ATABASCA
POWERED BY WWPASS TECHNOLOGY

Customer Case Study

Wachstum mit Sicherheit – Am Beispiel eines SaaS-Unternehmens für Dokumentenmanagement

Egal in welcher Industrie oder in welchem Anwendungsbereich, heutzutage stehen alle digitalisierten Unternehmen vor zwei kritischen Sicherheitsherausforderungen:

1. **Die Unternehmen müssen sicherstellen, dass Nutzer auch diejenigen sind, für die sie sich ausgeben und**
2. **Die Unternehmen müssen garantieren, dass alle vorhandenen Daten geschützt werden – sowohl während der**

Speicherung als auch während der Übertragung.

Um diese Anforderungen zu erfüllen, bietet die **von Atabasca Systems AG (ATABASCA) bereitgestellte WWPass Technologie eine All-in-one-Lösung für eine Multifaktorauthentifizierung und client-seitige Verschlüsselung**, die Ihrem Unternehmen hilft, diese beiden Herausforderungen zu meistern. Und zwar nahtlos, sicher und ohne Ihren bisherigen Workflow zu stören.

Wir möchten Ihnen anhand eines konkretes Beispiel präsentieren, wie ein ATABASCA-Kunde **diese Sicherheitshürden gemeistert und dabei gleichzeitig die Möglichkeit für ein globales Wachstum geschaffen hat**. Die Software as a Service (SaaS) Dokumentenmanagement-Plattform unseres Kunden bietet eine Lösung, die nahezu jedes moderne Unternehmen benötigt: Cloudbasiertes Workflow- und Dokumentenmanagement, mobiles Arbeiten, Reportings und Analysen und ein digitales System für den Austausch und die Verwaltung von Dateien.

Mit einem bestehenden Portfolio von mittleren bis großen Kunden, sowohl im privaten als auch im öffentlichen Bereich, ist die Beispiel-Firma nach der Zusammenarbeit mit ATABASCA nun bestens aufgestellt für weiteres Wachstum. Die Zusammenarbeit mit ATABASCA **hat nicht nur die Sicherheit gestärkt, sondern gleichzeitig die operationale Effizienz und die User Experience verbessert**.

Die Herausforderungen

1 Eindeutige Kundenauthentifiziereng basierend auf E-ID

2 Client-seitige Verschlüsselung der Nutzerdaten

Um neue Kunden weltweit zu akquirieren, musste das Unternehmen **zwei kritische Herausforderungen** für ihr Dokumentenmanagement lösen. Aufgrund der Datenschutzgrundverordnung (DSGVO) musste eine bessere Nutzerauthentifizierung für interne Anwender (wie Systemadministratoren) und externe Anwender (Kunden des Unternehmens) eingeführt werden, um die Vertraulichkeit und Sicherheit der Daten zu gewährleisten. Gleichzeitig wollte das Unternehmen die allgemeine Sicherheit ihrer Produkte stärken. Denn bislang wurden Dokumente unverschlüsselt in der Cloud gespeichert. Dadurch ergab sich das Risiko, dass während Backups, Systemupdates und anderen Wartungsroutinen, Dateien potentiell von Systemadministratoren oder anderen internen Nutzern hätten eingesehen werden können. **ATABASCA konnte beide dieser Probleme für das Unternehmen meistern**: Mit dem Einsatz der **Secure Universal Identity von WWPass (SUID)**, welche die Notwendigkeit von Nutzernamen und Passwörter abschafft und gleichzeitig eine nahtlose Ende-zu-Ende-Verschlüsselung erlaubt.

1 Eindeutige Kundenauthentifizierung

Um die erste Herausforderung anzugehen – eine eindeutige und sichere Nutzerauthentifizierung – ergab eine Analyse **vier mögliche Lösungen**:

1. Zwei-Faktor-Authentifizierung mithilfe von SMS-Nachrichten als zweiten Faktor.
2. Zwei-Faktor-Authentifizierung mit einem One-time Password (OTP) als zweiten Faktor.
3. Starke Authentifizierung mithilfe einer Smartcard.
4. Starke Authentifizierung mithilfe der SUID von WWPass.

