

TRICIPHER AUTHENTICATION GATEWAY (TAG)



The TriCipher Authentication Gateway (TAG) acts as a services layer for web applications reducing the time to deploy strong authentication, increasing authentication performance, and ensuring the security of the login process by providing a single standardized strong authentication service for use by every application within an organization.



“When we needed to find a two-factor authentication vendor to satisfy the FFIEC regulatory requirements, we looked at TriCipher because they were being used by several of our service providers. As part of our TACS deployment, we chose to deploy the TriCipher Authentication Gateway so that we could meet very aggressive timelines to implement multi-factor authentication.

Now, we have a strong authentication infrastructure being leveraged by five applications. If we add applications or want to provide different authentication methods, we don't have to disrupt our users or network infrastructure.”

Barry Haddix
Vice President Information Technology
Southeast Corporate

The Problem

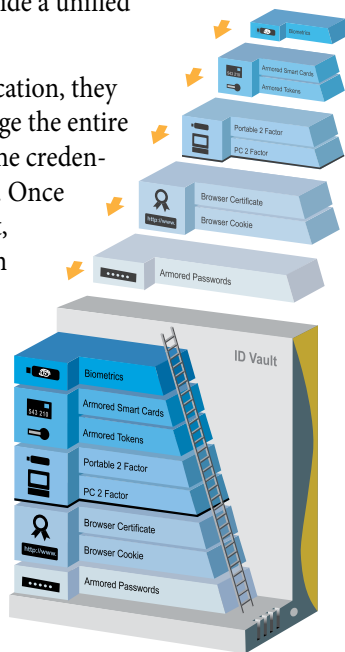
Today, businesses build, maintain and outsource a variety of web-based applications that are delivered to customers and business partners. Delivering these applications quickly, ensuring business continuity, and protecting access to sensitive data within these applications is critical to acquiring customers, generating revenue, and lowering costs. Each business to business (B2B) and business to customer (B2C) web applications has different business requirements necessitating different forms of authentication (Passwords, Tokens, Smart Cards, Biometric, etc.) When business have multiple B2B and B2C web applications, building authentication systems into each web application individually is costly to maintain, limits business agility, and often creates security vulnerabilities.



The TriCipher Solution

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, based on patent pending technology, 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.



Benefits

- Reduce the time to deploy strong authentication
- Increase the authentication performance of web applications
- Secure the user login process

What Makes TAG Different?

Existing authentication systems are designed as standalone authentication products that integrate with one application at a time and offer a single authentication method such as passwords, tokens or smart cards. As a result, each web application must go through a costly and time consuming integration process. Each time the integration is done, there is a potential to create serious security vulnerabilities. If the threat environment or business requirements change, every web application must be modified to integrate a new authentication technology.

When using the TAG as part of the TriCipher Armored Credential System (TACS), businesses deploy a unified authentication infrastructure once for all application and all authentication methods. Using a single standardized authentication infrastructure lowers costs, reduces time to market for new applications, and improves security.

TAG Features

Pre-Built Login Pages

The TAG is shipped with pre-built login pages that are customized to integrate seamlessly with customer web applications.

Fraud Detection Integration

The TAG makes integration with 3rd party fraud detection systems fast and easy.

Integrated Secondary Authentication

When users aren't able to provide their credentials, the TAG pre-built workflows provide a variety of secondary authentication methods including knowledge-based authentication (security questions) or out-of-band one time passwords.

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.

Integration Plug-ins

The TAG offers Plug-ins to integrate with leading web servers.

Authentication Type Notification

The TAG can notify web servers of what type and strength of credential was used to authenticate providing critical data that can be used for access control and risk decisions.

