VU

Onboarding Management

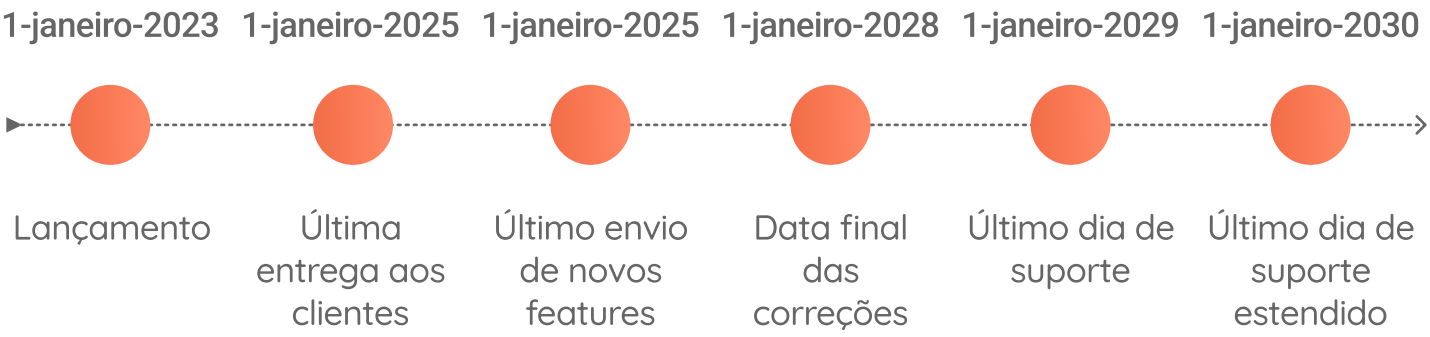
Datasheet

Versão 2.0.0

End of Life

Onboarding Management v2.0

...



O que é?

O **Onboarding Management®** é responsável por validar a identidade das pessoas para evitar o roubo de identidade.

Impede a utilização fraudulenta da informação privada de uma pessoa, autenticando a sua identidade remotamente, através da análise do documento de identidade e da verificação biométrica do rosto, voz e impressão digital.

Oferece métodos mais seguros de registro e autenticação de usuários, pois os dados biométricos de uma pessoa não podem ser compartilhados e são menos vulneráveis a ataques de engenharia social. Além disso, a singularidade biométrica de cada usuário mitiga as chances de sucesso em casos de fraude devido a ataques em massa de força bruta.

A tecnologia **Onboarding Management®** simplifica a experiência de registro e autenticação do usuário com credenciais que não precisam ser lembradas, recuperadas ou gerenciadas.

Benefícios

• Valida a identidade de forma remota com provas de vida ativas, passivas e filtros de antispoofing.

• Promove a inclusão ao aumentar a conversão de usuários em locais remotos.

• Gera um escore de identidade automático, com patamares configuráveis.

• Reduz os custos das transações para o cliente.

• Atende às exigências dos órgãos de regulação bancária e transacional.

• Permite a integração da prova de vida em qualquer canal digital (ChatBot, WhatsApp, Mobile App, Web, entre outros).

• É uma solução de software completa e escalável que pode ser facilmente integrada a qualquer sistema existente.

• Gerencia o ciclo de vida dos cidadãos durante o processo de transformação digital.

Solução modular

O **Onboarding Management®** é personalizável e modular, para que cada cliente selecione as funcionalidades que deseja incorporar em cada etapa do processo de cadastramento de seus clientes, adaptando-se a cada modelo de negócio.

Possui dois módulos principais: **ID + Face®**. Esses módulos compõem a versão padrão do produto, que também pode ser complementada com os módulos **Voice®** e **Touch®**, dependendo do tipo de onboarding que se deseja implementar.

Módulos

VU ID+Face

O **ID + Face**® autentica a identidade das pessoas de forma remota, através da análise do **documento de identidade e da biometria facial.**

VU Voice

Voice® autentica a identidade das pessoas de forma remota, por meio de **identificação da voz**.

VU Touch

O **Touch**® autentica a identidade das pessoas de forma remota, através do reconhecimento de **impressões digitais**.

VU

ID + Face

Onboarding Management

Datasheet

Versão 2.0.0

O que é?

Os módulos **ID+Face®** são os principais componentes do **Onboarding Management®** e permitem autenticar de forma remota a identidade das pessoas ao ler seus DNIs e tirar algumas selfies.

Fornece a possibilidade de gerenciar a identidade das pessoas de forma segura, escalável e de fácil manutenção, além de ser execytadi em qualquer ambiente e por qualquer canal selecionado (ChatBot, WhatsApp, aplicativo mobile, Web, entre outros).

O módulo **ID+Face®** oferece opções flexíveis de registro e autenticação de usuários que atendem aos parâmetros de segurança definidos por diferentes países, proporcionando uma experiência de usuário otimizada e sem atritos.

