ID.me

HEALTHCARE

Welcome Kit FAQ's

GENERAL — END USER — TECHNICAL

ABOUT ID.ME

Who is ID.me?

ID.me is a federally-certified credential service provider (CSP). Our mission is to democratize the identity verification process while upholding the utmost level of security. We're able to verify any legitimate user, including all those demographics left behind by traditional CSPs.

The ID.me solution allows users to verify their identity online in order to access their benefits and services. Users can complete the process remotely, by themselves. In addition, ID.me is the only CSP to offer remote video call-based verification – supervised by a US-based employee trained and certified to verify identity – for users who are unable to complete the self-service verification process.

ID.me is one of only four identity providers that meet the U.S. government's most rigorous requirements for online identity proofing. ID.me provides the strongest identity verification system available to prevent fraud and identity theft. We use bank-grade encryption to keep personal information safe and we give the user control over which services and businesses can see and share their information.

ID.me is a trusted partner of government agencies, healthcare platforms, financial institutions, and other businesses to verify and authenticate their users.

CERTIFICATIONS

NIST
ID.me is the only CSP in the United States certified to NIST 800-63-3 IAL2/AAL2, as well as its predecessor NIST 800-63-2 LOA3. The certification assessment was supervised by the Kantara Initiative, a GSA Trust Framework solution provider.

FedRAMP
ID.me currently holds a FedRAMP In Process designation

SOC
ID.me has a SOC 2 Type 1 certification

Where can I get the ID.me logo, ID.me button, or direction on ID.me branding?

See our brand asset resources.

View Brand Assets →

ONBOARDING

How much time does an integration take from start to go live/product launch?

The time it takes from the start of integration to go live for a high-assurance identity proofing workflow depends on the partner's timeline and need, but typically ranges between 4-6 weeks. These are the milestones we need to hit before go live:

1. **Technical integration**
2. **Development of onboarding/implementation resources for education of internal teams, external stakeholders, and end users**
3. **Development of the communication strategy for notification of internal teams, external stakeholders, and end users**
4. **Establishment of the partner-to-ID.me customer support process**
5. **Review of the workflow in staging with a QA screenshare (~2 weeks before go live date)**
6. **Review of the workflow in production with a pilot test using real end users (~1 week before go live date)**
7. **Team trainings of partner implementation and customer support teams**

What happens to end users who encounter problems with the self-service workflow?

ID.me averages a 90% success rate for end users in our self-service, do-it-yourself workflow for LOA3 and IAL2 identity proofing. Although this average is well above the industry standard, we believe in No Identity Left Behind and, thus, we developed Virtual In-Person Proofing (supervised remote proofing) where end users may complete their identity verification on a video call.

We anticipate based on previous integrations that about 3-5% of end users will need to transition to our video call identity proofing solution. Additionally, we anticipate an approximate 3-5% of end users will need support from the partner or ID.me support team during initial registration or enrollment with ID.me. We will finalize the partner-to-ID.me customer support process during onboarding. **Ultimately, ID.me verifies over 99% of legitimate end users.**

Why is a QA screenshare important?

The QA screenshare is a quality assurance (QA) check of our integrated software solution completed in the staging environment prior to moving to production. It offers a 'first look' for decision-makers from all contributing teams to review the newly coordinated workflow and serves as a functionality check of all back-end redirects between the partner and ID.me. During the QA screenshare, technical functionality issues as well as non-technical inputs, suggestions, or modifications should be addressed.

Attendees to the QA screenshare should include a decision-maker from each contributing party. We recommend a lead contributing engineer as well as a minimum of one business-side point of contact, like a project manager or customer success manager. When all parties agree that the QA screenshare is a success, we will coordinate the move to production.

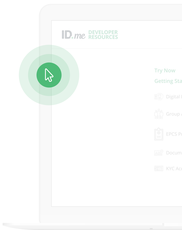
Why is pilot testing important?

During the pilot test (or beta test), real end users run through the coordinated ID.me + partner solution in production. This initial test offers:

1. **The first look at the real-time calls to authoritative databases**
2. **A functionality check in production before the fully integrated solution is advertised to end users**
3. **A chance to observe any friction points that have previously gone unnoticed**

The pilot test is conducted by having an end user join a video conference call, share their screen, and showcase the clickthrough workflow as they attempt to complete the coordinated solution.

