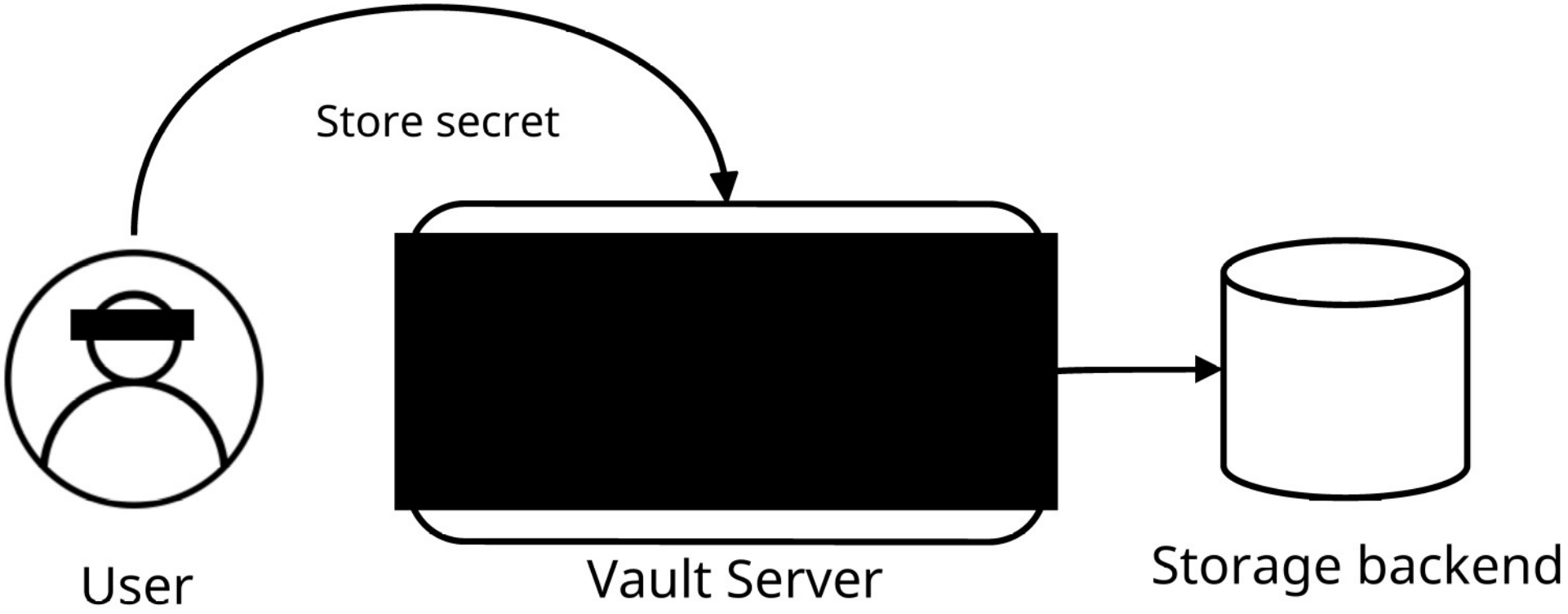
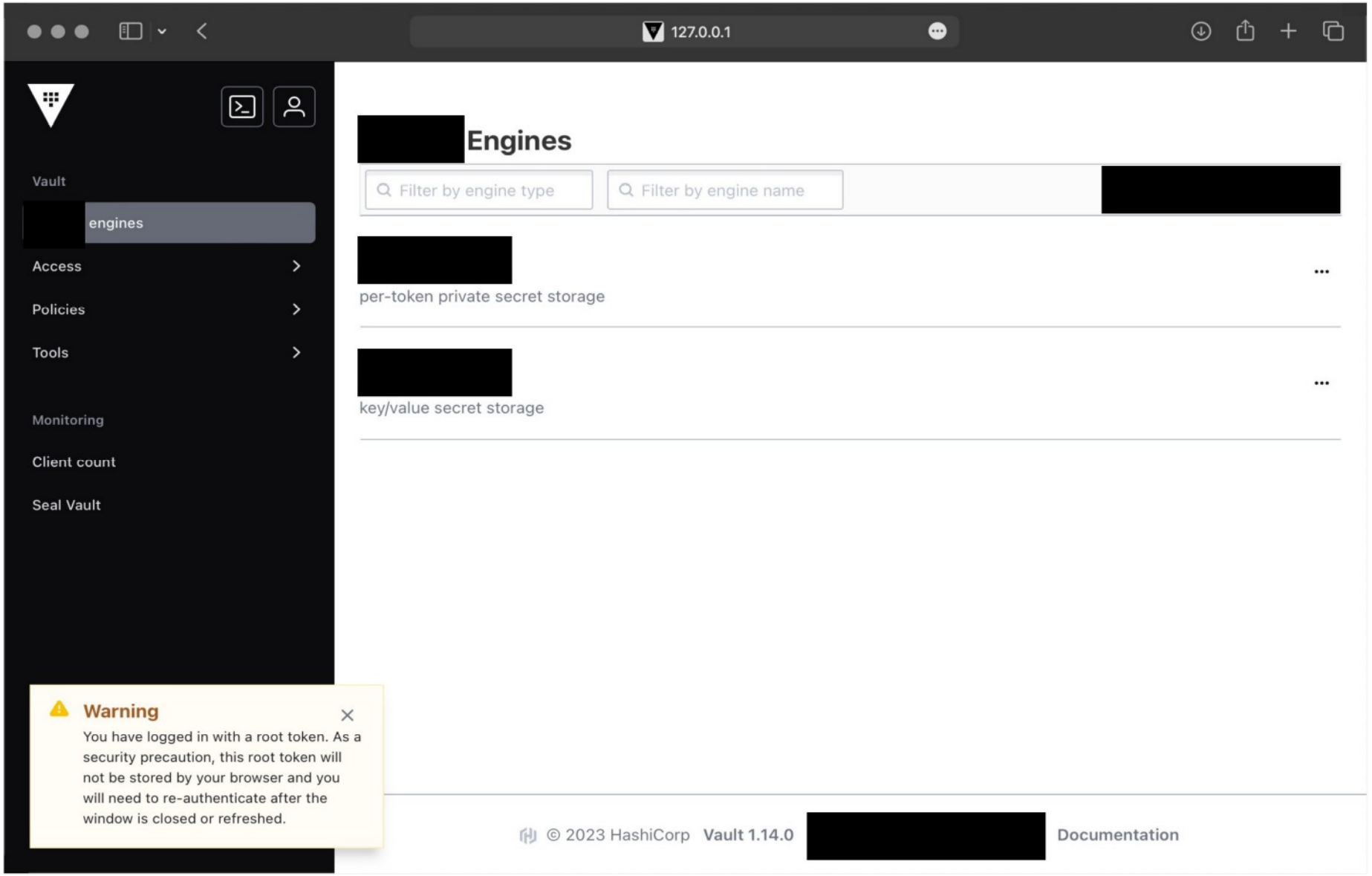
[redacted] Storing [redacted]

