VU

Onboarding Management

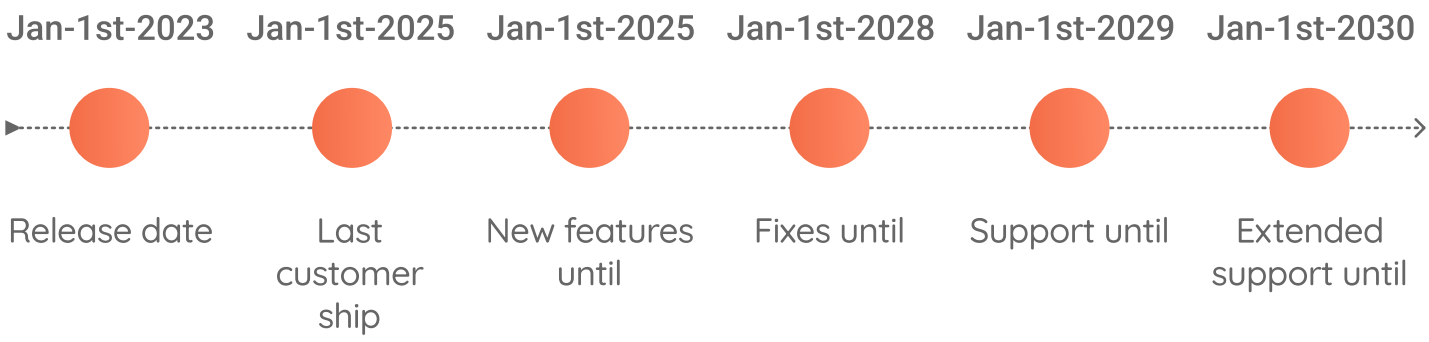
Datasheet

Version 2.0.0

End of Life

Onboarding Management v2.0

...



What is?

Onboarding Management® is responsible for validating people's identities to prevent identity theft.

It prevents the fraudulent use of a person's private information, authenticating their identity remotely, by analyzing their ID and biometric face, voice, and fingerprint verification.

It offers more secure methods of user registration and authentication, as a person's biometric data cannot be shared, and it is less vulnerable to social engineering attacks. In addition, the biometric uniqueness of each user mitigates the chances of success in cases of fraud due to massive brute force attacks.

Onboarding Management® technology simplifies the user enrollment and authentication experience with credentials that do not need to be remembered, retrieved, or managed.

Benefits

• It remotely validates identity with active and passive proof-of-life tests and anti-spoofing filters.

• It favors inclusion by increasing the conversion of users in remote locations.

• It automatically generates an identity score, with configurable thresholds.

• It lowers transaction costs for the client.

• It complies with the requirements of banking and transactional regulatory bodies.

• It allows the integration of proof-of-life tests in any digital channel (ChatBot, WhatsApp, Mobile App, Web, among others).

• It is a complete and scalable software solution that can be easily integrated into any digital system.

• It manages the life cycle of citizens during the digital transformation process.

Modular solution

Onboarding Management® is customizable and modular, so each client can select the functionalities they want to incorporate at each stage of their client's registration process, adapting it to their business model.

It has two main modules: **ID + Face®**. These modules constitute the standard version of the product, which can also be complemented with the **Voice®** and **Touch®** modules, depending on the type of onboarding process that you want to implement.

Modules

VU ID+Face

ID + Face® authenticates the identity of people remotely, through the analysis of their **ID and facial biometrics.**

VU Voice

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

VU Touch

Touch® authenticates the identity of people remotely, through **fingerprint recognition.**

VU

ID + Face

Onboarding Management

Datasheet

Version 2.0.0

What is?

ID+Face® modules are the main components of **Onboarding Management®** and allow remotely authenticating people's identities by reading their IDs and taking some selfies.

It provides the ability to manage people's identity in a secure, scalable, and easy-to-maintain way, in addition to running in any environment and through any selected channel (ChatBot, WhatsApp, mobile application, Web, among others).

The **ID+Face®** module offers flexible user registration and authentication options that comply with security parameters set by different countries while providing a frictionless and optimized user experience.

