



Enabling Scale for a SaaS Document Management Company

No matter the industry or scope, in today's landscape every digitally-enabled business faces two critical security hurdles: **ensuring your users are who they say they are, and ensuring their data is secure at rest and in transit**. To meet these demands, **WWPass® provides a patented, all-in-one solution for multi-factor authentication and client-side encryption** that empowers your business to overcome both obstacles seamlessly, securely, and without disrupting your existing workflow.

Here's an example of how one WWPass customer **solved these security hurdles while also opening the doors to major global growth potential**. Their software-as-a-service (SaaS) document management platform offers solutions critical to nearly every modern business: cloud-based workflow and document management, mobile workflow, reporting and analysis, and an electronic file system for document exchange and management.

With an existing portfolio of mid- to large-sized clients in both the public and private sectors, the company is now poised for even greater scale after engaging with WWPass — a collaboration that **enhanced security while also boosting operational efficiency and improving user experience**.

The Challenges

1 Strong Customer Authentication 2 Client-Side Encryption for User Data

To win new global business, the Company had an immediate need to solve **two critical challenges** for their document management system. As a result of the European Union's General Data Protection Regulation (GDPR) legislation, they needed to implement strong customer authentication for both internal users (such as system administrators) and external users (the Company's clients) in order to ensure confidentiality and integrity of credentials. At the same time, the Company sought to increase their

product's overall security. Because documents stored in their cloud-based system were unencrypted, there was a risk that during backups, system updates or other routine file maintenance operations, files could potentially be accessed by system administrators or other internal users. **WWPass technologies addressed both of the Company's challenges in a single solution**: a WWPass Key that entirely eliminates the need for usernames and passwords while also enabling seamless, end-to-end client-side encryption.

1 Strong Customer Authentication

To address the Company's first challenge — strong customer authentication — an analysis of the current landscape offered **four potential solutions**:

1. Two-factor authentication with text message (SMS) code as the second factor
2. Two-factor authentication with one-time password (OTP) as the second factor
3. Strong authentication using a smartcard
4. Strong authentication using WWPass

Because of the Company's large, frequently changing roster of external users and corporate clients, **smartcard-based authentication was quickly ruled out** due to low flexibility, poor scalability and very high cost. **SMS-based two-factor authentication was also dismissed right away**, in this case due to its inherent insecurity; in fact, NIST ceased recommending SMS-based two-factor authentication in 2016, and the latest draft of its Digital Identity Guidelines (Special Publication 800-63B) notes that "out-of-band verification using SMS is deprecated, and will no longer be allowed in future releases of this guidance."

While OTP-based authentication using a secure out-of-band method such as a mobile app is more secure than SMS, **the OTP user experience is far from ideal**; now users have not one, but two passwords to deal with. Additionally, implementing OTP would have required the Company to set up extra, costly hardware and software — including an additional server just for OTP, with extremely high availability and a geographically distributed mirror for backup or contingency purposes. **With these considerations in mind, the best solution was clear: WWPass password-free authentication.**

2 Client-Side Encryption for User Data

When it came to the second challenge — protecting user documents — **the Company required client-side, end-to-end encryption so that their customers' data was never revealed unencrypted**. However, because this sort of encryption requires the use

of carefully managed public and private keys, this presents a hurdle: **How to issue, store, manage and revoke keys in a way that is both secure and simple to use?** One of the major strengths of the Company's platform is its availability as both a web application and multiplatform mobile app, making storing and managing private keys in the OS, browser, or on a trusted platform module too inflexible of an option.

Using any kind of **hardware secure module (HSM) to manage keys located on-premise was also not a viable option**, since this would require internal resources to manage and ensure baseline requirements and service level agreements. Additionally, the HSM-based cloud solution does not fully resolve the issue of unauthorized access to private keys by managers of HSM systems.

One potential solution — **deriving encryption keys from users' passwords** and storing these keys in encrypted form on the server side — is accepted by many vendors, but has **a number of deal-breaking limitations**. Because passwords are usually human-readable, they often exhibit low complexity even if they meet traditional "strong password" standards, meaning that keys based on such passwords have low entropy. Plus, even if all users chose "perfect" passwords, these might still appear in log files used for auditing purposes and thus available to system administrators.

Even worse, in a system where keys are generated from passwords, changing a user's password makes key management extremely difficult or even impossible — and "solving" that problem by failing to architect a password-change procedure leads to **GDPR noncompliance**.

