

TRICIPHER ARMORED VPN



TriCipher Armored VPN provides a strong authentication solution for SSL VPNs that cuts remote access authentication costs by 85% or more, simplifies the end user experience and protects against attacks that compromise one time password (OTP) Tokens.



“By 2008, Secure Sockets Layer virtual private networks will be the primary remote-access method for more than two-thirds of business teleworking employees, more than three quarters of contractors and more than 90% of casual employee access (0.8 probability).”

*Gartner, Inc.
“Magic Quadrant for SSL VPN, North America, 3Q06”
by John Girard
December 27, 2006*

The Problem

Enterprises are moving towards Secure Socket Layer (SSL) Virtual Private Networks (VPN) as the method of choice for providing remote access to their employees, business partners and contractors. While using web browsers for remote access to the enterprise has tremendous usability and cost benefits, putting a remote access portal on the public Internet can also introduce a vulnerable entry point into the enterprise network. If an SSL VPN relies on a username and password to authenticate users, hackers targeting enterprise users can steal the user's password and gain unauthorized access to the enterprise networks. However, existing options for providing two factor authentication such as OTP Tokens are costly to operate, hard to use, and can be easily circumvented by man in the middle attacks. Enterprises need to provide strong authentication to protect remote access but require a lower cost, easier to use, and more secure alternative to OTP Tokens.

The TriCipher Solution

The TriCipher Armored Credential System (TACS) provides a strong authentication solution for SSL VPNs that can cut remote access authentication costs in half, prevent attacks that compromise passwords and OTP Tokens and is as easy to use as entering a username and password.

- On-boarding
- Deployment
- Replacing devices
- Temporary access
- Out of synch troubleshooting

What Makes TriCipher Different?

TriCipher Armored VPN provides a secure, easy to use, and low cost authentication for SSL VPNs with the flexibility to choose authentication factors:

Low Cost

TriCipher provides unparalleled levels of authentication strength at a fraction of the cost of OTP Tokens. Instead of purchasing dedicated hardware authentication devices that must be integrated, provisioned, inventoried, managed and replaced, TriCipher's solution enables strong credentials to be self-provisioned and self-activated as software on a PC or on portable devices that users already carry, such as USB smart drives or other removable media. TriCipher Armored VPN also leverages standards that are built into virtually every SSL VPN (client SSL) and web browser (CAPI, PKCS#11) to eliminate integration steps, lowering implementation and maintenance costs.

Easy to Use

The TriCipher interface is simple, appears automatically only when users need to authenticate and doesn't change the familiar experience of entering a username and password. Conversely, OTP Tokens, biometrics and smart cards require customers to deal with new security concepts involving constantly changing "passcodes", drivers and readers that require education.

In addition, users can self-provision their ID Tool ToGo by downloading and installing it on any off-the-shelf USB drive. Self-provisioning makes it easy for users to get remote access up and running without waiting for a Token or smart card in the mail.



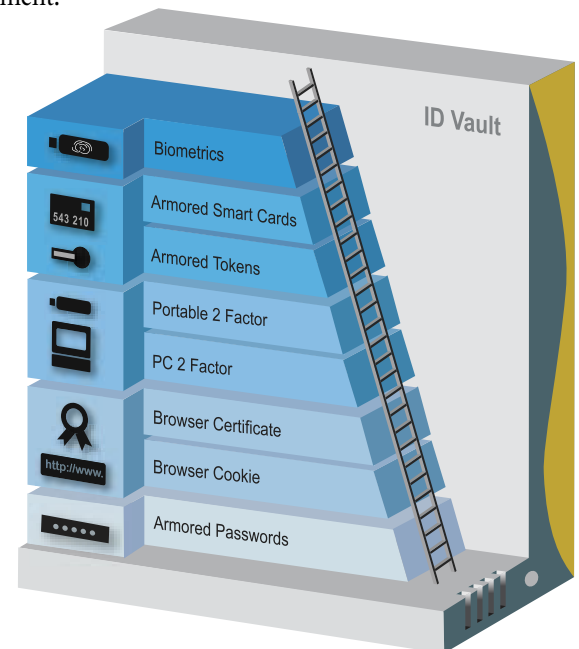
The TriCipher ID Tool ToGo is the first secure, easy to use, and low cost strong authentication device that can be self-provisioned to an existing USB Smart Drive.

Secure

OTP Tokens are vulnerable to theft of users' credential by Trojans, Keystroke loggers, Pharming, Man in the Middle and Man in the Browser attacks. The TriCipher ID Vault appliance (FIPS 140-2 Level 2) uses strong PKI-based multi-part credentials in combination with two-way SSL to prevent the theft of credentials.

TriCipher Authentication Ladder™

TriCipher's Authentication Ladder™, part of the Armored VPN solution, gives enterprises the flexibility to choose a variety of authentication factors including passwords, PCs, portable devices (USB, removable media), tokens or smart cards. Once installed, the TriCipher Authentication infrastructure can be leveraged for a variety of other applications in the enterprise, including internal and external portals, digital signatures and encryption key distribution and management.



How Does it Work?

