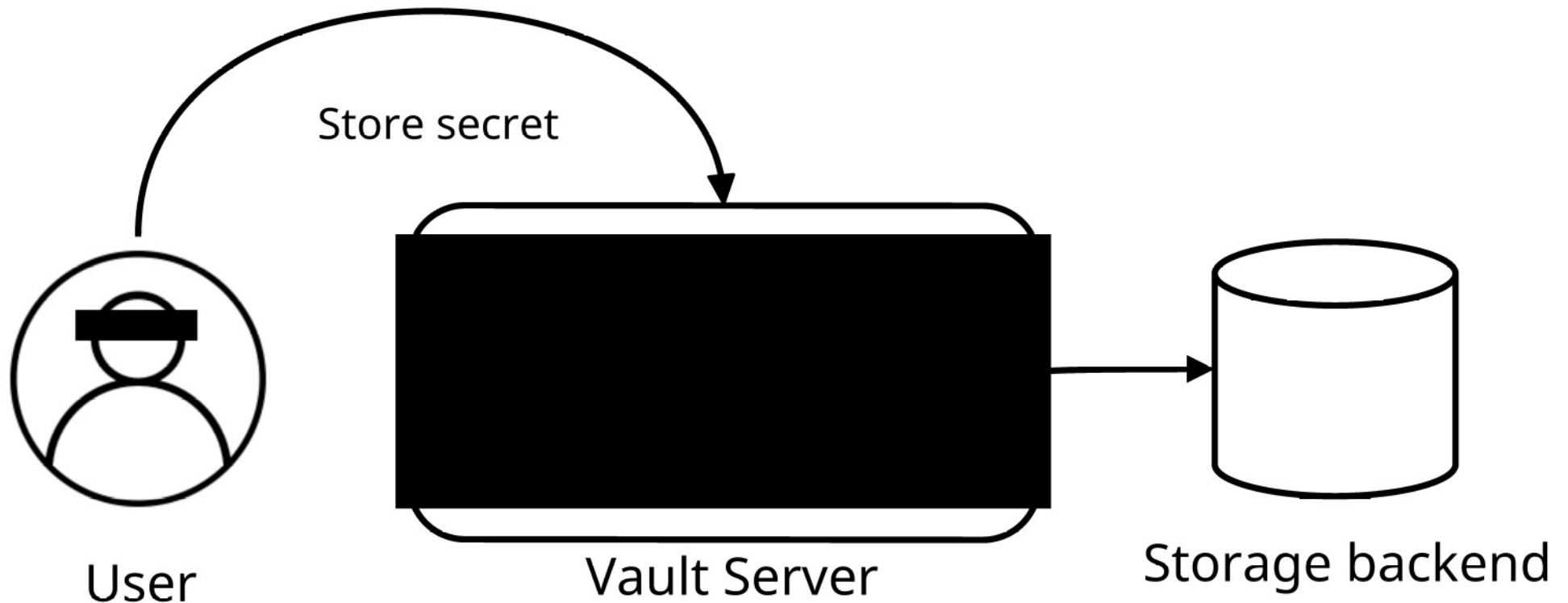


# Storing

- 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)

The screenshot shows the HashiCorp Vault web interface. The browser address bar displays '127.0.0.1'. The left sidebar contains a navigation menu with the following items: Vault, engines (highlighted), Access, Policies, Tools, Monitoring, Client count, and Seal Vault. The main content area is titled 'Engines' and features two search filters: 'Filter by engine type' and 'Filter by engine name'. Below the filters, two engine entries are listed:

- per-token private secret storage
- key/value secret storage

A yellow warning box is present in the bottom left corner with the following text:

**Warning**  
You have logged in with a root token. As a security precaution, this root token will not be stored by your browser and you will need to re-authenticate after the window is closed or refreshed.

The footer of the page includes the HashiCorp logo, '© 2023 HashiCorp Vault 1.14.0', and a 'Documentation' link.

# Secrets - GUI Demo (2)

The screenshot displays the Vault web interface for creating a secret. The left sidebar contains navigation links: Vault, Secrets engines (selected), Access, Policies, Tools, Monitoring, Client count, and Seal Vault. The main panel shows the 'Create secret' form with the following elements:

- Back navigation: [secret](#)
- Section: **Create secret**
- Field: [Redacted]
- Section: **Path for this secret**
- Field: [Redacted]
- Section: **Secret data**
- Key:
- Value: [Redacted]
- Expandable section: [Show secret metadata](#)
- Action:

At the bottom of the page, there is a blacked-out area, a link to [Upgrade to Vault Enterprise](#), and a link to [Documentation](#).

