



PROTECTING FINANCIAL SERVICES OUTSOURCING COMPANIES

Global outsourced investment processing and asset management firm delivers integrated risk based authentication and identity management to 1.5M end users with TriCipher and CA SiteMinder.®



OVERVIEW

Challenge	Solution	Benefit
<p>Deploy FFIEC compliant second factor authentication without disruption to user experience or infrastructure.</p> <p>Protect online services for a broad array of end user constituencies.</p> <p>Offer multiple authentication factors for varying levels of risk and application sensitivity.</p>	<p>TriCipher Armored Credential System (TACS) integrated with CA's SiteMinder identity and access management system deliver a unified authentication and identity management infrastructure that prevents fraud and theft, enables customers to meet changing business requirements with no impact to users or applications.</p>	<p>Combined strong authentication and web access management from a single environment.</p> <p>Protects identities and sensitive applications from fraud and theft.</p> <p>Empowers individual clients to define their own online services protection schema.</p>

COMPANY BACKGROUND

Investment processing outsourcing solutions serving private and institutional customers with a broad array of asset and wealth management applications and services.

5000 business unit customers supporting 1.5M end users and 8000 customer service and IT professionals across institutions.

Online treasury services for commercial customers as well as underwriting services for large corporations and financial institutions.

This leading global provider of outsourced asset management, investment processing and investment operations delivers innovative solutions that help corporations, financial institutions, financial advisors and affluent families create and manage wealth. They provide investment and fund processing services to investment managers, supporting a full range of investment products including mutual funds, hedge funds, private equity funds, and separately managed accounts.

Helping banks and trust institutions manage and process investments for their clients and helping independent investment advisors manage wealth for their affluent and institutional customers, their well defined strategy of providing a breadth of financial solutions to their customers - what they need, when they need them, and how they want them delivered - is the core to their success in the marketplace, the root of shareholder value, and remains their foundation for trillion dollar growth.

BUSINESS DRIVERS

Single strong authentication infrastructure to support multiple institutional customers.

Mitigate financial data access vulnerabilities and identity compromise.

Provide end users heightened security without personal intrusion.

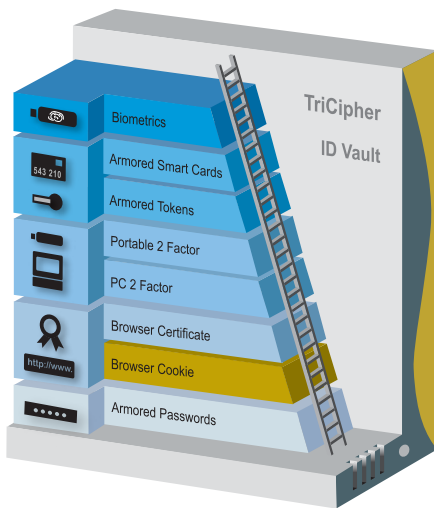
Extensible solution that will evolve in step with regulatory requirements.

The scope of this provider's highly sensitive institutional and corporate online services required a single strong authentication infrastructure capable of delivering a variety of authentication factors and strengths based on the risk levels of the services being accessed. Of utmost consideration was the requirement to provide an assured computing environment for both institutional customers and their end users - one that supported both access management and strong authentication in a highly scalable solution.

In addition to a requirement to meet FFIEC guidelines, the various institutions' end point users required assurance that their financial information and online sessions be safe without disrupting the convenience of their experience. Yet as each institution offers different services, they needed flexibility to deploy varying levels of authentication appropriate for their unique needs and do so with the ability to self-administer credential and identity management on an ongoing basis as their user base constitution and services evolve over time.

AUTHENTICATION SOLUTION

TriCipher Armored Credential System (TACS)



TriCipher's Authentication Ladder enables the Financial Services outsourcer to offer their customers a wide variety of authentication options to meet the varied business requirements of their private and institutional customers. As threats evolve and business requirements change, customers can increase their authentication strength without requiring any change to the infrastructure.

