wwpass®

The Future of Multifactor Authentication

MFA with NO usernames — convenient, secure, strong WWPass® authentication moves beyond the password to protect both your data and your users

Good security starts at the login screen — and that's where WWPass comes in. Our innovative, patented multifactor authentication (MFA) solution solves the information security infrastructure's biggest deficiency by conveniently, yet securely, protecting your data and your users. With just one self-managed WWPass Key mobile app or token, users can easily log in to all their enabled applications without the need for inherently insecure username/password architectures. WWPass technologies keep application data and user identity information separate and hidden from all other applications, preserving both user and application privacy — even from WWPass itself.

What makes WWPass different from other MFA systems? **Unlike the others, WWPass uses "something you have" — the WWPass Key token or WWPass smartphone app — as the user's primary credential.** This eliminates the need for username/password pairs and closes the door to first-order threats ranging from compromised credentials to SQL injections. Users enjoy the convenience of never having to remember username/password details; behind the scenes, real user credentials (never exposed to users or applications) are stored and managed by WWPass' secure, distributed cloud storage, which makes them disappear when not in use. Additional verification factors (biometrics, IP whitelists, geolocation or even, if desired, passwords) can be added for additional security as needed.

Secure enough for finance and healthcare settings, but easy enough for consumer applications, both WWPass Key app and phisical token also offer convenient user self-service. Even the WWPass Key hardware token can be easily revoked and re-generated by the user if it's lost or stolen. And because of WWPass' innovative data storage methodology, your users benefit from the convenience of true single sign-on to applications both inside and outside your enterprise, while you rest in the knowledge that data about your application is kept securely compartmentalized.

In short, WWPass represents the future of MFA: convenient, secure, flexible and strong. After all, when it comes down to it, good authentication isn't a matter of the number of factors — it's a matter of ensuring trust.

Why WWPass is Different

Security

- Eliminates usernames and passwords for good
- Stops phishing and spoofing attacks
- Prevents security risks from duplicate credentials
- Encrypted, fragmented, globally distributed data storage

Usability

- One key grants access to many accounts
- No more credentials to remember or manage
- Access multiple resources from computers, phones, tablets

Affordability

- Self-service management reduces service desk costs
- Flexible, affordable, cost-effective pricing

Flexibility

- Offer authentication via choice of hard token or phone

Extensibility

- Easy integration into virtually any Web-based environment
- Outstanding scalability

Which is Right For Your Enterprise: WWPass Key app or hardware token?

WWPass Key mobile app

- **Uses our free, convenient smartphone/tablet app** (iOS and Android) to log into enabled Web resources
- No additional software is needed on the access device; users can use anything with a Web browser
- To log in, users scan a QR code generated on the login screen (or tap the QR code if the login screen is on the user's smartphone or tablet)
- Recovering of lost or stolen phones/tablets is done via an email address provided by the user at time of registration
- Applications using WWPass Key app can also be configured to use other authentication types for migration/backup purposes

WWPass Key hardware token

- **Uses proprietary USB or NFC PassKey tokens** with the strongest secure element commercially available
- For added security, WWPass Key token users must also install the WWPass Security Pack extension on their Windows, Mac OS or Linux PC (not currently supported on smartphones/tablets)
- Self-service token management, including revoking lost or stolen Keys and generating replacements
- WWPass Key can be used to authenticate to applications using PKI certificates, such as Windows® computers, remote desktops, VPNs and SSH connections — and with an unlimited number of certificates, users can log into all their enabled resources
- Certificates also can be used for encrypting Microsoft Outlook® and Mozilla® Thunderbird® email, and for data encryption services like Microsoft BitLocker®

Mobile app for simplicity, Token for versatility: Both versions of WWPass authentication offer **a higher level of security at a lower cost**

Versatile, secure, convenient: WWPass use cases

IT Systems Integrator

The company's 400 support engineers use **WWPass app** to access a BMC® Remedy® service desk. On-site and remote access is protected using IBM® Security Access Manager with the WWPass authentication module.

