cloaked

Cloaked Security White Paper

Version 1.0 - January 23, 2024

Table of Contents

Our Security Principles 03

- Zero-knowledge architecture including end-to-end encryption 04
- Keep it simple for users 05

How We Secure Cloaked Vaults 06

- Each user's data is encrypted in its own, separate vault 07
- Access controls 07
- Cloaked doesn't have access to user vaults, never stores primary passwords 07
- Securing local access 08

Hashing, Encryption, and Key Management 09

- Cryptographic methods for layered security 10
- Key creation 10
- Cloaked separates the data encryption key and the device authentication keys 12
- Secrets used to protect user data 13
- Email/phone/text routing 14

Authentication for Cloaked User Accounts 15

- Primary user passwords 17
- One time passwords 17
- Passwords + key 18
- Two-factor authentication (2FA) options 18
- Device authentication 19

Recovering Your Cloaked Account 20

- What to do if you forget your privacy user password 21
- Recovering your account using your encrypted recovery key 21

Cloaked Single Sign-On (SSO) 23

- Using Cloaked's SSO service 24
- Trusted devices 24

Protecting Your Data at Rest: Double Layered Encryption from Client to Cloud 25

- First-layer encryption 26
- Second-layer encryption 26
- Trusted Foundations 27

Securing Communications by Encrypting in Transit 28

- HTTPS as a Fortress 29
- OpenSSL as the Gatekeeper 29
- Embracing the Latest in TLS 29

Infrastructure Security 32

- What we store 33
- How it's stored 33

Protecting Against Bad Actors 35

- Our Prohibited Use Policy 36
- Bad actor mitigation 36
- Internal control environment 36

Our Security Principles

Version 1.0 - January 23, 2024

Our Security Principles

Cloaked isn't just a platform, it's a refuge. A place where **comfort** reigns, your **security** is paramount, and your privacy is never a question. We tore down the labyrinthine walls of old-school security and built a world where it's simply there, woven into the fabric of every interaction.

No more toggles, no more menus. Just peace of mind knowing your data is shielded by the strongest protocols, protected by the brightest minds. **With Cloaked, control is yours.** Take back your digital life, one effortless step at a time.

The following principles drive our approach:

Zero-knowledge Architecture: At Cloaked, your privacy is your sovereign territory. We believe you deserve complete control over your data, without any intrusion or surveillance. That's why we built Cloaked on the unshakeable foundation of zero-knowledge architecture with the added principle of removing persistent access to your vaults, data, or communications. This means only you have the keys to your digital vault. Your secrets, known only to you, act as the sole gateway to your encrypted data. We can't see, access, or analyze your information, ever. This not only shields your data from us, but also eliminates Cloaked as a potential target for attackers seeking to exploit our servers. With Cloaked, your privacy is self-governed, your data empowered, and your peace of mind guaranteed.

Keep it Simple: At Cloaked, your privacy is your sovereign territory. We believe you deserve complete control over your data, without any intrusion or surveillance. That's why we built Cloaked on the unshakeable foundation of zero-knowledge architecture with the added principle of removing persistent access to your vaults, data, or communications. This means only you have the keys to your digital vault. Your secrets, known only to you, act as the sole gateway to your encrypted data. We can't see, access, or analyze your information, ever. This not only shields your data from us, but also eliminates Cloaked as a potential target for attackers seeking to exploit our servers. With Cloaked, your privacy is self-governed, your data empowered, and your peace of mind guaranteed.

How we Secure Cloaked Vaults

Version 1.0 - January 23, 2024

How We Secure Cloaked Vaults

Access Controls

User vaults are protected by multiple layers of defense including systems design and technical controls. For example, user vaults are unique and separated by user, and isolated from Cloaked's corporate infrastructure. This protects against the potential threat of cascading access. Additionally, we separate testing, staging, and production data into different engineering environments to protect user data from development and test activities. Employee access to each environment is limited by least privileged access (including time-based) and logged for monitoring and auditing.

Cryptographically Enforced Controls

Cloaked's servers cannot grant access to your vault to someone who doesn't have your Primary User Password or keys. This is a cryptographically enforced control to ensure that only you can access, decrypt, or change your data.

Other cryptographically enforced controls protect:

- Changing the associated emails address or phone number on your Cloaked account
- Preventing Cloaked servers (or employees) from ever learning your password or secret keys

Securing Local Access

Access to your encrypted data requires your Primary User Password, known only to you. When you create your Cloaked account, your Primary User Password serves as the master key, transformed by the Argon2id algorithm into a “Secret Box Key”. The Secret Box Key is then used to encrypt and decrypt your private key directly on your device using the XSalsa20 and Poly1305 algorithms.

This ensures your private key never leaves your device unencrypted. An additional "Authentication Key" derived from the Secret Box Key controls account access. To unlock your data, you need your Password, Username, and successful authentication through these derived keys.

