DevOops 2023

Как мы захотели автоматизировать Vault CE и во что его в итоге превратили

Mikhail Pakhomov

kaspersky

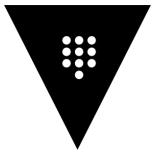
Intro

- 4 года в IT
- ИБ специалист
- Python и Golang
- DevOps в Kaspersky Lab

С чего все началось

Один девопс

Один девопс



HashiCorp Vault

Один девопс

kvv2/

kv_eeae3db7

Secrets Engine

Один девопс

secrets kvv2

kvv2 Version 2

Secrets Configuration

Filter secrets

first_service

root_token_on_vault

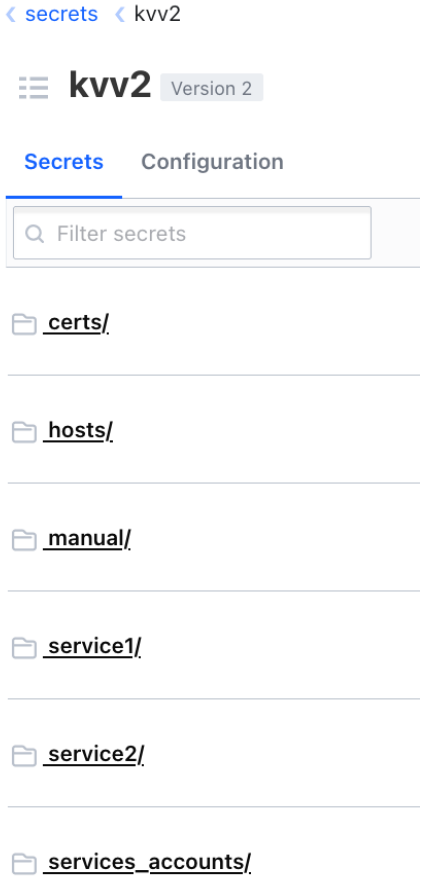
test/

Много девопсов

Один разработчик

Много девопсов

Один разработчик



Много девопсов

Много разработчиков

Какие-то менеджеры

Кто-то еще

Много девопсов

Много разработчиков

Какие-то менеджеры

Кто-то еще

Аутентификация

Много девопсов

Много разработчиков

Какие-то менеджеры

Кто-то еще

Аутентификация

Спейсы

Много девопсов

Много разработчиков

Какие-то менеджеры

Кто-то еще

Аутентификация

Спейсы

Автоматизация

Много девопсов

Много разработчиков

Какие-то менеджеры

Кто-то еще

Аутентификация

Спейсы

Автоматизация

Безопасность

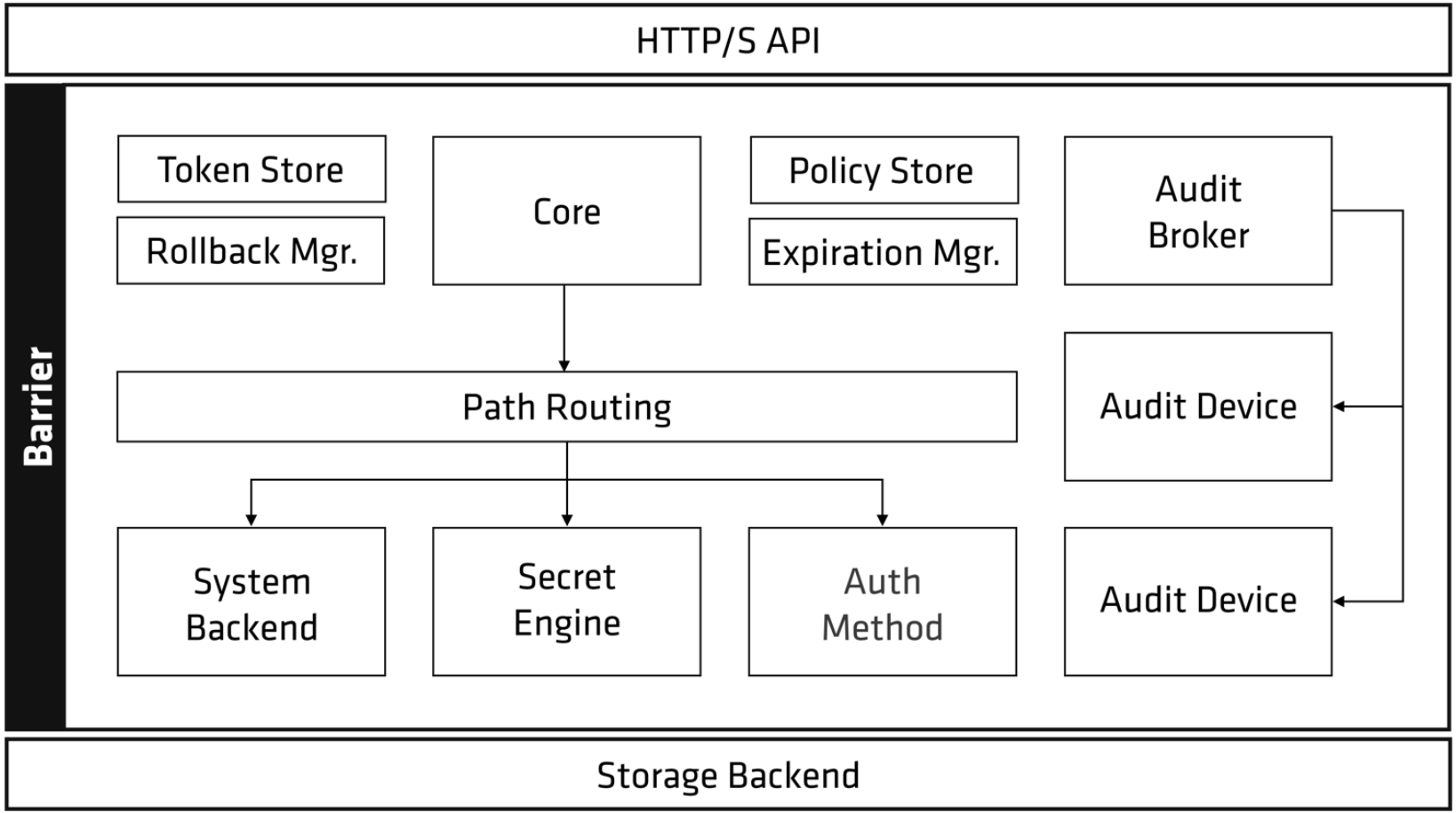
Требования

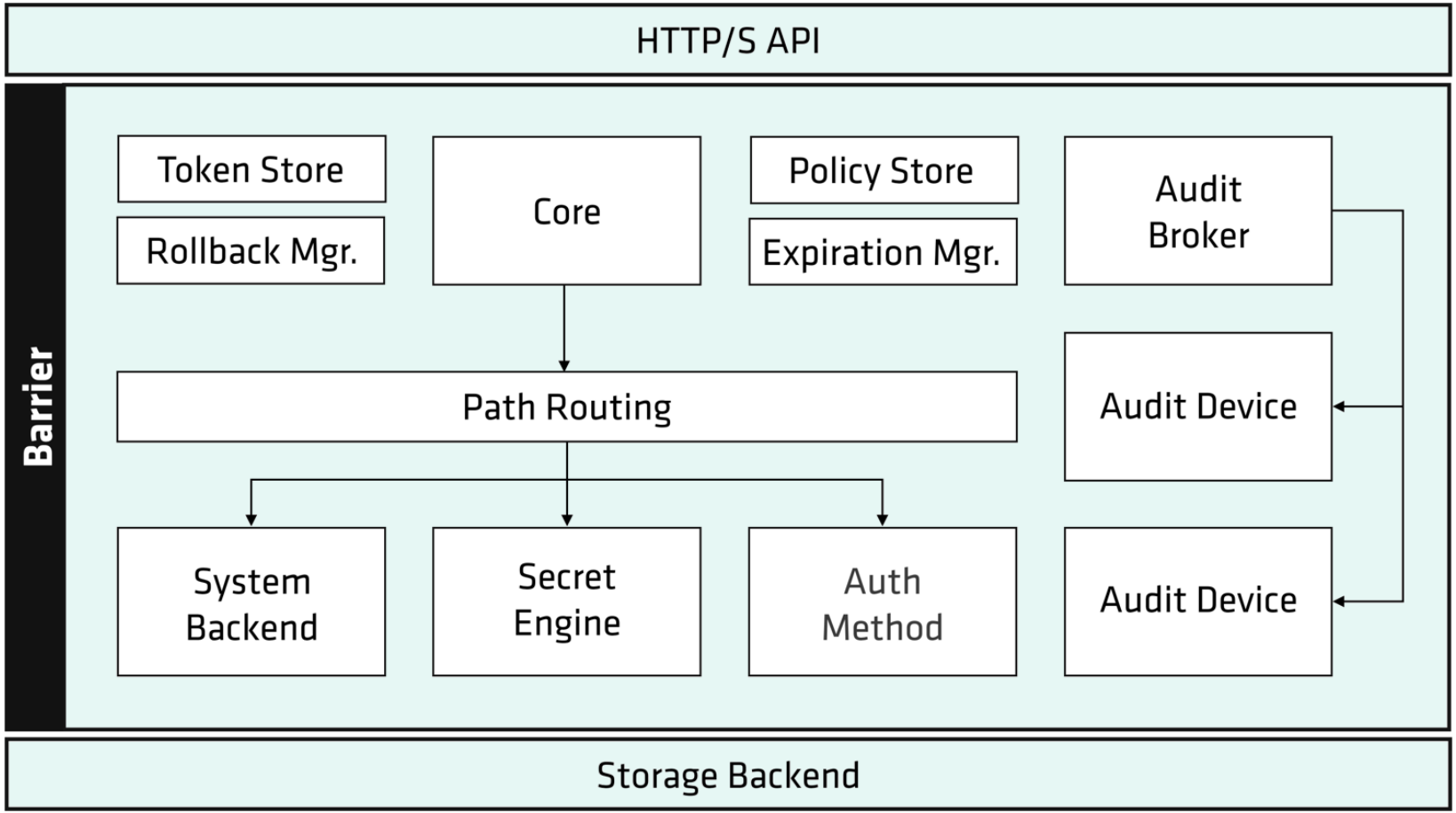
Единый защищенный сервис

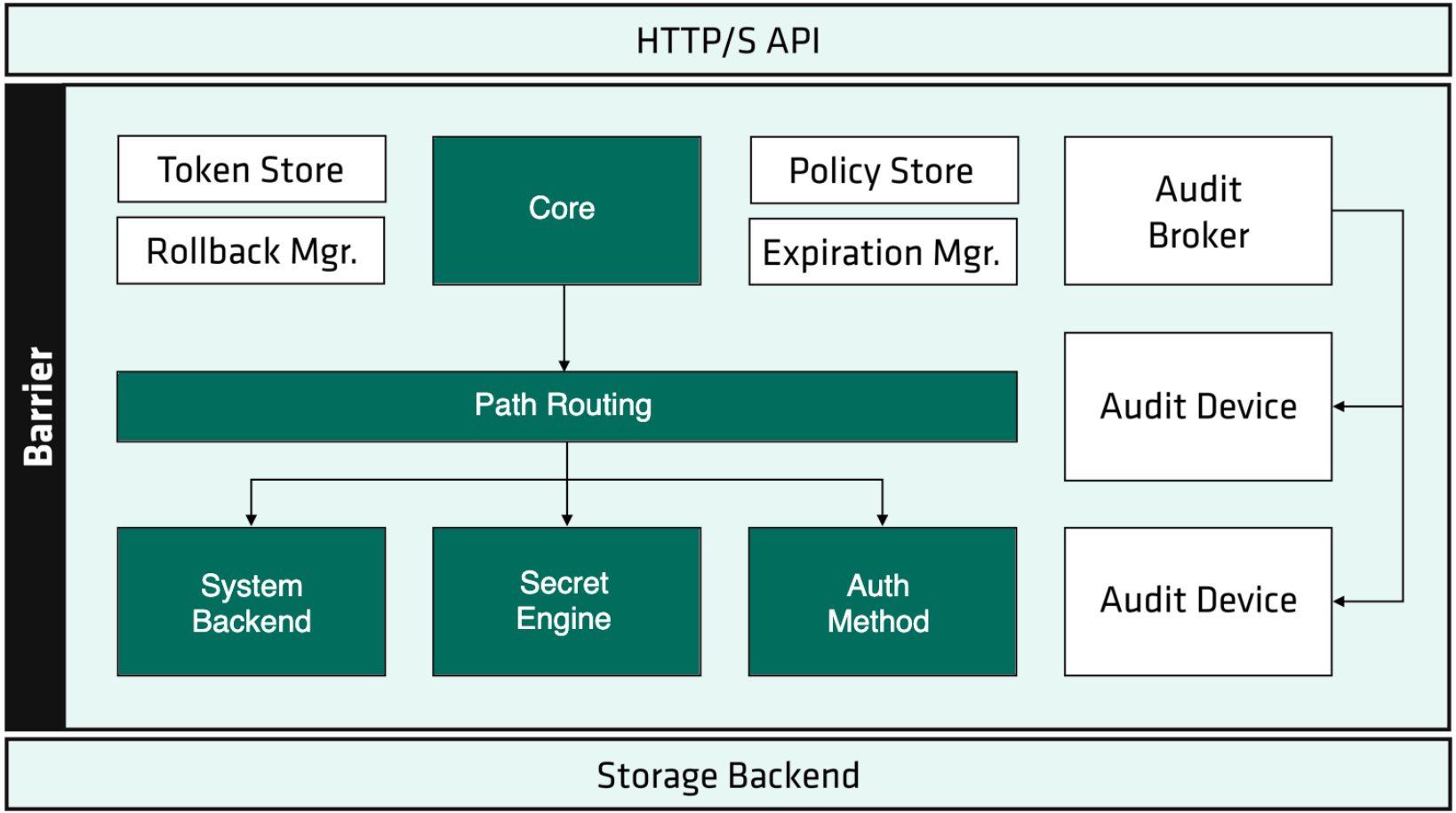
Делегирование доступов по спейсам

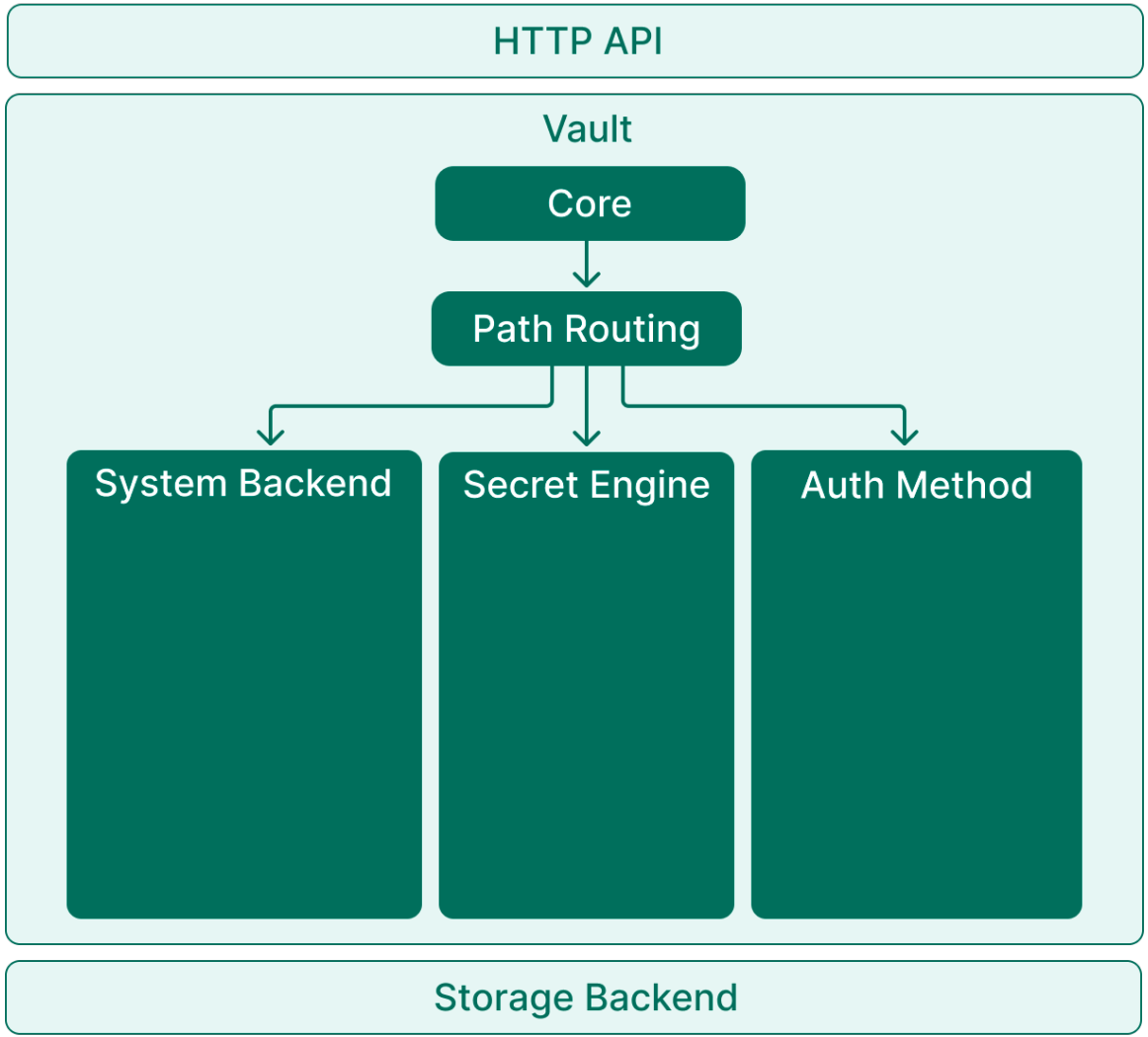
Удобный интерфейс аутентификации

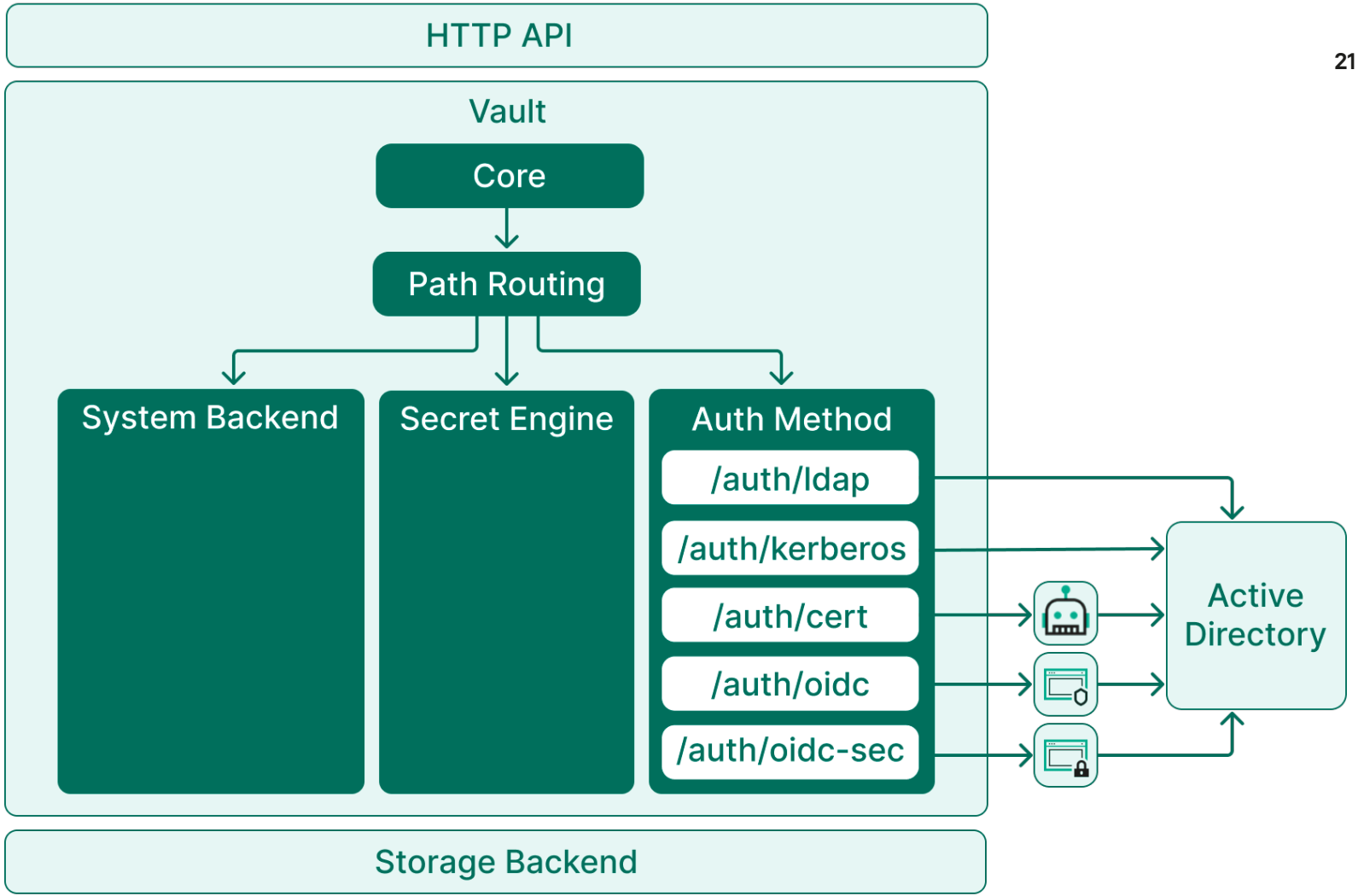
Как организовали доступ

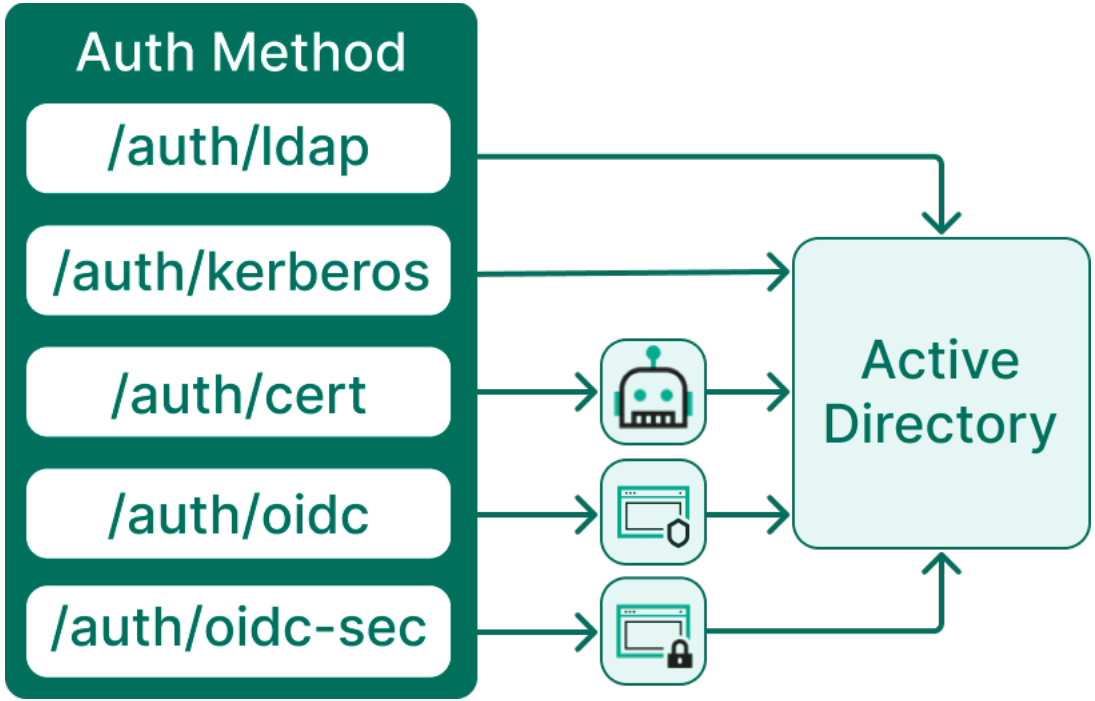

HTTP/S API
Barrier
Token Store
Rollback Mgr.
Core
Policy Store
Expiration Mgr.
Audit Broker
Path Routing
Audit Device
System Backend
Secret Engine
Auth Method
Audit Device
Storage Backend

