VU

Onboarding Management

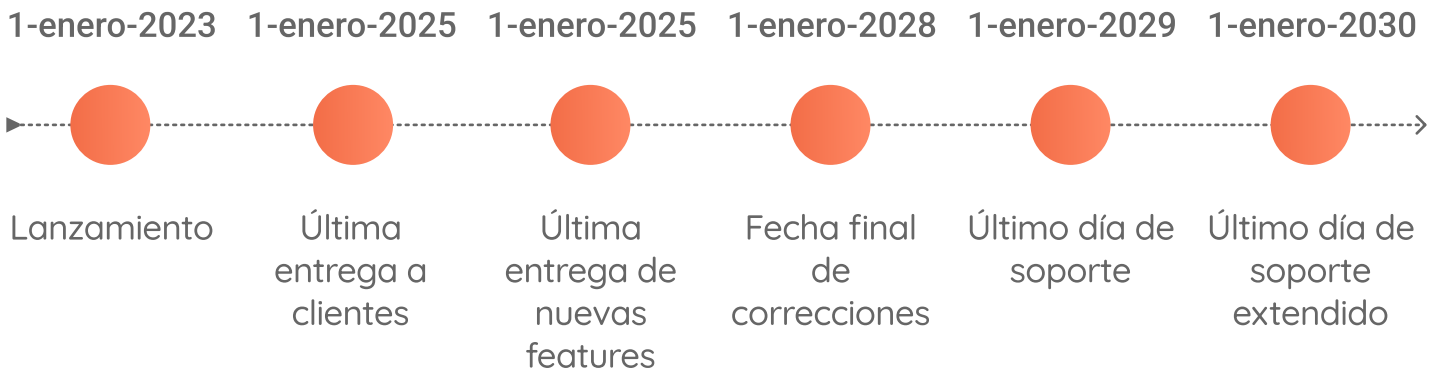
Datasheet

Versión 2.0.0

End of Life

Onboarding Management v2.0

...



¿Qué es?

Onboarding Management® se encarga de validar la identidad de las personas para prevenir la suplantación de la identidad.

Previene el uso fraudulento de la información privada de una persona, autenticando su identidad de forma remota, mediante el análisis del documento de identidad y la verificación biométrica del rostro, voz y huella dactilar.

Ofrece métodos más seguros de registro y autenticación de usuarios, ya que los datos biométricos de una persona no se pueden compartir y son menos vulnerables a los ataques de ingeniería social. Además, la singularidad biométrica de cada usuario mitiga las posibilidades de éxito en casos de fraude por ataques masivos de fuerza bruta.

La tecnología de **Onboarding Management®** simplifica la experiencia de enrolamiento y autenticación de usuarios con credenciales que no requieren ser recordadas, recuperadas o administradas.

Beneficios

• Valida la identidad de manera remota con pruebas de vida activas, pasivas y filtros de antispoofing.

• Favorece la inclusión al incrementar la conversión en usuarios en lugares remotos.

• Genera un score de identidad automático, con umbrales configurables.

• Disminuye los costos de las transacciones para el cliente.

• Cumple con los requisitos de los organismos de regulación bancaria y transaccional.

• Permite integrar prueba de vida en cualquier canal digital (ChatBot, WhatsApp, Mobile App, Web, entre otros).

• Es una solución de software completa y escalable que se puede integrar fácilmente con cualquier sistema existente.

• Gestiona el ciclo de vida de los ciudadanos durante el proceso de transformación digital.

Solución modular

Onboarding Management® es personalizable y modular, para que cada cliente seleccione las funcionalidades que quiere incorporar en cada etapa del proceso de enrolamiento de sus clientes, adaptándose a cada modelo de negocio.

Cuenta con dos módulos principales: **ID + Face®**. Dichos módulos conforman la versión estándar del producto, que además puede complementarse con los módulos Voice® y Touch®, según el tipo de onboarding que se quiera implementar.

Módulos

ID + Face® autentica la identidad de las personas de manera remota, a través del análisis del **documento de identidad y la biometría facial.**

Voice® autentica la identidad de las personas de manera remota, a través de la identificación de la **voz.**

Touch® autentica la identidad de las personas de manera remota, a través del **reconocimiento de las huellas dactilares.**

VU

ID + Face

Onboarding Management

Datasheet

Versión 2.0.0

¿Qué es?

Los módulos **ID+Face**® son los componentes principales de **Onboarding Management**® y permiten autenticar de forma remota la identidad de las personas al leer sus identificaciones y tomar algunas selfies.

Brinda la capacidad de gestionar la identidad de las personas de forma segura, escalable y de fácil mantenimiento, además de ejecutarse en cualquier entorno y a través de cualquier canal seleccionado (ChatBot, WhatsApp, aplicación móvil, Web, entre otros).

Ofrece opciones flexibles de enrolamiento y autenticación de usuarios que cumplen con los parámetros de seguridad establecidos por diferentes países al tiempo que brinda una experiencia de usuario optimizada y sin fricciones.

