

Tokenless Two Factor Authentication Ensures Secure Remote Access

Network security requires a solid offensive and defensive strategy that addresses the volatile and dynamic state of internet threats, man-in-the-middle attacks and the ever evolving list of vulnerabilities facing organizations today. The old notion of 'you are only as strong as your weakest link', rings true now more than ever.

As such, two factor authentication has become not just a method of security, but truly a requirement for a multi-layered approach to security. Secure remote access that is legitimate without being cumbersome to network users or administrators is a necessity among viable and mobile workforces.

Tokenless two factor authentication solutions are an improvement on the traditional choices, which eliminate the vulnerability associated with lost or stolen tokens or other PKI authentication issues subject to attack by viruses and other malicious programs. In addition, tokenless solutions greatly eliminates any cost barriers that previously existed, especially among large enterprises.

Ensuring that the tokenless two factor authentication solution selected is reliable and easy to deploy is also essential. Many security products claim that they are easy and effective, but often times the infrastructure is so awkward and unmanageable in large networks. It's one thing if a security product is easy for a network admin to navigate and operate, but it should also be one that requires very little end-user education in order to truly work and be used as its intended. As security can be extremely expensive, especially for large organizations, tokenless solutions not only address the usability issue, but the cost factor as well. Tokens are very costly and are still subject to be lost, damaged, stolen or loaned to outsiders.

With tokenless two factor authentication solutions, an end-user logs in to a secure authentication server to register a password. At that point they are then given a one time password through an alternative medium, such as text message, email or phone, where they are required to answer a series of security questions. Once the user has successfully completed this process, they are authenticated with a certificate granting them VPN access.

Typically the components involve something you know, questions that only you know the answer to and something you have. When leveraging out-of-band registration another layer is added, requiring that the user have access to the outside medium, (their cell phone, email, etc).

[Tokenless](#) two factor authentication is just that, a security solution that requires more than one thing to authenticate a user and grant network and web-application access without an expensive and vulnerable token hindering the security process. The beauty of tokenless two factor authentication is the reduced expense. The sheer cost of supplying and replacing users with tokens can deter even the most security minded organizations, it just simply isn't feasible on a large scale. The biggest problem associated with tokens is you have to have the physical token in order to be granted access. Many users are so paranoid about losing or not being able to find their token when they need it that they carry the token with their laptop, some even adhere it directly to the pc. Now, not only is the individual laptop subject to unwanted access is found in the wrong hands, but the entire organization's network is at risk too.

With tokenless two factor authentication, these risks and extensive costs are removed, while the level of security an organization experiences benefits from out-of-band registration authentication.

About the Author

As an avid technology lover, Sam Brown follows tech movements within network security solutions, including [two factor authentication](#), tokenless and strong [SSL VPN authentication](#) solutions.

Source: <http://www.diyresource.com>