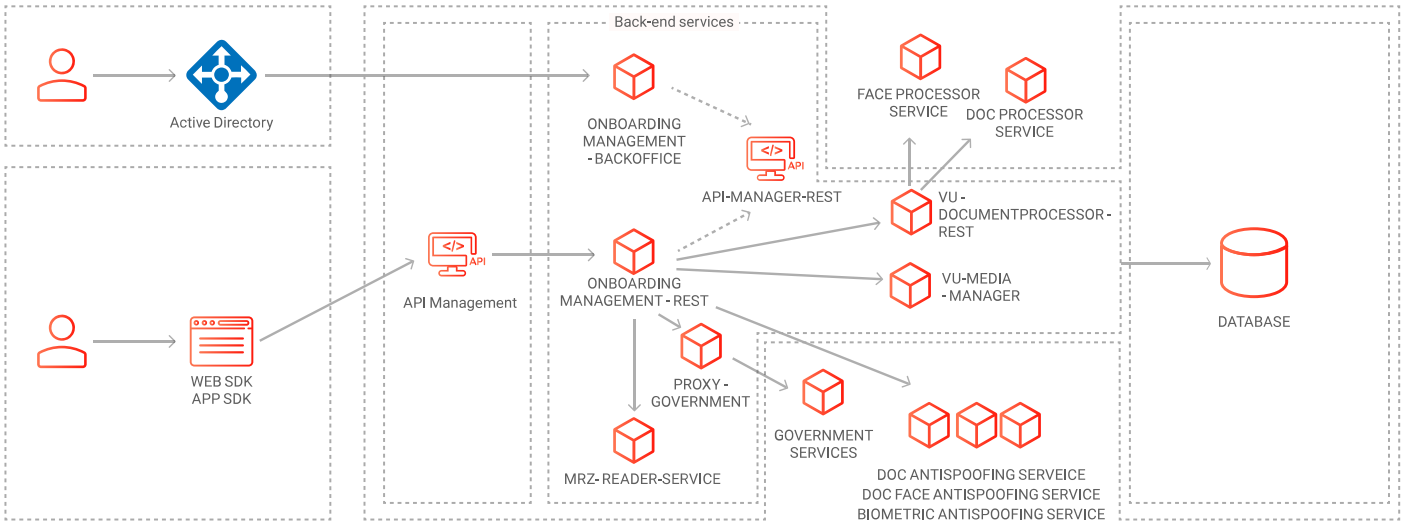
Benefits

- It can be used on any device with a camera.
- It is customizable and modular, which allows each client to select which features they want to incorporate at each stage of the onboarding process, adapting it to each business model.
- It carries out user authentication processes by evaluating unique facial characteristics: distances, depth, shape, colors, and skin layers, among others.
- Its features can be incorporated into existing applications without the need to create a new one.
- Liveness detection to verify that the captured face corresponds to that of a living person through the dynamic execution of a series of guided gestures in front of the device's camera.
- It offers different integration options with applications, web portals, and chatbots.

Outstanding use cases

- Remote and secure registration of bank accounts and credit cards.
- Check-in at hotels and airlines.
- Prevention of registration with forged identity documents.
- Validation of nominated voting and decision-making processes.
- Citizen and user registration.
- Transaction payment.
- Unlock home banking accounts.
- Patient identification and registration.

Logical functional diagram



Integration with government agencies

Our product has integration methods with government agencies from different countries that allow us to validate aspects of citizen identity reliably and securely.

Focus on the user experience

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

Onboarding flexibilization

NEW

The onboarding process can be carried out with any ID by configuring the data to extract from it (OCR, MRZ, and PDF417) and setting the validation flows required for each case.

• Template based

It offers the possibility of performing the onboarding process with different types of IDs using a series of templates developed and integrated into the *document processor**.

• Template-less

It offers the possibility of performing the onboarding process with any type of IDs, regardless of whether or not it has an integrated template.

UI Options
The solution offers different options to integrate with apps, web portals and chatbots.

- Mobile SDK
- Web ID
- Message ID
- API

***Document processor**: service that processes the user's ID and extracts the necessary information to validate its legitimacy.

ID+Face SDK

VU Security® offers the possibility of integrating this functionality into any existing application. Our **ID+Face®** SDK has all the necessary methods to ensure the following features:

MRZ reading
It automatically checks the data of the document.

OCR data extraction
It verifies and extracts data from any ID or credit card that contains OCR.

Barcode reading
It scans and decodes the information stored in the ID's barcode.

ID front and back capture
It gets and compares the front and back of the document for more accurate verification.

Selfie and life detection
It prevents identity theft by recognizing the person's presence on camera.

Antispoofing
It compares the person's face with the photos in the document to see if there are any inconsistencies.

ID normalizer
It reframes the ID image for better processing and verifies the presence of the photo and barcode.

Document type identification
Through an AI, it recognizes the type of document (with or without template) and detects any sign of forgery.

Government check
Verifica y contrasta la información del documento con los organismos gubernamentales.

Device geolocation
It recognizes unusual operations that may involve identity theft cases.

The SDK is delivered with a set of sample screens and features that allow the creation of a customized user experience. They reproduce the necessary conditions to preserve the security and integrity of the product, as well as to facilitate the transfer to the real implementation scenario.

