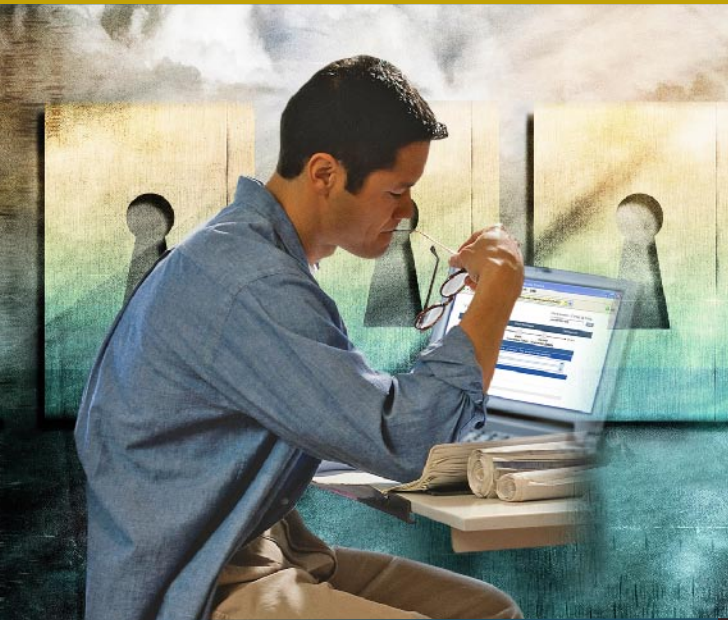


TRICIPHER SOLUTIONS BRIEF: ONLINE BROKERAGE



TriCipher provides strong credentials for online brokerage customers that enable brokerages to securely authenticate users, protect transactions and digitally sign documents.



“The attacks, which took place during the last three months, were launched by identity thieves in Eastern Europe and Asia who primarily used keylogging software delivered via Trojan horses or other malware to steal users’ confidential information. The hackers then logged into existing customer accounts - or created dummy accounts - to buy shares in little-traded stocks, driving prices up so they could sell their own previously purchased shares for a profit.”

*Eric Lai
Computer World*

The Problem

While online banks have received the most attention from the press and regulators (FFIEC), identity thieves and fraudsters have been attacking the online brokerages, which have more assets to plunder and can be used as part of “pump and dump” schemes that are more difficult to unravel. In October 2006, hackers broke into accounts at two large U.S. brokerages to execute fraudulent trades, manipulating stock prices in a “pump and dump” scheme. The attack caused \$22 million in losses to the brokerages and negative press exposure. With attackers consistently targeting online brokerage customers, online brokerages must implement stronger authentication to prevent fraud, protect their customers’ identities and increase confidence. If the industry does not proactively address the security of online brokerages, the Securities and Exchange Commission (SEC) will likely step in to mandate strong authentication as the FFIEC did for the online banking industry.

The TriCipher Solution

The TriCipher Armored Credential System (TACS) is a unified authentication infrastructure that protects online identities from fraud and identity theft by issuing and managing a variety of secure, easy to use, and low-cost credentials.

TriCipher’s strong credentials enable online brokerages to authenticate users, verify transactions and digitally sign documents. TriCipher strong user authentication ensures that the brokerage can verify each customer’s



The TriCipher Solution (continued)

identity; at the same time, customers can be assured that they are connecting to the legitimate brokerage website. TriCipher's Armored Transactions ensure that the any transaction the user submits on the online brokerage website isn't modified without the user's knowledge by a Man in the Middle or Man in the Browser attack.

TriCipher's document signing functionality enables customers to digitally sign documents such as new account application, 401K rollovers, 529 education savings account applications that currently required notarized signatures. With TriCipher, online brokerages can protect their customers, increase consumer confidence, and accelerate growth of the online channel.

Benefits

- Prevents ID Theft & Fraud
- Enables document signing
- Builds Consumer Confidence
- Grows the Online Channel

What Makes TriCipher Different?

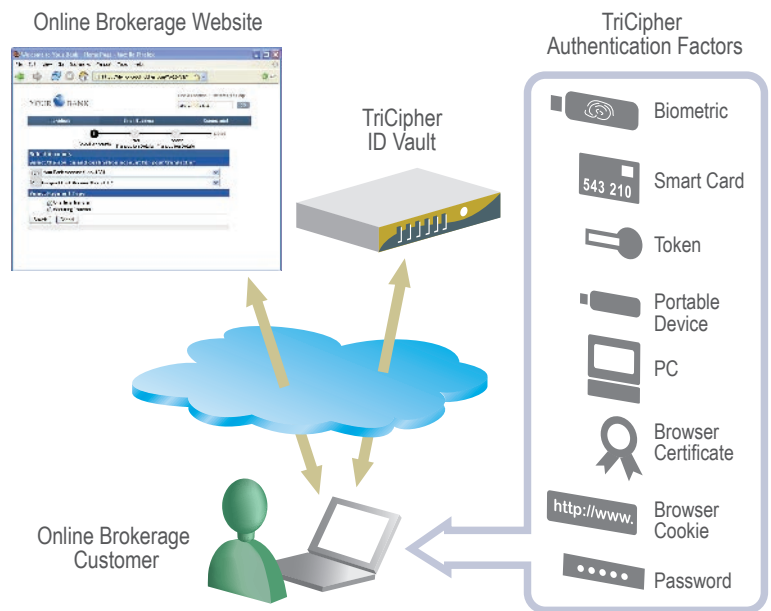
Existing options for establishing online identities such as passwords, cookies, pictures, and tokens have been proven inadequate by fraudsters, while stronger forms of authentication, such as traditional PKI, smart cards, and biometrics, have failed to realize their potential because they are difficult to use and deploy, and simply cost too much to make business sense. Everyone, including customers, online businesses, and government regulators, recognizes the immediate need to move beyond passwords to an easy-to-use, secure, and low-cost system that will protect against fraud and identity theft.

The TriCipher Armored Credential System (TACS) is the only unified authentication infrastructure that provides a secure, easy-to-use and low-cost authentication system for online brokerages. TACS provides more effective security than traditional PKI, is as easy to use as entering a username/password and has a low cost, both per user and per transaction.

How Does it Work?

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 a would-be attacker to steal the entire credential to 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.

The TriCipher ID Vault appliance is a FIPS 140-2 Level 2 rated appliance that securely manages user information, digitally signs transactions, and authenticates users as part of the TriCipher Armored Credential System (TACS). The TriCipher Armored Credential System (TACS) can be implemented using both a zero-footprint user experience and a ID Tool plug-in. The zero-footprint user experience provides basic multi-factor authentication using passwords, browser cookies and/or browser certificates, combined with a personalized confidence image and text. The ID Tool plug-in option provides strong mutual authentication that can authenticate users and transactions and digitally sign documents.



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