VU

CIAM

Customer Identity and Access Management
(Gestão de Acesso e Identidade do Cliente)

Datasheet

v 1.1.35

O que é CIAM?

É um conjunto de módulos que permitem gerenciar as identidades de colaboradores, fornecedores, parceiros e clientes de corporações, empresas e organizações governamentais. Fornece mais que apenas acesso, pois estabelece uma relação segura entre o cliente e a organização. Facilita o compartilhamento dos dados dos quais dependem os recursos de cross-marketing e business intelligence. Permite equilibrar a segurança com experiências de usuário sem fricção.

VU CIAM se baseia em quatro pilares: proteção da identidade digital, gestão de riscos, biometria, prevenção de fraude.

Como funciona?

VU CIAM permite que as organizações tenham e forneçam experiências digitais seguras e sem fricção para seus clientes, ao mesmo tempo em que coleta e gerencia a identidades dos clientes. As soluções VU CIAM operam em larga escala e com alto desempenho em diferentes canais de interação com o cliente, como web e mobile.

Gestão do conhecimento

O sistema permite ter uma visão global dos clientes, através da consolidação de identidades digitais.

Transparência de dados

O sistema fornece informações sobre os usuários para gerar oportunidades de vendas, respeitando os regulamentos e políticas de privacidade.

Experiência unificada do usuário

Permite a conversão e retenção de clientes através de registros consistentes e opções de autenticação, compartilhando credenciais e dados entre os diversos canais de interação.

Gestão e controle de acessos

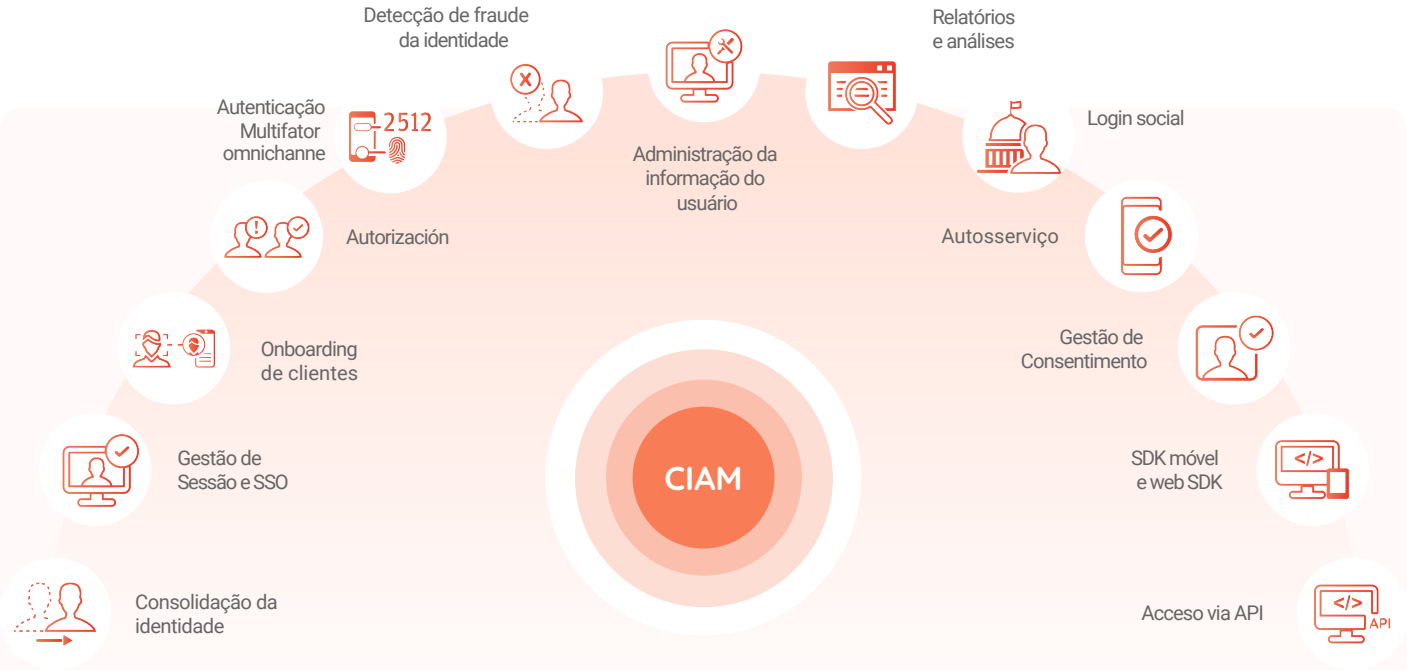
Gestão do ciclo de vida

Autenticação robusta

Único ponto de acesso

Omnichannel

O que os módulos integrados da VU CIAM permitem?



