VU

CIAM

Customer Identity and Access Management

Datasheet

v 1.1.35

¿Qué es?

Es un conjunto de módulos que permiten gestionar las identidades de colaboradores, proveedores, socios y clientes de corporaciones, empresas y organizaciones gubernamentales. Provee más que solo acceso, porque establece una relación segura entre el cliente y la organización. Facilita el compartir los datos de los que dependen las capacidades cross-marketing y de inteligencia comercial. Permite equilibrar la seguridad con experiencias de usuario sin fricción.

VU CIAM se basa en cuatro pilares: protección de la identidad digital, gestión de riesgo, biometría y prevención de fraude.

¿Cómo funciona?

VU CIAM permite a las organizaciones tener y proveer experiencias digitales seguras, sin fricción, para sus clientes, al mismo tiempo que colecta y administra las identidades de los clientes. Las soluciones de VU CIAM operan a grandes escalas y alto rendimientos, sobre diferentes canales de interacción de los clientes, como web y mobile.

Gestión del conocimiento

El sistema permite tener una visión global de los clientes, mediante consolidación de identidades digitales.

Transparencia de datos

El sistema entrega información sobre los usuarios para generar oportunidades de venta, respetando las regulaciones y políticas de privacidad.

Experiencia de usuario unificada

Habilita la conversión y retención de clientes a través de registros consistentes y opciones de autenticación compartiendo credenciales y datos entre los distintos

Gestión y controlde accesos

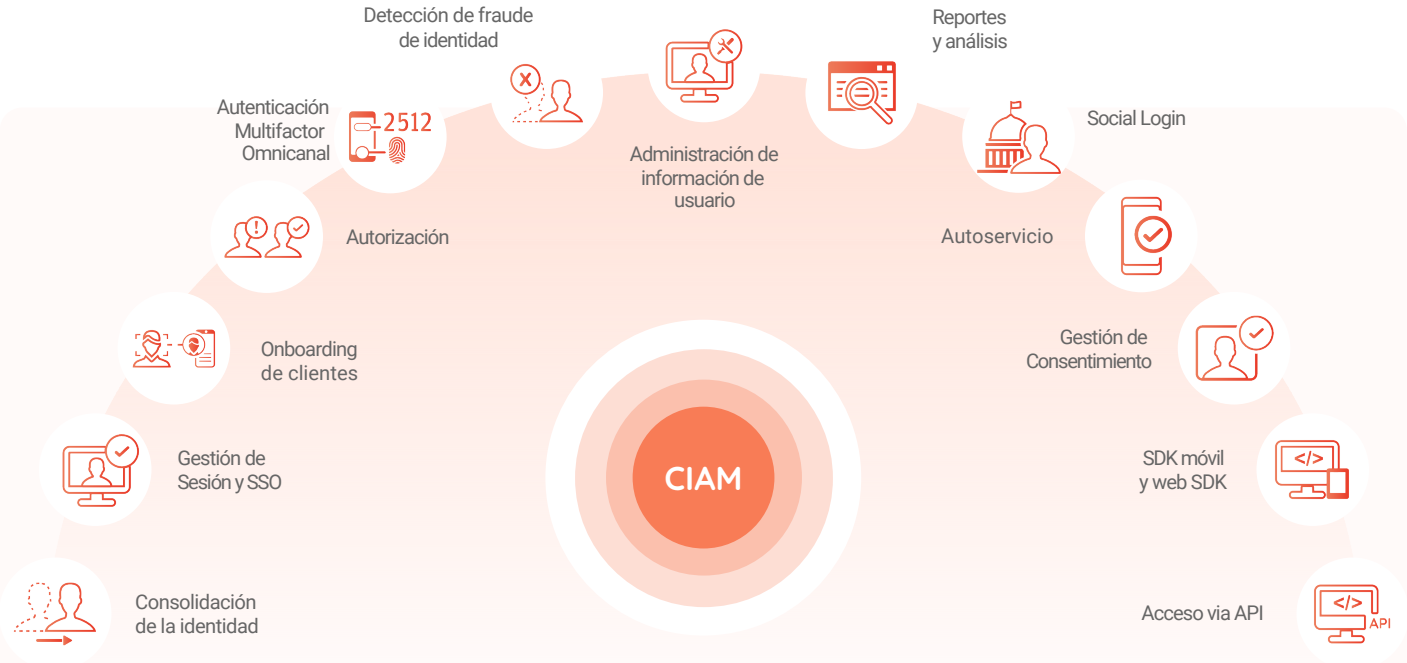
Gestión del ciclo de vida

Autenticación robusta

Único punto de acceso

Omnicanalidad

¿Qué permiten los módulos integrados de VU CIAM?



