



PROTECTING ELECTRONIC PAYMENTS NETWORKS

Major Electronic Payments Network delivers integrated strong authentication, identity, and access management to 1600 institutions with TriCipher and CA SiteMinder®.



OVERVIEW

Challenge	Solution	Benefits
<p>Deliver strong authentication for 1600 institutions on an individualized basis.</p> <p>Safeguard multiple financial applications for thousands of banks with a single authentication system.</p> <p>Offer multiple authentication factors for varying constituencies and applications.</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>Unified identity, access management and strong authentication infrastructure.</p> <p>Protects ATM Network customers from online fraud and theft.</p> <p>FFIEC compliant with freedom of choice in authentication form factors.</p>

COMPANY BACKGROUND

ASP providing ACH, EFT, EBT, and POS services into competitive local markets.

1600 institutional customers with 3200 delegated administrators.

Strong authentication implemented to protect access to sensitive web-delivered applications such as funds viewing, transfer management and gift card administration.

This ATM network provider is one of the largest regional electronic funds transfer (EFT) networks in the U.S. Servicing more than 1600 financial institutions and merchants, they provide ATM, POS, EBT and ACH services as well as authorization, merchant services and Internet banking, along with a variety of account and funds transfer management applications for their commercial customers.

With a diverse customer base that spans a variety of network connectivity and computing resources, this provider must make its sensitive, high-value applications available over the public Internet, requiring protection on an institution by institution basis of credentials and web assets, with secure management of identities and access rights.

BUSINESS DRIVERS

Secure web delivered applications across multiple institutions.

Comply with FFIEC guidelines on access to sensitive data and authentication.

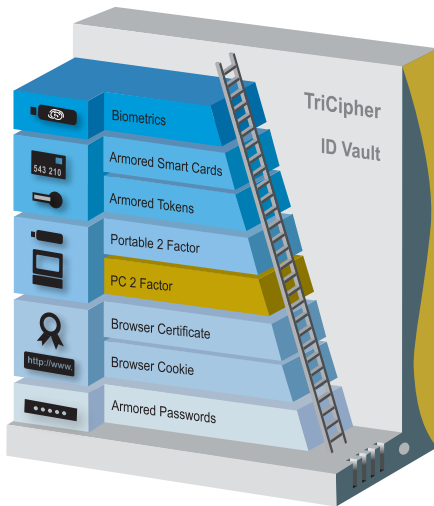
Integrate a flexible strong authentication infrastructure with CA SiteMinder that enables customer to choose from a variety of authentication strengths.

Delivering a variety of EFT services and associated funds transfer management applications across multiple institutions requires access and authorization capabilities that will insure that no other institution can access another institution's applications, and that every user is authorized to use each application and service with full authentication. For sensitive applications such as network wide funds transfer monitoring and tracking, the exposure and consequences in the event of inappropriate access or external intrusions can be significant.

As each institution subscribes to different services, with different user policies, and different network connectivity, this ATM network provider needed a highly flexible solution that would allow their client institutions to choose the method of strong authentication preferred for various classes of users and services, and that would provide protection against current and evolving online attacks.

AUTHENTICATION SOLUTION

TriCipher Armored Credential System (TACS)



TriCipher's Authentication Ladder enables the ATM Network provider to offer their customers a wide variety of authentication options to meet the varied business requirements of their 1600 customers. As threats evolve and business requirements change, customers can increase their authentication strength without affecting their infrastructure.

