WWPass® PassKey™
Strong Authentication

The First Line of Defense

In 2013 there were over 2,000 reported data breaches that exposed more than 800 million records.[i] Many of these breaches occurred as the result of malware that used multiple attack vectors. All too often it is discovered that hackers gained access to the secure data after stealing username and password credentials from an unsuspecting user.

The April 2014 disclosure regarding the 'Heartbleed' bug in OpenSSL is another example of why the username and password as the first line of defense is not working as a secure method of authentication.

Two-factor Authentication

Two-factor authentication is unquestionably more secure. Standards such as PCI and government regulations such as HIPAA require the use of two-factor authentication for accessing certain data.

Two-factor authentication (2FA) is defined as using two of the following to prove your identity:

- Something you know – like an access code
- Something you have – a token or card
- Something you are – fingerprint or retinal scan

One of the organizations that were breached in 2013 did use 2FA for their vendor portals; but did not require 2FA for 'low-level' vendors. The investigation showed that it was a low-level vendor's username and password that was used to launch the massive security breach.

Arguably the most popular 2FA solution in use is text-to-mobile OTP (one time password). While this is a very convenient solution, it does have some drawbacks; you have to give out your mobile phone number and your mobile device could easily become infected with malware that intercepts your text messages.

Multi-factor is a loosely used term that also applies to 2FA. Logically, the more factors you have the more reliable and secure the authentication should be. Multi-factor and two-factor are generally one-sided, as the user must prove who she is to the service provider. However, the service provider does not have to prove who they are to the user.

WWPass Authentication

WWPass® provides a patented authentication solution that definitively validates the user and the service provider. Through this multi-lateral authentication, the service provider is ensured of the identity of the user, and the user can be certain that they are accessing the website or application they intended.

When a user chooses to log on to a service provider using the WWPass authentication services, the service provider is authenticated with WWPass first. This helps to protect the user from 'spoofed' websites that are used to steal user credentials for legitimate websites.

The user is asked to provide their PassKey™ and an access code to prove their identity to WWPass. Once authenticated, a secure channel is established between the user and WWPass to complete the authentication process with the requesting service provider.

The PassKey is a cryptographic device using Java Card technology. The PassKey provides functionality that is similar to a traditional Smart Card and can be used in multiple interfaces and form factors including USB, NFC, SmartPhone, and CAC.

Using the WWPass solution, the service provider further enhances the secure access of the user and associated data while minimizing their risk and

liability. Any user specific data that is required to complete the authentication (such as an account number or other unique identifier) is encrypted by the PassKey, transmitted over SSL, stored within a unique Data Container (DC) and encrypted again.

The Data Container can be compared to a safe deposit box at a bank. In order to open the safe deposit box, you will need your private key and the bank key. The data in the DC can only be accessed by the user and the service provider associated with the DC. Once both parties have been authenticated, the data can be deciphered using a unique encryption key that was generated when the data was initially written to the DC using the individual identifiers of both parties.

The PassKey can also be used for certificate based authentication with PKI implementations. The users certificates are stored in a DC and can only be accessed by the PassKey holder. Unlike typical smart cards or tokens, no data is stored on the PassKey. This eliminates the need to engage in the lengthy and difficult process of certificate revocation and replacement.

Should the user lose their PassKey, his certificates and identities are easily recoverable. The user can simply create a new PassKey through a self-service portal and easily retrieve her existing certificates with no administrative overhead.

With WWPass authentication, only one PassKey is needed to access multiple service providers or applications. The data associated with each service provider and the user is stored in a unique DC for each relationship. This means that there is no cross-pollination of data between service providers.

Whether you need to secure a website, payment system, eShop, vendor portal, customer portal, internal systems, or remote access, you can easily integrate the WWPass PassKey to ensure that your users' accounts and company data are secured against the prying eyes of hackers.

About WWPass

WWPass is a technology leader in cloud-based authentication and storage services providing convenient and secure access to applications, networks, web sites, and web portals. Our patented mutual authentication solution helps organizations meet regulatory compliance requirements while reducing their operational costs and capital investments.

Features and Benefits

- Unparalleled multi-factor authentication
- Multiple form factors
- Multi-lateral authentication of user and service provider
- Eliminates username and password
- Flexibility of authentication methods:
    - PKI certificates
    - Two-factor
    - As a second factor
- Reduces risk and liability
- Aides in meeting regulatory compliance
- Lowers capital investment
- User self-service recovery portal
- Decreases administrative overhead
- Protection against phishing and website spoofing

Product Requirements

Operating Systems

- Windows 7/8/8.1
- Windows Server 2003/2008/2012
- OS X 10.8/10.9
- Ubuntu Linux 12.04 LTS and 14.04 LTS

Browsers

- Chrome 20 and above
- Internet Explorer 8 and above
- Firefox 27 and above
- Safari 5 and above

Mobile Devices

- Android
- Bluetooth or WiFi

[i] Source: Data Breach QuickView – An Executive's Guide to 2103 Data Breach Trends
https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf

