

TRICIPHER SOLUTIONS BRIEF: SSL VPN



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



“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 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.

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. Unlike legacy Internet Protocol Security (IPSEC) VPNs, SSL VPNs authenticate users and encrypt traffic using the SSL protocol that is built into the Internet, taking advantage of user's familiarity with web browsers. SSL VPNs are also an ideal solution for quickly providing remote access to a large number of users in emergency situation such as a pandemic, natural disaster, or terrorist attack.

While using web browsers for remote access to 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 uses weak legacy authentication credentials such as passwords or OTP Tokens, hackers targeting enterprise users with Trojans, Keystroke Loggers, Man in the Middle, or Man in the Browser attacks can easily steal the credential and gain unauthorized access to the enterprise networks. These attacks work because SSL VPNs only use one-way SSL (i.e. server only), which authenticate the SSL VPN server to the user.

To effectively protect SSL VPNs from attacks targeting their login credentials, enterprises need to increase the security of their user credentials to provide strong two-way SSL authentication (i.e. client and server). However, total cost of hardware, provisioning, and user education costs of existing OTP Tokens or smart cards using traditional Public Key Infrastructure (PKI) are too expensive to make business sense.



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.

Benefits

- Reduces cost of authenticating remote users
- Prevents attacks that defeat password and OTP Tokens
- Increases flexibility of authentication factors
- Enables self-provisioning and self-activation in the field supporting disaster recovery scenarios (natural disaster, pandemic, terrorist attack)

What Makes TriCipher Different?

TACS 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 or smart cards. Instead of purchasing dedicated hardware authentication devices (tokens or smart cards) that must be integrated, provisioned, inventoried, managed and replaced, TriCipher's patented multi-part credential enables strong credentials to be self-provisioned and self-activated as software or on portable devices that users already carry such as USB smart drives or iPods. TACS 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 smart 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.



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

TriCipher and TriCipher Armored Credential System are either registered trademarks or trademarks of TriCipher, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners.

Secure

Weak user credential such as passwords and 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 user credentials in combination with two-way SSL to prevent the theft of credentials.

Flexible Authentication Options

TriCipher's Authentication Ladder™ gives enterprises the flexibility to choose a variety of authentication factors including passwords, PCs, portable devices (USB, iPod), tokens or smart cards.

How Does it Work?

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 combined, making it virtually impossible for an attacker to steal the entire credential to gain unauthorized access to an SSL VPN.

To implement TACS, 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 plug-in or on a portable device such as a USB smart drive (ID Tool ToGo).

When a user attempts to login to a web application with cardholder data, the TriCipher ID Tool is invoked automatically, and the user is prompted to authenticate himself to the ID Vault by entering his username and password. Once authenticated with the TriCipher ID Vault, the web browser communicates the digital certificate needed to login to the SSL VPN using two-way SSL.

