VU

CIAM

Datasheet

Version 1.8.0

What CIAM is

Maintaining digital identities of customers and collaborators in a secure and frictionless environment is an ongoing challenge for companies. On one hand, consumers are increasingly demanding simplicity of use, security, and control over their data; on the other hand, criminals are using increasingly sophisticated methods to commit fraud. Companies need modern tools to meet these challenges.

VU Customer Identity and Access Management® is a solution for managing the lifecycle of the identities of employees, partners, and customers in companies and organizations.

- It allows to integrate of services and user data repositories under the same architecture, which facilitates the management of credentials and robust authentication mechanisms
- It balance security with frictionless user experiences
- It controls access to the organization's various resources to mitigate inherent risks
- It centralizes the management of customer identity and access information, according to configurable security policies
- It allows users to manage their information, including registering, updating data, managing consents, reviewing their accesses, equating password, configuring their authentication methods

Benefits

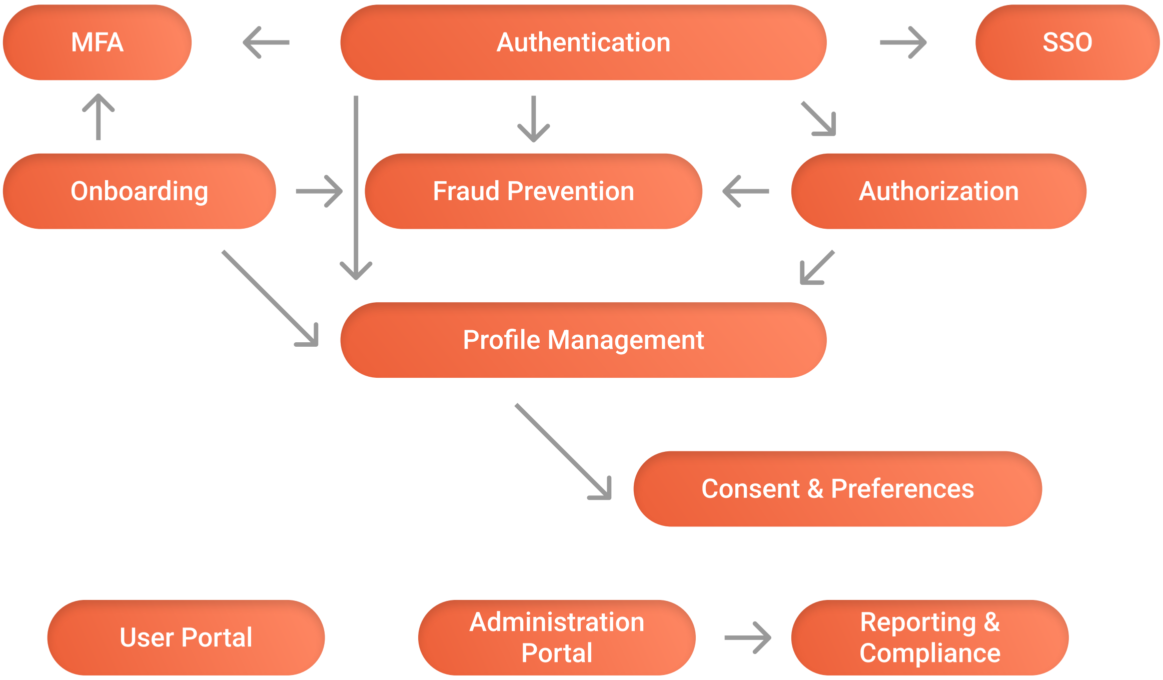
VU CIAM® has multiple benefits that add value to the business and its customers.

Any organization serving consumers should consider implementing a **CIAM** solution because it provides:

- A holistic customer perspective, which allows organizations to understand the actions of their customers in the different channels
- A unified customer experience, which allows you to convert and retain customers through a secure and frictionless experience, into registration and authentication processes
- Consolidated user information, including registration processes, login, application usage, consents, demographic data
- Compliance with privacy regulations
- Scalability to support millions of customer identities
- Low operational risk:
  - It balances a high level of safety with low friction
  - It prevents fraud and phishing