Public Wireless Internet Service Provider

For a maximum-flexibility solution, the company uses **WWPass app** for authenticating both subscriber and ad-hoc customers — administered provisioning for the former, self-provisioning for the latter.

Health Insurance Company

System admins in this company's high-security environment use the strength of **WWPass token** to securely access corporate resources using VMWare® and Windows® Remote Desktop.

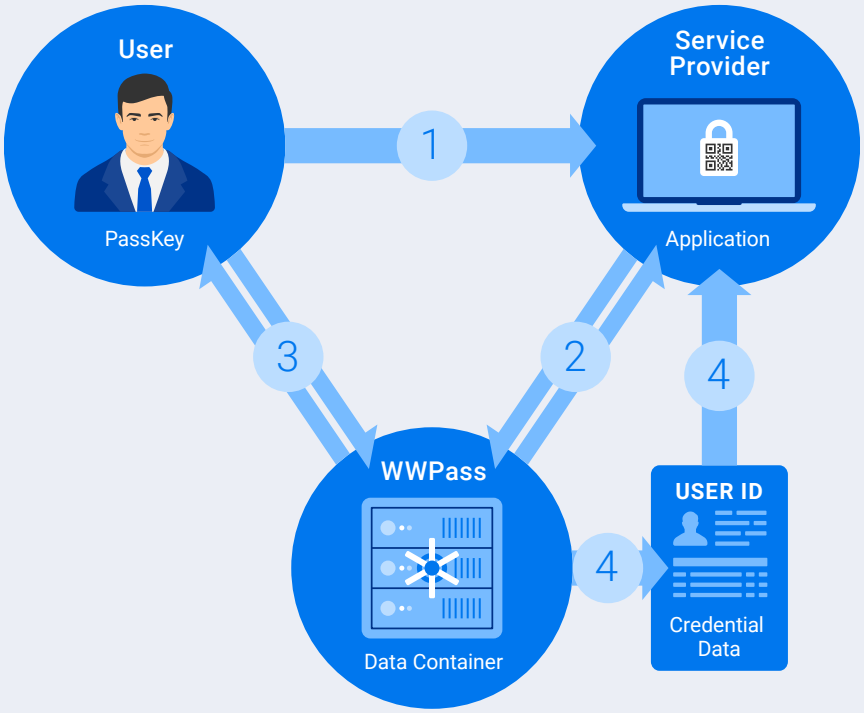
Easy Integration With Most Environments and Access Management Systems

Implementing MFA shouldn't be a hurdle in itself — and with WWPass, it isn't. **Both WWPass Key app and token can be integrated into virtually any Web-based environment**, and mobile app and token can be used simultaneously or separately depending on your business needs. User provisioning under WWPass is flexible, too; it can be done by your administrators, or you can allow users to create accounts themselves (ideal for e-commerce).

When it comes to integration, WWPass engineers can be contracted for customized assistance. Want to do it yourself? Our free WWTools™ software development kits, available for most popular programming languages, make the job easier. For example, adding WWPass authentication to IBM Security Access Manager can be completed in a matter of hours.

SSO integration is simple, too: Using Gluu SSO + WWPass MFA, in SAML-enabled applications such as Salesforce, Google Docs or Dropbox, it's easy to eliminate usernames and passwords. And if your needs extend to corporate VPNs, WWPass can easily be integrated with solutions including Fortinet, Juniper, Cisco and OpenVPN, with remote access in Windows and VMWare environments using computers and/or select thin clients.

How wwpass authentication works



1. **User initiates login to service provider** using their WWPass Key.
2. **Service provider and WWPass bi-laterally authenticate** via PKI certificate exchange.
3. **User key and WWPass bi-laterally authenticate** using symmetric keys.
4. Using a one-way function, **WWPass combines the user and service provider IDs** to create a pointer to one or more application-specific **data containers**, which are sent to the service provider via SSL for use in authentication. **Each data container is unique to both the user and the application**, ensuring security for both.