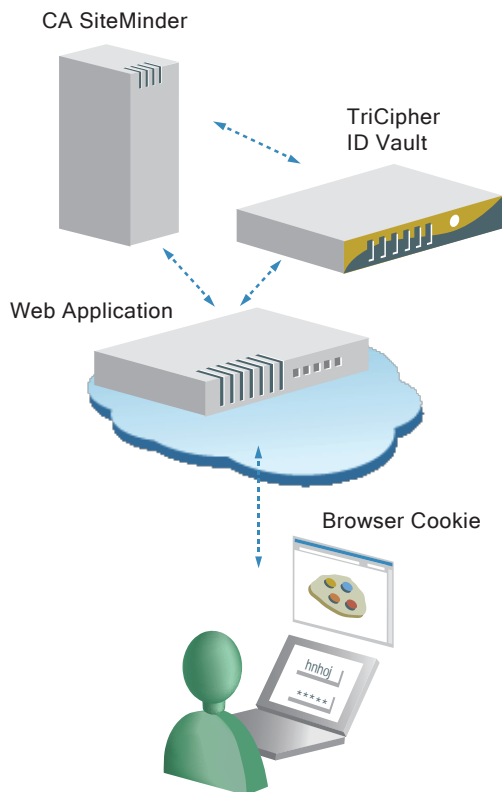
The TriCipher Armored Credential System (TACS) was chosen as a more flexible and more economical alternative to a previously installed one time password solution. With the capability to deliver multiple authentication factors from a single infrastructure, the TriCipher solution provides flexible choices in identity protection within a scalable architecture. In addition, the rich TACS API set provides a standard interface to multiple platforms providing authentication services across a heterogeneous environment of SiteMinder protected resources.

As a provider of various levels of value added services, the Financial Services outsourcer required a solution that would rapidly integrate to existing applications and management interfaces without disruption and that would empower their clients with the self-administered capability to define access policies and authentication schema for protection of sensitive personal and financial data most appropriate for each institution, as well as to provide optional tiers of authentication across the administration hierarchy. With TACS, the outsourcer is enabled its clients to achieve baseline FFIEC guideline requirements while offering an extensible means to add varying token levels as both application and user needs change over time.

At the outset, the outsourcer has deployed the Browser 2 Factor level of the TACS ladder enhancing login security beyond username and password without changing the user experience, or requiring any additional software at the user's desktop.

The second factor in this implementation is an encrypted, persistent cookie that contains the userid. Users also select personalized confidence images and text in order to authentication to the website on each access. Once verified to the authentic website, users then input their credentials. Once successfully logged in, users are access authorized by SiteMinder.

AUTHENTICATION, ACCESS & IDENTITY MANAGEMENT



With SiteMinder protected applications, the TACS ID Vault is used to store and validate the instance of the userid and the second factor within the encrypted cookie. When a user begins access to a SiteMinder protected application, a custom authentication scheme within the CA SiteMinder policy server redirects the user to a TriCipher web page (custom pages can be implemented with TriCipher APIs) which validates the second factor for the user, and requests the user's password.

The collection page takes the user's credentials, and userid, and passes a deviceid from the cookie along with the user's password, in an XML string format and submits the request to the TriCipher custom authentication scheme. The incoming request is validated against the TACS ID vault. If the authentication is successful, the custom authentication scheme provides assertion to SiteMinder of the valid authentication of the user.

The TriCipher page gets the SiteMinder cookie, and sets the cookie on the user's browser, redirecting them to the originally requested target page and login. In this manner, the login process to SiteMinder protected applications is preserved. Then, the userid and password can be validated through SiteMinder to apply the existing hierarchy of the SiteMinder authorization schemes specific to the user.

The Browser 2 Factor implementation provides an easy to use, non-disruptive multi-factor authentication solution that increases security beyond what is provided by passwords alone. As user credentials are stored on the TACS FIPS 140-1 Level 2 rated appliance, potential dictionary attacks against existing data stores are prevented.

BUSINESS BENEFITS

Multi-factor authentication infrastructure for less than the cost of single factor strong authentication solutions.

Reduction in liability and increased consumer and corporate trust drive market share improvements.

Self administration of credential, authentication, and entitlement management from a single infrastructure reduces overhead and provides individualized security on a per institution basis.

With a combined TriCipher TACS and CA eTrust SiteMinder[®] solution, the company is able to expand and evolve their web based offerings with complete protection of user identities and sensitive data, without platform constraint - a critical factor in continuing to deliver competitive offerings. Each of their client institutions are fully empowered with the ability to define and apply the data and identity protection schema most appropriate for their customer base and services.

With TriCipher's flexible authentication ladder, the outsourcer will be able to offer multiple forms of strong authentication by institution, by service, and by user class, all within a single infrastructure and all within a uniform access management environment - one that will gracefully accommodate new services while providing regulatory compliance.

TriCipher, Inc.
750 University Ave. Suite 100
Los Gatos, CA. 95032
650-372-1300
www.tricipher.com

 **TRICIPHER**
Protecting Online Identity™

©Copyright 2007, TriCipher, Inc. All rights reserved.