpenIDC), and coordinates the creation, sharing and verification of digital documents.



Cloud-native stack on Azure: Container Apps (running the microservices), Cosmos DB for MongoDB (document/device data), Cache for Redis (OTP & pairing codes), Application Gateway + WAF, Key Vault, Azure DNS, VPN Gateway.



Production monitoring: Azure Monitor (metrics, dashboards, alerts) and Application Insights (response time, exceptions, usage telemetry) for continuous oversight and rapid issue diagnosis, operated by the Contractor.



Citizen Support Platform



digital-citizen.gov.cy/techniki-ypostirixi: links by subject category — Application Operation (and Gov.gr Wallet), ID Card, Driving Licence, Motor Vehicle Roadworthiness Certificate, Fan Card, Minor's ID.



Submitting a new request (ticket): sign in with CY Login at support.digital-citizen.gov.cy → “Submit Request”. Contact details are filled in automatically and the request is routed to the L1 support level via the back office module.



Tracking the response: email with a unique reference number, notification once answered, viewable via “View Responses”. CY Login matters are handled by the DITS team through cyloginsupport@dits.dmrid.gov.cy
Support line 1450 provides L1 support and is handled by DMRID

digital-citizen.gov.cy/techniki-ypostirixi

1

Selecting the request category

Application operation, ID Card, Driving Licence, Roadworthiness Certificate, Fan Card, etc.

2

Sign in with CY Login

At support.digital-citizen.gov.cy — CY Login credentials are required

3

Submitting the Request

Contact details are filled in automatically from the CY Login profile

4

Unique Reference Number

Sent to the citizen by email immediately after submission

5

Routing & Assignment

Automatically to the competent authority and a specialised officer

6

Response Notification

Notification email → “View Responses” in the personal repository



Support Platform — Backoffice



Topics & Entry Channels: tree structure of up to 3 levels (subject areas → topics → sub-topics) with 3 topic types; each topic is configured separately for web submission.



Access Rights & SLA: for each topic, the responsible Departments and response team are defined and provide L2 support. The SLA is set centrally, with the option of exceptions per topic.



Roles & Central User Management: 6 user roles, from Ticket User to Administrator; accounts are created centrally via the admin module, with permissions assigned separately per subsystem.

TCM — TOPIC STRUCTURE



USER ROLES



DASHBOARD & CENTRAL MANAGEMENT

Dashboard
Requests within/outside SLA for the last 7 days · personal assignments (Special Assignment / Work Order)

User Management
Creation, modification, activation/deactivation of accounts

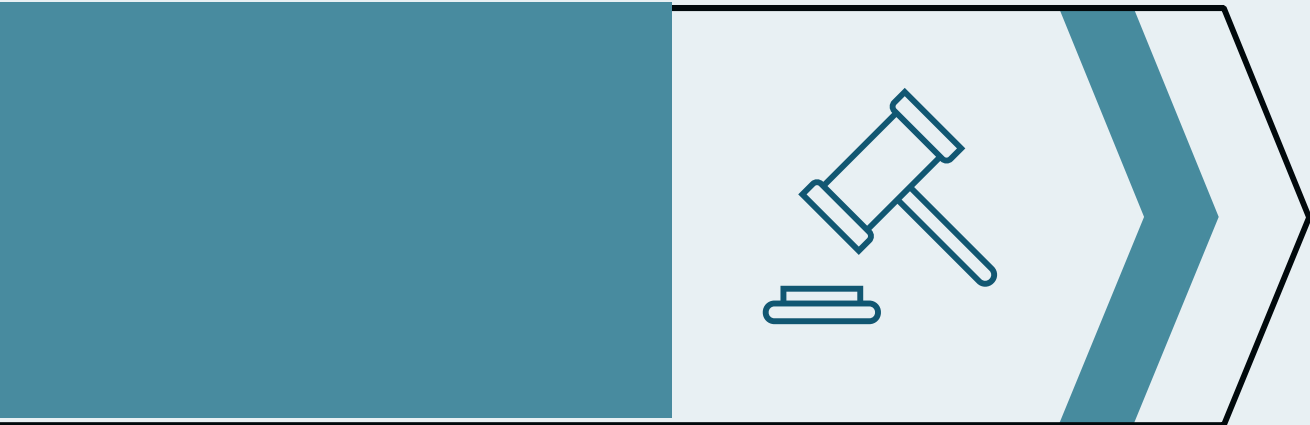
Group Management
Grouping of users with administrators and members per group