CIAM é uma série de módulos que permite gerenciar identidades e credenciais de colaboradores e fornecedores.

• **Gestão do ciclo de vida das identidades.** Criação, provisionamento, manutenção, desprovisionamento e sincronização de usuários e atributos. O registro do usuário pode estar no modo de autosserviço ou via API. Também pode ser integrado ao Secure Onboarding Process® para um registro com identidade verificada.

• **Gestão e controle de acessos.** Controle, monitoramento e auditoria de acesso aos recursos por meio dos serviços oferecidos pela rede interna ou externa da instituição. Permite uma gestão flexível de autorização baseada em regras ou RBAC.

• **Autenticação multicanal baseada em risco.** O sistema permite gerenciar mecanismos de autenticação robustos e biométricos, como tokens móveis, notificações push, SMS, reconhecimento facial, reconhecimento de voz e mecanismos fora da banda. A autenticação pode ser conectada à VU Fraud Analysis® e VU Device Fingerprint® para controlar acessos seguros com fricção mínima.

• **Início de sessão consolidado.** Usuários que estabeleçam sessões ativas podem acessar várias aplicações sem a necessidade de se autenticar várias vezes. Essa funcionalidade pode ser implementada em aplicações internas, externas e baseadas na nuvem, e os visitantes podem usar suas credenciais da sua sessão ativa para se autenticar em vários sistemas.

• **Autenticação federada e login social.** Compartilhar credenciais com outros siste-mas. Usar credenciais de outros sistemas, incluindo redes sociais e sistemas de autenticação na nuvem.

• **Autosserviço** que permite o registro quanto à gestão de dados pessoais, dados de contato, consentimentos, preferências, dispositivos e sessões.

• **Gestão de consentimento** através de diferentes modelos que incluem informação simples para usuários e textos legais, associadas a objetivos configuráveis. O usuário pode aceitar, rejeitar, revogar e reaceitar consentimentos, detendo total controle de acordo com as regras de privacidade de dados.

• **Prevenção de fraudes** por meio de regras configuradas associadas aos riscos de roubo de identidade.

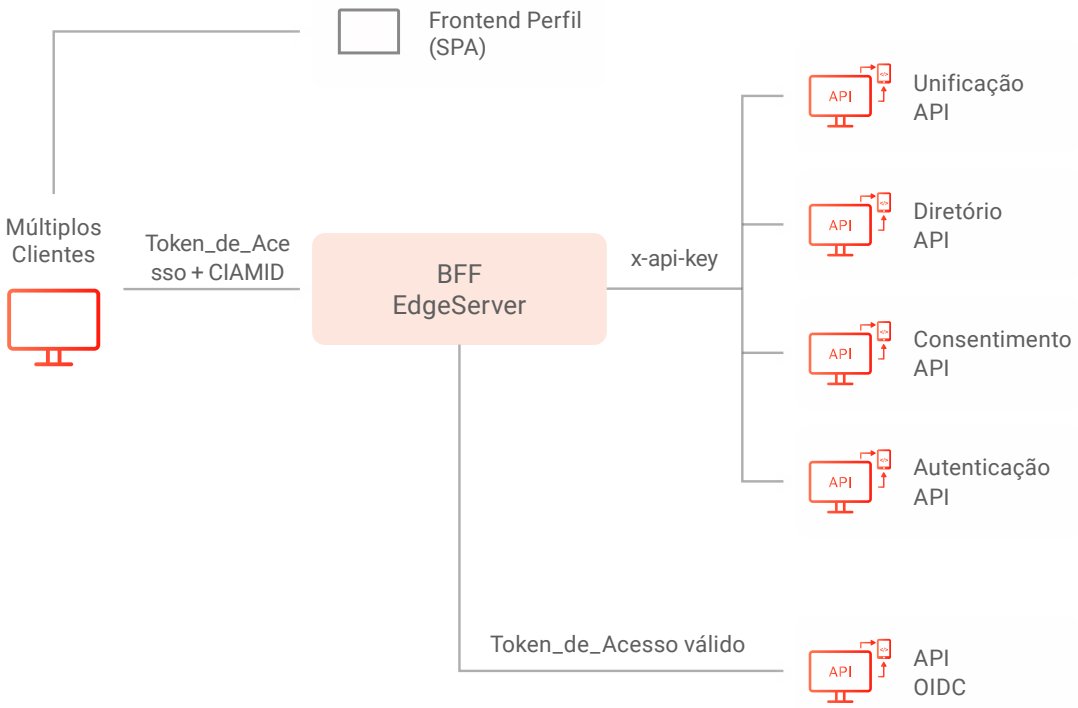
• **Consolidação de identidade**, que permite reunir com segurança múltiplas identidades digitais de uma pessoa para simplificar a gestão, permitir o cross-market-ing e melhorar a experiência do usuário

