DATA SHEET

WWPass® Authentication Service for IBM Security Access Manager 8.0

Overview

The WWPass Authentication Service provides strong hardware authentication and removes the need for username/password pairs.

Traditionally, users authenticate into IBM Security Access Manager protected resources with username and passwords. Usernames are used as the primary index in user databases, which creates a critical vulnerability. Likewise, complex and hard to remember passwords do not prevent a hacker from compromise the security through multiple well known attacks.

Second factor authentication, using one time password dongles or phone apps, slightly improve the resilience of the systems, but this too can be compromised with a number of well-known methods.

Use of the WWPass distributed storage system with a PassKey form factor allows complete elimination of human-handled access credentials, thus fully removing vulnerabilities, associated with:

- Credential sharing
- Key logging
- Credential re-use
- Phishing attacks
- Man-in-the-middle attacks

Product Specification

Compatibility

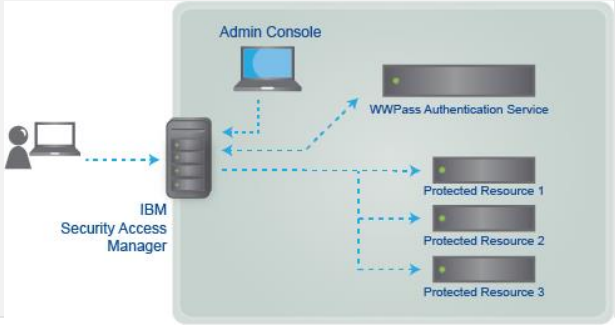
- IBM Security Access Manager (ISAM) 8.0

Client Requirements

- Security Pack v3.0 and above
- Internet access
- ***Supported Browsers***
  - Internet Explorer 8 and above (Windows)
  - Chrome 20 and above (Windows)
  - Firefox/Safari/Opera (Windows/Linux/MAC)

PassKey Form Factor

- **Hardware PassKey**
  - USB/NFC token
  - Plastic smartcard with NFC and ISO-7816 interfaces
  - Hybrid NFC/ISO-7816 Smartcard with additional HID-125 kHz door opener
- **Software PassKey**
  - Android with Bluetooth, Wi-Fi and NFC interfaces (PassKey for Mobile)
  - Android and iOS with QR code scan (PassKey Lite)



Product at a Glance

The WWPass Authentication Service provides a unique authentication solution for ISAM, which replaces the username with a secure PassKey ™.

The WWPass Authentication Service is a web service, which utilizes the IBM Security Access Manager (ISAM) External Authentication Interface (EAI). The WWPass service supports different authentication strength levels according to the ISAM specification.

When a user attempts to log in to a protected resource, authentication requests are transparently rerouted to the WWPass Authentication Service from the ISAM server. The request, on success, returns the user's credentials and the ISAM server redirects the user to the destination.