Managing
Digital Identities

Best Practices for Securing
Digital Identity Management Systems

VDart Digital

Contents

What is a Digital Identity?

A "digital identity" is a broad term that refers to the information about an individual or organization that exists on the internet. It not only contains the history of your behavior and actions online, but also can contain public and sensitive information that is unique to you or your organization. This type of information can be used for authenticating a user for various applications depending on the industry. Digital identities, for the most part, can be broken down into 4 different categories: a credential, character, user, and reputation.

Figure 1. Digital Identity break down.

As a credential

This typically refers to personal information that is unique to you as a person or company such as your name, your date of birth, your residence, your social security number, and your company's EID number. These are pieces of information that can often be targets of identity theft.

As a character

This often refers to information such as your social media accounts, dating apps, and career sites.

As a user

This describes the history of an individual on the internet and can cover a wide variety of historical actions ranging from website visits, online purchases, your search history, and even what emails you've opened and read.

As a reputation

This refers to data that describes various kinds of personal history like criminal records, credit scores, employment history, and residential history.

Benefits of Digital Identities

Improved efficiency

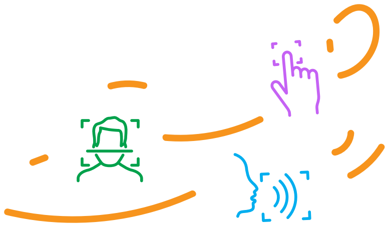
Having a single organized folder of various personal attributes allows for fast and reliable authentication for many applications ranging from banking to social media. Additionally, litigation issues can be mitigated when using digital identities because the system accessing your digital identity can have a higher degree of confidence of user identity. This can reduce the cost and regulations often required for business to conduct financial transactions.

Improved customer experience and security

Overall customer experience is enhanced because of how easy and convenient everyday transactions can be with a digital identity. Not having to constantly key username, passwords, credit card information, and other sensitive material not only reduces errors, but it makes the entire transaction much more efficient and secure.

Figure 2. Traditional Identity Management Systems Vs. Best in Class DIM's

Traditional Identity Management Systems	Best in Class DIM's
Fragmented and disparate databases create an inefficient user experience that requires multiple logins and passwords	Uses social logins like Facebook, Google, or LinkedIn and removes the need of users to keep track of usernames/passwords
Often over-collects unnecessary detailed user data	User-centric control over which specific data is shared to their applications
User data is highly centralized and a single point of failure	Uses blockchain technology to decentralize user data Encrypts and hashes user data to protect information against data breaches
Often only uses username/password style login credentials	Uses multi-factor authentication (MFA) that enables multiple, unique metrics of authentication like security keys, biometrics, and even text message codes



Risks of Digital Identity Management Systems (DIMS)

Traditionally, DIMS tend to be fragmented, relatively insecure, and overly centralized. While centralization can increase efficiency and convenience for users, if proper security protocols aren't followed by the DIMS sensitive information can be left vulnerable to hacks and identity theft. Additionally, owners of the digital identity often don't have control over which specific pieces of information they are sharing and can lead to privacy concerns for users. Allowing the user to moderate exactly which and when pieces of sensitive information are shared can drastically reduce privacy concerns as the flow of information is directly controlled and distributed with the user's knowledge rather than just granting total access to their full list of sensitive details.

Blockchain and Digital Identities

What is a blockchain?

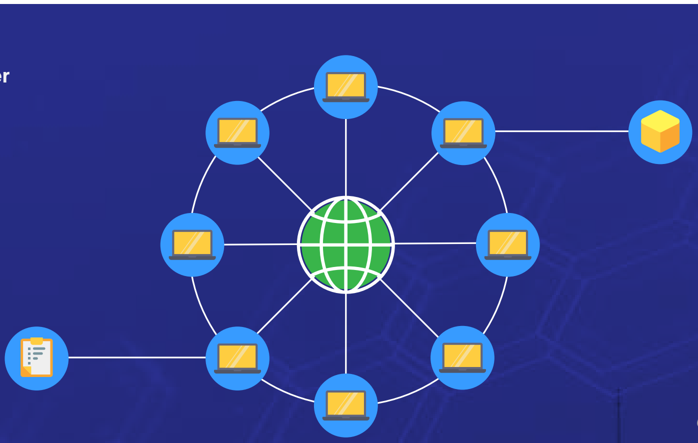
A blockchain is a decentralized ledger. Rather than storing whole, complete chunks of information in a single centralized location, pieces of the information are broken up and stored in many different locations across a network. Then, when the user wants to access the information, those pieces of information are reassembled again for access.

Imagine having a document with highly sensitive information in it: in traditional file management systems, the document is stored as a single discrete file and accessed through a clear hierarchy of file structures. This level of security and organization is perfectly fine for everyday use, but when someone has something that they want to keep private or anonymized, traditional file structures and security protocols can lead to vulnerabilities in a management system.

