What is?

Onboarding Management® is responsible for validating the identity of people to prevent identity theft.

Product components:

Onboarding Management® has two main modules: ID® and Face®.

These modules constitute the standard version of the product, which can also complement with the Voice® and Touch® modules, considering the type of onboarding that the client wants to implement.

Modules and complements

ID® & Face® authenticates the identity of people remotely, through the analysis of the identity document and facial biometrics.

Voice® authenticates the identity of people remotely, through voice identification.

Touch® authenticates the identity of people remotely, through the recognition of fingerprints.
Our Onboarding Management® solution is responsible for validating the identity of people to prevent identity theft.

ID® module is one of the main components of the tool since it enables remote authentication of people’s identity thanks to the reading of an identity document and a selfie. Thus, it manages the life cycle of citizens during the digital transformation process.

What is?

- Can be used in any camera-enabled device.
- It is customizable and modular. The client can select which functionalities are incorporated in each stage of the process.
- It is a complete, scalable software solution that can be easily integrated into the client’s existing system.
- The functionalities can be incorporated in existing applications without the need to create a new one.

Features:

Logical functional diagram
Integration with International Organizations

Enables the management of the identities of citizens

Our product has methods of integration with Government Organizations that allows the validation of aspects of the identity of citizens in a proven way in different countries.

Focus on user experience

At VU Security® we know that providing simple, intuitive, and secure experiences improves the reputation of institutions and increases the perception of trust on the part of citizens towards the organizations with which they must interact. That is why our focus is on constantly analyzing the user experience, proposing new features, and designing solutions related to their needs.

User interface options

The solution offers different options to integrate with applications, web portals and chatbots.

- Mobile SDK
- Web ID
- Message ID
- API

ID SDKs

VU Security® offers the possibility to integrate this functionality into existing applications. For this, it offers the SDK ID®, which has all the necessary methods for its operation:

- Registration
- Authentication
- Extraction of data from documents by OCR (ID, identity document, credit card)
• Document barcode reading
• Capture of the front of the document
• Capture of the back of the document
• Selfie capture
• Selfie validation with proof of life
• Obtaining the geolocation of the device

To improve the implementation experience and give the customer the freedom to generate the desired user experience, we provide a set of functions and a set of sample screens. This allows maintaining the necessary conditions to ensure the security and integrity of the product, as well as facilitating the transfer to the real implementation scenario.

**SDK® can be integrated as follows:**

<table>
<thead>
<tr>
<th>Technology</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android Java</td>
<td>Java</td>
</tr>
<tr>
<td>iOS</td>
<td>Swift</td>
</tr>
<tr>
<td>Web</td>
<td>Javascript</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Javascript, DART y TypeScript</td>
</tr>
<tr>
<td></td>
<td>Cordova, Ionic, React Native, Flutter</td>
</tr>
</tbody>
</table>
Integration API

It must be done through REST methods, always using a secure SSL channel (port 443).
The infrastructure is designed to integrate with any type of platform, regardless of the language used, through web services (POST/GET) published by ID®.

The application is made up of different methods, identified with functions aimed at the administrative management of use for end users. Communication between presentation layers and the product server is via SSL connections over TCP 443 port.

The available methods allow:
- Registration.
- Authentication.
- Extraction of data from documents by OCR (ID, identity document, credit card).
- Extraction of data from documents by reading the bar code and MRZ code.

**Image management recommendation**

- **Image format:** JPG
- **Minimum image size:** 600 x 720 pixels
- **Minimum image resolution:** 2 to 5 megapixels

**System requirements and compatibility**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Database</th>
<th>App Server</th>
<th>Java</th>
<th>Compatible devices (SDK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centos/Redhat 7.9</td>
<td>PostgreSQL 9 or later (*)</td>
<td>Tomcat 9.x</td>
<td>1.8</td>
<td>iOS 11 or later</td>
</tr>
<tr>
<td>Ubuntu 18.04 LTS (**), or later</td>
<td>MS SQL 2019 or later</td>
<td>Jboss 7.11 or later</td>
<td></td>
<td>Android 5 or later</td>
</tr>
<tr>
<td>Windows Server 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) Recommended
(**) We recommend using LTS versions
# Hardware sizing guidelines*

