VU

CIAM

Datasheet

Versión 1.8.0

¿Qué es?

Mantener identidades digitales de clientes y colaboradores en forma segura y sin fricción es un desafío permanente de las empresas. Por una parte, los consumidores exigen cada vez más simplicidad de uso, seguridad y control sobre sus datos, y por otra parte los delincuentes usan métodos cada vez más sofisticados para cometer fraude. Las empresas precisan herramientas modernas para enfrentar estos desafíos.

VU Customer Identity and Access Management® es una solución para administrar el ciclo de vida de las identidades de colaboradores, socios y clientes de empresas y organizaciones.

Permite la integración de servicios y repositorios de datos de usuario bajo la misma arquitectura, lo que facilita la administración de credenciales y mecanismos robustos de autenticación

Permite equilibrar la seguridad con experiencias de usuario sin fricción

Controla el acceso a los diversos recursos de la institución para mitigar riesgos inherentes

Gestiona de manera centralizada la información de identidades y accesos de los clientes, de acuerdo a políticas de seguridad configurables

Permite a los usuarios gestionar su información, incluyendo registrarse, actualizar datos, gestionar consentimientos, revisar sus accesos, recuperar contraseña, configurar sus métodos de autenticación s métodos de autenticación

Beneficios

VU CIAM® tiene múltiples beneficios que agregan valor al negocio y sus clientes. Cualquier organización que atiende a consumidores debería considerar implementar una solución CIAM porque proporciona:

Una perspectiva holística del cliente, que permite a las organizaciones comprender las acciones de sus clientes en los diferentes canales

Una experiencia de cliente unificada, que permite convertir y retener clientes mediante una experiencia segura y sin fricción, en procesos de registro y autenticación

Información consolidada de los usuarios, incluyendo procesos de registro, inicio de sesión, uso de las aplicaciones, consentimientos, datos demográficos

Cumplimiento de las regulaciones de privacidad

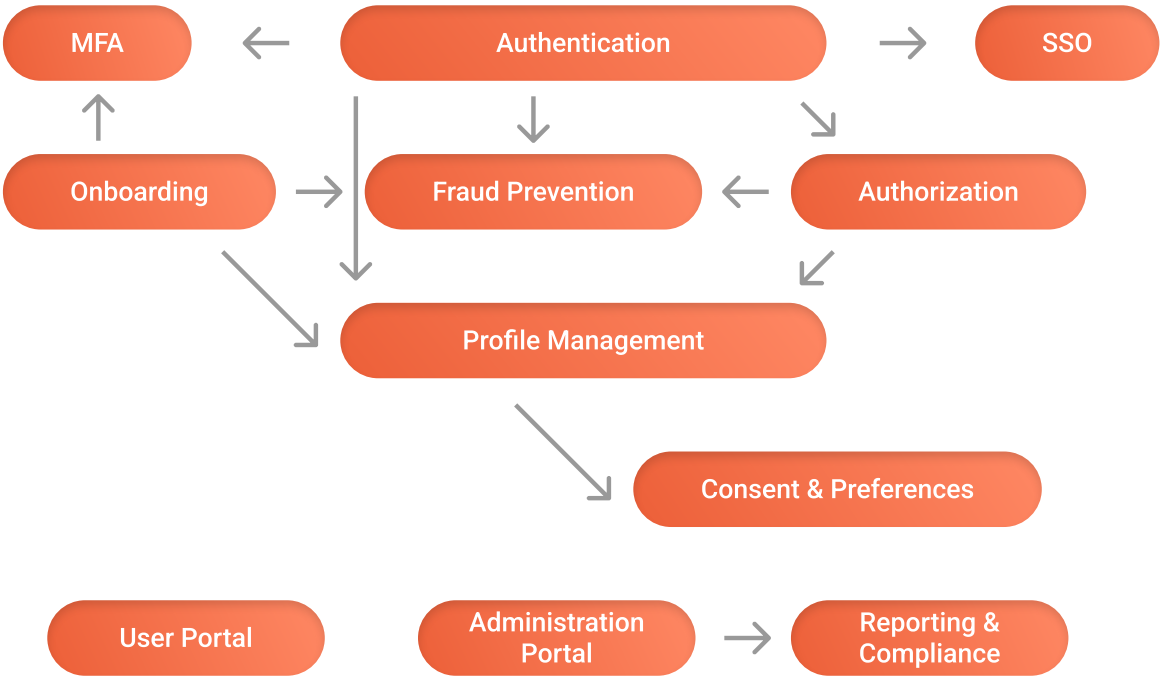
Escalabilidad para admitir millones de identidades de clientes