Secure Authentication — CY Login Flow



OpenID Connect with PKCE: The application uses the Authorization Code Flow with PKCE to protect the sign-in process.



Strong Authentication (2FA): after the personal CY Login credentials, an OTP is sent via SMS or Authenticator and biometrics, PIN or pattern are requested.



Quick Login: After the initial sign-in, the citizen can access the application using biometrics together with the existing secure session, without repeating the full CY Login process.

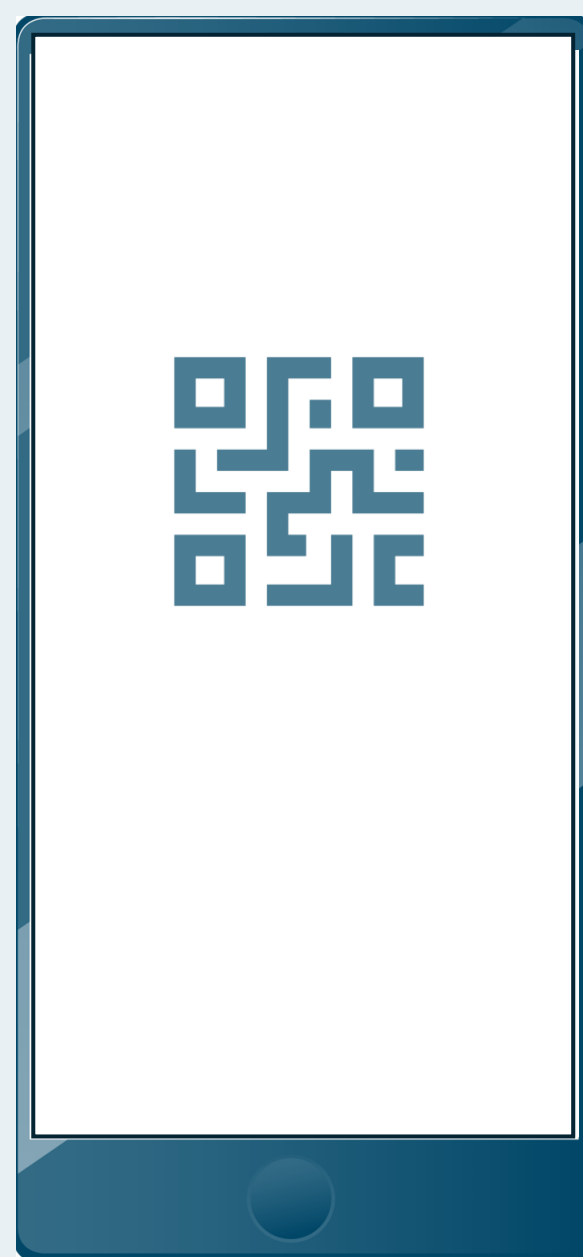
- 1 Sign in with CY Login**
The citizen selects “Sign in with CY Login” on the application’s home screen
- 2 Secure Authorization Request**
The application opens CY Login using OpenID Connect with PKCE
- 3 Entering Credentials**
Citizen enters CY Login credentials and confirms the OTP via SMS or Authenticator
- 4 2FA with OTP**
SMS or Authenticator · identity confirmation with biometrics, PIN or pattern
- 5 Push Token Registration**
The mobile application assigned a push token to receive push notifications
- 6 Subsequent Sign-ins**
Quick Login uses biometrics without repeating the full CY Login flow



Document validation in Digital Citizen

Verification via mobile

Both the Citizen and the Validator use the application to carry out the validation. The Citizen chooses to display the QR code of the document they want to present, and the Validator scans it using the verification function.



