**What is it?**

It is a set of modules for managing the identities of co-workers, suppliers, partners and customers of corporations, businesses and governmental organizations. It provides more than just access, because it creates a secure relationship between the customer and the organization. It makes it easier to share the data on which cross-marketing and business intelligence capabilities depend. It allows balancing safety with frictionless user experiences.

VU™ CIAM is based on four pillars: digital identity protection, risk management, biometrics and fraud prevention.

**How it works**

VUTM CIAM enables organizations to have and provide secure, frictionless digital experiences for their customers, while collecting and managing customer identities. VUTM CIAM solutions operate at large scales and high performance, over different customer interaction channels, such as web and mobile.

**Knowledge management**

The system provides a global view of customers through the consolidation of digital identities.
Data transparency

The system delivers information about users to drive sales opportunities, while complying with regulations and privacy policies.

Unified user experience

It supports customer conversion and retention through consistent registration and authentication options by sharing credentials and data across different businesses within an organization.

What do VU CIAM’s integrated modules allow us to do?

CIAM is a series of modules that allows to manage the identities of collaborators, providers, partners and customers.
• **Identity lifecycle management.** Creation, provisioning, maintenance, deprovisioning and synchronization of users and attributes. User registration can be done either on a self-service basis or through the API. It can also be integrated with Secure Onboarding Process for identity-verified registration.

• **Access control and management.** Control, monitoring and auditing of access to resources through the services offered by the internal or external network of the organization. Flexible management of role-based authorization or RBAC is supported.

• **Multichannel authentication based on risk.** The system allows managing strong and biometric authentication mechanisms, such as mobile tokens, push notifications, SMS, facial recognition, voice recognition and out-of-band authentication mechanisms. Authentication can be linked to VUTM Fraud Analysis and VUTM Device Fingerprin for secure access control with minimal friction.

• **Single sign-on.** Users who have active sessions can access various applications with no need to complete the authentication process repeatedly. This functionality can be implemented in internal, external and cloud-based applications, and visitors can use their active session credentials to sign on to various software systems.

• **Identity federation and social login.** It allows sharing credentials with other software systems, as well as using credentials from other software systems, including social networks and cloud-based authentication software systems.

• **Self-service** that allows registration for managing personal data, contact data, consents, preferences, devices and sessions.

• **Consent management through customized templates** that include simple information for users as well as legal documents associated with user-configurable purposes. The users can give, refuse, revoke and consent as well as give it again, so that they retain complete control, in accordance with data privacy rules.

• **Fraud prevention,** which is carried out through set rules connected to identity theft risks.

• **Identity consolidation,** which allows gathering multiple digital identities of a person in a secure way to simplify management, enable cross-marketing and improve user experience.

• **Integration and expansion of functionalities** through SDK and API tools, allowing VUTM CIAM to be integrated into the already existing application ecosystem.

• **Migration,** which can be done by progressive migration of clients or by batch migration. It also includes the option of secure pre-registration of passwords in a pre-release process.
The following diagram shows how a web or mobile application securely connects to VUTM CIAM. The VUTM CIAM EdgeServer module requires an access token and grants access to services only if the validation of the access token is successful.

Focus on user experience

We know that user experience is important in this type of solutions as it has an impact on the business, and security must be provided accordingly. Therefore, our product is designed and tested with users frequently, thus understanding and measuring their experience in order to maximize it.

Technical data

SDK for VUTM CIAM mobile devices provides a mobile software development kit (SDK) for integration into mobile applications. The goal is to simplify access to VUTM CIAM functions from a mobile application. Mobile SDK is available for both Android and iOS. The main features of this solution are one-time password (TOTP...
and HOTP) and secure device identification. Biometric capture process (face, voice) can also be integrated into through VU Secure Onboarding Process.

In addition, it is possible to integrate web applications by accessing the VUTM CIAM APIs. It includes a JavaScript-based solution to smooth integration with forms and device identification (browser).

**Integration architecture**
System and software requirements and compatibility

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Database</th>
<th>App Server</th>
<th>Java</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centos/Redhat 7.9 (*)</td>
<td>PostgreSQL 9 or higher (*)</td>
<td>Tomcat 9.31 or higher (*)</td>
<td>1.8</td>
</tr>
<tr>
<td>Ubuntu LTS (*)</td>
<td>MS SQL 2019 or higher</td>
<td>Jboss 7.11 or higher</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2019</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Recommended

Noteworthy use cases

• Leading retail company operating in multiple countries and diverse businesses seeking to identify and integrate digital identities and user credentials. Problem: there are different businesses and each of them has its own users, which makes user experience and cross-marketing difficult. Solution: a comprehensive vision of the customer, achieved through the unification of digital identities.

• A company that offers various services: financial, health and tourism services. Problem: very limited authentication system; need to support SSO between VUTM CIAM migrated systems and non-migrated systems. Solution: Integration between VUTM CIAM and legacy authentication system using federation capabilities.

Additional VU modules and products that enhance CIAM
The integration of our solutions can provide a comprehensive experience both for users and for the organization. Each and every solution brings a basic aspect into the security strategy.

Onboarding Management Modules
• ID
• Voice
• Touch

Authentication Management Modules
• Server

If you need more information or wish to schedule a demo of this solution, please email us at: sales@vusecurity.com