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 industry, national, and international standards bodies.

1.1.1 Components

The **IDEMIA Verify Product Suite** products interact with the rest of **IDEMIA's 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

1.1.2 Key functionalities

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

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

1.1.3   Verification

The **IDEMIA Mobile ID Verify App** is the front-facing part of the **IDEMIA Verify Product Suite**.

Note: You can obtain the IDEMIA branded app from your sales manager.

1.1.3.1   Relying Party

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

You can build **IDEMIA Mobile ID Verify Apps** for Android and iOS using 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 individual who serves as a verifier in-person can perform the in-person verification when the user submits their ID.

The credential holder is the individual who carries the identity document(s) (ID). The **IDEMIA Verify Product Suite** operates 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. The suite encrypts the user's identity attributes in the individual's smartphone and stores them only at the authoritative System of Record (SoR).

The method for verifying a 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.

1.1.4   Supported platforms and devices

Only smartphones are currently approved and supported for use on the **IDEMIA Mobile ID Verify App,** although it may function properly on individual laptops.

1.1.4.1   Android

This solution supports most Android smartphones (Android 7.x or newer) except the discontinued Samsung Galaxy S5.

1.1.4.2   iOS

This solution supports most Apple smartphones (iOS 11.x or newer) except the discontinued Apple iPhone 5S.

1.1.5   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

- Date of the latest update for attributes, status, and photo data

- Custom attribute request templates for the Relying Party

- Dynamic data display that renders results in a clear and concise manner

1.1.6   User experience

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

- Modern user interface with friendly instructional screens throughout

- Minimalistic attribute field names emphasize attribute values.

- At-a-glance age, trust level, and status icons (e.g., credential authentication results and age verification) with configurable thresholds.

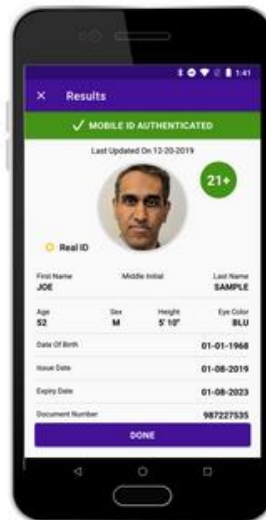- In-app user guides for quick at-a-glance support

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

2   IDEMA Verify SDK Package

2.1   Introduction

The **IDEMIA Verify Product Suite** consists of a back end set of SDKs, their related APIs, and documentation. You can implement the suite 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: You can find more detailed information about the IDEMIA Verify SDKs 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/

2.2   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

2.2.1   Exposed APIs

The related SDK documentation for **IDEMIA Mobile ID Verify Apps** describes the exposed APIs for **IDEMIA Verify SDKs**. These APIs are for devices that fit the following requirements:

- Android devices that run Android version 5 or later
- iOS devices that run iOS version 10 or later

    Note: Both devices must have a working camera and support BLE (Bluetooth Low Energy).

2.2.2   SDK installation package

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

2.2.2.1 Installation command

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

```
sudo dpkg –i Verify1.2.0.deb
```

2.3 SDK supported platforms and devices

The **IDEMIA Verify SDKs** allow you to build custom applications or integrate existing applications for the operating systems below and their corresponding devices.

2.3.1 Android SDKs

2.3.1.1 Supported devices

This solution supports most Android smartphones (Android 7.x or newer) except the discontinued Samsung Galaxy S5.

2.3.1.2 Skills required

The developers must have knowledge of the Android operating system.

2.3.1.3 Resources required

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

2.3.1.4 Tools required

The tools required are:

- Android Studio 3 or above
- Android SDK tools: preferred latest version (i.e., release 24.0 or above)
- JDK: preferred latest version (i.e., release 7.0 or above)
- Android device (i.e., emulator not supported)
- Minimum SDK version is 21 (i.e., Android 5.0)

2.3.2 iOS SDKs

2.3.2.1 Supported devices

This solution supports most Apple smartphones (iOS 11.x or newer) except the discontinued Apple iPhone 5S.

2.3.2.2 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

2.3.2.3 Resources required

The tools required for integration on a Macintosh are:

- Xcode 11.0 or above
- iOS SDK tools: release 11.0 or above (i.e., preferably latest version)
- Physical iOS device (i.e., simulator not supported)

2.3.2.4 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

2.3.3 Windows SDKs

2.3.3.1 Supported devices

The solution supports Windows smartphones (10.x or better).

2.3.3.2 Skills required

The developers need knowledge of:

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