

# WWPass Overview



## Background

Despite strong encryption, physically hardened server farms and other alleged safeguards, our most sensitive personal and business data is clearly vulnerable. Every week, we read about database breaches that impact millions of consumers and cost businesses dearly. Statistics back up the empirical impression that our data is not safe:

- In 2010, 8.1 million Americans were the victims of identity theft
- 85% of corporations have been breached in the last 24 months
- In 2010 there were over 100,000 phishing attacks, when fake websites impersonated a real one in order to trick visitors into divulging sensitive information
- The average cost to a corporation of a single data breach is over \$7 million, plus indirect costs such as increased customer churn
- The average cost to a consumer of a stolen identity is over \$3,000

Data and privacy protection fall into two areas:

- Access Control. There must a way to restrict access to the data or application to those who have proper authorization
- Secure Storage. Data must be stored in a way that protects against physical and electronic attack

Unfortunately, as the above data testifies, existing options fall short. Access control techniques are either weak (login/password, OpenID), or inconvenient for users (unique login/password for every application, one-time passwords). Storage protection methods such as encryption, firewalls, and physical security of web farms all offer would-be attackers points of vulnerability.

WWPass offers innovative, patent-pending authentication and storage technologies for enterprises, service providers and consumers that radically improve data safety in both of these areas.

## Current Vulnerabilities

As a corporation or online service provider, you have put a lot of time, effort, and money into securing the server farms that support your applications and databases. Yet how safe is your sensitive data? If you are like most companies, it is uncomfortably vulnerable.

- Most likely you require your customers, employees and business partners to authenticate into corporate or public services with nothing more than an easily-guessed login/password
- The lengths you have gone to to create thoroughly redundant storage systems have inadvertently multiplied the points of vulnerability to electronic attack
- Storing encryption keys and providing safety-valve “back doors” to servers create further exploitable areas of vulnerability

Whatever your specific applications and services, be they online or desktop-based, WWPass can greatly reduce their vulnerability—without sacrificing convenience.

## WWPass Secure Authentication

WWPass believes access control must be both secure and convenient. *Secure Authentication* is a WWPass service whose users hold a physical, cryptographic device called a PassKey that allows them to authenticate into WWPass-enabled applications. While such devices are already prevalent in the market, the PassKey is unique in several ways:

- It is not limited to a single application, but can be used for *all* WWPass-enabled applications
- It contains no personal identification information
- It is highly resistant to being hacked or key logged
- It can be used in conjunction with a second authentication factor such as a password for especially sensitive applications
- It is available in several form factors, including SmartCard, USB fob, NFC token
- If lost or stolen, it can be blocked and replaced instantly, electronically, and anonymously by the owner
- WWPass maintains no database of PassKey holders or their identities, eliminating another point of vulnerability
- Phishing is greatly diminished because *both* the user and the application authenticate themselves

## How it Works

In the WWPass scheme, the user:

- Holds a cryptographic PassKey that is unique but carries no personal information

- Presents the PassKey to authenticate into any WWPass-enabled application
- Provides a second authentication, such as a password, if requested to do so by the application
- “Looks” different to every application, even though the same PassKey is used

The application:

- Also has a cryptographic code that is unique but registered with WWPass
- Can set the number of authentication factors it requires depending on sensitivity level
- Is identified to the user

A transaction only takes place when *both* parties have authenticated with WWPass. This greatly reduces phishing.