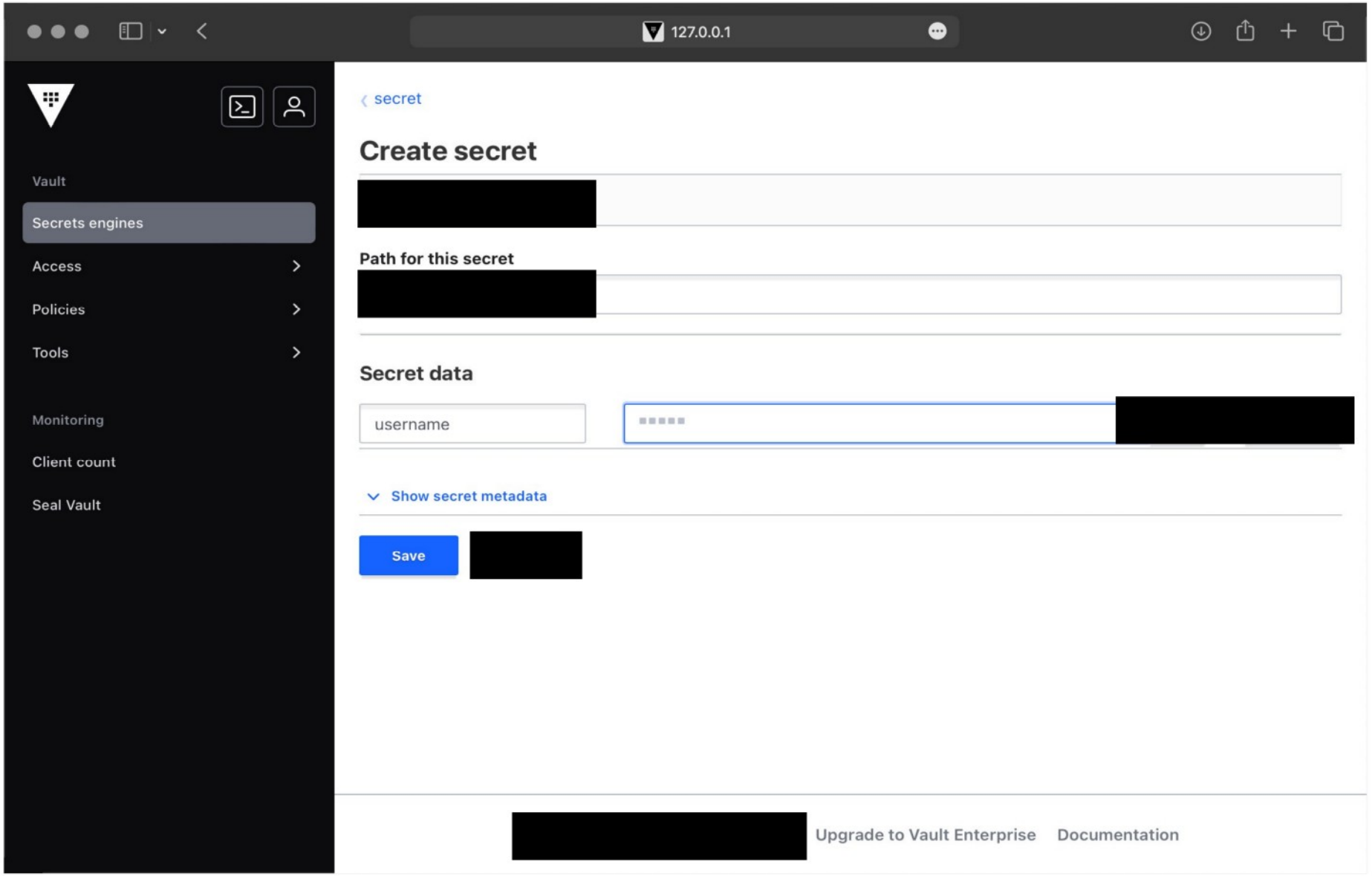
- Core features of Vault: [redacted]
- [redacted] engines: store, generate or encrypt data
- Multiple [redacted] engines each with their own features
- [redacted]



