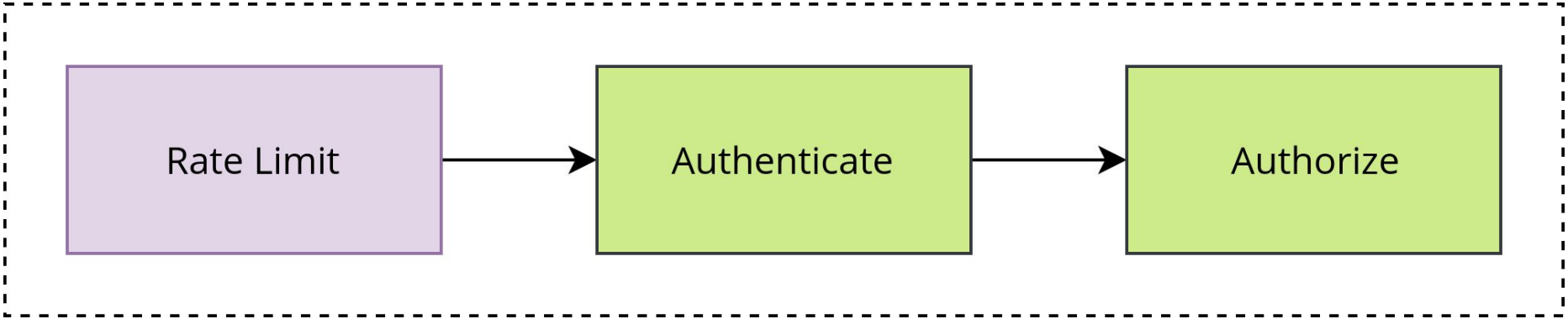
Securing
Cloud-Native Microservices

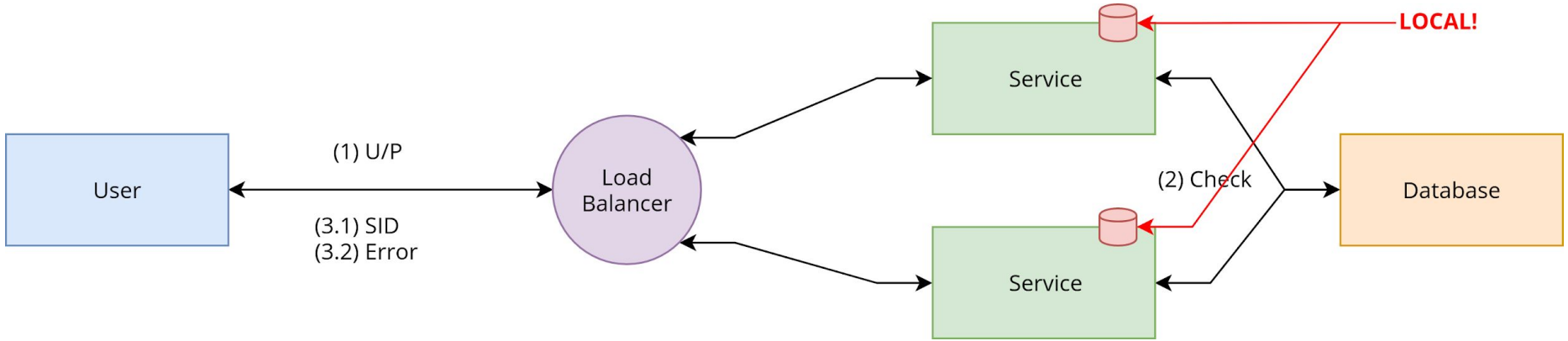
NMWA, FINKI 2020

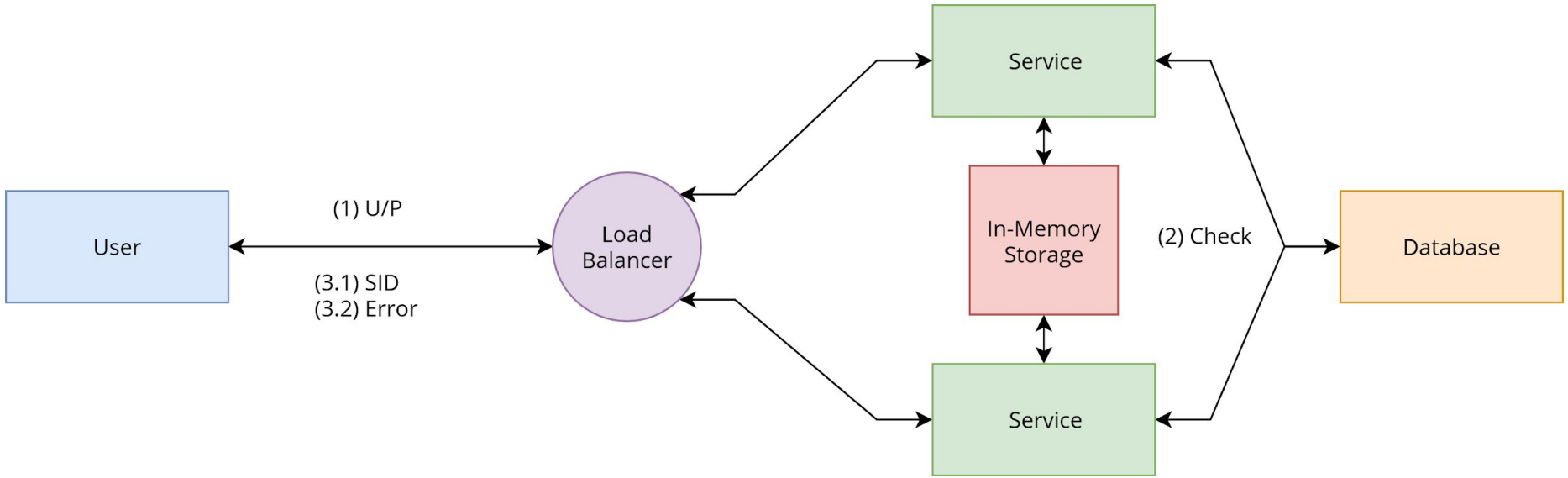
Sasho Najdov

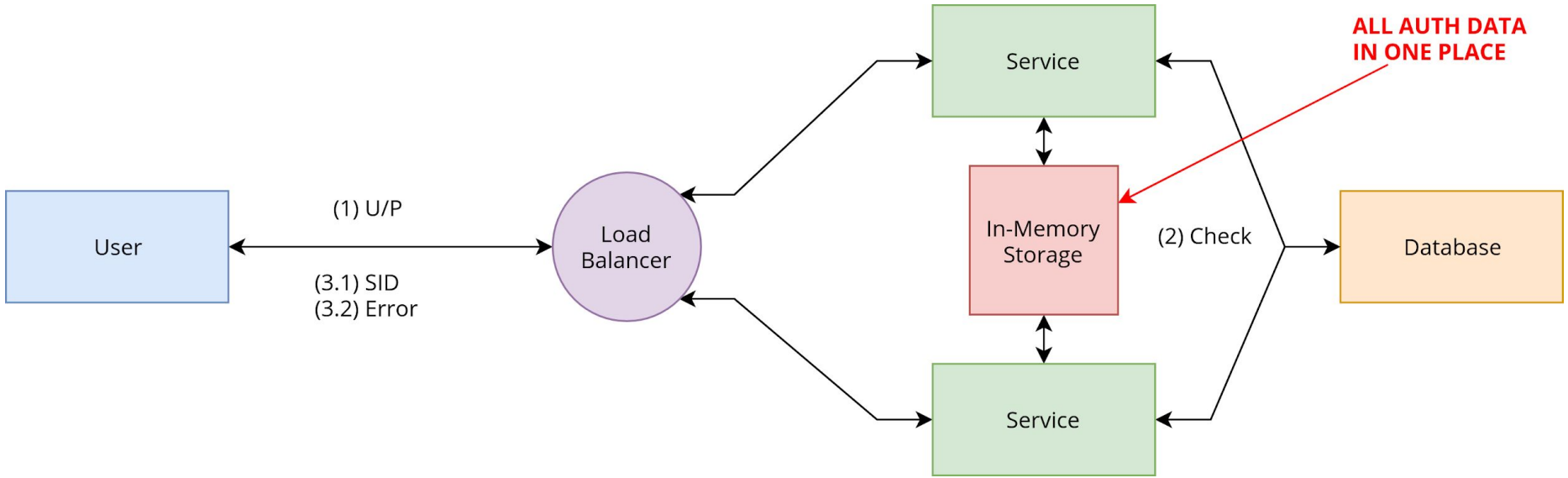
LinkedIn: /sasho-najdov
Website: snajdov.me
Email: snajdov@gmail.com

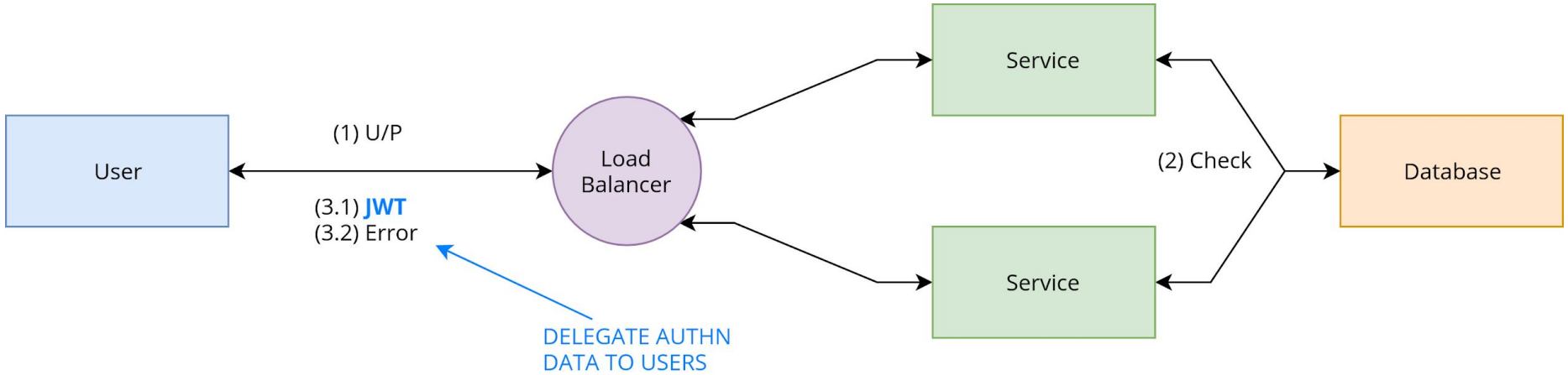

Rate Limit
Authenticate
Authorize


User
(1) U/P
(3.1) SID
(3.2) Error
Service
(2) Check
Database


LOCAL!
Service
User
(1) U/P
Load
Balancer
(2) Check
Database
(3.1) SID
(3.2) Error
Service


Service
User
(1) U/P
(3.1) SID
(3.2) Error
Load
Balancer
In-Memory
Storage
(2) Check
Database
Service


Service
ALL AUTH DATA
IN ONE PLACE
User
(1) U/P
(3.1) SID
(3.2) Error
Load
Balancer
In-Memory
Storage
(2) Check
Database
Service


User
(1) U/P
(3.1) JWT
(3.2) Error
Load Balancer
Service
Service
(2) Check
Database
DELEGATE AUTHN DATA TO USERS