SDK integration

	Technology	Delivery
Android	Java	SDK + Example
iOS	Swift	SDK + Example
Web	Javascript	SDK + Example
Hybrid Cordova, Ionic, React Native, Flutter	Javascript, Dart & TypeScript They make use of Native SDK	SDK + Example

Integration API

It is possible to implement it in any environment because it is cross-platform and provides an extensive integration capacity.

The application consists of different methods, with functions that allow end-user management. The communication between the visible layers and the product's server is through SSL connections over TCP 443 port.

It is designed to be integrated with any platform, regardless of the language used, via web services (POST/GET) published by **ID+Face®**.

The methods available allow to:

- Register and authenticate users
- Block and unblock users
- Monitor the application and the databases
- Remove users
- Manage and store user transactions

Digital client file

It generates a digital client file that includes the entire life cycle, the information of all the successfully carried out operations, and the seflies, without the need to use any intermediary software.

Case manager customization

It produces a paginated index via API REST containing all the user's operations, their status, the different scores obtained, and which ID elements were successfully read or not, capable of being integrated into any internal tool.

Face detection & verification engine

NEW

VU Face Engine® compares faces within the captured images to verify the user's identity with a high degree of accuracy. Since it was developed by VU, it integrates more organically with their products and allows to perform tasks like face detection, cropping, and aligning without the need to license other engines.

Asynchronous onboarding

NEW

It sends notifications every time an operation status changes, regardless of any process interruptions, thanks to a WebHook incorporated between the events.

It is carried out using REST methods, always using a secure SSL channel (port 443).

Queries must be made exclusively via a **private api-key.**

Image management recommendation

- Format: JPG
- Minimum size: 2 to 5 megapixels
- Minimum resolution: 600 x 720 pixels

Technical information

Hardware and software requirements

Operative system	Database	App Server	Java	Devices compatibility (SDK)
Centos/Redhat 7.9 (1)	Versión PostgreSQL 9 or superior	Tomcat 9.31 or superior (1)	11+	iOS 11 or superior
Ubuntu LTS (1)	MS SQL 2019 or superior (1) (2)	Jboss 7.11 or superior		Android 5 or superior
Windows Server 2019	MySQL 5.7			

(1) Recommended

(2) Supplied in the installation packages.

Server components

Users	Transactions per seconds	Cores	RAM	Storage	Estimated monthly storage
250.000	8	2	4	60 GB	25 GB
500.000	16	4	8	120 GB	50 GB
1.000.000	32	8	16	240 GB	100 GB
2.000.000	64	16	32	480 GB	200 GB
+2.000.000	Consult our team				

The calculations estimate habitual instances of the product. We suggest using it with the same characteristics as the ones presented for high availability configurations.

Support

Support level

NEW

VU will provide **level 3 support**.

Support includes a set of technologies and rights to help the customer maximize the investment made in VU licenses.

To contact VU Support, please send an email to: customer.support@vusecurity.com

As soon as your email is received, you will be automatically assigned a case and you will receive all the news related to your case in the same email thread.

If you want to add recipients, put them on a copy. Put Subject: [Name of the client] [Criticality] [Title of the problem].

Support cases are dealt with from **Monday to Friday from 9 a.m. to 6 p.m.** (Argentina).

Contact

Other VU Security products

Our solutions offer a 360° experience, each contributing an essential aspect to the security strategy of both users and organizations.

Authentication Management:

- Server
- SDK
- App

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

CIAM / IAM

If you need more information or want to schedule a demo of this solution, please write to us at: sales@vusecurity.com

VU

Voice

Onboarding Management

Datasheet

Version 2.0.0

What is?

Voice® is an **Onboarding Management**® module that allows you to identify people through the unique characteristics of their voice, such as tone, cadence, and volume.

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

Voice® takes dynamic data from the platform (such as date, username, ID, number of transactions, etc.) as a reference to generate a unique phrase that the user must repeat out loud to authenticate any transaction.

Authentication can be given by telephone, via the Internet, via WhatsApp, or in person at a self-consultation terminal.

Benefits

- It is hard to spoof and generally more convenient since it doesn't require remembering complex passwords.
- It creates a unique Voiceprint based on the user's voice patterns.
- It guarantees that the person who accesses a system or service is who they say they are, they are alive, and have the means to identify themselves.
- It does not require the sharing of personal information or credit card numbers to verify the person's identity.
- It allows choosing a unique identification phrase by repeating it in various ways to recognize the person's voice pattern.
- It creates a more flexible and conversational user experience, simplifying the user flow and reducing the time it takes to verify their identity.

Outstanding use cases

- Replacement of other biometric factors for identity authentication.
- Simplification of registration on the web or mobile applications for older people.
- Registration and access to the web or mobile applications for blind people.
- Proof of life from remote places.
- Substitution of credit card telephone validation.