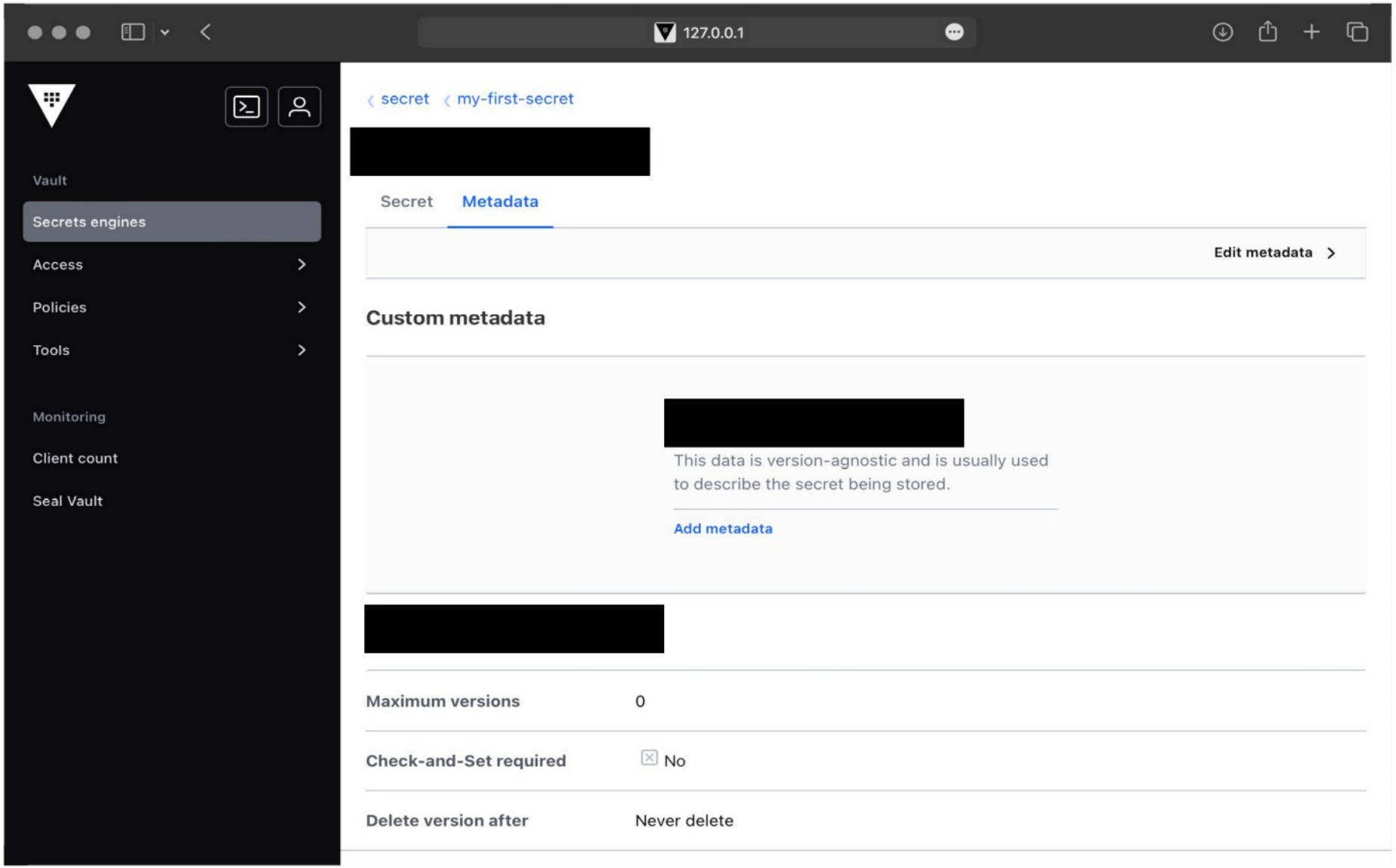
Secrets - GUI Demo (1)



Secrets - GUI Demo (2)



Secrets - GUI Demo (3)



[redacted] – CLI (1)

```
[redacted] kv -help
Usage: vault [redacted] [options] [redacted]

(...)

[redacted]
   delete              Deletes versions in the KV store
   destroy             [redacted]
   enable-versioning   Turns on versioning for a KV store
   get                 Retrieves data from the KV store
   list                List data or secrets
   [redacted]
   patch               Sets or updates data in the KV store without overwriting
   put                 Sets or updates data in the KV store
   [redacted]
   undelete            Undeletes versions in the KV store
```

Secrets – CLI (2)

```
$ vault kv put [redacted] password=[redacted]
======== Secret Path ========
[redacted]-second-[redacted]

======= Metadata =======
Key                [redacted]
---                -----
created_time       [redacted]
custom_metadata    <nil>
[redacted]         n/a
destroyed          [redacted]
version            1
```

Secrets – CLI (3)

```
[redacted] kv put [redacted]
======== Secret Path ========
[redacted]data/my-[redacted]

======= Metadata =======
Key                 Value
---                 -----
created_time        [redacted]
[redacted]          <nil>
deletion_time       n/a
destroyed           [redacted]
version             [redacted]
```

Secrets – [redacted]

```
$ [redacted] kv put [redacted]
======== Secret Path ========
secret/data/my-[redacted]

======= Metadata =======
Key                 Value
---                 -----
created_time        2023-12-25T11:24:02.241695Z
[redacted]          [redacted]
deletion_time       n/a
destroyed           [redacted]
version             3
```

[redacted] – CLI (5)

```
$ [redacted] kv get [redacted]-secret
======== Secret Path ========
[redacted]-secret

======= Metadata =======
[redacted]
---                    -----
[redacted]             2023-12-25T11:24:02.241695Z
custom_metadata        [redacted]
deletion_time          n/a
[redacted]             false
version                [redacted]

====== Data ======
[redacted]             Value
---                    -----
[redacted]             [redacted]
```

Secrets – CLI (6)

```
$ [redacted] -version=2 secret/[redacted]
======== [redacted] Path ========
[redacted]-secret

======= Metadata =======
[redacted]                Value
---                 -----
created_time        [redacted]
custom_metadata     [redacted]
deletion_time       n/a
[redacted]
version             2

====== Data ======
Key          Value
---          -----
[redacted]
```

[redacted] – CLI (7)

```
$ vault [redacted] -versions=2 [redacted]
[redacted] at: secret[redacted]-secret

$ vault [redacted]/my-second-secret
======== Secret Path ========
secret/[redacted]

======= Metadata =======
Key                 Value
---                 -----
created_time        2023-12-25T11:23:02.241695Z
custom_metadata     [redacted]
deletion_time       2023-12-25T11:28:02.241695Z
destroyed           [redacted]
version             2

[redacted]data
```

Secrets – [redacted]