Encrypted, Fragmented, Globally Distributed Data Storage — With No Backdoors

Both versions of WWPass Key use our patented, fragmented, encrypted and securely distributed cloud storage for user data — making it totally unobtainable by third parties, including WWPass itself. Users can rest easy in the knowledge that no element of their authentication activity, even metadata such as their browser, device, or location information, can be mined by WWPass for marketing or any other purpose. Application owners can enjoy the security of knowing that although their users' WWPass keys open many "doors", those "neighbor" services have no information about their own application.

WWPass' best-of-breed authentication protocol is unique among competitors because it makes user identity opaque not only to WWPass, but also to potential attackers. Because of WWPass' use of user- and application-specific data containers, the user's identifier is never presented to any application. What's more, a service provider cannot correlate a user's accounts across services, nor can an attacker capture a service provider's database.

Key to the success of this technology is the elimination of usernames. A user's authenticated identity under WWPass is primarily tied to a hardware or smartphone token he or she owns. This is in contrast to other MFA offerings, where "something you have" merely augments a fundamentally insecure username-and-password scheme in which attackers can glean a wealth of information from username alone, whether at rest or in transit.

> The user's identity is not only **unintelligible to attackers** — it is **never disclosed to WWPass itself**

What's more, with WWPass the full user identity is not even generated until the service provider or other associated party authenticates its own credential. Only the combination of the two unlocks a unique instance of the user's profile that is intended only for that specific use. The user can generate any number of IDs, creating associations that are not linkable except through information the user alone provides to the other party.

Users' profile data itself is stored via WWPass' innovative, patented cloud-based storage technology: a series of encrypted blocks distributed across a worldwide bank of geographically diverse servers, using a Reed-Solomon (n,k) redundancy scheme to safeguard user data containers against accidental data loss.

The WWPass advantage

There are many factors to consider when implementing MFA for your enterprise — but in a head-to-head comparison, **WWPass' authentication solution outperforms others in the market in security, convenience, and price.**

System	Eliminates Usernames	Self-Service Revoke/Recover	One Device, Many Sites	Mobile Friendly	Mail & Data Encryption	Affordability
RSA® SecurID	—	—	—	✔	—	High per-token cost
Yubikey	—	—	—	—	PGP (some versions)	High per-token cost
FIDO U2F	—	—	✔	✔	—	High per-token cost
Duo™ Security	—	✔	✔	✔	—	High cost when in roaming
Smartcards	✔	—	Limited	—	✔	High per-token cost
Google® Authenticator	—	—	Limited	✔ (not on same device)	—	Free
WWPass Key	✔	✔	✔	✔	✔	**Flexible, affordable pricing for all sizes of enterprise**

True Single Sign-On ... Inside and Outside Your Enterprise

We've all had to deal with the VIP user who asks to be able to log in to the corporate network using his or her LinkedIn ID — proof that even the most experienced users don't always make the best decisions when there's a trade-off between security and convenience. When you implement secure, convenient multifactor authentication from WWPass, your users will never need to make that choice.

Unlike traditional hardware-based MFA methods, every one of your users gets the benefits of true single sign-on in addition to our patented security technology. With WWPass solutions, your users can use their WWPass credentials to log in to any application worldwide that uses WWPass authentication. And thanks to our innovative, containerized data storage, information about your applications and services is always kept completely separate and secure from that of others.

Onboarding new users who already have WWPass credentials from somewhere else? They'll be able use their existing WWPass Key to access your applications and services. It's that easy — for your enterprise and for your users alike.

Ready to learn more?

WWPass' convenient, secure authentication technology makes securing your enterprise's applications and users something you can't afford to do without. And when it comes to learning more about building a solution for your organization, we're here to answer your questions, large or small — just visit wwpass.com today, or contact **info@wwpass.com** or **1.888.997.2771** for a personalized consultation with an expert from our integration team.

Want to dig a little deeper into the technical details? You can find a wealth of documentation about WWPass solutions, including whitepapers and datasheets, at **wwpass.com/documentation**.

wwpass®

WWPass Corporation

9 Trafalgar Square, Suite 240
Nashua, NH 03063

info@wwpass.com
wwpass.com