IDEMIA

Global Digital Platforms

IDEMIA Verify Product Suite

Product Guide - Version 2020.4

This document is optimized as an internal document. Contact your business unit or marketing team for an enhanced customer-facing version.

Documentation | Digital Identity

June 2020

This document describes the functions of the IDEMIA Verify Product Suite available as of the product/platform release number indicated in the document version number. IDEMIA Digital Identity products and components leveraged by the IDEMIA Verify Product Suite have additional functions and capability not included in this Product Guide. This document does not describe the functionality deployed by or exposed by any one IDEMIA business unit for any particular operational IDEMIA Verify Product Suite implementation for a given region or market segment, nor does it describe the functionality deployed for or exposed by any one end-customer. Please check with your IDEMIA business unit to determine what is available in your region or market segment.

Table of Contents

1 Overview of IDEMA Verify Product Suite

1.1 Introduction

The **IDEMIA Verify Product Suite** is a modular, scalable, and optimized suite of products that allows a person, business, agency, or other organization, to verify another individual's identity credential(s) in a cryptographically secure and trustworthy manner within seconds. It conforms to many industry, national, and international standards bodies.

1.1.1 Components

The **IDEMIA Verify Product Suite** products interact with the rest of IDEMIA's overall Digital ID Solution. This suite accommodates regional and local variations and is comprised of:

- IDEMIA Mobile ID Verify App – Android
- IDEMIA Mobile ID Verify App - iOS
- IDEMIA Verify SDK – Android
- IDEMIA Verify SDK – iOS
- IDEMIA Verify SDK – Windows
- IDEMIA Verify SDK – Linux

Some of the key functionalities of the **IDEMIA Verify Product Suite** are:

- in-person verification capabilities
- agnostic credential method detection
- custom attribute request templates
- dynamic display of credential holder's attributes
- dedicated help resources
- forced app upgrade, etc.

Note: The engagement between the IDEMIA Mobile ID Verify App and the IDEMIA Mobile ID App is conducted purely device-to-device. Neither the device running the IDEMIA Mobile ID Verify App nor the device housing the Mobile ID credential requires connection to the internet at the time of verification.

1.1.2 Verification

The **IDEMIA Mobile ID Verify App** is the front-facing part of the **IDEMIA Verify Product Suite**. The IDEMIA branded app can be obtained from your Sales Manager.

1.1.2.1 Relying Party

IDEMIA **Verify** is one of the components of the Digital Identity Solution that allows a Relying Party to verify an end-user's identity credential.

The **IDEMIA Mobile ID Verify Apps** for Android and iOS are built on their respective mobile SDKs. The apps feature a simple, easy-to-use interface that allows Relying Parties to perform verification of identity-based credentials quickly.

Note: An in-person verification is performed by an individual who serves as a verifier in person when the end-user submits their ID.

1.1.2.2 Credential holder

The credential holder is the individual who carries the identity document(s) (ID). The **IDEMIA Verify Product Suite** is designed to operate with a focus on verifying identity-based credentials while preserving personal privacy. Security is built-in at every step with an extensive multi-layer security design. Identity attributes are encrypted securely in the individual's smartphone and stored only at the authoritative System of Record (SoR).

The method for verifying an end-user's physical ID or **Mobile ID** credential in the **IDEMIA Mobile ID App** is quick, secure, and completely touchless. Credential holders will maintain possession of their smartphones or physical IDs throughout the verification process.

1.1.3 Supported platforms and devices

Only smartphones are currently approved and supported for use on the **IDEMIA Mobile ID Verify App** even though it may function properly on some tablet computers.

1.1.3.1 Android

Support is included for most Android smartphones (Android 7.x or newer) except the discontinued Samsung Galaxy S5.

1.1.3.2 iOS

Support is included for most Apple smartphones (iOS 11.x or newer) except the discontinued Apple iPhone 5S.

1.1.4 International standards

The **IDEMIA Mobile ID Verify App** provides in-person identity verification based on the following international standards:

- PDF417 barcode scanning capability meeting US AAMVA specifications
- QR code generation meeting ISO 18013-5 specifications
- transaction-driven data sharing and Issuing Authority attribute integrity
- signature check using cryptographic certificates (ISO 18013-5/BLE Bluetooth)
- original Issuing Authority color photo display with high resolution
- latest date when the attributes, status, and photo data were last updated
- custom attribute request templates for the Relying Party
- dynamic data display that renders results in a clear and concise manner

1.1.5 User experience

The **IDEMIA Mobile ID Verify App** user experience provides the following functionalities:

- modern end-user interface with friendly instructional screens throughout
- minimalistic attribute field names to emphasize the attribute values.
- at-a-glance age, trust level, and status icons (e.g., credential authentication results and age verification) with configurable thresholds.
- In-app end-user guides for quick at-a-glance support

Figure 1. IDEMIA Mobile ID Verify App with configurable age verification example.

IDEMIA Verify SDK Package

1.2 Introduction

Foundationally, the **IDEMIA Verify Product Suite** consists of a back-end set of SDKs, their related APIs, and documentation that can be implemented within an existing application on mobile and desktop platforms.

The **IDEMIA Verify SDK**s are available for integration on the following platforms:

- Android
- iOS
- Windows
- Linux

Note: More detailed information about the IDEMIA Verify SDKs can found in the respective SDK guides for each platform. The IDEMIA Verify SDK Guides are located on the IDEMIA digital portal at:

https://developer.idemia.com/

1.3 SDK Package items

The **IDEMIA Verify** SDK package contains the following items:

- Verify SDK library
- Verify SDK header files
- Verify SDK library dependencies
- Qt 5.14.0 libraries used in the SDK
- Other dependent libraries

1.3.1 Expose APIs

The **IDEMIA Verify** SDK has exposed APIs, which are described in more detail in the related SDK documentation for the **IDEMIA Mobile ID Verify Apps**. These APIs are for devices that fit the following requirements:

- Android device that runs Android version 5 or later
- iOS device that runs iOS version 10 or later
- must have a working camera
- must support BLE (Bluetooth Low Energy)

1.3.2 SDK Install Package

The **IDEMIA Verify SDK** package is a Debian package: **Verify1.2.0.deb**.