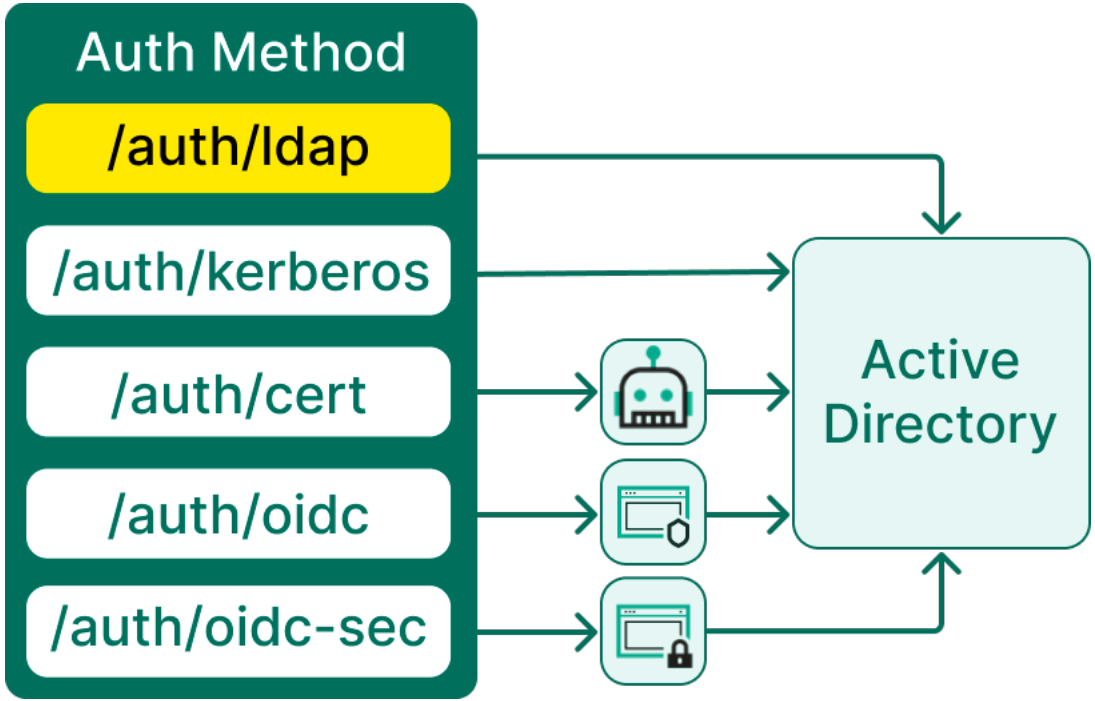

HTTP/S API
Barrier
Token Store
Rollback Mgr.
Core
Policy Store
Expiration Mgr.
Audit Broker
Path Routing
Audit Device
System Backend
Secret Engine
Auth Method
Audit Device
Storage Backend

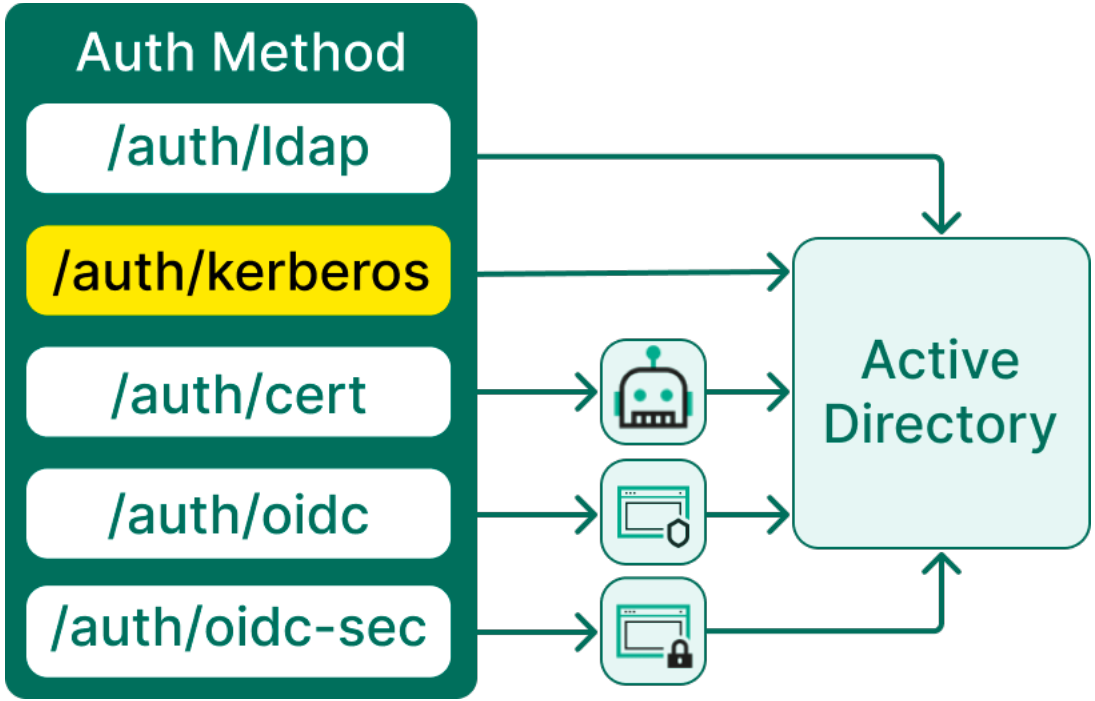

HTTP/S API
Barrier
Token Store
Rollback Mgr.
Core
Policy Store
Expiration Mgr.
Audit Broker
Path Routing
Audit Device
System Backend
Secret Engine
Auth Method
Audit Device
Storage Backend

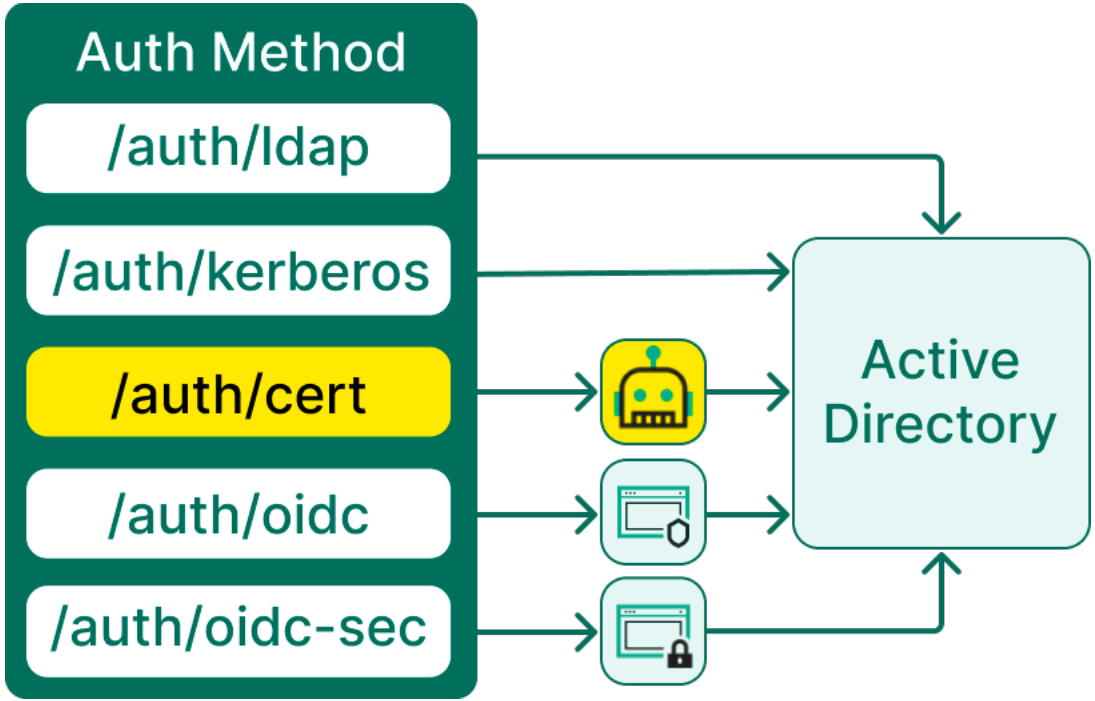

HTTP API
Vault
Core
Path Routing
System Backend
Secret Engine
Auth Method
Storage Backend


HTTP API
Vault
Core
Path Routing
System Backend
Secret Engine
Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory
Storage Backend

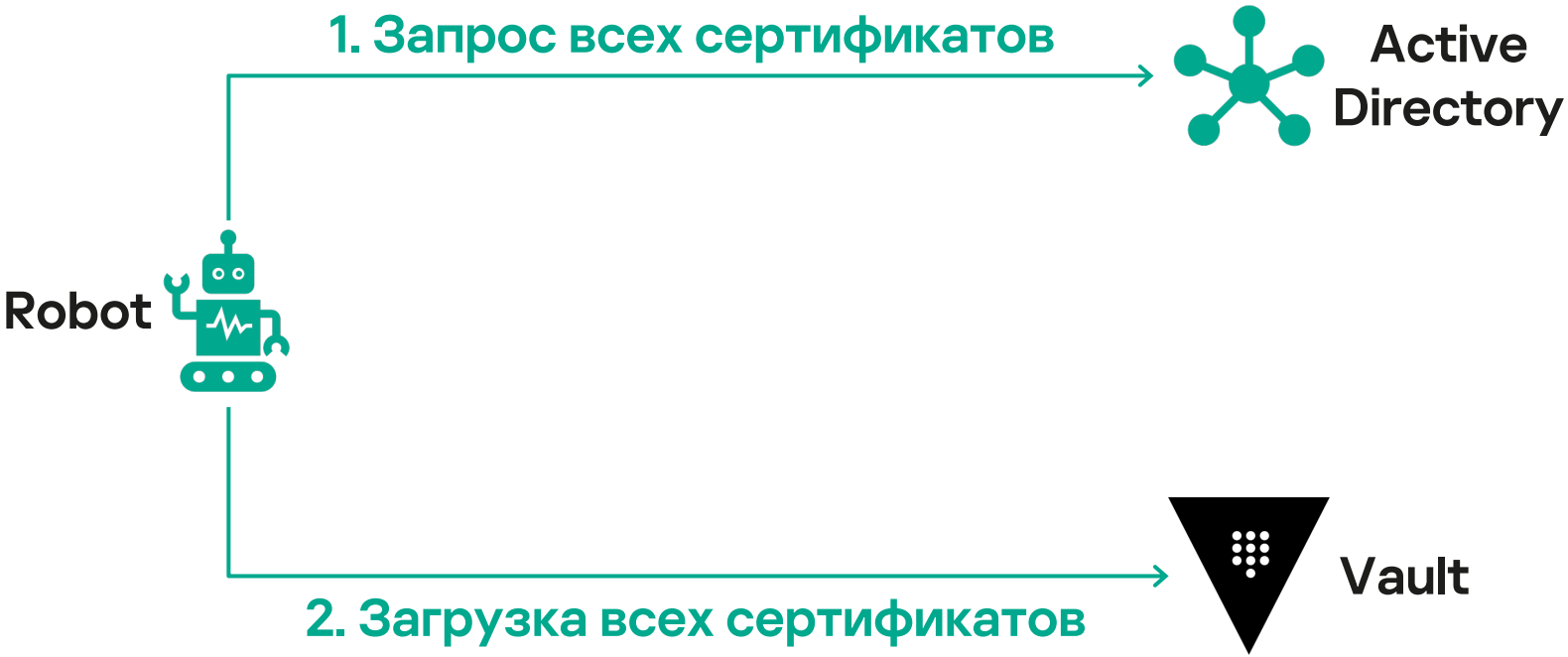

Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory


Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory


Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory


Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory

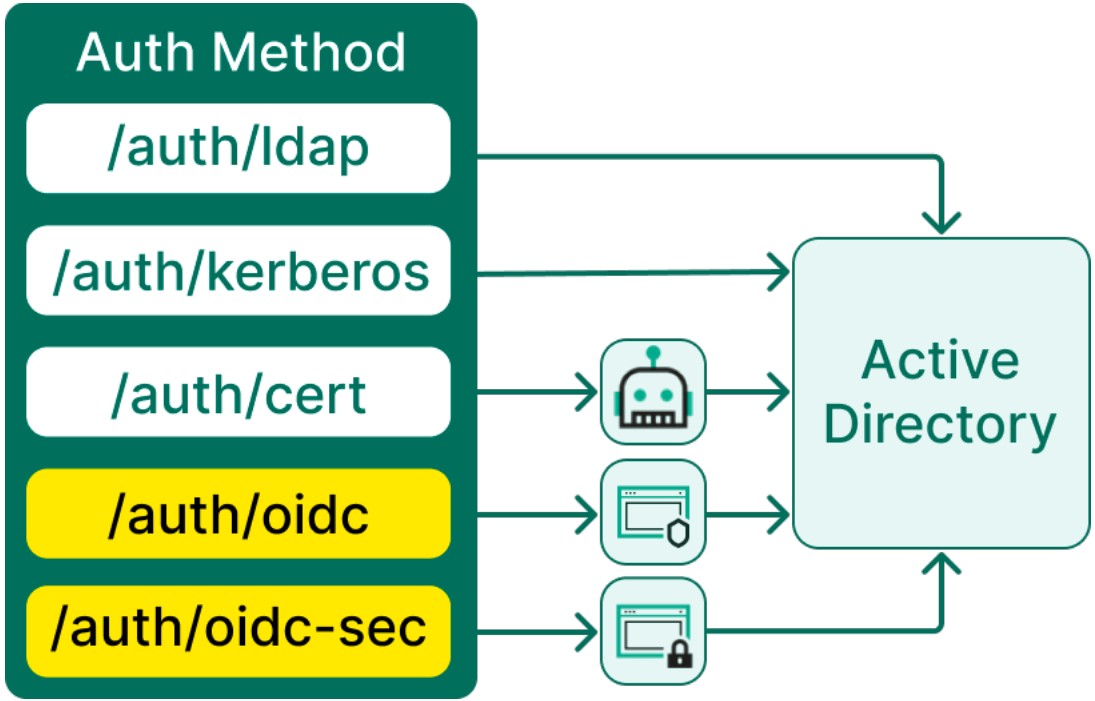
TLS Certs


1. Запрос всех сертификатов
Active Directory
Robot
2. Загрузка всех сертификатов
Vault

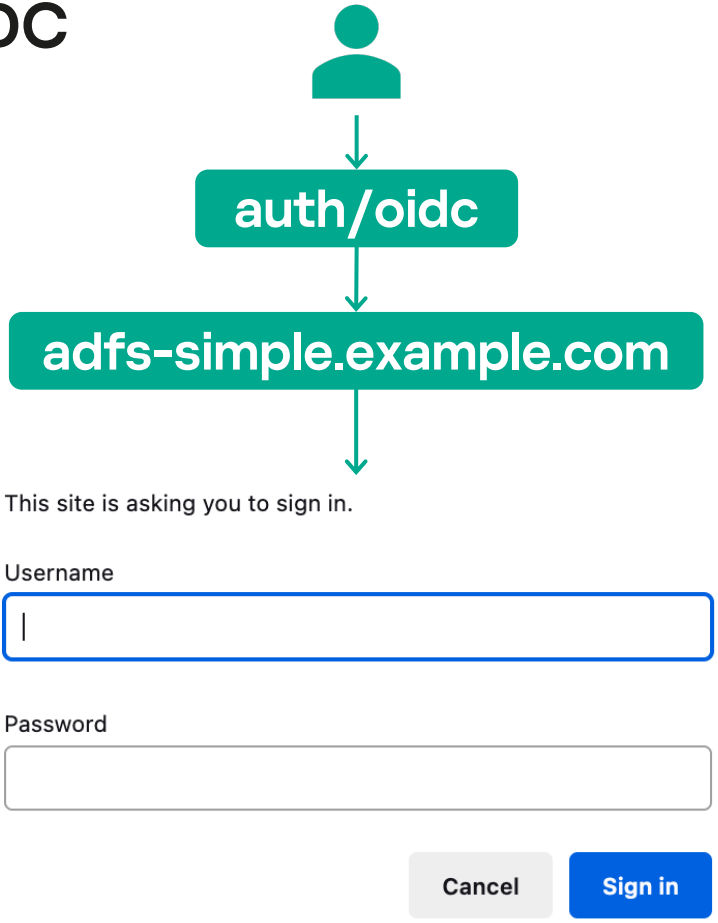
TLS Certs


```
$ vault list auth/cert/certs
Ivanov_I0

$ vault read auth/cert/certs/Ivanov_I0
certificate   -----BEGIN CERTIFICATE-----
              This is Ivan's public certificate
              -----END CERTIFICATE-----
```


Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory

OIDC

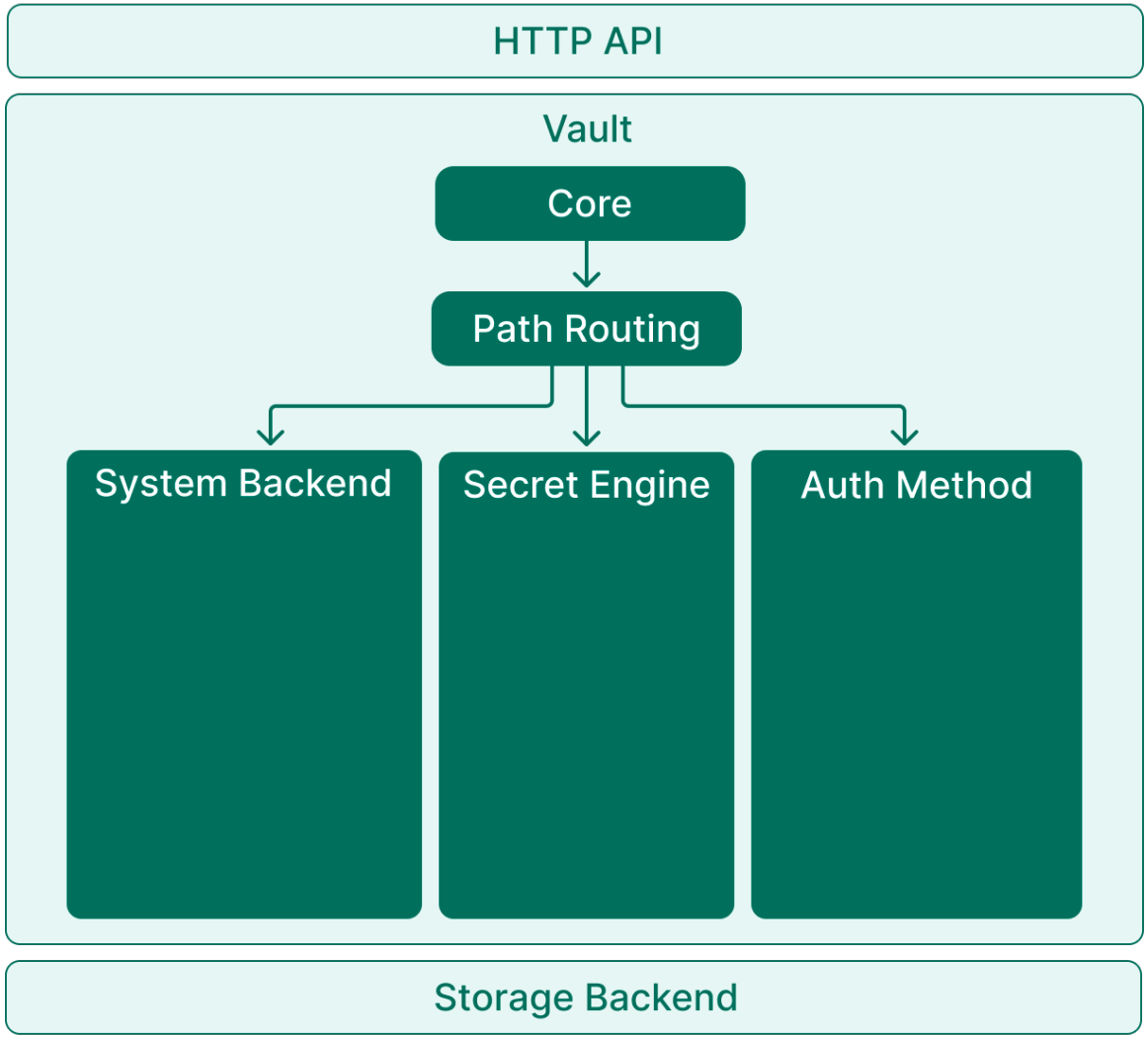

auth/oidc
adfs-simple.example.com
This site is asking you to sign in.
Username
Password
Cancel
Sign in