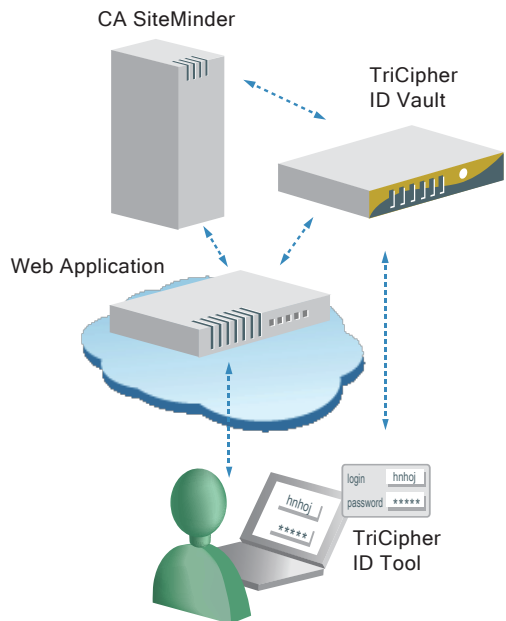
The ATM Network Provider chose the TriCipher Armored Credential System (TACS) in order to allow its customers to choose different levels of strong authentication depending on the nature of applications and services being accessed, and the roles of users within each customer's organization.

TACS implementation options enable the ATM Network Provider to support a range of strong authentication solutions with varying form factors that can be deployed now and in the future as customers' needs change. And the ability of TACS to rapidly integrate into existing applications and management interfaces without compromising functionality, ensured a non-disruptive rollout that required no change in user access administration.

With service delivery and customer experience retention at a premium, the ATM Network Provider selected the PC 2 Factor level on the TACS ladder of authentication form factors. PC 2 Factor delivers second factor strong authentication without the need for physical tokens using each user's PC as the second factor.

Each user's desktop is equipped with a small client component -- the TriCipher Identity Protection Tool (ID Tool), that is triggered in response to an SSL client authentication challenge invoked at login. The SSL challenge is sent to the TACS ID Vault and signed. A user key is generated by the ID Tool using a Trusted Device Marker (specific to each device whether a computer, portable device or smart card) and the user password. The user key and TACS key provide the credential to satisfy the SSL challenge - all transparent to the user. And since the full credential is never stored in any single place, it is virtually impossible to steal.

AUTHENTICATION, ACCESS & IDENTITY MANAGEMENT



The ATM Network Provider employs CA SiteMinder to provide application access management for sensitive applications such as network wide funds transfer monitoring. A key criteria was the ability to integrate strong authentication into the SiteMinder environment to provide a seamless service of access and identity management as well as strong authentication.

Since multiple institutions are supported with varying network connectivity and service subscriptions, SSL must be terminated at the DMZ rather than on the web application itself, therefore the SiteMinder X.509 authentication scheme cannot be used. Instead a TriCipher authentication scheme is loaded onto the SiteMinder policy server in order to manage credentialing within the SiteMinder environment. When users access SiteMinder protected applications, they are redirected to a certificate collection page that is protected by client certificates at the SSL termination point.

Users authenticate with the TriCipher ID Tool, and the SSL termination point passes certificate headers to the certification page whereupon the users' certificate serial number is extracted and passed to the TriCipher authentication scheme and then validated against the TACS appliance. Upon completion, a SiteMinder cookie is returned to the certificate collection page which then sets the cookie on the user's browser and redirects them to the actual destination page. This closed loop flow ensures that the authentication process is an integrated part of SiteMinder protected access.

For user identity management, IdentityMinder can be used to create and manage identities for the TACS ID Vault. From a single administration point, user management tasks such as create, delete, modify, and reset password can be performed - simultaneously updating IdentityMinder's managed end-point directory as well as user attributes within the TACS appliance.

BUSINESS BENEFITS

Applications and identities protected without user inconvenience and with complete mobility.

Application of authentication factors based on user role, access rights and access method.

Reduction in administration complexity with credential, authentication, and entitlement management from a single infrastructure.

With a combined TriCipher TACS and CA eTrust SiteMinder® solution, the ATM Network Provider is able to offer both web access management and strong authentication from a single integrated environment, and do so without infrastructure or customer disruption. New user populations can be quickly brought on line with individualized access and authorization schema. And as the providers' network and customer base grows, they can continue to deliver competitive, low cost, high value services that are fully protected and FFIEC compliant.

The combined TACS and SiteMinder solution will allow them to rapidly expand their web based applications, yet provide long term flexibility in choice of authentication factors, all while protecting highly sensitive applications and online identities from evolving threats.