wwpass®

Secure Universal Identity

What is WWPass?

Who We Are

WWPass is an Identity As A Service (IDaaS) company specializing in identity, authentication, access management & secure data storage.

What We Do

We battle data breaches and identity crimes with advanced authentication and data storage technology to deliver a user experience as convenient as it is secure.

Who We Serve

Organizations of all sizes in all industries with valuable information to protect who want to provide their customers and employees with superior security and convenience.

Use Cases:

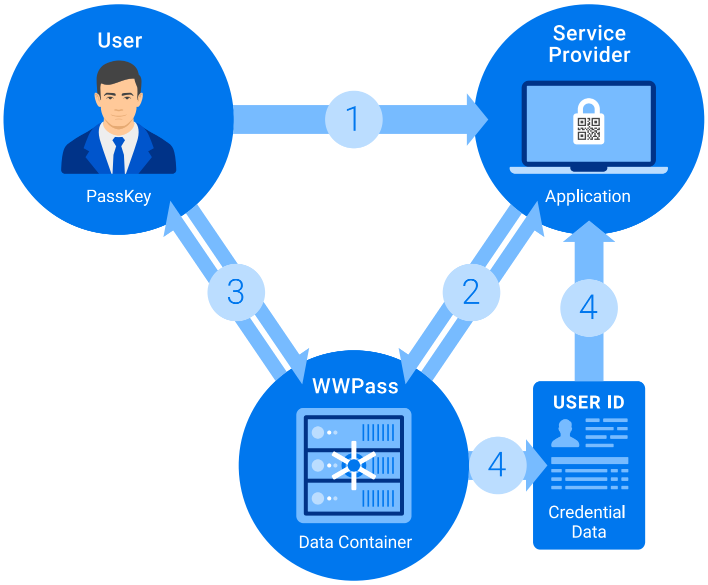
- Right-Factor Authentication for
  - Employees
  - Vendors/Contractors
  - Customers/Citizens
- Convenient, secure and password-less account access for users/customers
- Consolidation of many ID cards into one
- Consolidation of hard tokens, fobs & badges
- Secure, convenient employee and user logins
- Access management for controlled areas and sites
- Revenue protection with unshareable credentials for paid services

How We're Different:

- **Elimination of human readable credentials** – This is the leading cause of data breaches and identity crime.
- **ID consolidation** – combine all your accounts and ID cards into one single card. This includes:
  - Driver's License, professional license, hunting and fishing license or voter registration card
  - Birth certificate, Social Security card or passport
  - Employee or student ID cards
  - Health, dental, live and auto insurance cards
  - Membership cards (stores, museums, libraries, gyms, clubs, AAA or commuter bus and rail)
  - Rewards cards (frequent flyer, diner, hotel or rental car)
- **Limitless data segregation** – User and Service Provider accounts are completely isolated from each other, so one ID can work everywhere without cross contamination.
- **Secure Distributed Data Storage** – Extreme protection from hackers and resiliency for disasters.
- **ID Counterfeiting Prevention** – Scanning the ID instantly reveals if it is fake, stolen or modified.
- **Adaptability** – Easily integrate biometrics for additional layers of security.
- **Improved user experience** – One key opens many doors, and there's no need to remember lists of credentials which may already be compromised.
- **Reduced access management costs** – cut costs from password resets, using SMS as a second factor and using multiple authentication fobs or badges.
- **Revenue Protection** – Stop users from sharing redentials/ access with unpaying freeloaders.
- **Flexibility** – Choose from multiple form factors (Smartcard, USB, mobile, wearables, etc) to best meet the needs of any organization.

According to the Verizon's 2017 Data Breach Investigation Report, 81% of all data breaches result from using human readable credentials (HRC). In the U.S. alone, identity theft exceeded $112 billion over the previous 5 years.

How Secure Universal Identity Works



1. **User initiates login to service provider** using their WWPass PassKey.
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.

No Backdoors

The user's identity is unintelligible to attackers and it is never even disclosed to WWPass itself.