# Secrets - GUI Demo (3)

The screenshot shows the Vault web interface. The left sidebar contains navigation options: Vault, Secrets engines (selected), Access, Policies, Tools, Monitoring, Client count, and Seal Vault. The main content area shows the breadcrumb path < secret < my-first-secret. Below this, there are two tabs: Secret and Metadata (selected). A redacted area is visible above the tabs. The Metadata tab contains an 'Edit metadata >' button. Below this is a section titled 'Custom metadata' with a redacted area and a text block: 'This data is version-agnostic and is usually used to describe the secret being stored.' Below the text is an 'Add metadata' link. At the bottom, there are three rows of metadata settings: 'Maximum versions' set to 0, 'Check-and-Set required' set to No (checked), and 'Delete version after' set to Never delete.

< secret < my-first-secret

Secret Metadata

Edit metadata >

Custom metadata

This data is version-agnostic and is usually used to describe the secret being stored.

Add metadata

Maximum versions 0

Check-and-Set required  No

Delete version after Never delete

```
kv -help
```

```
Usage: vault [options]
```

```
(...)
```

```
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 - [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
```





# 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]
```

```
$ 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
```

```
$ 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 =====
```

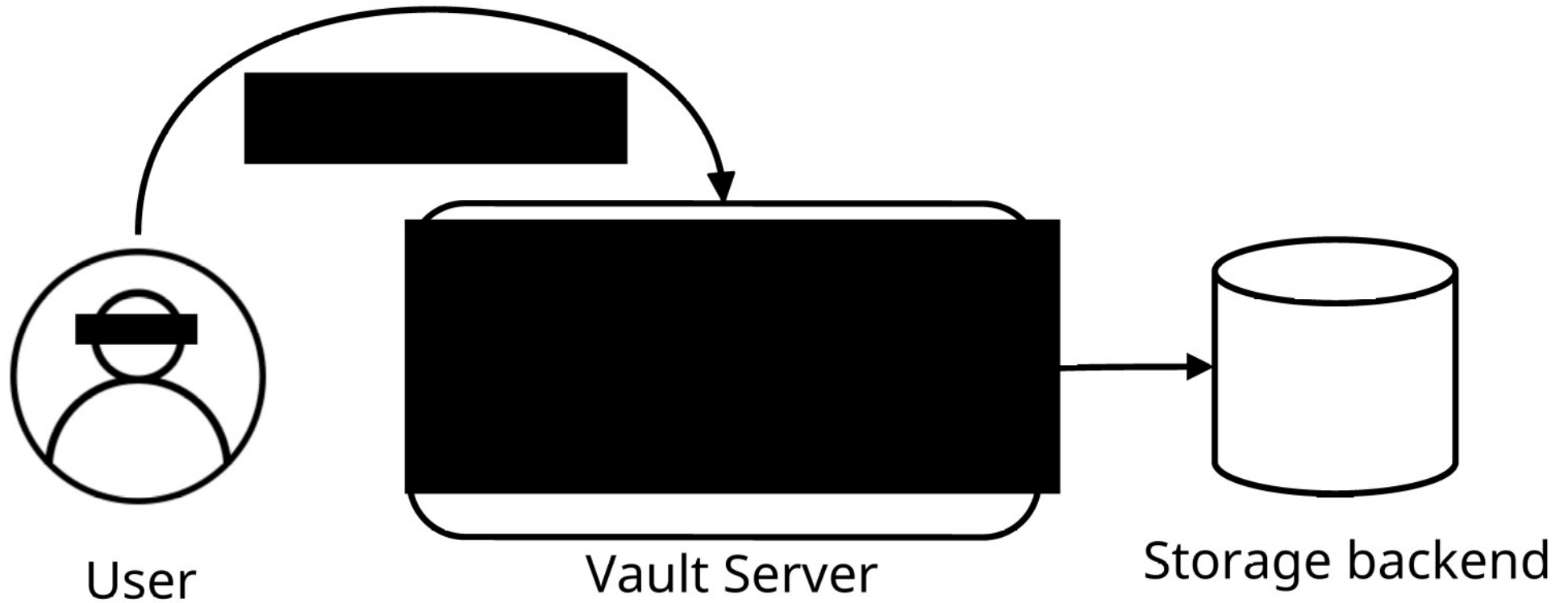
Key	Value
---	-----
[REDACTED]	[REDACTED]

# Secrets – [REDACTED]

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

# Secrets – Secrets Engines (1)

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



# 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]
<b>disable</b>	[REDACTED] All secrets are revoked. [REDACTED]
[REDACTED]	Moves the path for an existing secrets engine. Think of this like rename.
<b>tune</b>	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]
```