ALGORITHM HS256

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

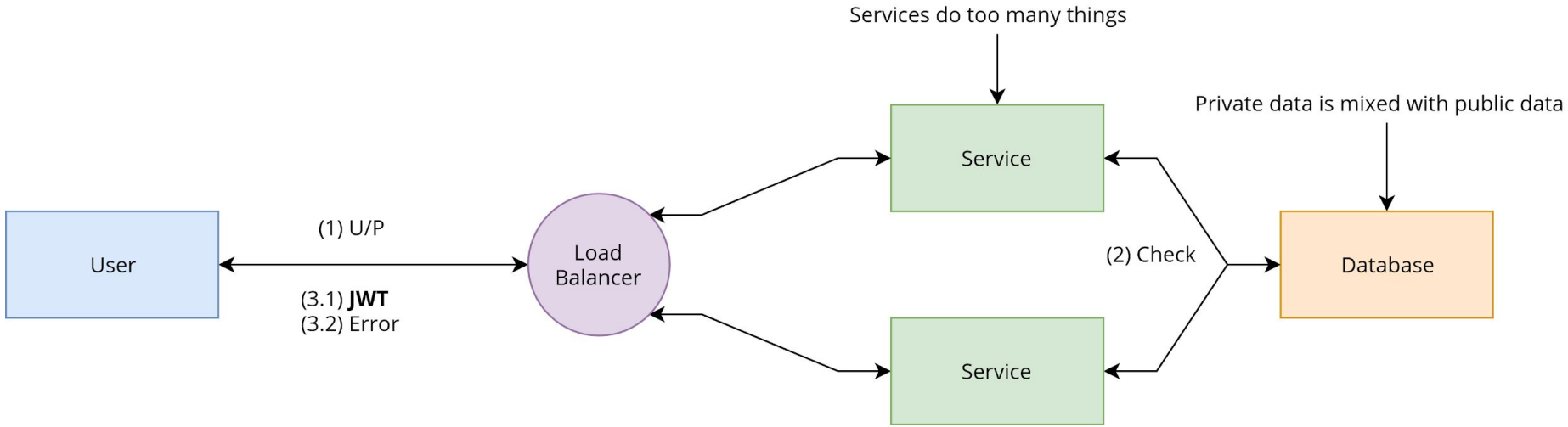
```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

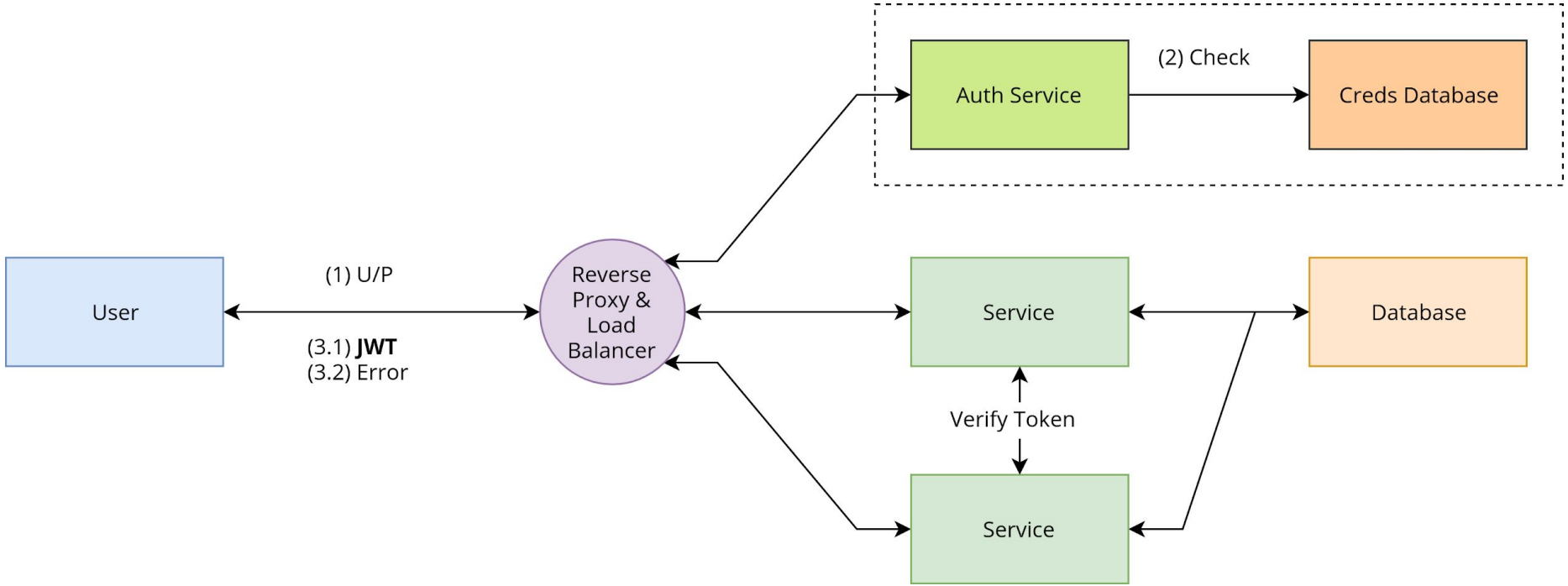
VERIFY SIGNATURE

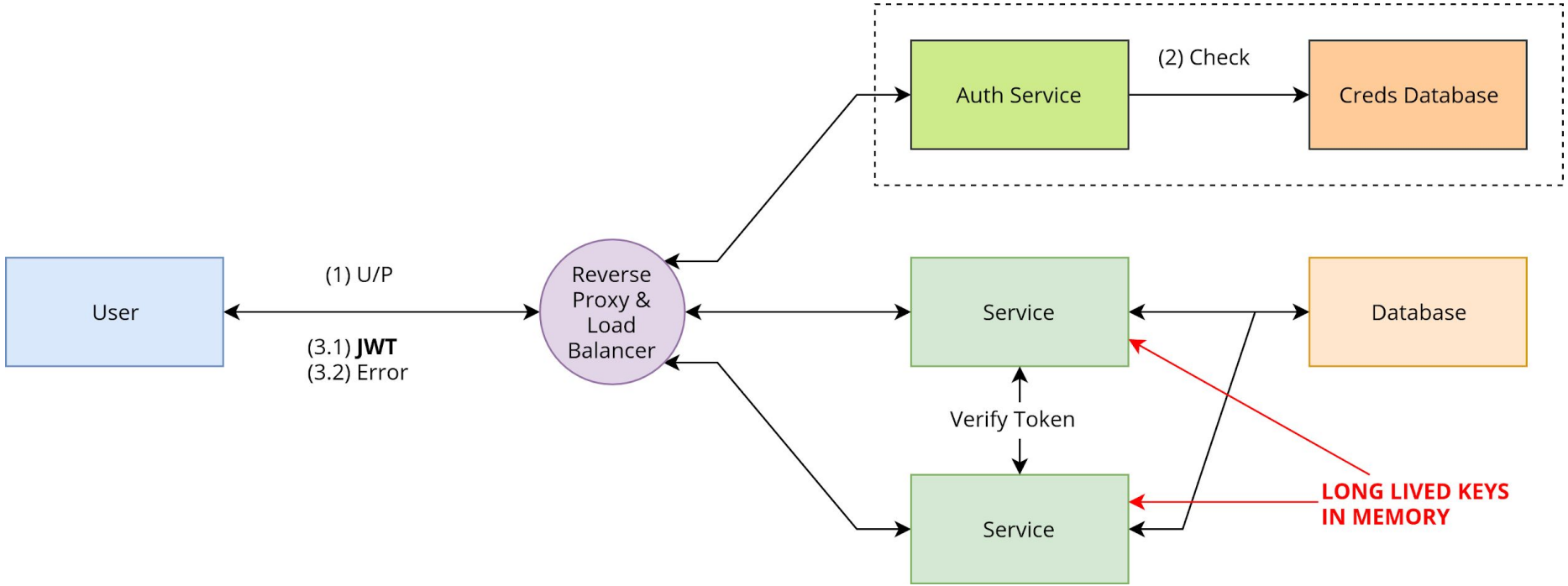
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) secret base64 encoded
```