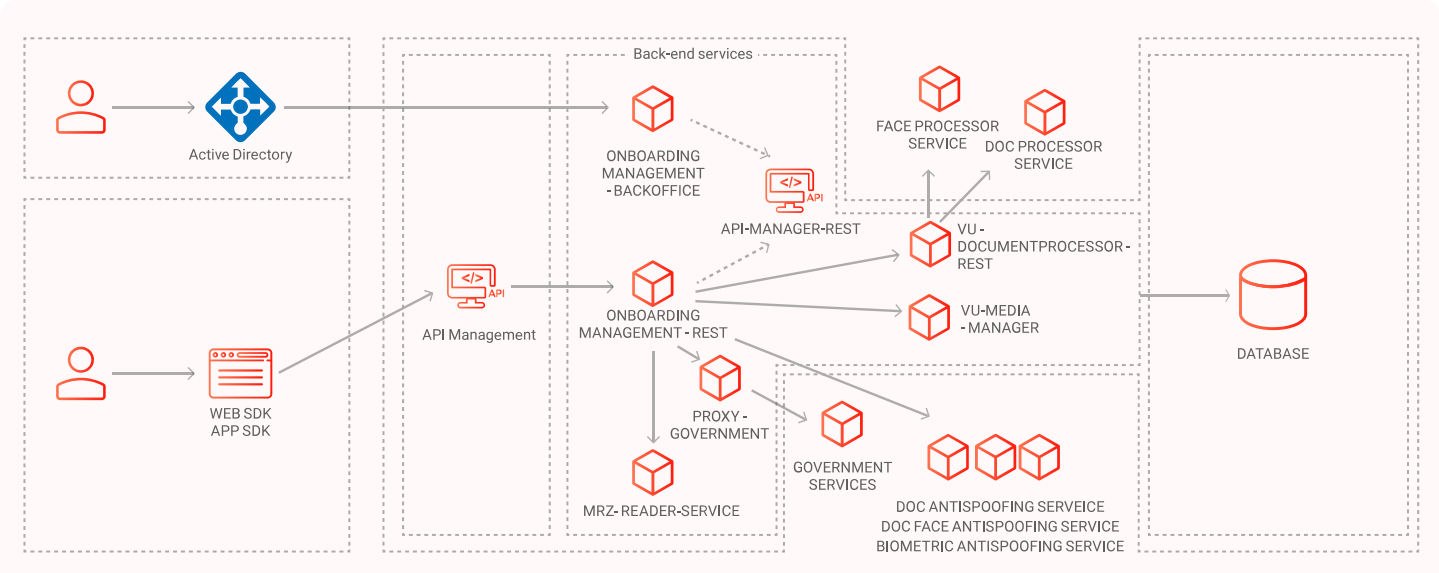
Beneficios

- Se puede utilizar en cualquier dispositivo que tenga cámara habilitada.
- Es personalizable y modular, lo cual permite a cada cliente seleccionar qué funcionalidades quiere incorporar en cada etapa del proceso, adaptándose a cada modelo de negocio.
- Realiza procesos de autenticación de usuarios evaluando los rasgos únicos de la cara: distancias, profundidad, forma, colores y capas de piel, entre otros.
- Las funcionalidades se pueden incorporar a aplicaciones existentes sin necesidad de crear una nueva.
- Detección de vida para verificar que el rostro capturado corresponde al de una persona viva mediante la ejecución dinámica de una serie de gestos guiados frente a la cámara del dispositivo.
- Ofrece distintas opciones para integrarse a aplicaciones, portales web y chatbots.

Casos de uso más destacados

- Alta remota y segura de cuentas bancarias y emisión de tarjetas de crédito.
- Check-in en hoteles y aerolíneas.
- Prevención de enrolamiento con documentos de identidad falsificados.
- Validación de procesos de votación y de toma de decisiones nominadas.
- Registro de ciudadanos y usuarios.
- Pago de transacciones.
- Desbloqueo de cuentas de homebanking.
- Identificación y enrolamiento de pacientes.

Diagrama lógico de funcionamiento



Integración con organismos gubernamentales

Nuestro producto tiene métodos de integración con organismos gubernamentales que permiten la validación de aspectos de la identidad de los ciudadanos de manera probada en distintos países.

Foco en la experiencia del usuario

En **VU Security®** sabemos que brindar experiencias simples, intuitivas y seguras permite mejorar la reputación de las instituciones y aumentar la percepción de confianza por parte de los ciudadanos hacia los organismos con los que debe interactuar. Por eso nuestro foco está puesto en analizar constantemente la experiencia de los usuarios, proponiendo nuevas funcionalidades y diseñando soluciones a medida de sus necesidades.

Onboarding más flexible

El proceso de onboarding se puede realizar con cualquier documento, configurando los datos a extraer del mismo (OCR, MRZ y PDF417) y definiendo los flujos de validación necesarios para cada caso.

• Con plantilla

Brinda la posibilidad de realizar el proceso de *onboarding* con diferente tipos de documentos utilizando una serie de plantillas previamente desarrolladas e integradas en el *document processor**.

• Sin plantilla

Brinda la posibilidad de realizar el proceso de *onboarding* con cualquier tipo de documento, independientemente de que tenga o no una plantilla ya integrada.

Opciones de interfaz de usuario
La solución ofrece distintas opciones para integrarse a aplicaciones, portales web y chatbots.