CIAM es una serie de módulos que permite administrar identidades y credenciales de empleados y proveedores.

• **Gestión del ciclo de vida de las identidades.** Creación, aprovisionamiento, mantenimiento, desaprovisionamiento y sincronización de usuarios y atributos. El registro de usuarios puede ser en modo autoservicio o vía API. También se puede integrar con Secure Onboarding Process® para un registro con identidad verificada.

• **Gestión y control de accesos.** Control, monitoreo y auditoría de acceso a los recursos a través de los servicios que ofrece la red interna o externa de la institución. Permite gestión flexible de autorización basada en roles o RBAC.

• **Autenticación multicanal basada en riesgo.** El sistema permite administrar mecanismos de autenticación robustos y biométricos, como tokens móviles, notificaciones push, SMS, reconocimiento facial, reconocimiento de voz y mecanismos fuera de banda. La autenticación puede conectarse a VU Fraud Analysis® y VU Device Fingerprint® para controlar accesos seguros con mínima fricción.

• **Inicio de sesión único.** Los usuarios que establezcan sesiones activas pueden acceder a diversas aplicaciones sin necesidad de autenticarse múltiples veces. Esta funcionalidad puede ser implementada en aplicaciones internas, externas y basadas en la nube, y los visitantes pueden usar las credenciales de su sesión activa para autenticarse en múltiples sistemas.

• **Federación de identidad y login social.** Compartir credenciales con otros sistemas. Usar credenciales de otros sistemas, incluyendo redes sociales y sistemas de autenticación en nube.

• **Autoservicio** que permite registro como para gestión de datos personales, datos de contacto, consentimientos, preferencias, dispositivos y sesiones.

• **Gestión del consentimiento** mediante plantillas versionadas que incluyen información simple para los usuarios y textos legales, asociadas a propósitos configurables. El usuario puede aceptar, rechazar, revocar y reaceptar consentimientos, de modo que tiene completo control, de acuerdo con las normas de privacidad de datos.

• **Prevención de fraude** mediante reglas configuradas asociadas a los riesgos de suplantación de identidad.

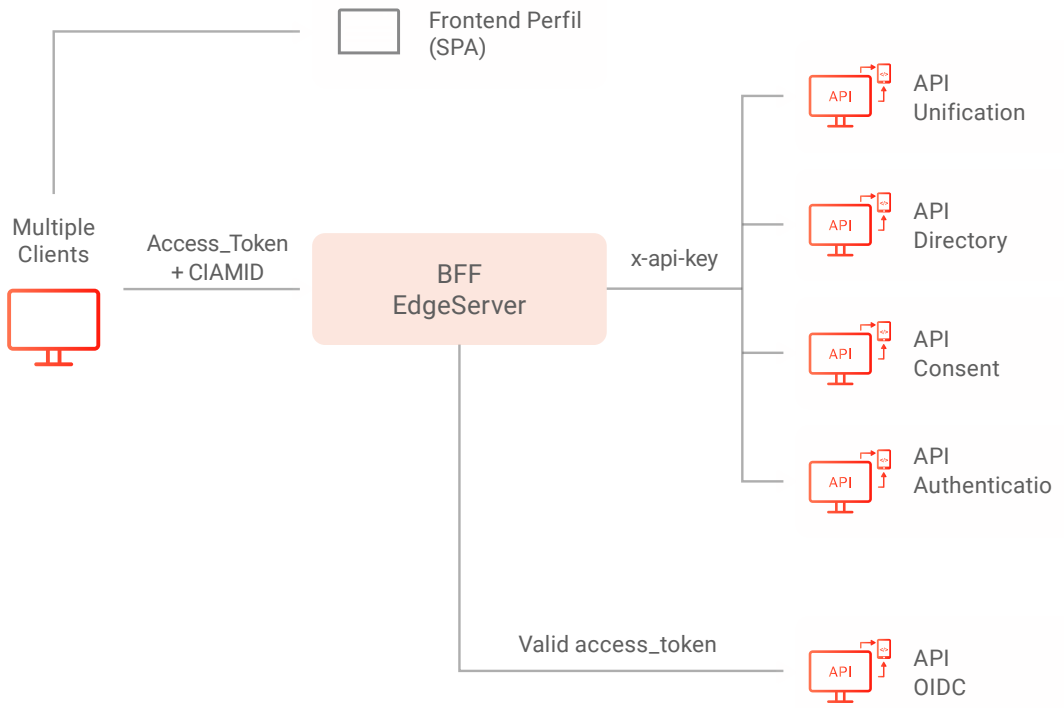
• **Consolidación de identidad,** que permite reunir en forma segura múltiples identidades digitales de una persona para simplificar la gestión, habilitar cross-marketing y mejorar la experiencia de usuario.