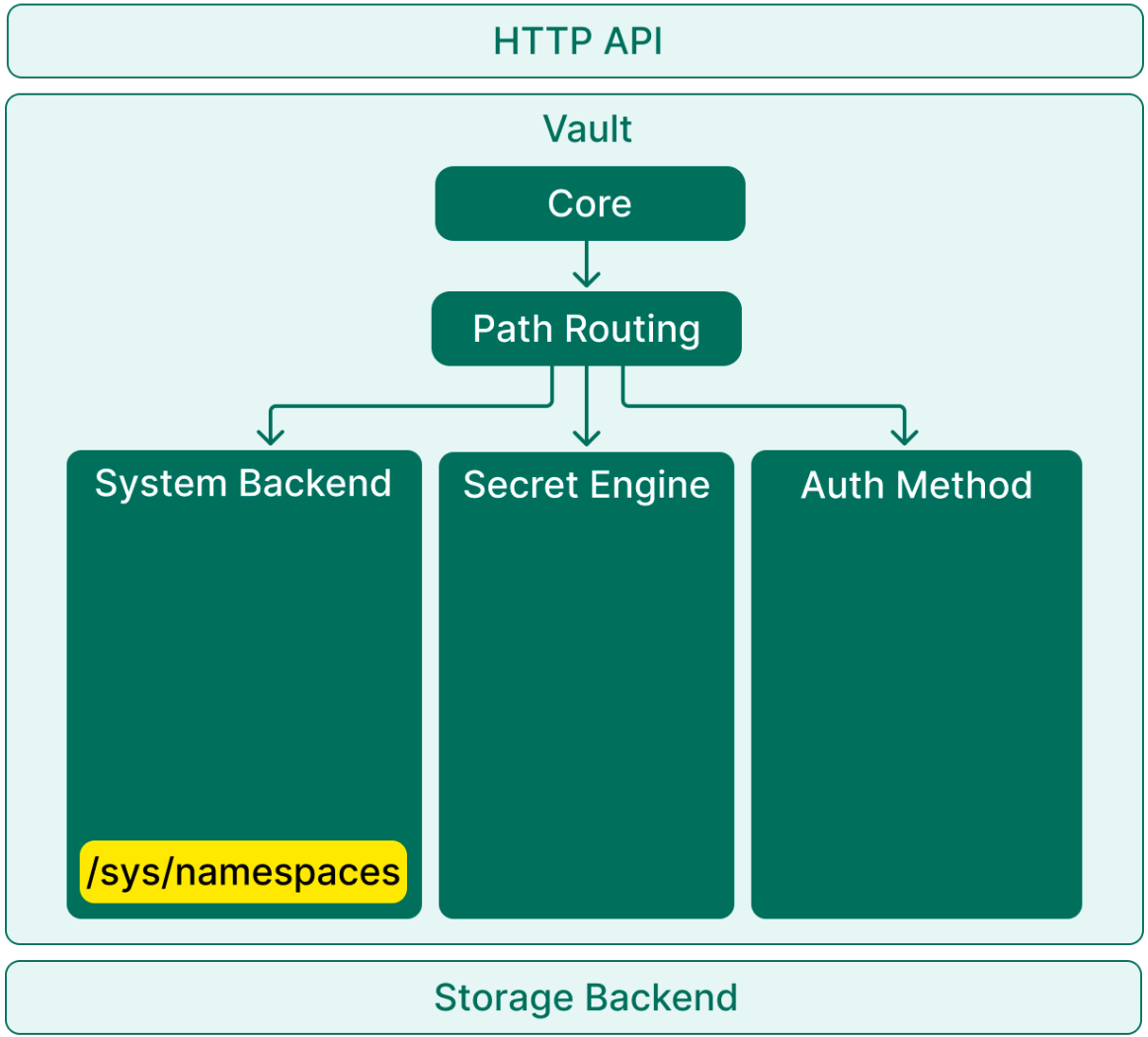

auth/oidc-sec
adfs-secure.example.com
This site has requested that you identify yourself with a certificate:
Organization: “AO Kaspersky Lab”
Issued Under: “Kaspersky”
Choose a certificate to present as identification:
Details of selected certificate:
Remember this decision
Cancel
OK

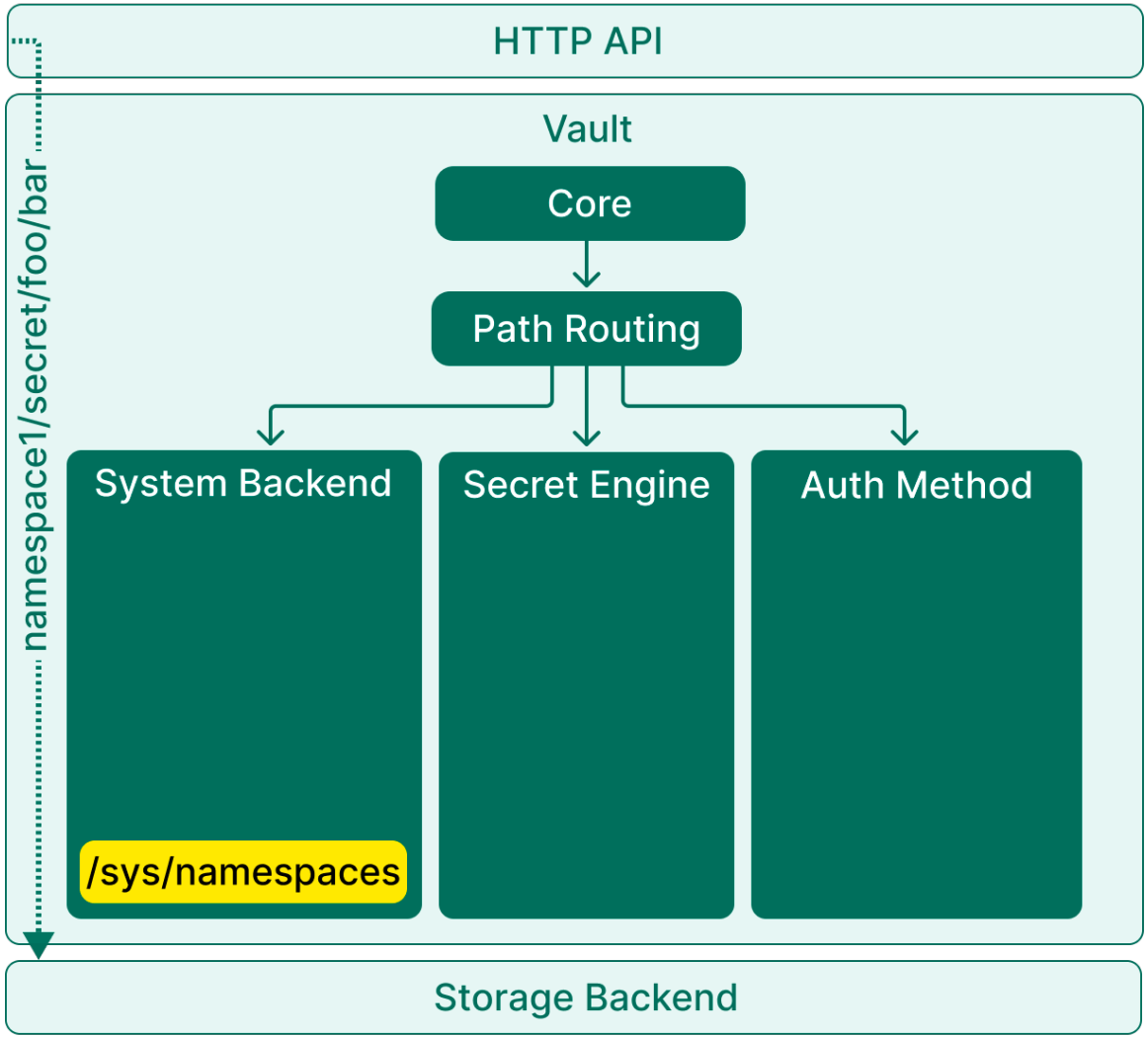
С чего все началось

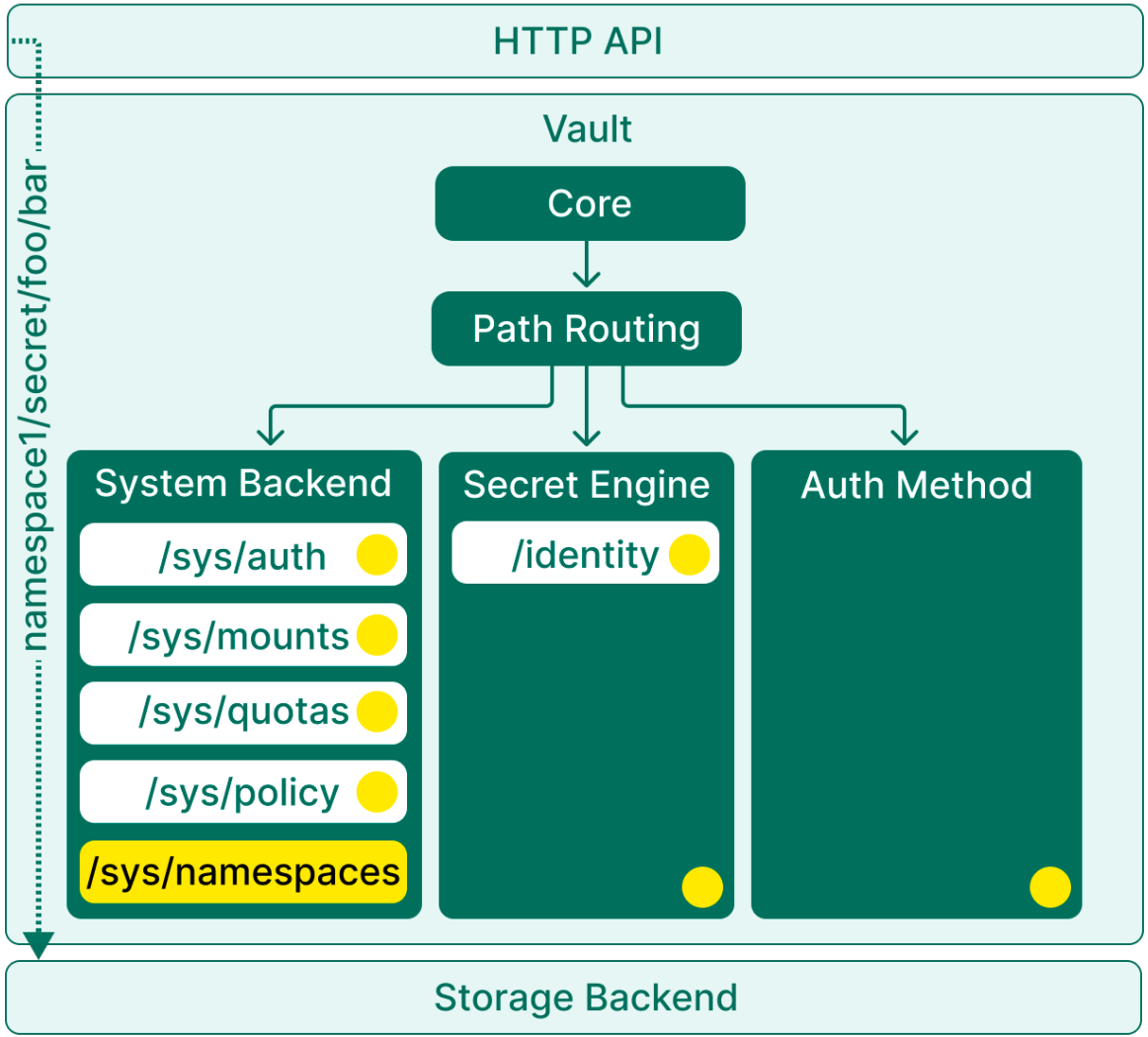
Как организовали доступ

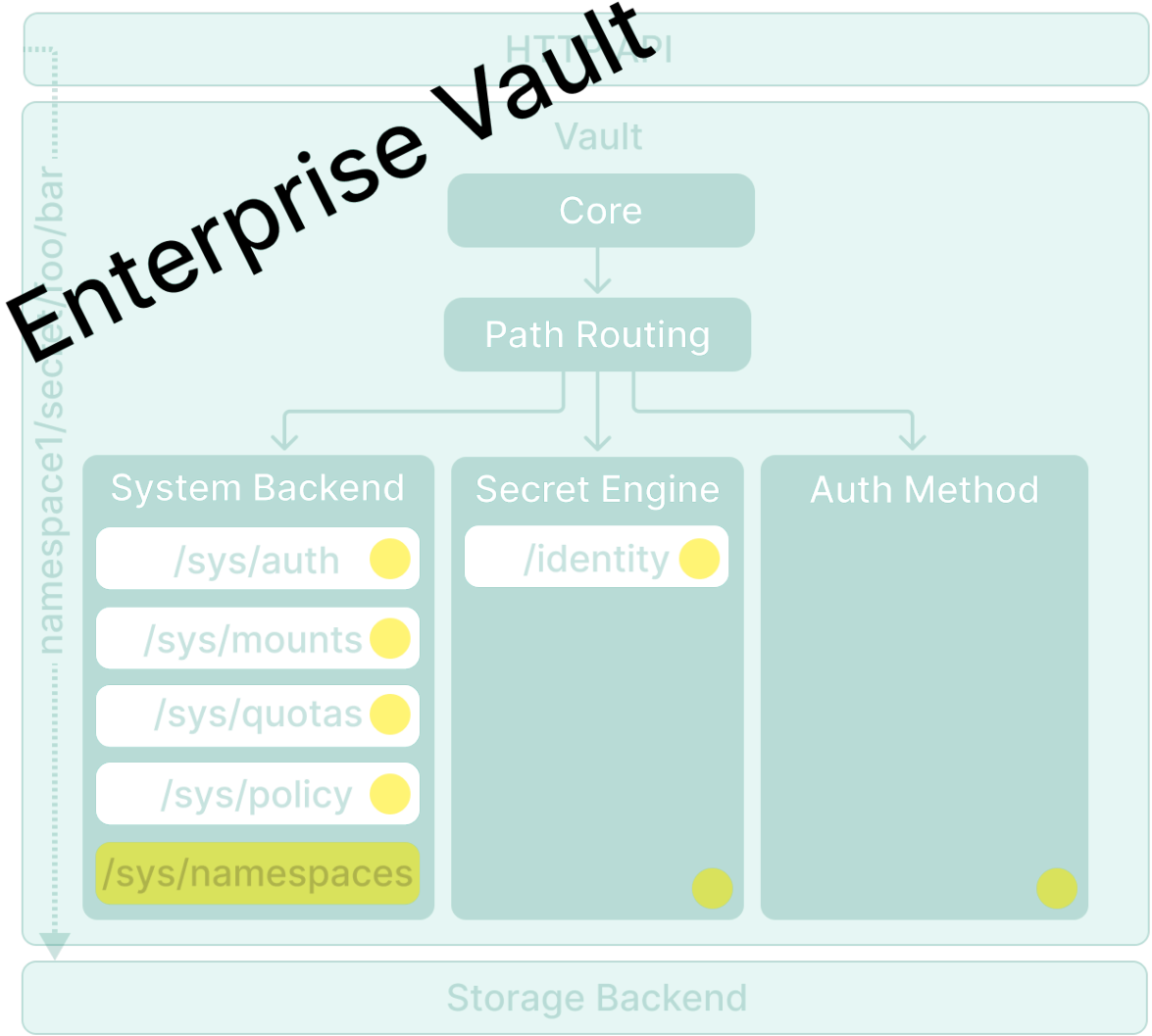
Как сделали свои спейсы


HTTP API
Vault
Core
Path Routing
System Backend
Secret Engine
Auth Method
Storage Backend


HTTP API
Vault
Core
Path Routing
System Backend
/sys/namespaces
Secret Engine
Auth Method
Storage Backend


HTTP API
Vault
Core
Path Routing
System Backend
/sys/namespaces
Secret Engine
Auth Method
namespace1/secret/foo/bar
Storage Backend


HTTP API
Vault
Core
Path Routing
System Backend
/sys/auth
/sys/mounts
/sys/quotas
/sys/policy
/sys/namespaces
Secret Engine
/identity
Auth Method
namespace1/secret/foo/bar
Storage Backend


Enterprise Vault
HTTP API
Vault
Core
Path Routing
namespace1/secret/foo/bar
System Backend
/sys/auth
/sys/mounts
/sys/quotas
/sys/policy
/sys/namespaces
Secret Engine
/identity
Auth Method
Storage Backend

Спейс

ast_common/

`kv_8ffb2f6f`

auto-generated (via SysC plugin) backend for "ast" team

ast_pki/

`pki_24ec9303`

auto-generated (via SysC plugin) backend for "ast" team

ast_ssh/

`ssh_ee626ef3`

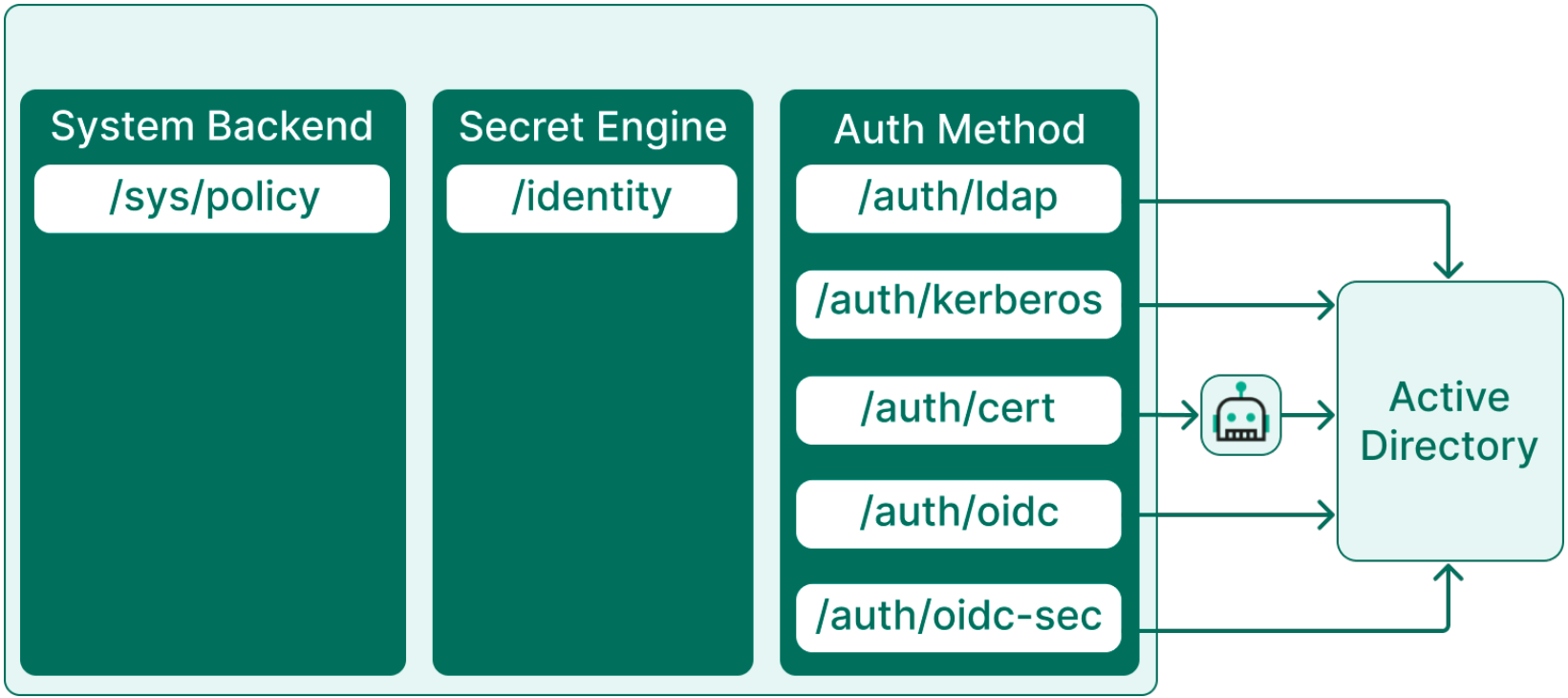
auto-generated (via SysC plugin) backend for "ast" team