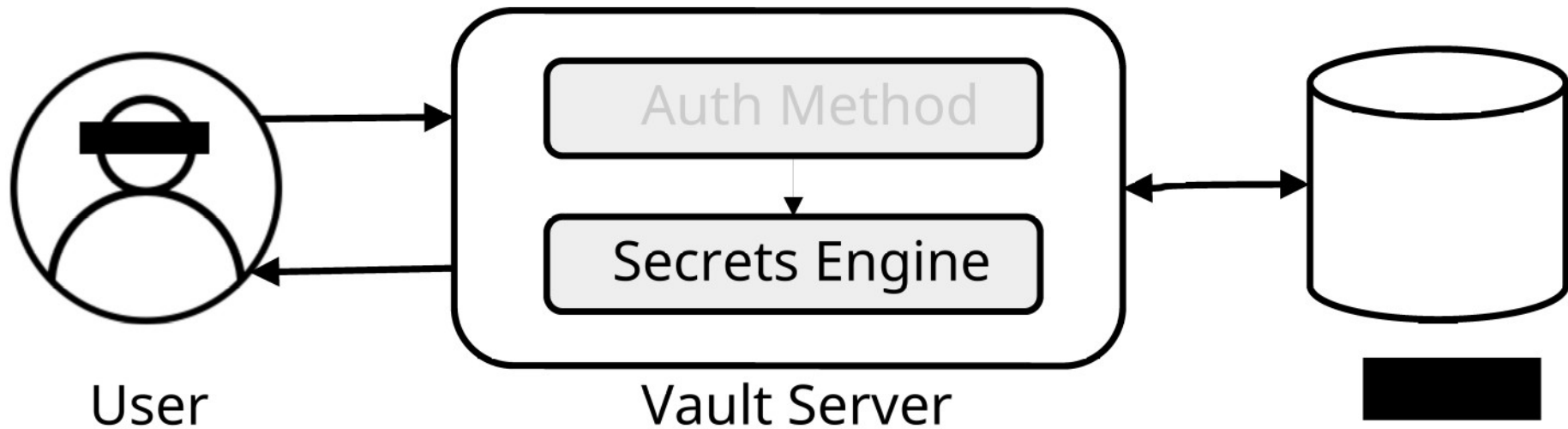
- Generic [REDACTED]
  - [REDACTED] (key)
  - Corresponding data (value)
  - [REDACTED] names must be [REDACTED]
  - Values [REDACTED] binary data
    - [REDACTED] (long string)
- Two modes
  - Non-versioned [REDACTED]
  - [REDACTED] (kv-v2)

# Secrets – Secrets Engine - [REDACTED]

- [REDACTED] written value [REDACTED]
- Kv-v2: [REDACTED]
  - Metadata and data of older [REDACTED]
- [REDACTED] is default
  - To enable [REDACTED]
    - [REDACTED]
    - kv-v2 in stead [REDACTED]
- Kv-v1 can [REDACTED]
  - Not the other way round
  - **vault** [REDACTED] <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.
<b>revoke</b> [REDACTED]	When a lease is revoked, [REDACTED] invalidated and prevents further renewals.
[REDACTED] <b>fix</b>	Revokes [REDACTED] path (e.g. <b>revoke -prefix azure/creds/developer</b> )