• **Integración y extensión** de las funcionalidades mediante herramientas tipo SDK y API, lo que permite integrar a VU CIAM en el ecosistema de aplicaciones existentes.

• **Migración** con opciones de migración progresiva de clientes o migración por lotes. Incluye posibilidad de pre-registrar contraseñas en forma segura durante un proceso previo a la salida a producción.

Diagrama lógico de funcionamiento

El siguiente diagrama muestra cómo se conecta una aplicación web o móvil en forma segura a VU CIAM. El módulo EdgeServer de VU CIAM exige un token de acceso y da acceso a los servicios sólo si la validación del token de acceso es correcta.



Foco en la Experiencia de Usuario

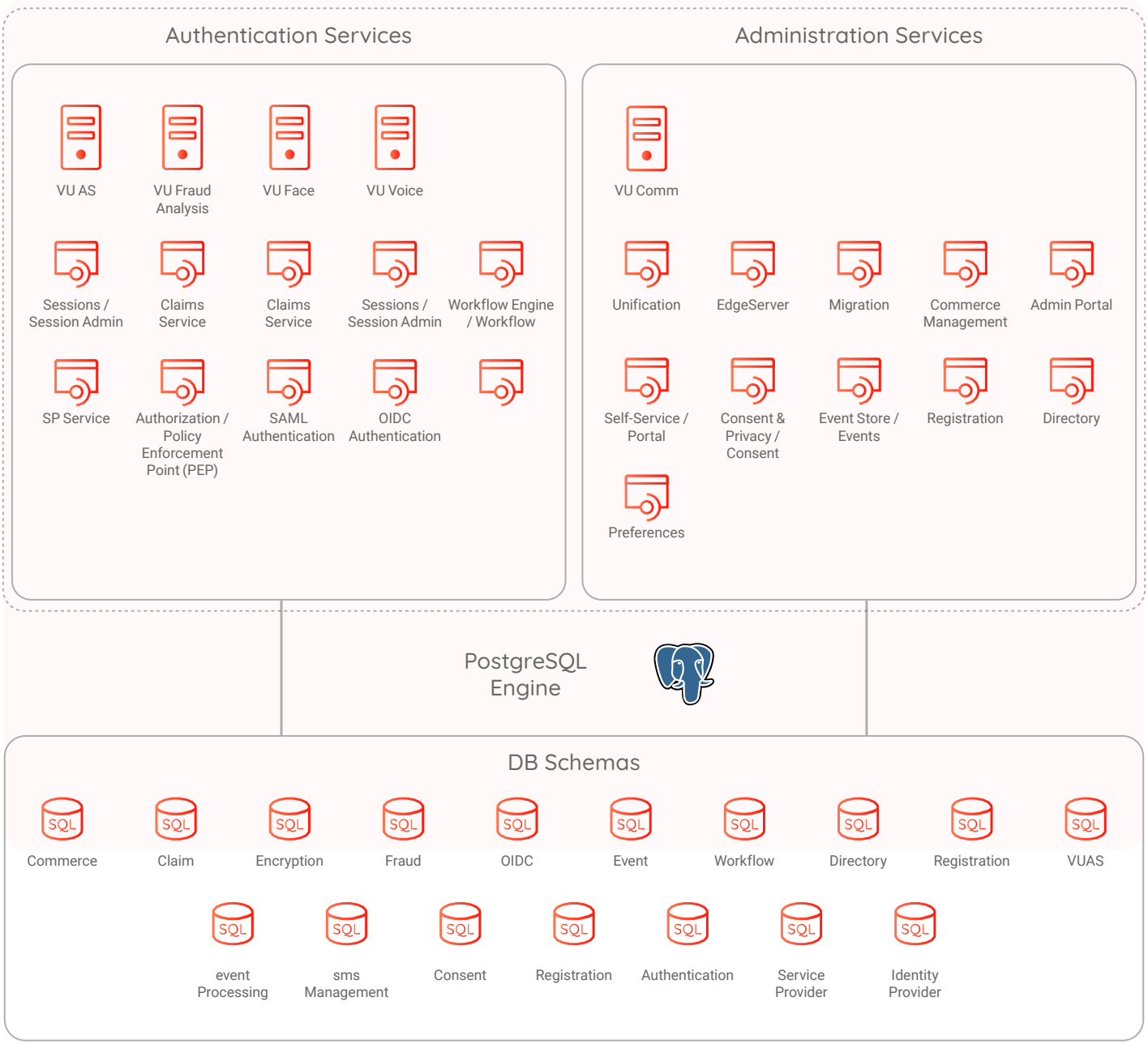
Sabemos que es importante la experiencia del usuario en este tipo de soluciones, porque entendemos que la experiencia del usuario afecta al negocio y la seguridad debe proveerse en función de eso. Por eso diseñamos y probamos con usuarios nuestro producto frecuentemente, entendiendo y midiendo la experiencia para poder maximizarla.