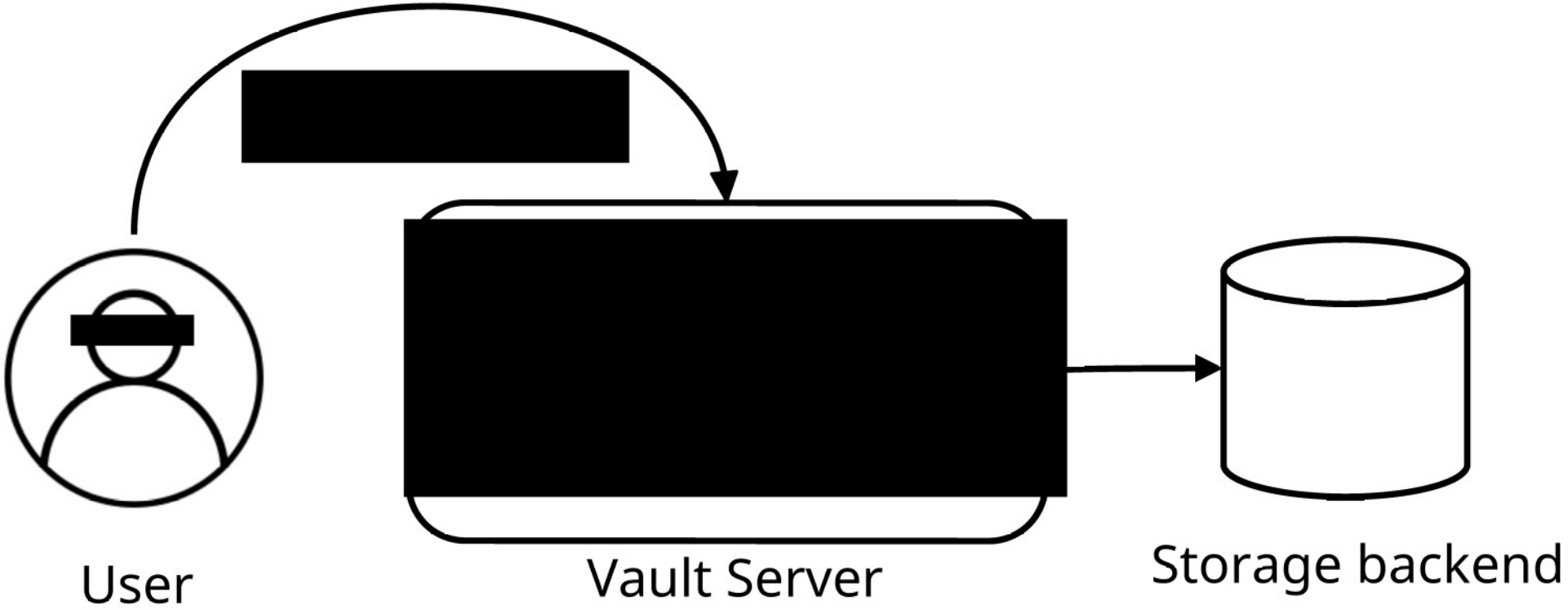
```
$ vault [redacted] secret/[redacted]
Success! [redacted] -secret
[redacted]
$ vault [redacted] -version=2 [redacted]
======== Secret Path ========
[redacted]
======= Metadata =======
[redacted]              Value
---                     -----
created_time            2023-03-17T11:28:09.13843Z
[redacted]
deletion_time           n/a
destroyed               [redacted]
version                 2
====== Data ======
Key          Value
---          -----
[redacted]   [redacted]
```

Secrets – [redacted]

Command	Description
`vault [redacted]`	[redacted] my-secret
[redacted] `my-secret password=vault2`	Stores key/value pair at secret/[redacted]
`vault kv delete [redacted]`	[redacted]
`vault kv undelete -version=2 [redacted]`	Restores version 2 of [redacted]
[redacted]	Permanently removes version 2 data from [redacted]
`vault kv metadeta delete -` [redacted]	Deletes metadata of version 2 for secret/my-secret
[redacted] `secret/my-secret`	Deletes all versions and metadata for [redacted]

Secrets – Secrets Engines (1)

- [redacted] generate or encrypt data
- Multiple [redacted] each with their own features



[redacted] Engines (2)

- [redacted] examples
  - [redacted]
  - Databases (dynamic)
  - Key/Value (static)
  - [redacted]
  - [redacted]
- Secrets engines are enabled at a given mount point
  - [redacted]
  - Secrets are stored inside that mount point

Secrets – [redacted] Lifecycle (1)

Option	Description
[redacted]	Enables a secrets engine at a path. [redacted]
`disable`	[redacted] All secrets are revoked. [redacted]
[redacted]	Moves the path for an existing secrets engine. Think of this like rename.
`tune`	Modifies [redacted] engine.

Secrets – [redacted] Lifecycle (2)

- [redacted]

```
$ [redacted] kv
Success! Enabled the kv secrets engine at: kv/
$ vault [redacted]
Success! Enabled the kv-v2 secrets engine at: kv-v2/
$ [redacted] -path=custom-[redacted]
Success! Enabled the kv secrets engine at: custom-kv/
```

[redacted]

```
[redacted] kv
Success! Disabled the secrets engine (if it existed) at: kv/
```

- Move

```
[redacted] secrets [redacted]
Started moving [redacted] engine [redacted] to [redacted]
[redacted] Finished moving secrets engine [redacted] to kv/ (..)
```

Secrets – Secrets Engine Lifecycle (3)

- Tune

```
$ vault [redacted]
Key                     Value
---                     -----
[redacted]              768h
description             n/a
[redacted]              false
max_lease_ttl           [redacted]

[redacted] -description="Vault Fundamentals" [redacted]
Success! [redacted] at: [redacted]

$ vault read [redacted]
[redacted]
---                     -----
[redacted]
description             [redacted]
[redacted]
[redacted]
```

Secrets – [redacted] Store (1)