Registration and authentication process

User registration

- The registration process asks the user to enter from 1 to 10 audios to generate their password (keyword or phrase), which can be customized or defined by default by the system configuration.
- The amount of audio required is configurable.
- If **Voice**® is integrated with **ID+Face**®, this process will also create a user in that module.
- The base64-encoded customer voiceprint is generated and stored in the database.

Static user authentication

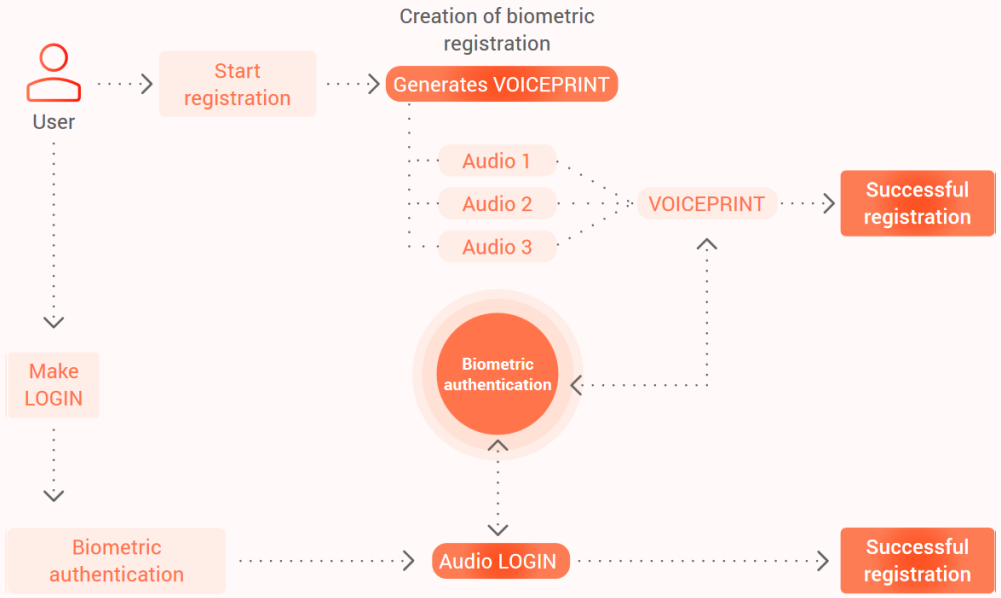
- Every time a user attempts to access the system (within the app, IVR, etc.), they are prompted to repeat out loud the passphrase entered during registration to authenticate the transaction.
- The entered word is compared to the user's voiceprint stored in the database.
- Voice API returns a value that represents the percentage of similarity between the two audios.
- The required percentage for successful authentication is configurable and can be between 0 and 1, where 1 is 100%.
- If the biometric characteristics of both audios reach or exceed the required percentage of similarity, the user's identity is authenticated. If they do not pass it, it is rejected.

User authentication by challenge

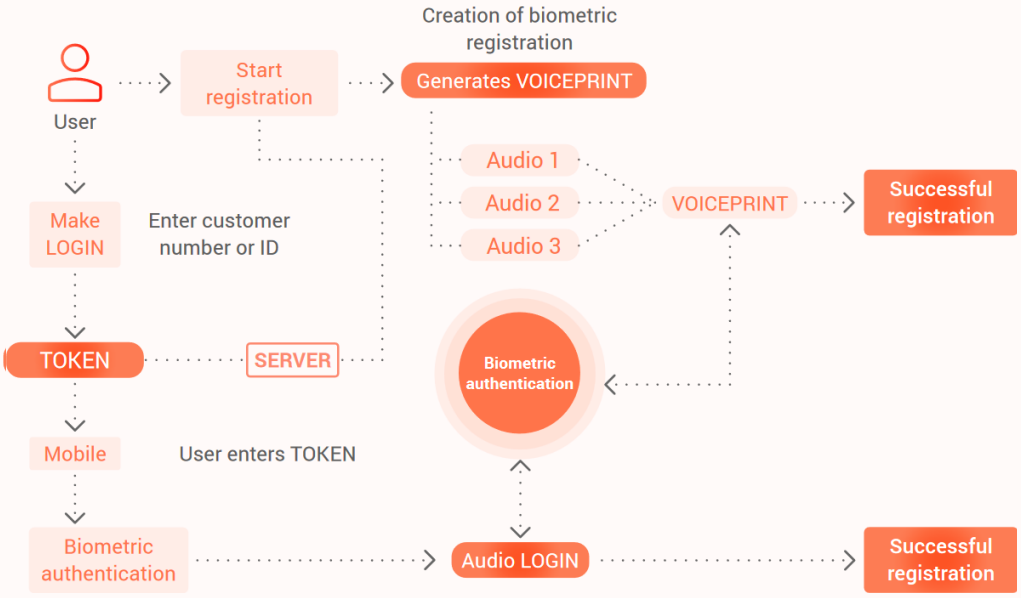
- Every time a user attempts to access the system (within the app, IVR, etc.), they are prompted to enter a group of random words, as part of a verbal challenge.
- The entered words are compared to the user's voiceprint stored in the database.
- Voice API returns a value that represents the percentage of similarity between the two audios.
- The required percentage for successful authentication is configurable and can be between 0 and 1, where 1 is 100%.
- If the biometric characteristics of both audios reach or exceed the required percentage of similarity, the user's identity is authenticated. If they do not pass it, it is rejected.