- Mobile SDK
- Web ID
- Message ID
- API

***Document processor**: servicio que procesa el DNI del usuario y extrae la información necesaria para validar su legitimidad.

SDK de ID+Face

VU Security® ofrece la posibilidad de integrar esta funcionalidad a sus aplicaciones existentes. Para ello, se ofrece el SDK de **ID+Face®**, que dispone de todos los métodos necesarios para su funcionamiento:

Lectura de MRZ
Coteja automáticamente los datos del documento.

Extracción de datos por OCR
Verifica y extrae datos de cualquier ID, DNI o tarjeta de crédito con OCR.

Lectura del código de barra
Escanea y decodifica la información almacenada en el código de barras del documento.

Captura del frente y dorso del documento
Obtiene y compara el frente y el dorso del documento para una verificación más precisa.

Detección de vida y selfie
Previene el robo de identidad al reconocer la presencia de la persona frente a la cámara.

Antispoofing
Compara el rostro de la persona con las fotos del documento para ver si hay alguna inconsistencia.

Normalizador de documento
Reencuadra la imagen del documento para un mejor procesamiento y verifica la presencia de la fotografía y el código de barras.

Identificación del tipo de documento
A través de una IA, reconoce el tipo de documento (con o sin plantilla) y detecta cualquier signo de falsificación.

Chequeo gubernamental
Verifica y contrasta la información del documento con los organismos gubernamentales.

Geolocalización del dispositivo
Reconoce operaciones inusuales que puedan implicar casos de robo de identidad.

El SDK se entrega con un conjunto de pantallas de muestra y funciones que permiten diseñar una experiencia de usuario personalizada. Las mismas reproducen las condiciones necesarias para conservar la seguridad e integridad del producto, así como facilitar el traslado al escenario de implementación real.

Integración del SDK

	Tecnología	Entrega
Android	Java	SDK + Ejemplo
iOS	Swift	SDK + Ejemplo
Web	Javascript	SDK + Ejemplo
Híbrido Cordova, Ionic, React Native, Flutter	Javascript, Dart y TypeScript Hacen uso de SDK Nativos	SDK + Ejemplo

API de integración

Es posible implementarlo en cualquier entorno tecnológico porque es multiplataforma y proporciona una amplia capacidad de integración.

La aplicación consta de diferentes métodos, identificados con funciones que permiten la gestión de usuarios finales. La comunicación entre las capas visibles y el servidor del producto se realiza mediante conexiones SSL a través del puerto TCP 443.

Está diseñado para integrarse con cualquier plataforma, independientemente del idioma utilizado, a través de servicios web (POST/GET) publicados por **ID+Face®**.

Los métodos disponibles permiten:

- Registro y autenticación de usuarios
- Bloqueo/Desbloqueo de usuarios
- Eliminación de usuarios
- Gestión y almacenamiento de las operaciones del usuario

Legajo digital NUEVO

Genera un legajo digital del cliente que incluye todo el ciclo de vida, la información de todas las operaciones realizadas con éxito y las seflies, sin necesidad de utilizar ningún software intermediario.

API para la gestión manual de casos NUEVO

Produce un índice paginado vía API REST que contiene todas las operaciones del usuario, sus estados, las diferentes puntuaciones obtenidas y qué elementos del documento se leyeron o no correctamente, con posibilidad de integrarlo a cualquier herramienta interna.

Motor de detección y verificación de rostros NUEVO

VU Face Engine® compara los rostros dentro de las imágenes capturadas para verificar la identidad del usuario con un alto grado de precisión. Dado que fue desarrollado por VU, se integra de manera más orgánica con sus productos y le permite realizar las tareas de detección, recorte y alineación de rostros sin necesidad de licenciar otros motores.

Onboarding asincrónico NUEVO

Envía notificaciones cada vez que una operación cambia de estado, independientemente de las interrupciones del proceso, gracias a la incorporación de un WebHook entre los diferentes eventos.

Se realiza mediante métodos REST, siempre utilizando un canal seguro SSL (puerto 443).

Las consultas deben realizarse exclusivamente a través de una **api-key privada**.

Recomendación de manejo de imágenes

- Formato: JPG
- Tamaño mínimo: 2 a 5 megapíxeles
- Resolución mínima: 600 x 720 píxeles

Información técnica

Requisitos y compatibilidad de hardware y software

Sistema operativo	Base de datos	App Server	Java	Compatibilidad dispositivos (SDK)
Centos/Redhat 7.9 (*)	Versión PostgreSQL 9 o superior	Tomcat 9.31 o superior (*)	11+	iOS 11 o superior
Ubuntu LTS (*)	MS SQL 2019 o superior (*) (**)	Jboss 7.11 o superior		Android 5 o superior
Windows Server 2019	MySQL 5.7			

* Recomendado.

** Provisto en los paquetes de instalación.

Componentes de servidor

Usuarios	Transacciones por segundo	Cores	RAM	Almacenamiento	Almacenamiento mensual estimado
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	Consultar con nuestro equipo				

Los cálculos son estimados de acuerdo con instancias habituales del producto. Para configuraciones de alta disponibilidad, se sugiere utilizar instancias de iguales características a las presentadas.