Credentials

are

Encrypted

then

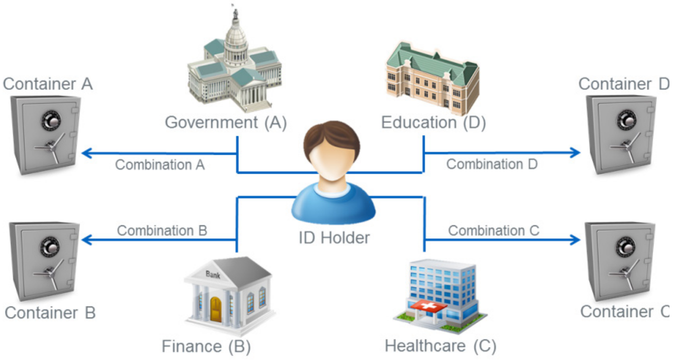
Fragmented

then

Geographically distributed

Limitless Data Segregation and Commitment to Privacy

- Link one ID card to unlimited service providers.
- Each link creates a unique "data container," accessible only to:
  1. ID holder
  2. Service provider



Minimum Requirements for Universal ID:

7 Laws → applied to → 6 Contexts

1. User control and consent:

Technical identity systems must only reveal information identifying a user with the user's consent.

2. Minimal disclosure for a constrained use:

The solution which discloses the least amount of identifying information and best limits its use is the most stable long-term solution.

3. Justifiable parties:

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4. Directed identity:

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5. Pluralism of operators and technologies:

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6. Human integration:

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human to machine communication mechanisms offering protection against identity attacks.

7. Consistent experience across contexts:

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

1. Browsing:

A self-asserted identity for exploring the web while giving away no real data

2. Personal:

A self-asserted identity for sites with which the user wants an ongoing but private relationship (including name and a long-term email address)

3. Community:

A public identity for collaborating with others

4. Professional:

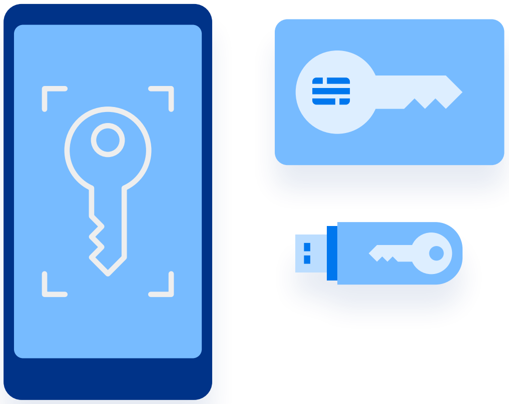
A public identity for collaborating issued by employers

5. Credit card:

An identity issued by financial institutions

6. Citizen:

An identity issued by the government



Basic Implementation Information

Identity authority prints and issues cards on site (similar to military RAPIDS)

- Card set contains 1 ID card and 2 service cards
- Identity authority agent activates card set at kiosk
- Identity authority agent pairs accounts to card
- Citizen can later pair their card with personal accounts (ex. Banking, medical, insurance, etc)
- The Citizen's ID card set can be used to login to accounts with all WWPass enabled Service Providers

Basic Use Information

Citizen inserts ID into smartcard reader

- Reader connects to WWPass to validate ID (one to many)
- Reader requests additional factors required by service provider (one to one)
  - Biometrics
  - Access code
- WWPass validates that the ID is real (not counterfeit) and that the correct person is presenting it (not an imposter)
- WWPass allows the citizen to pass through the security checkpoint or access to their account with the Service Provider

Peripheral Hardware Accessories

- Smartcard sets (1 PassKey ID and 2 Service Keys)
- Smartcard printers
- Smartcard readers
  - USB/keyboard/laptop port
  - Portable hand-held devices
- Smartcard kiosks
  - For issuing IDs
  - For validating IDs
- NFC door locks
  - Separate technology available on smart card platform

> "There are risks and costs to a program of action. But they are far less than the long range risks and costs of comfortable inaction."
>
> *— John F. Kennedy*

1155 Elm Street, Manchester, NH 03101

+1 888 997-2771
info@wwpass.com