# Secrets – Dynamic Secrets - [REDACTED]

---





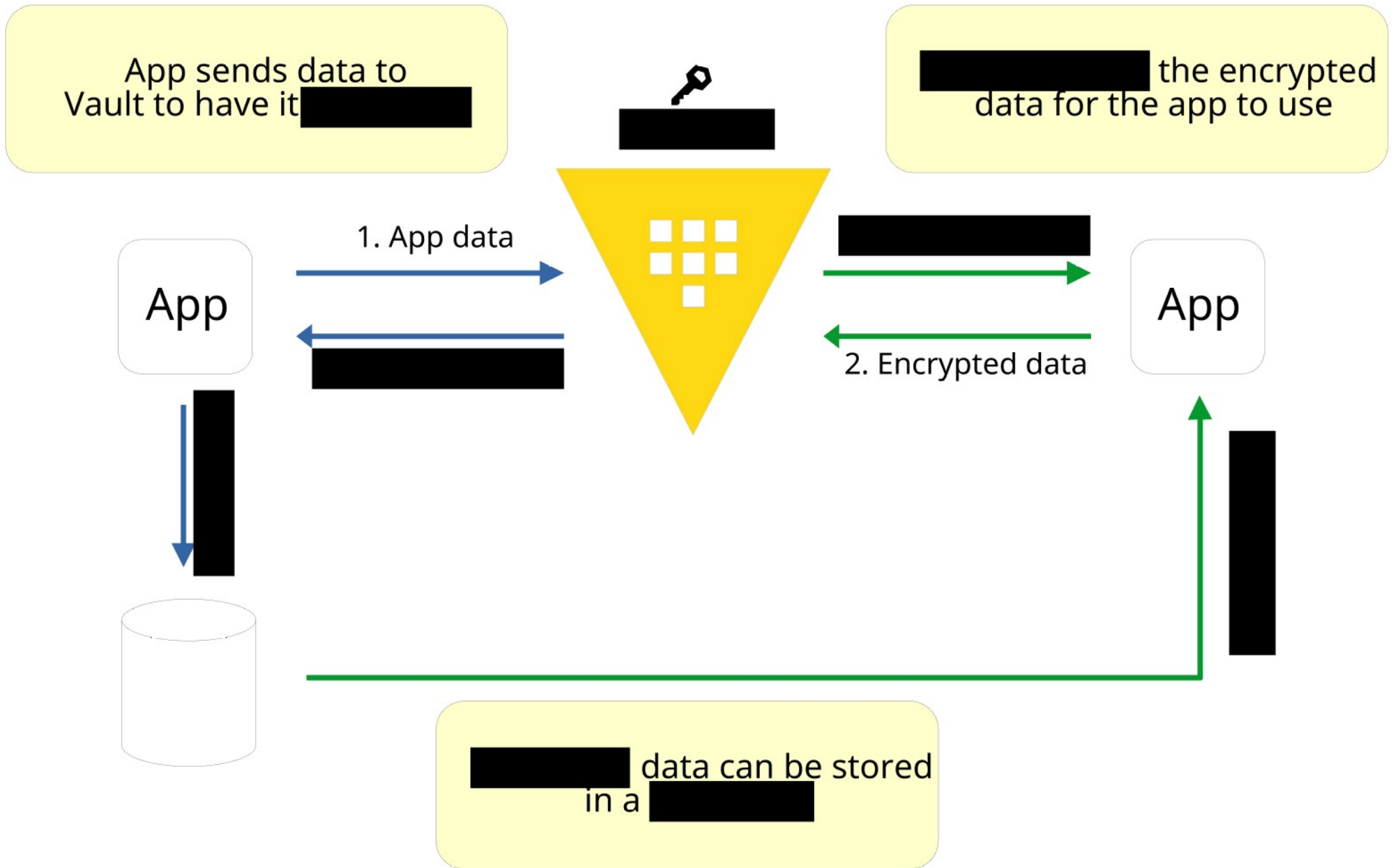
# Secrets – Secrets [REDACTED] Generic

- 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 in [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)

```
$ ██████████ transit/keys/keyname
```

```
Success! Data written to: transit/keys/keyname
```

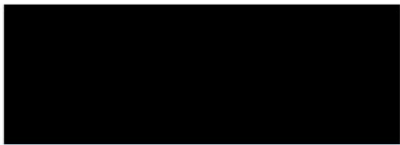
```
$ vault write ██████████ \
  plaintext=$██████████ base64)
```

```
Key          Value
---          -
ciphertext   vault:v1:dJmop+WmCk19Fw1E4n6cv6+ExfefdB83p6(....)
██████████
```

```
$ ██████████ decrypt/keyname \
  ciphertext=vault:v1:██████████+ExfefdB83p6(...)
```

```
Key          Value
---          -
plaintext    ██████████
```

```
$ ██████████ --decode <<< ██████████
Encrypt this text
```