Soporte

Nivel de soporte

NUEVO

VU proveerá de soporte nivel 3.

El soporte provee un conjunto de tecnologías y derechos que tiene el cliente para ayudarlo a potenciar al máximo su inversión realizada en las licencias de VU.

Para contactarse con VU Support, enviar un correo a: customer.support@vusecurity.com

A partir de la recepción de su correo, se le asignará un caso de manera automática y recibirá todas las novedades relacionadas con su caso en el mismo hilo de correos.

En caso de querer agregar destinatarios, ponerlos en copia. Colocar en Asunto: [Nombre del cliente] [Criticidad] [Título del problema].

Los casos de soporte se tratan de **lunes a viernes de 9 a 18hs** (Argentina)

Contactos

Otros productos de VU Security

Nuestras soluciones ofrecen una experiencia 360°, cada una aportando un aspecto fundamental a la estrategia de seguridad tanto de usuarios como de organizaciones.

Authentication Management:

- Server
- SDK
- App

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

CIAM / IAM

Si necesitas más información o quieres agendar una demo de esta solución, por favor escríbenos a: sales@vusecurity.com

Voice

Onboarding Management

Datasheet

Versión 2.0.0

¿Qué es?

Voice® es un módulo de **Onboarding Management**® que permite identificar personas a través de las características únicas de cada voz, tales como tono, cadencia y volumen.

Una vez implementado e integrado con el sistema de la empresa responsable de buscar usuarios, **Voice**® genera infinidad de frases aleatorias que el usuario utilizará para registrarse.

Tomando como referencia datos dinámicos de la plataforma (tales como fecha, nombre de usuario, ID, número de transacciones), **Voice**® genera una frase única que el usuario deberá repetir en voz alta y de forma natural para poder autenticar la transacción (por ejemplo: "VU Security® es un proveedor de soluciones de seguridad de la información").

La autenticación puede darse por vía telefónica, vía internet, WhatsApp o bien, presencial en una terminal de auto-consulta.

Beneficios

- Es difícil de falsificar y, en general, más conveniente ya que no requiere recordar contraseñas complejas.
- Crea un Voiceprint (huella de voz) único teniendo en cuenta los patrones individuales de la voz del usuario.
- Garantiza que la persona que accede a un sistema o servicio es quien dice ser, está viva y cuenta con los medios hábiles para identificarse.
- No requiere compartir información personal o el número de tarjeta de crédito para verificar la identidad.
- Permite elegir una frase de identificación única repitiéndola de varias formas a fin de reconocer ese patrón de voz.
- Crea una experiencia de usuario más flexible y conversacional, lo que facilita el flujo y reduce el tiempo que lleva verificar la identidad.

Casos de uso más destacados

- Reemplazo de otros factores biométricos para la autenticación de identidades.
- Facilidad de registro en aplicaciones web o móbiles para personas mayores.
- Registo e ingreso en aplicaciones web o móbiles para personas no videntes.
- Prueba de fe de vida desde lugares remotos.
- Reemplazo de validación telefónica de tarjetas de crédito.

Proceso de registro y autenticación

Enrolamiento del usuario

- El proceso de enrolamiento solicita al usuario ingresar de 1 a 10 audios para generar su contraseña (palabra o frase clave), la cual puede ser personalizada o definida por defecto por la configuración del sistema.
- La cantidad de audios requeridos es configurable.
- Si **Voice**® está integrado a **Server**®, este proceso también creará un usuario en ese módulo.
- El voiceprint (patrón de voz) del cliente, codificado en Base64, se genera y almacena en la base de datos.

Autenticación estática del usuario

- Cada vez que un usuario intenta acceder al sistema (dentro de la aplicación, IVR, etc.), se le solicita que repita en voz alta la frase de contraseña ingresada durante su enrolamiento para autenticar la transacción.
- La palabra ingresada se compara con la huella de voz del usuario almacenada en la base de datos.
- API Voice devuelve un valor que representa el porcentaje de similitud entre ambos audios.
- El porcentaje requerido para una autenticación exitosa es configurable y puede estar entre 0 y 1, donde 1 es 100%.
- Si las características biométricas de ambos audios alcanzan o superan el porcentaje de similitud requerido, se autentica la identidad del usuario. Si no lo pasan, es rechazado.

