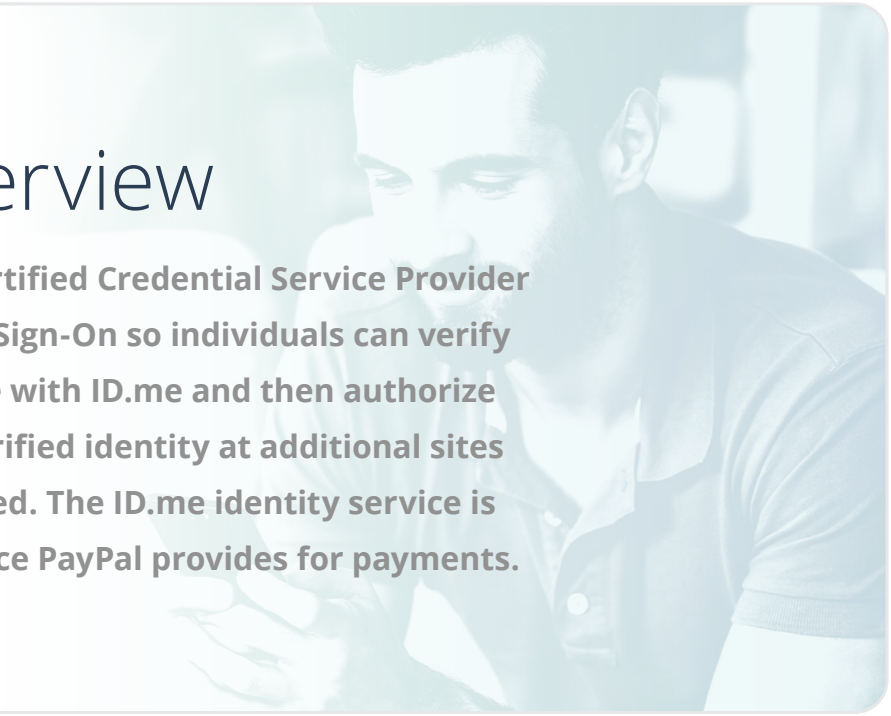
Legal and Privacy Policies

ID.me



ID.me Overview

ID.me is a federally certified Credential Service Provider that provides a Single Sign-On so individuals can verify their identity one time with ID.me and then authorize the release of their verified identity at additional sites where ID.me is accepted. The ID.me identity service is analogous to the service PayPal provides for payments.

THE NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE

The National Institute of Standards and Technology (NIST) has awarded ID.me more than five million dollars in grant funding since 2013 due to ID.me's unique potential to increase trust and user control over data in the market by providing a secure and interoperable digital identity. NIST runs the program office for the National Strategy for Trusted Identities in Cyberspace (NSTIC), an initiative that promotes the adoption of secure and interoperable digital credentials in the market.

ID.me adheres to NSTIC's guiding principles to issue digital credentials that are:

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-effective and Easy to Use

STANDARDIZED

Today, ID.me is the only Credential Service Provider in the United States certified against the most rigorous technical and policy controls established by the federal government for citizen authentication, NIST 800-63-2 Level of Assurance 3 and NIST 800-63-3 Identity Assurance Level 2 and Authenticator Assurance Level 2. ID.me is the first identity provider in the United States of America to issue a federally-certified digital identity that is interoperable across the federal, state, and local levels of government as well as in other sectors of the economy, including healthcare and life sciences. Notable customers include the Department of Veterans Affairs, Treasury, Allscripts, Fidelity, MGM, and Apple.

ID.me provides the highest access rates, offering multiple options for identity verification as part of our "No Identity Left Behind" commitment:

Unsupervised remote: Automated verification via a personal computer or mobile device that includes physical IDs, mobile network operator (MNO) data, and fraud and compliance checks. Typically completed in under five minutes.

Supervised remote: Identity evidence is presented and an individual joins a video chat with an authorized "Trusted Referee" to assist the validation process.

In-person verification: Beginning June 2021, individuals can verify their identity at one of over 500 retail locations. This method provides an option for those without internet or with device issues to complete their identity proofing.

WHAT COMPLIANCE STANDARDS DOES ID.ME MEET?

ID.me's Identity Gateway has achieved The Federal Risk and Authorization Management Program (FedRAMP) Moderate Authorization which required assessment by an accredited third-party assessment organization (3PAO) and additional reviews and approvals by the FedRAMP Program Management Office (PMO). The platform also holds certification for NIST 800-63 through the Kantara Initiative Trust Framework which independently assesses providers for digital identity operations. As an enterprise, ID.me has been designed and operates in alignment with NIST CyberSecurity Framework (CSF), NIST 800-53, and NIST 800-63 standards and controls. ID.me has also achieved AICPA SOC2 Type 1 attestation. By meeting and maintaining these standards, ID.me prioritizes the security and privacy of user information.