WWPass provides several additional features and security safeguards:

- WWPass is also authenticated and cannot be emulated
- WWPass maintains no database of user identities
- Lost or stolen PassKeys can be blocked and replaced online by the user quickly and anonymously

## Examples of Use

WWPass Secure Authentication is ideal for the following applications:

- Authenticated access to any website involving sensitive transactions or data
  - Online banking and financial services
  - Remote access to corporate VPN services
  - Protected cloud storage
- Authenticated access to desktop-resident applications
  - Electronic safe deposit boxes
  - Secure password storage
- Controlled access to physically secure areas
- Portable Digital Rights Management (DRM)

## Advantages

- Single authentication method and device for everything
  - PassKey unlocks all WWPass-enabled applications
- Bi-lateral

- Mutual authenticity assurance guards against phishing
- Multi-factor capable
  - Sensitive applications can require additional factors
- User anonymous to WWPass
  - No hackable database of identities
- Immediate, ubiquitous, private support
  - Offered via web site
  - User can disable and replace lost or stolen PassKey without revealing identity to anyone

## WWPass Dispersed Storage

*Dispersed Storage* takes data storage to an unprecedented level of security by fragmenting and dispersing encrypted data to storage centers around the world. This technique results in far safer data storage for many reasons:

- A complete set of stored data does not exist in any one place. Hacking into a WWPass server yields only data fragments
- Stored data is not linked to any personal identification information. Hacking into a WWPass server does not yield data that can be associated with any particular person
- WWPass-stored data is encrypted, but unlike other storage services, WWPass does not hold any encryption keys. Enticing a WWPass employee to assist in a hack would be fruitless
- Stored data can *only* be re-assembled and delivered upon presentation of the owner's and the application's PassKeys. Not even WWPass has access to complete data
- There are no back doors to data stored on WWPass

## How it Works

In the WWPass scheme, data is stored in four steps:

- Step 1: Incoming data is encrypted using an encryption key that is unknown to WWPass
- Step 2: Encrypted data is divided into twelve discreet fragments
- Step 3: Data fragments are disbursed to data centers located around the world
- Step 4: Data can only be re-assembled, decrypted and delivered with proper user and application authentication

## Examples of Use

WWPass Dispersed Storage is ideal for the following applications:

- Storage of any highly sensitive data
  - Corporate databases
  - Medical records
  - Legal files
  - Financial records
  - Customer records
- Enhanced Digital Rights Management (DRM)
- Electronic safe deposit box
- Fortified cloud computing

## Advantages

- Data is accessible only with both the user's and the application's PassKey
- No single point of vulnerability
  - Hacking into a WWPass server would yield only partial, unidentifiable, encrypted data
- Fragments are stored redundantly
- No back doors
  - Although data is encrypted, neither WWPass nor the application holds encryption keys
- Data is anonymous
  - WWPass does not know data owner's identity

## The Value of WWPass to You

Implementing WWPass provides enterprises and Service Providers with multiple benefits:

- Provide your employees and customers with a secure yet convenient authentication method that they can also use for many other purposes
- Better secure VPN and other internal resources
- Offer users greater assurances against phishing
- Can be used with all applications, be they web- or desktop-based
- Can also be used to control access to physically-secure areas
- Safeguard your most valuable and sensitive data against costly, reputation-damaging incursion

- Offer your users peace of mind that their data is stored far more safely than previously possible
- Can be used with any service where data sensitivity is a factor: online banking and financial transactions, cloud storage, medical records, “e-vault” services, etc
- Differentiate services in the marketplace
- Add new, “fortified” versions of existing services

## Implementing WWPass

WWPass technology is easily integrated into existing applications and environments.

- Full Secure Authentication SDK/API's are available for most popular web server modules, such as Apache
- A full Dispersed Storage SDK/API is available for integration into your database applications
- WWPass' specialized Developer Support Desk will provide assistance as needed
- Dispersed Storage is also available as a standalone module, Personal Secure Storage (PSS), with a full user interface and documentation. PSS can also be private-labeled
- PassKeys can be purchased from WWPass in low quantities or in bulk
- No need to initialize or otherwise support PassKeys; your users will be able to do that themselves using our web-based Key Services tool

## Contacting WWPass

For further information, contact WWPass at 1-888-WWPASS1 (1-888-997-2771) or visit [www.wwpass.com](http://www.wwpass.com).