Once you’ve logged into and decrypted your vault, data is loaded into local memory. The client is constrained to use only data decrypted using your unique key. If you choose to save your credentials for auto-filling instead of inputting your Primary User Password every time, they are encrypted and stored locally.

Hashing, Encryption, and Key Management

Version 1.0 - January 23, 2024

Hashing, Encryption, and Key Management

Cloaked employs several cryptographic methods to provide layered protection for user data:

- **Elliptical Curve Cryptography**

  with 256-bit key generated by Curve25519 is used to create asymmetric keys during account creation, which is then used for client-side encryption.

- **Argon2id**

  a specific variant of the Argon2 KDF (key derivation function), tackles several security issues related to password hashing and key derivation, offering significant improvements over older methods like PBKDF2. Here are some key security issues Argon2id addresses:

  - **Memory-hardness to protect against brute-force attacks –** Argon2id is deliberately memory-intensive, requiring attackers to allocate large amounts of RAM to crack passwords efficiently. This significantly increases the cost and difficulty of brute-force attacks compared to less resource-hungry KDFs.

  - **Tunable parallelism to protect against side-channel attacks –** Tunable parallelism: Argon2id allows specifying a "parallelism degree," limiting the number of CPU threads used for computations. This mitigates side-channel

attacks that exploit timing differences in multi-threaded implementations.

- **Data-dependent memory accesses to guard against GPU-powered attacks -** Argon2id uses memory accesses that depend on the input password, making it harder for attackers to utilize specialized hardware like GPUs for efficient cracking.

- **Adjustable cost factor to protect against rainbow table attacks –** Argon2id allows setting a "cost factor" that controls the number of memory iterations and overall computation time. Increasing this factor makes precomputed rainbow tables less effective and significantly slows down attackers.

- **Key stretching to defend against weak password exploits –** Argon2id stretches the password input through multiple rounds of memory-intensive computations, amplifying the entropy even for weak passwords and creating stronger derived keys.

Additional Benefits of Argon2id:

- **Salt integration –** Argon2id incorporates salting by default, ensuring unique keys for each user even with identical passwords.

- **Verifiable random function –** It incorporates a verifiable random function (VRF) that allows verifying the integrity of the KDF without compromising the password itself.

- **Xsalsa20-Poly1305**

  with 256-bit key combines two cryptographic algorithms for authenticated encryption. Cloaked deploys it to perform data encryption client-side to ensure confidentiality while also verifying data integrity. Each key is only used once.

Cloaked Vaults

While your data is client-side encrypted, your vault is additionally encrypted at rest and in-transit using Advanced Encryption Standard (AES) 256-bit encryption and TLS 1.3. All data encryption and cryptographic key generation is done locally by the client on your device to ensure that Cloaked never has access to your decryption keys or decrypted data.

Device Authentication

We use a unique User Device Key to authenticate each person on our servers. When you create a new Cloaked account, reinstall the Cloaked app, or add a new device to your account, a unique User Device ID is auto-created by the device OEM. To nullify the potential compromised password attack vector, Cloaked separates the data encryption key and the device authentication keys.

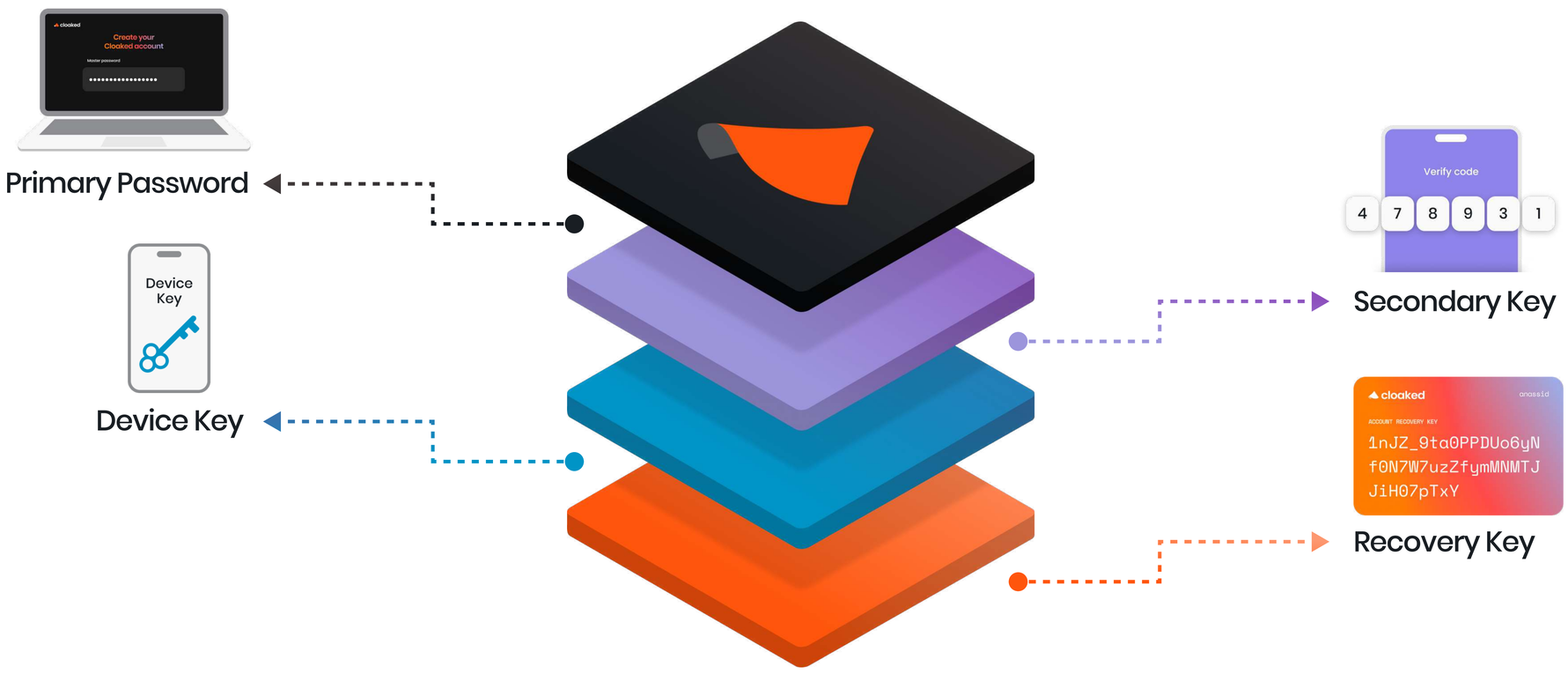
To protect both access to your account and the privacy of your data, your Cloaked account employs a pair of encryption keys: a public key that everyone can see and a private key kept hidden as your account's true gateway. These keys are generated using Curve25519, relying on a cryptographically secure random number generator for guaranteed unpredictability.