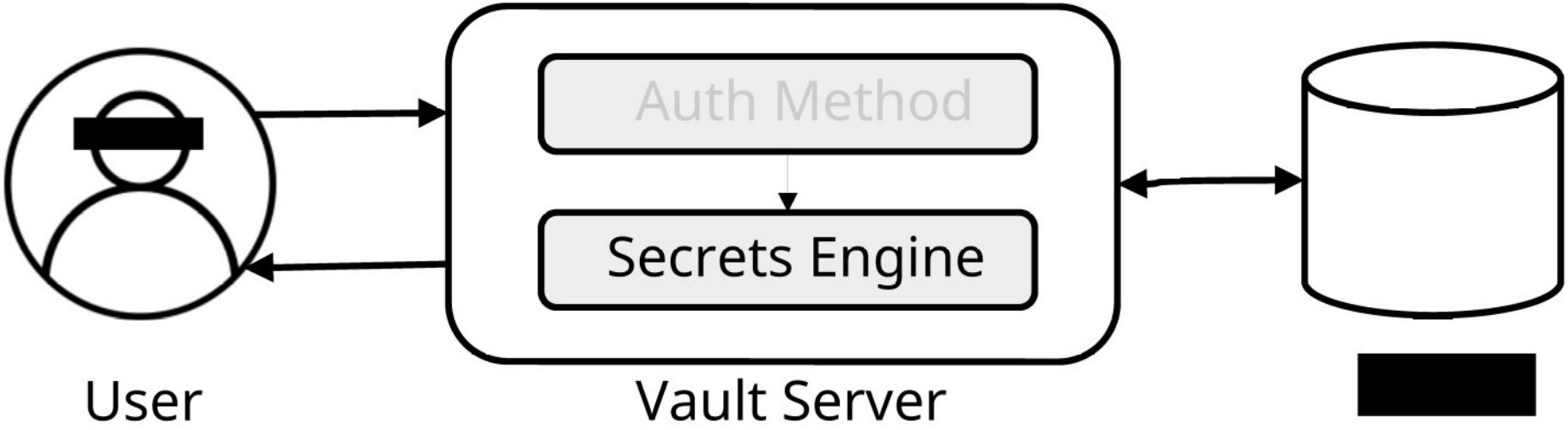
- Generic [redacted]
  - [redacted] (key)
  - Corresponding data (value)
  - [redacted] names must be [redacted]
  - Values [redacted] binary data
    - [redacted] (long string)
- Two modes
  - Non-versioned [redacted]
  - [redacted] (kv-v2)

Secrets – Secrets Engine -

- written value
- Kv-v2:
  - Metadata and data of older
- is default
  - To enable
    -
    - **kv-v2** in stead
- Kv-v1 can
  - Not the other way round
  - **vault** **<MOUNT>**

Secrets – Dynamic Secrets (1)

- Certain secrets [redacted] on dynamic secrets
- Secrets: [redacted] generation



Secrets – Dynamic Secrets – [redacted]

- Each dynamic secret [redacted]
  - [redacted] containing information
    - Time [redacted]
    - Renewability
- When lease has expired
  - Vault [redacted] the data
- Manual revocation is also possible
- [redacted] with a prefix of the secrets engine
- GUI is complimentary, [redacted] most configuration
  - GUI can be useful for lease observation / [redacted]

Secrets – Dynamic Secrets – [redacted]

[redacted]	Description
[redacted]	Renews the lease on a secret, extending the time it can be used before [redacted] revokes it.
revoke [redacted]	When a lease is revoked, [redacted] invalidated and prevents further renewals.
[redacted]**fix**	Revokes [redacted] path (e.g. **`revoke -prefix azure/creds/developer`**)

Secrets – Dynamic Secrets - [redacted]

