1 IDEMIA Mobile ID Solution

1.1 Digital Solution Overview

IDEMIA's multi-tenet **Mobile ID Solution** is modular, scalable, and optimized for regulated applications. The solution focuses on enhancing personal privacy while simultaneously automating key individual functions. This solution ensures security at every step with an extensive, multi-layered security design.

The IDEMIA **Mobile ID Solution** conforms to industry, national, and international standards bodies, and it accommodates regional or local variations with services co-located or spread across multiple cloud instances or data centers, as needed.

The IDEMIA **Mobile ID Solution** consists of various modules and key functions as shown in Figure 1.

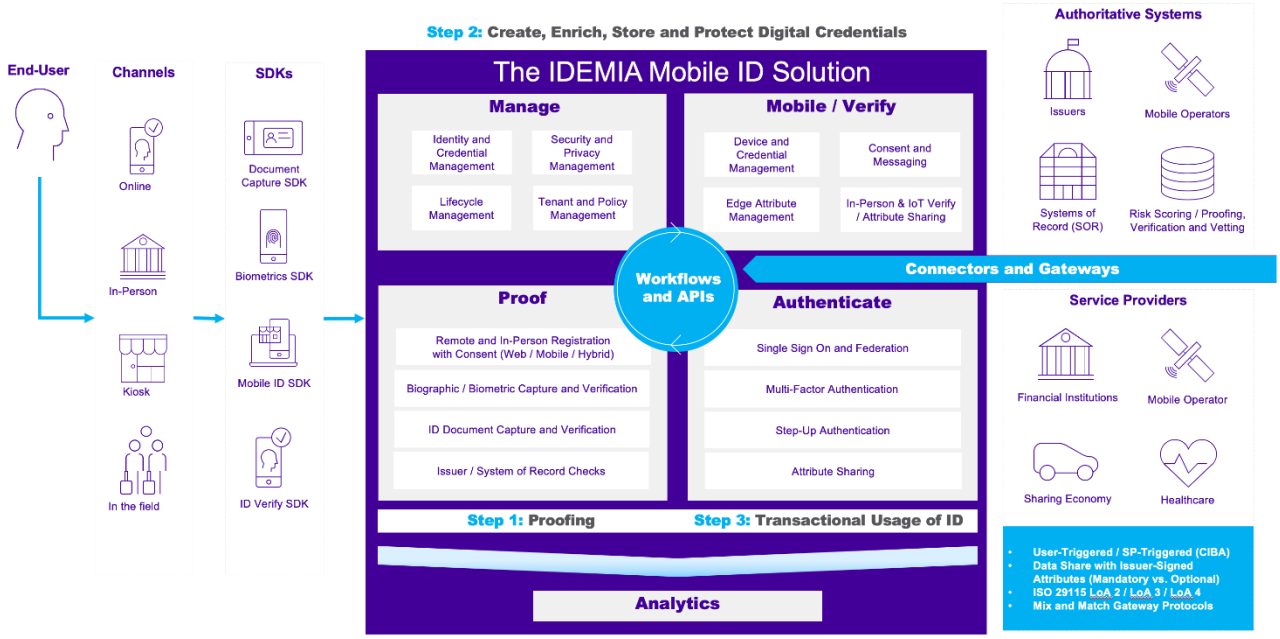

Figure 1. You can install the microservices-based Mobile ID Solution in IDEMIA's secure cloud, a private cloud, or on-premises.

This product guide focuses on the **Mobile** and **Verify** modules and the four primary components making up the **Mobile ID Solution**:

- IDEMIA **Mobile ID App**
- IDEMIA **Mobile ID Verify App**
- IDEMIA **idFabric™**
- IDEMIA **Identity Server**

This document describes key information regarding how the **Mobile** and **Verify** modules support and interact with the remaining modules.

Note: *Supplemental product guides cover the Mobile ID Verify App, idFabric™ and Identity Server modules in more exhaustive detail.*

1.2 IDEMIA Mobile ID App

The **Mobile ID App** hosts a secure, authenticated, fully functional digital credential supported in both Android and iOS smartphones. The user can apply or register to receive their digital credential remotely or in-person.

1.2.1 Mobile ID App

The **Mobile ID App** is available to all users for public download in the *Apple App Store* and *Google Play Store*. Each Issuing Authority can publish a white-labeled version of the application of the standard IDEMIA **Mobile ID App** with custom branding for the icon and splash screens.

The **Mobile ID App** leverages native *iOS* and *Android* capabilities to achieve a higher level of security and the best user experience for both online and offline access. It also leverages operating system libraries and/or frameworks, as well as **IDEMIA** and third-party SDKs.

1.2.2 Registration

The user can apply or register to receive their digital credential remotely or in-person.

1.2.2.1 Remote registration

When a user registers remotely, the **Mobile ID App** captures the following set of information from the registrant using configurable workflows:

- Phone number with SMS verification
- Biographic and biometric attributes
- Images and metadata
- Government and other identity documents (ID)
- Large format documents (e.g., utility bills or birth certificates)
- Questionnaire and survey selections (e.g., yes/no toggles and picklists)

- Affidavits that have signatures signed on the smartphone screen
- In-app payment (e.g., renewal fees, in-app subscription fees, or premium add-ons)

1.2.2.2 In-person registration

The **Proofing** services allow attribute and ID authentication by performing optional matching against the presented IDs and/or System(s) of Record (SoR). The user must follow the steps below to complete in-person registration:

1. Download the **Mobile ID App**.
2. Scan a dynamic QR code on the verifier's screen or a printed QR code.
3. Complete a selfie match.
4. Select a PIN.