Logical functional diagram

No server integration



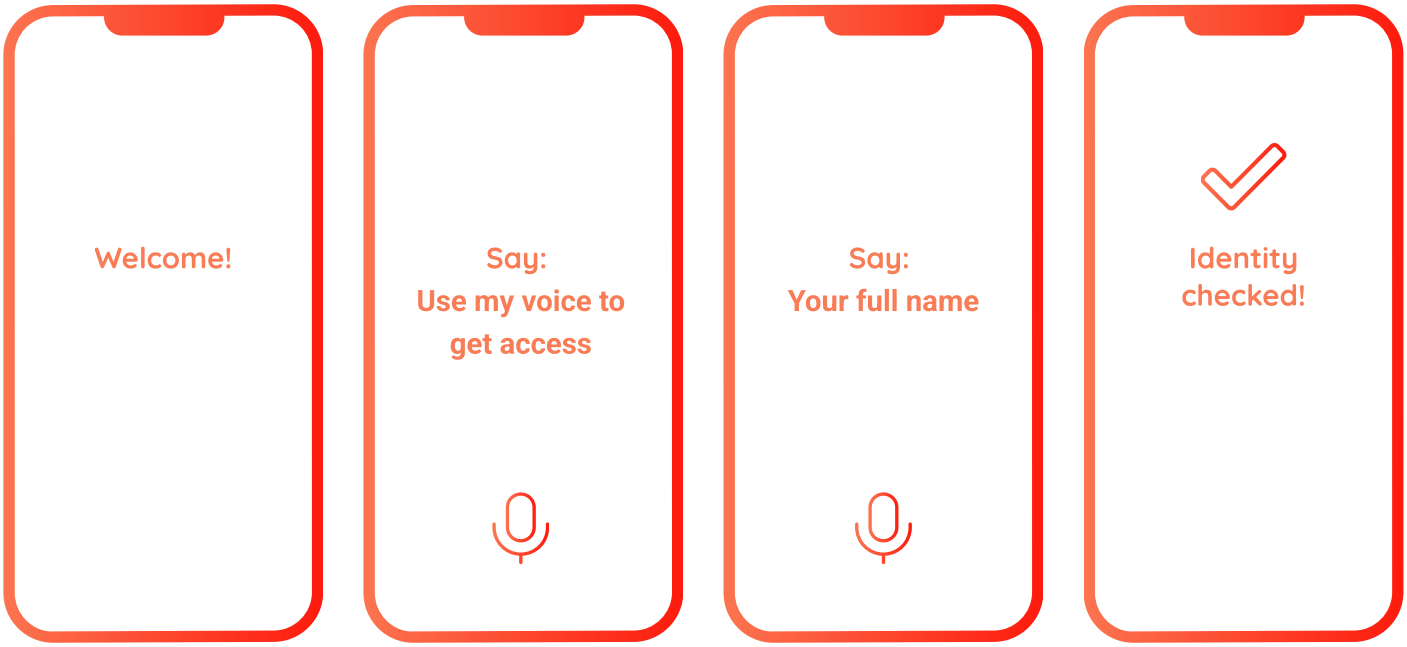
With Server integration



Focus on the user experience

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

Customer journey



New user registration

Voice pattern validation

Biometric identification (voice)

Results

Voice SDK

VU Security® offers the possibility of integrating this functionality into any existing application. Our **Voice®** SDK has all the necessary methods to ensure the following features:

Configurable passphrase
It sends 1-10 audios to the API to register the user.

Biometric login
It checks the biometric consistency of the user's audio with the passphrase.

Authentication by challenge
It generates a (configurable) number of words or phrases, as a challenge, that the user must repeat.

Anti-spoofing
It uses Deep Learning to detect potential identity theft threats by saying the passphrase.

Voiceprint updates
Updates the user's biometric registration, adding new Base64-encoded audios.

Proof of life
Anti-spoofing algorithms that identify the use of spoofing artifacts and accurately determine the liveliness of the voice.

Integration API

The application consists of different methods, with functions that allow end-user management. The communication between the visible layers and the product's server is through SSL connections over TCP 443 port.