Información Técnica

SDK para dispositivos móviles VU CIAM proporciona un kit de desarrollo de so□ware móvil (SDK) para integrarse en aplicaciones móviles. El objetivo es simplificar el acceso a las funciones de VU CIAM desde una aplicación móvil. Mobile SDK está disponible tanto para Android como para iOS. Las característi-

cas principales son la contraseña de un solo uso (TOTP y HOTP) y la identificación segura del dispositivo. También es posible integrar el proceso de captura biométrica (rostro, voz) mediante VU Secure Onboarding Process®. Además, es posible integrar aplicaciones web, mediante el acceso a las API de VU CIAM. Incluye una solución basada en JavaScript para facilitar la integración con formularios y la identificación del dispositivo (browser).

Arquitectura de integración



Requisitos y Compatibilidad de Software

Sistema Operativo	Base de Datos	App Server	Java
Centos/Redhat 7.9 (*)	PostgreSQL 9 o superior (*)	Tomcat 9.31 o superior (*)	1.8
Ubuntu LTS (*)	MS SQL 2019 o superior	Jboss 7.11 o superior	
Windows Server 2019			

*Recommended

Casos de uso destacados

• Empresa líder en retail con presencia en múltiples países y diversos negocios con necesidad de identificar e integrar identidades digitales y credenciales de los usuarios. Problema: los múltiples negocios tienen usuarios separados lo que dificulta la experiencia del usuario y cross-marketing. Solución: una visión integrada del cliente, lograda a través de la unificación de identidades digitales.

• Empresa de servicios diversos, tanto financieros, salud y turismo. Problema: sistema de autenticación muy limitada; necesidad de soportar SSO entre sistemas migrados a VU CIAM y sistemas no migrados. Solución: Integración entre VU CIAM y el sistema de autenticación antiguo usando capacidades de federación.

Otros módulos y productos de VU que potencian CIAM

Nuestras soluciones se integran para ofrecer una experiencia 360 tanto para los usuarios como para la organización. Cada solución aporta un aspecto fundamental a la estrategia de seguridad.

Módulos de Onboarding Management
- ID
- Voice
- Touch

Módulos de Authentication Management
- Server

Si necesita más información o desea programar una demostración de esta solución, contáctenos en sales@vusecurity.com