2 types of QR Codes

01

QR Code Scan where, as part of the process, the Citizen receives an OTP via push notification, which they must provide to the Validator so that the Validator can gain access to the document's details.

02

Quickscan where, through this function, a single-use QR code is generated with a lifetime of a few minutes. Once scanned by the Validator, access to the document's details is immediate. (used at stadiums, concerts, etc.)



Document Validation — QR Code Scan



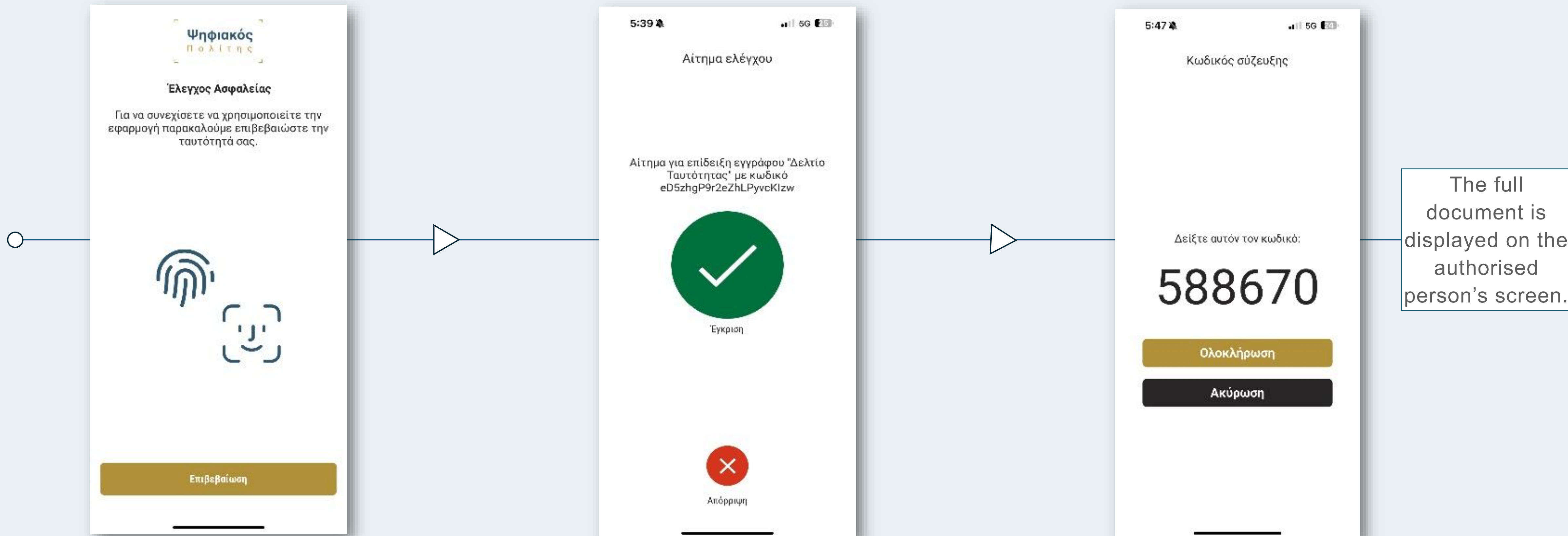
Step 1: The citizen selects the digital document they wish to have verified and presses the “Show QR Code” button.

Step 2: The document’s QR code appears on the citizen’s screen.

Step 3: The authorised person selects the Document Validation function and scans the QR code.