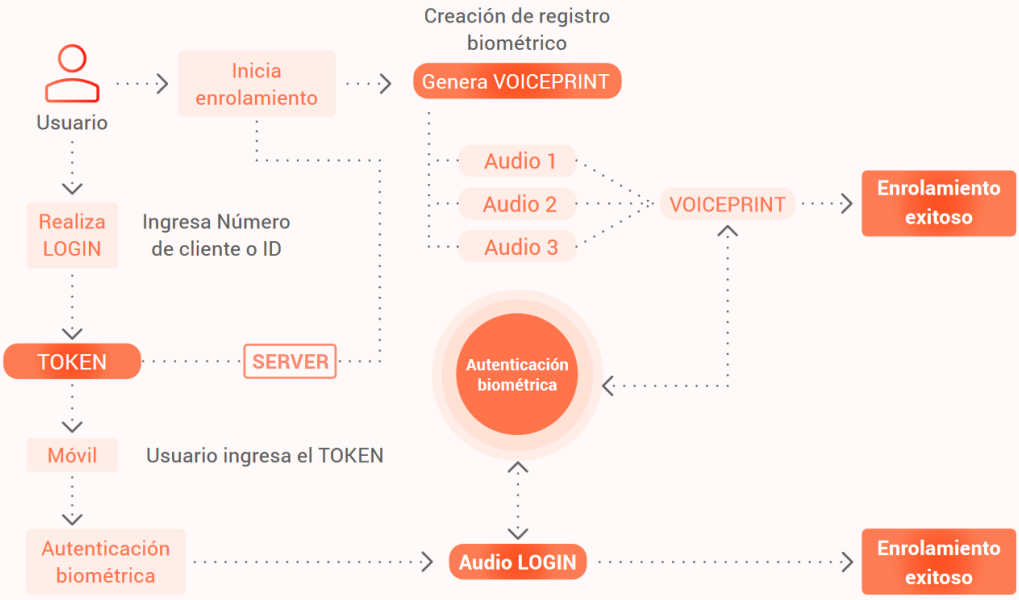
Autenticación del usuario por desafío

- Cada vez que un usuario intenta acceder al sistema (dentro de la aplicación, IVR, etc.), se le solicita que ingrese un grupo de palabras aleatorias, como parte de un desafío verbal.
- Las palabras ingresadas se comparan con la huella de voz del usuario almacenada en la base de datos.
- API Voice devuelve un valor que representa el porcentaje de similitud entre ambos audios.
- El porcentaje requerido para una autenticación exitosa es configurable y puede estar entre 0 y 1, donde 1 es 100%.
- Si las características biométricas de ambos audios alcanzan o superan el porcentaje de similitud requerido, se autentica la identidad del usuario. Si no lo pasan, es rechazado.

Diagrama lógico de funcionamiento básico

Sin integración con Server

Con integración con Server



Foco en la experiencia del usuario

En VU Security® sabemos que brindar experiencias simples, intuitivas y seguras permite mejorar la reputación de las instituciones y aumentar la percepción de confianza por parte de los ciudadanos hacia los organismos con los que debe interactuar. Por eso nuestro foco está puesto en analizar constantemente la experiencia de los usuarios, proponiendo nuevas funcionalidades y diseñando soluciones a medida de sus necesidades.

Proceso del usuario

Registro de nuevo usuario

Validación de patrón

Identificación biométrica (voz)

Devolución de resultados

SDK de Voice

VU Security® ofrece la posibilidad de integrar esta funcionalidad a sus aplicaciones existentes. Para ello, se ofrece el SDK de **Voice®**, que dispone de todos los métodos necesarios para su funcionamiento:

Passphrase configurable
Envía entre uno y diez audios a la API para registrar al usuario.

Login biométrico
Chequea la consistencia biométrica de los audios del usuario con la frase de contraseña.

Autenticación por desafío
Genera un número (configurable) de palabras o frases, a modo de desafío, que el usuario debe repetir.

Anti-spoofing
Utiliza Deep Learning para detectar posibles amenazas de robo de identidad al decir la frase de contraseña.

Actualización del Voiceprint
Actualiza el registro biométrico del usuario, agregando audios nuevos codificados en Base64.

Prueba de vida
Los algoritmos anti-spoofing identifican el uso de artefactos de fraude y determinan con precisión la vivacidad de la voz.

API de integración

La aplicación consta de diferentes métodos, identificados con funciones que permiten la gestión de usuarios finales. La comunicación entre las capas visibles y el servidor del producto se realiza mediante conexiones SSL a través del puerto TCP 443.

Es posible implementar **Voice®** en cualquier entorno (teléfono, internet, mensajería o terminales de autoconsulta), integrando métodos públicos y privados que permitirán:

- Registro y autenticación de usuarios
- Bloqueo/ Desbloqueo de usuarios
- Eliminación lógica de usuarios (soft-delete)
- Eliminación física de usuarios (hard-delete)*
- Gestión y almacenamiento de las operaciones del usuario

(*) Requiere que dicho usuario se haya **borrado de manera lógica previamente**, mediante el método softDeleteUser().

Motores

- Voice Verification: API REST interna desarrollada en Python, servida mediante Flask.
- Antispoofing: API REST interna desarrollada en Python, servida mediante Flask.
- Azure speech: API REST de Microsoft.

Recomendación de manejo de audios

- Formato: WAV. 16 Bits PCM
- Frecuencia de muestreo: 8.000 Hz para el canal telefónico y 16.000 Hz para WhatsApp.
- Duración: entre 4.500 ms y 15.000 ms
- Codificación: audios en Base64

Información técnica

Requerimientos de hardware y software

Sistema operativo	Base de datos	App Server	Java	Compatibilidad dispositivos (SDK)
Centos/Redhat 7.9 (1)	Versión PostgreSQL 9 o superior	Tomcat 9.31 o superior (1)	1.8	iOS 11 o superior
Ubuntu LTS (1)	MS SQL 2019 o superior (1) (2)	Jboss 7.11 o superior		Android 5 o superior
Windows Server 2019				

(1) Recomendado
(2) Se recomienda utilizar versiones LTS.