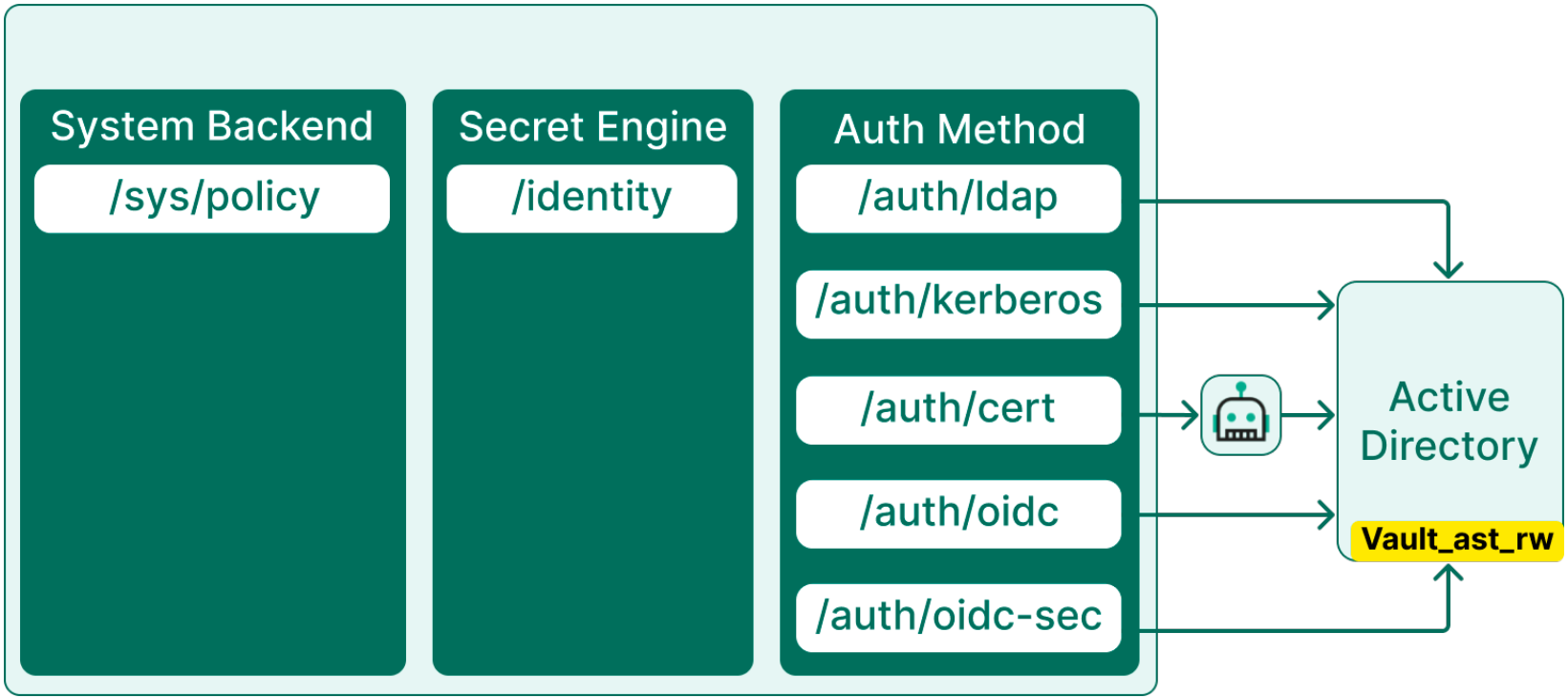
AST – Advanced Security Team

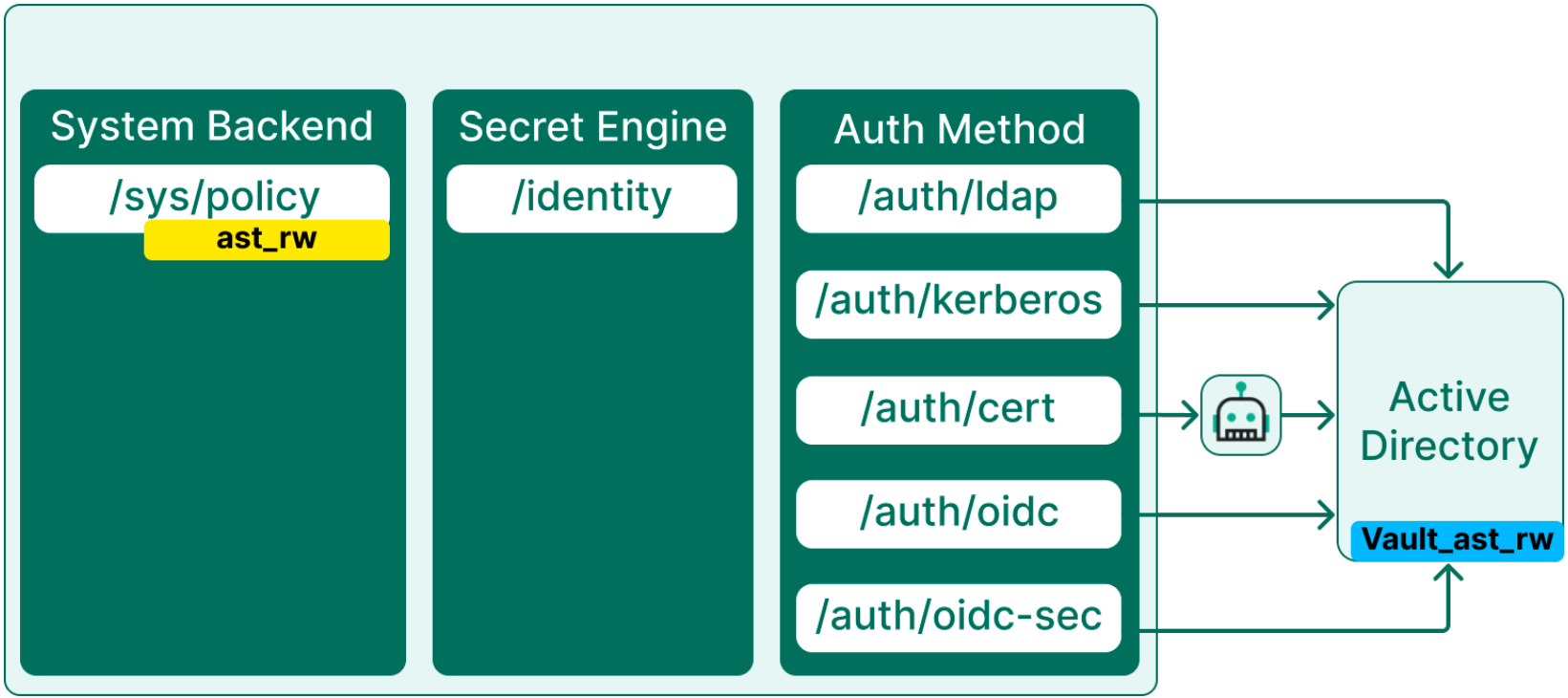
Политика для спейса (ast_rw)

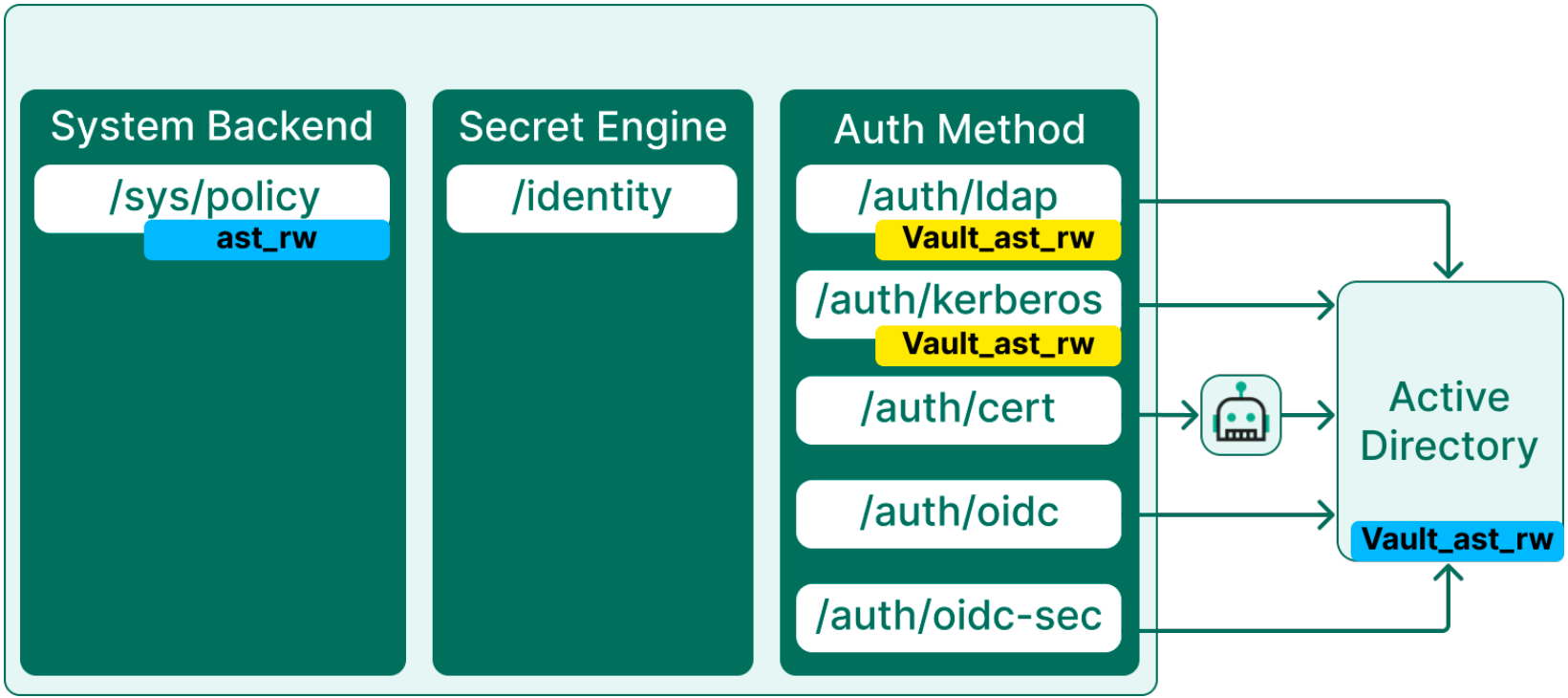

```
path "ast_*" {
    capabilities = [...]
}
```

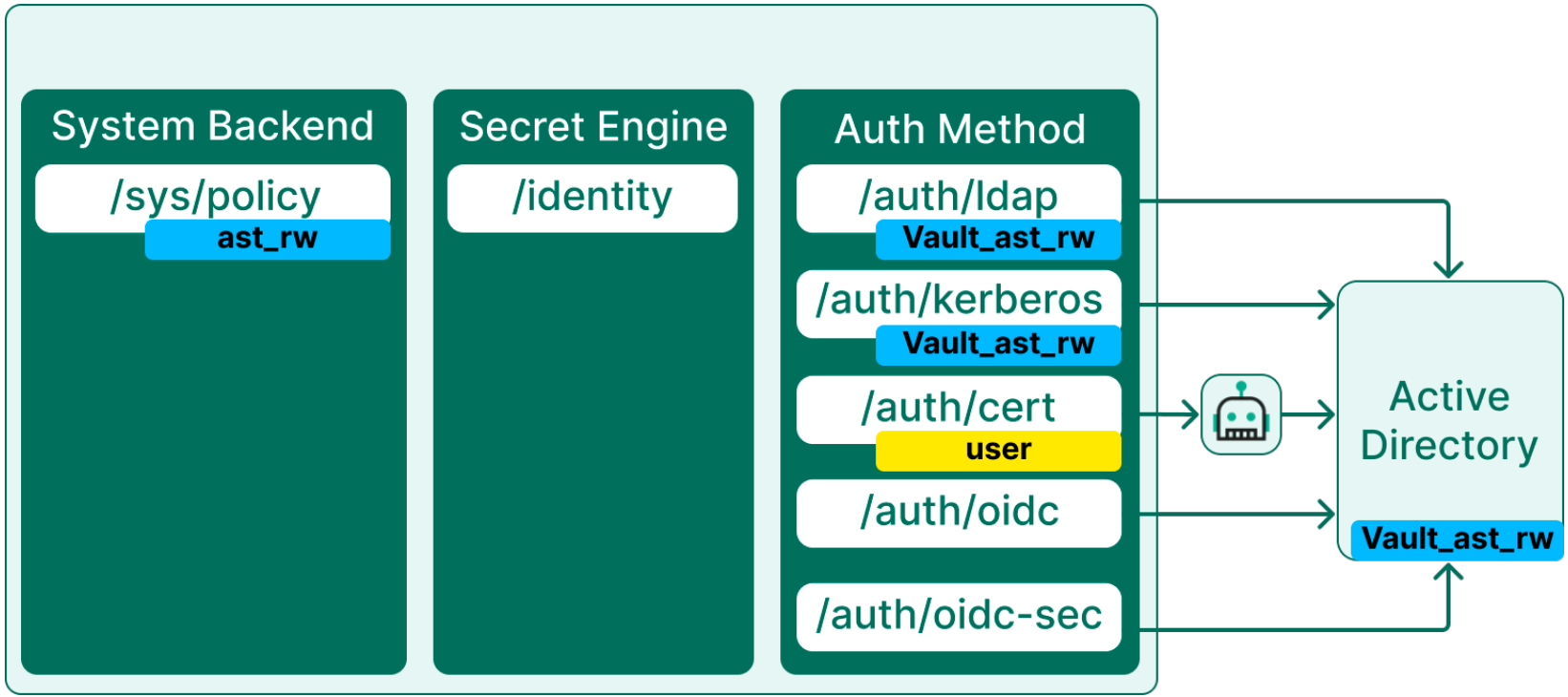
Создание спейса

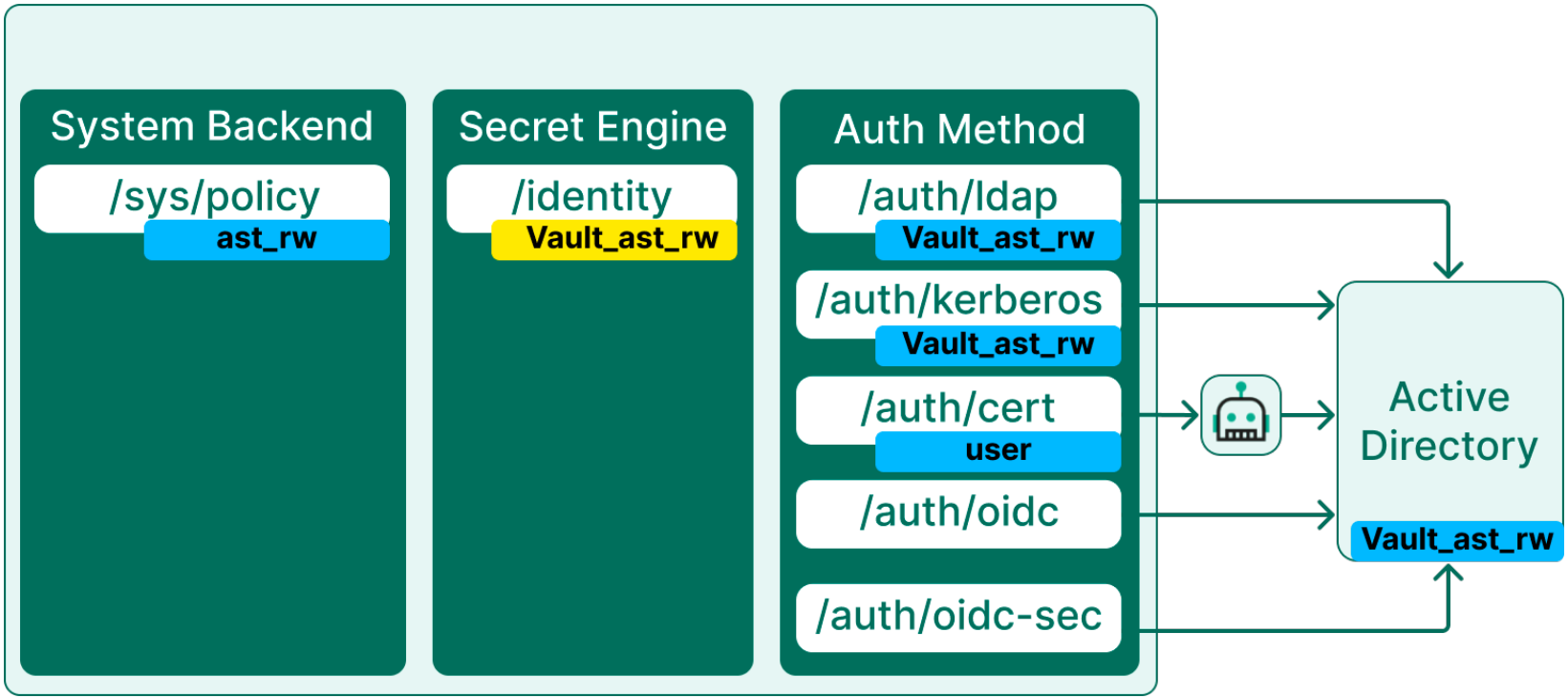

System Backend
/sys/policy
Secret Engine
/identity
Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory

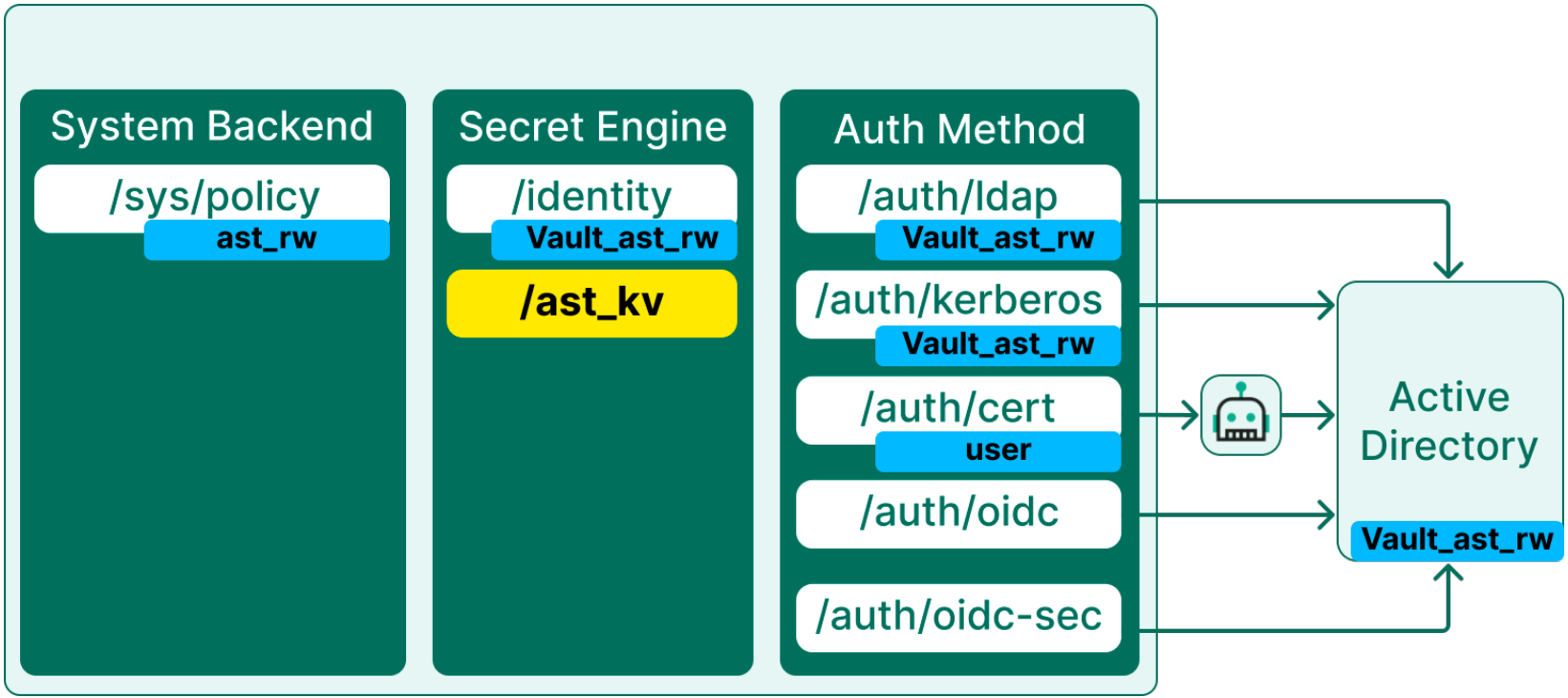

System Backend
/sys/policy
Secret Engine
/identity
Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory
Vault_ast_rw

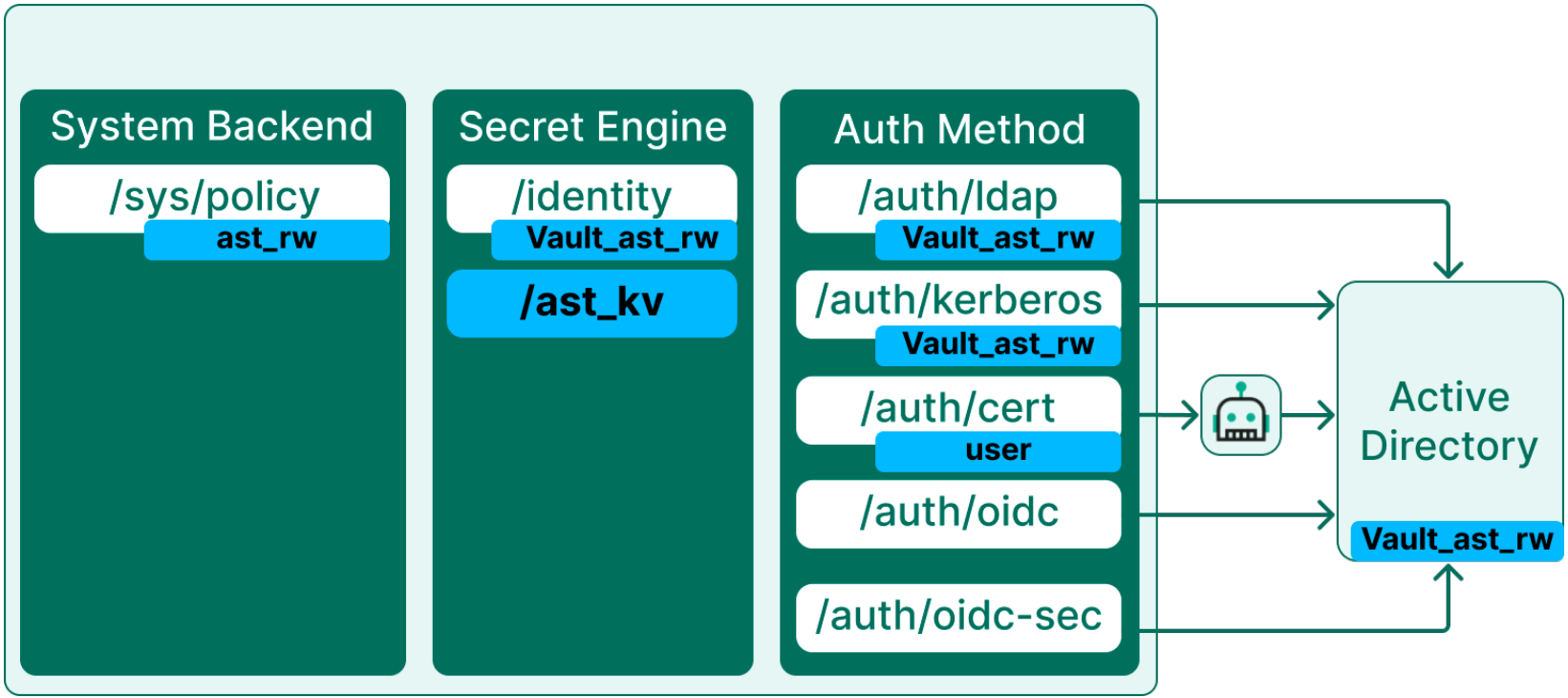

System Backend
/sys/policy
ast_rw
Secret Engine
/identity
Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory
Vault_ast_rw