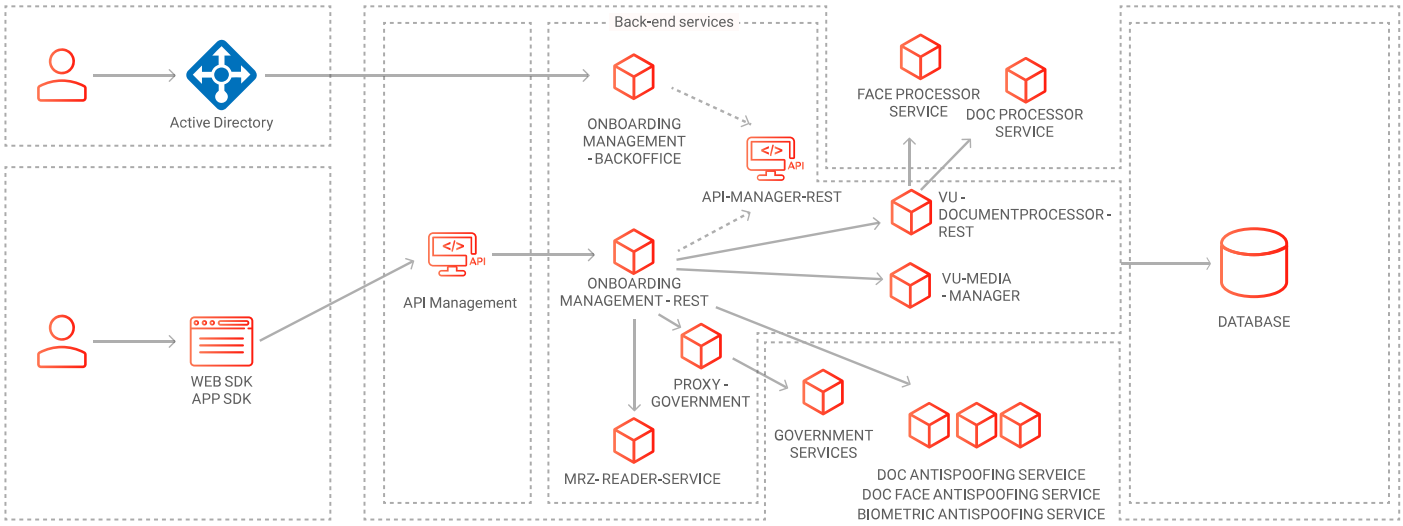
Benefícios

- Pode ser usado em qualquer dispositivo com câmera habilitada.
- É personalizável e modular, o que permite a cada cliente selecionar quais funcionalidades ele deseja incorporar em cada etapa do processo, adaptando-se a cada modelo de negócios.
- Realiza processos de autenticação de usuários avaliando as características únicas do rosto: distâncias, profundidade, formato, cores e camadas de pele, entre outros.
- As funcionalidades podem ser incorporadas em aplicativos existentes sem a necessidade de criar um novo.
- Detecção de vida para verificar se o rosto capturado corresponde ao de uma pessoa viva através da execução dinâmica de uma série de gestos guiados em frente à câmera do dispositivo.
- Oferece diferentes opções de integração com aplicativos, portais web e chatbots.

Casos de uso mais destacados

- Registro remoto e seguro de contas bancárias e emissão de cartões de crédito.
- Check-in em hotéis e companhias aéreas.
- Prevenção de inscrição com documentos de identidade falsificados.
- Validação dos processos de votação e tomada de decisões nomeadas.
- Registro de cidadãos e usuários.
- Pagamento de transações.
- Desbloqueio de contas de homebanking.
- Identificação e cadastro de pacientes.

Diagrama lógico de funcionamiento



Integração com órgãos governamentais

Nosso produto possui métodos de integração com órgãos governamentais que permitem a validação de aspectos da identidade dos cidadãos de forma comprovada em diversos países.

Foco na experiência do usuário

Na **VU Security**® sabemos que proporcionar experiências simples, intuitivas e seguras melhora a reputação das instituições e aumenta a percepção de confiança dos cidadãos nas organizações com as quais devem interagir. É por isso que nosso foco está em analisar constantemente a experiência do usuário, propondo novas funcionalidades e projetando soluções sob medida para suas necessidades.

Onboarding mais flexível

O processo de onboarding pode ser realizado com qualquer documento, configurando os dados a serem extraídos dele (OCR, MRZ e PDF417) e definindo os fluxos de validação necessários para cada caso.

• Com modelo

Oferece a possibilidade de realizar o processo de onboarding com diferentes tipos de documentos utilizando uma série de modelos previamente desenvolvidos e integrados no *document processor**.

• Sem modelo

Oferece a possibilidade de realizar o processo de onboarding com qualquer tipo de documento, independentemente de ter ou não um modelo já integrado.

Opções de interface do usuário
A solução oferece diferentes opções de integração com aplicativos, portais web e chatbots.