• **Integração e extensão de funcionalidades** por meio de ferramentas SDK e API que permitem que o VU CIAM seja integrado ao ecossistema de aplicações existentes.

• **Migração com opções de migração progressiva** de clientes ou migração em lotes. Inclui a possibilidade de prédefinir senhas de forma segura anteriormente à subida para produção.

Diagrama lógico de funcionamento

O diagrama a seguir mostra como um aplicativo web ou móvel se conecta de forma segura ao VU CIAM. O módulo EdgeServer VU CIAM demanda um token de acesso e libera acesso aos serviços somente se a validação deste token for bem-sucedida.



Foco na experiência do usuário

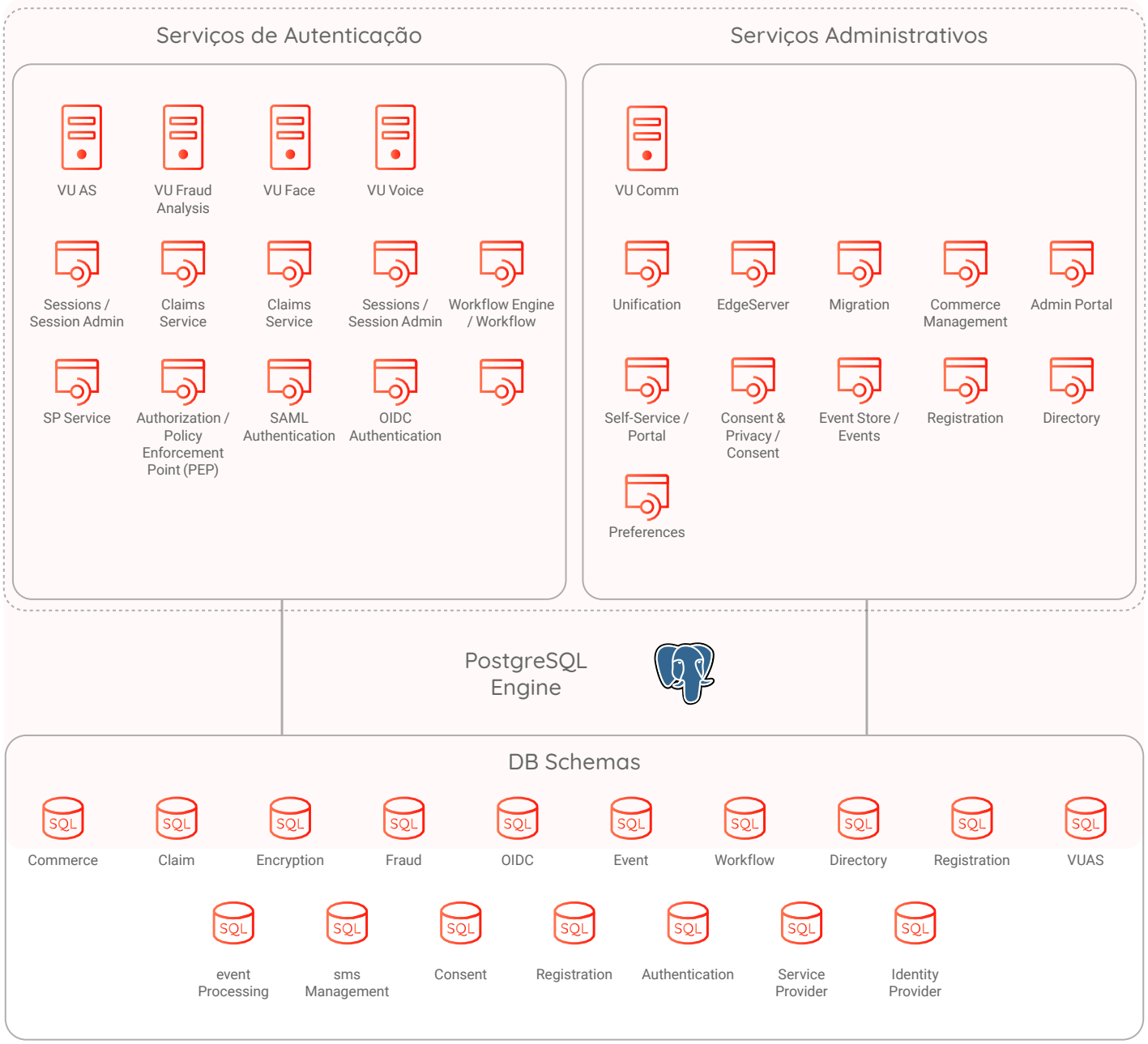
Sabemos que a experiência do usuário é importante neste tipo de solução porque entendemos que esta afeta diretamente o negócio, e a segurança deve ser fornecida com base nisto. É por isso que projetamos e testamos nosso produto com participação dos usuários frequentemente, entendendo e medindo sua experiência de forma a torná-la sempre melhor.