# Secrets Engine – Transit (3)

---



# 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]



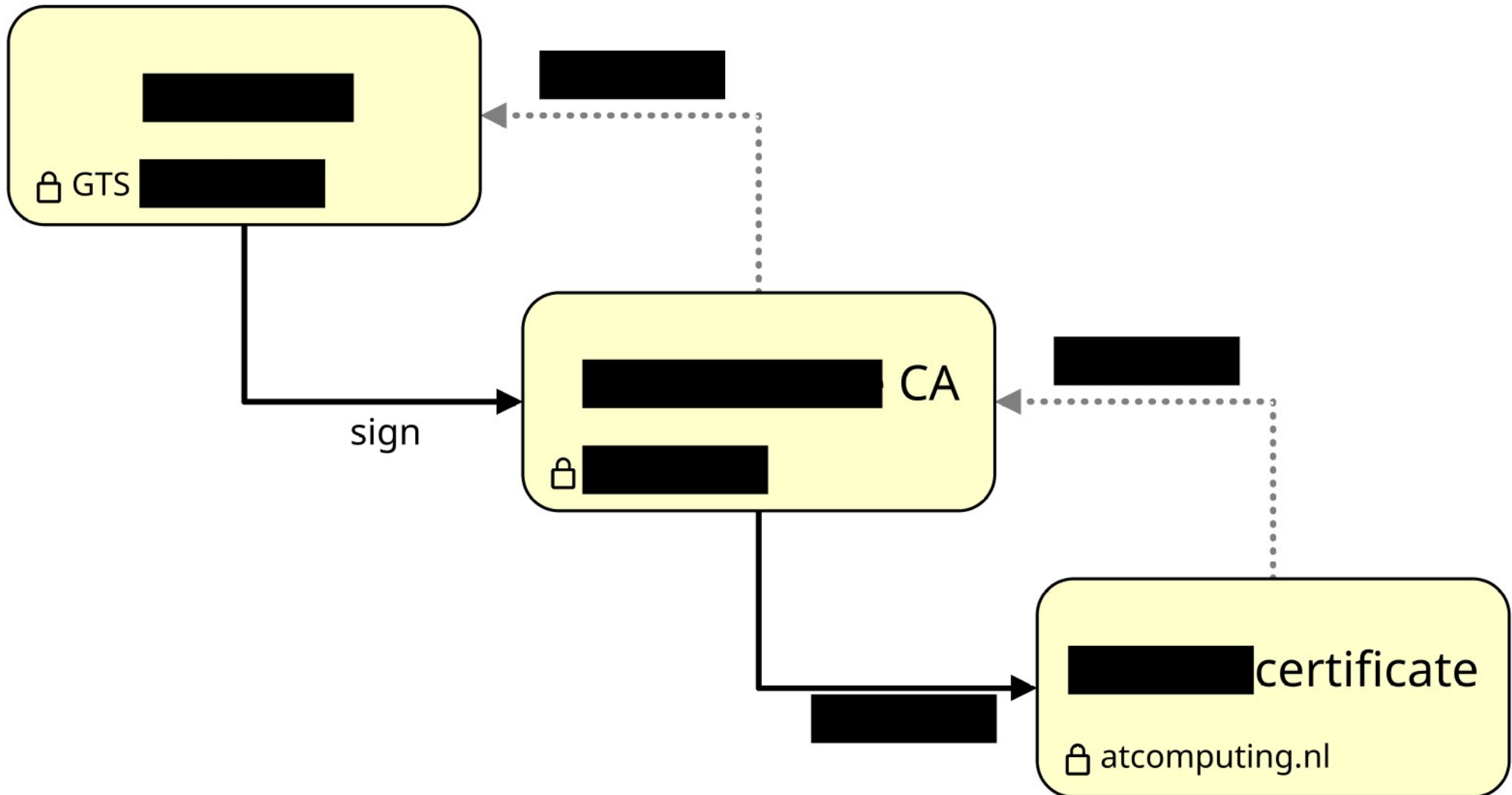
