Two-Factor Authentication: Certificates Versus Tokens

Trustwave®

Two-factor authentication uses two components to authenticate a user's identity when accessing a network from a remote location. This traditionally consists of a factor the user has or possesses (e.g., hardware token) and a factor the user knows (e.g., username and password).

Trustwave's on-demand Two-Factor Authentication (2FA) solution couples digital certificates, representing user's identities, with your existing Virtual Private Network (VPN) infrastructure to deliver a more cost-effective solution and greater usability.

Why is Trustwave Certificate-Based Authentication Better Than a Token?

Trustwave delivers reliable, secure authentication at a fraction of the cost of tokens. We eliminate the need to track inventory and maintain associated hardware and software. We also leverage existing infrastructure and the entire solution is managed via an easy-to-use Web portal to eliminate the pains of implementation and on-going maintenance. Trustwave's on-demand, two-factor authentication solution does not require any additional hardware or tokens to be shipped or lost, and uses self-enrollment for end users — which means it can be activated immediately!

Cost Savings: Trustwave Two-Factor Authentication costs up to 3X less than traditional and outdated token-based offerings. And, with no physical tokens to lose or malfunction, no replacement shipping costs are incurred with Trustwave 2FA.

Minimal Management and Maintenance: Deploying token solutions can be a nightmare for any company to manage, from overseeing the inventory to properly managing token resets upon failed authentication attempts. No hardware support is needed for our Two-Factor Authentication solution; all management and credential distribution is accomplished through the Trustwave MyIdentity portal.

User Experience: Trustwave's solution makes establishing authenticated network and application access easy for end users. No numbers to remember or type incorrectly. No token to lose or misplace. No token resets and help desk calls.

Benefits of Trustwave Two-Factor Authentication

- Leverages customer's existing VPN authentication infrastructure
- No separate hardware purchase required; software-only solution that can be deployed quickly
- Users access a simple Web portal, enter an enrollment code, download the certificate and install it on their remote system—all in a matter of minutes!

Costs	Token-Based Authentication	Trustwave 2FA	Advantages of Trustwave 2FA
Up-front implementation	$$$$$	$	• No hardware to purchase • No software to license
Per user	$$$	$	• No hardware manufacturing cost
Hardware and infrastructure	$$$$	N/A	• No customer infrastructure needed • No hardware needed
On-going maintenance	$$$	$	• No hardware maintenance • No software maintenance • No Certificate Authority audit requirements • Self-service enrollment • No token replacements • Self-service revocations

About Trustwave

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure - from the network to the application layer – to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817

Trustwave®
Security begins with Trust™