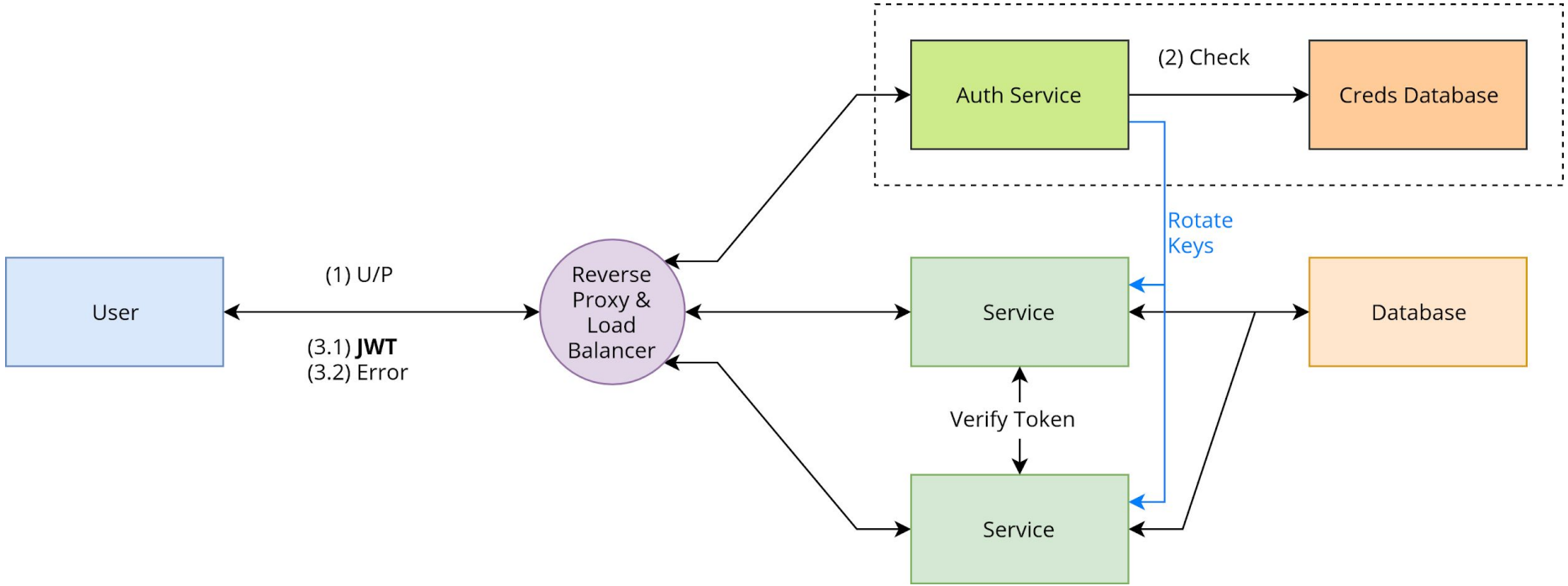
Signature Verified

SHARE JWT


Services do too many things
Private data is mixed with public data
Service
User
(1) U/P
(3.1) JWT
(3.2) Error
Load Balancer
(2) Check
Database
Service


Auth Service
(2) Check
Creds Database
User
(1) U/P
(3.1) JWT
(3.2) Error
Reverse Proxy & Load Balancer
Service
Database
Verify Token
Service


Auth Service
(2) Check
Creds Database
User
(1) U/P
(3.1) JWT
(3.2) Error
Reverse Proxy & Load Balancer
Service
Database
Verify Token
Service
LONG LIVED KEYS IN MEMORY


Auth Service
(2) Check
Creds Database
Rotate
Keys
User
(1) U/P
(3.1) JWT
(3.2) Error
Reverse
Proxy &
Load
Balancer
Service
Database
Verify Token
Service

Encoded PASTE A TOKEN HERE


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtp
ZCI6ImxvYzFmMzJkZjFzeiJ9.eyJzdWIiOiIxMjM
0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF
0IjoxNTE2MjM5MDIyfQ.VcH9jDWzg3nm9YE5qQi8
-kPYjlKW8c_3WSmON4LaVpA
```


Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE


```
{
  "alg": "HS256",
  "typ": "JWT",
  "kid": "loc1f32df1sz"
}
```


PAYLOAD: DATA

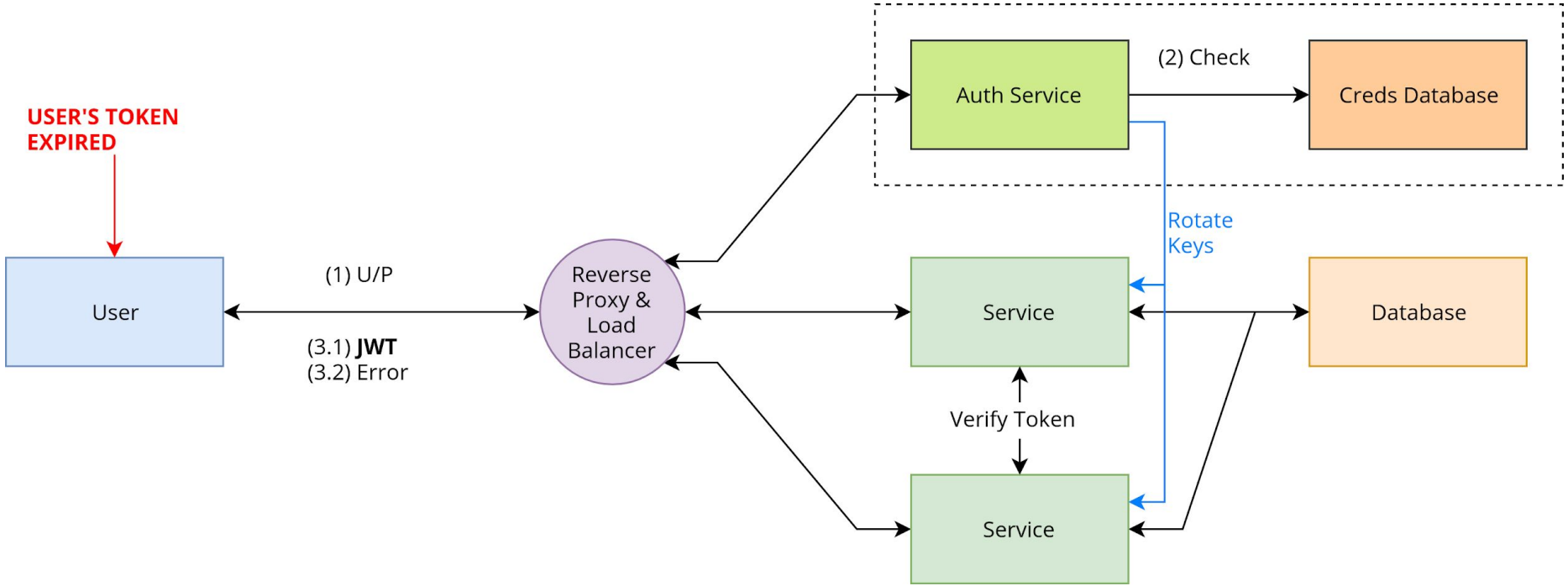

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

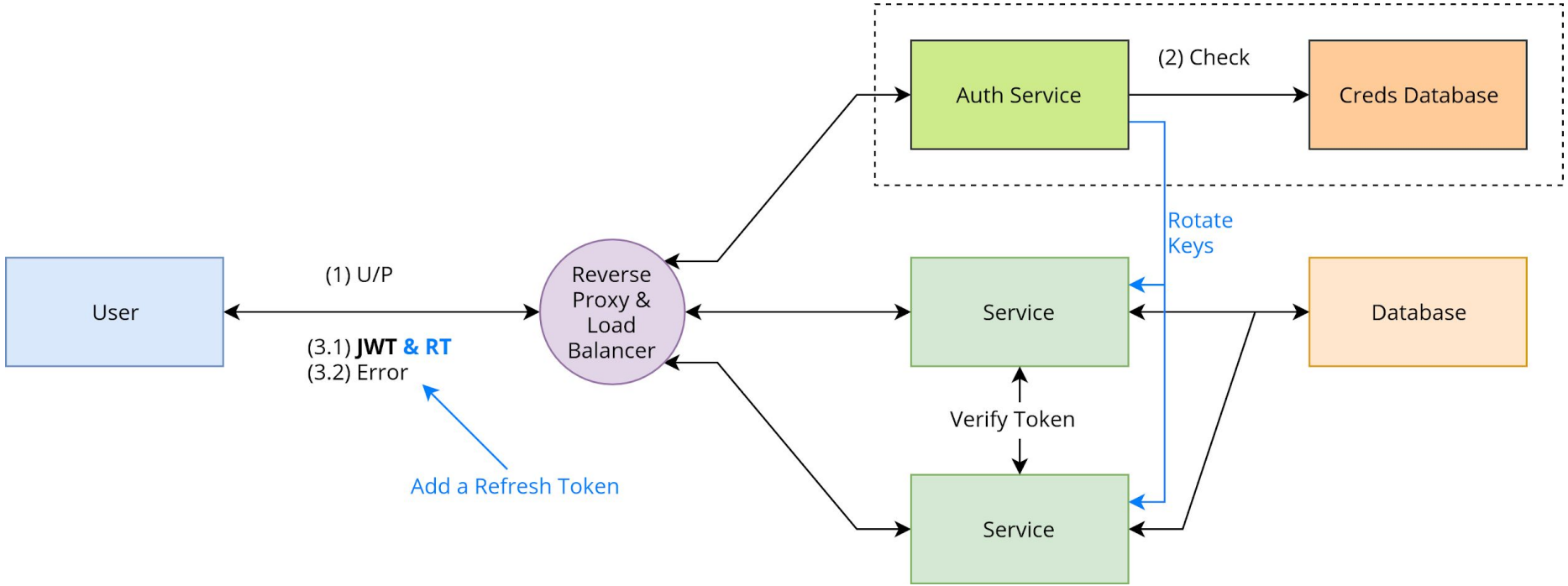

VERIFY SIGNATURE

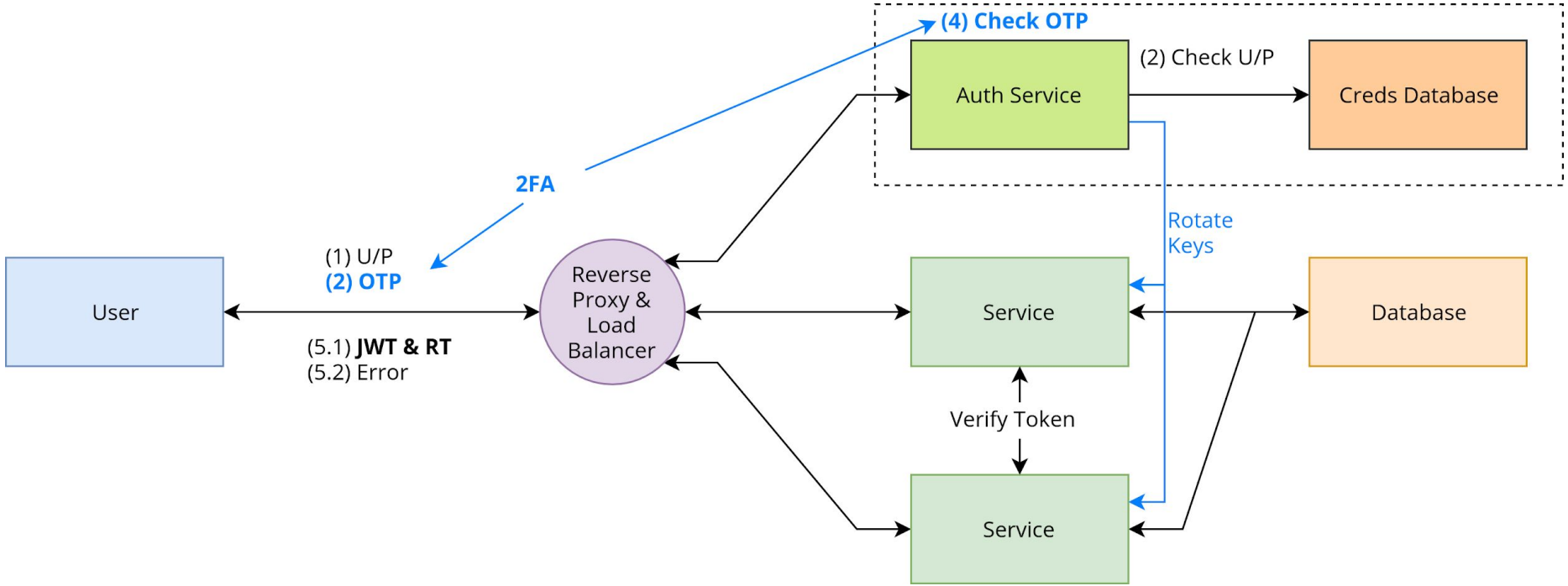
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

Signature Verified

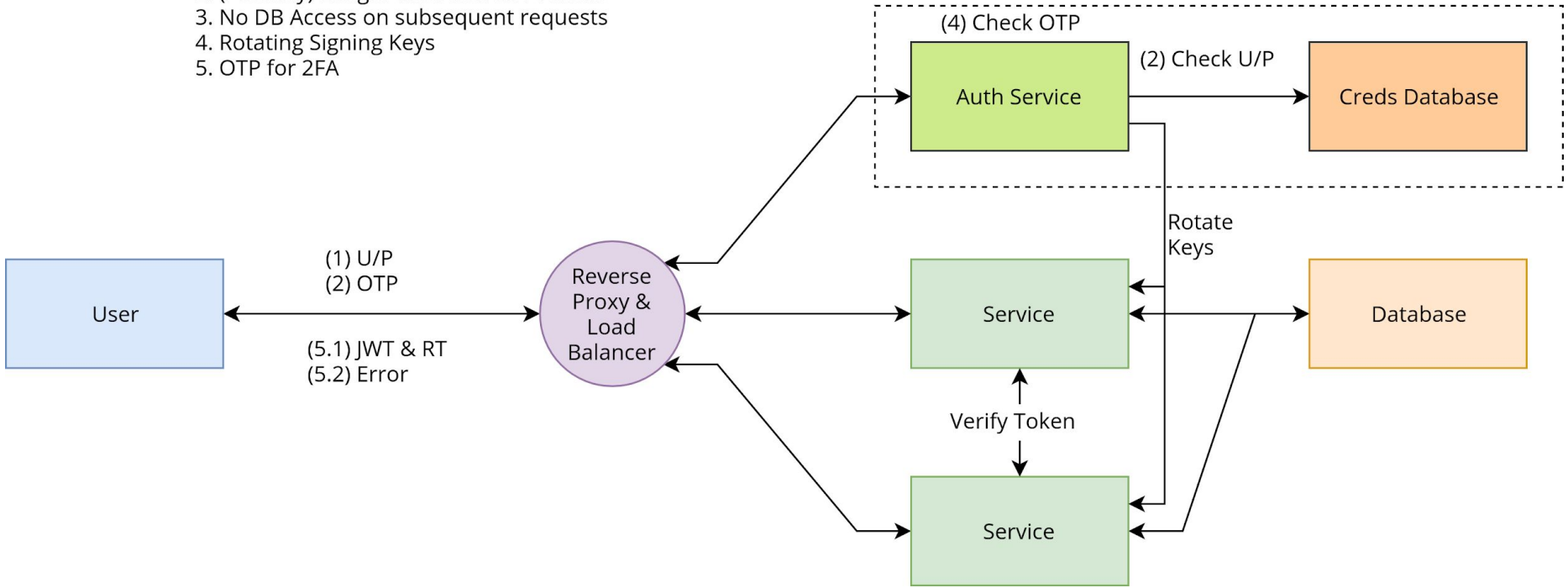
SHARE JWT

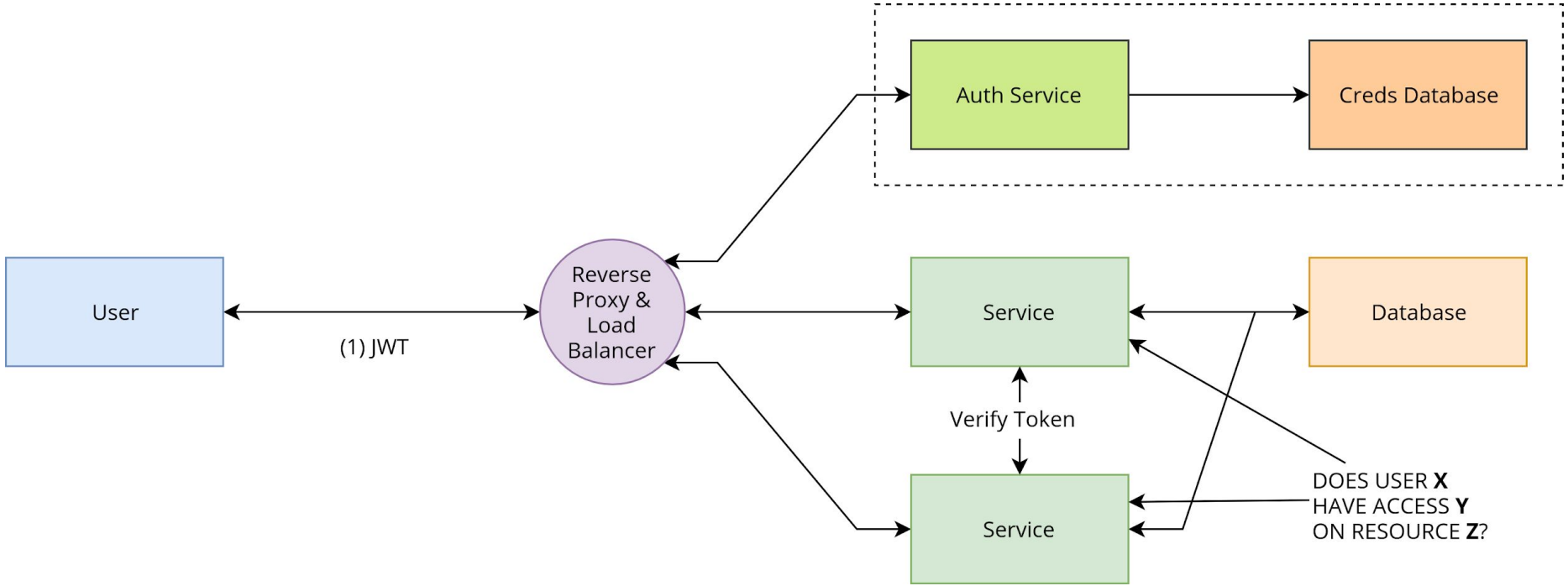

USER'S TOKEN EXPIRED
User
(1) U/P
(3.1) JWT
(3.2) Error
Reverse Proxy & Load Balancer
Auth Service
(2) Check
Creds Database
Rotate Keys
Service
Database
Verify Token
Service

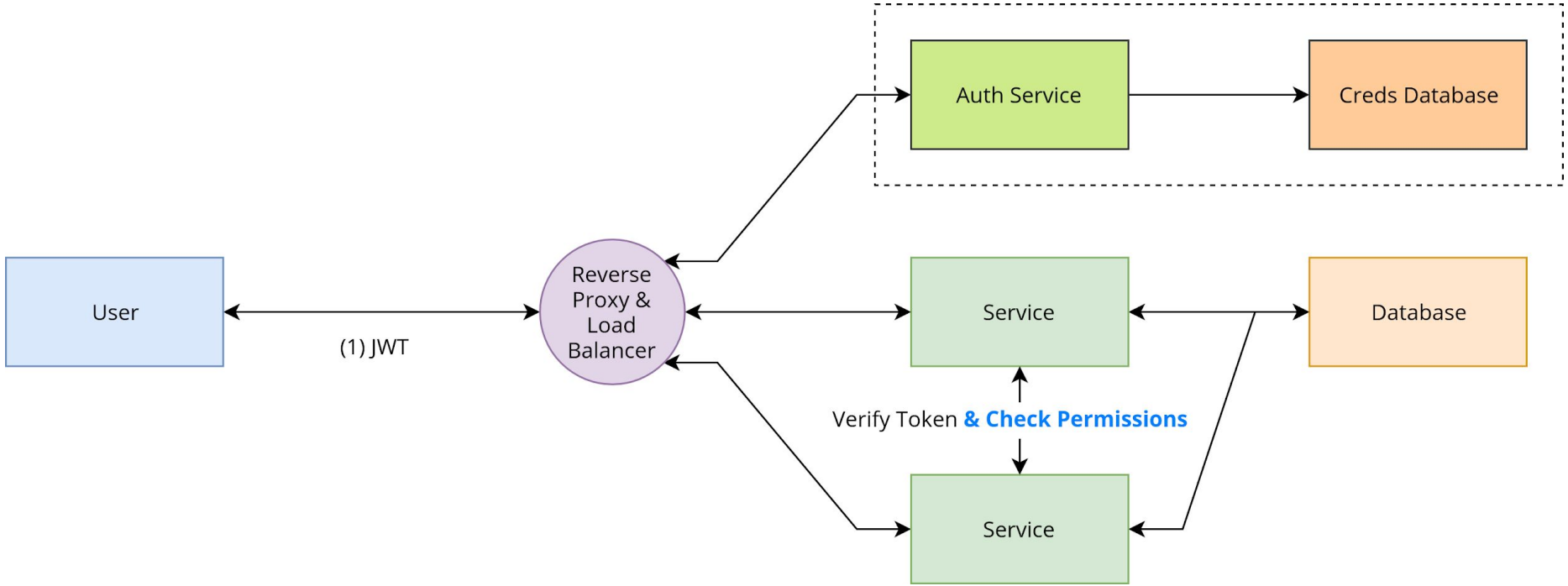

Auth Service
(2) Check
Creds Database
Rotate
Keys
User
(1) U/P
Reverse
Proxy &
Load
Balancer
Service
Database
(3.1) JWT & RT
(3.2) Error
Verify Token
Add a Refresh Token
Service

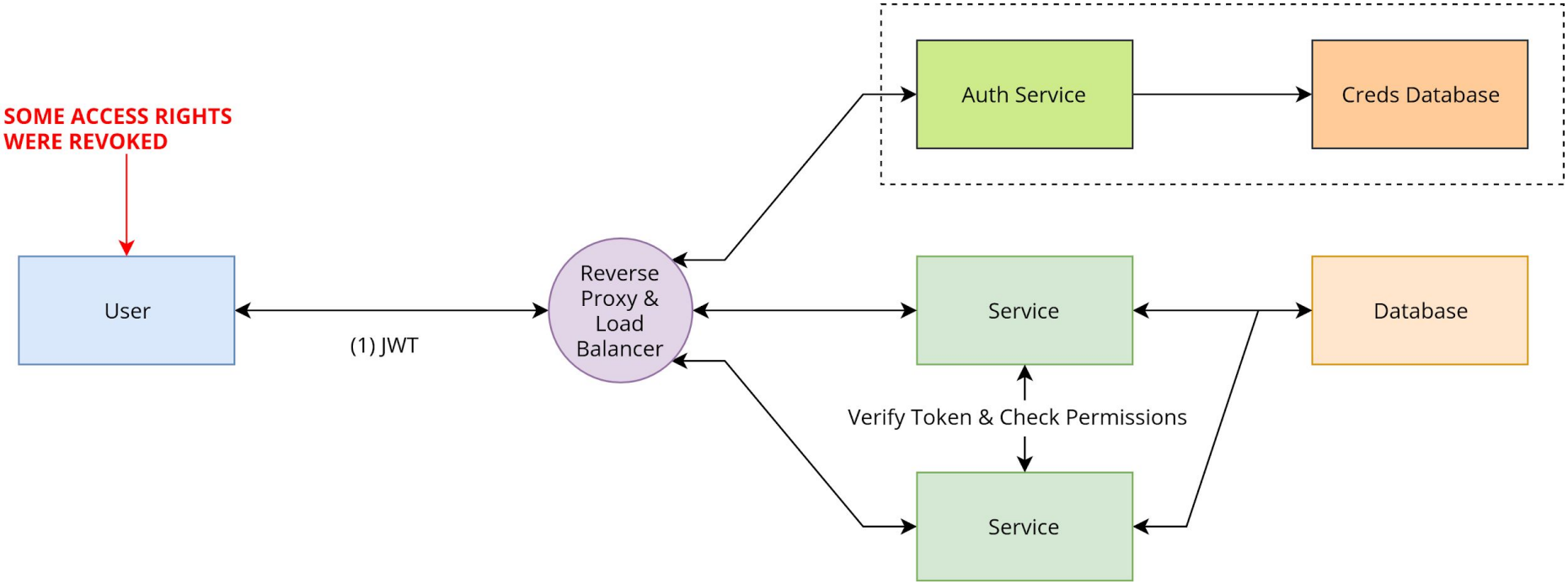