## Traditional

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

## Vault process

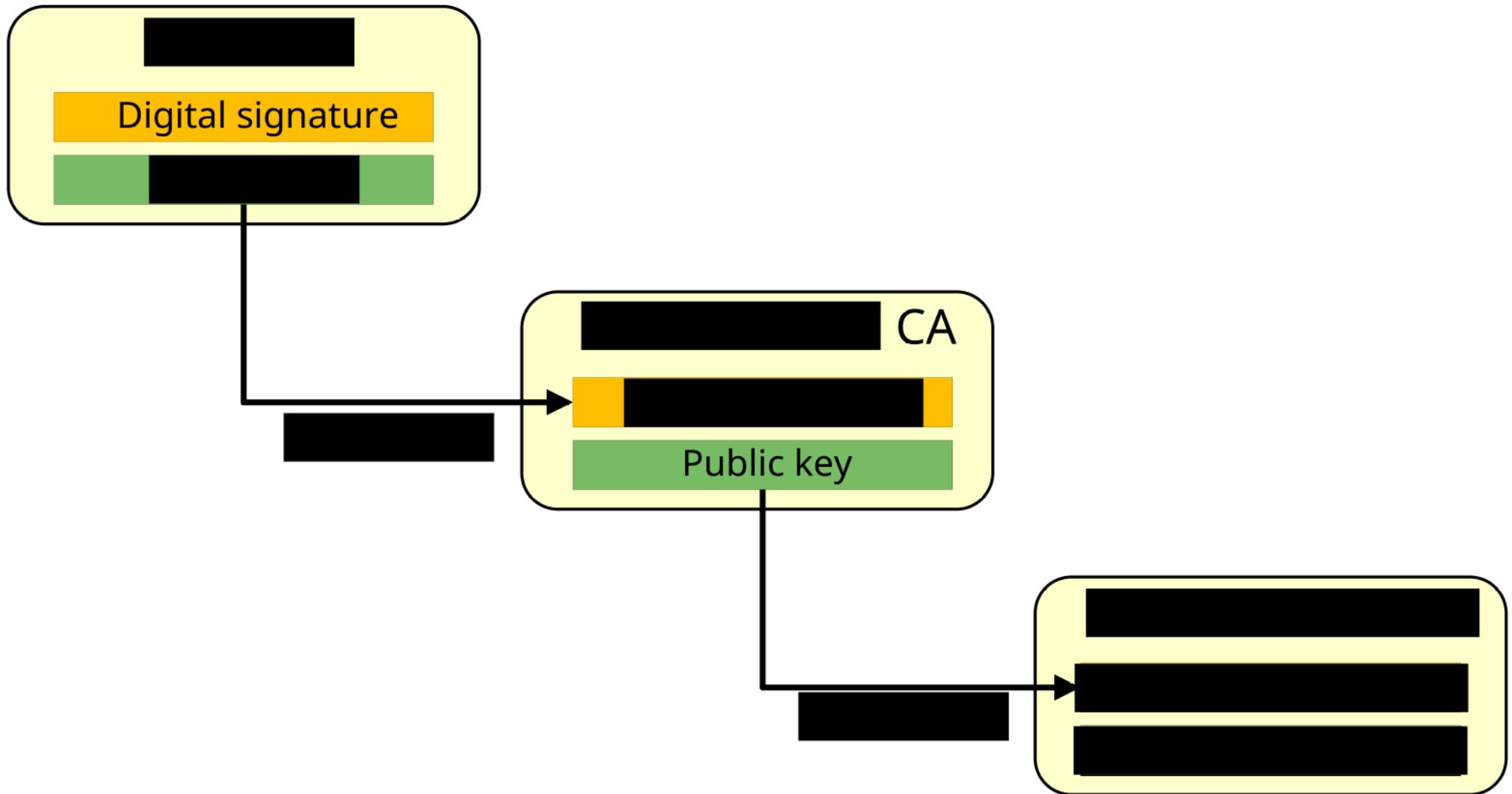
- "common name"
- Certificate, private generated