Componentes del servidor

Usuarios	Almacenamiento en BS	Transacciones por segundo	Cores	RAM	Almacenamiento del sistema
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

Los cálculos son estimados de acuerdo con instancias habituales del producto. Para configuraciones de alta disponibilidad, se sugiere utilizar instancias de iguales características a las presentadas.

Soporte

Nivel de soporte

NUEVO

VU proveerá de soporte nivel 3.

El soporte provee un conjunto de tecnologías y derechos que tiene el cliente para ayudarlo a potenciar al máximo su inversión realizada en las licencias de VU.

Para contactarse con VU Support, enviar un correo a: customer.support@vusecurity.com

A partir de la recepción de su correo, se le asignará un caso de manera automática y recibirá todas las novedades relacionadas con su caso en el mismo hilo de correos.

En caso de querer agregar destinatarios, ponerlos en copia. Colocar en Asunto: [Nombre del cliente] [Criticidad] [Título del problema].

Los casos de soporte se tratan de **lunes a viernes de 9 a 18hs** (Argentina)

Contactos

Otros productos de VU Security

Nuestras soluciones ofrecen una experiencia 360°, cada una aportando un aspecto fundamental a la estrategia de seguridad tanto de usuarios como de organizaciones.

Authentication Management:

- Server
- SDK
- App

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

CIAM / IAM

Si necesitas más información o quieres agendar una demo de esta solución, por favor escríbenos a: sales@vusecurity.com

Touch

Onboarding Management

Datasheet

Versión 2.0.0

¿Qué es?

Touch® es un módulo de **Onboarding Management®** que permite autenticar la identidad de las personas de manera remota, a través del reconocimiento de cualquiera de sus huellas dactilares.

Para llevar a cabo la identificación, la persona introduce su huella dactilar mediante un dispositivo lector de huellas dactilares. La muestra se compara con la muestra presentada durante su enrolamiento y con las validaciones proporcionadas por las entidades gubernamentales. Si se encuentra una coincidencia, se autentica la identidad de la persona.

Se compone de tres diferentes métodos: enrolamiento, identificación y validación de huellas dactilares por parte de entidades gubernamentales, y puede funcionar como parte de una autenticación multifactor (MFA), facilitando la experiencia de usuario.

Beneficios

- Está diseñado para poder integrarse con cualquier otra plataforma, independientemente del idioma utilizado.
- Permite configurar la huella de qué dedo se le solicitará al usuario para aprobar el proceso de registro y autenticación.
- Ofrece métodos de inicio de sesión rápidos, fáciles y no invasivos.
- Se puede alojar en un segmento de servidor con una configuración de red local tradicional y acceder al mismo desde Internet o Intranet.
- Las entidades gubernamentales informan de manera asincrónica sobre el resultado de la operación.
- Los logs transaccionales se guardan en la base de datos.
- Está preparado para ser utilizado con Docker.

Casos de uso más destacados

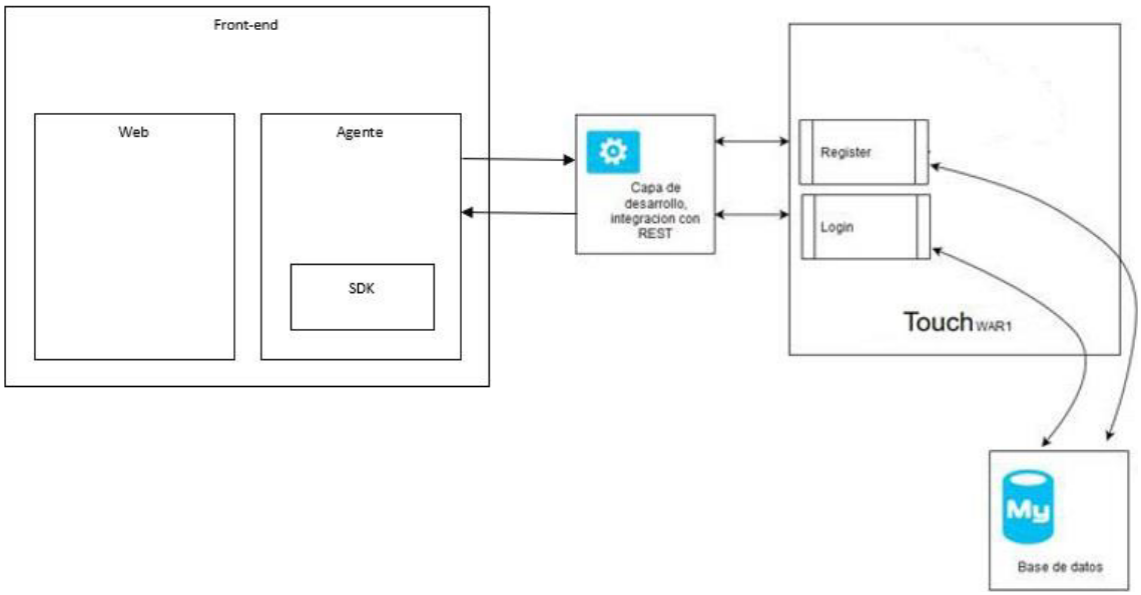
- Prevención de enrolamiento con documentos de identidad falsificados.
- Enrolamiento de ciudadanos y pasaportes biométricos.
- Control de asistencia de alumnos y empleados.
- Desbloqueo de cuentas de homebanking, o billeteras y dispositivos digitales.
- Firma de documentos digitales o confirmación de pagos virtuales.