DOES ID.ME STORE PERSONALLY IDENTIFIABLE INFORMATION (PII)?

ID.me Branded Solutions: Yes, we store PII in our ID.me branded implementations (non-white label). As a federally-certified identity provider, ID.me is required to store individuals' attributes in order to make the digital identity interoperable at a high level of assurance such as LOA3 and IAL2. These attributes are encrypted in transit and at rest using FIPS 140-2 validated cryptography that has been independently reviewed and approved as part of our FedRAMP authorization. ID.me adheres to NARA's minimum records retention requirement of seven years and may alter those requirements based on changes to any superseding law, regulation, or policy that requires a different record retention period for audit purposes.

Private/White Label Solutions: No, we do not store PII for white label identity proofing that is custom to the brand of our partner's existing login if the end user chooses to log in with an option other than ID.me.

While ID.me powers the identity proofing and MFA for all login options where it is integrated, ID.me does not persist any PII after a white label proofing session because the user did not choose ID.me as their preferred login option. The white label solution does use the same encryption mechanisms as the branded implementation while the date is transiting the system.

DO SITES THAT USE ID.ME SEND ANY USER DATA TO ID.ME?

No. ID.me is an independent Credential Service Provider. Sites that use ID.me may refer a user to ID.me to get credentialed but those sites do not pass any user data to ID.me. Once the user is appropriately credentialed, then ID.me releases the user's verified identity back to the referring site only after the user has given explicit consent. The user experience is similar to PayPal but for identity.

DOES ID.ME SELL OR SHARE INFORMATION WITH THIRD PARTIES?

ID.me never sells or releases user information to a third party without the explicit consent of the end user on a case-by-case basis. Our stance is that the user, and the user alone, is in control of their data and whether they wish to share it with an organization in a given context. Similar to Visa's role in payments, the credential holder decides if they wish to share data with a given organization. ID.me's role is to move that data at the request of the end user and to make sure that the receiving organization can trust the assertion that the user is making about their identity. ID.me's business model is built upon monetizing trust and convenience while the user is in full control over how or if their information is shared.

HOW DOES ID.ME GATHER CONSENT?

When an organization requests data from a user for the first time, ID.me appropriately authenticates the user based upon the sensitivity of the data the organization is requesting. After the user is authenticated, ID.me presents a consent screen that lists each data element

the organization is requesting from them. The user must provide explicit consent in order for ID.me to release their information.

HOW DOES ID.ME APPLY PRIVACY FILTERS TO TRANSACTIONS?

ID.me audits each application and the context of the transaction so that the application is only requesting data elements that are reasonably associated with the transaction. By applying privacy filters, ID.me can dynamically adjust the consent screen and data payloads so that the user is never asked to share more information than is necessary to complete a transaction. For example, if a website needed to verify that an individual was over the age of 21, then ID.me would only allow the app to ask the user to assert they are over 21 rather than for their date of birth.

HOW DOES ID.ME ALIGN WITH CCPA, GDPR AND EMERGING PRIVACY REGULATIONS?

ID.me has been architected from inception in order to provide users with complete control over their information. ID.me only shares data with third parties upon receipt of the user's explicit consent after the user has been authenticated at the appropriate level of assurance and after the user has reviewed the specific data elements the application is requesting. Additionally, ID.me minimizes the data elements that an application may request based on the context of the transaction.

Users may access an ID.me account management page at any time to review the applications that have access to their information and which data elements they authorized for release. Users may revoke application access to their data via the account management page. Users may also delete their ID.me account and associated data at any time.

Users are "opted out" from any type of data sharing by default without exception. ID.me's architecture and complete deference to user control are compatible with GDPR, CCPA and all similar emerging privacy regimes that empower users to control their data.

DOES HIPAA OR A BAA APPLY TO ID.ME?

Because ID.me does not receive data from our partners, we do not believe that HIPAA or BAA requirements apply. We are willing to sign a BAA as long as the individual's right to control their own data via the ID.me credential is clearly preserved. For example, if someone were to use their PayPal account to buy something from a merchant, the merchant shouldn't therefore be able to take control of that person's PayPal account and the associated data. We have language we have used with other healthcare partners to execute a BAA while enabling people to maintain control of their own data through ID.me.

ID.me has been architected from inception in order to provide users with **complete control over their information.**