## Certificate chain ██████████

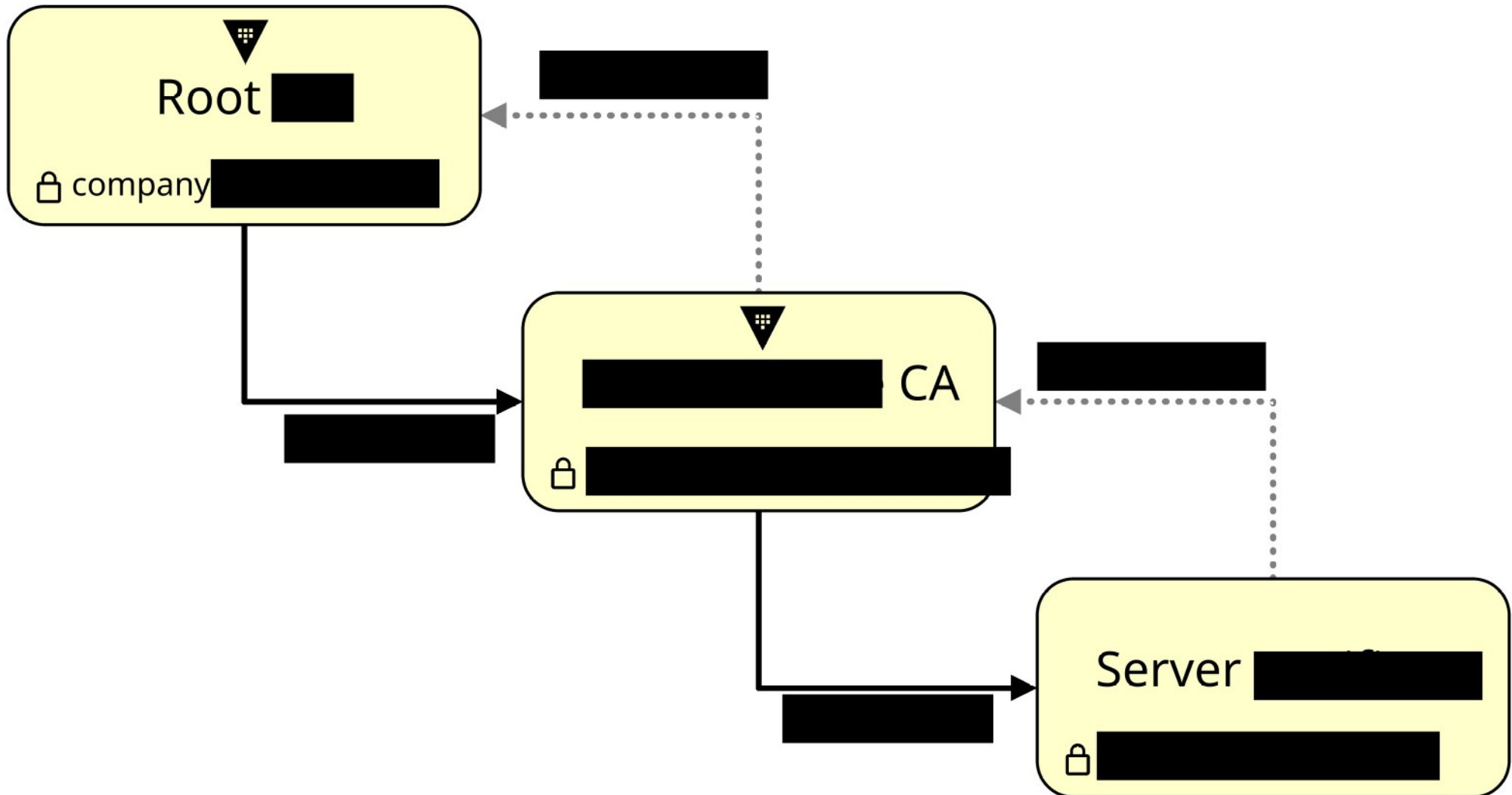


# Secrets - [REDACTED]

[REDACTED] example



Certificate Vault



# Secrets – Secrets Engine – [REDACTED]

---



Root CA



# 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]  
[REDACTED] hvs.[REDACTED]JMp0RsRRnLc0cDc  
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]	[REDACTED]
token_accessor	hvs.[REDACTED]JbEyQQEeA
token_duration	1m
[REDACTED]	[REDACTED]
token_policies	["default"]
identity_policies	["default"]
policies	["default"]
[REDACTED]	[REDACTED]

```
$ vault read [REDACTED]  
[REDACTED]tempsecret
```