(4) Check OTP
Auth Service
(2) Check U/P
Creds Database
2FA
Rotate
Keys
(1) U/P
(2) OTP
User
Reverse
Proxy &
Load
Balancer
Service
Database
(5.1) JWT & RT
(5.2) Error
Verify Token
Service

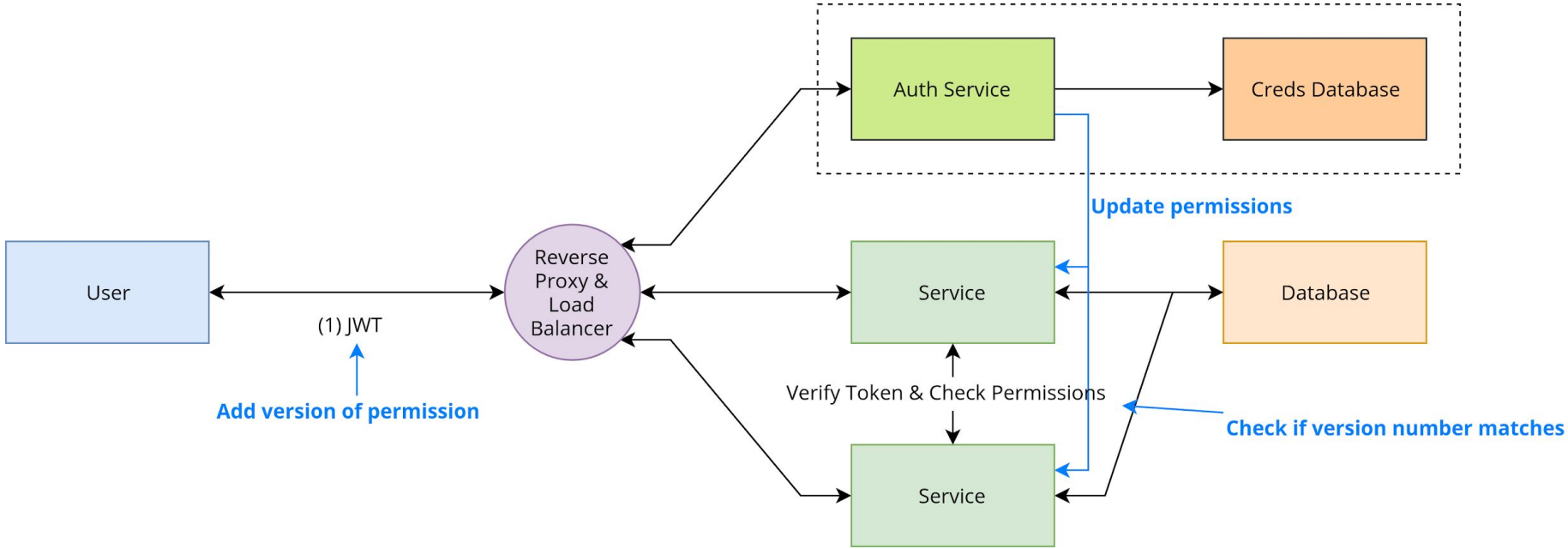
1. Short-lived Tokens
2. (Possibly) Longer-lived Refresh Tokens
3. No DB Access on subsequent requests
4. Rotating Signing Keys
5. OTP for 2FA

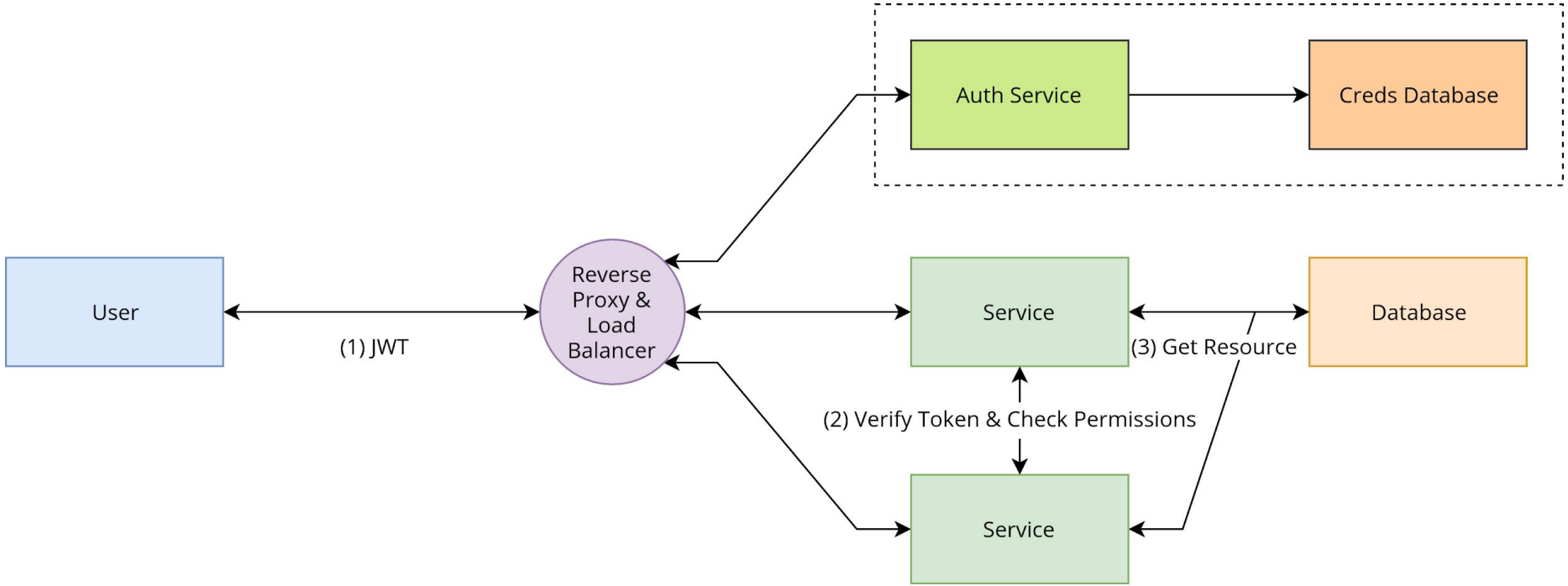



Auth Service
Creds Database
User