1.3.2.1 Installation Command

Run the following command to install the **Verify1.2.0.deb** package on your terminal:

```
sudo dpkg -i Verify1.2.0.deb
```

1.4 SDK supported platforms and devices

The **IDEMIA Verify SDKs** can be used to build custom applications or integrate into existing applications for the operating systems below and their corresponding devices.

1.4.1 Android SDKs

1.4.1.1 Supported devices

Support is included for most Android smartphones (Android 7.x or newer), except the discontinued Samsung Galaxy S5.

1.4.1.2 Skills required

The developers must have knowledge of the Android operating system.

1.4.1.3 Resources required

Integrations are supported for PC Windows, Linux, or Macintosh.

1.4.1.4 Tools required

The tools required are:

- Android Studio 3 or above
- Android SDK tools: preferred latest version (release 24 or above)
- JDK: preferred latest version (7 or above)
- Android device (emulator is not supported)
- Minimum SDK version is 21 (Android 5.0)

1.4.2 iOS SDKs

1.4.2.1 Supported devices

Support is included for most Apple smartphones (iOS 11.x or newer), except the discontinued Apple iPhone 5S.

1.4.2.2 Skills required

The developers need knowledge of:

- iOS frameworks built in Xcode 11.0 or higher
- Swift 5.0 or higher
- Mac OS 10.14 or higher

1.4.2.3 Resources required

The tools required for integration on a Macintosh are:

- Xcode 11.0 or above
- iOS SDK tools: release 11 or above (preferably latest version)
- Physical iOS device (simulator is not supported)

1.4.2.4 Permissions required

The required permissions in the app `info.plist` file are:

- Privacy - Bluetooth Always Usage Description
- Privacy - Bluetooth Peripheral Usage Description
- Privacy - Camera Usage Description

1.4.3 Windows SDKs

1.4.3.1 Supported devices

Support is included for Windows smartphones (10.x or better).

1.4.3.2 Skills required

The developers need knowledge of:

- C#
- UWP framework ver#16299 and above in Visual Studio 2017 and above

1.4.3.3 Resources required

The tools required are:

- Windows 10 v1703 or higher
- Visual Studio 2017
- Webcam on PC
- Bluetooth on PC

For testing the SDK, a smartphone (iOS/Android) with the `OkMobileId` application.

1.4.4 Linux SDKs

1.4.4.1 Supported devices

Support is included for RedHat Enterprise Linux versions 6, 7, 8, and Raspbian running on the latest Raspberry Pi 4 module.

1.4.4.2 Skills required

The developers need knowledge of:

- C++
- Framework: Qt for App (Optional)
- Operating System: Ubuntu 18.04 (Linux)

1.4.4.3 Packages required

Integrations happen on a Linux machine. The packages required are:

- **2D barcode encoder/decoder**: QZxing or any related library
- **Bluetooth Bluez**: Bluetooth stack for Linux family kernel-based. The tested version for bluez is 5.48. Use the following command for installing the bluez:

```
sudo apt-get install bluetooth bluez
```

- IDEMIA Verify SDK **package**

1.5 Setup IDEMA Mobile ID Verify App

This section provides instructions for setting up the **IDEMIA Mobile ID Verify App** on the mobile device. To setup the app on an Android or iOS device:

1. Download and install the **IDEMIA Mobile ID Verify App** for your Android or iOS device. You can get the app from your Sales Manager.
2. Launch the app by tapping the icon shown below:

3. Tap **I agree to the above** to accept the Terms of use and Privacy statement

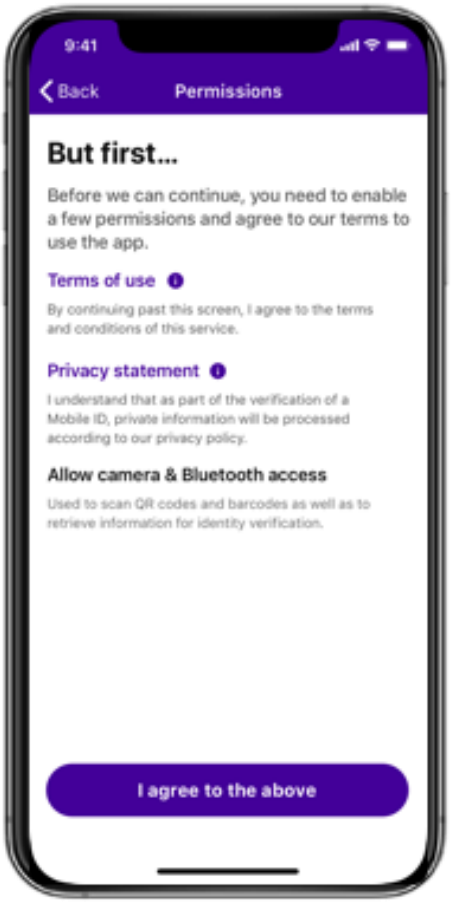

Figure 2. Permissions screen example.

4. Tap **Allow camera & Bluetooth access** so the app can access device features needed to perform verification operations.

Note: This app uses the device's camera to scan barcodes, and Bluetooth Low Energy (BLE) to communicate with and transfer data from devices with the IDEMIA Mobile ID App.

1.6 Verify credential holder's identity

The **IDEMIA Mobile ID Verify App** can verify a credential holder's identity by either reading a QR code or scanning a barcode.