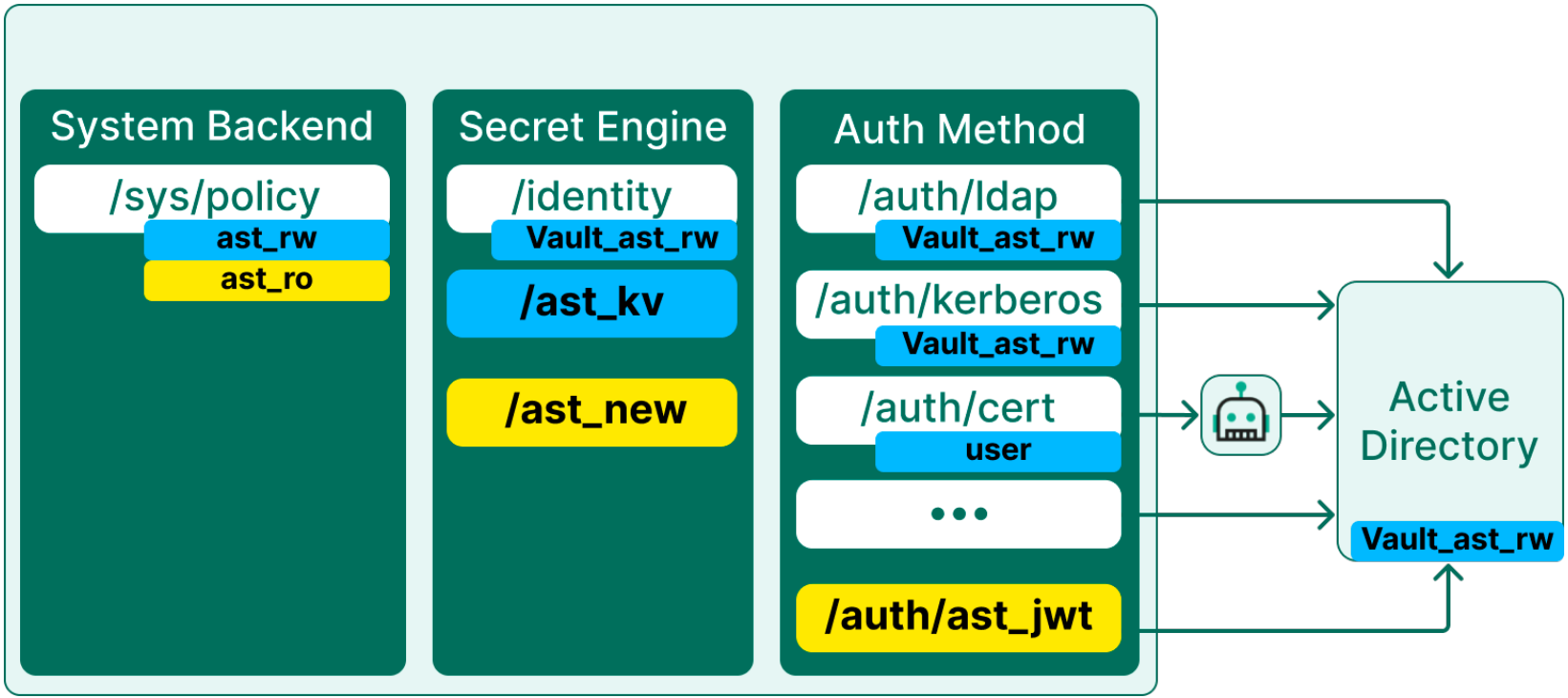

System Backend
/sys/policy
ast_rw
Secret Engine
/identity
Auth Method
/auth/ldap
Vault_ast_rw
/auth/kerberos
Vault_ast_rw
/auth/cert
/auth/oidc
/auth/oidc-sec
Active Directory
Vault_ast_rw


System Backend
/sys/policy
ast_rw
Secret Engine
/identity
Auth Method
/auth/ldap
Vault_ast_rw
/auth/kerberos
Vault_ast_rw
/auth/cert
user
/auth/oidc
/auth/oidc-sec
Active Directory
Vault_ast_rw


System Backend
/sys/policy
ast_rw
Secret Engine
/identity
Vault_ast_rw
Auth Method
/auth/ldap
Vault_ast_rw
/auth/kerberos
Vault_ast_rw
/auth/cert
user
/auth/oidc
/auth/oidc-sec
Active Directory
Vault_ast_rw


System Backend
/sys/policy
ast_rw
Secret Engine
/identity
Vault_ast_rw
/ast_kv
Auth Method
/auth/ldap
Vault_ast_rw
/auth/kerberos
Vault_ast_rw
/auth/cert
user
/auth/oidc
/auth/oidc-sec
Active Directory
Vault_ast_rw


System Backend
/sys/policy
ast_rw
Secret Engine
/identity
Vault_ast_rw
/ast_kv
Auth Method
/auth/ldap
Vault_ast_rw
/auth/kerberos
Vault_ast_rw
/auth/cert
user
/auth/oidc
/auth/oidc-sec
Active Directory
Vault_ast_rw


System Backend
/sys/policy
ast_rw
ast_ro
Secret Engine
/identity
Vault_ast_rw
/ast_kv
/ast_new
Auth Method
/auth/ldap
Vault_ast_rw
/auth/kerberos
Vault_ast_rw
/auth/cert
user
•••
/auth/ast_jwt
Active Directory
Vault_ast_rw

Требования к управлению спейсом

Хранилища секретов

Методы аутентификации

Объекты аутентификации и политики

Разграничение доступа

Требования к управлению спейсом

Хранилища секретов

Методы аутентификации

Объекты аутентификации и политики

Разграничение доступа

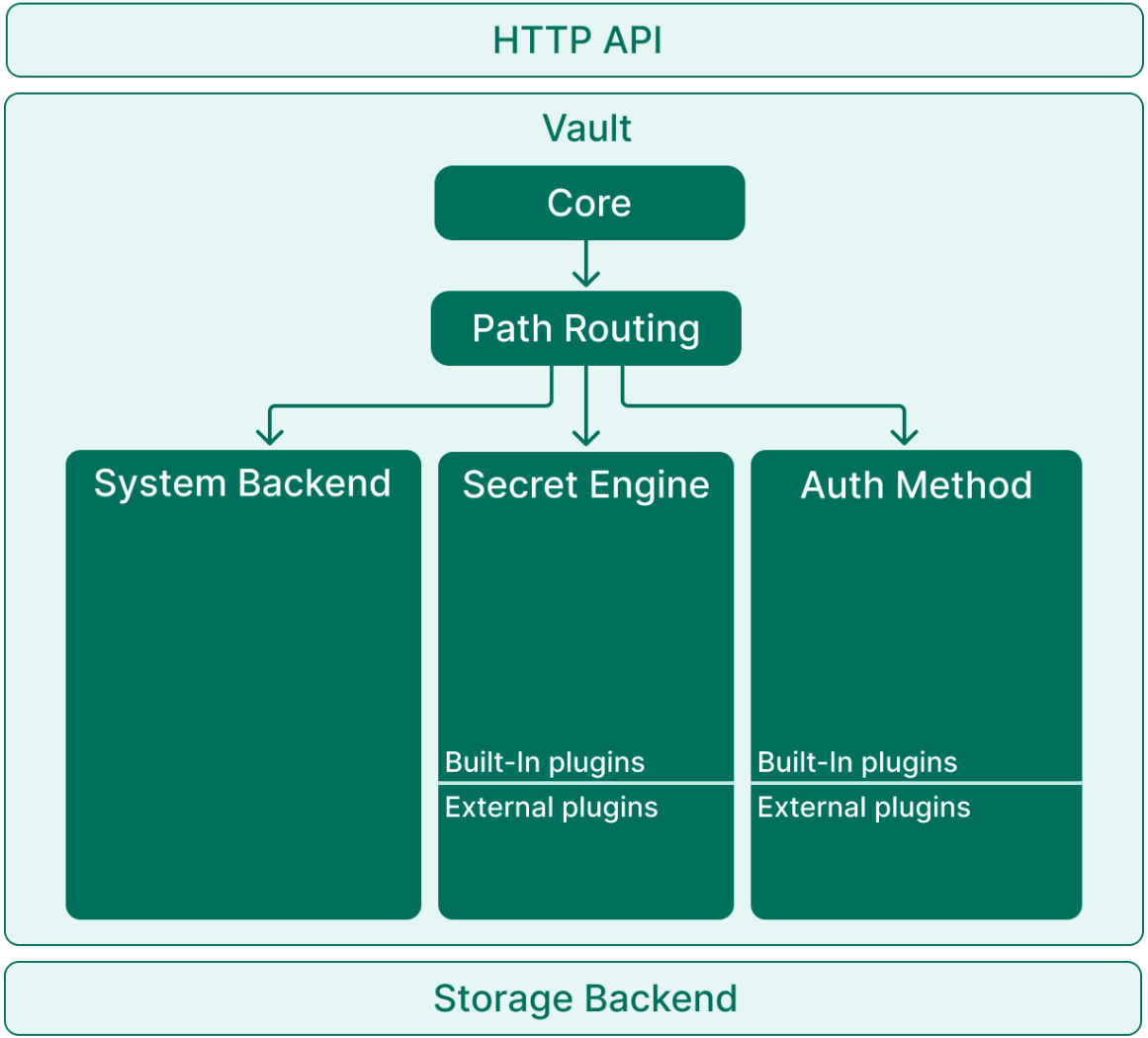
Доступ к системным путям – невозможен

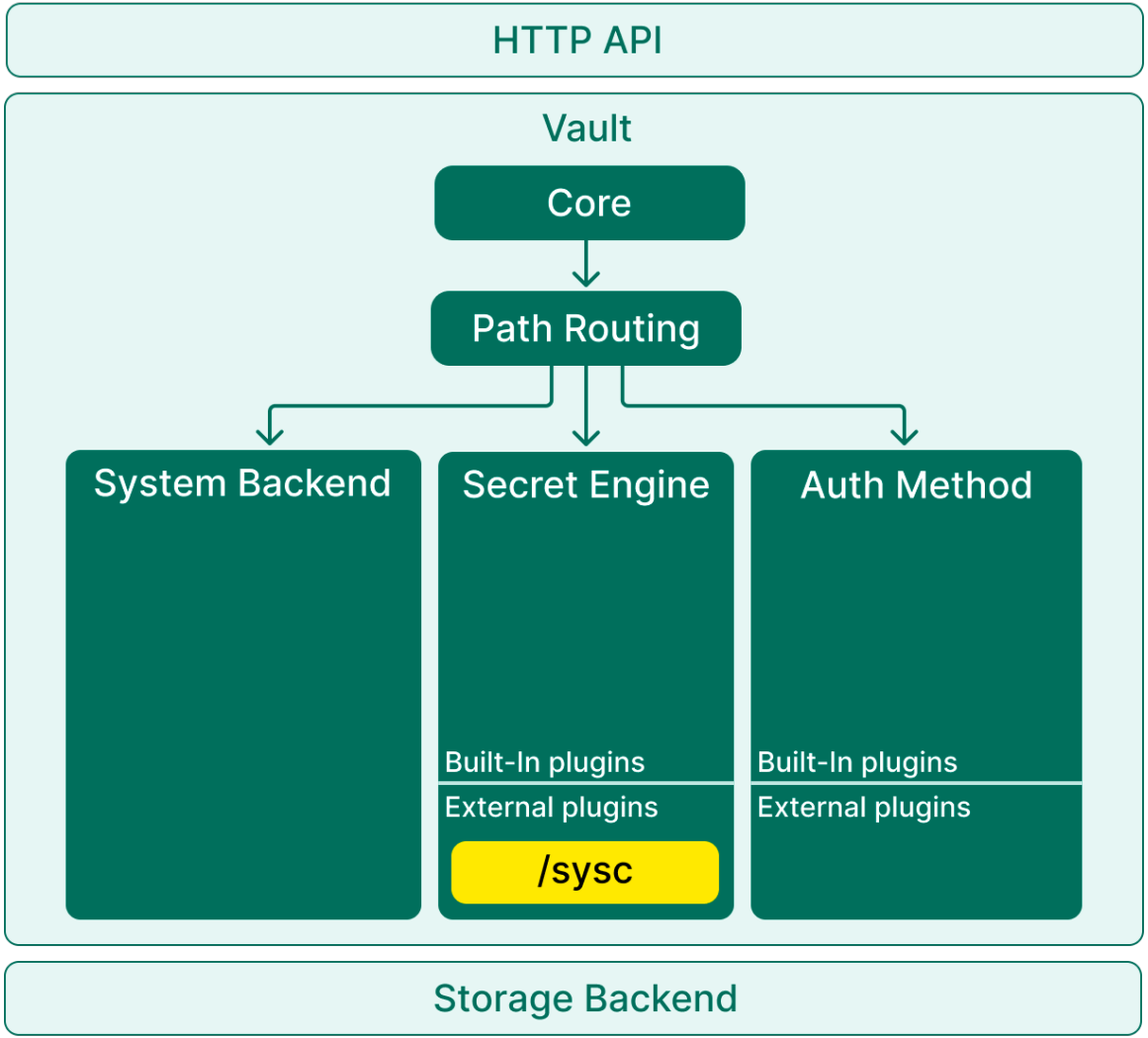
/sys/mounts/ast_*

/sys/auth/ast_*

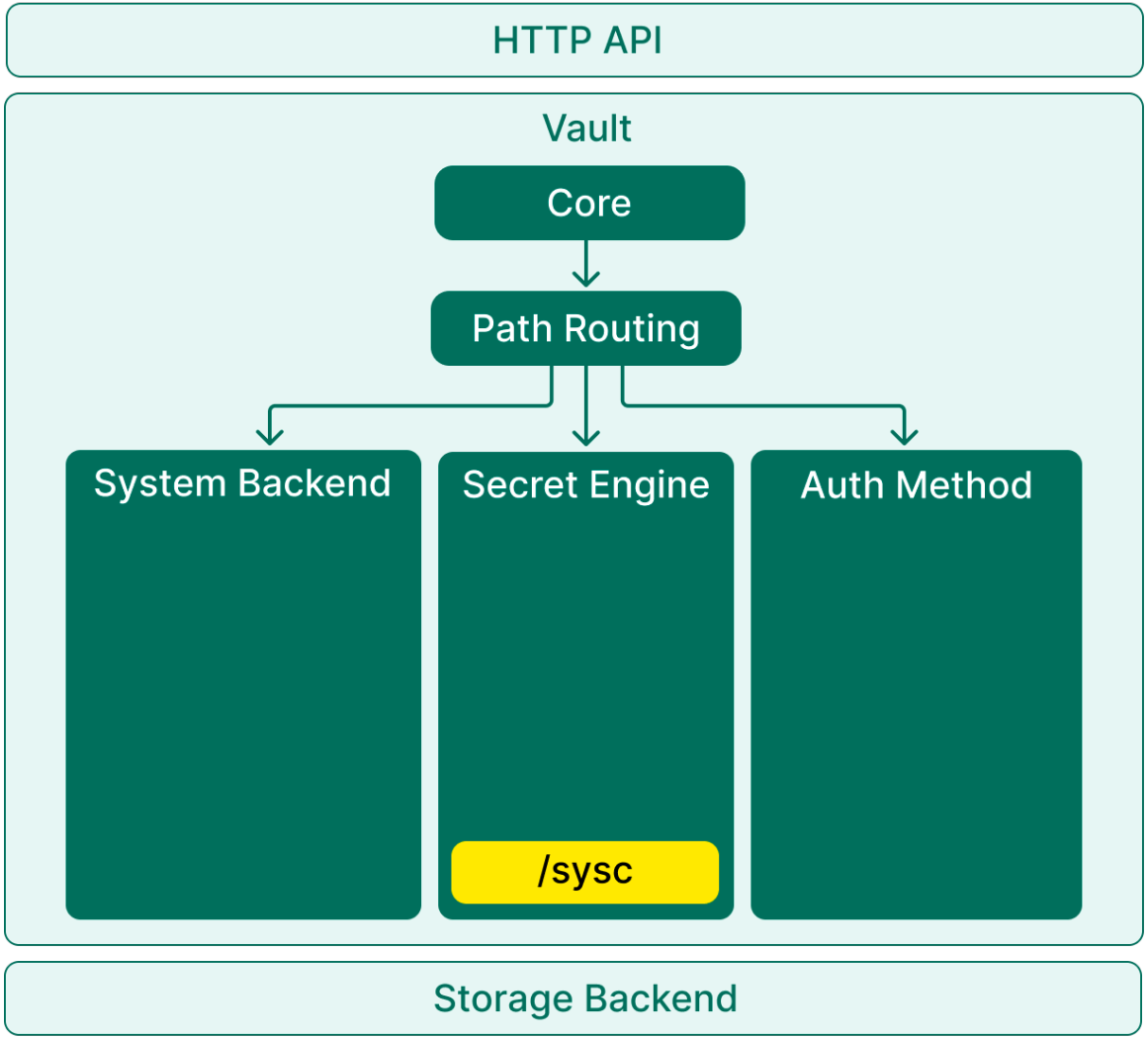
/sys/policy/ast_*

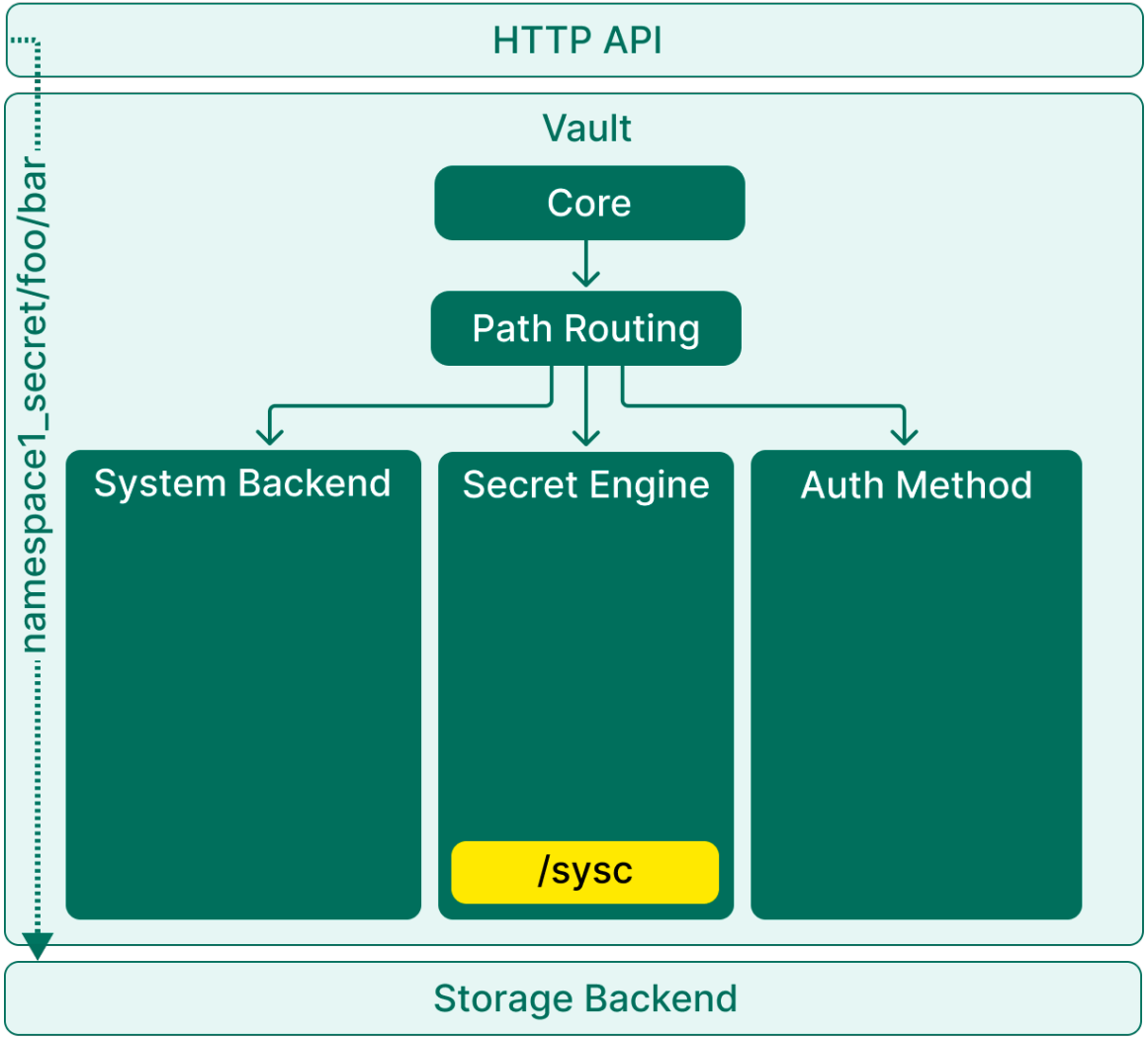
/auth/ast_*

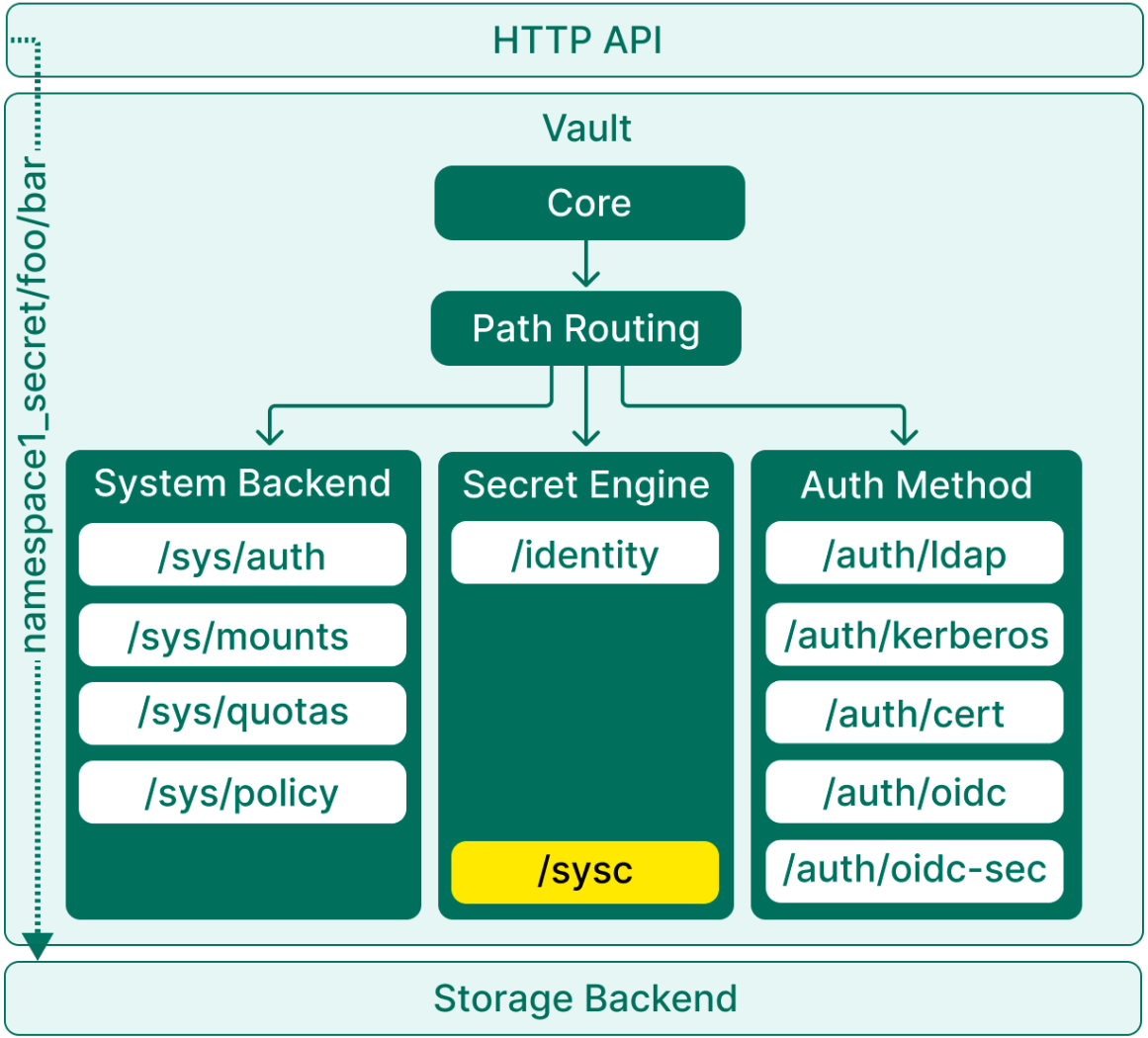

HTTP API
Vault
Core
Path Routing
System Backend
Secret Engine
Built-In plugins
External plugins
Auth Method
Built-In plugins
External plugins
Storage Backend