Your private key, the one your device uses to decrypt your data, is encrypted for further protection with a special key derived from your password. This password-derived key is crafted using an algorithm called Argon2id, making brute-force attacks significantly harder. The key then undergoes further transformations to become your password authentication key, the essential login credential for your account.

When creating keys, we use each browser's API for browser-based cryptography and the native libraries in iOS and Android for our mobile apps. We also use the Argon2 reference library compiled into Web Assembly (Wasm) or linked to the mobile.

Below is a list of different secrets we use to secure your vaults and their contents:

Vault security



Secret	Description	Use
User Primary Password	User-generated password The client side employs Argon2id to ensure a user plaintext password is not transmitted by Cloaked outside of the user's device. However, the resulting hash isn't directly stored. Instead, it undergoes further transformations to create a password authentication key. This key is then sent to the backend during user registration. Notably, the backend doesn't simply store the key as-is. Instead, it applies an additional layer of security by applying PBKDF2 to the key before finally storing it in the database.	Account access
User Secondary Key	Random 32-byte number generated server-side	Two-factor authentication
Device Key	Random 32-byte number client-side Auto-generated for each device	Authenticates each authorized device linked to your account
Recovery Key	Random 32-byte number client-side Generated during account creation	Recover your account if you forget your primary password

Email/Phone/Text Routing

The contents of your emails and SMS messages are protected at rest in our cloud environment using zero access encryption. This means only you can read them because only you have the private key to decrypt them. That key itself is encrypted and stored on your device.

However, please remember that due to third party email and SMS protocols, emails and text messages sent outside of Cloaked are not encrypted with your private key.

Authentication for Cloaked User Accounts

Version 1.0 - January 23, 2024

Authentication for Cloaked User Accounts

Cloaked is an end-to-end encrypted system which protects access to your vault and your data by restricting encryption and decryption to your account (rather than on our servers) using multiple keys derived from secrets unknown to us or our servers. Your password and secret key are used to derive the key we use for authenticating you, ensuring that it's really you logging into your account.

We use a 3-layer authentication process that looks like this:

1. To access your account, you must have your Primary User Password and the code from your chosen multi-factor authentication options (also referred to as your Secondary User Key)

2. In order to download the data from your vault onto your device, your device is authenticated using your Device Key.

3. Finally, to decrypt the contents of your vault, Cloaked will authenticate you using your publicly and private keys

Account passwords

You are the only one who knows your Primary User Password and when you use it to authenticate yourself in the Cloaked app or a browser, the data from your vault is loaded into the memory of your authorized device and decrypted using your unique key.

All communication between the Cloaked app on your device and Cloaked's servers takes place over SSL/TLS cryptographic protocol. Cloaked account recovery is possible with a secret recovery key. Without this or your Primary Password, you won't be able to access your account. This is to ensure the security of your data even if Cloaked systems are compromised. The recovery key feature outlined in the following section allows you to reset your Primary Password and recover your data while maintaining our zero-knowledge architecture.