1.6.1 Generate QR code

The **IDEMIA Mobile ID App** generates an ISO 18013-compliant QR code that allows engagement with the **Mobile ID** credential holder's device. The **IDEMIA Mobile ID Verify App** reads the QR code and triggers a data transfer using *Bluetooth Low Energy* (BLE).

The results of the **Mobile ID** credential holder's identity credential information display in the **IDEMIA Mobile ID Verify App** on the Relying Party's device (i.e., only when the credential holder approves the request).

To generate the QR code:

1. The Relying Party opens the **IDEMIA Mobile ID Verify App** and the home screen displays a button with **I'm ready to scan**

Figure 3. Opening the IDEMIA Mobile ID Verify App.

2. The end-user whose **Mobile ID** credential needs verification opens their **IDEMIA Mobile ID App** on their smartphone, and it displays a Quick Response (QR) code for the Relying Party to scan.

Note: This QR code is generated in the Mobile ID App and is compliant with the international standard for mobile IDs, ISO 18013.

Figure 4. End-user shares QR code.

3. The Relying Party taps **I'm Ready to Scan**
4. The Relying Party aims their rear-facing camera at the QR code on the **Mobile ID** credential holder's device, aligning the code so it is centered in the on-screen frame.
5. When the QR code properly aligns within the frame, the **IDEMIA Mobile ID Verify App** automatically captures the image of the QR code. This triggers the BLE engagement with the **Mobile ID** credential holder's device.

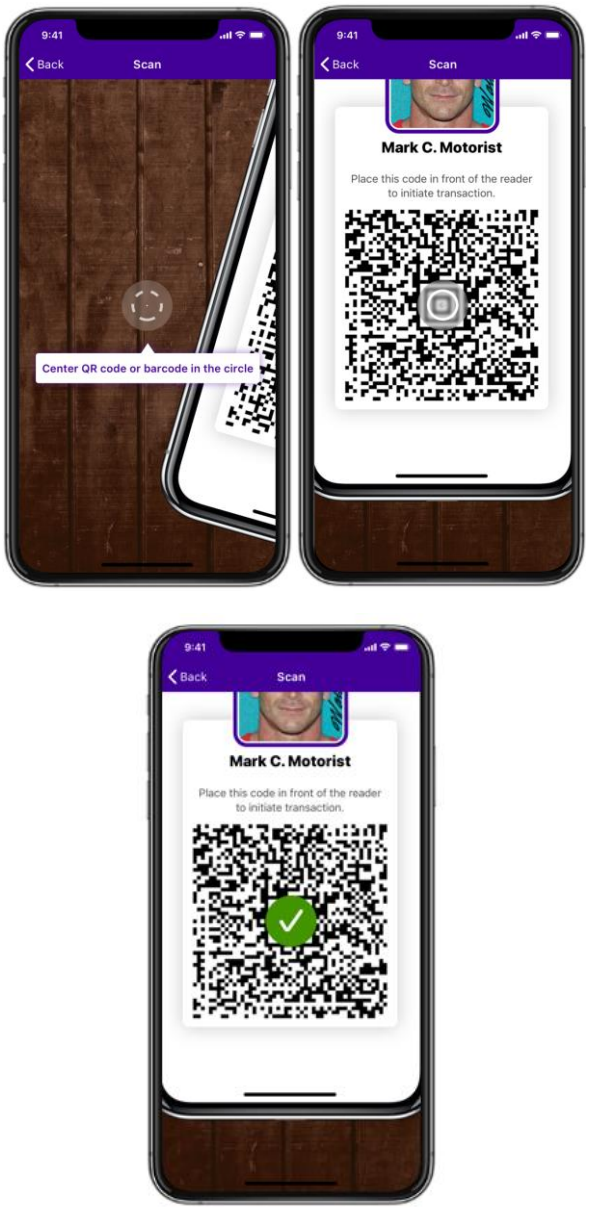

Figure 5. Scanning the QR code example.

7. As soon as the scan is successful, the **IDEMIA Mobile ID Verify App** automatically communicates with the **Mobile ID App** over Bluetooth Low Energy (BLE) without requiring a pairing process.

Figure 6. Device engagement example.

6. The verifying device sends a request for attributes to the **Mobile ID** credential holder's device. The **Mobile ID** credential holder will see a message:

7. The request will list the specific attributes that are being requested, and the **Mobile ID** credential holder will be prompted to **Accept** sharing or **Decline** the transaction.

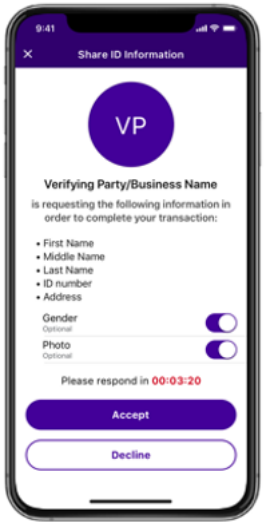

***Figure 7**. Attribute request example that a Mobile ID credential holder sees.*

8. Once the **Mobile ID** credential holder accepts the request for their attributes, the attributes transfer via Bluetooth (BLE) to the Relying Party's device:
    a) If the data is successfully received, the information from the identity credential housed in the **Mobile ID App** displays on the Relying Party's device.

Figure 8. Receiving data example.

    b) If the **Mobile ID** credential was determined to be authentic, a banner displays at the top of the screen with a checkmark and **MOBILE ID AUTHENTICATED**

c) The screen also displays a circle indicating that the **Mobile ID** credential holder is above or below a certain age threshold. This eliminates the need for the Relying Party to manually search for the end-user's date of birth.

©

Figure 9. Results screen example.

d) If the **Mobile ID** credential is not verified, the screen displays a banner with the message **MOBILE ID NOT AUTHENTICATED**.

Figure 10. Mobile ID credential not authenticated example.

e) The Relying Party can clear the results from the screen by tapping **DONE** to delete all data and prepare the verifying device to perform the next verification.