• Mobile SDK
• Web ID
• Message ID
• API

***Document processor**: serviço que processa o DNI do usuário e extrai as informações necessárias para validar sua legitimidade.

SDK de ID+Face

VU Security® oferece a possibilidade de integrar esta funcionalidade em seus aplicativos existentes. Para isso, é oferecido o **ID+Face®** SDK, que possui todos os métodos necessários para seu funcionamento:

Leitura de MRZ
Verifica automaticamente os dados do documento.

Extração de dados por meio de OCR
Verifica e extrai dados de qualquer ID, DNI ou cartão de crédito com OCR.

Leitura do código de barras
Digitaliza e decodifica as informações armazenadas no código de barras do documento.

Captura de frente e verso do documento
Obtém e compara a frente e o verso do documento para uma verificação mais precisa.

Detecção de vida e selfie
Evita roubo de identidade reconhecendo a presença da pessoa em frente à câmera.

Antispoofing
Evita roubo de identidade reconhecendo a presença da pessoa em frente à câmera.

Normalizador de documentos
Reenquadra a imagem do documento para melhor processamento e verifica a presença da foto e do código de barras.

Identificação do tipo de documento
Por meio de IA, reconhece o tipo de documento (com ou sem modelo) e detecta qualquer indício de falsificação.

Checagem governamental
Verifica e compara as informações do documento com os órgãos governamentais.

Geolocalização do dispositivo
Reconhece operações incomuns que podem envolver casos de roubo de identidade.

O SDK é fornecido com um conjunto de telas e recursos de amostra e funções que permitem criar uma experiência de usuário personalizada. Elas reproduzem as condições necessárias para preservar a segurança e integridade do produto, bem como para facilitar a transferência para o cenário de implementação real.

Integração do SDK

	Tecnologia	Entrega
Android	Java	SDK + Exemplo
iOS	Swift	SDK + Exemplo
Web	Javascript	SDK + Exemplo
Hybrid Cordova, Ionic, React Native, Flutter	Javascript, Dart & TypeScript Eles usam o SDK Nativo	SDK + Exemplo

API de integração

É possível implementá-lo em qualquer ambiente tecnológico porque é multiplataforma e oferece uma ampla capacidade de integração.

O aplicativo abrange diferentes métodos, identificados com funções que permitem a gestão dos usuários finais. A comunicação entre as camadas visíveis e o servidor do produto é feita por meio de conexões SSL pela porta TCP 443.

Está desenhado para se integrar com qualquer plataforma, independentemente do idioma utilizado, através de serviços web (POST/GET) publicados pelo **ID+Face®**.

Os métodos disponíveis permitem:

- Registro e autenticação de usuários
- Bloqueio/desbloqueio de usuários
- Monitoramento do aplicativo e banco de dados
- Exclusão de usuários
- Gerenciamento e armazenamento de operações do usuário

Histórico digital NOVO

Gera um arquivo (histórico) digital do cliente que inclui todo o ciclo de vida, a informação de todas as operações realizadas com sucesso e as selfies, sem necessidade de recorrer a qualquer software intermediário.

API para gerenciamento manual de casos NOVO

Produz um índice paginado via API REST que contém todas as operações do usuário, seu status, as diferentes pontuações obtidas e quais elementos do documento foram lidos corretamente ou não, com possibilidade de integrá-lo com qualquer ferramenta interna.

Motor de detección y verificación de rostros NOVO

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 assíncrono NOVO

Envia notificações sempre que uma operação muda de estado, independentemente das interrupções do processo, graças à incorporação de um WebHook entre os diferentes eventos.

Realiza-se usando métodos REST, sempre usando um canal SSL seguro (porta 443).

As consultas devem ser feitas exclusivamente por meio de uma **API key privada**.

Recomendação de manejo de imagens

- Formato: JPG
- Tamanho mínimo: 2 a 5 megapixels
- Resolução mínima: 600 x 720 pixels

Informação técnica

Requisitos e compatibilidade de hardware e software

Sistema operativo	Base de dados	App Server	Java	Compatibilidade com dispositivos (SDK)
Centos/Redhat 7.9 (1)	Versión PostgreSQL 9 ou superior	Tomcat 9.31 ou superior (1)	11+	iOS 11 ou superior
Ubuntu LTS (1)	MS SQL 2019 ou superior (1) (2)	Jboss 7.11 ou superior		Android 5 ou superior
Windows Server 2019	MySQL 5.7			

(1) Recomendado

(2) Fornecido nos pacotes de instalação.

Componentes do servidor

Usuários	Transações por segundos	Cores	RAM	Armazenamento	Armazenamento mensal 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	Consulte nossa equipe				

Os cálculos são estimados de acordo com instâncias usuais do produto. Para configurações de alta disponibilidade, sugere-se o uso de instâncias com as mesmas características das apresentadas.

Suporte

Nível de suporte NOVO

A VU fornecerá **suporte de nível 3**.