Attendees to the pilot test should include a decision-maker from each contributing party. We recommend a lead contributing engineer as well as a minimum of one business-side point of contact, like a project manager or customer success manager.



WORKFLOW

What are the five main steps of the LOA3 and IAL2 flow?

1. **Create an account**
2. **Secure account with multi-factor authentication (MFA)**
3. **Verify identity**
4. **Submit NPI and/or DEA numbers (as required)**
5. **Consent to send data to partner**

What are the main differences between the LOA3 and IAL2 flow?

There are two key differences between proofing at LOA3 and IAL2:

1. **LOA3 identity proofing allows for the end user to verify their identity by answering knowledge-based questions (KBA) about their credit history**
2. **LOA3 identity proofing does not require a selfie for biometric matching to the user's ID**

IAL2 does not allow for KBA and does require a selfie. The exclusion of KBA and requirement for a selfie introduces more friction in the IAL2 flow. However, IAL2 is more secure because of these requirements. KBA is known to be an easily spoofable option because of the availability of personal information on the dark web.

ID.me's policies are modular and configurable. Our team will work with you to ensure the policy settings are appropriate for your risk level. For example, if you choose to utilize our LOA3 policy, ID.me can still remove the KBA option from the identity verification choices presented to the end user.

VERIFICATION

Do end users ever have to re-verify their identity with ID.me?

ID.me believes that you should never ask people to do the same thing twice. End users only verify their identity once with ID.me and should never have to re-verify their identity as long as their account remains active. If an LOA3 or IAL2 account shows no activity for 18 months, their account is deemed "inactive" and the end user must re-verify for security purposes.

If an end user already has an ID.me account they used with another EPCS software, will they have to complete the identity proofing process for a second time with ID.me?

If an end user already has an ID.me account verified to LOA3 or IAL2, they will not have to re-verify. Their ID.me verified identity is portable, meaning they can bring it with them wherever they go. In this case, the end user can bypass the "Create An ID.me Account" screen and simply "Sign-In" with their pre-existing ID.me username and password.

VIDEO CALL

Why do some end users have to "Verify on a Video Call"?

If your end users run into trouble verifying their identity using the do-it-yourself process for any reason, they will see a "Verify on a Video Call" button. They'll need to click the button to complete verification. Once they do, they'll be routed to meet with one of ID.me's Trusted Referees, a Virginia-based employee trained and certified to verify identity on a video call.

There are a variety of reasons why an end user might be asked to verify their identity on a video call, including inaccurate data stored by credit bureaus, lack of credit history, phone not being associated with their name, or even unclear document photos.

Video call-based identity proofing allows for "No Identity Left Behind," so that all demographics can verify their identities, despite those limitations.

Based on previous data, we estimate about 3-5% of the total end-user base may need additional help via our video-call process.

AUTHENTICATION

Does ID.me send hardware tokens or security keys, like FIDO U2F, to end users?

ID.me does not issue hardware tokens or security keys. End users should consult with their healthcare institution, EHR, or e-prescribing solution for further direction on security keys.

What app do end users use for authentication with ID.me?

End users will utilize the ID.me Authenticator app for multi-factor authentication with ID.me. With the Authenticator app, they will:

1. **Secure their account upon creation**
2. **Authenticate each additional session, ensuring that they are the same person who previously verified their identity on that account**

The end user is prompted to download this app during the ID.me enrollment process. The ID.me Authenticator app is DEA-compliant with a FIPS 140-2 encryption level. The ID.me Authenticator app may be configured to deliver push notifications or configured as a code generator.

SECURITY

Why does ID.me require SSN?

ID.me verifies the identities of millions of people across the world. Our primary goal is to make sure that someone is who they say they are before granting access to exclusive benefits or permissions at one of our partners. Sometimes our verification process requires collecting sensitive pieces of information, like social security number (SSN) or a photo of government ID.

When someone is requesting high-value access, like to personal information or for restricted permissions, the verification process requires more stringent methods due to the increased risk of fraud. The SSN enables financial records lookup and utility records lookup in order to corroborate a unique person's name, date of birth, and address.