Note: No personally identifiable information (PII) is ever stored on the Relying Party's device or in the cloud.

1.6.2 Scan PDF417 barcode

The **IDEMIA Mobile Verify App** can scan the PDF417 barcode of a physical ID or a digital ID that is rendered in the **IDEMIA Mobile ID App**. Scanning the barcode allows the end-user's identity attributes to be seen on the Relying Party's device.

To use the app to scan barcode:

1. The Relying Party opens the **IDEMIA Mobile ID Verify App** and the home screen displays a button with **I'm ready to scan**. The Relying Party waits until the Mobile ID credential holder is ready to share their PDF417 barcode before tapping the button.

Figure 11. Opening the app example.

9. The end-user whose identity-based credential needs to be verified either opens their **IDEMIA Mobile ID App** on their smartphone and displays the PDF417 barcode or holds out their physical ID with the PDF417 barcode for the Relying Party to scan.

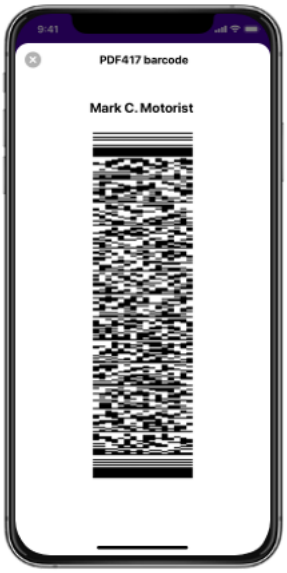

Figure 12. PDF417 presentation example.

10. The Relying Party, taps **I'm ready to scan**. The Relying Party then aims their rear-facing camera at the PDF417 barcode and aligns it so that it's centered within the on-screen frame. When the PDF417 barcode properly aligns within the frame, the **IDEMIA Mobile ID Verify App** automatically captures the image of the PDF417 barcode.

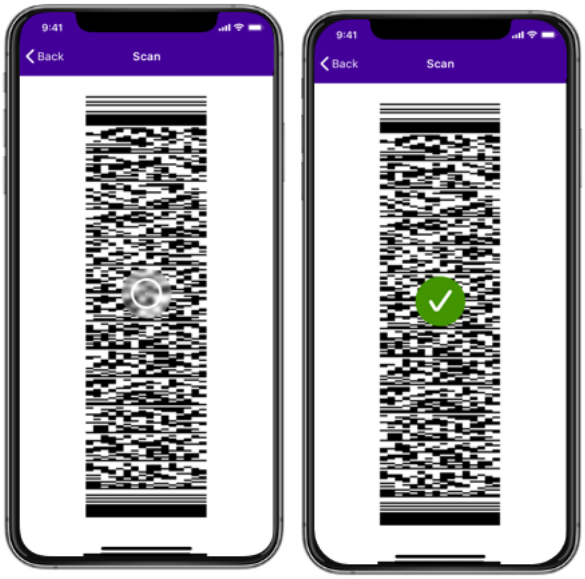

Figure 13. PDF417 scanning example.

11. The Relying Party can view the **Mobile ID** credential holder's results on their device.
12. The Relying Party can clear the results from the screen by tapping **DONE.** This action completely deletes the data. No *personally identifiable information* (PII) is ever stored on the Relying Party's device or in the cloud. The verifying device is ready to perform the next verification.

Figure 14. PDF417 results example.

2 Technical Features

2.1 Introduction

These are some of the distinguishing features of the **IDEMIA Mobile Verify ID App**.

- Completely touchless machine-to-machine (M2M) design
- No internet connection needed
- Adherence to IS0 18013 guidelines
- Personally identifiable information (PII) is protected at all times, never being stored on the verifying device or in the cloud
- QR Code & BLE capability
- PDF417 barcode scanning and rendering
- Auto-detection of credential authentication method
- Pre-set age verification settings for common age verification scenarios

2.2 Table of features

The table below describes the available features.

Feature/Function	Credential	Platform
QR Code + BLE transfer	Mobile ID	Android, iOS (SDKs & apps) Linux, Windows (SDKs)
PDF417 Scanning	Physical ID Mobile ID	Android, iOS (SDKs & apps) Linux, Windows (SDKs)
Optical Inspection	Mobile ID	Android, iOS (SDKs & apps)
Custom Templates	Mobile ID	Android, iOS (SDKs & apps)
Credential Auto-Detection	Physical ID Mobile ID	Android, iOS (apps)
Dynamic Display	Mobile ID	Android, iOS (apps)
Not for Official Use Indicator	Mobile ID	Android, iOS (apps)
Decline Notification	Mobile ID	Android, iOS (apps)

Feature/Function	Credential	Platform
Age Verification	Physical ID and Mobile ID PDF417 (18-25); Mobile ID QR code + BLE transfer (21+)	Android, iOS (SDKs & apps) Linux, Windows (SDKs)

2.2.1 ID verification methods

The **IDEMIA Mobile ID Verify App** can verify a physical ID or a **Mobile ID** credential in a variety of ways. Some methods only support verifying the physical ID while other methods only support verifying the **Mobile ID** credential. Some do both:

Methods	Physical ID	Mobile ID Credential
QR Code for device engagement and *Bluetooth Low Energy* (BLE) for data transfer	No	Yes
PDF417 Barcode Scanning	Yes	Yes
Optical Inspection	No	Yes
LineCode Verification	Yes	No

2.2.2 QR Code and BLE

A Relying Party can use this method of verification to authenticate a **Mobile ID** credential device-to-device with the security methods as outlined in ISO ISO-18013. This method uses modern security certificates.