1.2.2.3 Identity verification

PKI technology allows the signing of all user credentials with their bundled attributes. The Issuing Authority's root key creates a digital certificate, and it stores these attributes in one of the following ways:

- User's smartphone only: *Identity-on-the-Edge*
- SoR
- Using a hybrid approach: *Identity-on-the-Edge* and SoR

The public certificate is available to Relying Parties for validating the integrity of the attributes shared by the user during the transaction.

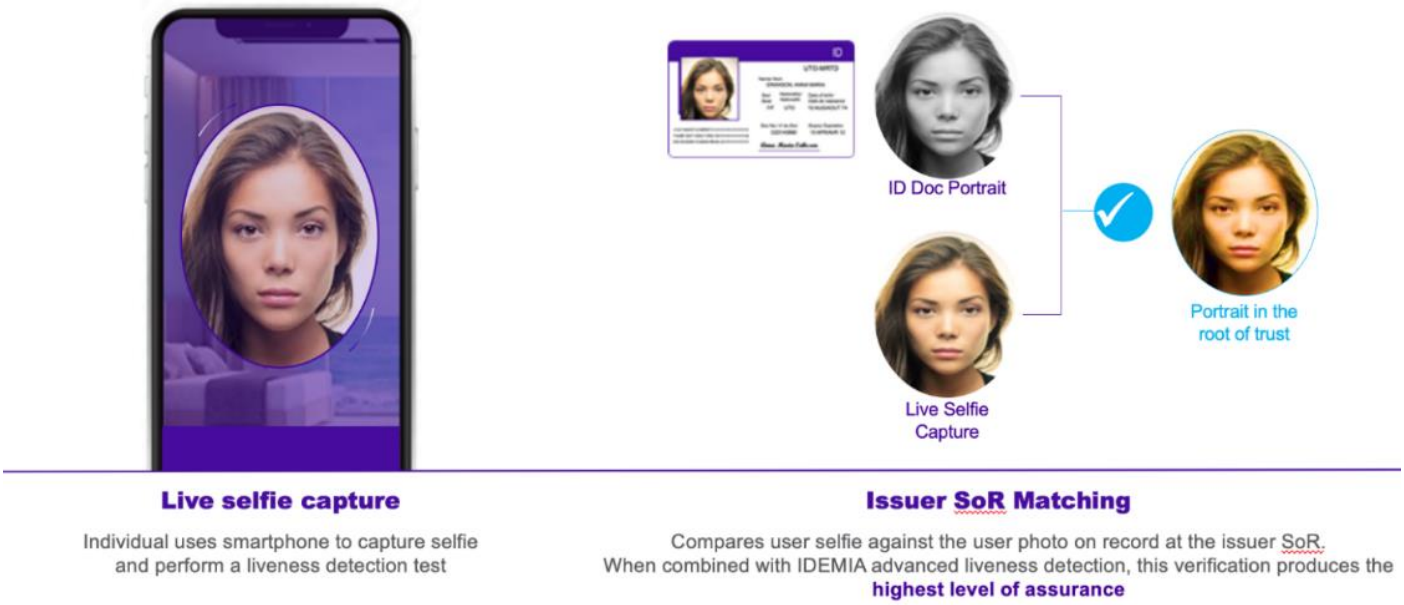

Figure 2. The Mobile ID proofing services use advanced methods to authenticate a government ID that belongs to the person presenting it.

1.2.2.4 Credentials

The **Mobile ID** credentials includes a close-color replica of the front and back of the ID, the orientation (horizontal or vertical), and the user's profile with all the information displayed on the physical ID.

A banner at the bottom of the screen provides shared information about the user's **Mobile ID** credential obtained from the corresponding PKI public certificates.

1.2.3 App navigation and user experience

The **Mobile ID** credential includes a close color replica of the front and back of the ID as shown in Figure 3. It includes the orientation (horizontal or vertical) and the user's profile with all the information on the physical ID.

A banner at the bottom of the screen provides the following tabs:

- **Me**: This tab displays the attributes that make up the digital credential (linked privileges, statuses, endorsements, or restrictions for quick reference), and allows the user to launch in-person identity verification and data sharing functions.
- **IDs**: This tab displays the front and back rendering or badge of a corresponding physical ID card for branding or visual inspection purposes.

- **Scan**: The QR code scanner function enables the user to perform various tasks, including in-person registration, registration trigger, and logical access functions (online websites and web applications running on a second device). It supports mobile applications and web applications running on the same smartphone, and the user can tap on a soft button to switch apps from mobile to web.
- **Requests**: This tab provides the inbox for active transaction requests, and it stores the history of any personal information and attributes shared as a part of the transaction.
- **More**: Users can use this tab to access various settings, configurations, documentation, FAQs, privacy policy, terms of use, feedback, and support.

Figure 3. Mobile ID App modern user experience and design