O suporte fornece um conjunto de tecnologias e direitos que o cliente tem para ajudá-lo a maximizar seu investimento em licenças da VU.

Para entrar em contato com o VU Support, enviar um e-mail para: customer.support@vusecurity.com

Assim que seu e-mail for recebido, um caso será atribuído a você automaticamente e receberá todas as novidades relacionadas ao seu caso no mesmo thread de e-mail.

Se quiser adicionar destinatários, colocá-los em cópia. Colocar no Assunto: [Nome do cliente] [Criticidade] [Título do problema].

Os casos de suporte são atendidos de **segundas a sextas das 9h às 18h** (Argentina).

Contatos

Outros produtos da VU Security

Nossas soluções oferecem uma experiência 360°, cada uma contribuindo com um aspecto fundamental para a estratégia de segurança de usuários e organizações.

Authentication Management:

- Server
- SDK
- App

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

CIAM / IAM

Se você precisar de mais informações ou quiser agendar uma demonstração desta solução, escreva para: sales@vusecurity.com

Voice

Onboarding Management

Datasheet

Versão 2.0.0

O que é?

Voice® é um módulo **Onboarding Management®** que permite identificar pessoas através das características únicas de cada voz, como tom, cadência e volume.

Uma vez implementado e integrado ao sistema da empresa responsável pela busca de usuários, o **Voice®** gera inúmeras frases aleatórias que o usuário utilizará para se registrar.

Tomando como referência dados dinâmicos da plataforma (como data, nome de usuário, ID, número de transações), o Voice® gera uma frase única que o usuário deve repetir em voz alta e natural para autenticar a transação (por exemplo: "VU Security é um fornecedor de soluções de segurança da informação").

A autenticação pode ser feita por telefone, via internet, WhatsApp ou pessoalmente em um terminal de autoconsulta.

Benefícios

- Difícil de falsificar e geralmente mais conveniente, pois não requer a memorização de senhas complexas.
- Cria um Voiceprint (impressão de voz) única com base nos padrões de voz individuais do usuário.
- Garante que a pessoa que acessa um sistema ou serviço é quem afirma ser, está viva e tem meios para se identificar.
- Não requer o compartilhamento de informações pessoais ou número de cartão de crédito para verificar a identidade.
- Permite escolher uma frase de identificação única, repetindo-a de várias maneiras para reconhecer esse padrão de voz.
- Cria uma experiência de usuário mais flexível e conversacional, facilitando o fluxo e reduzindo o tempo necessário para verificar a identidade.

Casos de uso mais destacados

- Substituição de outros fatores biométricos para autenticação de identidades.
- Facilidade de registro nos aplicativos web ou mobile para idosos.
- Registro e entrada nos aplicativos web ou mobile para pessoas cegas.
- Prova de vida de locais remotos.
- Substituição de validação telefônica de cartões de crédito.

Processo de registro e autenticação

Cadastro do usuário

- O processo de cadastro solicita que o usuário insira de 1 a 10 áudios para gerar sua senha (palavra ou frase chave), que pode ser personalizada ou definida por padrão pela configuração do sistema.
- A quantidade de áudios necessários é configurável.
- Se o **Voice**®estiver integrado ao **ID+Face**®, este processo também criará um usuário nesse módulo.
- O voiceprint (padrão de voz) do cliente, codificado em Base64, é gerado e armazenado no banco de dados.

Autenticação estátoca do usuário

- Toda vez que um usuário tenta acessar o sistema (dentro do aplicativo, IVR, etc.), é solicitado que ele repita em voz alta a frase da senha inserida durante o registro para autenticar a transação.
- A palavra inserida é comparada com a impressão de voz do usuário armazenada no banco de dados.
- O API Voice retorna um valor que representa a porcentagem de similaridade entre os dois áudios.
- A porcentagem necessária para uma autenticação bem-sucedida é configurável e pode estar entre 0 e 1, onde 1 é 100%.
- Se as características biométricas de ambos os áudios atingirem ou excederem a porcentagem de similaridade exigida, a identidade do usuário é autenticada. Se não atingirem o valor exigido, o usuário é rejeitado.