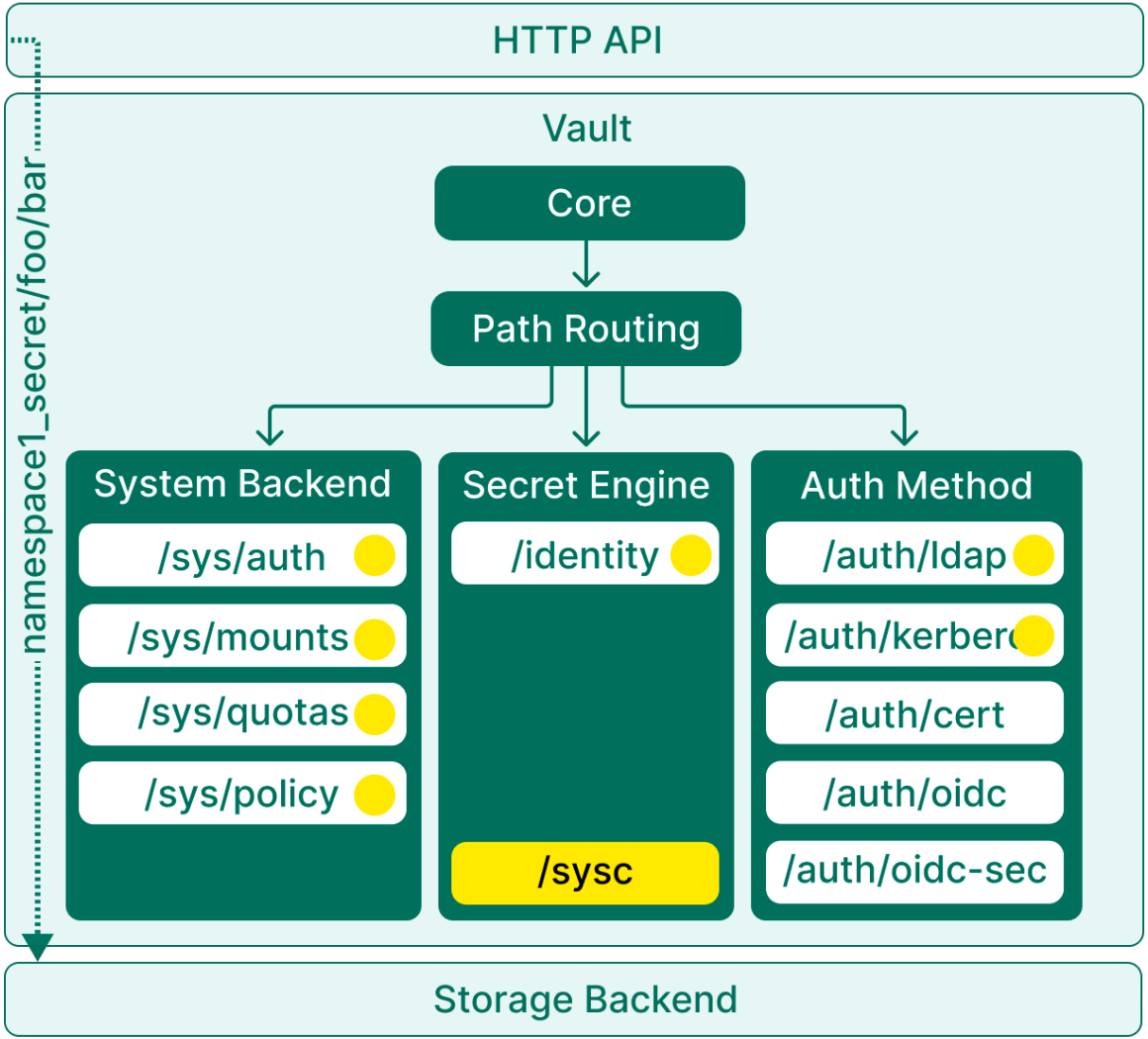


SysC –
System
Custom


HTTP API
Vault
Core
Path Routing
System Backend
Secret Engine
/sysc
Auth Method
Storage Backend


HTTP API
Vault
Core
Path Routing
System Backend
Secret Engine
Auth Method
/sysc
namespace1_secret/foo/bar
Storage Backend


HTTP API
Vault
Core
Path Routing
namespace1_secret/foo/bar
System Backend
/sys/auth
/sys/mounts
/sys/quotas
/sys/policy
Secret Engine
/identity
/sysc
Auth Method
/auth/ldap
/auth/kerberos
/auth/cert
/auth/oidc
/auth/oidc-sec
Storage Backend

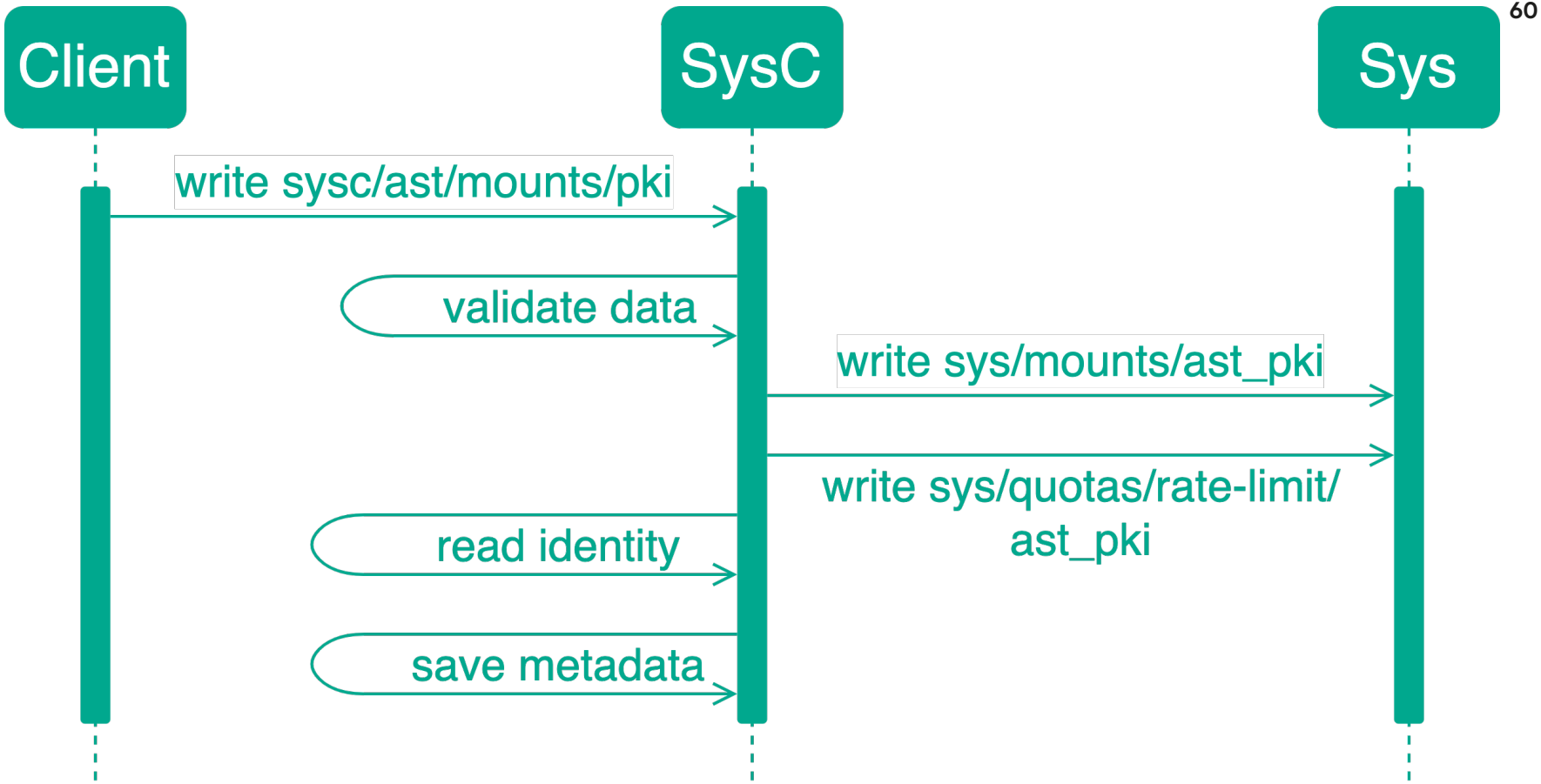

HTTP API
namespace1_secret/foo/bar
Vault
Core
Path Routing
System Backend
/sys/auth
/sys/mounts
/sys/quotas
/sys/policy
Secret Engine
/identity
/sysc
Auth Method
/auth/ldap
/auth/kerber
/auth/cert
/auth/oidc
/auth/oidc-sec
Storage Backend

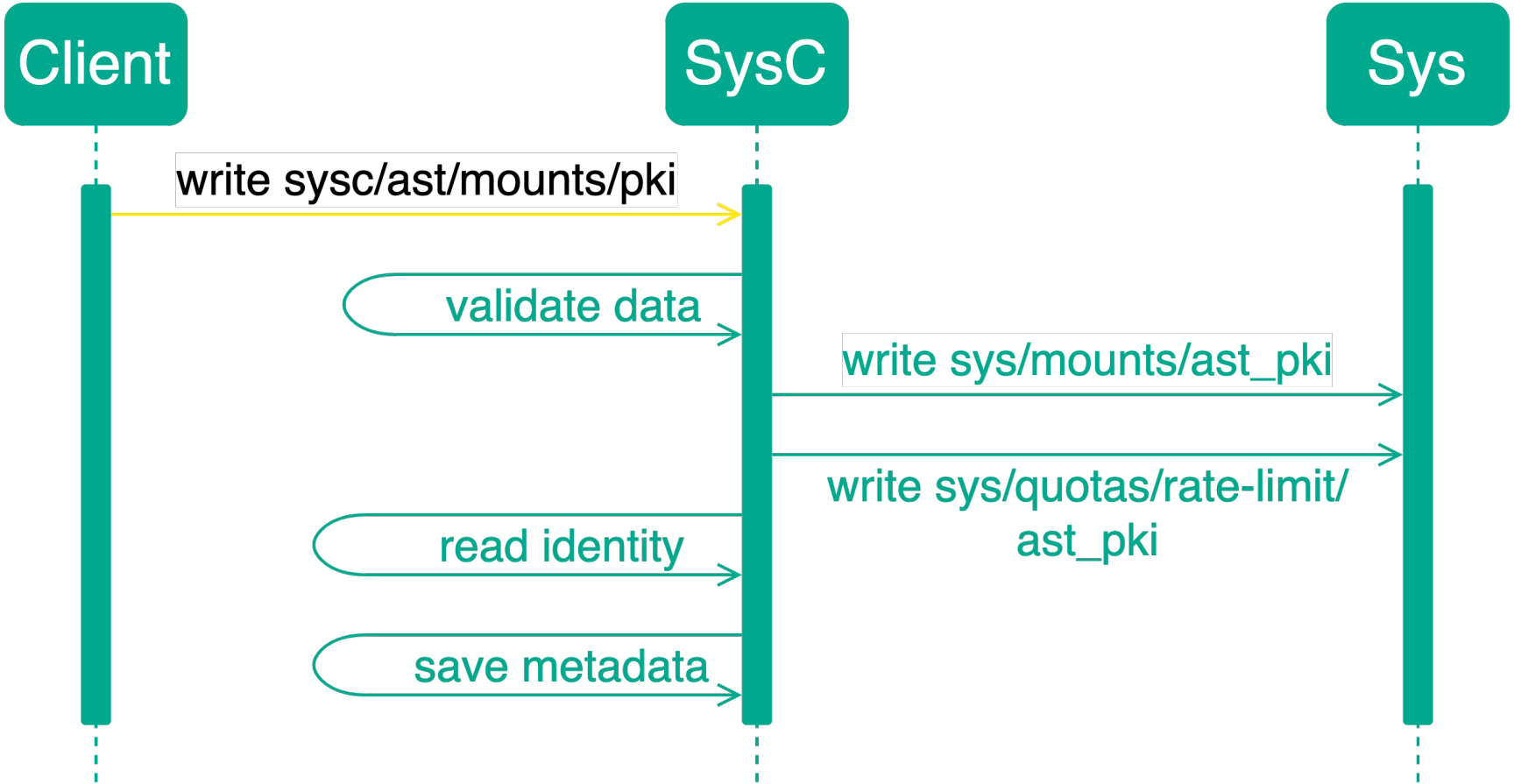
Дополнение к политике для спейса (ast_rw)

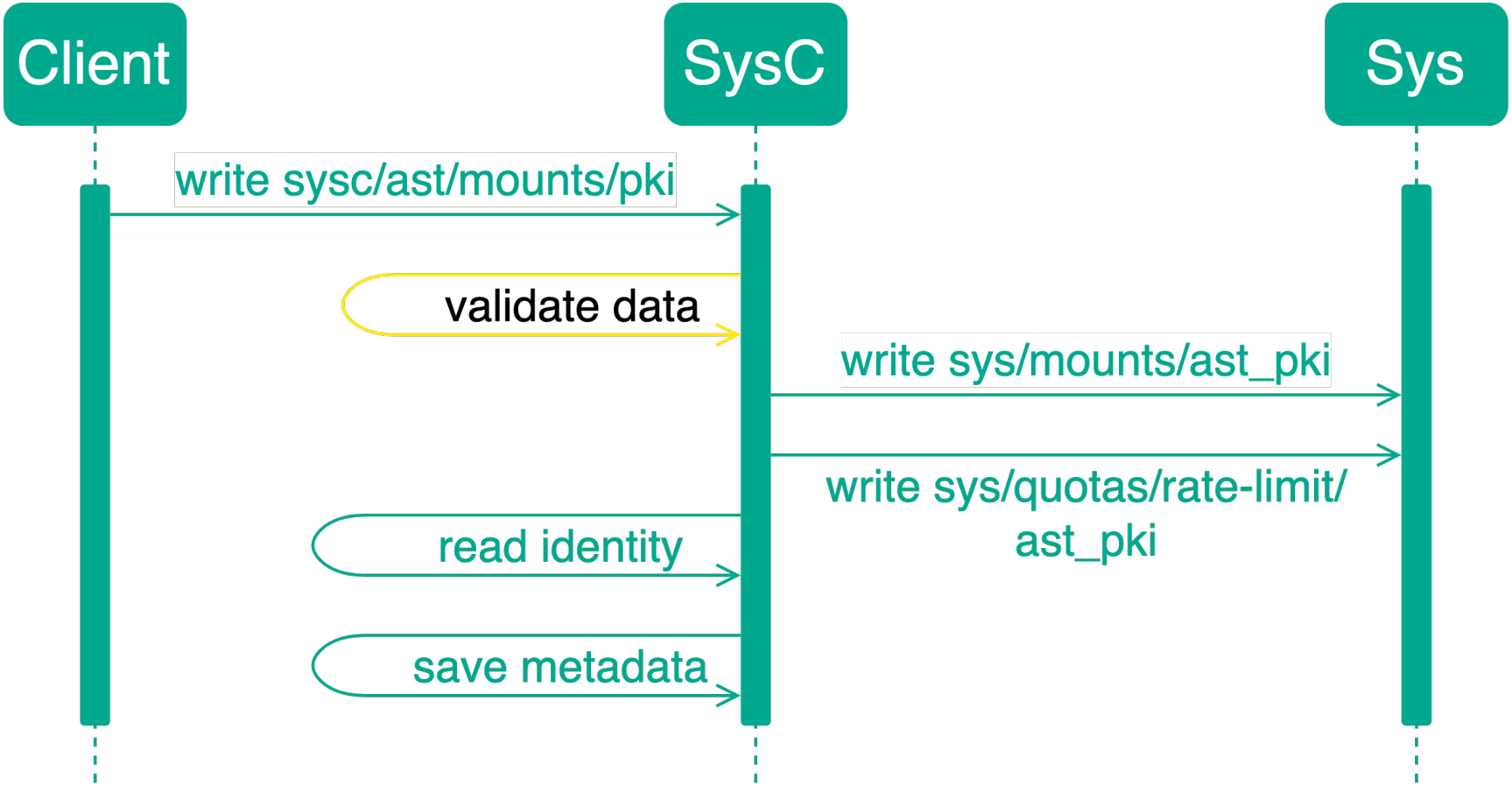

```
path "sysc/ast/*" {
    capabilities = [...]
}
```