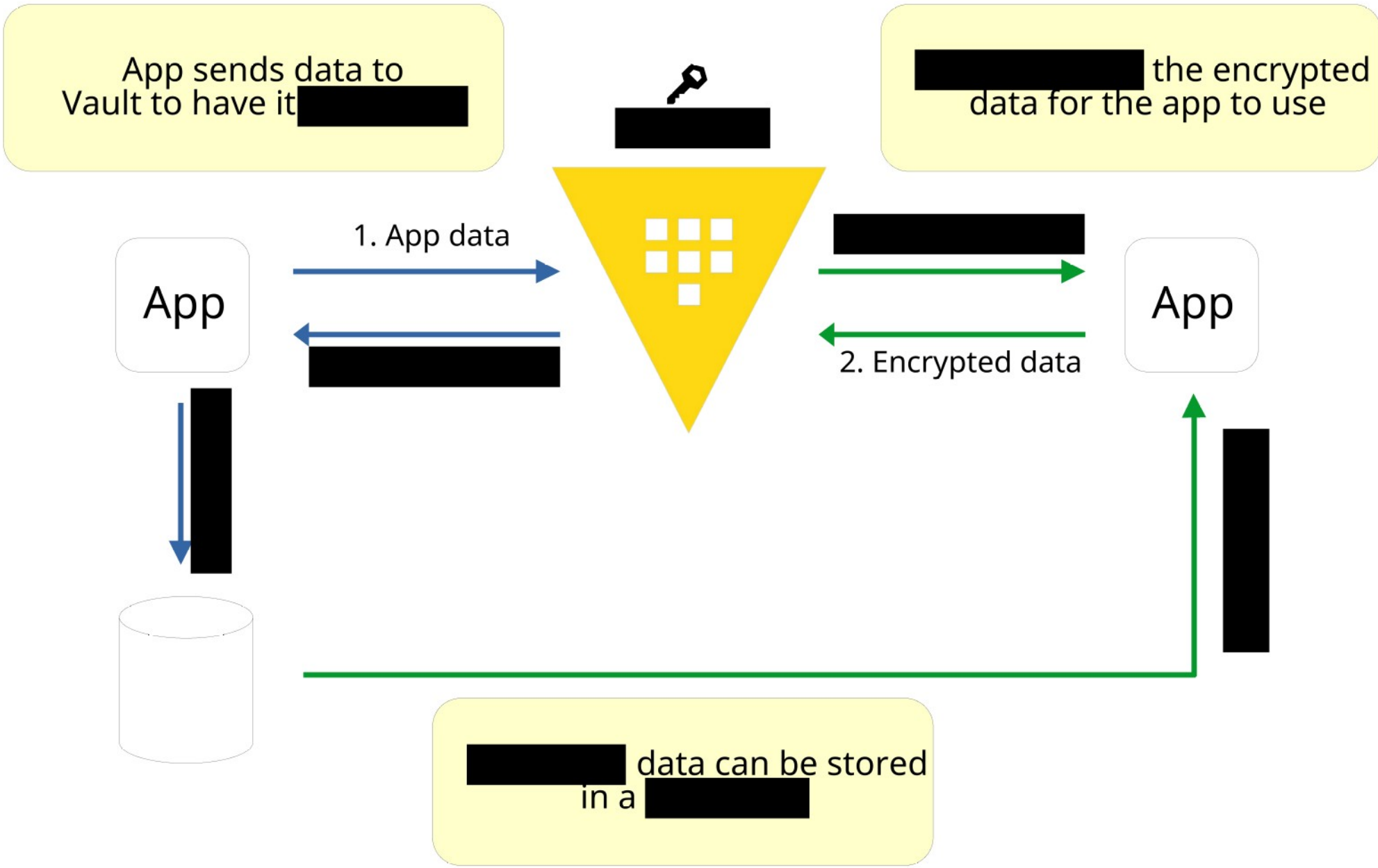
Secrets – Secrets [redacted] Generic

- A few secrets [redacted] generic
- No [redacted] external [redacted] is needed
  - K/V (already covered)
  - Transit
  - [redacted]
  - PKI
  - [redacted]

Secrets – [redacted] – Transit [redacted]

- Offers [redacted] Service
  - Developers do not have to know everything about [redacted]
- Handles cryptographic [redacted] transit
  - Vault does [redacted] the secrets engine
- Use case
  - Encrypt data from applications while [redacted] data ir [redacted]
- Data gets encrypted by an encryption key
  - [redacted] AES key is standard
  - Can be rotated
- Accepts [redacted] base64 [redacted] strings

Secrets – [redacted] – Transit (2)



Secrets – Secrets Engine – Transit (3)

```
$ [redacted] transit/keys/keyname
Success! Data written to: transit/keys/keyname

$ vault write [redacted] \
    plaintext=$[redacted] base64)
Key             Value
---             -----
ciphertext      vault:v1:dJmop+WmCk19Fw1E4n6cv6+ExfefdB83p6(....)
[redacted]

$ [redacted] decrypt/keyname \
    ciphertext=vault:v1:[redacted] +ExfefdB83p6(...)
Key             Value
---             -----
plaintext       [redacted]

$ [redacted] --decode <<< [redacted]
Encrypt this text
```

[redacted]

Secrets Engine – Transit (3)

[redacted]

Secrets – Secrets Engine – [redacted] (1)

- TOTP stands for [redacted] Password
- Temporary password with short lifetime
  - Expires [redacted] 120 or 240 seconds
- Example: Google [redacted]
- Can act as
  - Generator (like [redacted])
  - [redacted] sign-in service)

Secrets – Secrets Engine – TOTP (2)

```
$ vault [redacted] totp
Success! Enabled the totp secrets [redacted]

$ vault write [redacted]
    totp/keys/training \
    [redacted]
    issuer=ATComputing \
    [redacted]fundamentals.io | \
    base64 -d > [redacted]

$ vault read totp/[redacted]
Key     Value
---     -----
[redacted]  160211
```

Secrets – Secrets [redacted] (1)

- [redacted] dynamic X.509 [redacted]
- Only high [redacted] of the PKI secrets engine
  - PKI is too [redacted]
- [redacted] certificate store
- Can act as [redacted]
  - Intermediate [redacted]
- Cuts through the usual [redacted]
- Allows [redacted]

Secrets – Secrets Engine – PKI [redacted]

Traditional [redacted]

