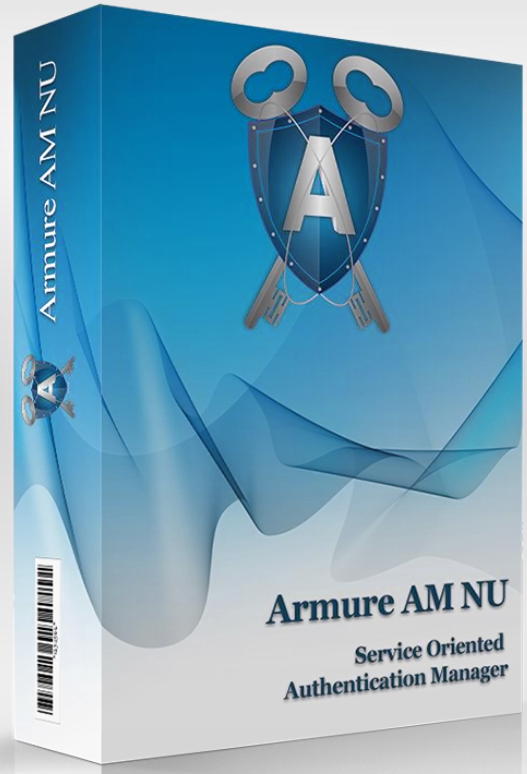
Armure AM



Service Oriented

Authentication Manager

NU edition

- Pluggable
- Standards Based
- Micro Services
- On Demand Scaling

A chain is as strong as its weakest link. A system is as secure as its most vulnerable piece. Don't let a weak authentication mechanism break your system security. Authentication managers provide strong authentication support in a layered manner at the application infrastructure level.

"The U.S. Government's National Information Assurance Glossary defines strong authentication as layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information."

The above definition is consistent with that of the European Central Bank, as discussed in the strong authentication entry.

What is Armure AM?

Armure AM is a service oriented authentication manager that allows you to setup a **strong authentication infrastructure**.

Armure AM integrates with variety of user repositories over number of protocols; once integrated **you can define authentication policies and enforce multi-factor authentication using one time password (OTP) and PKI certificates.**

Armure AM Key Features

Token based 2-factor authentication

Armure AM provides OTP support using OATH complaint hard/soft tokens; standards based tokens promotes vendor independence.

- Time-based OTP (TOTP) Hard/Soft Tokens
- Counter-based OTP (HOTP) Hard/Soft Tokens
- SMS and EMail Tokens
- Additional channels such as IVR can be implemented as an add-on

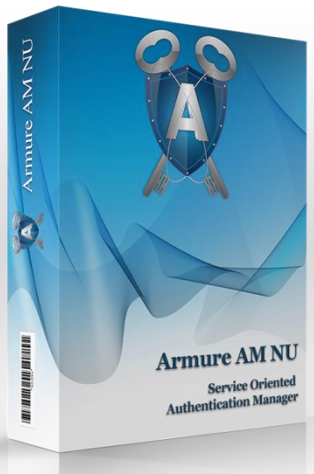
Support for soft token helps reduce cost and management overheads of hard tokens.

Multi-Protocol Support

Pluggable protocol handlers provide extensible support for multiple client channels. RADIUS protocol support helps implement AAA security protocols. Using standard RADIUS server Armure AM supports OTP for VPN, SSH and PAM access control.

User Repository Integration

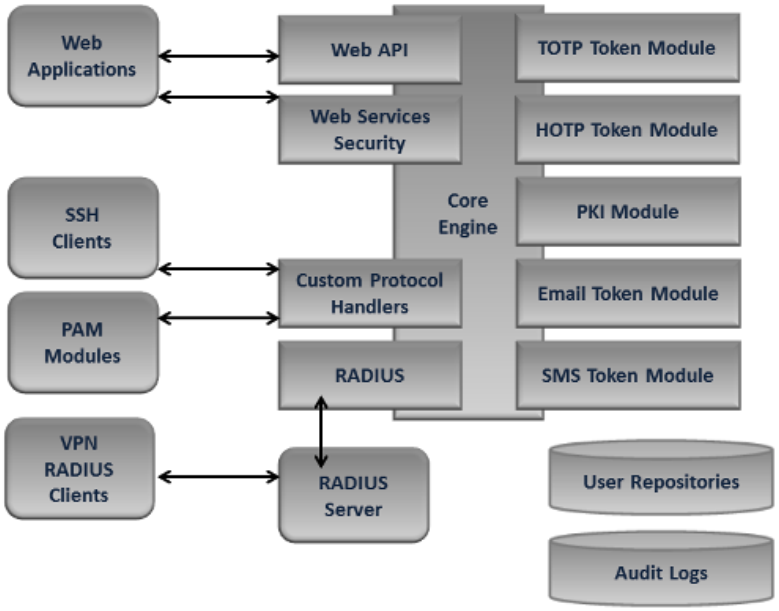
Armure AM provides plugins to integrate enterprise user repositories. Standard plugins provide support for LDAP and Database based user repositories. Plugin modules allow support for custom user repositories.



Why Armure AM?

Security landscape keeps evolving with discovery of new vulnerabilities and implementation of respective defense mechanisms. Your security infrastructure should be responsive and agile to enable you to keep pace with the landscape evolution.

Armure AM brings the required responsiveness and agility to your application authentication infrastructure. Built on OSGI platform, Armure AM leverages the framework plug-ability and implements authentication components as micro-services. OTP, protocol handlers and related functionalities are implemented as OSGI bundles.



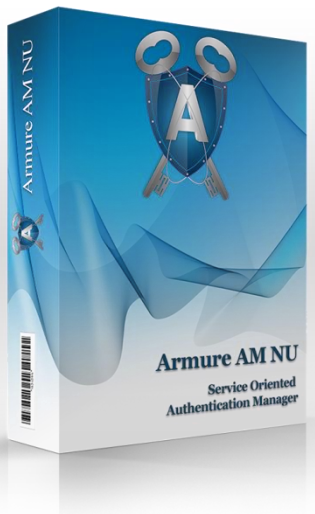
Armure AM design is based on the OATH reference architecture 2.0.

Armure AM design is based on OATH Reference Architecture 2.0.

Key design principles of the Armure AM architecture:

- **Pluggable architecture**
- **OATH Standards based**
- **Micro services framework design**
- **Scalable performance**

Armure AM is implemented on OSGI platform. All the components are implemented as OSGI bundles. The design allows update of existing bundles or deployment of new bundles at runtime.



Interested!

For further details please contact us:

Simplified IT Solutions

Regus Business Centre Mumbai, Level 15, Dev Corpora, Pokharan Road No.1, Eastern Express Highway, Thane (West), 400 601

Phone: 6700 4855

Website: www.simplifyit.in

Email: contact@simplifyit.in

UAE Operations:

1201, West line baqala/Venicia Laundry Building, Near Hotel Dana, Behind Colours Hypermarket, Electra Steer, Abu Dhabi,

United Arab Emirates

United States Operations:

One Lincoln Center, 18W140 Butterfield Road, Oakbrook Terrace, Suite 1500, Oak Brook, Illinois, 60181

Website: www.armureauth.com