

Secure Device Authentication



DevicePass™

Secure Device Authentication

Each computer device has its own unique characteristics. DevicePass creates a unique "deviceprint", a digital fingerprint of the device, using the device's characteristics including hard disk ID, CPU serial number and network MAC address etc. Combining the deviceprint with a user name and password, online and corporate applications can restrict network access to only trusted devices and authenticated users.

DevicePass provides a simple, cost-effective way to achieve strong, two-factor authentication for remote access to enterprise networks, internet and mobile applications.

Key Features and Benefits

One-Time Deviceprint

Once a device has been registered, its real deviceprint will not be directly used in the authentication process. Instead, in every authentication, a one-time deviceprint derived from the real deviceprint is generated and submitted to the server. This innovative way of authenticating a device using one-time deviceprint prevents the replay attack - a problem that other device-based authentication products commonly suffer from.

Real-Time Interrogation

Furthermore, the DevicePass client does not store the deviceprint. At each authentication request, the DevicePass client checks the hardware parameters in real-time, which makes the replay attack impossible.

Auto Synchronisation

DevicePass offers the flexibility that allows the user to change some hardware components in their device, without re-registering the device. If a device becomes "unsynchronised" as the result of hardware changes, DevicePass can automatically update the deviceprint with the new hardware configuration as long as the changes are within the allowed threshold set by the service.



Works with Mobile Phones

In addition to desktop and laptop computers, DevicePass is also able to authenticate smart phones operating on Microsoft Windows Mobile.

Two-Factor Authentication

Combines device identification with a user name and password to restrict network access to authorized devices and authenticated users. No additional expensive hardware is required.

Transparent Authentication

Provides device-level authentication through the same authorization process with which users are already familiar. Since DevicePass doesn't alter the end-user experience, there's no user interaction, learning curve or training required.

Copyright © 2007 Deepnet Security Ltd. All rights reserved. Deepnet Security, Deepnet Anti-Phishing, Deepnet Authentication, MobileID, PocketID, FlashID, SmartID, MobilePass, DevicePass, RemotePass, TypeSense, VoiceSense are among the trademarks of the Company in the United Kingdom, United States and/or other countries. All other trademarks are the property of their respective owners.