Document Validation — QR Code Scan



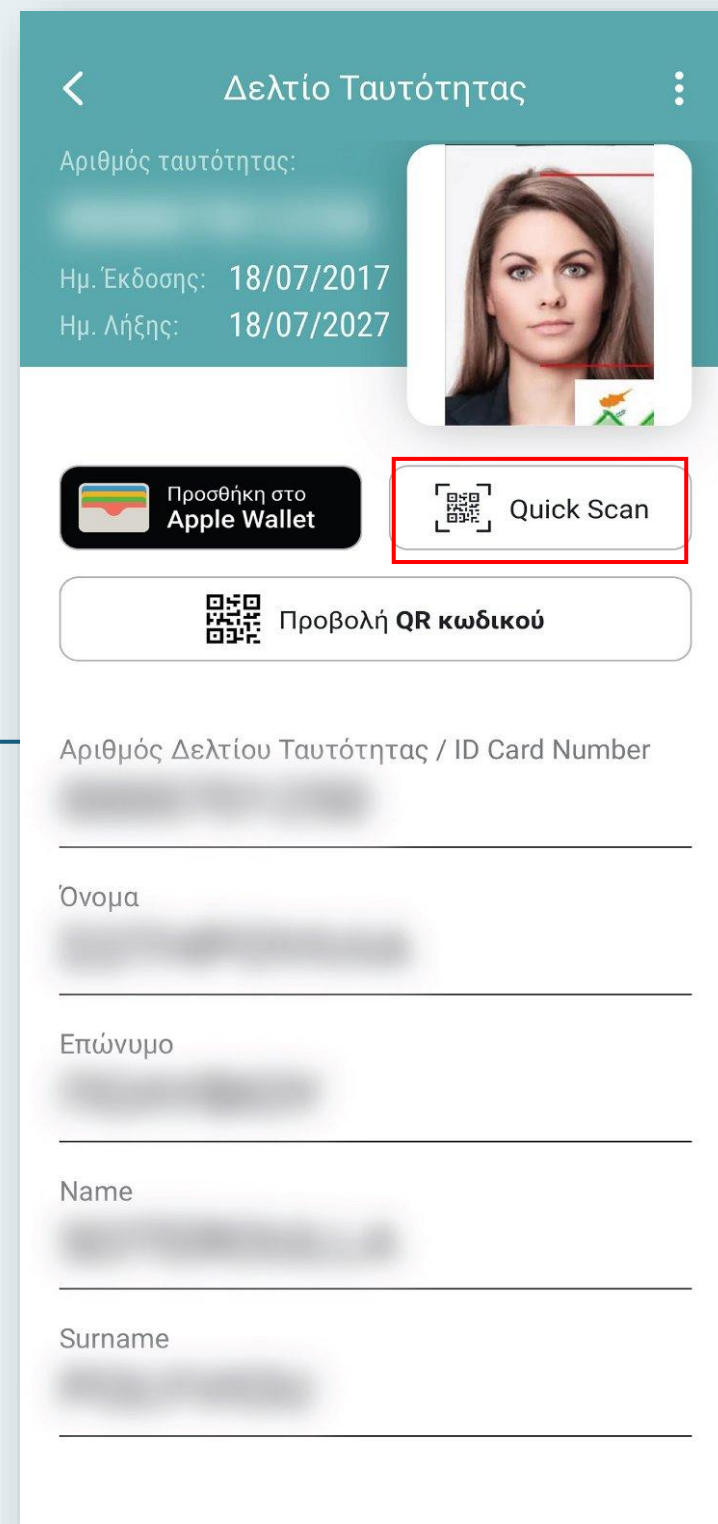
Step 4: The citizen receives the verification request and is asked to confirm their identity using biometrics. They select "Confirm".

Step 5: The citizen's phone then displays the screen below, where they are asked to give their approval for the document verification by tapping the green tick, marked "Approve".

Step 6: A unique code appears on the citizen's screen, which they must show or state to the authorised person as part of the verification process. The citizen selects "Complete".