Fortunately, the WWPass solution for client-side, end-to-end encryption suffers from none of these afflictions. Because **WWPass uses chained cryptographic keys in concert with a master key generated by its WWPass Key authentication device**, there is no need to repeatedly revoke and reissue keys — in fact, **users don't need to be aware of the existence of keys at all, just as they don't have to worry about passwords**.

The Solution

One Device for Password-Free Authentication & Convenient Client-Side Encryption

Strong, Password-Free Authentication

WWPass' all-in-one solution addresses both of the Company's needs in a single device — starting with easy, password-free authentication. Every user is issued a **WWPass Key, a cryptographic microcomputer in the form factor of the user's choice:** mobile app, smart card, or USB+NFC fob. Users manage the WWPass Key via a self-service web portal or mobile app (a WWPass-patented solution), and there is no personal information stored on the device itself. If needed, an additional factor (such as a PIN or fingerprint/face recognition) is freely programmable.

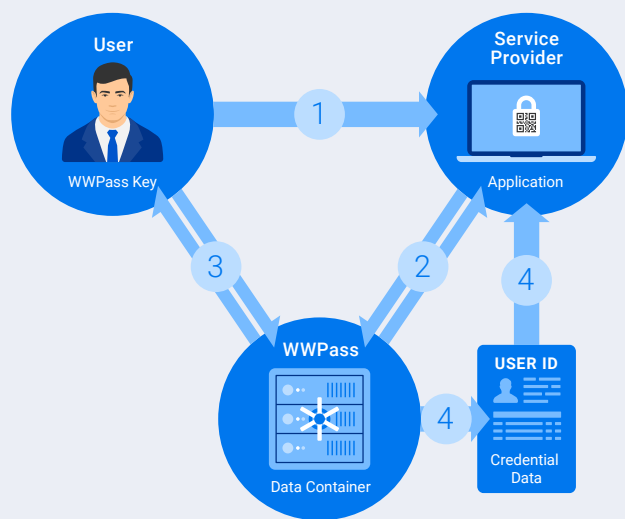
When the user successfully authenticates with the WWPass Key, **non-human-readable credentials**



(NHRC) are created instead of a username/password pair and are then sent to the service provider in encrypted, fragmented form by WWPass using its patented Distributed Data Storage system. This has **two benefits**: First, if a hacker were to obtain NHRC data, it would be useless because there is nowhere for them to enter it in the authentication process. Second, encryption and fragmentation ensure that all users are completely anonymous to WWPass.

Transitioning to WWPass password-free authentication **took the Company just three months** after proof of concept, and required **no disruptions** to normal operation. Existing users migrated by first accessing the system with their new WWPass Key and then binding it to their existing username/password pair. New users were introduced directly by binding the NHRC of the user into the Company's existing identity and access management system. After a three-month transition, username/password login was completely stopped, **enabling a myriad of benefits**:

- **Convenient for users:** Enables easy access to all of a platform's resources — web, mobile, and desktop application — with no passwords to remember
- **Convenient for IT support:** Users can self-manage their WWPass Key without external help
- **Beneficial for business:** No drop in productivity due to password resets or lockouts



- 1 User starts a login using their WWPass Key
- 2 Service provider and WWPass mutually authenticate
- 3 WWPass Key and WWPass mutually authenticate
- 4 WWPass delivers user's NHRC to the service provider

WWPass password-free authentication

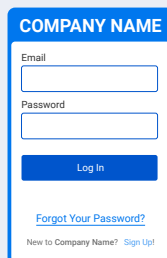
- **Flexible form factors:** The WWPass Key can take the form of an iOS/Android app, smartcard or USB+NFC fob, depending on business or user needs
- **No human-readable credentials:** Eliminates the fundamental security problems of data breaches involving weak, default or stolen passwords
- **Regulatory compliance:** WWPass' multiple factors and security layers ensure compliance with GDPR, HIPAA, NIST, PCI DSS and others
- **Zero-knowledge:** Identity management is separated from access management, with access management outsourced to WWPass using zero-knowledge technology

Convenient Client-Side Encryption

The Company's second task — implementing end-to-end, client-side encryption with a pain-free user experience — was also solved using the WWPass Key. **Because the WWPass Key can generate a master encryption key that never leaves the device, it can also be used for client-side encryption.**

This solution **secures user data using a chain of cryptographic keys**. First, the WWPass Key generates a provider-specific encryption key, which is then securely sent to the user's device (phone, tablet or computer) for use by the mobile or web application that requires it. Then, that application uses the provider-specific key to encrypt individual project and file encryption keys, as well as encrypt the contents of the stored files. This means that **there is never any need to reveal the WWPass Key's master encryption key to anyone** — not a cloud storage vendor, not WWPass, not even the Company itself.