Voice® can be implemented in any environment (telephone, internet, messaging, or self-service terminals), integrating public and private methods that allow to:

- Register and authenticate users
- Block and unblock users
- Monitor the application and the databases
- Logically remove users (soft-delete)
- Physically remove users (hard-delete)*
- Manage and store user transactions

(*) The user **must be previously deleted logically**, using the softDeleteUser() method.

Engines

- Voice Verification: Internal REST API developed in Python, served by Flask.
- Antispoofing: Internal REST API developed in Python, served by Flask.
- Azure speech: Microsoft API REST.

Audio management recommendation

- Format: WAV. 16 Bits PCM
- Sample rate: 8,000 Hz for the phone channel and 16,000 Hz for WhatsApp.
- Duration: between 4,500ms and 15,000ms
- Coding: audio files in Base64

Technical information

Hardware and software requirements

Operative system	Database	App Server	Java	Devices compatibility (SDK)
Centos/Redhat 7.9 (1)	Versión PostgreSQL 9 or superior	Tomcat 9.31 or superior (1)	1.8	iOS 11 or superior
Ubuntu LTS (1)	MS SQL 2019 or superior (1) (2)	Jboss 7.11 or superior		Android 5 or superior
Windows Server 2019				

(1) Recommended
(2) LTS versions are recommended

Server components

Users	BS storage	Transactions per seconds	Cores	RAM	System storage
1 a 100.000	65 GB	8	2	4	60 GB
200.000	130 GB	16	4	8	80 GB
300.000	200 GB	36	8	16	100 GB
400.000	260 GB	64	16	32	120 GB
500.000 +	325 GB	128	32	64	140 GB

The calculations estimate habitual instances of the product. We suggest using it with the same characteristics as the ones presented for high availability configurations.

Support

Support level

NEW

VU will provide **level 3 support**.

Support includes a set of technologies and rights to help the customer maximize the investment made in VU licenses.

To contact VU Support, please send an email to: customer.support@vusecurity.com

As soon as your email is received, you will be automatically assigned a case and you will receive all the news related to your case in the same email thread.

If you want to add recipients, put them on a copy. Put Subject: [Name of the client] [Criticality] [Title of the problem].

Support cases are dealt with from **Monday to Friday from 9 a.m. to 6 p.m.** (Argentina).

Contact

Other VU Security products

Our solutions offer a 360° experience, each contributing an essential aspect to the security strategy of both users and organizations.

Authentication Management:

- Server
- SDK
- App

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

CIAM / IAM

If you need more information or want to schedule a demo of this solution, please write to us at: sales@vusecurity.com

Touch

Onboarding Management

Datasheet

Version 2.0.0

What is?

Touch® is an **Onboarding Management®** module that allows remote authentication of people's identities by recognizing any of their fingerprints.

In order to carry out the identification, the person enters their fingerprint using a fingerprint reader device. The sample is compared with the sample submitted during enrollment and with the validations provided by government entities. If the fingerprints match, then the person's identity is authenticated.

It consists of three different methods: registration, identification, and validation of fingerprints by government entities, and it can work as part of multi-factor authentication (MFA), facilitating the user experience.

Benefits

- It is designed to be able to integrate with any other platform, regardless of the language used.
- It allows configuring the fingerprint of which finger the user will be asked to approve the registration and authentication process.
- It offers fast, easy, and non-invasive login methods.
- It can be hosted on a server segment with a traditional local network setup and accessed from the Internet or Intranet.
- Government entities report asynchronously on the result of the operation.
- Transactional logs are saved in the database.
- It is ready to be used with Docker.

Outstanding use cases

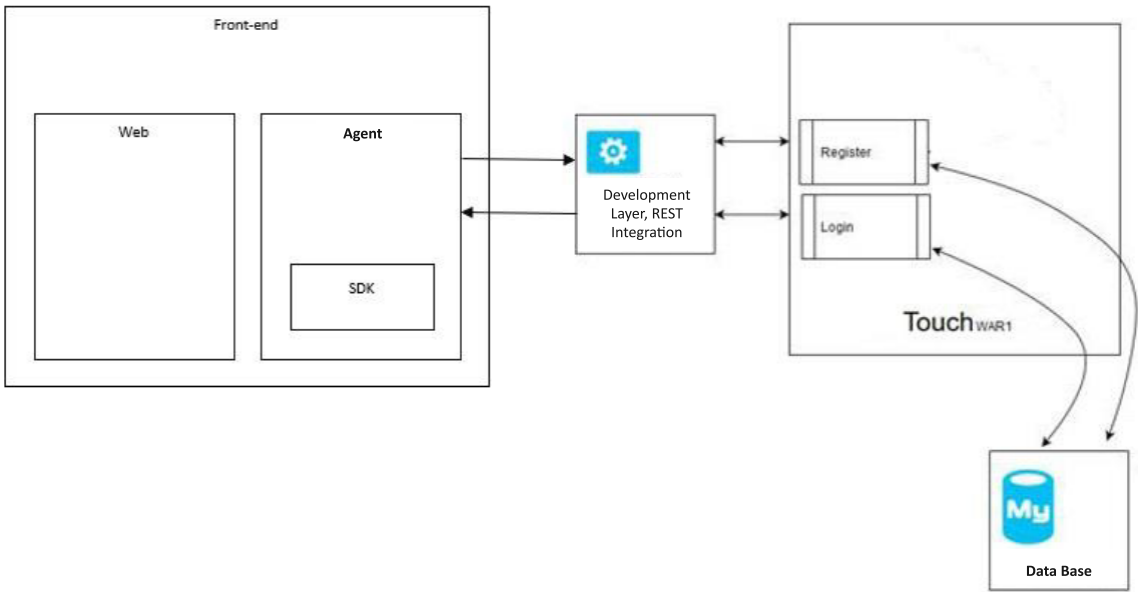
- Prevention of enrollment with forged identity documents.
- Citizen enrollment and biometric passports.
- Student and employee attendance control.
- Unblocking of home banking accounts, for wallets and digital devices.
- Digital document signature or virtual payment confirmation.