2.2.2.1 QR code – device engagement

Currently, this method does not verify physical IDs. The process is described below:

1. An end-user elects to share their **Mobile ID** credential through the **IDEMIA Mobile ID App**.
2. The **IDEMIA Mobile ID App** creates a QR code, which allows the end-user's device to engage directly with the Relying Party's device that contains the **IDEMIA Mobile ID Verify App**.
3. The **IDEMIA Mobile ID Verify App** requests attributes from the **Mobile ID** credential holder.
4. The **Mobile ID** credential holder consents to the request.
5. Data then transfers from the end-user's smartphone to the Relying Party's device using BLE.
6. The Relying Party can view the results on their device.

Figure 15. *Request notification example that a* ***Mobile ID*** *credential holder would see.*

This transaction works with iOS, Android, and Linux SDKs to an iOS-based the **IDEMIA Mobile ID App** QR code and BLE transfer.

2.2.3 Scan and render barcodes

The **IDEMIA Mobile ID Verify App** scans PDF417 barcodes on a physical ID or **Mobile ID** credential to:

- consume the PDF417 barcode
- display the attributes for verification, including a quick age indicator
- provide a button to re-render the PDF417 barcode in case a secondary scan is required

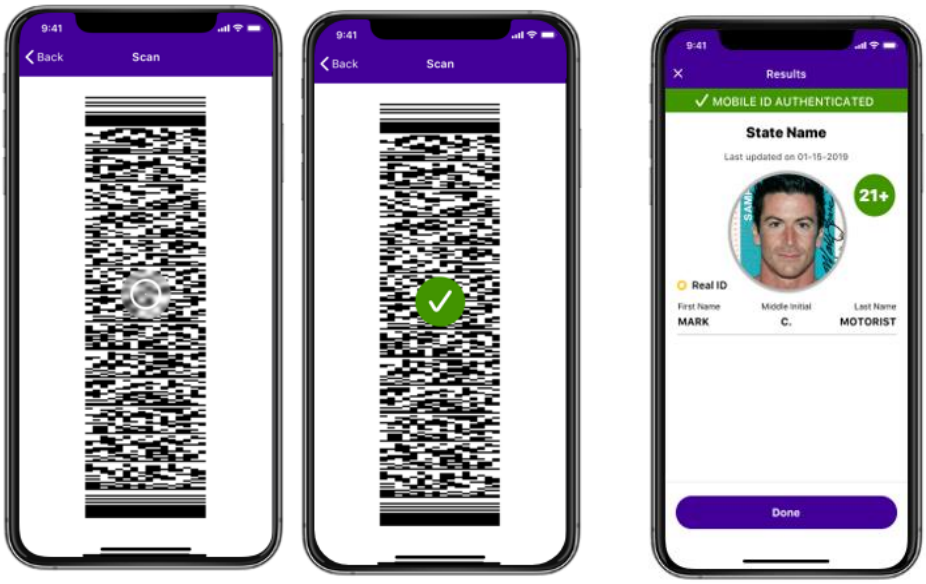

***Figure 16**. Scanning a PDF417 barcode example.*

The PDF417 barcode can be found on the end-user's physical ID or the digitally rendered one found in the **IDEMIA Mobile ID App** or through a chosen privacy view pre-chosen by the end-user in the **IDEMIA Mobile ID App**.

The end-user presents their physical ID or the digitally rendered version in the **IDEMIA Mobile ID App** to the Relying Party.

- The Relying Party scans the PDF417 barcode as presented.
- The attributes display on the Relying Party’s device.
- When displaying a PDF417 barcode, a circle appears on the **IDEMIA Mobile ID Verify App** screen with a “21+” or “not 21+” depending on the results. This can be customized by a Relying Party so they can choose which age threshold they prefer (over 18, 25, etc.).

Note: There is no BLE connection for this transaction. The attributes are shared with the Relying Party but the PDF417 barcode itself, is not considered as secure as using a QR code.

2.2.4 Optical Inspection of QR code

The Optical Inspection screen assists in verifying a **Mobile ID** credential during off-line in-person verification. The **IDEMIA Mobile ID Verify App** activates the smartphone camera and generates the end-user's portrait plus a QR code. The app uses the **Biometric Capture SDK** for image processing and matching. The encrypted digital representation of the portrait provides a security mechanism to ensure that a different photo has not been laid over the end-user's photo.

The functionalities of Optical Inspection include:

- The QR code contains all fields for the transaction and a secure, encrypted digital representation of the portrait associated with the Mobile ID credential. A biometric template is used to compare the captured portrait with the end-user's credential. The biometric template contains facial recognition data, such as the distance between the credential holder's eyes, length of the nose, etc.
- The photo displayed for the Relying Party matches the photo associated with the **Mobile ID** back-end service. The Relying Party scans the whole screen to get a return value from the Biometric Capture SDK confirming whether the captured portrait matches the QR code as compared with the biometric template.
- The Biometric Capture SDK parses the QR code (including the hash of the image), takes a portrait of the image, and calculates a fresh hash (i.e., the hash in the QR code plus the hash in portrait) to calculate a score. The Biometric Capture SDK then returns a matching or not matching score for verification.
- The **IDEMIA Mobile ID Verify App** displays an indicator of the authentication status, the set of attributes, and an image of the captured and processed photo.

Notes:

- **This feature is currently only supported in Android and in iOS Linux; Windows capability compatibility is yet to be determined.**
- **This feature does not verify physical IDs.**
- **There is no BLE data transfer during this transaction.**
- **This method is considered to be more secure than using a PDF417 barcode, but is thought to be easier to use than the ISO 18913 scan which uses a QR code and BLE data transfer.**
- **Currently the process is proprietary to IDEMIA, but it is moving towards standardization.**

2.2.5 Cutomizable attributes

The **IDEMIA Mobile ID Verify App** allows relying parties the capability to pick and choose which attributes they want to request from the end-user during verification with custom templates. The **IDEMIA Verify SDK**s also support this functionality.