| Number of users | Parent instance | Secondary instance | | |
|-----------------|-----------------|-------------------|---|---|---|---|---|
|                 | Processor | Memory | Processor | Memory | Transactions per second | Required storage capacity | LOG storage | Onboarding storage |
| 1 a 10,000      | 8 processing threads | 6 GB RAM | 8 processing threads | 6 GB RAM | 16 | 120 GB - HD | 178 GB - HD | 120 GB - HD |
| 10,000 a 50,000 | 16 processing threads | 8 GB RAM | 16 processing threads | 8 GB RAM | 32 | 240 GB - HD | 980 GB - HD | 240 GB - HD |
| 50,000 a 100,000 | 32 processing threads | 16 GB RAM | 32 processing threads | 16 GB RAM | 64 | 480 GB - HD | 4,4 TB - HD | 480 GB - HD |
| 100,000 a 250,000 | 64 processing threads | 32 GB RAM | 64 processing threads | 32 GB RAM | 128 | 960 GB - HD | 6,3 TB - HD | 960 GB - HD |
| 250,000 a 1,000,000 | 128 processing threads | 64 GB RAM | 128 processing threads | 64 GB RAM | 256 | 2 TB - HD | 24 TB - HD | 2 TB - HD |

* The calculations and estimates contemplate the functioning on high availability.

# Outstanding use cases

- Remote and secure registration of bank accounts and credit card issuance.
- Check-in at hotels and airlines.
- Prevention of registration with false identity documents.
- Validation of voting and decision-making processes.
Other VU modules and products that reinforce ID®

Our products offer a 360° experience for both users and organizations. Each solution provides an additional layer of protection to their security strategy.

Onboarding Management® modules
• Face®
• Voice®
• Touch®

Authentication Management® modules
• Server®

VU Fraud Analysis®

For more information or to request a demo, contact us by mail at: sales@vusecurity.com
Onboarding Management® is responsible for validating the identity of people to prevent identity theft.

Face® module constitutes the first mass implementation platform for facial authentication.

The recognition of individuals is done by analyzing people's faces using reference points and the distance between these points. In turn, the registration of movements and actions, such as a wink or a smile, is used to prevent identity theft.

It is cross-platform and can be integrated with Microsoft and Cisco Systems®. It can be implemented in the background, without bothering the user.

Face® works by evaluating in real time the video captured by cameras with Intel® Real Sense™ technology, making a correct capture even if the user is in motion, to see, understand, interact, and learn from their environment.

Integration with International Organizations

Enables the management of the identities of citizens

Our product has methods of integration with Government Organizations that allows the validation of aspects of the identity of citizens in a proven way in different countries.
Focus on user experience

At VU Security® we know that providing simple, intuitive, and secure experiences improves the reputation of institutions and increases the perception of trust on the part of citizens towards the organizations with which they must interact. That is why our focus is on constantly analyzing the user experience, proposing new features, and designing solutions related to their needs.

Technical information

Face SDKs

VU Security® offers the possibility of integrating the Face® SDK into existing customer applications, considering the different stages of interaction:

- Registration
- Authentication

For this reason, Face® includes a set of functions that allow the appearance of the screens to be configured. In turn, to facilitate the implementation experience, a set of sample screens is provided so that the client can select the most appropriate one for the brand identity of your company or institution.

Thus Face® guarantees the necessary conditions to preserve the security and integrity of the product in real implementation scenarios.

SDK® can be integrated as follows:

<table>
<thead>
<tr>
<th>Technology</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android Java</td>
<td>Java</td>
</tr>
<tr>
<td></td>
<td>Android Java</td>
</tr>
<tr>
<td></td>
<td>Javascript, DART y TypeScript</td>
</tr>
<tr>
<td></td>
<td>Make use of Native SDKs</td>
</tr>
<tr>
<td></td>
<td>Hybrid Cordova, Ionic, React Native, Flutter</td>
</tr>
<tr>
<td></td>
<td>Javascript, DART y TypeScript</td>
</tr>
<tr>
<td></td>
<td>Make use of Native SDKs</td>
</tr>
<tr>
<td></td>
<td>Javascript, DART y TypeScript</td>
</tr>
<tr>
<td></td>
<td>Make use of Native SDKs</td>
</tr>
</tbody>
</table>

© 2022 VU Inc. All rights reserved.
It must be done through REST methods, always using a secure SSL channel (port 443).
The infrastructure is designed to integrate with any type of platform, regardless of the language used, through web services (POST/GET) published by Face®.