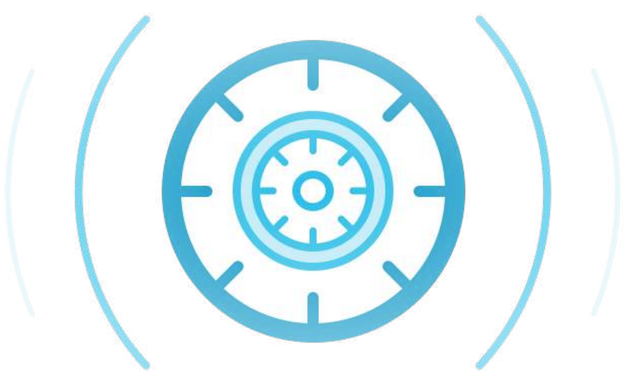


Figure 1 : Your account password, like a combination to a lock, is something that you know.

One Time Passwords

One time passwords are used to authenticate you during two different use cases:

1. During **account recovery**, we will send a one-time, time-bound recovery code to the email address or phone number registered to your Cloaked account. However, in addition to this one-time code, you will also need access to the unique Recovery Key that was generated when you created your account.
2. If you link a **two-factor authentication app** to your Cloaked account, you will be required to provide the authentication code from the app, in addition to your password, each time you login to Cloaked.

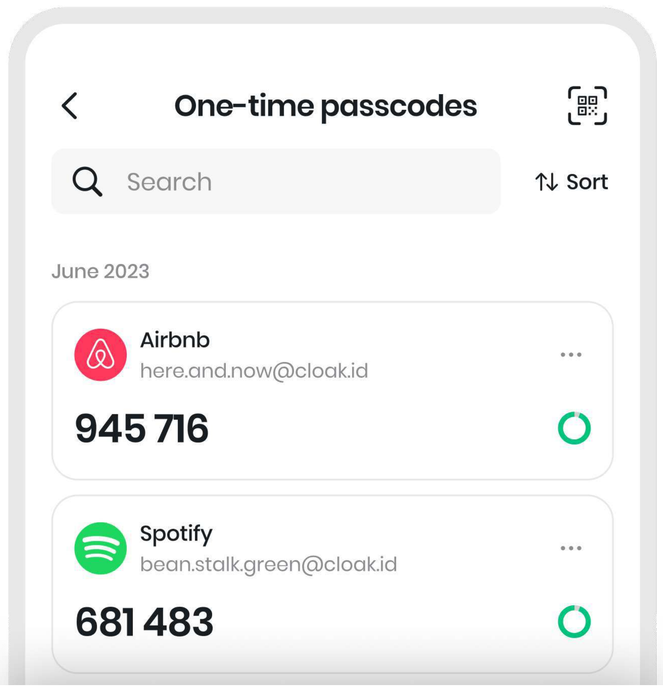


Figure 2 : One Time Password (TOTP)

Using Passwords + Keys

Decrypting your data requires your Primary User Password and your Secret Key. Cloaked does not have access to either of these, so you need to take good care of them. Requiring multiple secrets, each created and protected in a different way, increases the security of your account by protecting against things like credential stuffing or a compromise of Cloaked's internal systems.

Figure 3 : Master password and Secret key combination.

Two-Factor Authentication (2FA)

For additional security, you can link your Cloaked accounts to 2-factor authentication (2FA) methods such as text, email, or third-party apps. Support for physical keys and other methods is on our roadmap. When using 2FA, both your Primary User Password and the authenticator code are necessary for decrypting your vault.

If you chose to link your account to a 2FA application, all user data, both local and that sent to Cloaked servers, will be encrypted with a new key generated by a combination of your Primary User Password and the new, randomly generated Secondary Key (SK) stored on the Cloaked server.

At a high level, the authentication process using an authentication app like Google Authenticator, Okta, or Duo looks like this:

4. Link your Cloaked account with a 2FA application, following the instructions provided by your chosen application.

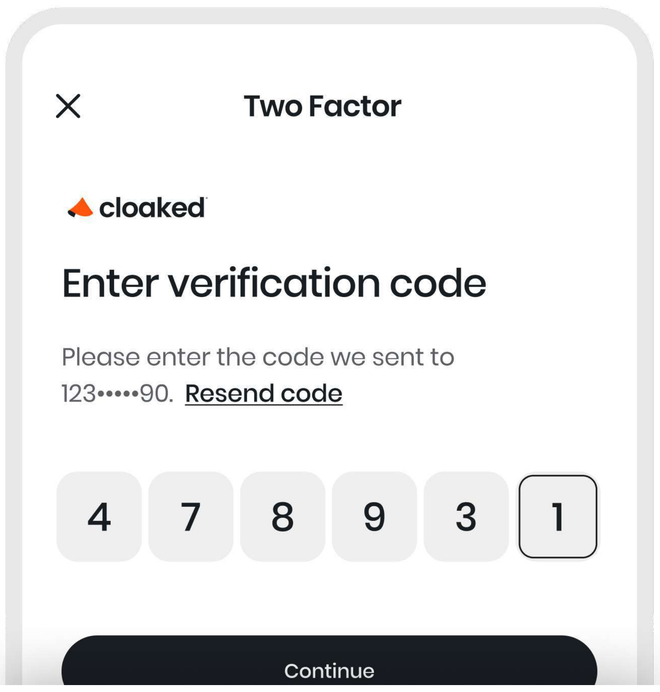


Figure 4 : Two-Factor Authentication (2FA), an authentication code is sent to the user's mobile device.