Wegen des großen Kundenstammes und dem häufigen Hinzufügen und Wechseln neuer Nutzern und Unternehmenskunden, wurde eine **Authentifizierung mithilfe von klassischen Smartcards schnell verworfen**. Smartcards bieten wenig Flexibilität, skalieren schlecht und verursachen hohe Kosten. **Die SMS-basierte Zwei- Faktor-Authentifizierung wurden ebenfalls gleich verworfen**, in diesem Fall wegen der inhärenten Sicherheitslücken. Tatsächlich empfiehlt das NIST (National Institute of Standards and Technology) seit 2016 nicht länger den Einsatz von Zwei-Faktor- Authentifizierungen via SMS. Im neusten Entwurf ihrer „Digital Identity Guidelines (Special Publication 800-63B)" gehen sie sogar noch einen Schritt weiter: „Out-of-band verification using SMS is deprecated, and will no longer be allowed in future releases of this guidance."

Während die OTP-basierte Zwei-Faktor-Authentifizierung eine sichere Out-of-band-Authentifikation nutzt, zum Beispiel mithilfe einer App, ist die **User Experience alles andere als ideal**; denn Nutzer müssen nicht nur mit einem, sondern gleich mit zwei Passwörtern hantieren. Außerdem hätte die Implementierung von OTP oder Pusch Benachrichtigungen verlangt, dass das Unternehmen teure, zusätzliche Hard- und Software einsetzte — inklusive eines zusätzlichen Servers nur für OTP, mit sehr hoher Verfügbarkeit und geografischen verteilten Mirrors für Backups oder Notfallanwendungen. **Nach diesen Überlegungen war die beste Lösung klar: Die passwortfreie Authentifizierung von WWPass**.

2 Client-seitige Verschlüsselung der Nutzerdaten

Für die zweite Herausforderung – dem Schutz der Kunden-dokumente — **benötigte das Unternehmen eine client-seitige Ende-zu-Ende-Verschlüsselung, so dass die Nutzerdaten zu keinem Zeitpunkt unverschlüsselt vorliegen würden**. Diese Art der Verschlüsselung verlangt ein sorgsames Management der Private und Public Keys. Auch darin steckt eine Herausforderung: **Wie speichert, managet, widerruft und gibt man solche Schlüssel aus, so dass sie sowohl sicher als auch einfach nutzbar sind?**

Eine der großen Stärken der Plattform unseres Kunden ist die Verfügbarkeit sowohl als Webanwendung, als auch als Multi-plattform-App. Dadurch ist allerdings das Speichern und Management der Private Keys im Browser, dem Betriebssystem oder in einem vertrauenswürdigen Plattformmodul als Option nicht flexibel genug.

Ein **lokales Hardware-Sicherheitsmodul (HSM) zur Verwaltung der Keys zu verwenden, war ebenfalls keine praktikable Lösung**, schließlich hätte das bedeutet, dass sowohl interne Ressourcen für das Management und die Grundversorgung eingesetzt, als auch Servicerahmenverträge abgeschlossen werden müssten. Außerdem hätten die HSM-basierten Cloudangebote nicht gänzlich das Problem des unautorisierten Zugangs zu privaten Keys durch Administratoren der HSM-Systeme gelöst.

Eine Möglichkeit – **die Ableitung der Verschlüsselungskeys von Nutzerpasswörtern** und die Speicherung dieser in verschlüsselter Form auf dem Server – wird zwar von vielen Anbietern akzeptiert, hat aber **eine ganze Reihe von unakzeptablen Limitierungen**. Denn Passwörter müssen in den meisten Fällen „menschenlesbar" sein; sie weisen deshalb häufig einen niedrigen Komplexitätsgrad auf, selbst wenn sie den herkömmlichen Standards für „starke Passwörter" genügen. Daher haben alle Keys, die auf solchen Passwörtern basieren, eine niedrige Entropie.

In der fatalen Konsequenz bedeutet ein System, bei dem Keys auf Basis von Passwörter generiert werden, auch, dass eine Passwortänderung der Nutzer das Keymanagement erschwert oder gleich unmöglich macht – und als „Lösung" eine Passwortänderung zu unterbinden bedeutet, dass man **nicht DSGVO-konform handelt**.

Glücklicherweise hat die WWPass-Lösung für client-seitige Ende-zu-Ende-Verschlüsselung keine dieser Mängel. Denn **WWPass nutzt verkettete kryptographische Schlüssel in Kombination mit einem Masterkey, der durch die SUID generiert wird**, es gibt keine Notwendigkeit immer wieder Keys zu widerrufen und neu auszugeben. **Nutzern muss nicht einmal bewusst sein, dass Keys existieren, genauso wenig, wie sie sich um Passwörter sorgen müssen. Und trotzdem sind alle Daten sicher**.