The application is made up of different methods, identified with functions aimed at the administrative management of use for end users. Communication between presentation layers and the product server is via SSL connections over TCP 443 port.

The available methods allow:
• Registration.
• Authentication.
• Block/Unblock users.
• Delete users.

**System requirements and compatibility**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Database</th>
<th>App Server</th>
<th>Java</th>
<th>Compatible devices (SDK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centos/Redhat 7.9</td>
<td>PostgreSQL 9 or later (*)</td>
<td>Tomcat 9.x</td>
<td>1.8</td>
<td>iOS 11 or later</td>
</tr>
<tr>
<td>Ubuntu 18.04 LTS (**), or later</td>
<td>MS SQL 2019 or later</td>
<td>Jboss 7.11 or later</td>
<td>Android 5 or later</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) Recommended

(**) We recommend using LTS versions
Hardware sizing guidelines*

<table>
<thead>
<tr>
<th>Number of users</th>
<th>Processor</th>
<th>Memory</th>
<th>Parent instance</th>
<th>Secondary instance</th>
<th>Transactions per second</th>
<th>Required storage capacity</th>
<th>LOG storage</th>
<th>Onboarding storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 a 10.000</td>
<td>8 threads</td>
<td>6 GB</td>
<td>8 processing</td>
<td>8 processing</td>
<td>16</td>
<td>120 GB - HD</td>
<td>178 GB - HD</td>
<td>120 GB - HD</td>
</tr>
<tr>
<td>10.000 a 50.000</td>
<td>16 threads</td>
<td>8 GB</td>
<td>16 processing</td>
<td>8 processing</td>
<td>32</td>
<td>240 GB - HD</td>
<td>980 GB - HD</td>
<td>240 GB - HD</td>
</tr>
<tr>
<td>50.000 a 100.000</td>
<td>32 threads</td>
<td>16 GB</td>
<td>32 processing</td>
<td>16 processing</td>
<td>64</td>
<td>480 GB - HD</td>
<td>4,4 TB - HD</td>
<td>480 GB - HD</td>
</tr>
<tr>
<td>100.000 a 250.000</td>
<td>64 threads</td>
<td>32 GB</td>
<td>64 processing</td>
<td>32 processing</td>
<td>128</td>
<td>960 GB - HD</td>
<td>6,3 TB - HD</td>
<td>960 GB - HD</td>
</tr>
<tr>
<td>250.000 a 1.000.000</td>
<td>128 threads</td>
<td>64 GB</td>
<td>128 processing</td>
<td>64 processing</td>
<td>256</td>
<td>2 TB - HD</td>
<td>24 TB - HD</td>
<td>2 TB - HD</td>
</tr>
</tbody>
</table>

* The calculations and estimates contemplate the functioning on high availability.

Outstanding use cases

- Citizen registration.
- Payment of transaction.
- Unblocking of homebanking accounts.
- Patient identification.
- Patient registration.
Other VU modules and products that reinforce Face®

Our products offer a 360° experience for both users and organizations. Each solution provides an additional layer of protection to their security strategy.

Onboarding Management® modules
• ID®
• Voice®
• Touch®

Authentication Management® modules
• Server®

VU Fraud Analysis®

For more information or to request a demo, contact us by mail at: sales@vusecurity.com
**What is?**

**Onboarding Management®** is responsible for validating the identity of people to prevent identity theft.

**Voice®** module is designed to identify people through their unique characteristics of each voice, such as tone, cadence, and volume.

**How does it work?**

Once implemented and integrated with the company’s system responsible for authenticating users, **Voice®** generates countless random phrases that the user will use to register.

Based on dynamic data from the platform (such as date, username, ID, number of transactions), **Voice®** produces a unique phrase that the user must repeat out loud and naturally to authenticate the transaction (for example: “VU Security is a provider of information security solutions”).

Authentication can be given by telephone, internet, or in person at a self-service terminal.