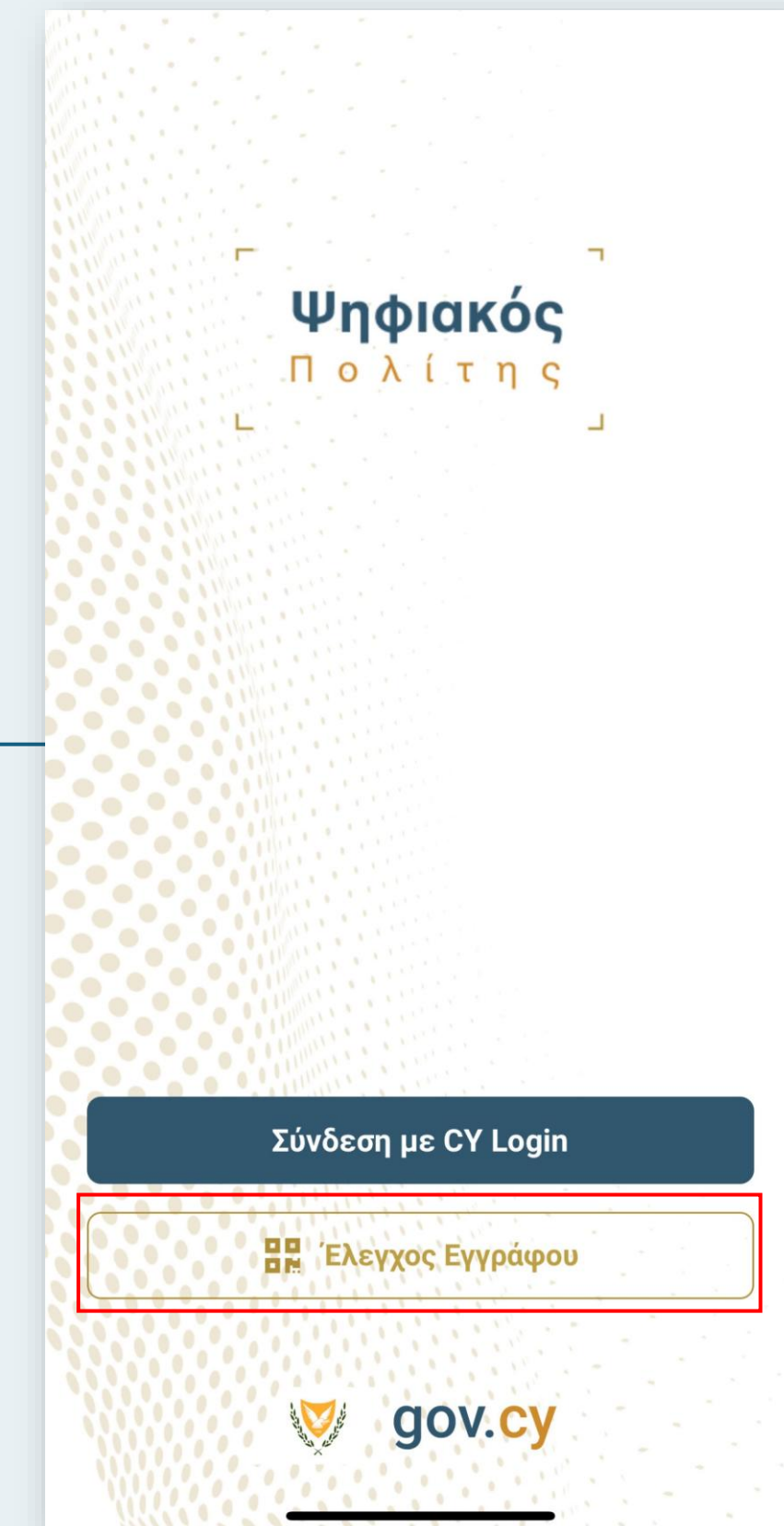
Document Validation — QuickScan



Step 1: The citizen selects the digital document they wish to have verified and selects the “Quick Scan” button.