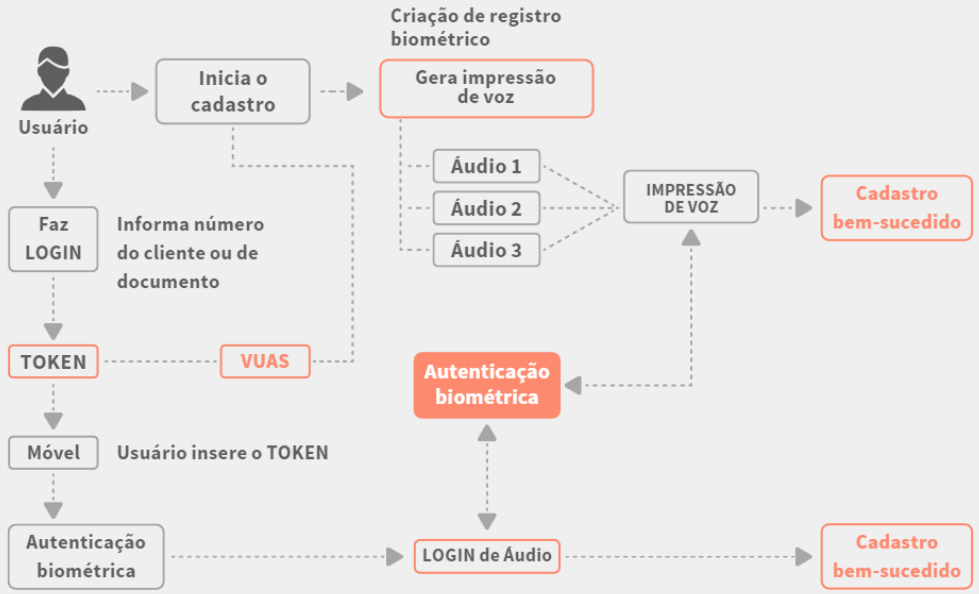
Autenticação do usuário por desafio

- Toda vez que um usuário tenta acessar o sistema (dentro do aplicativo, IVR, etc.), é solicitado que ele digite um grupo de palavras aleatórias, como parte de um desafio verbal.
- As palavras inseridas são comparadas com a impressão de voz do usuário armazenada no banco de dados.
- O API Voice retorna um valor que representa a porcentagem de similaridade entre os dois áudios.
- A porcentagem necessária para uma autenticação bem-sucedida é configurável e pode estar entre 0 e 1, onde 1 é 100%.
- Se as características biométricas de ambos os áudios atingirem ou excederem a porcentagem de similaridade exigida, a identidade do usuário é autenticada. Se não atingirem o valor exigido, o usuário é rejeitado.

Diagrama lógico de funcionamiento básico

Sem integração com Server

Com integração com Server



Foco na experiência do usuário

Na **VU Security**® sabemos que proporcionar experiências simples, intuitivas e seguras melhora a reputação das instituições e aumenta a percepção de confiança dos cidadãos nas organizações com as quais devem interagir. É por isso que nosso foco está em analisar constantemente a experiência do usuário, propondo novas funcionalidades e projetando soluções sob medida para suas necessidades.

Processo do usuário

Cadastro de novo usuário

Validação de padrão de voz

Identificação biométrica (voz)

Resultados

SDK de Voice

VU Security® oferece a possibilidade de integrar esta funcionalidade em seus aplicativos existentes. Para isso, é oferecido o **Voice**® SDK®, que possui todos os métodos necessários para seu funcionamento:

Passphrase configurável
Envia entre um e dez áudios à API para registrar o usuário.

Login biométrico
Verifica a consistência biométrica dos áudios do usuário com a frase da senha.

Autenticação por desafio
Gera um número (configurável) de palavras ou frases, como um desafio, que o usuário deve repetir.

Anti-spoofing
Usa Deep Learning para detectar possíveis ameaças de roubo de identidade ao dizer a frase da senha.

Atualização do Voiceprint
Atualiza o registro biométrico do usuário, adicionando novos áudios codificados em Base64.

Prova de vida
Os algoritmos antispoofing identificam o uso de aparelhos de fraude e determinam com precisão a vivacidade da voz.

API de integração

O aplicativo abrange diferentes métodos, identificados com funções que permitem a gestão dos usuários finais. A comunicação entre as camadas visíveis e o servidor do produto é feita por meio de conexões SSL pela porta TCP 443.

É possível implementar o **Voice**® em qualquer ambiente (telefone, internet, mensagens ou terminais de autoatendimento), integrando métodos públicos e privados que permitirão:

- Registro e autenticação de usuários
- Bloqueio/desbloqueio de usuários
- Monitoramento do aplicativo e banco de dados
- Exclusão lógica de usuários (soft-delete)
- Exclusão física de usuários (hard-delete)*
- Gerenciamento e armazenamento de operações do usuário

(*) Requer que tal usuário **tenha sido previamente deletado de maneira logica**, através do método softDeleteUser().

Motores

- Voice Verification: API REST interna desenvolvida em Python, servida mediante Flask.
- Antispoofing: API REST interna desenvolvida em Python, servida mediante Flask.
- Azure speech: API REST da Microsoft.

Recomendação de manejo de áudios

- Formato: WAV. 16 Bits PCM
- Frequência de amostragem: 8.000 Hz para o canal telefônico e 16.000 Hz para o WhatsApp.
- Duração: entre 4.500 ms e 15.000 ms
- Codificação: áudios em Base64

Informação técnica

Requisitos e compatibilidade de hardware e software

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

(1) Recomendado

(2) Fornecido nos pacotes de instalação.