**Features:**

- Registration is carried out considering the client’s flow by recording audio with predefined phrases.
- The user registers by recording between 1 and 10 audios with his voice. The exact amount is configurable by the customer.
- The registration will be successful when the comparisons of each audio against the previously entered audios exceed a certain threshold, configurable by the client.
- To validate, the Voice API returns a value that represents the percentage of this similarity, between 0 and 1, where 1 is 100%.
- The audio files are saved in a database, consuming their storage quota.

**Applications**

- Identity validation
- Login in interfaces for blind people
- Proof of life
- Replacement of telephone validation of credit cards

© 2022 VU Inc. All rights reserved.
Benefits

• Replace other biometrics factors where and when requires.
• Facilitates use for senior citizens.
• Allows use in interfaces for visually impaired persons.
• Enables proof of life from remote locations.

User process

New user registration

Pattern validation

Biometric identification (voice)

Return of results

SAY: “Use my voice as a form of secure access”

SAY: Full Name

IDENTITY VALIDATED
Standard integration architecturer

Registration

• Registration request with 1 to 10 audios
• A Base64 encoded voiceprint is generated and stored

Validation

• Through the initial interface, enter the user and the identity number (within the App, IVR, etc.) to be developed by the client.
• Play user audio.
• Carry out the biometric comparison.
• Successful or failed validation is obtained.
Integration architecture + Server

Registration

- Registration begins, requiring user data (identity document, address, etc.).
- This entry creates a user in the Server.
- Enrollment request with 1 to 10 audios.
- Generation and storage of a voiceprint encoded in Base64.

Validation

- Through the initial interface, enter the user and identity document number (within the App, IVR, etc.) to be developed by the client.
- User audio output.
- Perform the biometric comparison.
- Successful or failed validation is obtained.
System requirements and compatibility

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Database</th>
<th>App Server</th>
<th>Java</th>
<th>Compatible devices (SDK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centos/Redhat 7.9</td>
<td>PostgreSQL 9 or later (*)</td>
<td>Tomcat 9.x</td>
<td>1.8</td>
<td>iOS 11 or later</td>
</tr>
<tr>
<td>Ubuntu 18.04 LTS (**) or later</td>
<td>MS SQL 2019 or later</td>
<td>Jboss 7.11 or later</td>
<td></td>
<td>Android 5 or later</td>
</tr>
<tr>
<td>Windows Server 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) Recommended
(**) We recommend using LTS versions

Hardware sizing guidelines*

• Audio Format: WAV Format, 16 Bit PCM. Preferably at a sampling frequency of 16000 Hz.
• Within the flow, Voice needs to receive the audio in Base64 to process the information.

<table>
<thead>
<tr>
<th>Number of users</th>
<th>Parent instance</th>
<th>Secondary instance</th>
<th>Transactions per second</th>
<th>Required storage capacity</th>
<th>LOG storage</th>
<th>Onboarding storage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Processor</td>
<td>Memory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8 processing threads</td>
<td>6 GB RAM</td>
<td>8 processing threads</td>
<td>6 GB RAM</td>
<td>16</td>
<td>120 GB - HD</td>
</tr>
<tr>
<td>1 a 10.000</td>
<td>8 GB RAM</td>
<td>8 GB RAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.000 a 50.000</td>
<td>16 processing threads</td>
<td>8 GB RAM</td>
<td>16 processing threads</td>
<td>8 GB RAM</td>
<td>32</td>
<td>240 GB - HD</td>
</tr>
<tr>
<td>50.000 a 100.000</td>
<td>32 processing threads</td>
<td>16 GB RAM</td>
<td>32 processing threads</td>
<td>16 GB RAM</td>
<td>64</td>
<td>480 GB - HD</td>
</tr>
<tr>
<td>100.000 a 250.000</td>
<td>64 processing threads</td>
<td>32 GB RAM</td>
<td>64 processing threads</td>
<td>32 GB RAM</td>
<td>128</td>
<td>960 GB - HD</td>
</tr>
<tr>
<td>250.000 a 1.000.000</td>
<td>128 processing threads</td>
<td>64 GB RAM</td>
<td>128 processing threads</td>
<td>64 GB RAM</td>
<td>256</td>
<td>2 TB - HD</td>
</tr>
</tbody>
</table>

* The calculations and estimates contemplate the functioning on high availability.
For more information or to request a demo, contact us by mail at: sales@vusecurity.com