Security Assertion Markup Language (SAML) Support

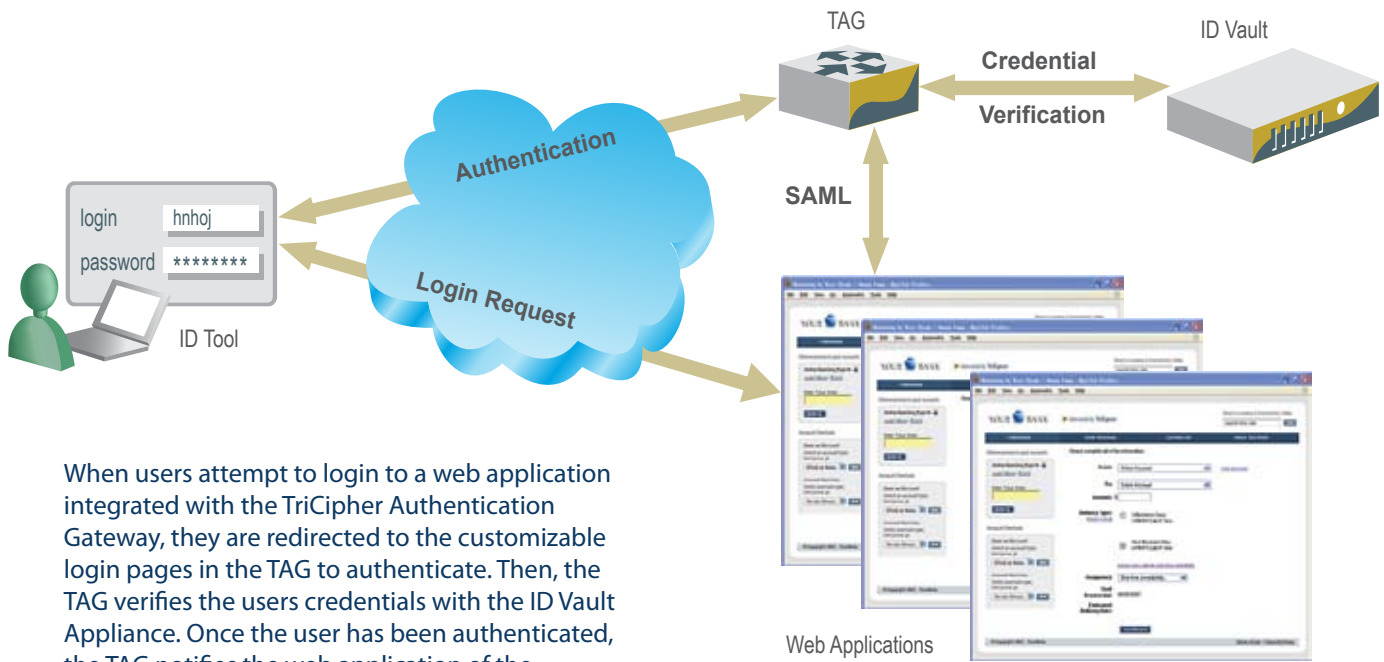
The TAG delivers SAML assertions to notify the web application of the authentication results.

Scalability

The TAG is designed to enable rapid scalability with unlimited capacity.

Hardened Appliance

The TAG is delivered on a hardened platform to protect the login process.



When users attempt to login to a web application integrated with the TriCipher Authentication Gateway, they are redirected to the customizable login pages in the TAG to authenticate. Then, the TAG verifies the users credentials with the ID Vault Appliance. Once the user has been authenticated, the TAG notifies the web application of the authentication results using SAML.

Functional Capabilities

Authentication

- Browser 2 Factor (B2F) Cookie
- Browser 2 Factor (B2F) Certificate
- PC 2 Factor
- Portable 2 Factor
- Armored Tokens
- Armored Smart Cards
- Compatible with TACS ID Vault 3.2 and above

Threat Assessment

- Covelight Percept Real-time Online Fraud Management integration module

Web Servers

- IIS 6.0 and later
- Apache 1.x (Linux)
- Apache 2.0 (Linux, Windows)

Security protocols

- SAML
- SSL
- TLS

Web Servers Management

- HTTP based
- SSH
- External Syslog
- SNMP

Browser support

- Internet Explorer 5.1, 5.5, 6.0, 7.0 or later
- Firefox 1.5 or later
- Mozilla 1.7.11 or later
- Netscape 7.2 or later

Technical Specifications

Physical Specifications

Form factor:

2U server chassis

Dimensions:

(H x W x D) 3.445 inches (87.5 millimeters) x 16.930 inches (430 millimeters) x 26.457 inches (672 millimeters)

Weight:

Approximately 30 lbs

Rack mountable:

19-inch standard rack mountable, EIA-310D

Hardware Specifications

Processor:

Intel Dual Xeon, 3.0 Gigahertz (GHz), 800 Megahertz (MHz)

Memory:

4 Gigabyte (GB) DDR2 400 MHz, ECC registered

On-board LANs:

Two 10/100 /1000Base-TX ports

Drives:

73 GB Ultra 320 SCSI Hard Drive

Serial port:

Console port, DCE (DB9-F), RS 232-C, 9600 Baud, 8-N-1

Power supply:

Up to 2 700W, 100-240VAC, 50-60Hz, hot swappable in redundant configuration

Cooling:

4 system fans

System Level Environmental Ranges

Operational Temperature:

+10 degrees C to +35 degrees C (50 degrees F to 95 degrees F)

Non-Operating Temperature:

-40 degrees C to +70 degrees C (-40 degrees F to 158 degrees F)

Non-Operating Humidity:

90% (non-condensing at 35 degrees C)

Regulatory and Standards Compliance

Safety:

UL60950-CSA60950, EN60950, IEC60950

Electromagnetic Compatibility:

(EMC) CE marking, FCC Part 15 Class A, CISPR 22 Class A, EN55022 Class A, EN55024 Class A, EN61000-3-2, EN61000-3-3, AS/NZS 3548 Class A

Restriction of Hazardous Substances:

(RoHS) 2002/95/EU Compliant

Waste from Electrical and Electronic Equipment: (WEEE)

2002/96/EU Compliant



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: +1.650.372.1324

Fax: +1.650.372.1301

TriCipher EMEA sales:

Email: sales@tricipher.com

Phone: +33-(0)1-53-53-68-07

Fax: +33-(0)1-53-53-67-00



IdenTrust
We Put The Trust In Identity