

While many of these products face challenges enrolling end-users, they are good solutions to the challenge of strong authentication, says **Peter Stephenson**.

Multifactor authentication today usually means two factors: something you know and something you possess. There are a few examples of true (i.e., more than two simultaneous) multifactor authentication, but these mostly are for deployment in high security environments and

almost always include biometrics. However, the “something you possess” may or may not be a token.

This begs the question of whether a token, a password/PIN and a certificate constitute multifactor authentication.

Tokens now come in all types, as well. Key fobs, hard cards and

USB tokens all are available and all are competent and easy-to-use. One major challenge for multifactor authentication, regardless of how simple to use the tokens are, is enrollment. Distribution of tokens across a geographically disbursed enterprise can be challenging.

Armored Credential System



Vendor	TriCipher
Price	starts at \$25,000
Contact	www.tricipher.com

The TriCipher Armored Credential System (TACS) is just that: a truly integrated system that delivers authentication with the strength

of public key infrastructure (PKI) that offers the ease of entering a user name and password. The TACS' major components are comprised of ID Vault, a FIPS 140 level II-rated appliance that manages user information, digitally signs transactions and authenticates.

The TriCipher Authentication Gateway (TAG) acts as the service layer for web-based applications to provide the user with the appropriate level of access. The TAG is shipped customized with preconfigured logon pages mak-

ing deployment and integration easier for the customer. The Armored VPN provides a strong authentication for VPN applications, which is easy for remote users to authenticate.

This product, from an end-user perspective, was very simple to use, especially considering all the high level authentication actions being performed seamlessly in the background. The TriCipher ID tool, Togo, is not just a token, but a simple, cost-effective USB smart drive that authenticates user credentials. The ease of initial deployment of the product is good. The addition of the TAG appliance within a corporate existing architecture will make system integration easier.

Performance of this system is first rate, and during the testing phases the product worked without a single glitch or interruption. The speed at which a user can authenticate and start working is excellent.

Documentation is in-depth and concise. All manuals for deployment and administration are well laid out and easy to understand. Documentation is well written and easy to follow and provides the

reader with a walk-through of deployment and configuration.

Support for the TACS is good — 24/7 mission critical support is available by email or phone.

The TriCipher ID vault, which is required, starts at \$25,000. The TAG is an optional purchase starting at \$15,000. Credentials are priced from \$1 to \$10 per user based on volume and credential type. Additional optional modules include: Armored VPN, Armored Identity Management, MySignatureBook (digital signing) and Armored Transactions.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★☆
Performance	★★★★★
Documentation	★★★★★
Support	★★★★☆
Value for money	★★★★☆
OVERALL RATING	★★★★★
Strengths	Good ease of use and a strong feature set.
Weaknesses	Deployment is best with the optional (extra cost) Application Gateway (TAG).
Verdict	Very good product with solid capability, flexibility and ease of use. Recommended.



The TriCipher Armored Credential System (TACS) is just that: a truly integrated system that delivers authentication with the strength of public key infrastructure (PKI) that offers the ease of entering a user name and password.

Peter Stephenson



TRICIPHER
Protecting Online Identity™

Quan Duke Tran
Large Enterprise Sales Manager
650-376-8326
quan.tran@tricipher.com