Bajo riesgo operativo:

- Equilibra un alto nivel de seguridad con baja fricción
- Previene el fraude y la suplantación de identidad

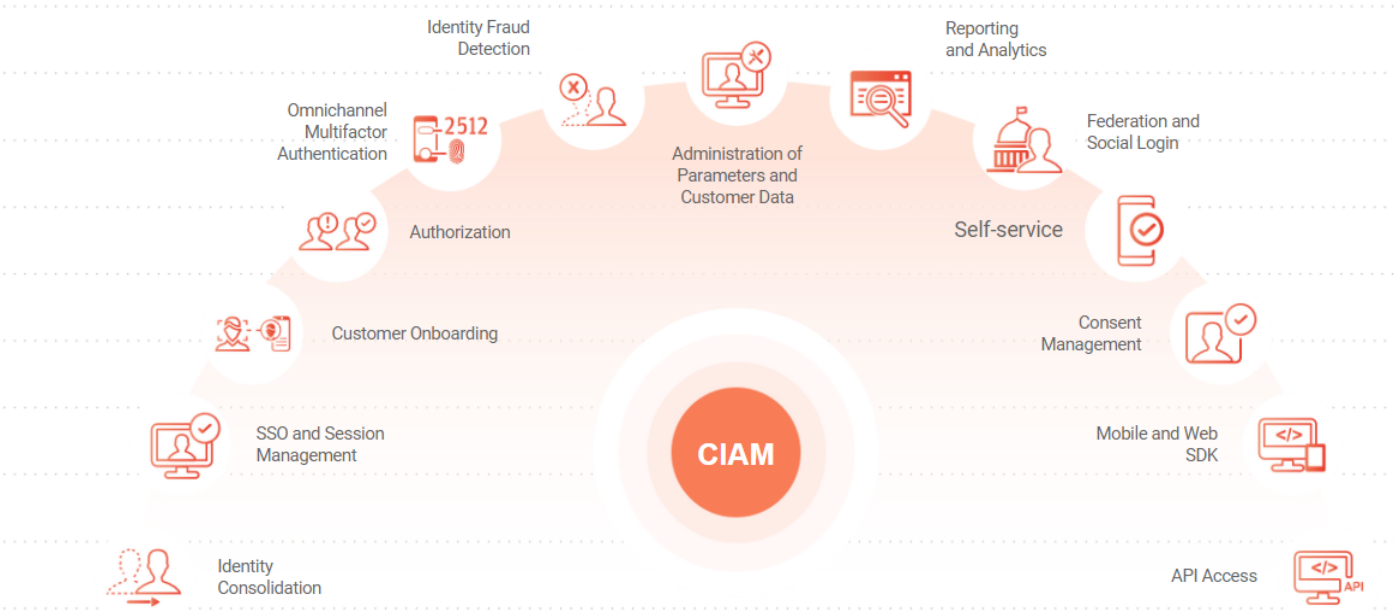
Solución modular

CIAM está estructurado como un conjunto de grupos funcionales interdependientes.
El diagrama muestra la arquitectura a nivel conceptual.