2.2.5.1 Select and deselect attributes

To select attributes in the **IDEMIA Mobile ID Verify App** the Relying Party does the following:

1. Click the **Gear** icon and select **Attribute Settings** to choose from the standard set of attributes. or define a custom set of attributes to request from the end-user.
2. On the **Custom** screen, slide the button to the right for the desired attribute to select it.
3. On the **Custom** screen, slide the button to the left for the desired attribute to deselect it. When a button is deselected it will appear as faded out.

Note: The end-user must consent to share the attributes before the data transfers from the end-user's smartphone to the Relying Party's device.

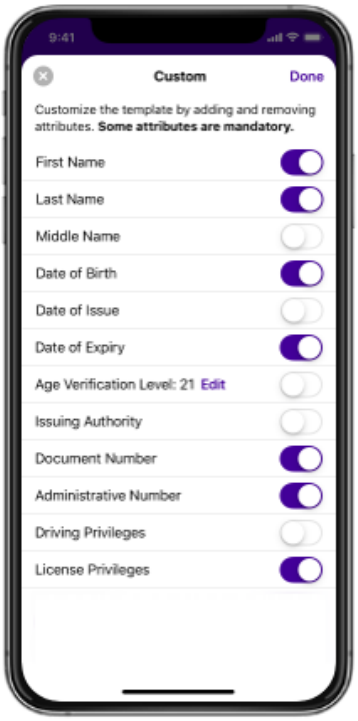

Figure 17. *The Relying Party can choose some or all of the attributes they want to request from the end-user.*

2.2.6 Credential Auto-Detection

This feature allows for a single optical "scan" button with no extra step required to select a verification method. Tapping the **I'm Ready to Scan** button launches the ability for the **IDEMIA Mobile ID Verify App** to detect the method of sharing presented automatically, whether it be a QR code, PDF417 barcode, or Optical Inspection screen.

Figure 18. *Automatic credential method detection example.*

2.2.7 Physical ID Verification

The **IDEMIA Mobile ID Verify App** can verify a stand-alone physical ID using these steps:

1. The Relying Party scans the PDF417 barcode with the **IDEMIA Mobile ID Verify App.**
2. The Relying Party sees the attributes display on their device.

2.2.8 Dynamic Display of Data

The **IDEMIA Mobile ID Verify App** can dynamically display data on the app's various screens based on the attributes chosen by the Relying Party, requested to the end-user, or received back from the end-user's smartphone.

If one or more attributes are not chosen, those are removed from the request information sent to the end-user. The missing attributes do not show up on the end-user's **IDEMIA Mobile ID App** as blank, "null", or similar. This prevents an unnecessary waste of screen space and improves end-user experience.

2.2.9 Forced App Upgrade

The **IDEMIA Mobile ID Verify App** contains a mechanism that automatically notifies the Relying Party that their current version of the app is out of date when opening the app.

The only two options are to update the app or exit the app. The Relying Party will not be able to use the app again until they upgrade to the latest version. They make their choice by tapping on the appropriate link.

This allows IDEMIA to ensure an **IDEMIA Mobile ID Verify App** user has the latest, most secure version. This also addresses and fixes or major functionality changes.

Figure 19. Expired app notification example.

2.2.10 "Not for Official Use" Indicator

The **IDEMIA Mobile ID Verify App** provides the ability to use a demo-only version of a **Mobile ID** credential. In this case, the app will display a clear banner across the top of the app stating **FOR DEMO USE ONLY- NOT A VALID ID**

Figure 20. Demo-use only indicator example.

2.2.11 Decline Notification

If the **Mobile ID** credential holder declines the request, the Relying Party will see the *Results* screen indicating declined attributes. If presented with this option, the Relying Party can tap **Try again,** depending on the scenario. Error messages have been conformed across operating systems.

2.2.12 Privacy By Design

The **IDEMIA Mobile ID Verify Product Suite** keeps the end-user's personally identifiable information (PII) and other attributes private by design.

From the ground up, the **IDEMIA Mobile ID Verify Product Suite** has focused on minimizing the exposure, transfer, and sharing of an end-user's information:

- Any PII (or other attributes) that are used in a transaction are always encrypted while in transit.
- Any PII (or other attributes) that are used in a transaction are discarded from the system as soon as the transaction is complete.
- The **IDEMIA Mobile ID Verify Product Suite**, and all of its related products, meet or exceed industry standards.
- The **IDEMIA Mobile ID Verify Product Suite** provides for end-to-end security.

2.2.13 Mobile ID Verify App Settings

Settings for the **IDEMIA Mobile ID Verify App** allow the Relying Party to view information regarding:

- About
- FAQ
- Help
  Quick Guides
- Age Verification
- Attribute Settings
- Terms of use
- Privacy Policy
- Age Verification and Attribute Settings are changeable.

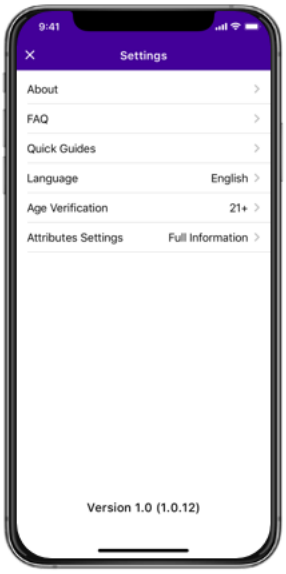

Figure 21. Setting menu example.

2.2.13.1 Age Verification

The *Age Verification* setting allows a Relying Party to change the preferred age that will show up in the verification results after they scan a PDF417.

- The **IDEMIA Mobile ID Verify App** will display the chosen age threshold as (Age+) in green if the end-user presenting the ID is over that age.
- The **IDEMIA Mobile ID Verify App** will display the chosen age threshold as (Age-) in red if the end-user presenting the ID is not over that age.

To change the age verification threshold, the Relying Party taps on the **Gear** icon inside the **IDEMIA Mobile ID Verify App** and taps on **Age Verification**.

