

PROTECTING GLOBAL FINANCIAL SERVICES COMPANIES

Global financial services company delivers secure services and protects identity of banking customers with TriCipher TACS and CA eTrust SiteMinder.®



OVERVIEW

Challenge	Solution	Benefits
<p>Provide immediate second factor authentication without disruption to end users.</p> <p>Provide choice in authentication factors for different classes of users and online services.</p> <p>Accommodate individual needs of institution administrators - evolve and scale with changes in service offerings and regulations.</p>	<p>TriCipher Armored Credential System (TACS) and CA's eTrust SiteMinder identity and access management system, deliver strong authentication and enhanced security for online financial services from a single infrastructure. With self administration capabilities for each subscribing institution, every user's identity and sensitive information is fully protected.</p>	<p>Protects an array of institutions and their customers from fraud and identity theft.</p> <p>Increases customer loyalty and confidence in using the online channel.</p> <p>Immediate FFIEC compliance with flexibility to apply a variety of authentication factors as both threats and regulatory requirements evolve.</p>

COMPANY BACKGROUND

Financial services company with outsourced asset management, investment processing and operations solutions.

Providing Internet delivered consumer and commercial banking applications.

Protected access by customer service and IT professionals across diverse range of investment advisors, trust institutions and banks.

This Global Financial Services company services wealth and investment management firms with a wide range of both consumer facing and corporate banking applications including account and financial management applications, bill pay and funds transfer applications, cash management applications, and investment decision applications. Addressing a broad end-user community, their customers constitute investment advisors, trust institutions and full service banks, all of whom have varying service and application protection needs.

For the customer service and IT professionals who provide end user administration and management support within this provider's customer community, the ability to rapidly deploy second factor authentication by FFIEC deadlines, and administer authentication factors by service and user type within their existing application and identity management infrastructure was crucial.

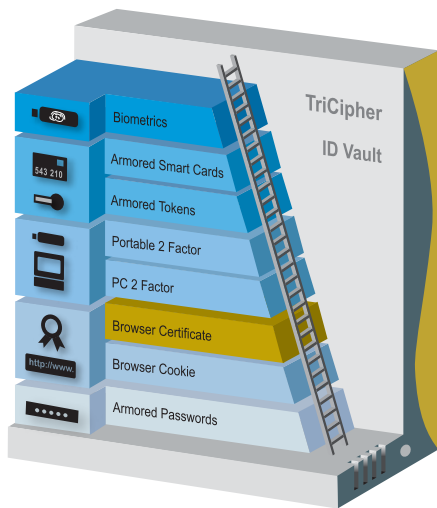
BUSINESS DRIVERS

Protect user identities and privacy across an array of online financial applications without impacting customer experience.

Deliver highly trusted services to institutional customers with authentication schema that can scale and evolve to guard against threats in the future.

Comply rapidly with FFIEC guidelines, and provide options to extend identity protection and access management as regulations and services evolve.

AUTHENTICATION SOLUTION



TriCipher's Authentication Ladder enables this global Financial Services company to offer their customers a wide variety of authentication options to meet the varied business requirements of their institutional customers and their end users. As threats evolve and business requirements change, each customer can increase their authentication strength according to the risks associated with the services being offered.

With highly sensitive applications delivered online, this global Financial Services company must at all times provide an assured computing environment - both for its financial institution customers, and their end users. With hundreds of institutions to service and hundreds of thousands of downstream end users, the solution chosen had to be scalable to meet current and future needs, provide choice in authentication factors, offer protection from existing and emerging threats, and provide a single infrastructure environment from which to administer identity and access management as well as strong authentication.

The company's commercial banking customers were looking for an array of strong authentication capabilities that could be assigned by the risk levels of specific applications and associated sensitive data. Self-administration was a key requirement, as was the ability to evolve authentication factor choices as compliance requirements evolve. And the company's customers needed heightened security and identity protection, without disruption to their normal user experience or invasion of privacy.