Algunas funciones principales de **CIAM** son:

Authentication es responsable de identificar positivamente a los usuarios. Lo hace basado en servicios de autenticación multifactor (*MFA*) y los datos de perfiles de usuarios (*Profile Management*). También puede verificar la seguridad usando **Fraud Prevention**.
SSO o *single sign-on* simplifica el proceso de autenticación de un usuario reconociendo sesiones activas previamente.
Authorization determina si un usuario autenticado puede o no realizar ciertas operaciones, por ejemplo, tener acceso a una aplicación.
Onboarding carga datos de usuarios validados en *Profile Management*, el cual administra la información personal y de contacto.
Consent and Preferences registra los permisos y preferencias del usuario en relación a las aplicaciones.
Unificación de identidades permite consolidar identidades digitales y lograr una visión única del cliente/ usuario a partir de información en diversos proveedores de identidad.
User Portal permite a los usuarios revisar y editar su información.
Administration Portal permite configurar las múltiples opciones de CIAM, incluye consulta de reportes operativos y extracción de información tanto en modo *batch* como en tiempo real, incluyendo notificaciones a usuarios y notificaciones de eventos del sistema que pueden ser consumidas por otros sistemas de información.



Alcance funcional

Autenticación multifactor

- Uso de protocolo SAML
- Uso de protocolo OpenID Connect
  - Flujo estándar authorization_code, resource owner credentials/password y client_credentials
  - Flujo extendido otp y derived_token
- Métodos de entrega/generación de OTP:
  - SMS
  - Email
  - Push notification
  - **Authentication Management App** u otros autenticadores móviles
- Uso de motor de reglas de **Fraud & AML** según configuración de cada proveedor de servicio:
  - Autorizar directamente
  - Solicitar más autenticación, con segundo factor de autenticación
  - Denegar acceso
- Formulario de login incluye función de recuperación de contraseña, con posibilidad de invocar al motor de reglas:
  - Autorizar recuperación de contraseña
  - Denegar recuperación de contraseña

Login único (SSO)

- La sesión iniciada en un proveedor de servicio se usa para lograr acceso transparente a otro proveedor de servicio
- SSO soporta los protocolos OpenID Connect y SAML
- Administración de sesiones incluye inicio de sesión, estado de sesión, fin de sesión

Autorización, RBAC, ABAC

- Autorización basada en roles
- Relación entre grupos de Active Directory y roles
- Permisos de acceso definidos para cada proveedor de servicio:
  - Control de acceso a aplicaciones basado en atributos con uso del motor de reglas

Registro de usuarios en Directory

Módulo Directory administra la información del perfil del usuario y organizaciones.

- Registro de usuarios con datos mínimos, según la configuración
- Registro progresivo permite agregar más información para enriquecer el perfil del usuario
- Gestión del ciclo de vida del usuario
- Variantes del proceso de registro
    - Configuración de datos a solicitar por cada proveedor de servicio
    - Configurar plantilla de consentimiento de registro
    - *Registro unificado*: buscar una identidad digital con datos coincidentes y agregar información en lugar de crear una nueva identidad
    - Omitir contraseña (se puede agregar después)
    - Permitir registro incompleto de usuario
- Modos de registro
    - Formulario configurable de **VU CIAM**
    - Uso de API con formulario propio del proveedor de servicio o registro de migración progresiva
- Uso del motor de reglas para validar un registro de usuario y cambio de datos sensibles

Federación y login social

- Federación externa
    - Login social con proveedor de identidad externo basado en protocolo OpenID Connect
    - Proceso de login crea una identidad automáticamente si no existía usando los datos del proveedor de identidad
    - Acceso a *Active Directory*
- Federación interna
    - Permite ingresar a un proveedor de servicio con las credenciales de otro proveedor de servicio
- Configuración para cada proveedor de servicio
    - Proveedores de identidad admisibles
    - Datos por entregar en el token jwt o SAML response

Gestión de consentimientos y preferencias

- Creación de propósitos de consentimiento según necesidades de cada instalación
- Plantillas de consentimiento *(consent templates)*
  - Definen el formato de un consentimiento
  - Incluyen texto para interfaz con el usuario y texto legal
- Creación, revocación de consentimientos de usuario basada en una plantilla
  - Identifica al usuario que da el consentimiento y al proveedor de servicio que recibe el consentimiento
  - Consentimientos compuestos agrupan varios consentimientos atómicos
- Auditoría de consentimientos
- Registro de consentimientos históricos (anteriores a CIAM)
- Preferencias de usuario están basadas en plantillas de preferencias, que definen tipos enumerados
  - Pueden asociarse a un consentimiento para dar detalles de este
  - Pueden asociarse a un proveedor de servicio o ser globales