With a blockchain implemented management system, the file that was once stored in a single location is chopped up into thousands of pieces and spread out across an entire network. When combined with proper encryption, this distributed system becomes drastically more secure as it can only be reassembled with the proper encryption key.

In addition to being more secure, blockchains are immutable. Blockchains are decentralized ledgers which means there is no single source of record keeping. Part of the blockchain validation process is a network-wide consensus of any ledger update. Every time the network is updated, those clusters of ledger updates (called "blocks") are chained to the prior batch of ledger updates to give a perfect record of all transactions/updates on the blockchain ledger. Because every single prior block is kept on the ledger in chronological order, the ledger is said to be "immutable" due to the incredible difficulty behind faking or spoofing a transaction.

Figure 3. Decentralized Ledger



Best Practices for Digital Identity Management Systems

1. **Reduce personalized user data exposure** - By minimizing the collection and use of unnecessary user data, digital identity management systems can reduce a user's exposure in the event of a data breach/hack. Often times a business can make the mistake of using overly identifiable information (like social security numbers for example). Rather, the database should either use some type of coded usernames or, when possible, encryption to protect sensitive material.

2. **Offer multi-factor authentication (MFA)** - There many many MFA options ranging from a simple SMS text code to physical hardware that generates a temporary key. All these MFA options have their pros and cons, but the common denominator is they all offer a second line of defense in the event a hacker tries to falsely authenticate as a user. By enabling multiple forms of unique authentication, the business can have a higher degree of accuracy when authenticating users.

3. **Encryption** - The act of encryption, while not as secure as hashing, offers a great layer of protection in the event of a hack. Encryption is a two-way function that will scramble a message while transmitting data and then unscramble it with the use of an "encryption key". As long as the hacker does not maintain access to the encryption key, they will never be able to retrieve the encrypted data. However, a major problem with encrypted messages is often times the encrypted password is stored on the same server as the encryption key. While unlikely, it is still possible for a hacker to steal a list of encrypted passwords or user data AND the encryption key -- rendering the encryption meaningless.

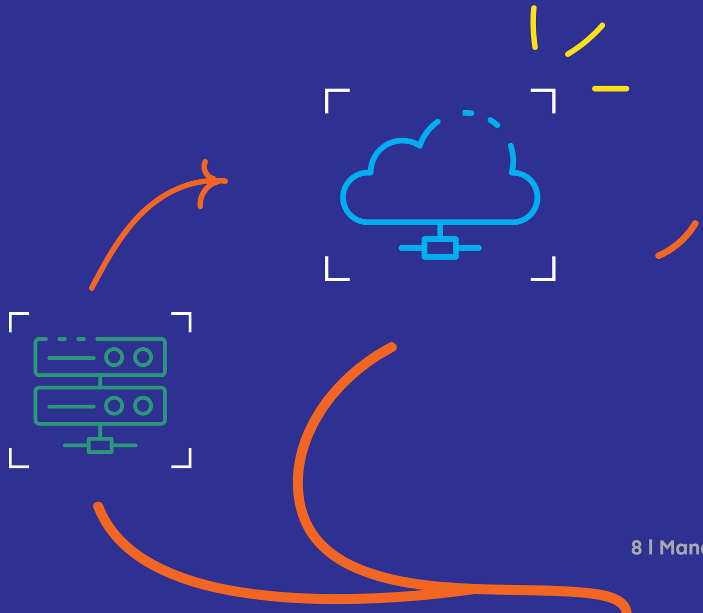
4. **Hashing** - One way to add an additional layer of security to the encryption process is through "hashing". Hashing is the process of using a function that will receive a user input and reassign it another value and store it in a database. The benefit of hashing functions is the database never physically stores any of the user data and only stores the unique end product of the hashing function called a "hash value". And since it is essentially impossible to guess what hashing function a system uses, even in the event of a hack, the list of hashvalues provides no vulnerability to the user data.

How can we help?

VDart Digital has a strong track record of providing simple and scalable digital identity management solutions. We partner with industry leaders to provide a robust yet customizable management system that fits their growing security needs. From biometric authentication on mobile apps to financial security with blockchain technologies, VDart will curate an easy, streamlined solution that works for you.

One of VDart's most recent projects provided a seamless transition from the client's original platform to the best in class identity management platform:

- The platform is a simple, flexible, and secure identity management solution that provides real-time authentication and will continue to seamlessly support millions of users as they continue to migrate in the following years
- The final product was a highly available cloud-based and containerized cluster infrastructure that allows for a wide variety of secure authentications and social login integration such as Facebook, Apple, and Google
- On average, we saved 25% of the projected cost: the architecture is so flexible and robust that it allows multiple environments to be shared within the same cluster and, when shared, can provide a 50% cost reduction
- Simplified authentication process and created a better user experience with seamless integration between phone and vehicle while delivering seamless access to valuable information and applications



STAY CONNECTED

VDart Digital
sales@vdartdigital.com
https://www.vdart.com/solutions/

Connect With Us
https://www.linkedin.com/company/vdartdigital

Follow Us
https://twitter.com/vdartdigital

VDart Digital