DATA SHEET

WWPass Multi-Factor Authentication for Microsoft Windows

Overview

Microsoft Windows supports two methods of authentication within enterprise domains: username and password and digital certificates (PKI) on smart cards. Nowadays username and password pairs are considered to be extremely vulnerable, especially when used for remote access. Certificate-based authentication with smart cards provides strong two-factor access to domain computers, both local and remote.

WWPass leverages its patented technology for authentication and personal data storage to implement a Windows Logon solution. This solution is based on a hardware security device, a PassKey. It is a cryptographic microcomputer in a form factor of either a USB token or plastic smart card. The PassKey interacts with WWPass' core network to access encrypted user credentials. These credentials are restored by the PassKey and used in mathematical transformations during authentication procedure.

Product at a Glance

The PassKey requires WWPass Security Pack – a software bundle that provides drivers and tools to support WWPass cryptographic services.

WWPass Windows Logon is fully compatible with Microsoft's "Smart Card Mini-driver" specification, supporting all possible certificate applications in the Microsoft Windows environment.

Product Specification

Prerequisites

- Corporate network with deployed Windows Domain, Active Directory and Certificate Authority services

Requirements

- OS
  - Windows 7/8.1/10
  - Windows Server 2008 or 2012 Virtual Desktop Infrastructure (formerly Terminal Services)
  - VMWare View virtual desktops
- Terminal
  - Any Windows desktop
  - Linux with *FreeRDP* or *rdesktop* applications
  - Standard smart card reader for plastic cards (not required for USB tokens)
- WWPass Security Pack

- *No certificates/private keys are stored on hardware tokens*. All sensitive data is encrypted, fragmented and geographically dispersed over WWPass storage nodes.
- *Self-service hardware device management*. Users can easily revoke lost devices and create replacement keys. No personal information is lost.
- *Improved card presence detection*. Eliminates involuntary remote session breaks.
- *Support for multi-domain authentication*. The WWPass Credential Provider can be activated in a multi-domain environment.
- *Variety of form-factors*. Including USB/NFC tokens and plastic cards. Hybrid devices compatible with 125 kHZ HID physical access cards are also available.
- *Advanced certificate management tool*. WWPass' Security Pack comes with its own certificate manager which allows users to import, view and delete certificates.

 | WWPass | 1155 Elm Street, Manchester, NH 03101 | Tel: +1.603.836.4932 or +1.888.997.2771 | www.wwpass.com