Step 2: The document's QR code appears on the citizen's screen.

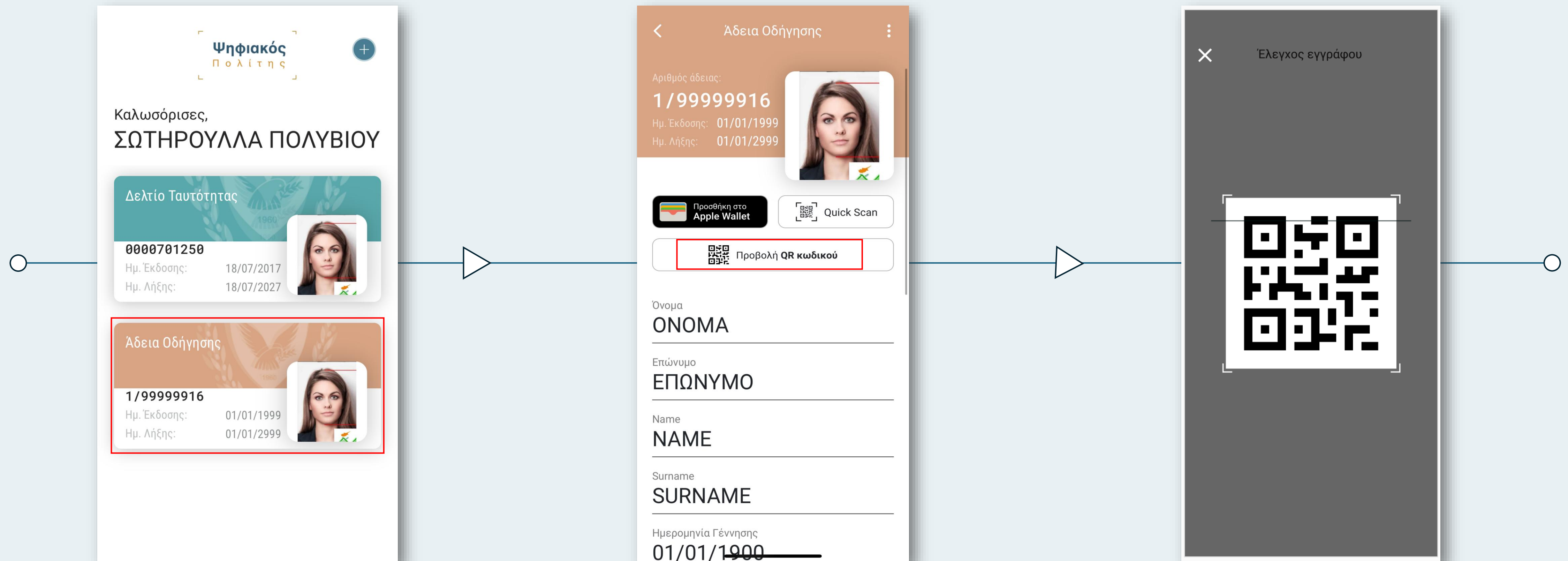


Step 3: The authorised person selects the Document Validation function and scans the QR code.

The full document is displayed on the authorised person's screen.



Document Validation — GOV.CY Website



Step 1: The citizen selects the document to be verified from their digital "wallet" (e.g. Driving Licence).

Step 2: They open the document and select "Show QR Code" to make it available for validation.

Step 3: The device displays the document's QR code full-screen, ready to be scanned by the Validator.



Document Validation — GOV.CY Website

gov.cy Επαλήθευση εγγράφου

< Back

Συμπληρώστε τον κωδικό επαλήθευσης

Κωδικός Επαλήθευσης

Εύρεση

Θα χρειαστείτε μια συσκευή με λειτουργία κάμερας, π.χ. έναν υπολογιστή, ένα κινητό ή ένα tablet.