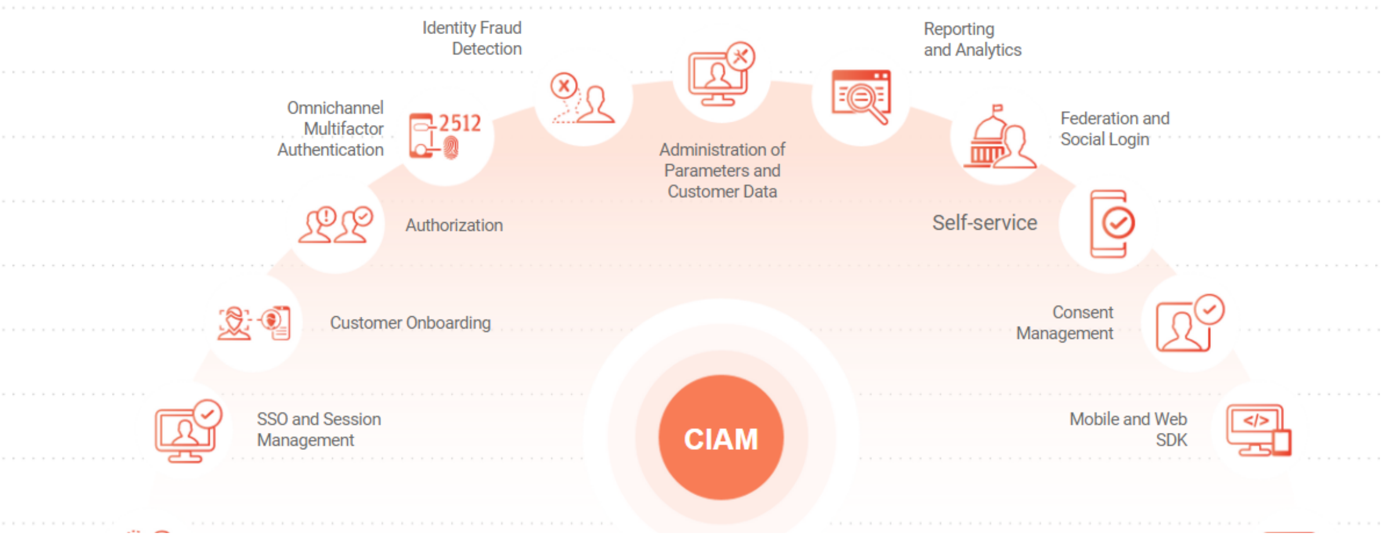
Modular solution

CIAM is structured as a set of interdependent functional groups. The diagram shows the architecture at the conceptual level.



Some main functions of **CIAM** are:

Authentication is responsible for positively identifying users. It does this based on multi-factor authentication (MFA) services and user profile data (Profile Management). You can also check security using **Fraud Prevention**.
SSO or *single sign-on* simplifies the process of authenticating a user by recognizing previously active sessions.
Authorization determines whether or not an authenticated user can perform certain operations.
Onboarding uploads validated user data to Profile Management, which manages personal and contact information.
Consent and Preferences records the user's permissions and preferences in relation to the systems.
Identity unification, which makes it possible to consolidate digital identities and achieve a single view of the customer/user based on information from various identity providers.
An Administration Portal that allows you to configure the multiple CIAM options, includes consultation of operational reports and extraction of information both in batch mode and in real time, including notifications to users and notifications of system events that can be consumed by other information systems.
A User Portal that allows users to review and edit their information.


Identity Fraud Detection
Reporting and Analytics
Omnichannel Multifactor Authentication
2512
Administration of Parameters and Customer Data
Federation and Social Login
Authorization
Self-service
Customer Onboarding
Consent Management
SSO and Session Management
CIAM
Mobile and Web SDK

Functional scope

Multifactor authentication

- Use of SAML protocol
- Us of OpenID Connect protocol
    - Flow authorization_code flow, resource owner credentials/password and client_credentials
    - Extended OTP and derived_token flows
- OTP delivery/generation methods
    - SMS
    - Email
    - Push notification
    - **Authentication Management App** or other mobile authenticators
- Use of **Fraud** rule engine according to configuration of each service provider
    - Authorize directly
    - Request more authentication, with second factor authentication
    - Deny access
- Login form includes a password recovery function, with the possibility of invoking the rule engine
    - Authorize password recovery
    - Deny password recovery

SSO

- A session logged in a service provider is used to transparently gain access to another service provider
- SSO supports OpenID Connect and SAML protocols
- Session management includes login, session state, end of session

Authorization, RBAC, ABAC

- Role-based authorization
- Relationship between Active Directory groups and roles
- Access permissions defined for each service provider:
    - Attribute-based application access control with use of the rule engine

Registering users in Directory

Directory module manages user and organization profile information

- User registration with minimal data, depending on configuration
- Progressive registration allows you to add more information to enrich the user's profile
- User lifecycle management
- Variants of the registration process
  - Configuration of data to be requested by each service provider
  - Configure registration consent template
  - Unified registration: Search for a digital identity with matching data and add information instead of creating a new identity
  - Omit password (can be added later)
  - Allow incomplete user registration
- Registration modes
  - **VU CIAM** configurable form
  - Using APIs with the service provider's own form or registration by progressive migration log
- Using the rule engine to validate a user registration and change of sensitive data