The Relying Party then chooses an age verification choice between “18+” and “25+”.

The new choice automatically saves and is visible when the Relying Party taps **Back** to go back one screen.

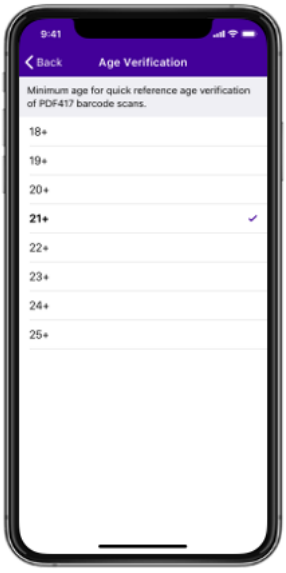

Figure 22. *Age verification settings example.*

Figure 23. *Age verifications result screens examples with different age thresholds.*

2.2.13.2 Attribute Settings

The *Attribute Settings* allows the Relying Party to change the template of the attribute request that will go out to **IDEMIA Mobile ID App** end-users. There are two choices:

- *Standard Information* with the option to view the attributes that will be requested
- *Custom* with the option to view and edit the attributes that will be requested

Standard Information

The *Standard Information* option is on by default within the **IDEMIA Mobile ID Verify App.** When this option is set, the following attributes are included in the request:

- Portrait
- REAL ID
- First Name
- Last Name
- Street Address
- City
- State
- Postal Code
- Birth Date
- Issue Date
- Expiry Date
- Age Verification 21
- Age in Years
- License Number
- Driving Privileges
- Gender
- Height
- Eye Color
- Last Update Timestamp

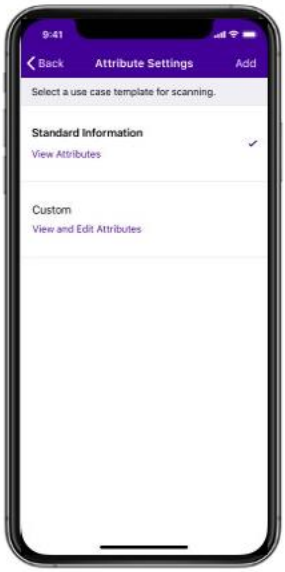

***Figure 24**. Standard Information menu example.*

Custom

When the Relying Party chooses this option, the Relying Party is able to choose which attributes they want requested of the **IDEMIA Mobile ID App** end-user. Toggle each choice to the right to enable it. The following attributes are available in this section:

- Portrait
- REAL ID
- First Name
- Last Name
- Street Address
- City
- State
- Postal Code
- Birth Date
- Issue Date
- Expiry Date
- Age Verification 21
- Age in Years
- Birth Year
- License Number
- Administrative Number

- Driving Privledges
- Gender
- Height
- Eye Color
- Hair Color
- Nationality
- Birth Place
- Issuing Country
- Issuing Authority
- Issuing Jurisdiction
- Portrait Timestamp
- Last Update Timestamp
- Next Update Timestamp
- Validity Date
- Full Name (UTF)

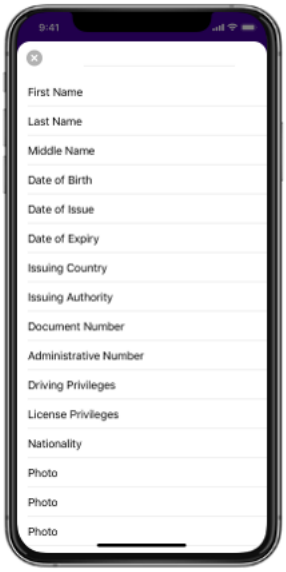

Figure 25. *Custom attributes menu choice example.*

2.3 Help and Support

2.3.1 In-App Quick Guides

The **IDEMIA Mobile ID Verify App** includes quick user guides inside the app for key functions. This content is the same content found in IDEMIA's offline quick guides.

Figure 26. Quick guide example.

2.3.2 FAQs

The Relying Party can access frequently asked questions inside the app by tapping on the **Gear icon**, then tapping on **FAQ.** A list of questions will display.

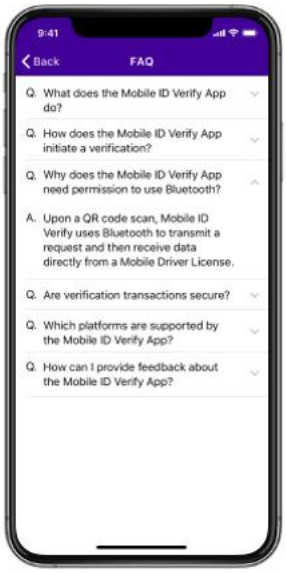

Figure 27. FAQ example.

2.3.3 Dedicated Help Resources

The Relying Party can access the dedicated help resources by tapping on the **Gear** icon in the **IDEMIA Mobile ID Verify App**. The Relying Party then taps on **Help** within the menu. A link to a support email address and a dedicated help phone number display.

3 International Standards

3.1 ISO/IEC 18013-5 Standard

ISO 18013-5 is the standard under development for digital driver's licenses and related mobile ID interoperability. The **IDEMIA Verify Product Suite** supports the N1677 and N1818 draft versions of ISO 18013-5.

IDEMIA periodically updates its software to support new draft versions of the ISO/IEC 18013-5 standard and has committed to support the final standard version. However, IDEMIA does not attempt to support every interim draft version that is released.

4 Security Measures and Privacy

The **IDEMIA Mobile ID Verify Product Suite** authenticates the validity of an identity-based credential via stringent security measures. This assures a Relying Party that the credential they have been presented with belongs to the end-user who is presenting it. The various layers of security provide confidence that the credential has not been tampered.

