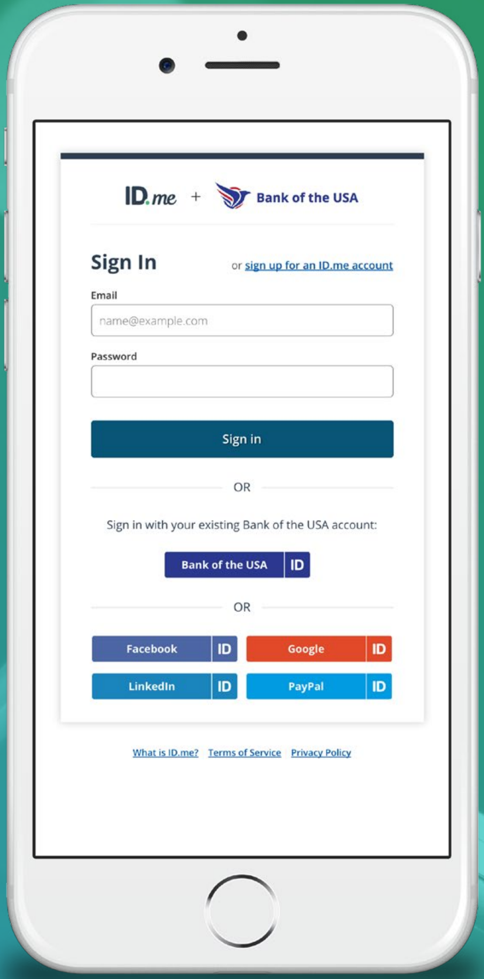
How Federated Identity Can Increase Access to Services and Benefits Online

ID.me



Americans choose federated identity for account creation and sign-in whenever they click “Login with Google” or “Login with Facebook.”

In 2016, a record high 88% of all online accounts were created with federated logins.

And it’s no wonder – the average user today manages 90 unique online accounts.

People are unable to remember a new, unique password for all of their accounts, a problem that federated identities solve to streamline account creation and sign-in for low-risk transactions.

Federated identity offers an opportunity for government agencies and enterprises to drive account registration and increase access to important services. The challenge lies in strengthening those logins to meet federal standards.

What is Federated Identity?

Federated identity refers to linking an individual's electronic identity, authentication and personal attributes across multiple websites and identity management systems, often in tandem with a Single Sign-on (SSO). When the user logs into an account using a federated identity, the website trusts the identity provider to validate the credentials using industry standard security protocols such as SAML 2.0, OpenID Connect, and OAuth 2.0.

Why Do Users Prefer Federated Identity?

Users choose federated logins over individual logins because they solve two problems with the user experience: password fatigue and registration abandonment.

PASSWORD FATIGUE

> Having to create a new username and password discourages 58% of consumers from signing up for a new account.

Users are simply fed up with creating a new username and password for every account they own. A Janrain survey found that passwords discourage 58% of consumers from signing up for a new account. Dashlane, a leading password manager, reports that the average user manages 90 unique online accounts at any given time. Users have more passwords than they can handle, and the prospect of creating a new password only to forget and reset it later is enough to dissuade users from creating an account at all.

Password fatigue also pushes users towards password habits that leave their accounts vulnerable to phishing and data breaches. A Pew Research cybersecurity study found that 65% of adult Americans use memory alone to keep track of passwords, and 39% use the same password across multiple accounts. When users have too many passwords to remember, they fall into a pattern of reusing the same easily-guessed credentials. Once a user's password is phished or exposed in a data breach, all accounts using those common passwords become vulnerable to takeover. According to Pew, many users are aware that reusing passwords is dangerous, but they do it anyway because remembering a complex password is too difficult.

Federated identity systems ease the mental burden of remembering multiple complex passwords by linking a user's digital identity to multiple accounts using a single secure credential. After a user has already created an account with a federated login once, they can use it to instantly create or access an account at another participating website, eliminating the need to remember a new password.

REGISTRATION ABANDONMENT

Passwords aren't the only pain point users face when creating new accounts. Registration can be a frustrating process when organizations require multiple fields, including name, address, date of birth, phone number, and social security number. Four in five users are bothered by traditional account registration, and 54% would rather leave a site than create a new account, says Blue Research.

> 88% of users report inputting false or incomplete information when registering for a new account in order to cut time.

Moreover, 88% of users report inputting false or incomplete information when registering for a new account in order to cut time. The bottom line: when users sign up for a site to achieve a specific goal, they'll sacrifice accuracy and security to get the service they want faster.

Federated identity allows users to bypass account registration altogether by tying their attributes to a credential they already have. The convenience of clicking a single button to establish a new account can mean the difference between acquiring or losing a new user.

A preference for using federated identity to create new accounts already exists. In 2016, 88% of all online accounts were created using federated identities, according to LoginRadius. Janrain also found in 2016 that 95% of users are aware of federated logins such as Google and PayPal, and 58% realize the value and convenience of using them.

> 58% **of consumers realize the value and convenience of using federated identities.**

Challenges with Social Media Driven Federated Identity

While federated identities are a popular mode of login on low-risk sites, their security functionalities are not always sufficient to access high-risk sites, such as bank accounts or government agencies. Because there aren't any widely adopted federated identity solutions for high-value services, organizations often enforce their own strict login procedures in order to protect user data during transactions – a solution that addresses short-term needs at the expense of creating a fragmented login ecosystem and a frustrating user experience over the long-term.

Federated identity need not imply a loss of security or privacy. It is possible to simultaneously offer users the easy experience of federated identity while safeguarding their personal data.

How ID.me Does Federated Identity Differently

ID.me binds a legal identity to a shared login in a manner that meets the federal government's most rigorous requirements for remote identity proofing and authentication. For example, Vets.gov users have the choice to use a federated login to initiate account creation. This allows users to avoid creating a whole new password and minimizes the fields of data that user needs to provide in the identity proofing flow. Once registration is complete, ID.me identity proofs the user and secures their account with possession-based authenticators such as a FIDO-certified security key. Users can then use their identity-proofed Vets.gov login to access other partners that accept ID.me credentials, e.g., other government websites, financial institutions, healthcare providers.

Over 50% of new Vets.gov users sign up using a federated identity options like DS Logon, Facebook, PayPal, etc.

Over 50% of new Vets.gov users sign up using a federated identity options like DS Logon, Facebook, PayPal, etc. ID.me's technology allows users with legacy DS Logon and MyHealtheVet logins to access Vets.gov services without creating yet another login, while strengthening the credential they already use. It also allows users who don't have those legacy logins, such as older military veterans, to access Vets.gov using a social login with which they are already familiar.

ID.me offers a risk-based authentication model that gives users the flexibility to secure their federated identities only as far as the transaction requires. Users trying to access publicly available information, like an article about GI Bill benefits, can access that resource with an email and password. Only when a user takes an action that requires identity proofing, like talking to their doctor via chat about a medical issue, do they have to verify their identity.

Once a veteran has established a federated identity with ID.me on Vets.gov, they can use the same credentials on other high-security platforms that utilize ID.me. To prove their identity to a second federal agency, the process is simple: login, authenticate with 2FA, and consent to the personal information shared with that platform. The entire process takes three clicks.

ID.me's credentials are currently accepted by three different federal agencies and over 200+ other relying parties in the public sector, healthcare, financial services, and e-commerce.

ID.me

Trusted Online Identity Verification

ID.me provides fast, secure and compliant identity verification using a federated approach to credentialing. It is already trusted by federal agencies and corporations to securely manage millions of individual identities. For more information, visit **business.ID.me**.

CONTACT INFO:
Sales@ID.me