How Identity Proofing Works with login.gov

What we need to verify a user's identity

1 piece of strong evidence and 2 pieces of fair evidence

1. Strong evidence is evidence with a photo or biometric that uniquely identifies the person.
    a. Login.gov accepts a state-issued ID or government employee ID (PIV/CAC).
2. Evidence with a reference number that uniquely identifies the person, or is based on knowledge of that person's private information. Login.gov accepts:
    a. Financial records tied to their Social Security Number (SSN), and
    b. Full name and phone number or full name and mailing address

Identity proofing with a state-issued ID

1. The user begins IAL2 identity proofing.
2. The user uploads their state-issued ID. They can use their phone or computer to upload images of the front and back of their state-issued ID. (Strong Evidence)
3. The user takes a selfie. They can use a phone or computer to take a current photo of themselves.
4. login.gov checks the authenticity of the ID for security features and alterations to the image, and confirms that the image on the ID matches the selfie. We perform a facial match and liveness check on the selfie. This ensures the applicant is the same person as the owner of the identification being presented. The images are discarded after checking the authenticity of the ID and selfie. If the image uploads fail 4 times, they must wait 24 hours to try again.
5. The user enters their SSN. (Fair Evidence)

6. The user verifies that their name, date of birth (DOB), address, and SSN are correct. We obtain their name, DOB, and address from their ID. They can only edit their address and SSN.

7. login.gov validates the name, DOB, and SSN against issuing or authoritative sources, and verifies that they belong to a single person. If the check fails 3 times, they must wait 24 hours to try again.

8. login.gov confirms that the user's SSN and state-issued ID are verified.

9. Does the user have a valid phone number tied to their name, address, and SSN? The phone number must be a U.S. number.

    a. If the user has a valid phone number,

        i. The user enters their phone number for verification. (Fair Evidence)

        ii. login.gov verifies that the name and address on the user's phone and ID match. We check phone records to match the user's name, address and SSN. If the check fails 3 times, they must wait 24 hours to try again.

        iii. The user enters a one-time security code to prove they have possession of the phone.

        iv. The user re-enters their password to protect their data.

        v. login.gov provides the user with a personal key to use if they forget their password. The user must enter their personal key to confirm that they saved the key.

        vi. IAL2 identity proofing is complete. login.gov encrypts the user's PII. Only the user can decrypt and access it. The user provides explicit consent to allow us to share any data with a service provider.

    b. If the user does not have a valid phone number,

        i. The user confirms that they want to receive a letter to their address on file. We obtain their address from their ID.

        ii. The user re-enters their password to protect their data.

iii. login.gov provides the user with a personal key to use if they forget their password. The user must enter their personal key to confirm that they saved the key.

iv. login.gov sends the user a letter with a unique code and instructions by mail. This code is valid for 30 days.

v. The user signs in to login.gov and enters the code they received by mail. (Fair Evidence)

vi. IAL2 identity proofing is complete. login.gov encrypts the user's PII. Only the user can decrypt and access it. The user provides explicit consent to allow us to share any data with a service provider.

Identity proofing with a government employee ID

1. The user begins IAL2 identity proofing.
2. The user connects their government employee ID. They connect their card, select their certificate, and enter their PIN. (Strong Evidence)
3. login.gov checks the authenticity of the ID. We verify that the certificate they use was issued by a federal entity. If the check fails 4 times, they must wait 24 hours to try again.
4. The user enters their name, date of birth (DOB), address, and SSN.
5. The user verifies that the information they entered is correct.
6. login.gov validates the name, DOB, and SSN against issuing or authoritative sources, and verifies that they belong to a single person. We also check that the first and last name match the PIV/CAC. If the check fails 3 times, they must wait 24 hours to try again.
7. login.gov confirms that the user's SSN and state-issued ID are verified.
8. Does the user have a valid phone number tied to their name, address, and SSN? The phone number must be a U.S. number.
    a. If the user has a valid phone number,
        i. The user enters their phone number for verification. (Fair Evidence)

ii. login.gov verifies that the name and address on the user's phone and ID match. We check phone records to match the user's name, address and SSN. If the check fails 3 times, they must wait 24 hours to try again.

iii. The user enters a one-time security code to prove they have possession of the phone.

iv. The user re-enters their password to protect their data.

v. login.gov provides the user with a personal key to use if they forget their password. The user must enter their personal key to confirm that they saved the key.

vi. IAL2 identity proofing is complete. login.gov encrypts the user's PII. Only the user can decrypt and access it. The user provides explicit consent to allow us to share any data with a service provider.

b. If the user does not have a valid phone number,

i. The user confirms that they want to receive a letter to their address on file. We obtain their address from their ID.

ii. The user re-enters their password to protect their data.

iii. login.gov provides the user with a personal key to use if they forget their password. The user must enter their personal key to confirm that they saved the key.

iv. login.gov sends the user a letter with a unique code and instructions by mail. This code is valid for 30 days.

v. The user signs in to login.gov and enters the code they received by mail. (Fair Evidence)

vi. IAL2 identity proofing is complete. login.gov encrypts the user's PII. Only the user can decrypt and access it. The user provides explicit consent to allow us to share any data with a service provider.