Componentes do servidor

Usuários	Armazenamento BS	Transações por segundos	Cores	RAM	Armazenamento do 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

Os cálculos são estimados de acordo com instâncias usuais do produto. Para configurações de alta disponibilidade, sugere-se o uso de instâncias com as mesmas características das apresentadas.

Suporte

Nível de suporte

NOVO

A VU fornecerá **suporte de nível 3**.

O suporte fornece um conjunto de tecnologias e direitos que o cliente tem para ajudá-lo a maximizar seu investimento em licenças da VU.

Para entrar em contato com o VU Support, enviar um e-mail para: customer.support@vusecurity.com

Assim que seu e-mail for recebido, um caso será atribuído a você automaticamente e receberá todas as novidades relacionadas ao seu caso no mesmo thread de e-mail.

Se quiser adicionar destinatários, colocá-los em cópia. Colocar no Assunto: [Nome do cliente] [Criticidade] [Título do problema].

Os casos de suporte são atendidos de **segundas a sextas das 9h às 18h** (Argentina).

Contatos

Outros produtos da VU Security

Nossas soluções oferecem uma experiência 360°, cada uma contribuindo com um aspecto fundamental para a estratégia de segurança de usuários e organizações.

Authentication Management:

- Server
- SDK
- App

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

CIAM / IAM

Se você precisar de mais informações ou quiser agendar uma demonstração desta solução, escreva para: sales@vusecurity.com

Touch

Onboarding Management

Datasheet

Versão 2.0.0

O que é?

O **Touch®** ® é um módulo **Onboarding Management®** que permite autenticar a identidade das pessoas de forma remota, através do reconhecimento de qualquer uma das suas impressões digitais.

Para realizar a identificação, a pessoa insere sua impressão digital usando um dispositivo leitor de impressões digitais. A amostra é comparada com a amostra apresentada durante o cadastro e com as validações fornecidas por entidades governamentais. Se for encontrada uma correspondência, a identidade da pessoa será autenticada.

É composto por três métodos diferentes: cadastro, identificação e validação de impressões digitais por entidades governamentais, podendo funcionar como parte de uma autenticação multifator (MFA), facilitando a experiência do usuário.

Benefícios

- Está desenhado para poder integrar-se com qualquer outra plataforma, independentemente do idioma utilizado.
- Permite configurar a impressão digital de qual dedo será solicitada ao usuário para aprovar o processo de registro e autenticação.
- Oferece métodos de login rápidos, fáceis e não invasivos.
- Pode ser hospedado em um segmento de servidor com configuração de rede local tradicional e acessado pela Internet ou Intranet.
- As entidades governamentais informam de forma assíncrona o resultado da operação.
- Os logs transacionais são salvos no banco de dados.
- Está pronto para ser usado com o Docker.

Casos de uso mais destacados

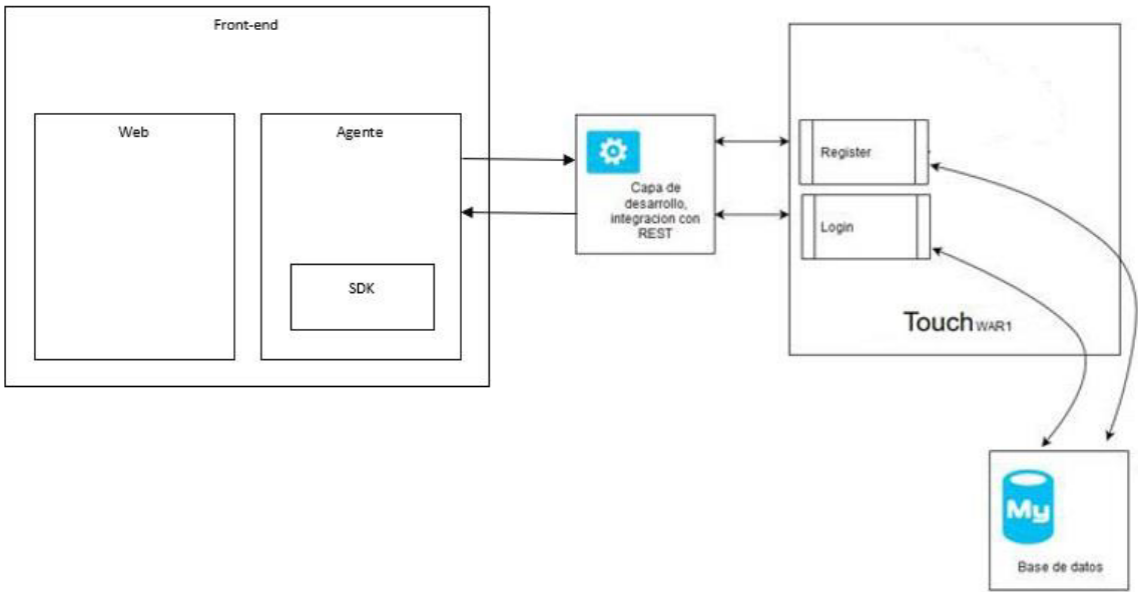
- Prevenção de inscrição com documentos de identidade falsificados.
- Inscrição de cidadãos e passaportes biométricos.
- Controle de assiduidade de alunos e funcionários.
- Desbloqueio de contas de homebanking ou carteiras e dispositivos digitais.
- Assinatura de documentos digitais ou confirmação de pagamentos virtuais.