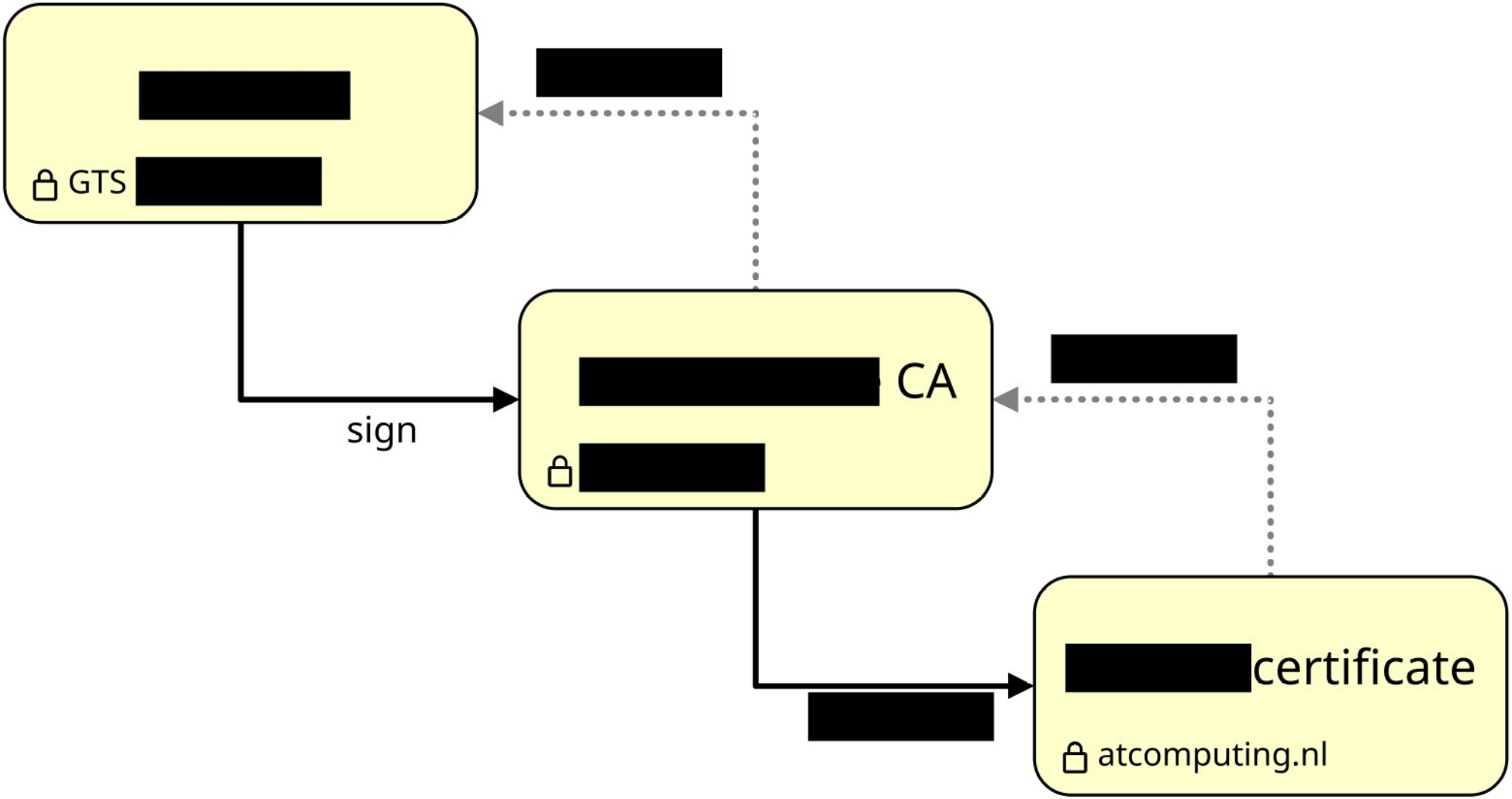
- Complicated [redacted]
  - TLS key-pair: [redacted] and private key
- Certificate Signing Request (CSR) specifies identity
  - [redacted]
- Certificate [redacted] creates certificate and signs it with its own private key
  - [redacted] to requester and can be decrypted with it's own private key

Vault process

- [redacted] "common name"
- Certificate, private [redacted] generated

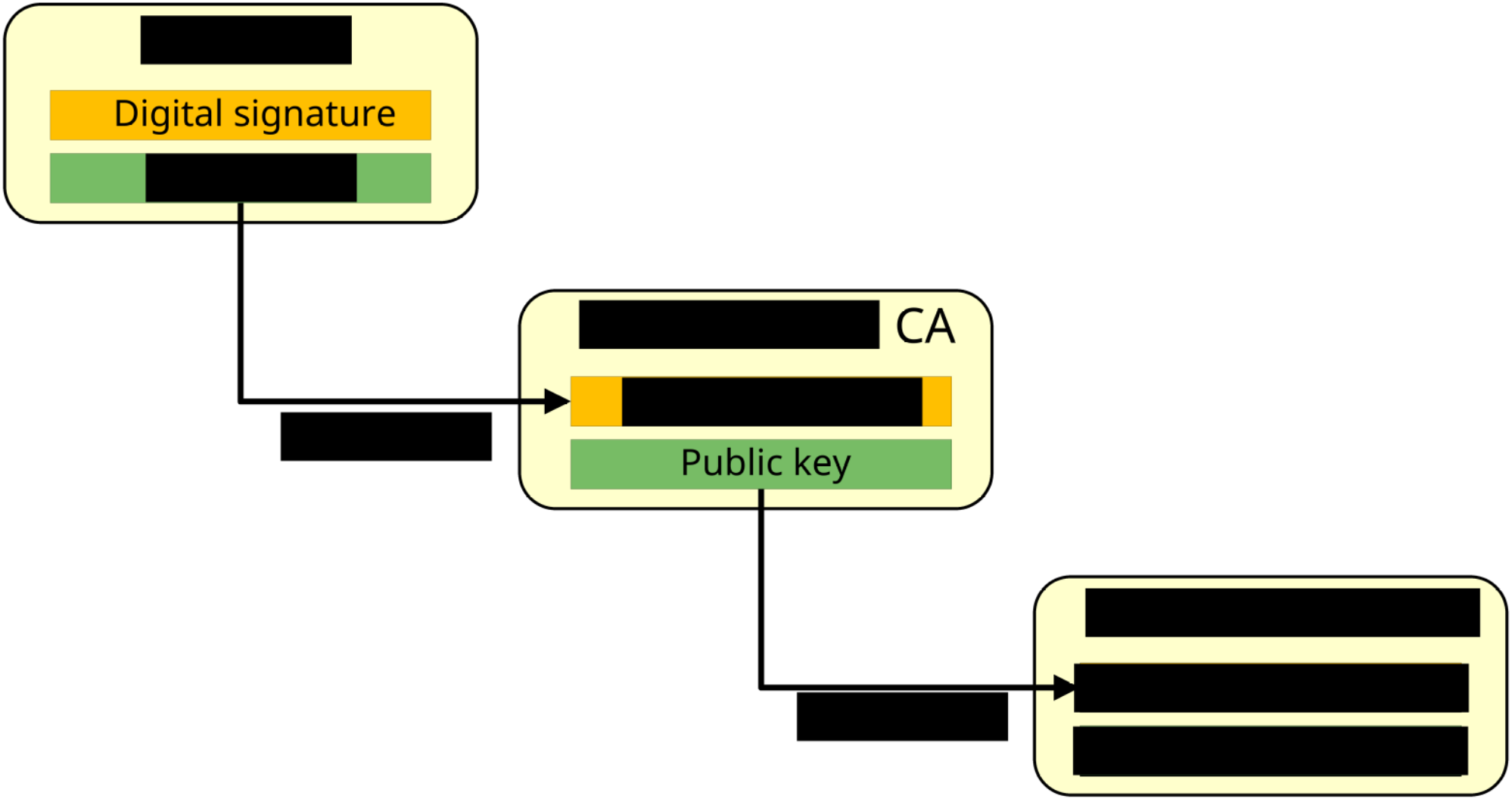
[redacted] – Secrets Engine – PKI (3)