Proceso de registro y autenticación de la huella digital

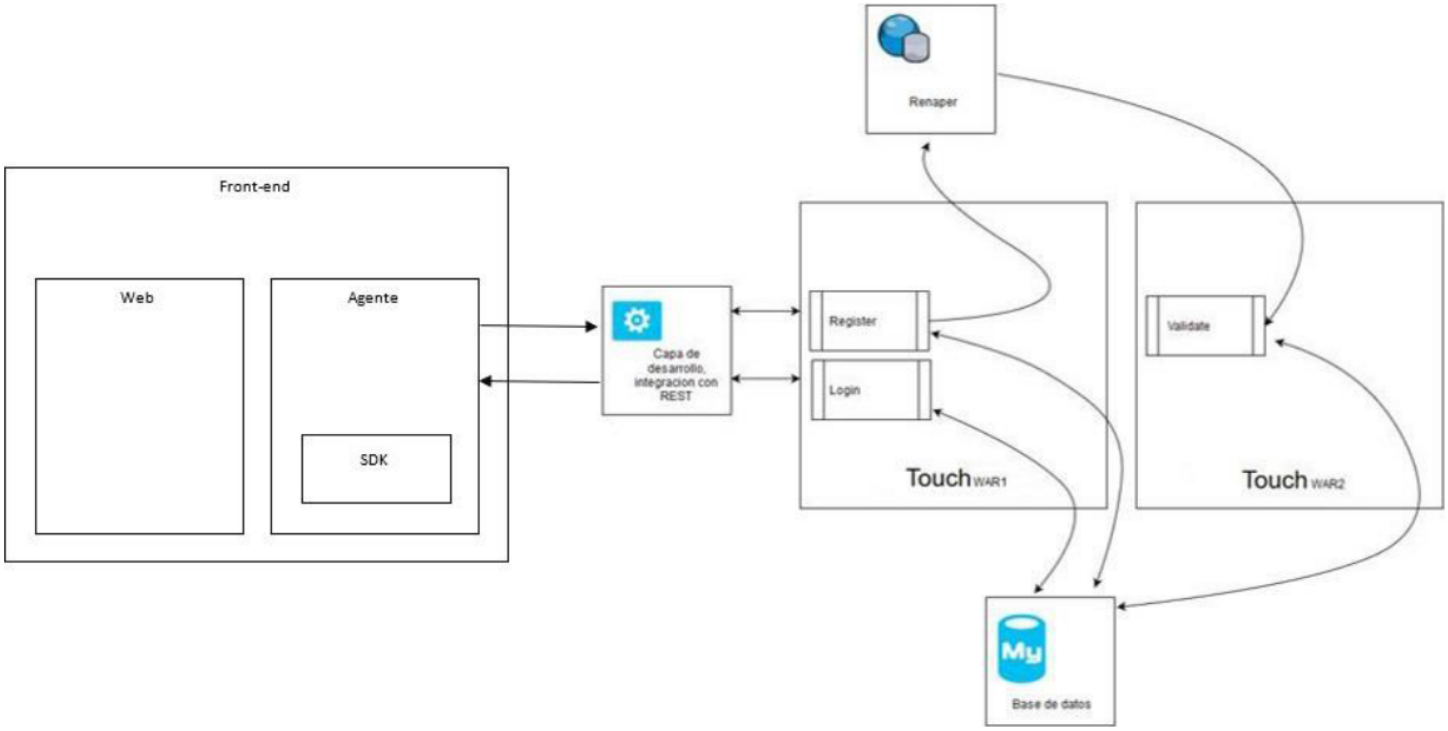
- El usuario coloca repetidamente uno de sus dedos en el sensor de huellas dactilares hasta que se registra la huella.
- El sistema comprueba si el usuario ya existe. En caso de que sea un nuevo usuario, asocia las huellas a ese usuario y las almacena en la base de datos.
- Si el usuario ya está en el sistema, verifica si la huella coincide con la almacenada en la base de datos. En caso de que las características biométricas de ambas huellas dactilares no coincidan, no se autentica la identidad del usuario.
- Asíncronamente, realiza una validación con las entidades gubernamentales correspondientes, para definir si la operación se aprueba o no.
- Se crea un registro de la operación en un archivo separado, independientemente de la condición de éxito o fracaso.

Diagrama lógico de funcionamiento

Sin integración gubernamental



Con integración gubernamental



Se realiza mediante métodos REST, siempre utilizando un canal seguro SSL (puerto 443).

Las consultas deben realizarse exclusivamente a través de una **api-key privada**.

Integración con organismos gubernamentales

Nuestro producto cuenta con métodos de integración con agencias gubernamentales de diferentes países que nos permiten validar aspectos de la identidad de los ciudadanos de manera confiable y segura.

