What is it?

It is a multi-factor authentication framework that centralizes user policies, passwords and their traceability. It provides a flexible, simple and personalized scheme when implementing a second factor system in the cloud through any device with Internet access.

Features:

- Optimizes investment and costs of technical and human resources.
- Avoids phishing, pharming and identity theft attacks, among others.
- It complies with the requirements of all banking and transactional regulatory bodies in Latin America.

Logic diagram of operation

User Interface Options

Integration API

The VUAS module is a solution that acts as an authentication core. Thanks to its wide integration capacity, it can be implemented in any type of environment or technological platform, regardless of the language used, through REST or SOAP Web services.
Communication between the presentation layers and the product server is through an SSL / TLS connection.

The available methods allow to:

- Enable and disable users and types of authentication factors.
- Validate credentials.
- Eliminate users and types of authentication factors from the platform.
- Modify and assign the password of a user on the platform.
- Add Access Control Service groups.
- Create, register, validate, block and unblock users.
- Delete authentication factors assigned to users.
- Provide unique codes (one time passwords) assigned to the user in the VU™ Mobile Tokens system.
- Validate the VU™ Mobile Tokens of an end user.
- Report the status of a user.
- Analyze transactions.
- Analyze events.
- Analyze and validate fingerprints.
**VU™ Mobile Tokens SDK**

The VU™ Mobile Tokens SDK can be integrated into:

<table>
<thead>
<tr>
<th>Technology</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>Java</td>
</tr>
<tr>
<td></td>
<td>SDK + Sample project</td>
</tr>
<tr>
<td>iOS</td>
<td>Swift</td>
</tr>
<tr>
<td></td>
<td>SDK + Sample project</td>
</tr>
<tr>
<td>Web</td>
<td>Javascript</td>
</tr>
<tr>
<td></td>
<td>SDK + Sample project</td>
</tr>
<tr>
<td>Híbrido</td>
<td>Javascript</td>
</tr>
<tr>
<td></td>
<td>SDK + Sample project</td>
</tr>
</tbody>
</table>

They make use of Native SDKs (Swift y Java)

### Software requirements and compatibility

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Database</th>
<th>App Server</th>
<th>Java</th>
<th>Device Compatibility (SDK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centos/Redhat</td>
<td>PostgreSQL 9 or higher (*)</td>
<td>Tomcat 9.31 or higher (*)</td>
<td>1.8</td>
<td>iOS 11 or higher (*)</td>
</tr>
<tr>
<td>Ubuntu LTS (*)</td>
<td>MS SQL 2019 or higher</td>
<td>Jboss 7.11 or higher</td>
<td></td>
<td>Android 5 or higher</td>
</tr>
<tr>
<td>Windows Server 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Recommended

### Integrations

- API REST
- Radius
### Access management
- Active Directory
- LDAP

### Management of records and reports
- PowerBI
- Kibana

### Mobile compatibility
- iOS
- Android

### Hardware dimensioning*

<table>
<thead>
<tr>
<th>Users</th>
<th>TPS</th>
<th>CORES</th>
<th>RAM</th>
<th>System Storage</th>
<th>Monthly DB Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>250,000</td>
<td>8</td>
<td>2</td>
<td>4</td>
<td>60 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td>500,000</td>
<td>16</td>
<td>4</td>
<td>8</td>
<td>120 GB</td>
<td>50 GB</td>
</tr>
<tr>
<td>1,000,000</td>
<td>32</td>
<td>8</td>
<td>16</td>
<td>240 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td>2,000,000</td>
<td>64</td>
<td>16</td>
<td>32</td>
<td>480 GB</td>
<td>200 GB</td>
</tr>
<tr>
<td>2,000,000+</td>
<td>Consult</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Dimensioning considers a set of pre-configured rules. The calculations are estimated according to usual instances of the product. For high availability configurations, it is suggested to use instances with the same characteristics as those presented.

**Featured use cases**

- Management of user access and their personal information.
- Secure VPN: secure access to virtual private networks.
- Virtual token: One-Time Password management.

**Other VU™ Products that enhance VU™ Application Server**

Our solutions are integrated to offer a 360 experience for both users and organizations. Each solution contributes a fundamental aspect to the security strategy.

- VU™ Voice Recogn
- VU™ Sign
- VU™ Face Recogn
- Secure Onboarding Process
- VU™ Fraud Analysis
- VU™ Comm

If you need more information or would like to schedule a demo of this solution, please contact us at corporate@vusecurity.com