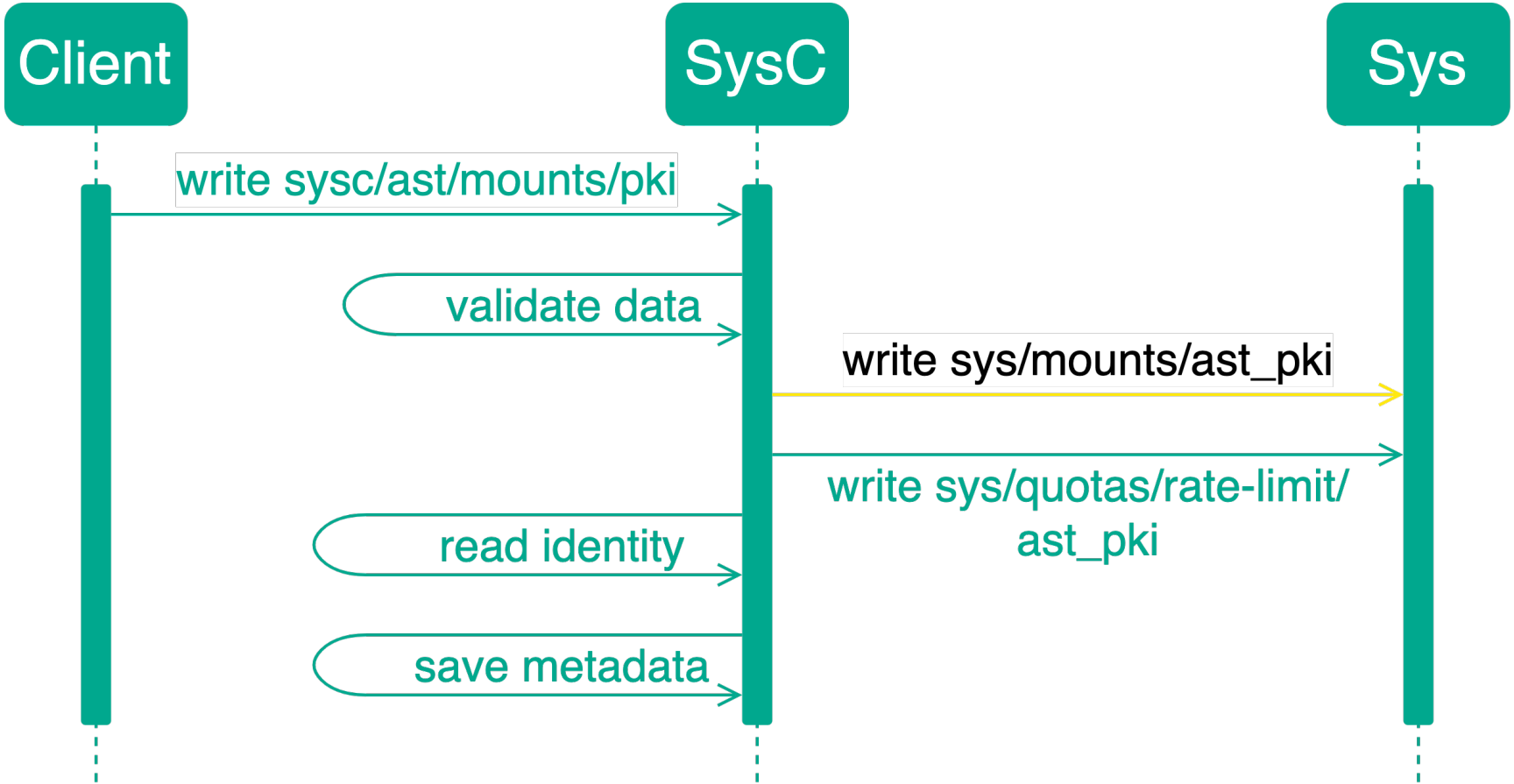
Плагин и его API

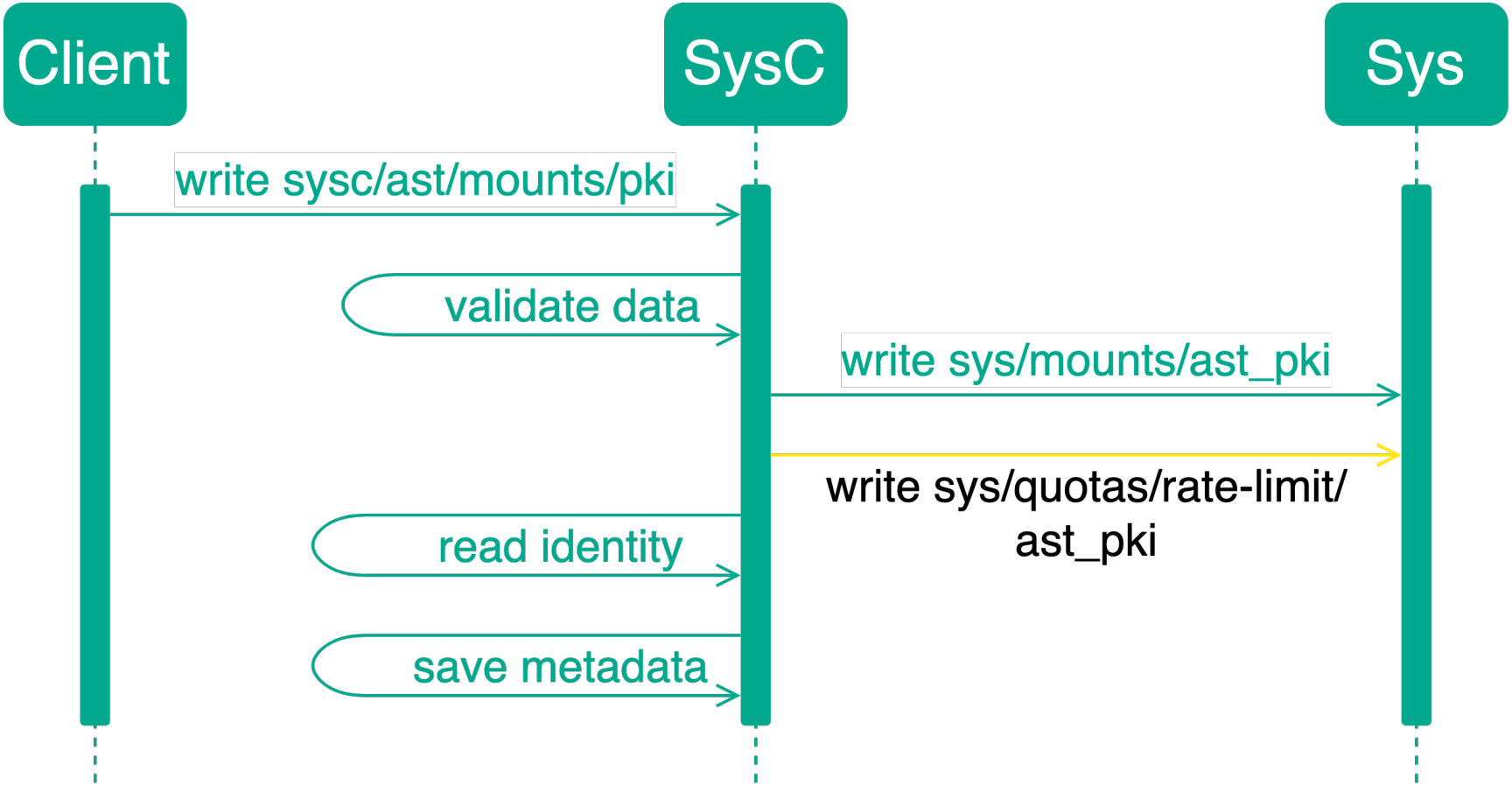
Плагин и его API

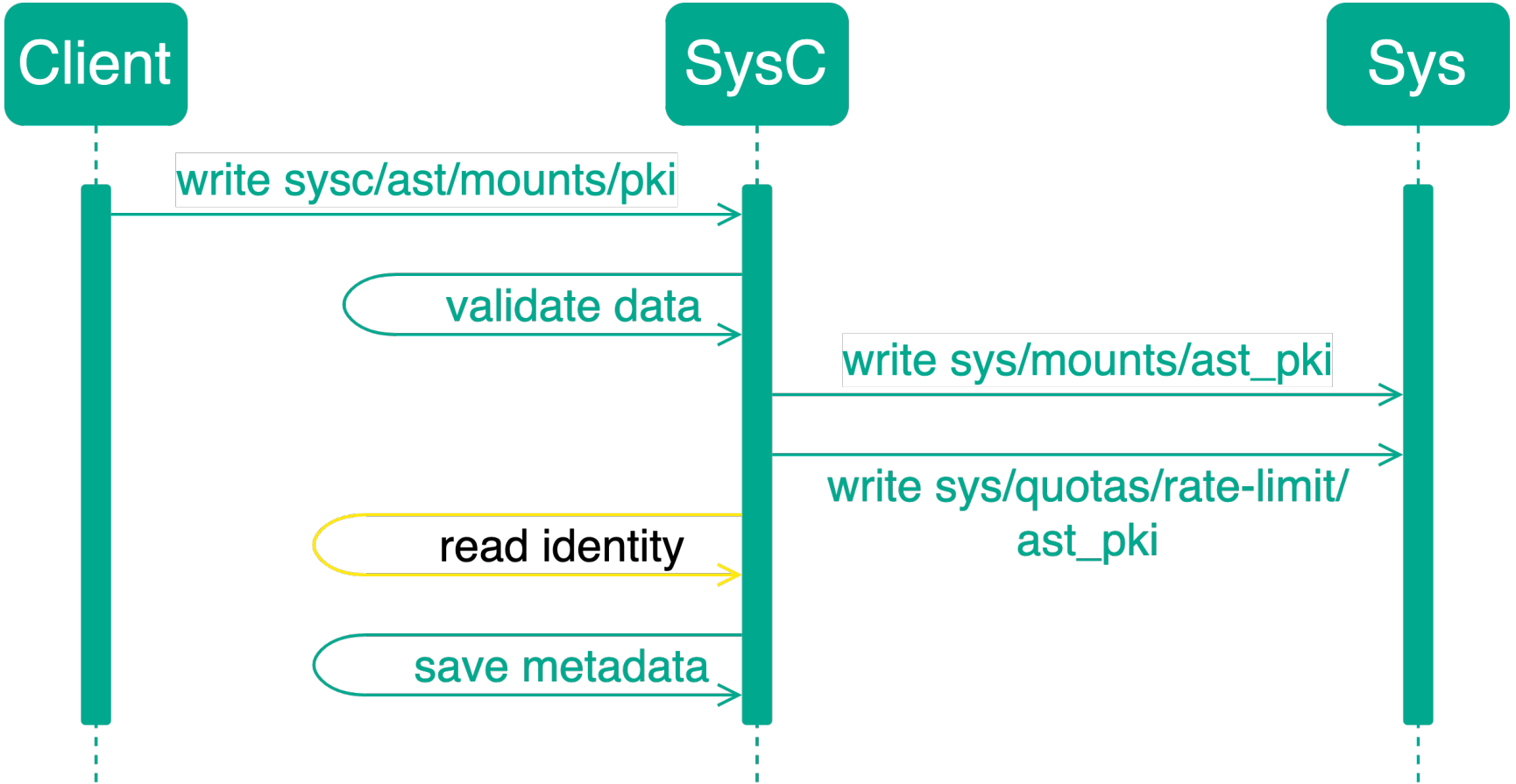

Client
SysC
Sys
write sysc/ast/mounts/pki
validate data
write sys/mounts/ast_pki
write sys/quotas/rate-limit/
ast_pki
read identity
save metadata

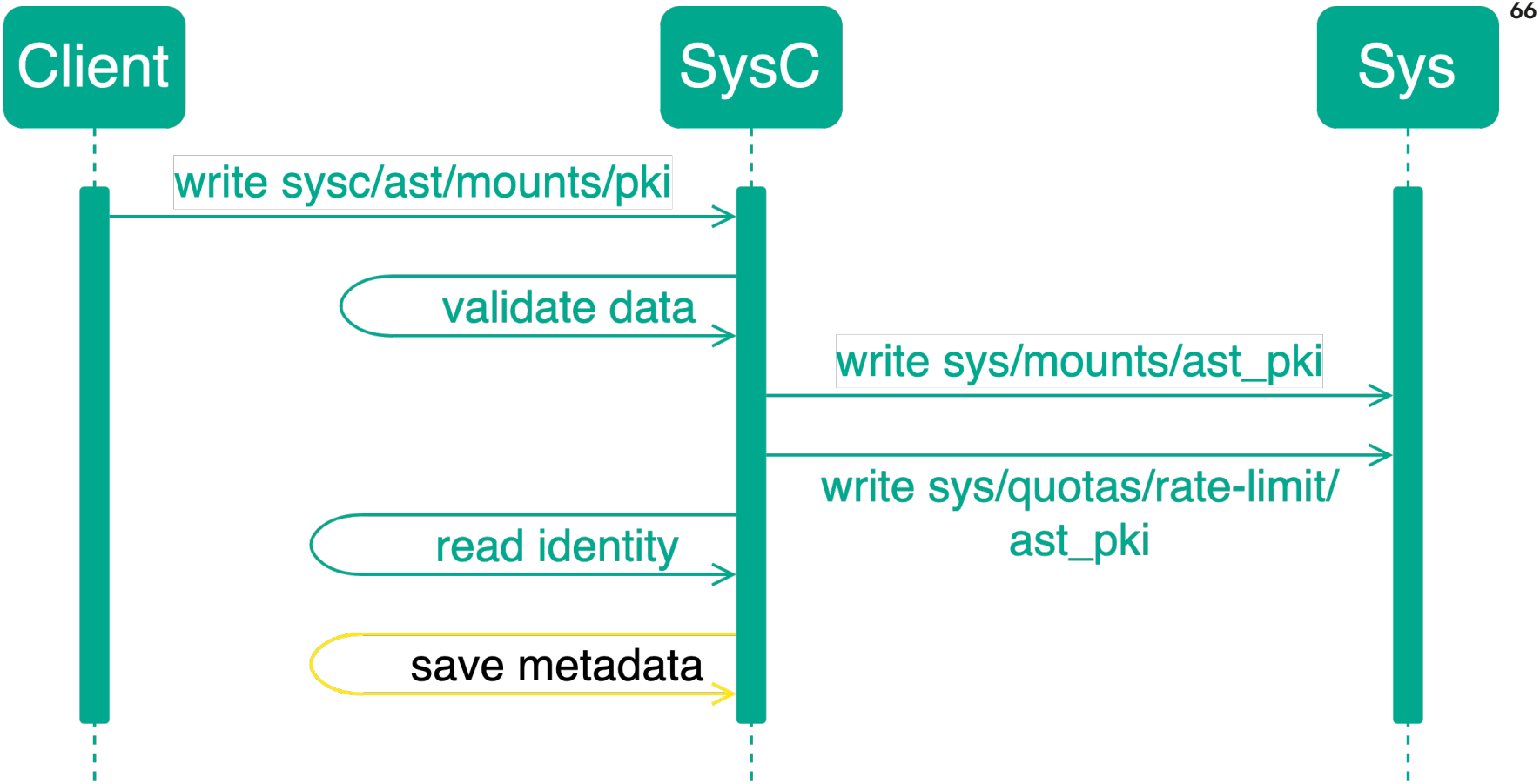

Client
SysC
Sys
write sysc/ast/mounts/pki
validate data
write sys/mounts/ast_pki
write sys/quotas/rate-limit/
ast_pki
read identity
save metadata


Client
SysC
Sys
write sysc/ast/mounts/pki
validate data
write sys/mounts/ast_pki
write sys/quotas/rate-limit/
ast_pki
read identity
save metadata

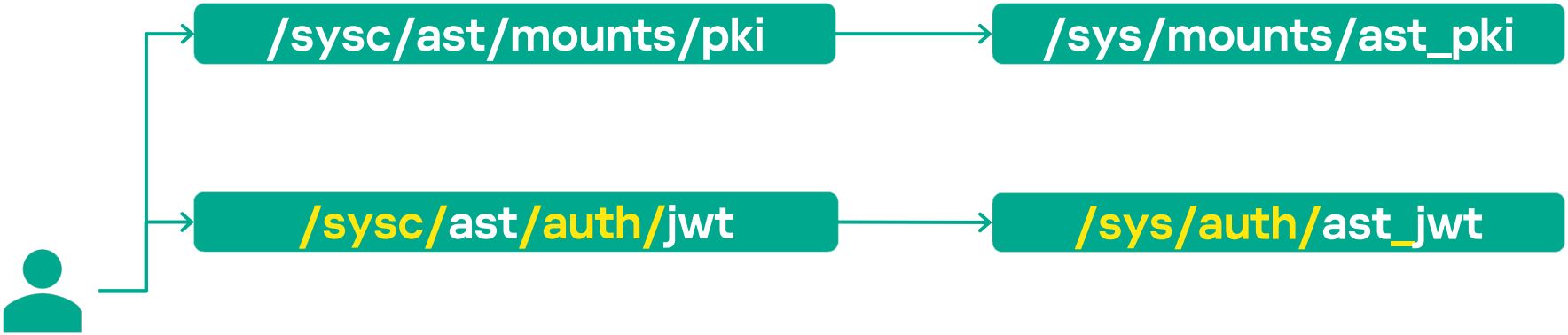

Client
SysC
Sys
write sysc/ast/mounts/pki
validate data
write sys/mounts/ast_pki
write sys/quotas/rate-limit/
ast_pki
read identity
save metadata

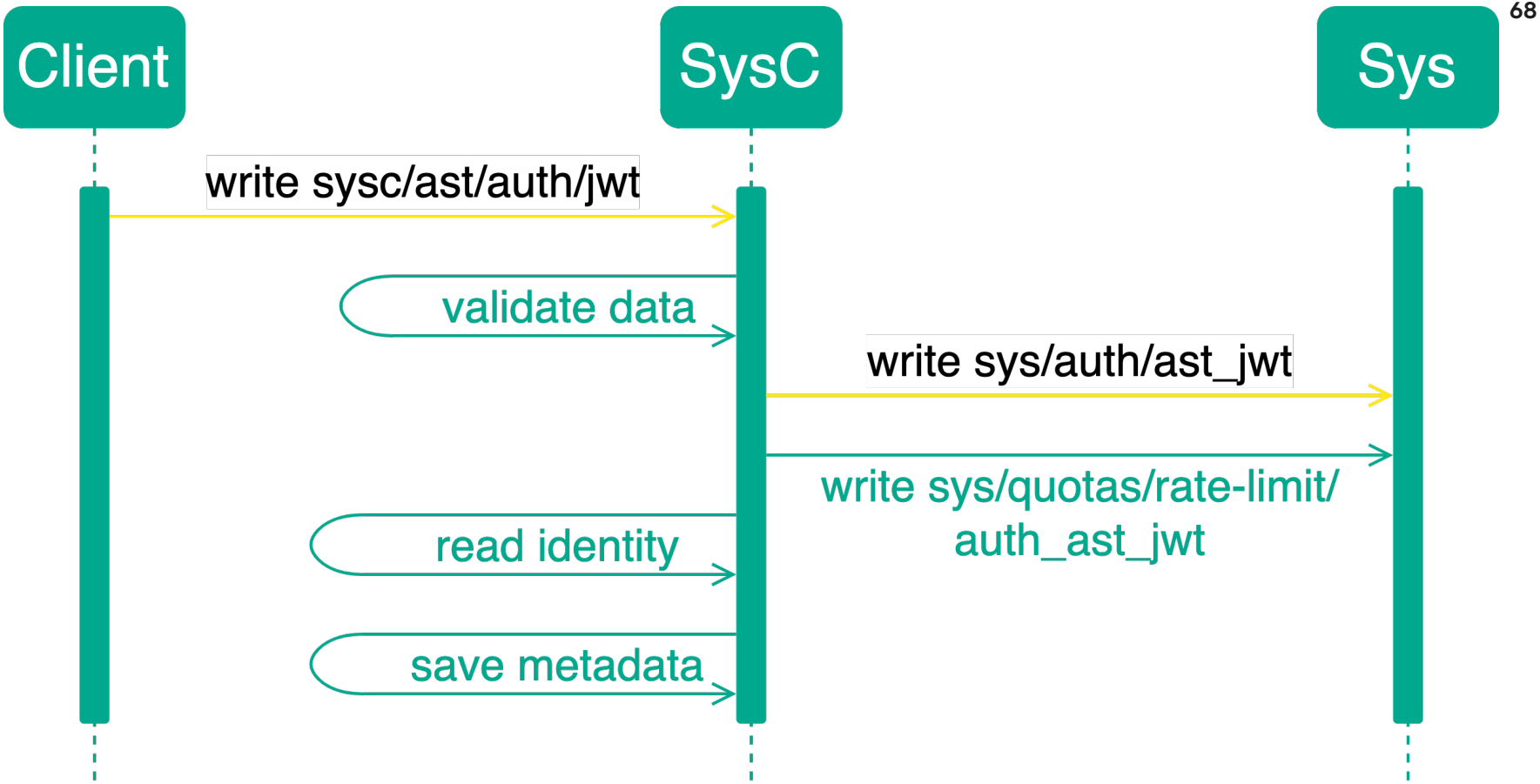

Client
SysC
Sys
write sysc/ast/mounts/pki
validate data
write sys/mounts/ast_pki
write sys/quotas/rate-limit/
ast_pki
read identity
save metadata


Client
SysC
Sys
write sysc/ast/mounts/pki
validate data
write sys/mounts/ast_pki
write sys/quotas/rate-limit/
ast_pki
read identity
save metadata

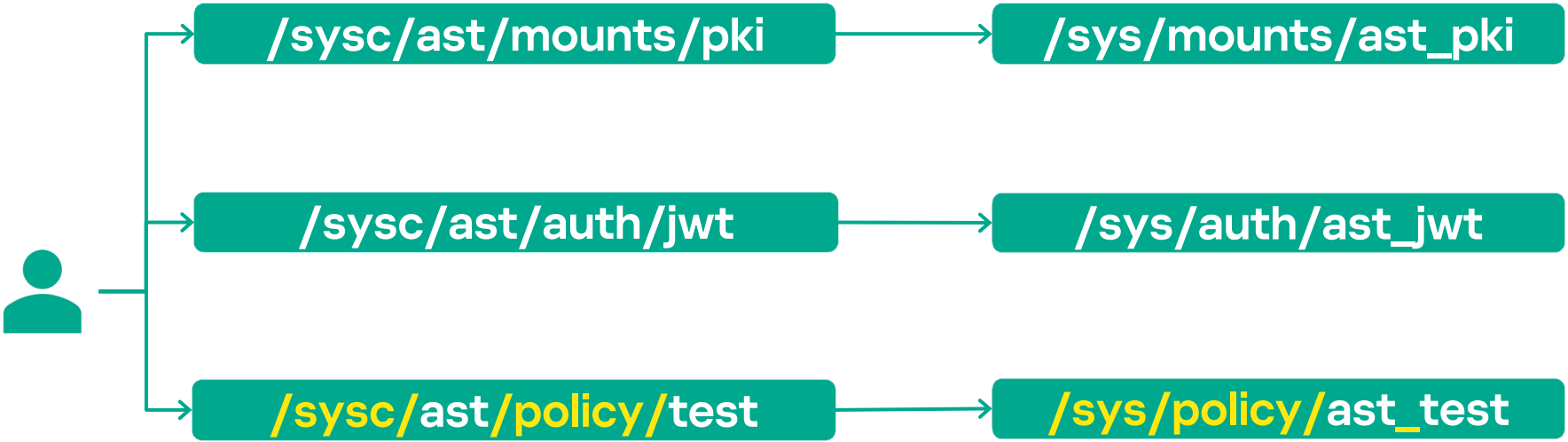

Client
SysC
Sys
write sysc/ast/mounts/pki
validate data
write sys/mounts/ast_pki
write sys/quotas/rate-limit/
ast_pki
read identity
save metadata

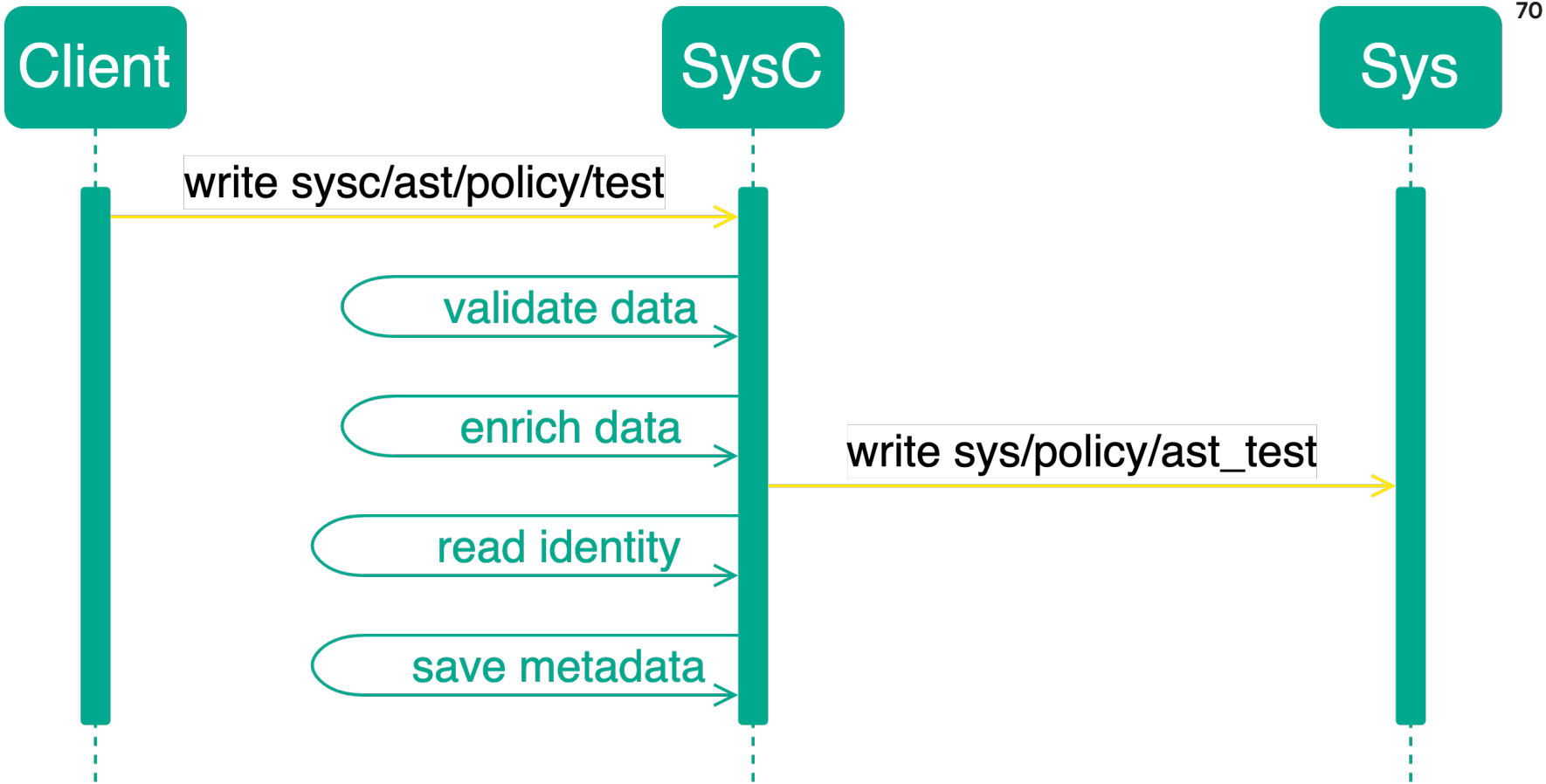
Плагин и его API

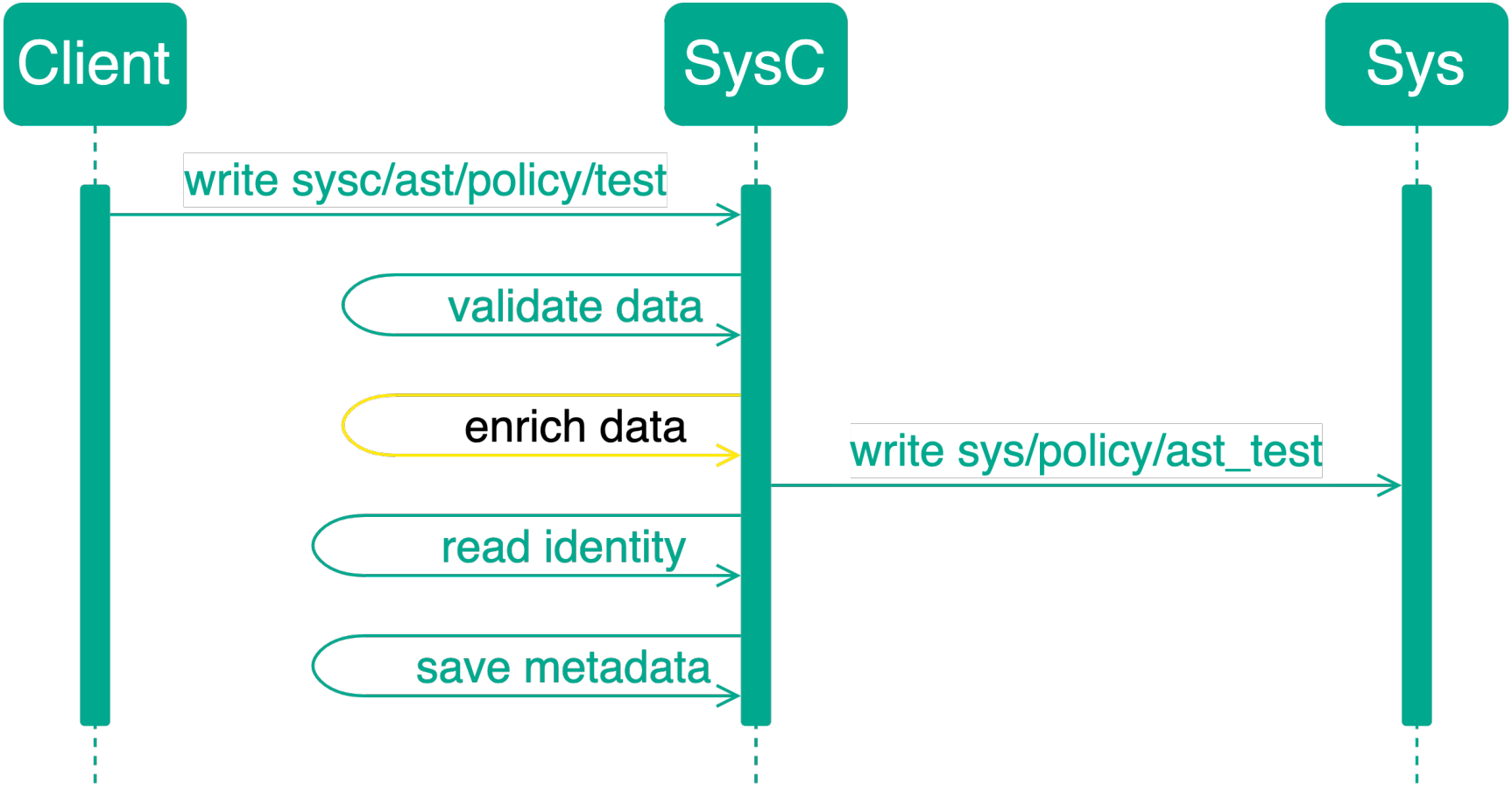



Client
SysC
Sys
write sysc/ast/auth/jwt
validate data
write sys/auth/ast_jwt
write sys/quotas/rate-limit/
auth_ast_jwt
read identity
save metadata

