

# TRICIPHER ARMORED CREDENTIAL SYSTEM (TACS)



The TriCipher Armored Credential System (TACS) is a unified authentication infrastructure that protects online identities from fraud and theft, builds customer confidence, and drives online channel growth.



*“We looked at numerous solutions and only the TriCipher Authentication Ladder enabled us to deploy and centrally manage many authentication strengths matched to different user risk profiles, and adjust authentication strength over time as needed.”*

*This mix of security and flexibility is an example of our commitment to protect our clients against online fraud in a very cost-effective method.”*

*Brian Hurdis  
Senior Executive Vice President, Chief Information and Privacy Officer Metavante Corporation*

## The Problem

Today, customers and businesses use their online identities to access confidential information and conduct important transactions. However, businesses are trusting customers based on insecure password credentials and customers have no reasonable way of knowing if they are dealing with a legitimate business or a fraudulent website. The result is rampant identity theft, Phishing and fraud that undermine confidence in the on-line channel. As new attacks defeat existing authentication methods and regulatory requirement increase, businesses are forced to choose between exposing their customers and responding to the threats with a new type of authentication that disrupts their users and infrastructure.

Authentication Method	Phishing 2004	Pharming 2005	MITM 2006	MITB 2007
Transaction Authentication	YES	YES	YES	YES
Smart Card + PKI	YES	YES	YES	NO
Software PKI	YES	YES	YES	NO
Tokens, Grid/Scratch Cards	YES	YES	NO	NO
Cookie, Text, Picture	YES	Maybe	NO	NO
IP Geo, Device Fingerprint	YES	Maybe	NO	NO
Password	NO	NO	NO	NO

YES Prevents the Attack  
NO Does not Prevent the Attack  
Maybe Depends on the Level of Sophistication

## Example Scenarios

### Online Banking

#### *Fraud and Identity Theft in Online Banking*

Online bank accounts have become a prime target for organized crime groups trying to commit online fraud and steal customers' identities. Attackers have developed a variety of methods to steal user passwords, security questions and identity information. Typically, fraudsters steal the user's credential, log into their account, empty the bank account and/or steal identity information to open new accounts in the customer's name. As Banks have deployed fraud detection systems and weak authentication methods such as cookies with personal security images, device fingerprinting and tokens, attackers have improved their methods to defeat new authentication methods. TACS prevents fraud and identity theft by providing banks with a secure, easy to use, and low cost authentication system that prevents Phishing, Pharming, keystroke logging, man in the middle and man in the browser attacks.

*"A single high-profile incident that is picked up by the major news media could instantaneously turn a significant number of online banking users back into check-writers who frequent bank branch teller windows. Even worse, the reputation damage could ruin a bank's entire franchise."*

George Tubin  
TowerGroup

### Online Brokerage

#### *Modifying a Stock Transaction to Manipulate a Stock Price (Pump & Dump)*

In October of 2006, hackers broke into accounts at two large U.S. brokerages to execute fraudulent trades in order to manipulate stock prices in a "Pump and Dump" scheme. The attack caused \$22 million in losses to the brokerages and negative press exposure. TriCipher's strong user and transaction authentication would have prevented the fraudsters from gaining access to the user's accounts and/or manipulating individual transactions.

*"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 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.

### Benefits

- Prevents ID Theft & Fraud
- Builds Consumer Confidence
- Grows the Online Channel
- Achieves Compliance (FFIEC, PCI, HIPAA)

### What Makes TriCipher Different?

The 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 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 Credential System (TACS) is the only unified authentication infrastructure that can provide a secure, easy to use and low cost authentication system for Business to Business and Business to Consumer web applications. TACS 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?

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 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.

## TriCipher ID Vault Appliance

The TriCipher ID Vault appliance is a FIPS 140-1 Level 2 rated appliance that securely manages user information, digitally signs transactions, and authenticates users as part of the TriCipher Armored Credential System (TACS). As the foundation of TACS, the ID Vault stores one part of every user's credential while the other portion is generated on the user's computer by the ID Tool plugin, making it virtually impossible for an attacker to steal the entire credential to log into an account to commit fraud or identity theft. The ID Vault integrates TriCipher's Authentication Ladder technology, which provides a range of authentication methods including passwords, browser cookies/certificates, PCs, portable devices, tokens, smart cards and biometrics.

**The TriCipher Authentication Ladder** enables businesses to provide a variety of authentication strengths to different types of users and web applications from a single unified authentication infrastructure.

When regulatory requirements or threats increase, businesses can easily move up the Authentication Ladder to provide more security to their users and applications without disrupting the user or the company's infrastructure.

## TriCipher Authentication Gateway (TAG) Appliance

As an integral part of the TriCipher Armored Credential System (TACS), The TriCipher Authentication Gateway (TAG) acts as a services layer for web applications. The TAG reduces the time to deploy strong authentication, increases authentication performance, and ensures the security of the login process by providing a single standardized strong authentication service for use by every application within an organization.

The TAG manages the authentication for every level of the TriCipher Authentication Ladder including passwords, browser cookies/certifications, PCs, portable devices, tokens, smart cards and biometrics to provide a unified authentication infrastructure. When users log into any web application, they are handed off to the TAG to manage the entire authentication process and verify the credentials of each user with the ID Vault. Once authenticated through the ID Vault, the TAG delivers the authentication results to the web application so that the user is given the appropriate level of access.