SDK de Touch

VU Security® ofrece la posibilidad de integrar esta funcionalidad a sus aplicaciones existentes. Para ello, el **SDK** de **Touch®** dispone de todos los métodos necesarios para garantizar las siguientes funciones:

Registro y lectura de huellas dactilares
Registro y autenticación de usuarios basados en huellas dactilares.

Aceptación de Términos y Condiciones
Puede consultar al sistema sobre la última versión de los T&C aceptados por el usuario.

Chequeo gubernamental
Verifica y contrasta la huella dactilar con la información proporcionada por los organismos gubernamentales.

Enrolamiento con cualquier huella dactilar
Las huellas digitales para el proceso de enrolamiento y autenticación son configurables.

Obtención de logs de acceso
Guarda un log de acceso de una línea por cada transacción hecha en el sistema.

Validación asincrónica
Las entidades gubernamentales reportan el resultado de manera asincrónica.

API de integración

La aplicación consta de diferentes métodos, identificados con funciones que permiten la gestión de usuarios finales. La comunicación entre las capas visibles y el servidor del producto se realiza mediante conexiones SSL a través del puerto TCP 443.

Es posible implementar **Touch®** en cualquier entorno (teléfonos móviles o terminales de autoconsulta), integrando métodos públicos y privados que permitirán:

- Registro y autenticación de usuarios
- Bloqueo/ Desbloqueo de usuarios
- Consulta de usuario existente
- Monitoreo de la aplicación y la base de datos
- Gestión y almacenamiento de las operaciones del usuario

Huelleros homologados

El escáner de huellas dactilares o huellero es un dispositivo electrónico óptico que se utiliza para capturar imágenes de huellas dactilares de las personas.

Los equipos homologados por **VU Security**® son:

- Lumidigm v311
- U.areU 4500

Los huelleros deben soportar las siguientes tecnologías para garantizar el intercambio y el almacenamiento de las huellas dactilares:

- WSQ (estándar utilizado por el FBI)
- ANSI 378
- ISO 19794-2

Recomendación de manejo de huellas

- Formato: JPG
- Codificación: en base64
- Encriptación: AES-256

Información técnica

Requerimientos de hardware y software

Sistema operativo	Base de datos	App Server	Java	Compatibilidad dispositivos (SDK)
Centos/Redhat 7.9 (1)	Versión PostgreSQL 9 o superior	Tomcat 9.31 o superior (1)	1.8	iOS 11 o superior
Ubuntu LTS (1)	MS SQL 2019 o superior (1) (2)	Jboss 7.11 o superior		Android 5 o superior
Windows Server 2019				

(1) Recomendado
(2) Se recomienda utilizar versiones LTS.

Componentes de servidor

Usuarios	Almacenamiento en BS	Transacciones por segundo	Cores	RAM	Almacenamiento del sistema
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

Los cálculos son estimados de acuerdo con instancias habituales del producto. Para configuraciones de alta disponibilidad, se sugiere utilizar instancias de iguales características a las presentadas.

Soporte

Nivel de soporte

NUEVO

VU proveerá de soporte nivel 3.

El soporte provee un conjunto de tecnologías y derechos que tiene el cliente para ayudarlo a potenciar al máximo su inversión realizada en las licencias de VU.

Para contactarse con VU Support, enviar un correo a: customer.support@vusecurity.com

A partir de la recepción de su correo, se le asignará un caso de manera automática y recibirá todas las novedades relacionadas con su caso en el mismo hilo de correos.

En caso de querer agregar destinatarios, ponerlos en copia. Colocar en Asunto: [Nombre del cliente] [Criticidad] [Título del problema].

Los casos de soporte se tratan de **lunes a viernes de 9 a 18hs** (Argentina)

Contactos

Otros productos de VU Security

Nuestras soluciones ofrecen una experiencia 360°, cada una aportando un aspecto fundamental a la estrategia de seguridad tanto de usuarios como de organizaciones.

Authentication Management:

- Server
- SDK
- App

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

CIAM / IAM

Si necesitas más información o quieres agendar una demo de esta solución, por favor escríbenos a: sales@vusecurity.com

Acerca de VU

VU es una compañía global de ciberseguridad, especializada en protección de la identidad y prevención de fraude, que desarrolla soluciones modulares, fáciles de integrar y adaptables tanto al ámbito corporativo como gubernamental.

Para lograrlo, utiliza tecnologías innovadoras basadas en la combinación de controles tradicionales de ciberseguridad, biometría, geolocalización, inteligencia artificial, *machine learning*, reconocimiento de documentación y análisis del comportamiento del usuario.

Más de 350 millones de personas en todo el mundo y más de 130 clientes en 30 países de América Latina, Europa y Estados Unidos utilizan la tecnología de VU para digitalizar sus negocios y aumentar el nivel de operaciones reduciendo los riesgos de ataques y la pérdida de información.

Sus alianzas estratégicas con Microsoft, Telefónica, IBM, BGH, Intel, Cisco y Accenture, entre otras compañías, ayudan a VU a cumplir su misión: crear experiencias seguras y sin fricción que mejoren la calidad de vida de ciudadanos y organizaciones.

vusecurity.com