Federation and social login

- External federation
  - Social login with external identity provider based on OpenID Connect protocol
  - Login process creates an identity automatically if it did not exist using identity provider data
  - *Active Directory* access
- Internal federation
  - Allows you to enter a service provider with the credentials of another service provider
- Configuration for each service provider
  - Admissible identity providers
  - Data to be delivered in the jwt token or SAML response

Management of consents and preferences

- Creation of consent purposes according to the needs of each installation
- *Consent templates*
    - Define the format of a consent
    - Include text for user interface and legal text
- Creation, revocation of user consents based on a template
    - Identifies the user who gives consent and the service provider who receives consent
    - Composite consents group several atomic consents
- Consent Audit
- Record of historical consents (prior to CIAM)
- User preferences are based on preference templates, which define enumerated types
    - They can be associated with a consent to give details of this
    - Can be associated with a service provider or be global

Compliance and GDPR

- **CIAM ID** serves as an alias in data pseudonymization
- Users
    - They have control over their consents and preferences
    - They can access and download their data
    - They have the right to be forgotten
- User data protection system
    - Data is encrypted in transit with TLS and passwords protected with additional asymmetric encryption
    - Multiple fraud detection mechanism

User Portal

- Application access data
- View/edition of
    - Personal data
    - Contact details
    - Consents and preferences
    - Credentials
- Devices and sessions
- Downloadable report of all data
- Right to be erased (right to be forgotten)
- Identity consolidation (verified unification)

Identity consolidation and unification

- Digital identity allows multiple accounts/credentials
- Types of identity unification
  - Automatic unification, based on configurable rules
  - Verified unification, based on configurable rules and with user verification
  - Unified registration (see User Registration above)
  - Manual unification, via API from a reliable application

Fraud detection

- Based on configurable rules
  - Device recognition, IP address
  - Geolocation rules, accumulators, action rules, complex CEP rules *(Complex Event Processing)*
- Configurable invocation from
  - Registration with identity creation
  - Registration with reuse of existing identity
  - Login
  - Password recovery
  - Password change
  - Changing sensitive data

Integration and administration

- Management portal allows you to query, create, modify, and delete configurations
  - Service Providers (OIDC, SAML)
  - Identity Providers
  - Businesses and shops
  - Consents and preferences
  - Custom attributes
  - Managing roles, permissions, and assigning roles to users
  - Consultation of operational reports
    - All events are logged in file logs and/or databases and/or message broker
    - Basic user management reports
    - Availability of reporting APIs for integration with external data analysis systems

- API Access
  - All functionalities have access via API
  - Access is protected by API Keys
  - Critical functions and access from the web have additional protection through OpenID Connect tokens
- SDK
  - Mobile SDK
    - Android and iOS
    - OTP seed management, device identification
  - Web SDK
    - JavaScript-based
    - Self-service integration forms
    - Device identification
- Migration
  - Bulk upload of user registration to CIAM with or without password

Distribution

VU CIAM can be purchased through software licensing (managed by the customer).
Software as a Service (SaaS), currently available through partners, will be offered soon.

Software requirements and compatibility

Operating system	Database	App Server	Java
Centos/Redhat 7.9 (*)	Version PostgreSQL 9 or higher	Tomcat 9.31 or higher (*)	1.8
Ubuntu LTS (*)	MS SQL 2019 or higher (*) (**)	JBoss 7.11 or higher	
Windows Server 2019			

*Recommended

Support

VU will provide level 3 support. Support includes a set of technologies and rights that the customer has to help them maximize the investment made in VU licenses.

Our partners can provide level 1 and/or level 2 support services, as well as implementation, integration and training services associated with CIAM.

Other VU products

Our solutions offer a 360° experience, each one contributing a fundamental aspect to the security strategy of both users and organizations.

Onboarding Management:

- ID
- Face
- Voice
- Touch

Fraud & AML:

- Fraud Analysis
- Device Fingerprint

Authentication Management:

- Server
- SDK
- App

Contact

For more information or to schedule a demo of this solution, please contact us at: sales@vusecurity.com

VU

About VU

VU is a global cybersecurity company, specializing in identity protection and fraud prevention. It develops modular solutions, easy to integrate and adaptable to both corporate and government environments.

To achieve this, VU uses innovative technologies based on the combination of traditional cybersecurity controls, biometrics, geolocation, artificial intelligence, machine learning, document recognition and user behavior analysis.

More than 350 million people around the world and 130 clients in 30 countries in Latin America, Europe and the United States use VU technology to digitize their businesses and increase the level of operations, reducing the risks of attacks and loss of information.

Its strategic alliances with Microsoft, Telefónica, IBM, BGH, Intel, Cisco and Accenture, among other companies, help VU fulfill its mission: build secure and frictionless experiences that improve the quality of life of citizens and organizations.

vusecurity.com