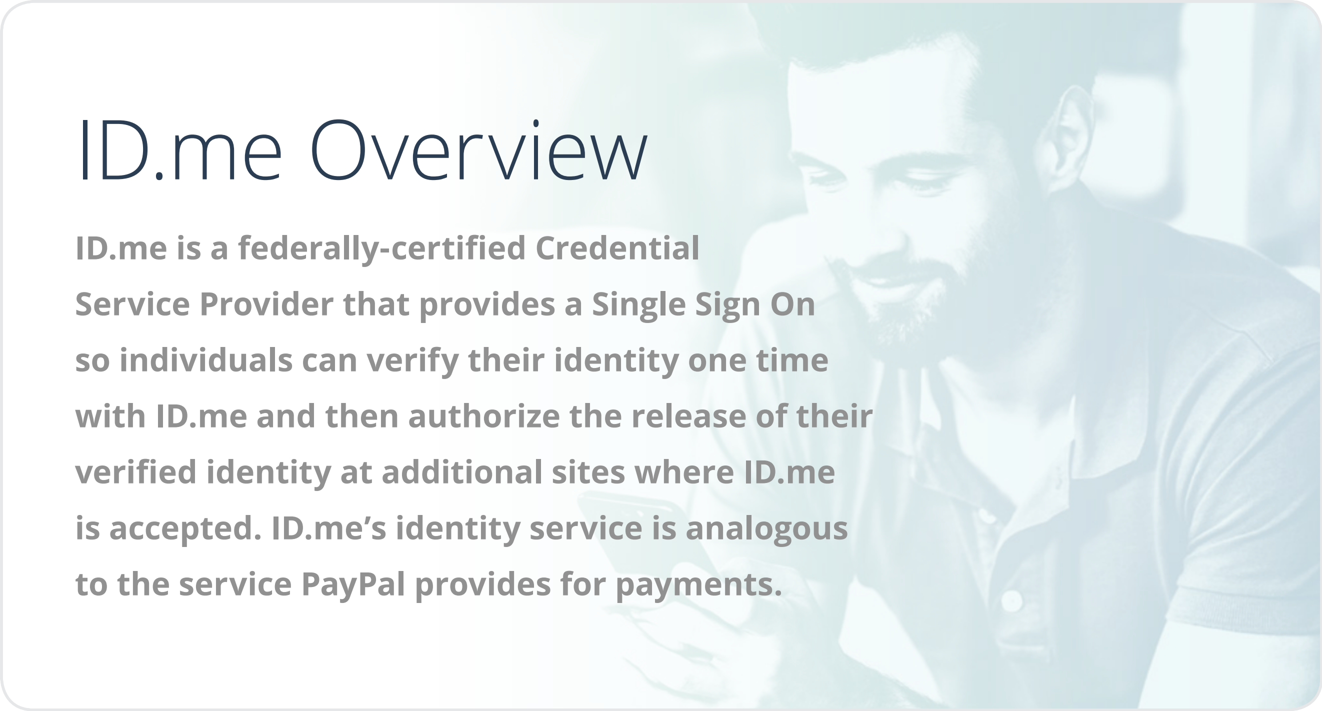
ID.me

LEGAL AND PRIVACY POLICIES



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. ID.me's 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 2012 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 Veterans Affairs, Treasury, Allscripts, Practice Fusion, and Apple.

HOW DID ID.ME OBTAIN FEDERAL CERTIFICATION?

ID.me is certified against NIST 800-63 through the General Services Administration's Federal Identity and Credential Access Management (FICAM) Trust Framework Services (TFS) program. The Kantara Initiative, a GSA FICAM approved auditing body, performed the audit and review of ID.me's compliance against NIST 800-63.

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 after the user has given consent. The user experience is similar to PayPal but for identity.

DOES FEDRAMP APPLY TO ID.ME?

FedRAMP is a program designed to impose appropriate controls over sites that store government data. Because ID.me does not receive any data from partner applications, including government agencies, FedRAMP does not technically apply. At the same time, ID.me follows NIST 800-53 and applies the technical and policy controls required to achieve FedRAMP Moderate status. In 2020, at the request of a federal agency, ID.me decided to pursue a full FedRAMP Moderate Authority to Operate (ATO). ID.me has already *achieved FedRAMP's In-Process designation* on the marketplace and expects to complete the process and achieve full authorization before the end of 2020.

DOES ID.ME STORE PII?

Yes. As a federally-certified identity provider, ID.me is required to store the individual's attributes in order to make the digital identity interoperable at a high level of assurance such as LOA 3 and IAL 2. ID.me adheres to NARA's minimum records retention requirement of seven years and sometimes increases those requirements if state law, regulation, or agency policy requires a longer record retention period for audit purposes.

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 and 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 ensures the user is appropriately authenticated 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 to ensure 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 to ensure 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 GDPR AND EMERGING PRIVACY REGIMES?

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 is compatible with GDPR and all similar emerging privacy regimes that empower users to control their data.

DOES HIPAA OR A BAA APPLY TO ID.ME?

No, not today. ID.me authenticates the user is who they claim to be, but ID.me does not handle, process, or store PHI. Additionally, ID.me does not receive any data, PHI or otherwise, from associated healthcare applications that use ID.me for authentication.
As a result, a BAA, which covers vendors that might have access to PHI, is not a relevant document because ID.me does not receive or access data from partner applications.

DOES ID.ME HAVE A SOC 2 CERTIFICATION?

Yes, a copy of ID.me's annual SOC 2 Type 1 Report is available to customers upon request. Additionally, ID.me is a *federally certified identity provider* audited against all of the relevant technical and policy controls required by NIST 800-63-3 Identity Assurance Level 2 and Authenticator Assurance Level 2 and NIST 800-63-2 Level of Assurance 3. From a security perspective, ID.me operates in compliance with NIST 800-53 FedRAMP Moderate.

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