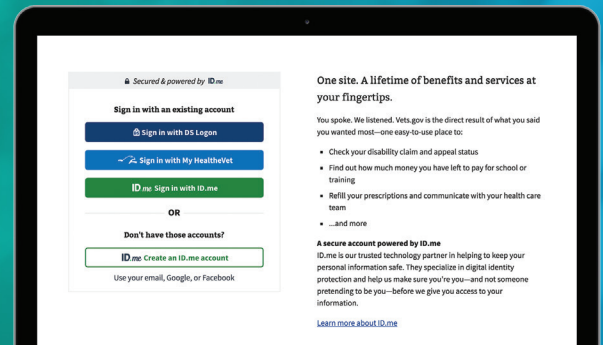




Enabling Secure Access for Veterans at Vets.gov

At the beginning of 2016, Veteran online benefits and services, such as refilling prescriptions or tracking disability claims, were embedded across 500 different Veteran-facing websites.



To streamline services and deliver a more cohesive user experience, the Department of Veteran Affairs (VA) launched Vets.gov, a secure digital portal that gives Veterans direct access to their benefits and resources online.

VA's objective was to improve the Veteran digital experience and better enable Veterans to discover and claim the benefits they earned through their service to our country. Vets.gov would become the Veteran community's digital front door to access all VA information, benefits, and services.

The Vets.gov team needed to protect the platform with robust identity verification. The team had two objectives:

1. Deploy a Secure NIST-compliant Login

To protect Veterans from fraud, Vets.gov had to meet the National Institute of Standards and Technology's (NIST) Digital Identity Guidelines (at the time, NIST 800-63-2 LOA3 and soon, NIST 800-63-3 IAL/AAL2). This meant that rather than relying on the security of a username or password alone, VA needed to incorporate robust identity proofing and two-factor authentication into its login process.

2. Strengthen Legacy Logins

Millions of Veterans already used DS Logon and MyHealthVet to login to VA websites. However, neither of those logins met NIST's LOA3 standards. Vets.gov needed to provide a transitional path to upgrade existing logins to meet NIST standards so these Veterans could still access the site.

Solution

The Vets.gov team contracted ID.me and Ad Hoc LLC to deliver an authentication process that was compliant with the federal government's most rigorous security standards, and provided a way for Veterans with existing login credentials (DS Logon and MyHealthVet to continue to use them while making them more secure).

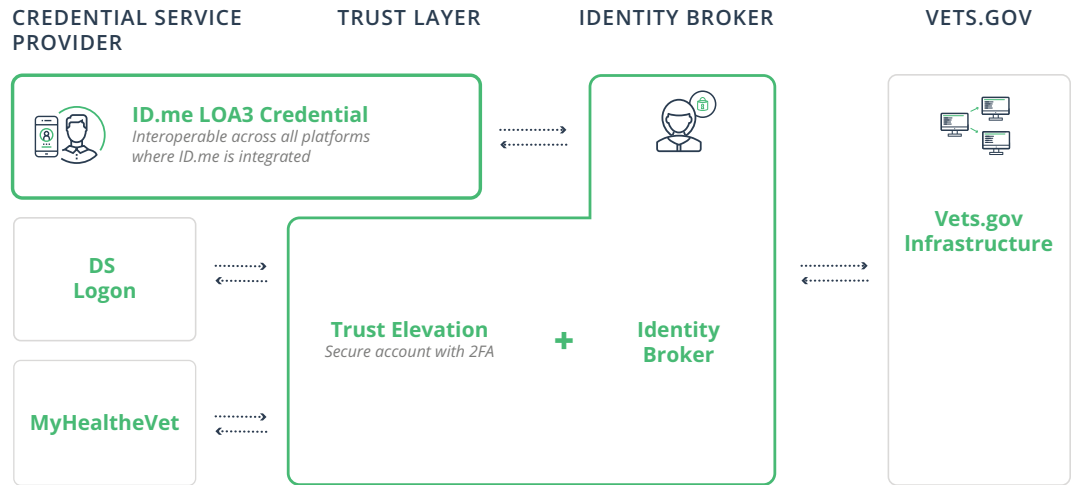
Vets.gov integrated ID.me's identity broker, LOA3 credentials and trust elevation solution.

ID.me Identity Broker and Trust Elevation

The ID.me identity broker provides a single point of integration to consume multiple credential service providers, in this case, ID.me, MyHealthVet, and DS Logon. The trust elevation solution allows users to make their MyHealthVet and DS Logon credentials more secure by binding a second authentication factor such as SMS or biometrics. This solution enables the VA to onboard veterans to Vets.gov with minimal disruptions by allowing them to use their existing DS Logon and MyHealthVet logins.

Figure 1:

ID.me's Role in Identity Verification and Authentication on Vets.gov



ID.me LOA3 Credential

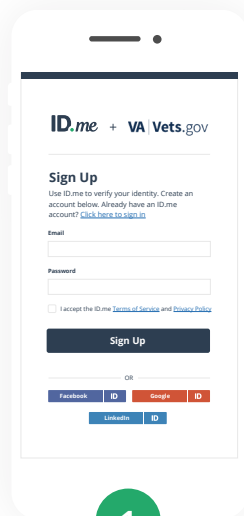
ID.me's LOA3 credential provides an end-to-end hosted NIST-compliant 800-63-2 identity verification flow (strictest federal standard for online identity proofing at the time of launch). The ID.me's platform is forward-aligned with the upcoming NIST 800-63-3, allowing Vets.gov to stay up-to-date with federal standards without an interruption of service.

Veterans verifying their identities on Vets.gov for the first time have a choice to upload a picture of their driver's license or passport. ID.me uses sophisticated machine vision and AI to verify the document's authenticity. In the background, ID.me verifies that the SIM in the mobile device used for the verification is associated with the applicant's identity and screen for potential indicators of fraud. To prevent future account takeover, Veterans secure their account with 2-factor authentication via a code sent by text message, a call to a landline, an app-based push notification, or a FIDO U2F security key.

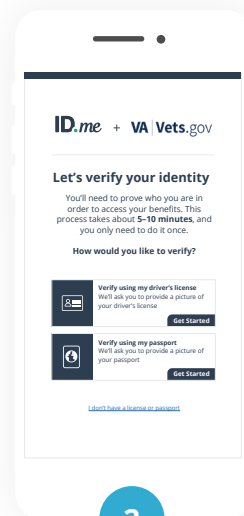
Figure 2:

ID.me LOA3 Verification Process on Vets.gov

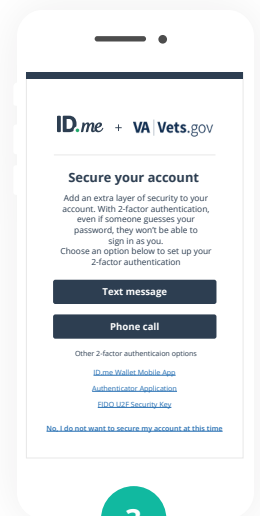
ID.me's NIST 800-63-2 LOA3 identity verification flow has the highest success rate in the industry.



User creates an account



User verifies their identity using online ID document verification



User secures their account with 2-factor authentication