4.1 Product Security Standards and Tools

The **IDEMIA Mobile ID Verify Product Suite** adheres to the following international standards and policies:

- *Personally identifiable information* (PII) data, and other sensitive information, is not stored but is encrypted in transit.
- The ISO 18013 related security mechanisms that are used in validation of credentials Encryption keys are not hard coded. Where required NIST FIPS 140-2 certified cipher-suites (cryptography algorithms) are used (AES 256-bit CBC/GCM or better).
- Encryption mechanisms also enable point-to-point message encryption between the mobile application and the **Mobile ID** back-end services.
- Static code security analysis on the source code before compiling.

4.1.1 App Protection

The **IDEMIA Mobile ID Verify App** has ProGuard protection built into the Android app to protect the code and mitigate a variety of threat vectors.

4.1.2 Data Security

The **IDEMIA Verify Product Suite** works to secure all personally identifiable information (PII) and other small chunks of data that pass through the **IDEMIA Mobile ID Verify App** and SDKs:

- The Merkle hash tree in the **IDEMIA Mobile ID Verify App** enables little to no PII to be stored in the cloud or on-premise servers.
- Only a single index, such as an ID number, is required as a primary index to be hashed, salted, and stored in the cloud or on-premise servers.
- Secure connections are created between the authoritative SOR and **idFabric**™ when **idFabric**™ is hosted in the cloud utilizing a VPN or a secure-tunnel-technology.

4.1.2.1 Security Assessments

Security assessments, including penetration testing, are conducted regularly via the best-in-class independent security firms, including those commissioned by our customers.

4.1.2.2 Vulnerability Mitigation Process

IDEMIA maintains a structured vulnerability mitigation process that includes configuration control board oversight, security scans, and code analysis tools:

- The IDEMIA *Change Control Board* (CCB) exists to govern the release of the IDEMIA software to pre-production and production environments. The CCB comprises core team members who work to set the process framework, review release outcomes (e.g. epics, stories, defects, etc.), and security posture, amongst others.
- A critical artifact reviewed prior to any release is the security scan results and potential changes in security posture.
- Static code analysis plays a central role in ensuring the quality and security of software products. IDEMIA leverages a static code analysis tool which generates metrics that are monitored continuously to identity any detects and security vulnerabilities within the scanned application.
- IDEMIA uses at least two of the leading code analysis tools which are available on the market at all times.

4.1.3 End-user and Workflow Level Privacy Controls

The **IDEMIA Verify Product Suite** employs significant privacy-enhancing design and implementation policies to enable end-user and workflow level privacy controls, including:

- Identity attributes are stored in the end-user's smartphone.
- IDEMIA provides transactional data with anonymized identity information. The Issuing Authority cannot track who specifically is using the **IDEMIA Mobile ID Verify App** for various applications and use cases over time.
- Identity information is only provided to owners or operators of verification endpoints with consent confirmed with the end-user for each transaction (type).
- Error messages have been conformed across operating systems.
- Identity information is only provided to owners or operators of verification endpoints with consent confirmed with the end-user for each transaction (type), including for both in-person and online transactions.
- Error messages have been conformed across operating systems.

4.1.4 Certificate Authorities (CA)

Issuing Authorities are able to use IDEMIA's self-signed certificates as part of their **Mobile ID** program by:

- leveraging IDEMIA's CA engine within ID Way implementations outside the United States and Canada; or
- leveraging HydrantID as a 3rd party CA in the United States and Canada.

  Note: The second option allows Issuing Authorities to host their own root, if required.

Additional CAs can be supported due to the levels of abstraction in the **Mobile ID** (credential) Issuance Service via a professional services engagement for a specific project.

5 Glossary

Term	Definition
2D barcode	Two-dimensional barcode is used to describe barcode formats that encodes information in multiple rows of bars and spaces stacked on top of each other. Also called a matrix barcode. Example: PDF417
API	Application Programming Interface
BLE	Bluetooth Low Energy is a wireless personal area network technology that was initial released as part of Bluetooth 4.0. BLE is supported by iOS 5 and later and by Android 4.3 and later.
CA	Certificate Authority
CCB	Change Control Board
DMV	The Department of Motor Vehicles (DMV), in many states of the United States of America, the name of the government department that issues driver's licenses and state ID cards
ID	Identity Document(s)
IDP	Identity Provider is an entity such as a DMV that creates, maintains, and manages identifying information and provides authentication services to relying applications within a federation or distributed network
ISO	International Organization for Standardization
ISO-IEC 18013	A standard for obtaining data and trusting data from a mobile driver's license (mDL)
ISO-IEC 18013-5	The part of the 18013 standard that covers the technical and interoperability requirements for mobile driver's licenses. **Note:** This standard is expected to be finalized later in 2020.
M2M	Machine-to-Machine is a direct data exchange between devices using any communications channel, including wired and wireless, without human interaction.
mDL	Mobile Driver's License
mID	Mobile ID credential
NIST	National Institute of Standards and Technology
NIST 800-63-3	SP (Special Publication) 800-63-3, Digital Identity Guidelines
OIDC	OpenID Connect is an authentication layer on top of OAuth 2.0, an authorization framework.
OP	OpenID Connect Provider

Term	Definition
Open ID	An open standard and decentralized authentication protocol promoted by the non-profit OpenID Foundation
PDF417	A stacked linear 2D barcode format that was selected as the standard for the machine-readable zone technology on driver's licenses.
PII	Personally Identifiable Identification
PIN	Personal Identification Number
QR Code	Quick Response Code, a 2-dimensional barcode that contains instructions or information for another device that scans it
REAL ID	A sect of minimum-security standards set by US Federal law for the issuance of sources of identification, such as driver's licenses.
REST	Representational State Transfer, a software architectural style that defines a set of constraints to be used for creating web services
RP	Relying Party
SDK	Software Development Kit
SOR	System-of-Record
UTF	Unicode Transformation Format

6 Appendix B – Mobile ID Verify App Screens

6.1 Tutorial Screens