Collecting the SSN also helps us make sure that an account can never be duplicated – whether accidentally by a legitimate individual or in a malicious attempt by someone pretending to be that person. This information is strictly used for verification and fraud prevention purposes. All information provided is secured and encrypted.

ID.me will never sell personal information, share it without consent, or use it for marketing or re-targeting purposes.

Is the ID.me Virtual In-Person Proofing video call recorded?

Yes, ID.me records the calls for end-user security. ID.me has numerous measures in place to secure the video call. The video recording and all data is securely encrypted and kept confidential, following our strict data privacy policies.

View Privacy Policies →

INTEGRATION

How does the partner move from the lower testing/ staging environment to production?

After all involved parties agree that the QA screenshare was successful, our integration engineer will coordinate the move to production and give your team the production keys. From there, we can schedule pilot testing with at least one real-end user. Once all parties agree that the pilot test is successful, we will go live.

Where can I find resources on technical integration?

For technical integration questions, visit our developer website. For additional questions, contact us via the developer site to reach our engineers or utilize your existing ID.me point of contact.

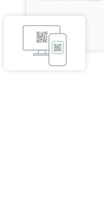
View Developer Website →

Can you provide more information about the ID.me audit trail for DEA compliance and related audits?

ID.me has an audit trail that you can leverage. You'll receive the PII and metadata on a transactional basis when we verify an end user's identity and subsequently authenticate the end user, but you can also point your DEA auditors to us if they have any questions. We've helped many EHR/EMR/e-prescribing software partners sail through their audits.

Should the partner maintain their own audit trail?

Yes, partners should maintain the audit trail on their side using ID.me's unique identifier. You'll need to maintain an audit trail both for when an end user completes identity proofing and for each time they prescribe. ID.me's integration engineers will provide more detailed information.



With regard to ID.me's Authenticator app, How often does ID.me experience downtime and how long does it last?

ID.me has averaged 99.99% availability over the last three years. ID.me commits to 99.99% uptime for our partners. Currently, our platform processes 220M-250M requests per month with an average response time of 90-110ms. ID.me does not have pre-scheduled downtime or outage periods. You can subscribe to realtime system updates by going to **status.id.me**.

CONFIGURABILITY

For EPCS, is there a way to alter ID.me's identity proofing process, for example by removing steps such as the phone check?

The phone check cannot be removed. ID.me's LOA3 and IAL2 workflows are certified to NIST SP 800-63-2 and 3, and the phone check is part of the certified process.

If, for any reason, end users have trouble verifying their identity, they will see the "Verify on a Video Call" button. They should click the button and proceed with a video call to complete their verification (for more information, see "Why do some end users have to Verify on a Video Call?").

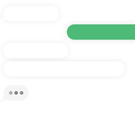
Which multi-factor authentication (MFA) options are available for eRx and EPCS?

eRx AUTHENTICATORS

- **SMS Text/Voice**
- **ID.me Authenticator App (Push Notification or Code Generator)**
- **FIDO U2F Security Keys**
- **Mobile Yubikey**

EPCS AUTHENTICATORS (FIPS 140-2 OPTIONS ONLY)

- **ID.me Authenticator App (Push Notification or Code Generator)**
- **FIDO U2F Security Keys**



Are SMS text messages allowed as an MFA option for EPCS?

No, SMS text messages are not allowed for EPCS. Authenticators using SMS and phone call verification currently fall under RESTRICTED as outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B, "Authentication and Lifecycle Management," sections 5.1.3.3 and 5.2.10.

If a partner has an LOA3 policy, why are end users being returned as IAL2? What qualifies an end user as being returned as IAL2 vs. LOA3 identity proofed?

For an LOA3 policy, users who successfully complete the do-it-yourself ID.me workflow will return as LOA3. The users who return as IAL2 have been routed to our Virtual In-Person Proofing workflow (i.e., completing identity proofing on a video call with a Trusted Referee). Virtual In-Person Proofing meets NIST's requirements for supervised remote identity proofing, which is defined under IAL2. Thus, anyone who completes the Virtual In-Person Proofing workflow will be returned as IAL2.

IAL2 supervised remote proofing requires additional documentation to be uploaded. A user needs either two primary documents or one primary and two secondary documents, as well as a selfie, before the user is able to join the video call.