Cumplimiento y GDPR

- **CIAM ID** sirve de alias en la pseudonimización de datos
- Los usuarios:
  - Tienen control sobre sus consentimientos y preferencias
  - Pueden acceder a sus datos y descargarlos
  - Tienen derecho al olvido
- Sistema de protección de datos de los usuarios
  - Los Datos están cifrados en tránsito con TLS y contraseñas protegidas con cifrado asimétrico adicional
  - Múltiples mecanismos de detección de fraude

Portal de Usuario

- Datos de acceso a aplicaciones
- Consulta/edición de:
  - Datos personales
  - Datos de contacto
  - Consentimientos y preferencias
  - Credenciales
- Dispositivos y sesiones
- Informe descargable de todos los datos
- Derecho a ser borrado (derecho al olvido)
- Consolidación de identidad (unificación verificada)

Consolidación y unificación de identidades

- Identidad digital permite múltiples cuentas/credenciales
- Tipos de unificación de identidades
  - Unificación automática, basada en reglas configurables
  - Unificación verificada, basada en reglas configurables y con verificación por parte del usuario
  - Registro unificado (ver *Registro de usuarios* más arriba)
  - Unificación manual, vía API desde una aplicación confiable

Detección de fraude

- Basado en reglas configurables
  - Reconocimiento del dispositivo, dirección IP
  - Reglas de geolocalización, acumuladores, reglas de acción, reglas complejas CEP *(Complex Event Processing)*
- Invocación configurable desde
  - Registro con creación de identidad
  - Registro con reutilización de identidad existente
  - Login
  - Recuperación de contraseña
  - Cambio de contraseña
  - Cambio de datos sensibles

Integración y administración

- Portal de administración permite consultar, crear, modificar, y eliminar las configuraciones
  - Service Providers (OIDC, SAML)
  - Identity Providers
  - Negocios y comercios
  - Consentimientos y preferencias
  - Atributos personalizados
  - Gestión de roles, permisos y asignación de roles a usuarios
  - Consulta de reportes operativos
    - Todos los eventos se registran en logs de archivos y/o bases de datos y/o message broker
    - Reportes básicos de gestión de usuario
    - Disponibilidad de APIs de reportes para integración con sistemas de análisis de datos externos

- Acceso API
  - Todas las funcionalidades tienen acceso vía API
  - Acceso está protegido mediante API Keys
  - Funciones críticas y acceso desde web con protección adicional mediante tokens OpenID Connect
- SDK
  - SDK Móvil
    - Android y iOS
    - Gestión de semillas de OTP, identificación del dispositivo
  - SDK Web
    - Basado en JavaScript
    - Formularios de integración para autoservicio
    - Identificación del dispositivo
- Migración
  - Carga masiva de registro de usuarios a CIAM con o sin contraseña

Distribución

VU CIAM se puede adquirir mediante licenciamiento de software (administrado por el cliente). Próximamente se ofrecerá la opción de software como servicio (SaaS), opción actualmente disponible a través de partners.

Requisitos y compatibilidad de software

Sistema operativo	Base de datos	App Server	Java
Centos/Redhat 7.9 (*)	Versión 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			

*Recomendado

Soporte

El soporte incluye un conjunto de tecnologías y derechos que tiene el cliente para ayudarlo a potenciar al máximo la inversión realizada en las licencias de VU. VU proveerá soporte nivel 3.

Nuestros partners pueden proporcionar servicios de soporte de nivel 1 y/o nivel 2, además de servicios de implantación, integración y entrenamiento asociados a CIAM.

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.

Onboarding Management:

- ID
- Face
- Voice
- Touch

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

Authentication Management:

- Server
- SDK
- App

Contactos

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