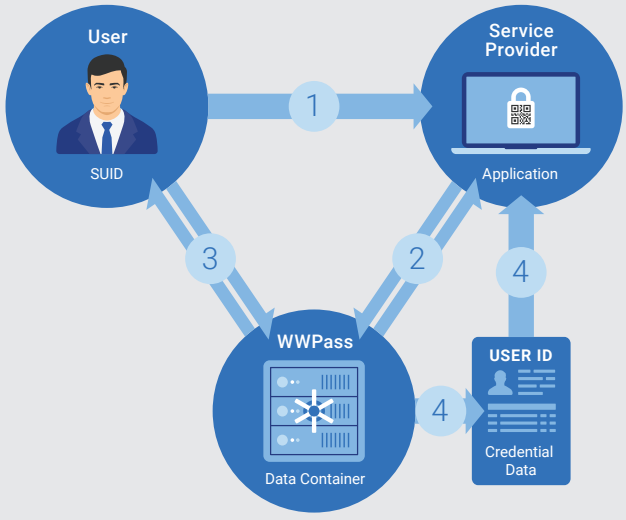
Die Lösung

Ihre E-ID für passwortfreie Authentifizierung und praktische client-seitige Verschlüsselung

Starke Authentifizierung ohne Passwort

Die WWPass All-in-One-Lösung meistert beide Herausforderungen des Unternehmens mit nur einem Gerät – angefangen mit einer einfacheren Authentifizierung ganz ohne Passwort. Jedem Nutzer wird eine **SUID** ausgehändigt, **ein kryptografischer Microcomputer in der Form, die am besten zum Nutzer passt**: Mobile App, Smartcard oder ein USB+NFC Schlüsselanhänger. Die Nutzer können ihre SUID über ein Webportal oder eine mobile App selbst verwalten (eine von WWPass-patentierte Lösung) und auf dem Gerät selbst werden keinerlei persönliche Informationen gespeichert.

Die verschiedenen Formen einer WWPass SUID



1. Der Nutzer meldet sich mithilfe seiner SUID an.
2. Der Service Provider und WWPass authentifizieren sich gegenseitig.
3. SUID und WWPass authentifizieren sich gegenseitig.
4. WWPass sendet NHRC Daten des Nutzers an den Service Provider.

Die passwortfreie Authentifizierung von WWPass

Falls ein zusätzlicher Faktor, wie ein PIN oder Fingerabdruck/ Gesichtserkennung benötigt wird, ist dies frei programmierbar.

Sobald sich der Nutzer erfolgreich mit seiner SUID authentifiziert hat, werden die vorher fragmentierte und verschlüsselt gespeicherte **non-human-readable credentials (NHRC) anstelle eines Nutzenamen- Passwort-Paares** aus dem von **WWPass patentierten „Distributed Data Storage System"** an den Service- Provider für die Identifizierung gesendet . Dies hat **zwei Vorteile**: Erstens, sollten Hacker an NHRC-Daten gelangen, wären diese nutzlos. Schließlich gibt es keinen Ort, an dem man sie zur Authentifizierung eingeben kann. Zweitens, Verschlüsselung und Fragmentierung sorgen dafür, dass alle Nutzer gegenüber WWPass komplett anonym bleiben.

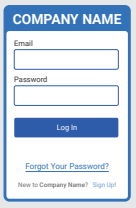
Die komplette Umstellung auf die passwortfreie Authentifizierung von WWPass **erfolgte ohne jegliche Unterbrechung** des normalen Betriebsablaufs. Bestehende Nutzer wurden zuerst migriert, in dem sie sich zunächst in das System mit ihrer neuen SUID eingeloggt haben und diese wurde anschließend mit dem bestehenden Nutzernamen und Passwort verknüpft. Neue Nutzer wurden direkt mit NHRC-Daten eingeführt und mit dem vorhandenen Identitäts- und Zugangsmanagement verknüpft. Nach der 3- monatigen Übergangsphase wurde der Log-in über Nutzernamen und Passwort komplett abgeschaltet, was eine **Reihe von Vorteilen mit sich brachte**:

- **Bequemlichkeit für Nutzer**: Einfacher Zugang zu allen Plattformenlösungen – Web, Mobile und Desktop – ohne sich ein Passwort merken zu müssen.
- **Entlastung für den IT-Support**: Nutzer können ihre SUID selbst verwalten, ohne externe Hilfe.
- **Vorteile für das Unternehmen**: Keine sinkende Produktivität durch das Zurücksetzen von Passwörtern oder durch temporäres Aussperren.
- **Flexible Formen**: Die SUID kann sowohl als iOS-/Android-App, Smartcard oder als USB+NFC-Schlüsselanhänger ausgestellt werden, je nach Wunsch des Unternehmens und des Nutzers.
- **Keine menschenlesbaren Daten**: Die Nutzung von NHRC-Daten eliminiert eine der grundlegenden Gefahren von Sicherheitslücken rund um schwache, gestohlene oder Standard-Passwörter.
- **Genügt den regulatorischen Anforderungen**: Die Zusammensetzung von WWPass Authentifizierung aus mehreren Sicherheitsfaktoren und -ebenen stellt sicher, dass die Technologie mit DSGVO, HIPAA, NIST, PCI DSS und anderen Vorgaben konform geht.
- **Zero-Knowledge-Protokoll**: Das Identitätsmanagement und die Rechteverwaltung werden vom Zugangsmanagement getrennt. Dabei wird die Authentifizierung mit Zero-Knowledge-Technologie zu WWPass outsourct.

Bequeme, client-seitige Verschlüsselung

Die zweite Aufgabe des Unternehmens – die Einführung einer client-seitigen Ende-Zu-Ende-Verschlüsselung, ohne die User Experience zu verschlechtern – wurde ebenfalls mithilfe der WWPass-SUID gelöst. **Da die SUID ebenfalls einen Masterkey erstellen kann, der das Gerät niemals verlässt, kann sie für client-seitige Verschlüsselung verwendet werden.**

Diese Lösung **sichert die Nutzerdaten mithilfe einer Reihe von kryptografischen Schlüsseln**. Basierend auf dem Masterkey generiert die SUID (Bild auf der Seite 4) jeweils einen provider-spezifischen Key. Dieser wird dann sicher zum Gerät des Nutzers übertragen (Mobiltelefon, Tablet oder Computer), um ihn über die Mobil- oder Webapplikation einzusetzen, sobald dieser angefordert wird. Diese Applikation benutzt den providerspezifischen Key, um jeweils einzeln das individuelle Projekt, die Dateien- Schlüssel und natürlich auch die Inhalte der gespeicherten Dateien zu verschlüsseln. Das bedeutet, dass **zu keinem Zeitpunkt eine Notwendigkeit besteht, den Masterkey der SUID jemand anderem zu enthüllen** – nicht gegenüber einem Cloudspeicheranbieter,



Überflüssig

Phase 0:
Nutzernamen und Passwörter
Unsicher und unbequem

Empfohlen

Phase 1:
WWPass Log-in
Optionale Nutzung des eigentlich überflüssigen Nutzernamens und Passworts

Verpflichtend

Phase 2:
WWPass Log-in
Nutzernamen und Passwörter werden komplett abgeschafft

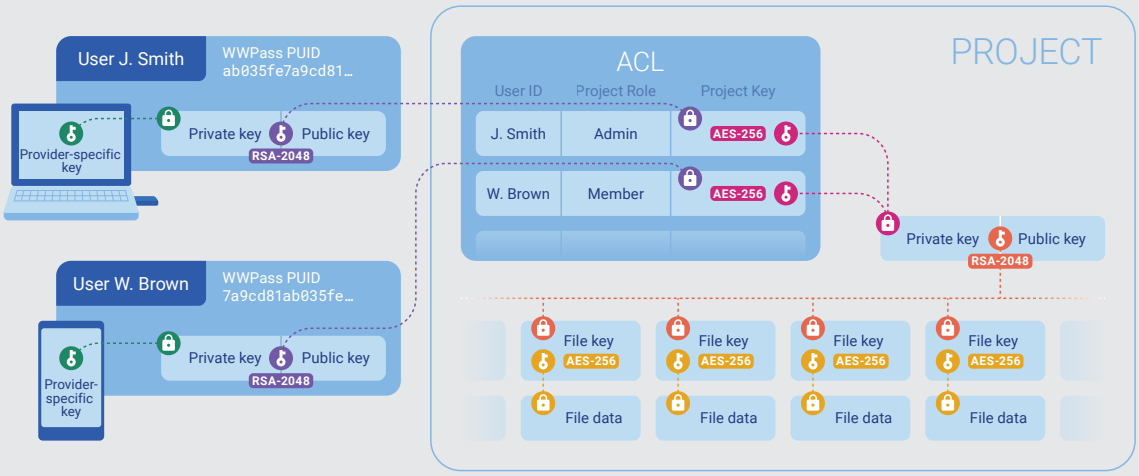
Umstellung auf eine passwortfreie Authentifizierung

nicht gegenüber WWPass, noch nicht einmal gegenüber dem eigenen Unternehmen.