Fingerprint registration and authentication process

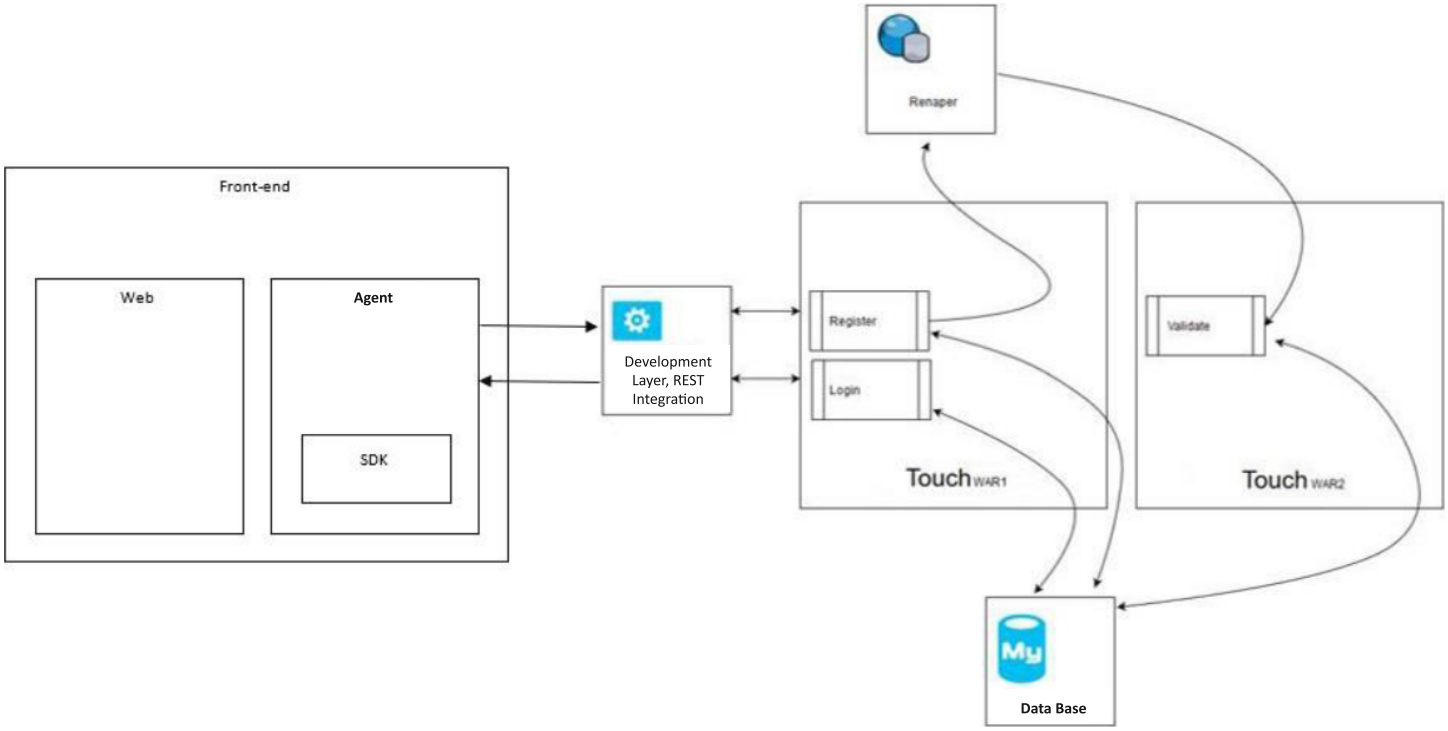
- The user repeatedly puts one of their fingers on the fingerprint sensor until the fingerprint is registered.
- The system checks if the user already exists. In case it is a new user, it associates the fingerprints to that user and stores them in the database.
- If the user is already in the system, it checks if the fingerprint matches the one stored in the database. In case the biometric characteristics of both fingerprints do not match, the user's identity is not authenticated.
- Asynchronously, it performs a validation with the corresponding government entities, to define whether the operation is approved or not.
- A record of the operation is created in a separate file, regardless of the success or failure condition.