5. The application's time-based on-time password (TOTP) algorithm will generate a six-digit passcode, factoring in the current time of day to ensure that each passcode is unique.

6. After entering your password into the Cloaked app, you will be asked to provide the passcode generated by the 2FA application.

7. From now on, each time you log into Cloaked, our servers will require a One-Time Password generated by the linked 2FA application.

8. Only after receiving and verifying this One-Time Password, will Cloaked servers send your Secondary User Key to the Cloaked client application on your device to download the encrypted contents of your vault.

9. Your public and private key pair is still required to decrypt your data once it's downloaded.

Recovering Your Cloaked Account

Version 1.0 - January 23, 2024

Recovering Your Cloaked Account

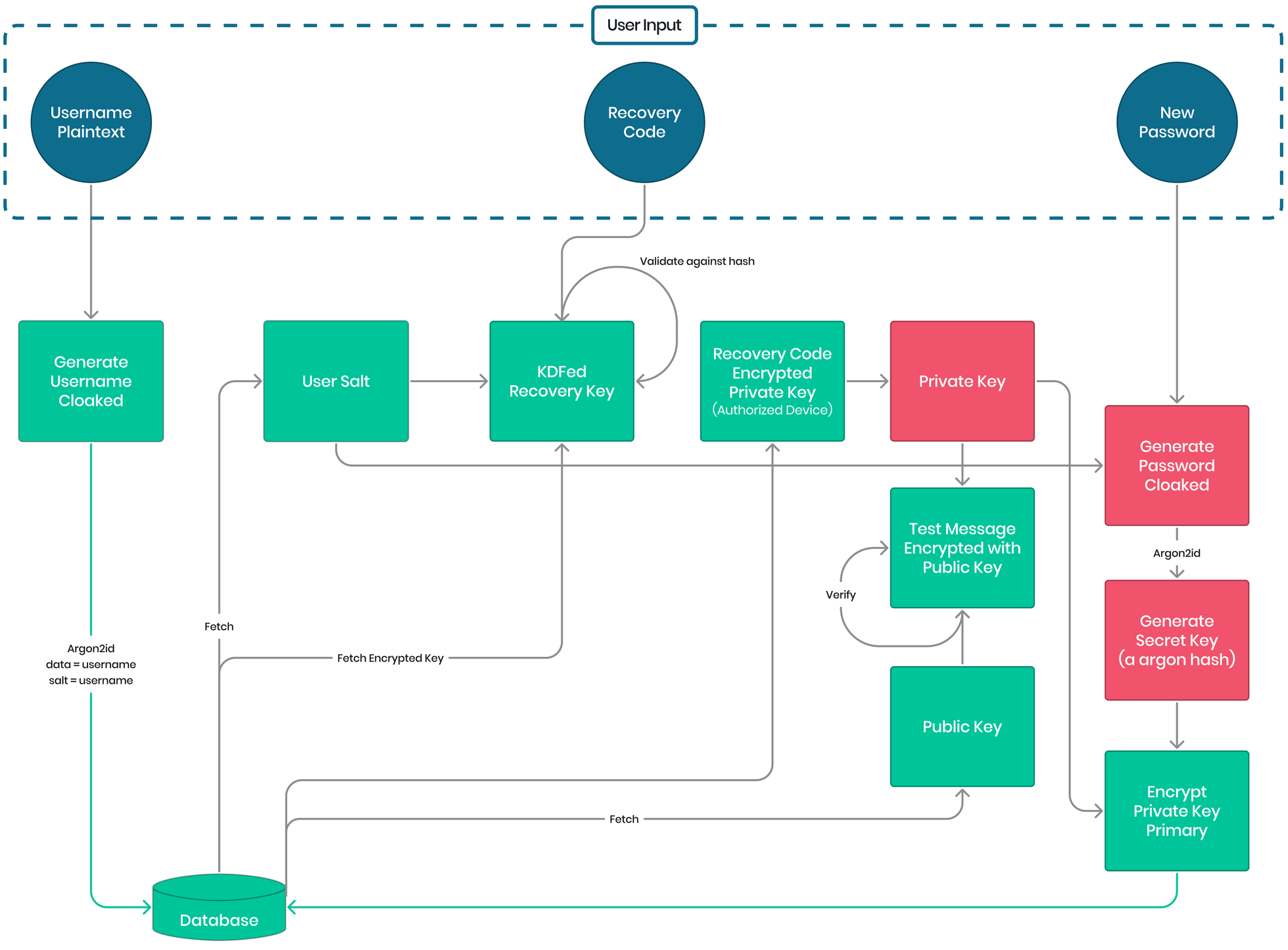


Figure 1 : Cloaked Account Recovery flow

If you forget your primary password, we have a process to help you regain access to your Cloaked account using an authorized device. Remember that only you know your primary password and it's never transmitted to or stored on Cloaked's servers. This preserves zero-knowledge security for your account and your data.