Processo de registro e autenticação de impressão digital

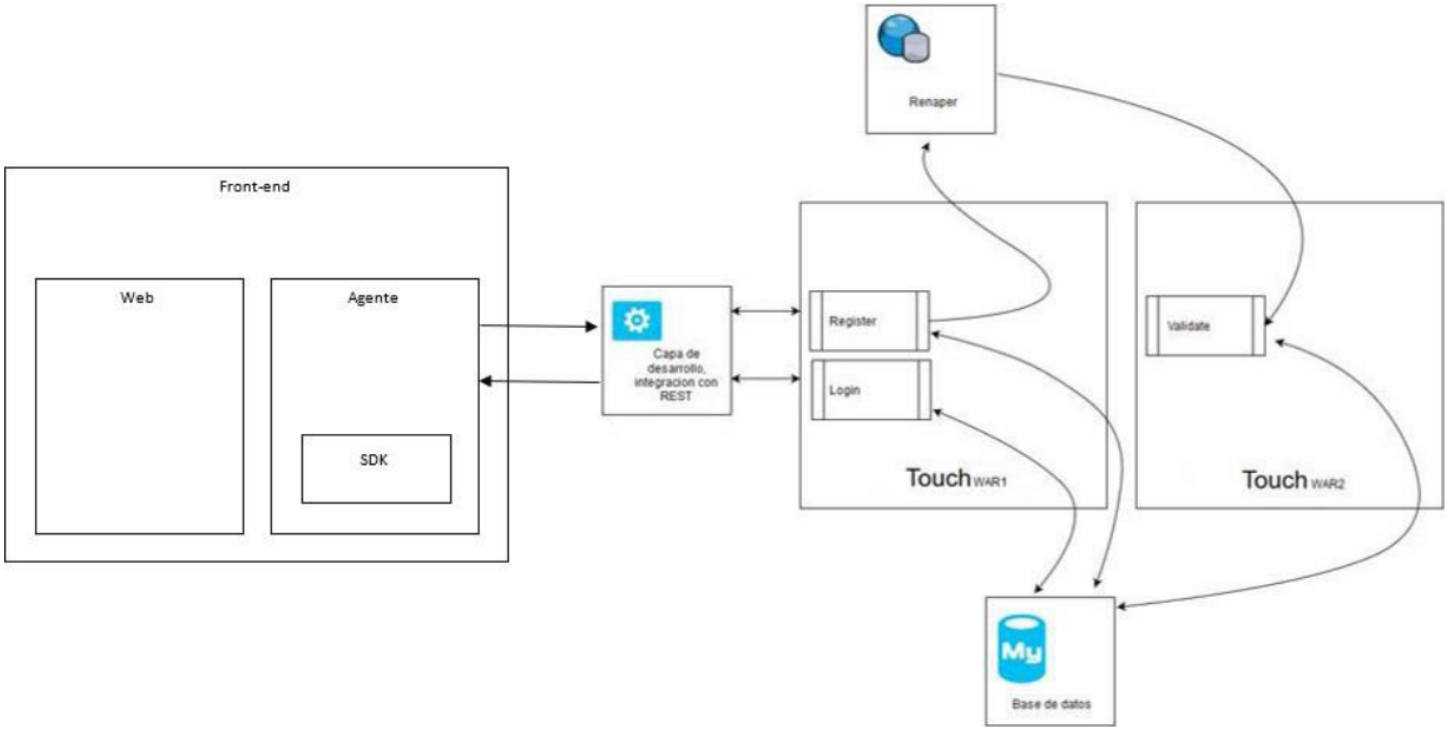
- O usuário coloca repetidamente um de seus dedos no sensor de impressão digital até que a impressão digital seja registrada.
- O sistema verifica se o usuário já existe. Caso seja um novo usuário, ele associa as impressões digitais a esse usuário e as armazena no banco de dados.
- Se o usuário já estiver no sistema, verifica se a impressão digital corresponde à armazenada no banco de dados. Caso as características biométricas de ambas as impressões digitais não coincidam, a identidade do usuário não é autenticada.
- De forma assíncrona, realiza uma validação junto aos órgãos governamentais correspondentes, para definir se a operação é aprovada ou não.
- Um registro da operação é criado em um arquivo separado, independentemente da condição de sucesso ou falha.

Diagrama lógico de funcionamiento

Sem integração governamental



Com integração governamental



Realiza-se usando métodos REST, sempre usando um canal SSL seguro (porta 443).

