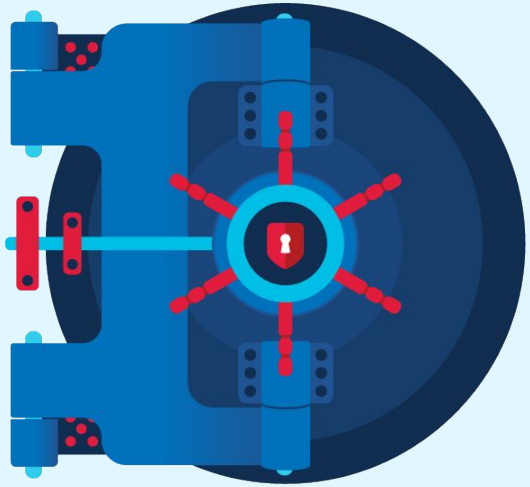
LOGIN.GOV

Privacy and Encryption

February 27, 2017



Security and privacy by design

How login.gov keeps personal information private

login.gov encrypts the personal information of each user separately, using a unique value generated from each user's password. Our encryption method works like a safe deposit box in a bank vault. Only the user has the key. Only the user can open the box to reveal the contents. Only the user knows the password, and only the user can decrypt their information.

security overview | technical description

Cryptography in a nutshell (hashing)

Hashing

- One-way (fingerprint)
- Fixed length
- Digest
- HMAC (Hashed Message Authentication Code)
- Salt (random string to make hashes with same input, unique)
- Fast for strings: SHA-256
- Slow for passwords: PBKDF2, bcrypt, scrypt

Takeaway: passwords are hashed

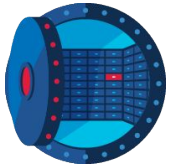
Cryptography in a nutshell (encryption)

Encryption

- Two-way (jigsaw puzzle)
- Variable length
- Symmetric (secret key) e.g. Advanced Encryption Standard (AES)
- Asymmetric (public key) e.g. HTTPS, SSH, PGP, RSA, PKCS

Takeaway: PII is encrypted

Privacy and security throughout the system



The vault

It's hard to break into the "vault," otherwise known as our database. login.gov implements the latest National Institute of Standards and Technology (NIST) standards for secure authentication and verification. Our plans for ongoing security include regular penetration testing and external security reviews.

The safe deposit box

Individual accounts get two layers of security. We require two-factor authentication as well as strong passwords that meet new NIST requirements.

We evaluate and implement new authentication methods as they become widely available to make sure that login.gov remains accessible and secure.

Your personal key

Encrypting personal data separately means that login.gov cannot share any information with other government entities without users' permission. Not even database administrators can decrypt a user's personal information without the user's password.

Technical Requirements of login.gov

Two flavors of PII:

- things LogIn.gov needs to know in order to operate properly (email, phone number for authentication)
- things only user, relying parties need to know (name, DOB, SSN, address)

Technical Requirements of login.gov (cont.)

Encryption uses FIPS-approved technology, multi-factor NIST model:

- User's password
- Server secret key
- Hardware security module (HSM)

Code:
https://github.com/18F/identity-idp/blob/master/spec/services/pii/nist_encryption_spec.rb

Technical Requirements of login.gov (cont.)

Duplicate SSNs not allowed for separate accounts. Enforced via hashed message authentication code (HMAC)

- Identify potential fraud
- Encourage single account per person

Cryptography of login.gov

- Symmetric keys: 256-bit AES (Advanced Encryption Standard)
- Symmetric encryption: AES-256 in GCM (Galois/Counter Mode) with 96-bit nonces
- HMAC with SHA-256 (Secure Hash Algorithm)
- Password hashing with scrypt