TriCipher Armored Credential System (TACS)

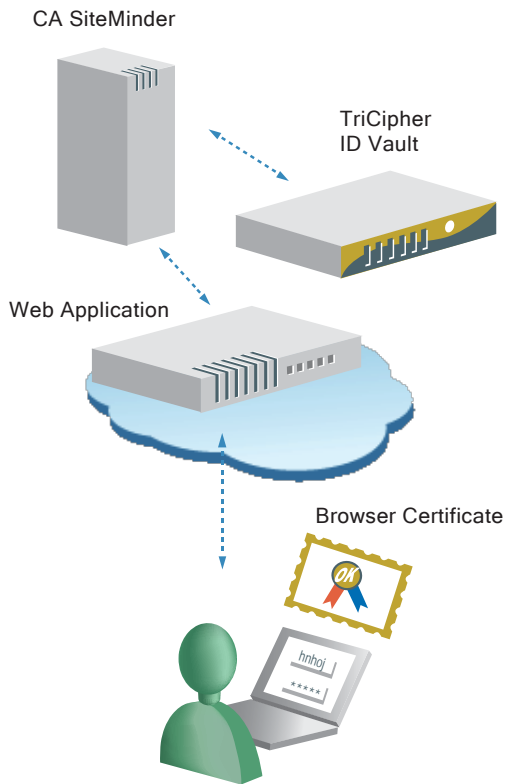
The global Financial Services company was looking for an authentication solution that would allow their customers' user administrators to select the authentication methodology most appropriate for their institution's needs. The cost and management hurdles to support multiple discrete authentication systems would be prohibitive. As a global provider, they needed a single solution that could offer multiple - and readily changeable - authentication factors, and one that would not incur disruption for either end users or administrators.

The TriCipher Armored Credential System was the ideal solution for their needs, offering a wide range of strong authentication options that can be deployed and managed from a single infrastructure. TACS allows each administrator to choose and apply authentication strength based on risk levels of the services being accessed, and based on user segments and entitlements.

Service quality and functionality are hallmarks for this provider, and because of the nature of services being offered, trust is the dominant factor in their relationship with their customers. The authentication ladder allows them to arm each of its customers with strong authentication within a CA eTrust SiteMinder® environment, exceeding compliance requirements yet without intruding into users' privacy or service experience.

The Browser Certificate implementation on the TACS authentication ladder was selected. With Browser Certificates, the company can offer a zero footprint second factor that will not be removed by the user or security software as is the case with cookie-based solutions. Within the SiteMinder environment, the TACS system is the certificate authority (CA). Using out of the box SiteMinder X.509 certificates, the Browser Certificate (B2F) implementation provides a second authentication factor to SiteMinder authentication schemes -- with no change to the SiteMinder authentication process.

AUTHENTICATION & ACCESS MANAGEMENT



The global Financial Services company wanted to provide immediate second factor authentication capabilities to its consumer facing wealth management applications to comply with year end FFIEC deadlines, Application access and Identity Management is provided through CA eTrust SiteMinder.® With a combined CA - TriCipher solution, the company enabled the user and service administrators for all of their customers to self administer user access rights, and two factor authentication within the SiteMinder environment.

Using client side mutual SSL enabled in the SiteMinder protected web login application, in conjunction with server side enabled SSL within the service applications, the TriCipher ID Vault is the intermediate certificate authority for SiteMinder protected applications.

When users login, their request is re-directed to a SiteMinder based credential page by a custom TriCipher authentication scheme resident in the SiteMinder policy server that is configured at a higher level of authentication than the existing SiteMinder application access authentication schemes. The userid and client certificate are retrieved after login to the credential page. The TriCipher authentication scheme ensures that the userid has previously authenticated and that the certificate matches. The certificate serial number is then extracted and matched with the certificate serial number in the TACS ID Vault, upon which a SiteMinder cookie is returned and the user is logged into their SiteMinder protected application.

With no change to a user's normal log in process, the combined CA - TriCipher solution adds a dependable second factor of authentication to existing SiteMinder authentication schemes, ensures that certificates are valid with separately stored certificate serial numbers, and allows customer administrators to assign second factor authentication based on risk and user segments and entitlements.

BUSINESS BENEFITS

Assured access management and strong authentication from within a single environment.

Enhanced customer trust and immediate second factor authentication with no disruption to customer experience.

Self administrable authentication schema and factor application aligns protection with risk.

With a combined TriCipher - CA eTrust SiteMinder® solution, this global Financial Services company is delivering strong authentication and enhanced customer trust within the same application and service protection infrastructure that their customers' administrators are already accustomed to. And with the TACS credential 'ladder', their customers can select the authentication factor most suitable for their individual institution's services and risk mitigation needs.

The combined solution's scalability will allow the company to rapidly expand their online offerings within a cost effective infrastructure that reduces liability, enhances customer trust, and provides long term protection for sensitive financial services offerings.

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



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