To recover an account, your local key – itself encrypted using your primary password – is also encrypted using a unique user recovery key. This recovery key is created and used for all of the authorized devices associated with your account.

If you need to recover your account, you will first be asked to verify your identity using a recovery code sent to the verified recovery email or phone number registered to your account. You will also need your secret Recovery Key that was auto-generated for you when you created your account. Once you're successfully logged in, you'll be able to create a new primary password for your account. Once verified, your recovery key is used to decrypt your local key, which in turn, enables your authorized device to decrypt your vault and its contents. The private key is then re-encrypted with your new primary password and re-synced to the Cloaked servers.

Because this process involves a change to your primary password, all of your trusted devices must be registered again to ensure the security of your account.

Cloaked Single Sign-On (sso)

Version 1.0 - January 23, 2024

Cloaked Single Sign-On

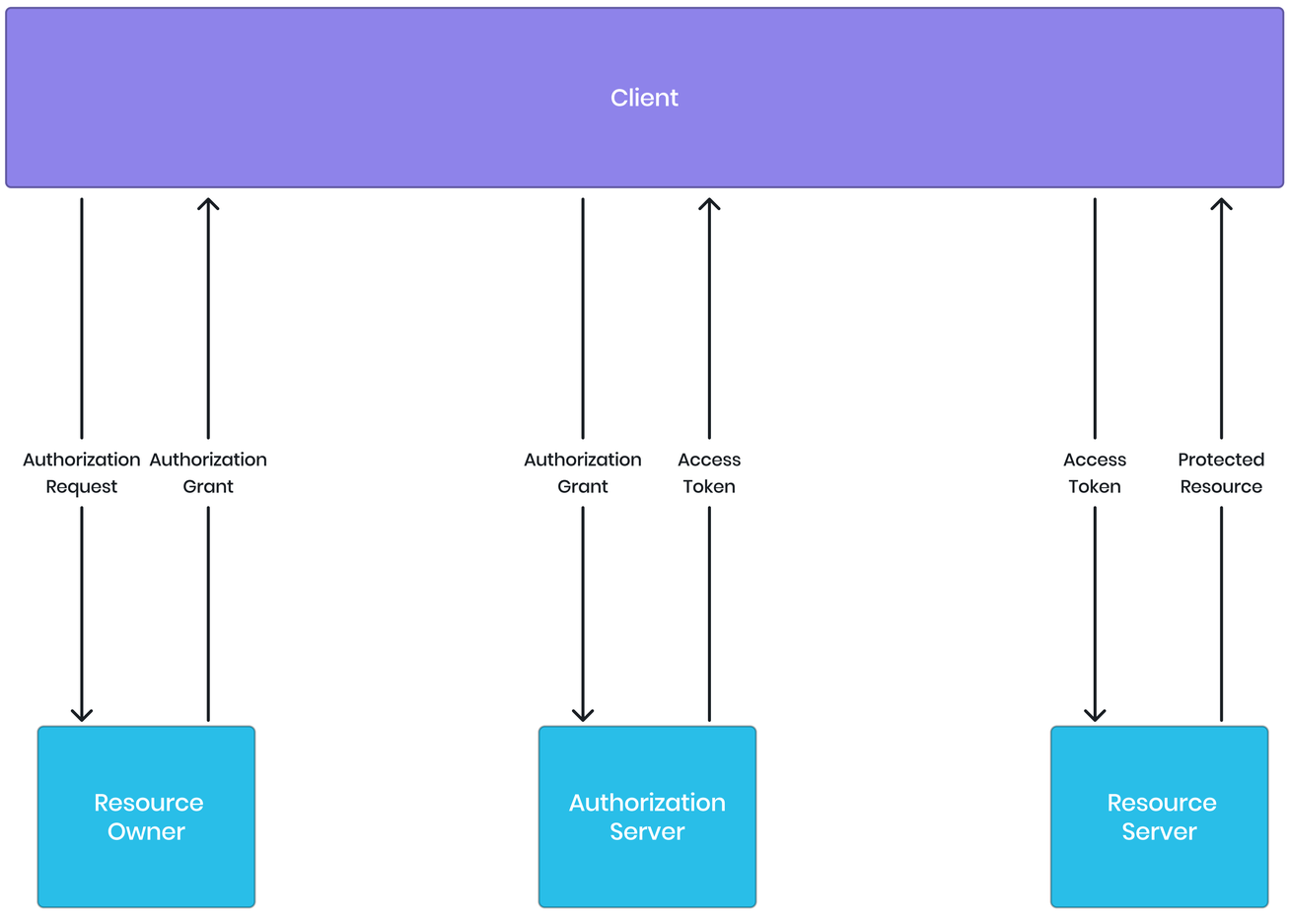


Figure 1 : Abstract Protocol Flow

Cloaked uses OAuth2.0 for token management and authorization grant workflow for all users as well as our own internal client applications, as if they were third parties. This protects against malicious applications while managing the token lifecycle. In the future, we expect customers will also be able to use Cloaked as an SSO provider.