Logical functional diagram

Without government integration



With government integration



It is carried out using REST methods, always using a secure SSL channel (port 443).

Queries must be made exclusively via a **private api-key.**

Integration with government agencies

Our product has integration methods with government agencies from different countries that allow us to validate aspects of citizen identity reliably and securely.

Touch SDK

VU Security® offers the possibility to integrate this functionality into any existing application. Our **Touch**® SDK has all the necessary methods to ensure the following features:

Fingerprint registration and reading
Fingerprint-based user registration and authentication.

Terms and Conditions Acceptance
It can consult the system about the latest version of the T&C accepted by the user.

Government check
Verifies and contrasts the fingerprint with the information provided by government agencies.

Sign up with any fingerprint
Fingerprints for the registration and authentication process are configurable.

Access logs
It saves one access log of one line for each transaction made in the system.

Asynchronous validation
Government entities report results asynchronously.

Integration API

The application consists of different methods, with functions that allow end-user management. The communication between the visible layers and the product's server is through SSL connections over TCP 443 port.

Touch® can be implemented in any environment (cellphones or self-service terminals), integrating public and private methods that allow to:

- Register and authenticate users
- Block and unblock users
- Monitor the application and the databases
- Check existing users
- Manage and store user transactions

Homologated fingerprints

A fingerprint scanner is an optical electronic device that is used to capture images of people's fingerprints.

VU Security® approved devices are:

- Lumidigm v311
- U.areU 4500

The devices must support the following technologies to ensure fingerprint storage and sharing:

- WSQ (the standard used by the FBI)
- ANSI 378
- ISO 19794-2

Fingerprints management recommendation

- Format: JPG
- Coding: image files in base64
- Encryption: AES-256

Technical information

Hardware and software requirements

Operative system	Database	App Server	Java	Devices compatibility (SDK)
Centos/Redhat 7.9 (1)	Versión PostgreSQL 9 or superior	Tomcat 9.31 or superior (1)	1.8	iOS 11 or superior
Ubuntu LTS (1)	MS SQL 2019 or superior (1) (2)	Jboss 7.1 1 or superior		Android 5 or superior
Windows Server 2019				

(1) Recommended
(2) LTS versions are recommended

Server components

Users	BS storage	Transactions per second	Cores	RAM	System storage
1 to 100.000	65 GB	8	2	4	60 GB
200.000	130 GB	16	4	8	80 GB
300.000	200 GB	36	8	16	100 GB
400.000	260 GB	64	16	32	120 GB
500.000 +	325 GB	128	32	64	140 GB

The calculations estimate habitual instances of the product. We suggest using it with the same characteristics as the ones presented for high availability configurations.

Support

Support level

NEW

VU will provide **level 3 support**.

Support includes a set of technologies and rights to help the customer maximize the investment made in VU licenses.

To contact VU Support, please send an email to: customer.support@vusecurity.com

As soon as your email is received, you will be automatically assigned a case and you will receive all the news related to your case in the same email thread.

If you want to add recipients, put them on a copy. Put Subject: [Name of the client] [Criticality] [Title of the problem].

Support cases are dealt with from **Monday to Friday from 9 a.m. to 6 p.m.** (Argentina).

Contact

Other VU Security products

Our solutions offer a 360° experience, each contributing an essential aspect to the security strategy of both users and organizations.

Authentication Management:

- Server
- SDK
- App

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

CIAM / IAM

If you need more information or want to schedule a demo of this solution, please write to us at: sales@vusecurity.com

About VU

VU is a global cybersecurity company, specializing in identity protection and fraud prevention. It develops modular solutions, easy to integrate, and adaptable to both corporate and government environments.

To achieve this, VU uses innovative technologies based on the combination of traditional cybersecurity controls, biometrics, geolocation, artificial intelligence, machine learning, document recognition, and user behavior analysis.

More than 350 million people around the world and 130 clients in 30 countries in Latin America, Europe, and the United States use VU technology to digitize their businesses and increase the level of operations, reducing the risks of attacks and loss of information.

Its strategic alliances with Microsoft, Telefónica, IBM, BGH, Intel, Cisco, and Accenture, among other companies, help VU fulfill its mission: to build secure and frictionless experiences that improve the quality of life of citizens and organizations.

vusecurity.com