As consultas devem ser feitas exclusivamente por meio de uma **API key privada**.

Integração com órgãos governamentais

Nosso produto possui métodos de integração com órgãos governamentais de diversos países que nos permitem validar aspectos da identidade dos cidadãos de forma confiável e segura.

SDK de Touch

VU Security® oferece a possibilidade de integrar esta funcionalidade em seus aplicativos existentes. Para isso, o SDK do **Touch®** SDK dispõe de todos os métodos necessários para garantir as seguintes funções:

Registro e leitura de impressões digitais
Registro e autenticação de usuários com base nas impressões digitais.

Aceitação dos Termos e Condições
Pode consultar o sistema sobre a última versão dos T&C aceitos pelo usuário.

Checagem governamental
Verifica e compara a impressão digital com as informações fornecidas pelos órgãos governamentais.

Cadastro com qualquer impressão digital
As impressões digitais para o processo de registro e autenticação são configuráveis.

Obtenção de logs de acesso
Salva um log de acesso de uma linha para cada transação feita no sistema.

Validação assíncrona
As entidades governamentais relatam o resultado de forma assíncrona.

API de integração

O aplicativo abrange diferentes métodos, identificados com funções que permitem a gestão dos usuários finais. A comunicação entre as camadas visíveis e o servidor do produto é feita por meio de conexões SSL pela porta TCP 443.

É possível implementar o **Touch®** em qualquer ambiente (celulares ou terminais de autoatendimento), integrando métodos públicos e privados que permitirão:

- Registro e autenticação de usuários
- Bloqueio/desbloqueio de usuários
- Monitoramento do aplicativo e banco de dados
- Consulta de usuário existente
- Gerenciamento e armazenamento de operações do usuário

Scanner de impressões digitais aprovados

O scanner de impressões digitais é um dispositivo eletrônico óptico usado para capturar imagens de impressões digitais das pessoas.

Os equipamentos homologados pela VU Security® são:

- Lumidigm v311
- U.areU 4500

As impressoras digitais devem suportar as seguintes tecnologias para garantir a troca e o armazenamento de impressões digitais:

- WSQ (padrão usado pelo FBI)
- ANSI 378
- ISO 19794-2

Recomendação de manejo de impressões digitais

- Formato: JPG
- Codificação: em base64
- Criptografia: AES-256

Informação técnica

Requisitos e compatibilidade de hardware e software

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

(1) Recomendado

(2) Fornecido nos pacotes de instalação.

Componentes do servidor

Usuários	Armazenamento BS	Transações por segundos	Cores	RAM	Armazenamento do sistema
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

Os cálculos são estimados de acordo com instâncias usuais do produto. Para configurações de alta disponibilidade, sugere-se o uso de instâncias com as mesmas características das apresentadas.

Suporte

Nível de suporte

NOVO

A VU fornecerá **suporte de nível 3**.

O suporte fornece um conjunto de tecnologias e direitos que o cliente tem para ajudá-lo a maximizar seu investimento em licenças da VU.

Para entrar em contato com o VU Support, enviar um e-mail para: customer.support@vusecurity.com

Assim que seu e-mail for recebido, um caso será atribuído a você automaticamente e receberá todas as novidades relacionadas ao seu caso no mesmo thread de e-mail.

Se quiser adicionar destinatários, colocá-los em cópia. Colocar no Assunto: [Nome do cliente] [Criticidade] [Título do problema].

Os casos de suporte são atendidos de **segundas a sextas das 9h às 18h** (Argentina).

Contatos

Outros produtos da VU Security

Nossas soluções oferecem uma experiência 360°, cada uma contribuindo com um aspecto fundamental para a estratégia de segurança de usuários e organizações.

Authentication Management:

- Server
- SDK
- App

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

CIAM / IAM

Se você precisar de mais informações ou quiser agendar uma demonstração desta solução, escreva para: sales@vusecurity.com

Sobre a VU

A VU é uma empresa global de cibersegurança, especializada em proteção da identidade e prevenção de fraude, que desenvolve soluções modulares, fáceis de integrar e adaptáveis tanto à esfera corporativa quanto governamental.

Para isso, utiliza tecnologias inovadoras baseadas na combinação de controles tradicionais de cibersegurança, biometria, geolocalização, inteligência artificial, machine learning, reconhecimento de documentação e análise do comportamento do usuário.

Mais de 350 milhões de pessoas em todo o mundo e mais de 130 clientes em 30 países da América Latina, Europa e Estados Unidos utilizam a tecnologia VU para digitalizar seus negócios e aumentar o nível de operações, reduzindo os riscos de ataques e perda de informações.

Suas alianças estratégicas com a Microsoft, Telefónica, IBM, BGH, Intel, Cisco e Accenture, entre outras empresas, ajudam a VU a cumprir sua missão: criar experiências seguras e sem atritos que melhorem a qualidade de vida de cidadãos e organizações.

vusecurity.com