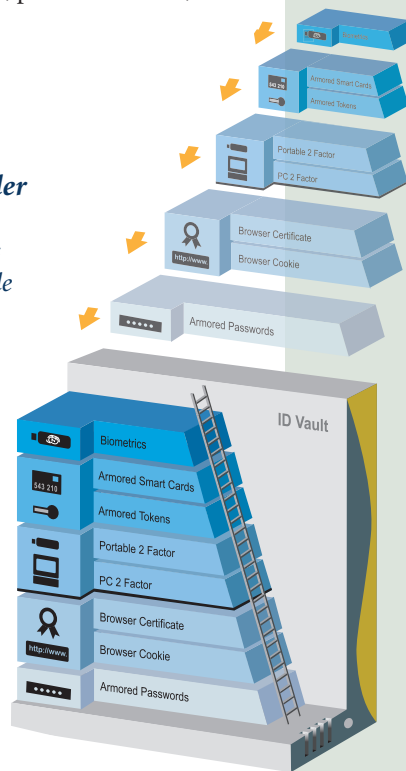
## Online Personal Health Records

Healthcare organizations are moving patient records online to lower the costs of maintaining paper-based records and provide easy access to healthcare providers. However, moving patient records online exposes them to the emerging threat of medical identity theft or other improper use of patient medical information. In accordance with the Health Insurance Portability and Accountability Act (HIPAA), government regulators have issued security guidance to secure electronic protected healthcare information (EPHI) that recommends implementing two factor authentication to access systems containing EPHI and strong encryption of EPHI when it is stored. TriCipher's multi-factor authentication system provides a secure, easy to use, and low cost solution for protecting online personal health records.

*"Medical identity theft—in which fraudsters impersonate unsuspecting individuals to get costly care they couldn't otherwise afford—is growing..."*

*And this isn't petty larceny. Experts note that while individuals who have had their credit-card data stolen are usually wrangling with their banks over losses of as little as a few thousand dollars, medical ID theft can leave victims, and the doctors and hospitals that provided the care, staring at bills that are exponentially higher."*

*Diagnosis: Identity Theft  
Business Week, January 8th, 2007*



## Flexible User Experience: Zero-Footprint and ID Tool Plug-in

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, digitally sign documents and encrypt email. The ID Tool plug-in integrates a variety of authentication options including PCs, portable devices, tokens, smart cards and biometrics. When a user attempts to login to an online application, sign a document, or encrypt/decrypt email, ID Tool is invoked automatically, and the user is prompted to authenticate himself to the ID Vault using a range of authentication factors including passwords, browser cookies/certificates, PCs, portable devices, tokens, smart cards and biometrics to provide a complete authentication system. One part of the TriCipher's patented multi-part credential is generated on the user's computer using ID Tool and the other portion is stored on the ID Vault appliance.

## TACS Features

### Multi-Part Credentials

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.



#### TriCipher Headquarters:

750 University Avenue, Suite 100  
Los Gatos, CA 95032  
Phone: +1.650.372.1300  
Fax: +1.650.372.1301

#### TriCipher US sales:

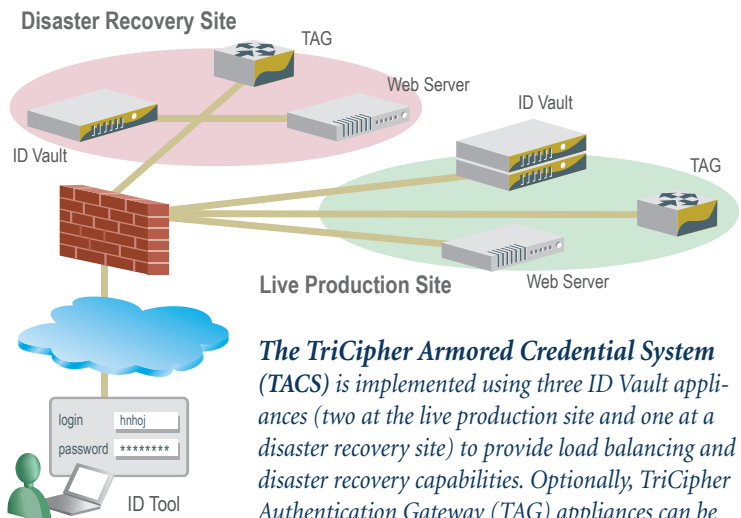
Email: sales@tricipher.com  
Phone: +1.650.376.8326  
Fax: +1.650.376.8301

#### TriCipher EMEA sales:

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

## TriCipher Authentication Ladder

With the TriCipher multi-part credential as the foundation, the Authentication Ladder integrates a variety of authentication methods including passwords, browser cookies/certificates, PCs, portable devices, tokens, smart cards and biometrics to provide a complete authentication system.



*The TriCipher Armored Credential System (TACS) is implemented using three ID Vault appliances (two at the live production site and one at a disaster recovery site) to provide load balancing and disaster recovery capabilities. Optionally, TriCipher Authentication Gateway (TAG) appliances can be used at both sites to speed deployment and quickly integrate with multiple web applications.*

## TriCipher Authentication Gateway

The TriCipher Authentication Gateway (TAG) enables organization to quickly integrate multiple web applications using Security Assertion Markup Language (SAML).

## TriCipher Armored Transactions

TriCipher Armored Transactions prevents man in the browser attacks that circumvent strong user authentication by authenticating each transaction, ensuring the integrity of the transaction and positively identifying the user submitting the transaction.

## Online Document Signing

Document signing enables businesses to increase revenue, improve customer satisfaction, and lower costs by eliminating paper-based signing requirements to do business online. TACS provides online document signing capabilities for Adobe Acrobat, Microsoft Word and other standards-based document applications using a single credential and user experience for both document signing and user authentication.

## Knowledge Based Authentication

TACS provides knowledge based authentication (KBA) workflows and data storage or can integrate with in-house or third-party KBA systems to provide integrated secondary authentication.