Σαρώστε QR Code

gov.cy © Republic of Cyprus, 2024

Trash

Step 4: The Validator goes to digital-citizen.gov.cy/validate/ and chooses either to manually enter the unique 22-digit document code or scan the QR code.

gov.cy Επαλήθευση εγγράφου

< Back

Συμπληρώστε τον κωδικό επαλήθευσης

Κωδικός Επαλήθευσης

Εύρεση

Θα χρειαστείτε μια συσκευή με λειτουργία κάμερας, π.χ. έναν υπολογιστή, ένα κινητό ή ένα tablet.

Ακύρωση

Trash

Step 5: The device's camera or a barcode scanner through the input field scans the document's QR code in real time, from within the browser.

gov.cy Επαλήθευση εγγράφου

< Back

Αντίγραφο άδειας οδήγησης

Προβολή

Κωδικός Πράξης Ελέγχου (Digital document unique code) iORly8o1Kp42rk8_ajB8cw

Χρονοσήμανση Πράξης Ελέγχου (Digital document issuance timestamp) 04/11/2024, 09:27:50

Άδεια Οδήγησης

Φωτογραφία άδειας οδήγησης

Κωδικός επαλήθευσης iORly8o1Kp42rk8_ajB8cw

Κατάσταση Το έγγραφο εκδόθηκε

Πρότυπο GOV-DIGITAL-CITIZEN-DRIVING-LICENCE

Ημερομηνία έκδοσης εγγράφου gov.cy 04/11/2024, 11:27:50

Step 6: The application confirms the unique 22-digit document code and displays the document's verified details — status, timestamp and unique verification code.



Document Validation — Security Protocol



Two Roles:
Citizen — verified citizen, holder of the document;
Validator — no sign-in required, can validate anonymously.



Temporary Validation Key: a unique key pair is generated on the Validator’s device solely for that specific validation and is deleted immediately afterwards.



End-to-end Encryption: the document is transferred as a JWE — signed with the FLEX Gateway’s key, encrypted with the Validator’s key; screenshots are not possible.

- QR Scan**
The Validator scans the Citizen’s QR code (“Show QR” or “Quick Scan”)
- Temporary Validation Pair**
Generated on the Validator’s device — unique to this validation
- Consent Request**
To the FLEX Gateway: document id + the Validator’s temporary public key
- Push Notification**
FLEX Gateway → Devices & Notifications → Firebase → Citizen’s device (JWE)
- Consent with Biometrics**
The Citizen approves the request; a pairing code is displayed
- Sharing the Code**
The Citizen verbally shares the pairing code with the Validator
- Document Delivery**
JWE encrypted with the Validator’s key → viewed → key deleted immediately



FLEX Gateway — Structure, Data Model & Infrastructure



Backend Services (Microservices): Containerised backend services support API request processing, document lifecycle operations, user and device registration, one-time-code processing, and notifications



Data Storage: Azure Cosmos DB for MongoDB stores application data related to registered devices, digital-document lifecycle, operational references and security-related records. Azure Cache for Redis supports temporary data, including one-time codes and pairing information



Environments: separate cloud environments (PROD, UAT) with scalable capacity — safe testing before every change to production.

FLEX GATEWAY INTERNAL SERVICES

OpenAPI Gateway	Flex-GW Resource Server
CY-Document Service	OTP Service
Registration Service	Notification Service

DATA MODEL — CORE COLLECTIONS (Cosmos DB / MongoDB)

Device Registration Data Status & details of citizens' registered devices
Document Lifecycle Data Metadata of digital documents
Operational Reference Data Document numbering counters/sequences
Security & Trust Data Document-signing certificates





Thank you



DEPUTY MINISTRY OF RESEARCH, INNOVATION AND DIGITAL POLICY



DEPUTY MINISTRY OF RESEARCH, INNOVATION AND DIGITAL POLICY