

EMPOWERING ORACLE ACCESS MANAGER™ WITH TRICIPHER STRONG AUTHENTICATION

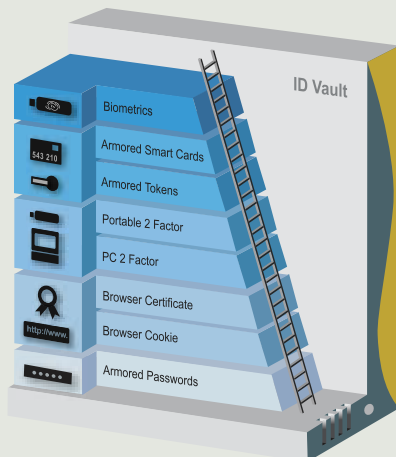


TriCipher Armored Identity Management integrated with Oracle Access Manager is a unified authentication and identity management infrastructure that protects sensitive information, valuable resources and critical applications from fraud and identity theft by issuing and managing a variety of secure, easy to use, and low cost credentials.



Benefits

- Protects Information, Resources and Applications from Man-In-the-Middle and Man-In-the-Browser attacks.
- Adapt authentication strength according to each application risk without disruption.
- TriCipher Authentication Ladder provides a range of strong authentication options that are more secure, easier to use, and lower cost than existing cookies, tokens, smart cards, and biometrics.
- Achieve Compliance quickly and stay compliant over time as regulations require stronger authentication.



The Problem

Businesses issue online credentials to verify their customers' identities. Once verified, Identity Management (IdM) and single sign-on (SSO) systems manage user access to confidential information, critical applications and allow them to conduct important transactions with a single credential. The ability to access many resources using a single credential has tremendous business benefits but it also dramatically increases the consequences if that credential is stolen by an attacker. Unfortunately, IdM and SSO systems often rely on weak authentication methods such as passwords, cookies, or one time password (OTP) tokens that are easy to defeat.

Before providing user access through an IdM or SSO system, it is critical to be certain of the user's identity. Without strong user authentication, attackers can steal the user's credentials and sensitive information, misappropriate valuable resources or compromise critical business applications.

ORACLE®

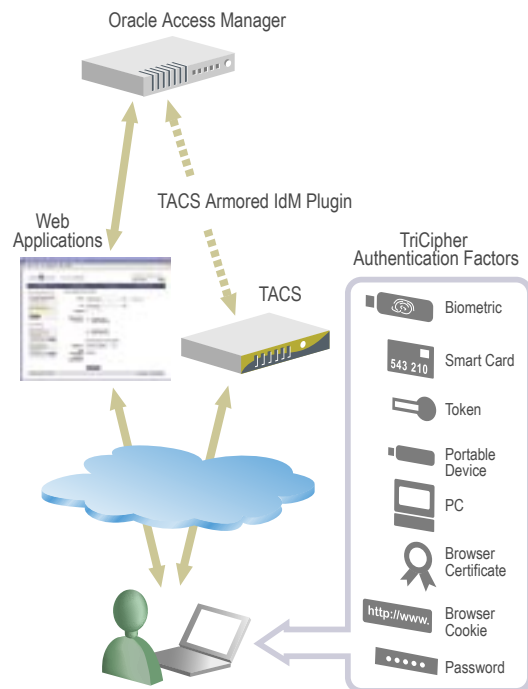
 **TRICIPHER**
Protecting Online Identity™

What Makes TriCipher Different?

The existing options for authentication and fraud prevention such as passwords, cookies, pictures and tokens have been proven inadequate by fraudsters, while stronger forms of authentication such as traditional Public Key Infrastructure (PKI), Smart Cards, and Biometrics have failed to realize their potential because they are difficult to use and deploy, and simply cost too much to make business sense. Everyone, including customers, online businesses, and government regulators recognize the immediate need to move beyond passwords to an easy to use, secure, and low cost system that will prevent fraud and identity theft. The TriCipher Armored Identity Management is the only unified authentication infrastructure that can provide a secure, easy to use and low cost authentication system that seamlessly integrates strong authentication with Oracle Access Manager. TriCipher provides more effective security than traditional PKI, is as easy to use as entering a username/password and has a low cost per user and transaction.

How Does it Work?

TriCipher Armored Identity Management integrates into Oracle Access Manager without requiring any changes to the customer applications. The TriCipher patented multi-part credential provides unparalleled protection of a user's online identity while maintaining the familiar user experience of entering a username and password. One part of the TriCipher credential is generated on the user's computer and the other portion is stored on the ID Vault appliance. To successfully authenticate, both parts of the credential must be combined, making it virtually impossible for an attacker to steal the entire credential and log into an account to commit fraud or identity theft. With the secure multi-part credential as the foundation, the TriCipher Authentication Ladder integrates a range of authentication factors including passwords, browser cookies/certificates, PCs, portable devices, tokens, smart cards and biometrics to provide a complete authentication system.



With Oracle Access Manager protected applications, the TriCipher TACS ID Vault is used to store and validate the instance of the userID and the second factor.

When a user begins access to an Oracle Access Manager protected application, based on the authentication factor required for strong authentication, the user is mutually identified either using a confidence image and text or using mutual SSL (digital certificates). Once the users' second factor is validated by TACS, the TriCipher integration plugin to Oracle Access Manager then authenticates and authorizes to Oracle Access Manager and gets the Oracle Access Manager single sign-on cookie, and sets the cookie on the user's browser, redirecting them to the originally requested destination page. In this manner, the login process to Oracle Access Manager protected applications is preserved and users are granted the "keys to the kingdom" after strong authentication.

Summary

The combined TriCipher and Oracle Access Manager™ solution gives organizations powerful and flexible strong authentication capabilities delivered within a single administrative infrastructure. TriCipher's flexible authentication factors and unique credential management features provide a highly secure method of credential management that dynamically evolves with changing user roles, entitlements and application services.

For more information on Oracle Identity Management solutions, visit www.oracle.com/identity.

Disclaimer: When Oracle conducts partner integration and testing, we verify only that the software integration functions according to the partner's proposed integration plan, and that it makes appropriate use of Oracle components and integration technologies in the environment specified in the published Integration Datasheet. Customers are solely responsible for the selection of all third-party software, including any integration software, used in conjunction with Oracle Identity Management and for the results of such use.

TriCipher and TriCipher Armored Credential System are either registered trademarks or trademarks of TriCipher, Inc. Oracle is a registered trademark of Oracle Corporation. All other trademarks are the property of their respective owners.



TriCipher Headquarters:

750 University Avenue, Suite 100
Los Gatos, CA 95032
Phone: +1.650.372.1300
Fax: +1.650.376.8301

TriCipher US sales:

Email: sales@tricipher.com
Phone: +1.650.376.8326
Fax: +1.650.372.1301

TriCipher EMEA sales:

Email: sales@tricipher.com
Phone: +44 (0) 1223 451075
Fax: +44 (0) 1223 451100