Плагин и его API




Client
SysC
Sys
write sysc/ast/policy/test
validate data
enrich data
write sys/policy/ast_test
read identity
save metadata


Client
SysC
Sys
write sysc/ast/policy/test
validate data
enrich data
write sys/policy/ast_test
read identity
save metadata

Плагин и его функционирование: policy – enrich data


```
rules=
"ast_common/*"="update"
```

```
path "ast_common/*" {
  rules = ["update"]
}
```

```
rules=
"auth/ast_*"="update"
```

```
path "auth/ast_*" {
  rules = ["update"]
  denied_parameters  = {
    "token_policies" = []
    "policies"       = []
  }
}
```

Плагин и его функционирование: policy – enrich data

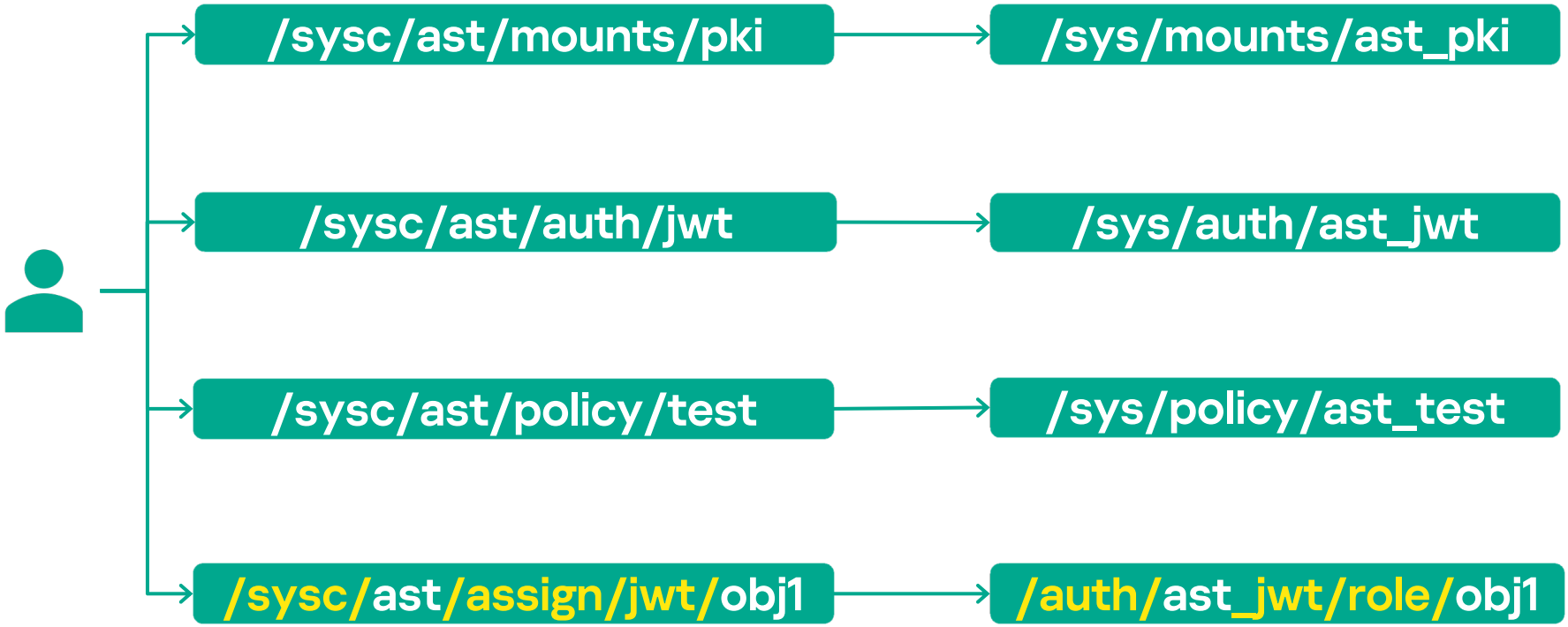

```
rules=
"ast_common/*"="update"
```

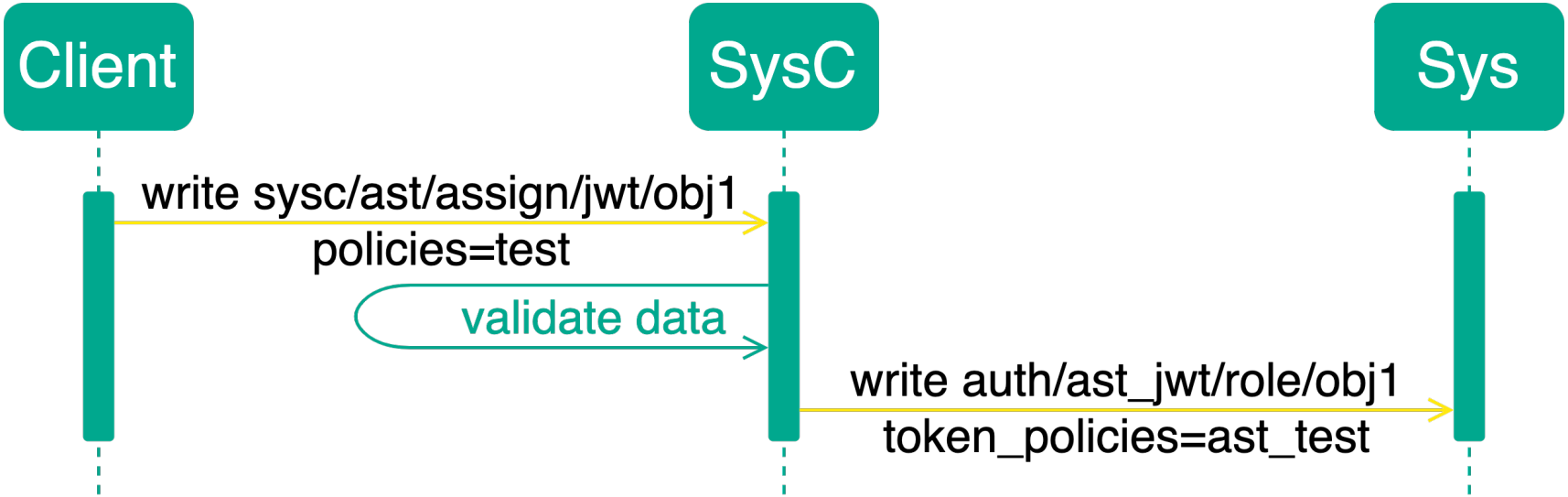
```
path "ast_common/*" {
  rules = ["update"]
}
```

```
rules=
"auth/ast_*"="update"
```

```
path "auth/ast_*" {
  rules = ["update"]
  denied_parameters  = {
    "token_policies" = []
    "policies"       = []
  }
}
```

Плагин и его API




Client
SysC
Sys
write sysc/ast/assign/jwt/obj1
policies=test
validate data
write auth/ast_jwt/role/obj1
token_policies=ast_test

Доступ к системным путям – возможен (через плагин)

/sys/mounts/ast_*

/sys/auth/ast_*

/sys/policy/ast_*

/auth/ast_*

Требования к управлению спейсом

Хранилища секретов

Методы аутентификации

Объекты аутентификации и политики

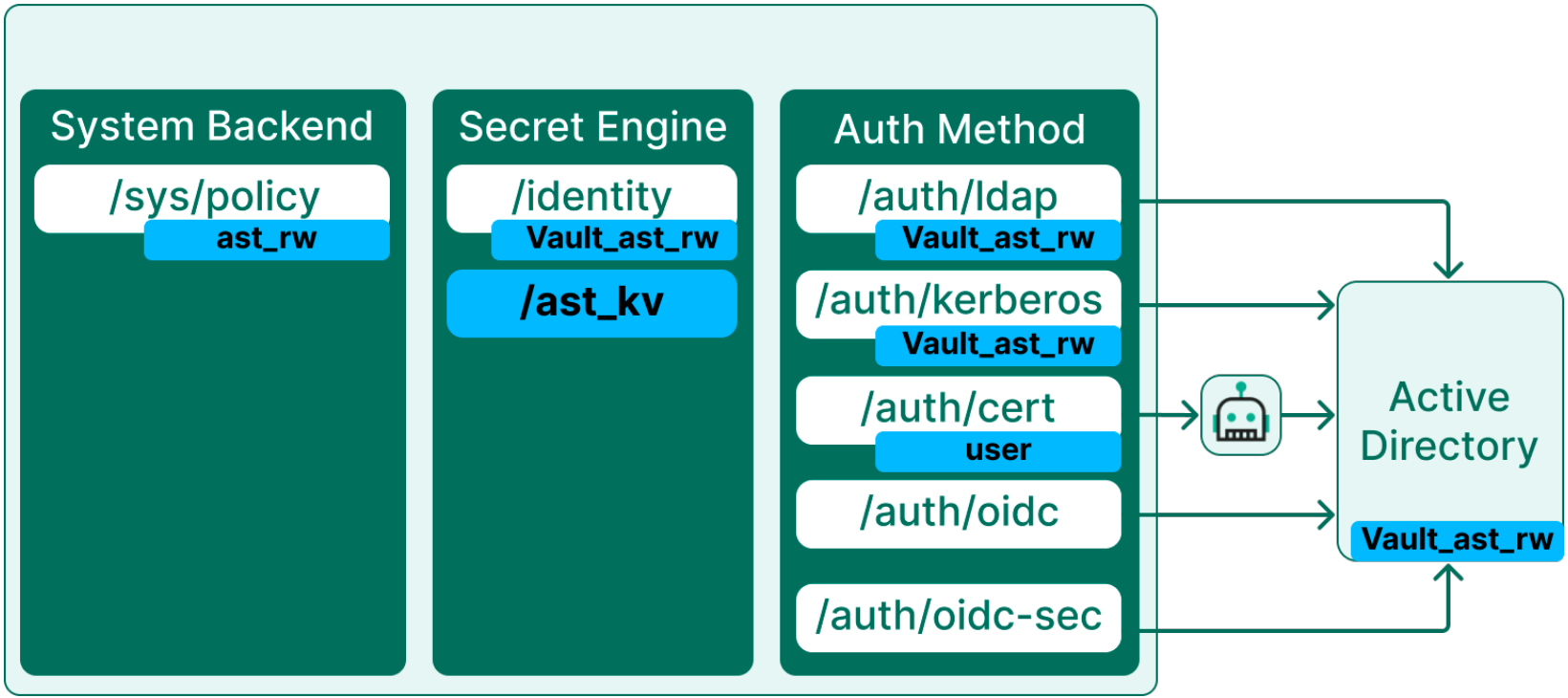
Разграничение доступа

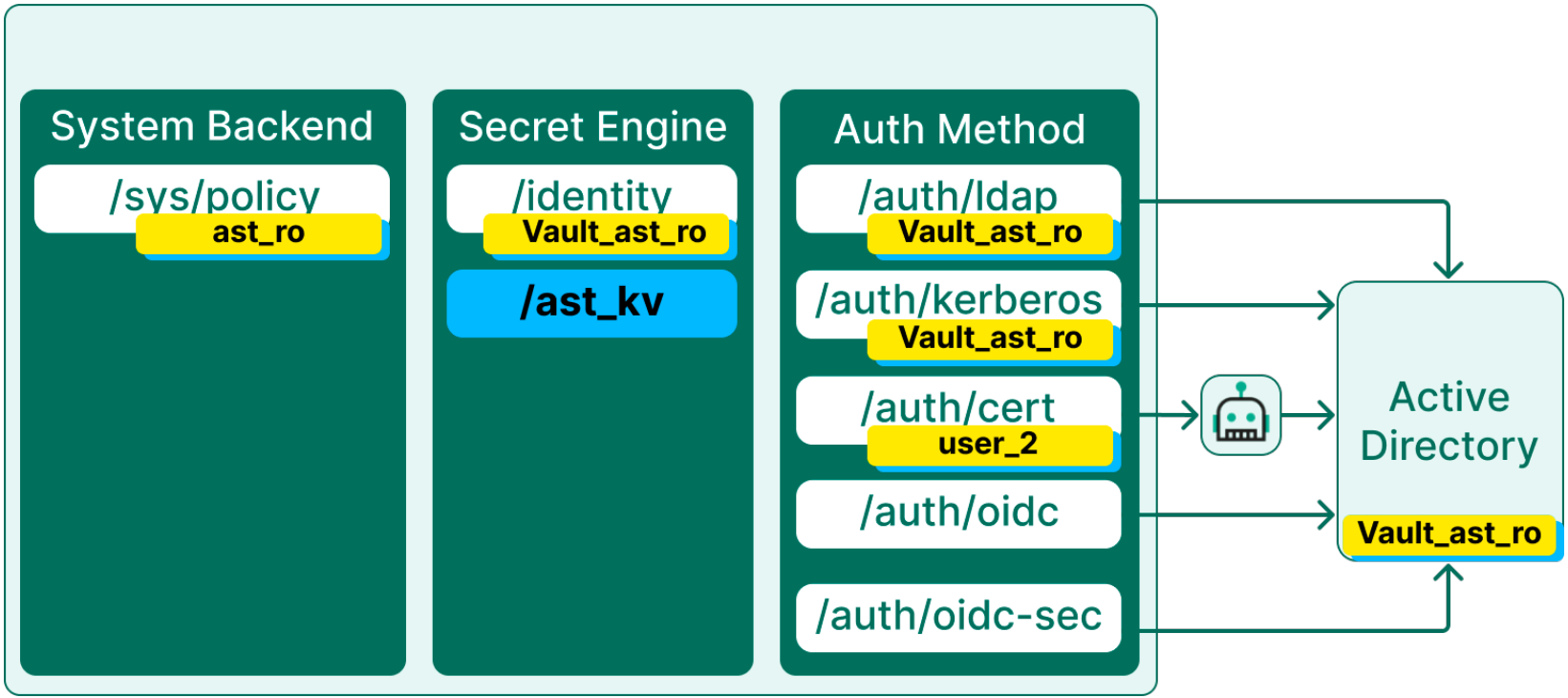
С чего все началось

Как организовали доступ

Как сделали свои спейсы

Как настроили разграничение прав


System Backend
/sys/policy
ast_rw
Secret Engine
/identity
Vault_ast_rw
/ast_kv
Auth Method
/auth/ldap
Vault_ast_rw
/auth/kerberos
Vault_ast_rw
/auth/cert
user
/auth/oidc
/auth/oidc-sec
Active Directory
Vault_ast_rw


System Backend
/sys/policy
ast_ro
Secret Engine
/identity
Vault_ast_ro
/ast_kv
Auth Method
/auth/ldap
Vault_ast_ro
/auth/kerberos
Vault_ast_ro
/auth/cert
user_2
/auth/oidc
/auth/oidc-sec
Active Directory
Vault_ast_ro

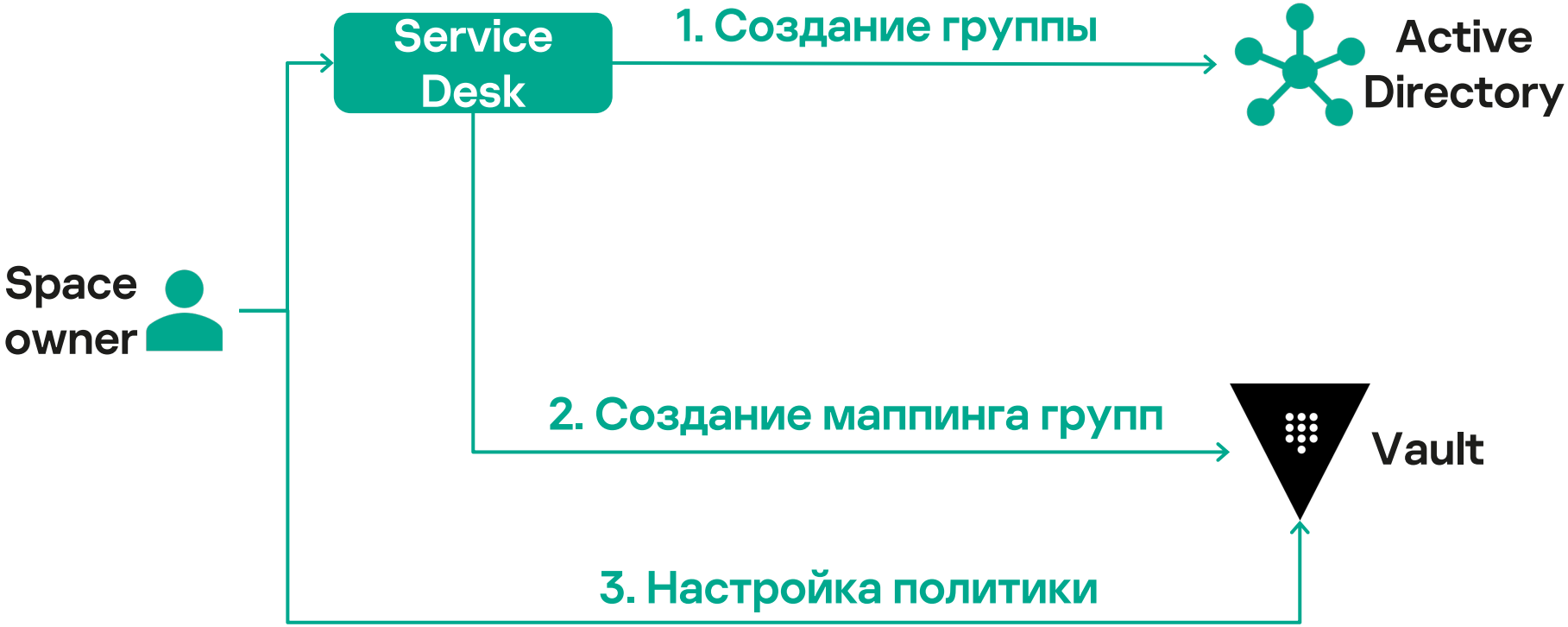
RBAC

Объект	Значение
Space	ast
Admin role	rw
Admin policy	ast_rw
Admin group	Vault_ast_rw

RBAC

Объект	Значение
Space	ast
Admin role	rw
Admin policy	ast_rw
Admin group	Vault_ast_rw
Custom role	ro
Custom policy	ast_ro
Custom group	Vault_ast_ro

RBAC: создание роли



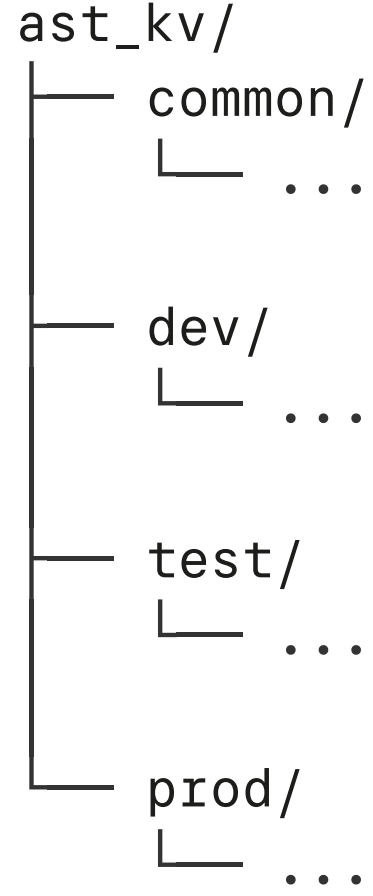
RBAC: свойства

Свои управляющие

Гранулированный доступ

Все определено через AD

RBAC: пример разграничения



RBAC: пример разграничения – Vault_ast_developer


```
ast_kv/
├── common/
│   └── ... # Read-only access
├── dev/
│   └── ... # Read-write access
├── test/
│   └── ... # Read-only access
└── prod/
    └── ... # Read-only-metadata access
```

С чего все началось

Как организовали доступ

Как сделали свои спейсы

Как настроили разграничение прав

Вместо заключения

Vault как основной OIDC провайдер

Спасибо

Mikhail Pakhomov pakhomovmikhail3@gmail.com @nilunne

kaspersky