In addition to implementing client-side encryption using WWPass technology, the Company put into place overall key management methods in accordance with NIST recommendations, with segregation of roles based on separation of duties, split knowledge and dual control. This means **system administrators are responsible only for system support and backup — they have no access to unencrypted documents or keys** and cannot manage access. While WWPass is responsible for performing



Obsolete

Phase 0: Usernames and passwords

Unsafe and inconvenient



Incentivized

Phase 1: WWPass login

Optional use of obsolete usernames and passwords



Mandatory

Phase 2: WWPass login

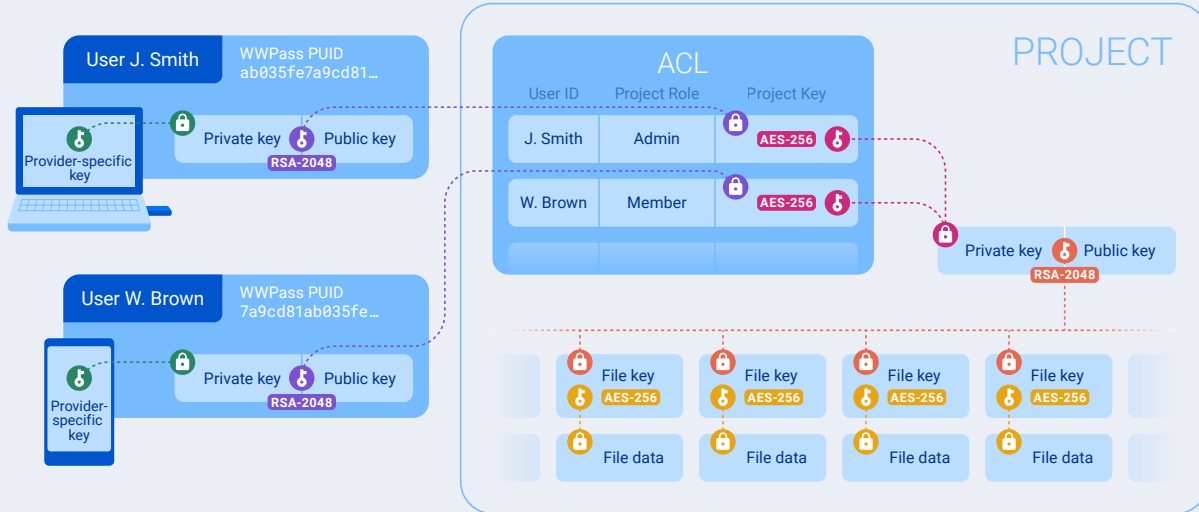
Obsolete usernames and passwords eliminated

Transitioning to password-free authentication

password-free authentication, it has no access to the Company's document management system, no access to user tokens, and zero knowledge about users.

Users own and manage their WWPass Keys, and are **easily able to restore them if lost or damaged without administrator intervention** thanks to patented WWPass technology. In the event of a WWPass Key restore, the user's master key and NHRC are also automatically restored, meaning that the **user does not experience any disruptions** in access to projects or data.

Implementing client-side encryption for the Company's platform took just two months from start to finish. All activities involved — architecture, server-side API development, code review, and testing — were performed in close cooperation between WWPass and Company teams.



Client-side encryption for the Company's document management system

The Results

Better security, lower operational costs, happier users — and more growth to come

Thanks to WWPass' all-in-one solution, the Company was able to **surmount two of its greatest security challenges in a matter of months**, improving its competitive position in the global market. Additionally, due to outsourcing of authentication to WWPass, **operational costs for password resets and other administrative tasks were slashed** while also **eliminating vulnerabilities** resulting from the use of human-readable credentials. As a result, the Company is now able to offer an easy-to-use, GDPR-compliant, highly secure document management solution, providing data owners the peace of mind of knowing the Company has zero knowledge of or access to sensitive data. This opens substantial new markets to the Company, **dramatically increasing their growth potential** in a world increasingly concerned with security risks.

Perhaps just as importantly, by implementing WWPass Key solution, **user experience was dramatically improved** by eradicating usernames and passwords for good. This measure alone **saved at least one minute per user per day**, compared to other multi-factor authentication methods — as well as **improving staff productivity by 5%** due to a drop in password reset requests and help desk calls, and **reducing security system administrative efforts by 20%**.

WWPass' authentication and encryption solutions have worked so well for the Company that their next step is working with WWPass to integrate digital signatures for documents using the same WWPass Key. **Isn't it time that your business starts down the same road?**