Certificate chain [redacted]



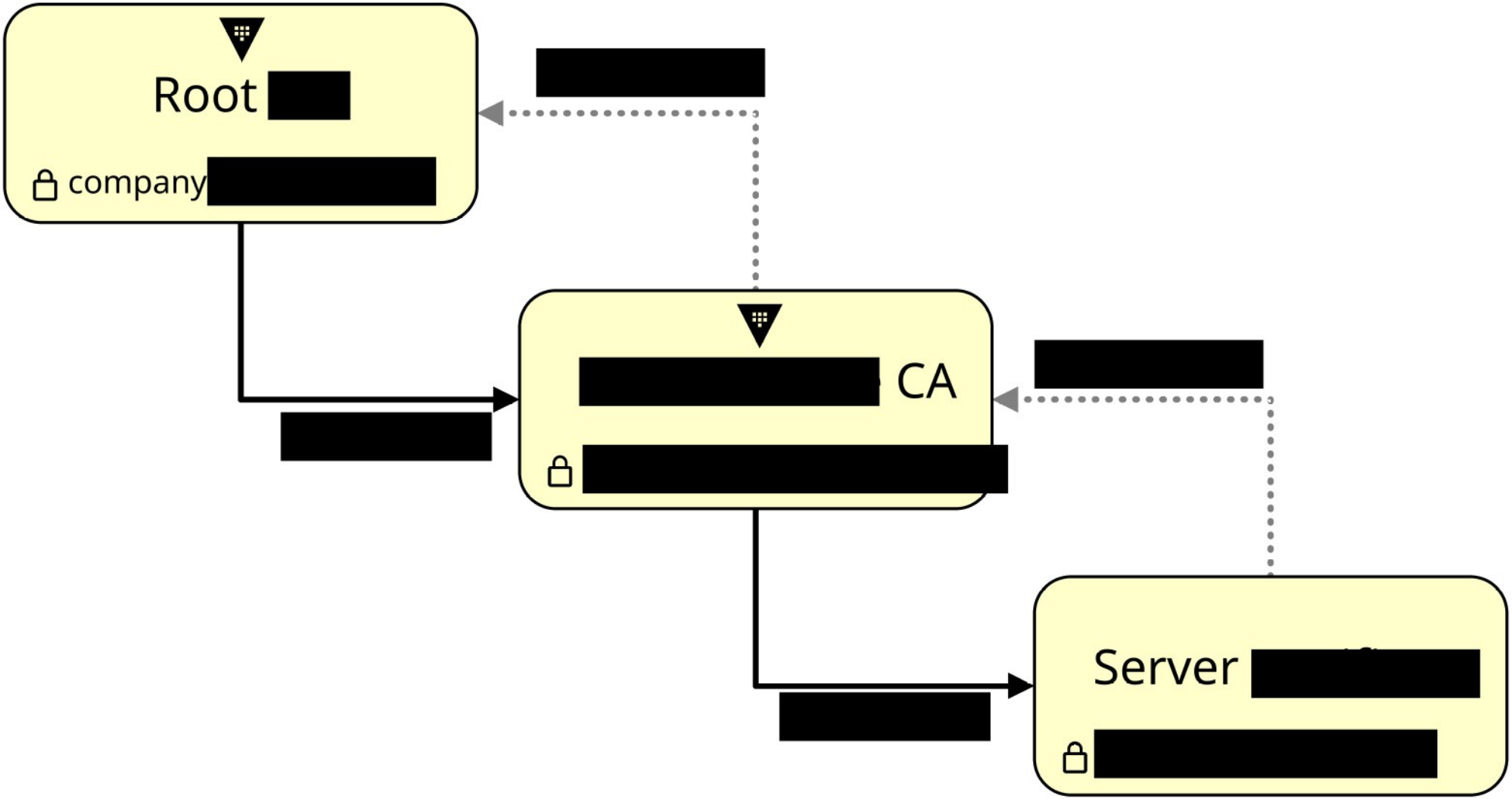
Secrets – [redacted]

[redacted] example



[redacted] Engine – PKI (4)

Certificate [redacted] Vault



Secrets – Secrets Engine – [redacted]

[redacted]

Root CA

[redacted]

Secrets – Secrets Engine – [redacted]

- Provides [redacted] for you alone
  - Only you can view these [redacted]
  - [redacted] your cubbyhole
- [redacted] by default
  - [redacted] enabled
- Paths are scoped per token
  - [redacted] destroyed
- No token can [redacted] cubbyhole

Secrets – Secrets Engine – Cubbyhole (2)

```
$ vault [redacted] password=[redacted]
[redacted]
                    hvs.[redacted]JMp0RsRRnLcOcDc
                    1m

$ vault [redacted] username=admin
Success! Data written to: [redacted]

$ [redacted] cubbyhole/tempsecret
Key          Value
---          -----
[redacted]

$ sleep [redacted]

$ [redacted] cubbyhole [redacted]
Error reading [redacted] Error making API request.

[redacted]
Code: 403. Errors:

[redacted]permission denied
```

Secrets – Secrets Engine – Cubbyhole (3)

```
$ vault [redacted]vault

[redacted]authenticated. The token information displayed below
is already stored in the token helper. [redacted] "vault login"
again. Future [redacted] automatically use this token.

Key                  Value
---                  -----
[redacted]           hvs.[redacted]JbEyQQEeA
token_accessor       [redacted]
token_duration       1m
[redacted]
token_policies       ["default"]
identity_policies    []
policies             ["default"]
[redacted]           [redacted]

$ vault read [redacted]
[redacted]tempsecret
```