Zusätzlich zur Implementierung der client-seitigen Verschlüsselung durch die WWPass-Technologie, setzte das Unternehmen ein Key-Management auf, das den NIST-Empfehlungen (National Institute of Standards and Technology) entspricht. Dabei werden Rollen je nach Aufgabenbereich getrennt, Wissen geteilt und so doppelt kontrolliert. Infolgedessen sind **Systemadministratoren nur noch für Systemsupport und Backups zuständig – sie haben darüber hinaus keinen Zugang zu unverschlüsselten Dokumenten oder Keys** und müssen auch nicht die Authentifizierungen verwalten. Zwar ist WWPass für die passwortfreie Authentifizierung verantwortlich, hat aber keinerlei Zugang zu den Dokumenten des Unternehmens, besitzt keinen Zugriff auf Usertokens und kennt die Nutzer nicht.

Nutzer **besitzen und managen ihre WWPass-SUID selbst** und können diese, sollte die SUID verloren gehen oder beschädigt werden, **ganz einfach wiederherstellen** – Dank der patentierten WWPass-Technologie, ohne dass ein Administrator überhaupt eingreifen muss. Im Falle einer SUID-Wiederherstellung, werden Masterkey und Zugang zu NHRC ebenfalls automatisch wiederhergestellt. Somit kann der Nutzer auf Projekte und Dateien durchgängig zugreifen und erfährt **keinerlei Unterbrechung in seiner Arbeit**.

Die **komplette Implementierung der client-seitigen Verschlüsselung für die Unternehmens-Plattform dauerte nur 2 Monate**. Alle nötigen Schritte – Softwarearchitektur, serverseitige API-Entwicklung, Code Review und Testing – wurden in enger Kooperation zwischen ATABASCA und dem Team des Unternehmens durchgeführt.



Client-seitige Verschlüsselung für das Dokumentenmanagement-System des Unternehmens

Das Ergebnis

Client-seitige Verschlüsselung für das Dokumentenmanagement-System des Unternehmens

Dank der WWPass All-in-One-Lösung war das Unternehmen in der Lage, **zwei seiner größten Sicherheitsrisiken in wenigen Monaten hinter sich zu** lassen und dabei gleichzeitig seine Wettbewerbsstellung im weltweiten Markt zu verbessern.

Außerdem konnten durch Outsourcen der Authentifizierung an WWPass die **operationalen Kosten für Passwort-Zurücksetzungen und andere administrative Tätigkeiten gesenkt werden**, während Sicherheitslücken geschlossen wurden, die durch menschenlesbare Zugangsdaten entstehen. Dadurch besitzt das Unternehmen nun eine einfache, DSGVO-konforme, sehr sichere Dokumentenmanagement-Lösung, die den Dateneigentümer gleichzeitig die Sicherheit bietet, dass das Unternehmen kein Wissen über sensible Daten verfügt. Das eröffnet dem Unternehmen ganz **neue Märkte und verbessert das Wachstumspotential**, in einer Zeit in der Schutz vor Sicherheitslücken immer wichtiger wird.

Außerdem konnte durch den Einsatz der WWPass-SUID-Lösung die User Experience immens verbessert werden. Schließlich müssen sich Nutzer nun nie wieder Nutzernamen oder Passwörter merken.

Im Vergleich zu anderen Multi-Faktor- Authentifizierungslösungen, **spart jeder Nutzer** durch diese Maßnahme allein **eine Minute Zeit pro Tag** ein. **Die Produktivität** der Belegschaft konnte **gesteigert** werden, da Anfragen für Passwort-Zurücksetzungen von nun an wegfielen, der IT-Support seltener angerufen wird und der **Verwaltungsaufwand für das Sicherheitssystem reduziert wird**. Dabei können sich die Systemadministratoren auf Maßnahmen mit höherer Priorität konzentrieren.

Die Authentifizierung und Verschlüsselung mit WWPass hat für das Unternehmen so gut funktioniert, dass es nun mit ATABASCA daran arbeitet, digitale Signaturen mithilfe der selben SUID umzusetzen. **Kontaktieren Sie uns, wenn Sie auch von diesen Vorteilen profitieren möchten.**

Rubisacherrain 25, CH-6440 Brunnen, Switzerland

Erfahren Sie mehr unter: wwpass.com
+41 41 820 57 21 | info@atabasca.ch