Informação Técnica

VU CIAM disponibiliza um kit de desenvolvimento de so□ware (SDK) para integração em aplicações móveis. O objetivo é simplificar o acesso aos recursos do VU CIAM a partir de um aplicativo móvel. O Mobile SDK está disponível para Android e iOS. As principais características são a senha de uso único (TOTP

HOTP) e a identificação segura do dispositivo.Também é possível integrar o processo de captura biométrica (rosto, voz) usando o VU Secure Onboarding Process®. Além disso, é possível integrar aplicações web acessando as APIs VU CIAM. Inclui uma solução baseada em JavaScript para facilitar a integração com formulários e identificação do dispositivo (browser).

Arquitetura de integração



Requisitos de Software e Compatibilidade

Sistema Operacional	Banco de Dados	App Server	Java
Centos/Redhat 7.9 (*)	PostgreSQL 9 ou superior (*)	Tomcat 9.31 ou superior (*)	1.8
Ubuntu LTS (*)	MS SQL 2019 ou superior	Jboss 7.11 ou superior	
Windows Server 2019			

*Recommended

Casos de uso em destaque

• Empresa líder de varejo com presença em vários países e diversos negócios, com a necessidade de identificar e integrar identidades digitais e credenciais de usuários. Problema: várias empresas do grupo têm usuários separados, o que dificulta a experiência do usuário e o cross-marketing. Solução: uma visão integrada do cliente, alcançada através da unificação de identidades digitais.

• Empresa de serviços diversos: financeiros, de saúde e turismo. Problema: sistema de autenticação muito limitado; necessidade de suportar SSO entre sistemas migrados para VU CIAM e sistemas não migrados. Solução: Integração entre o VU CIAM e o antigo sistema de autenticação usando recursos de federação de identidades.

Outros módulos e produtos VU que aprimoram o CIAM

Nossas soluções são integradas para oferecer uma experiência 360º para os usuários e para a organização. Cada solução oferece um aspecto fundamental para a estratégia de segurança.

Módulos de Onboarding Management
- ID
- Voice
- Touch

Módulos de Authentication Management
- Server

Se precisa de mais informações ou deseja agendar uma demonstração desta solução, por favor nos contate em sales@vusecurity.com