The TriCipher's Strong Credential

The TriCipher patented multi-part credential provides unparalleled protection of a user's credential while maintaining the familiar user experience of entering a username and password. One part of the TriCipher credential is derived 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 used in combination without sending either part over the Internet, making it virtually impossible for an attacker to steal the entire credential to gain unauthorized access to the SSL VPN.

User's Login Experience

For the end user, logging in with TriCipher Armored VPN is as simple as entering a username and password into the TriCipher ID Tool, which appears automatically when users go to the SSL VPN login page. The ID Tool can be installed either on the user's computer or, for mobile users, delivered on a USB drive or other removable media.

Self-Service Portal

The TriCipher Armored VPN Self-Service Portal dramatically reduces the cost of deploying and operating strong authentication for remote access by automating or eliminating the process of on-boarding, deployment, replacement of lost devices, temporary access and troubleshooting out of synch OTP Tokens.

On-boarding

TriCipher's Self-Service Portal enables users to request remote access through a simple web page, automatically initiates the approval process and sends the user instructions for activating their credential without the need to call the IT department.

Deployment

TriCipher dramatically simplifies strong authentication deployment by enabling users to self-provision Armored VPN PC or Portable credentials to existing computers, USB Drives or removable media without ever needing to ship anything. If the company wants to send users a pre-installed USB Drive for authentication, the cost is significantly lower than OTP Tokens because there is no need to provision a seed to the device and match a specific OTP Token to a specific user.

Replacing Lost Devices

The TriCipher Self-Service Portal has a web page to report lost devices and users can immediately download and activate a replacement credential to their PC or to an off-the-shelf USB Drive. Also, TriCipher credentials don't have battery failures or expire on a regular basis lowering the number of users who need replacements.

Temporary Access

Should a user require temporary access without their TriCipher credential, users can click on a link below their login and answer security questions and/or have a temporary access code sent to a registered phone number. With OTP Tokens, users who don't have their Token have to call the helpdesk to get temporary access.

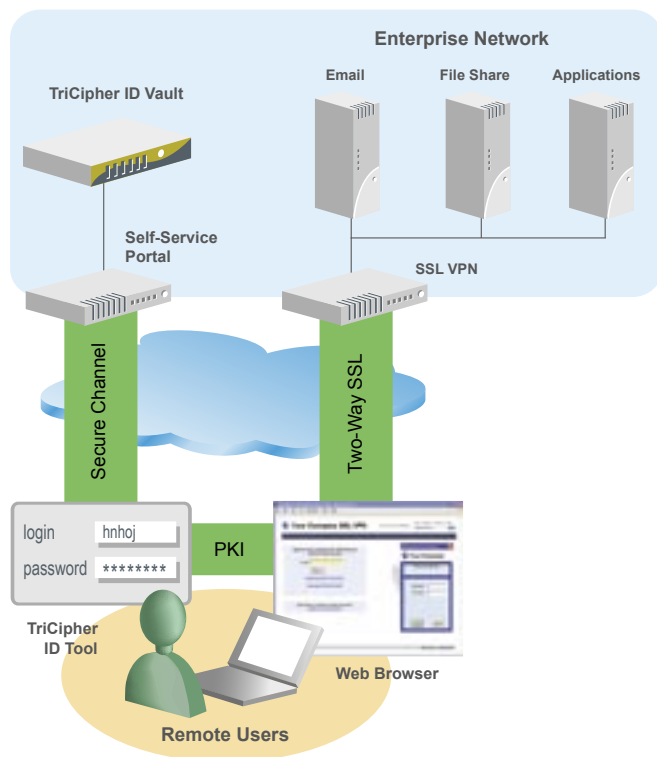
Out of Synch

TriCipher's patented credentials are PKI-based and don't require any synchronization of time or events between the authentication device and the server. OTP Tokens become out of synch with their server when exposed to extreme temperature (time-synchronous) or if the button is pressed too many times (event-based), causing user logins to fail and triggering a helpdesk cost.



SSL VPN Integration

To implement Armored VPN, the SSL VPN administrator simply needs to turn on client SSL on the SSL VPN, trust the TriCipher ID Vault as a Certificate Authority (CA) and provide users with the TriCipher ID Tool either as a software on their PC or on a portable device such as a USB smart drive (ID Tool ToGo).



Features

Self-Service Portal

TriCipher's Self-Service Portal enables users to request remote access through a simple web page, automatically initiates the approval process and sends the user instructions for activating their credential without the need to call the IT department.

TriCipher Multi-part Credential

TriCipher's patented multi-part credentials generate one part of the credential on the user's PC and store the other part on the ID Vault appliance, making the credential virtually impossible to steal.

ID Tool ToGo

TriCipher ID Tool ToGo provides a portable TriCipher credential that can be pre-provisioned by the company or self-provisioned by a user on a USB drive or other removable media.

Temporary Access with Secondary Authentication

TriCipher Armored VPN provides secondary authentication when users need temporary access to VPN without their TriCipher credential using integrated knowledge based authentication (KBA), SMS one time password (OTP), and voice OTP.



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: +1.650.376.8301

TriCipher EMEA sales:

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