Trusted devices: Devices successfully linked to your account using your Primary Password or SSO are given an auto-generated Device Key. These keys are random and unique to each device.

Protecting Your Data at Rest: Double Layered Encryption from Client to Cloud

Version 1.0 - January 23, 2024

Protecting Your Data at Rest Double Layered Encryption from Client to Cloud

At Cloaked, your privacy is paramount. We understand the critical nature of data security, which is why we implement a **double-layered encryption** approach to safeguard your information both **on your device and in the cloud.**

- First-layer encryption

  When you use Cloaked's encryption workflows, your data is transformed into an unreadable format **directly on your device**. This ensures that even if your device were compromised, your data remains secure.

- Second-layer encryption

  As your encrypted data journeys to our storage infrastructure, it undergoes **additional encryption through industry-standard protocols** employed by our underlying technologies. This additional layer further strengthens the protection of your sensitive information.

- ## Trusted Foundations

  Your encrypted data is split and rests in two locations:

  - **External personal vaults:** Your personal data vault, powered by a secure, external database provider, leverages **256-bit AES encryption at rest** and robust Transport Layer Security (TLS) to secure data in transit. The multi-data center architecture ensures redundancy and continuous protection, with backups also benefiting from high-grade encryption.
  - **Amazon Web Services (AWS):** Within AWS, your data resides in Amazon RDS encrypted DB instances utilizing the **industry-standard AES-256 encryption algorithm**. This additional layer adds yet another level of security and complies with stringent standards of a trusted cloud provider.

By relying on **rigorously evaluated solutions and established encryption protocols**, Cloaked empowers you to take control of your data privacy. You can be confident that your information is protected through every step of its journey, from your device to secure cloud storage.

Securing Communications by Encrypting in Transit

Version 1.0 - January 23, 2024

Securing Communications by Encrypting in Transit

At Cloaked, we understand that secure communication is the cornerstone of protecting your sensitive information. That's why we've implemented an unwavering commitment to using the most advanced cryptographic protocols available.

Here's how we safeguard your data in transit:

- ## HTTPS as a Fortress

  All communications between the Cloaked application and our servers are fortified by HTTPS, the industry-standard protocol for secure web communication. This establishes a secure tunnel, ensuring that your data remains impenetrable while traveling across the internet.

- ## OpenSSL as the Gatekeeper

  On the client side, we leverage OpenSSL, a renowned open-source toolkit, to execute HTTPS connections. OpenSSL's robust reputation for reliability and security further reinforces our commitment to protecting your data.

- ## Embracing the Latest in TLS

  We exclusively employ TLS 1.3, the most advanced and secure version of the Transport Layer Security protocol. This cutting-edge protocol offers enhanced performance, privacy, and resilience against potential attacks.

The Secure Handshake:

The diagram below visually illustrates the meticulous steps involved in establishing a secure TLS 1.3 connection between the Cloaked application and our servers:

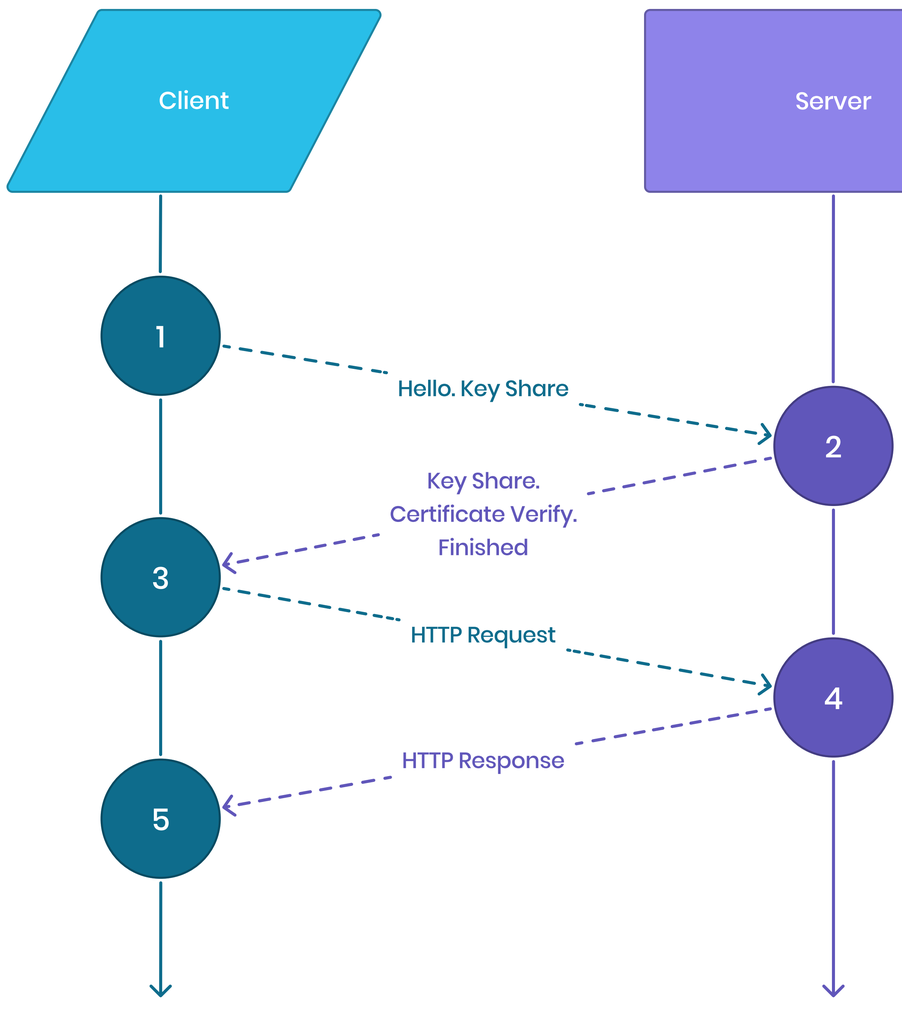


Figure 1 : TLS 1.3 Full Handshake

Key Steps for Unbreakable Protection:

1. **Cipher and Hash Harmony:** The client and server engage in a meticulous negotiation to select the most robust cipher and hash algorithms supported by both parties. This ensures the highest level of encryption and data integrity.

2. **Digital Certificate Assurance:** The server presents a digital certificate, serving as its verified online identification.

3. **Certificate Authority Validation:** The client meticulously verifies the authenticity of the certificate by consulting a trusted Certificate Authority. This process guarantees that you're communicating with the legitimate Cloaked servers.

4. **Shared Secret Genesis:** The client crafts a unique random number and encrypts it using the server's public key, ensuring only the server can decipher it. This encrypted number forms

the foundation for generating a shared secret key.

5. **Symmetric Key Fortification:** Both the client and server leverage the shared secret to generate a symmetric key. This key acts as a formidable lock, encrypting and decrypting all subsequent data exchanged between them.

Through this steadfast adherence to industry-leading protocols and meticulous key exchange, Cloaked establishes a virtually impenetrable fortress for your data in transit. You can rest assured that your information remains shielded from prying eyes, ensuring your privacy remains paramount.

Infrastructure Security

Version 1.0 - January 23, 2024

Infrastructure Security

Data We Store

We store account, vault endpoints, and user authentication information in a relational database in order to provide access to the appropriate account, vaults, and items in a vault once you've been successfully authenticated. This is separate from the authentication process required to encrypt or decrypt data in your vault, which also requires your secret key. Cloaked does not have access to passwords or secret keys.

To see a full list of the data Cloaked collects, please refer to our privacy policy.

How It's Stored

Cloaked uses a relational database in RDS on AWS to store account, vault endpoints, and user authentication information including:

- Usernames (hashed with Argon2id)
- Passwords (double hashed with Argon2id + PDKF2)
- Encrypted keys
- Cloaked identifiers such as email address and phone numbers.
- Relationships to objects like identities owned

Vault information is stored with a third party database provider, intentionally separated from Cloaked corporate infrastructure to limit single vendor risk within AWS.

Client-Side Data Encryption

Data you enter into the Cloaked client is encrypted locally on your device, including but not limited to: usernames, passwords, email addresses, phone numbers, notes, emails, SMS, call data, etc.

Server-Side Data Encryption

Email addresses and phone numbers used for recovery or routing purposes are encrypted and stored by Cloaked servers.

Protecting Against Bad Actors

Version 1.0 - January 23, 2024

Protecting Against Bad Actors

Prohibited Use

Our Prohibited Use Policy describes the types of user behavior, account activity, and organizations barred from using our products. This includes, but is not limited to unlawful behavior, abuse of other users, and fraud. Please read our policy for more information at cloaked.com/prohibited-use-policy.

Bad Actor Mitigation

Because of end-to-end encryption, Cloaked cannot see the contents of user vaults or messages in order to detect malicious behavior. Instead, we use a combination of threat intelligence, signals intelligence, and behavioral detection controls to identify, monitor, and block suspicious account activity. We also participate in information sharing with the technical and law enforcement communications regarding threat actors. To preserve the effectiveness of these systems, additional information is available only upon request and under the protection of an NDA.

Internal Access Controls

Cryptographically enforced controls protect your vault and its contents by Cloaked employees. For example, encryption and decryption of data in your vault is done locally on your device using your secret key, which is also stored on your device.

We also use technical controls to limit employee access and of account information stored on Cloaked based on job requirements. Access is also scoped using the privilege of least privilege to include only information that is required to perform individual tasks specific to an employee's role, such as customer support.

White paper Version History / Changelog

V1.0 First public release – **January 23, 2024**