(1) JWT
Reverse Proxy & Load Balancer
Service
Database
Verify Token
Service
DOES USER X HAVE ACCESS Y ON RESOURCE Z?

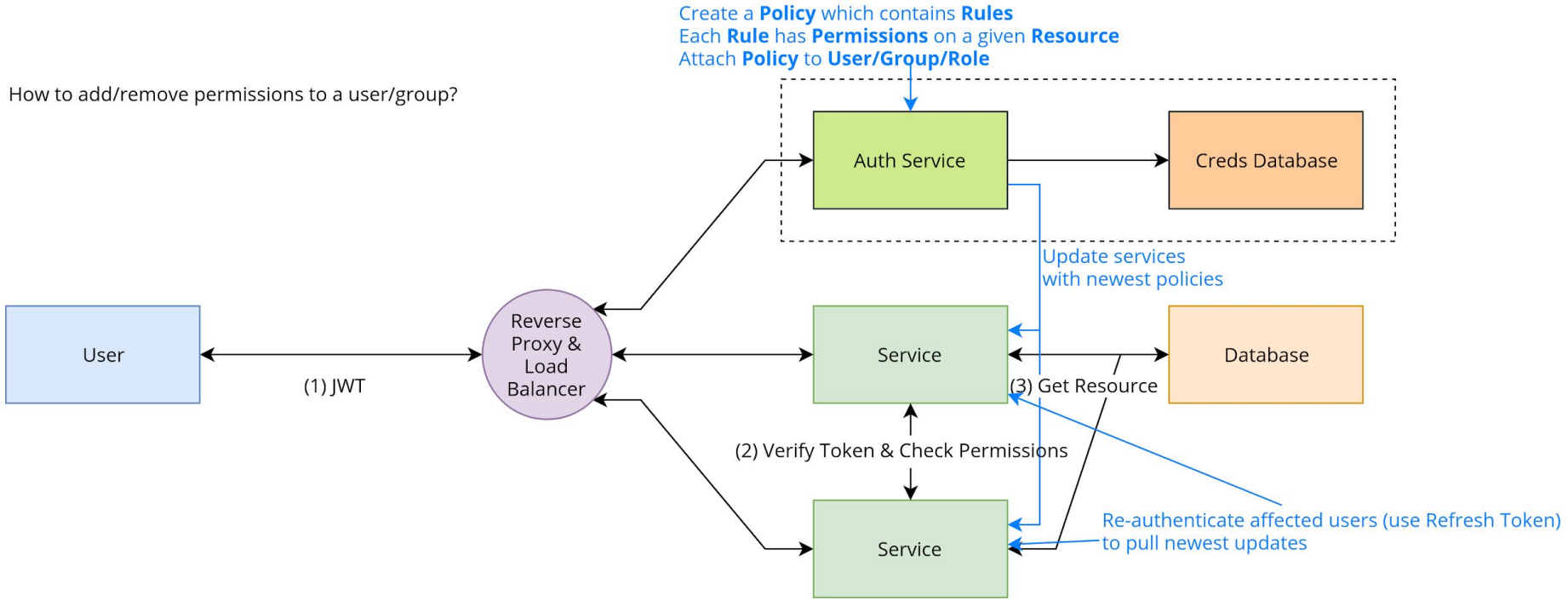

Auth Service
Creds Database
User
Reverse Proxy & Load Balancer
Service
Database
(1) JWT
Verify Token & Check Permissions
Service


SOME ACCESS RIGHTS
WERE REVOKED
User
(1) JWT
Reverse
Proxy &
Load
Balancer
Auth Service
Creds Database
Service
Database
Verify Token & Check Permissions
Service

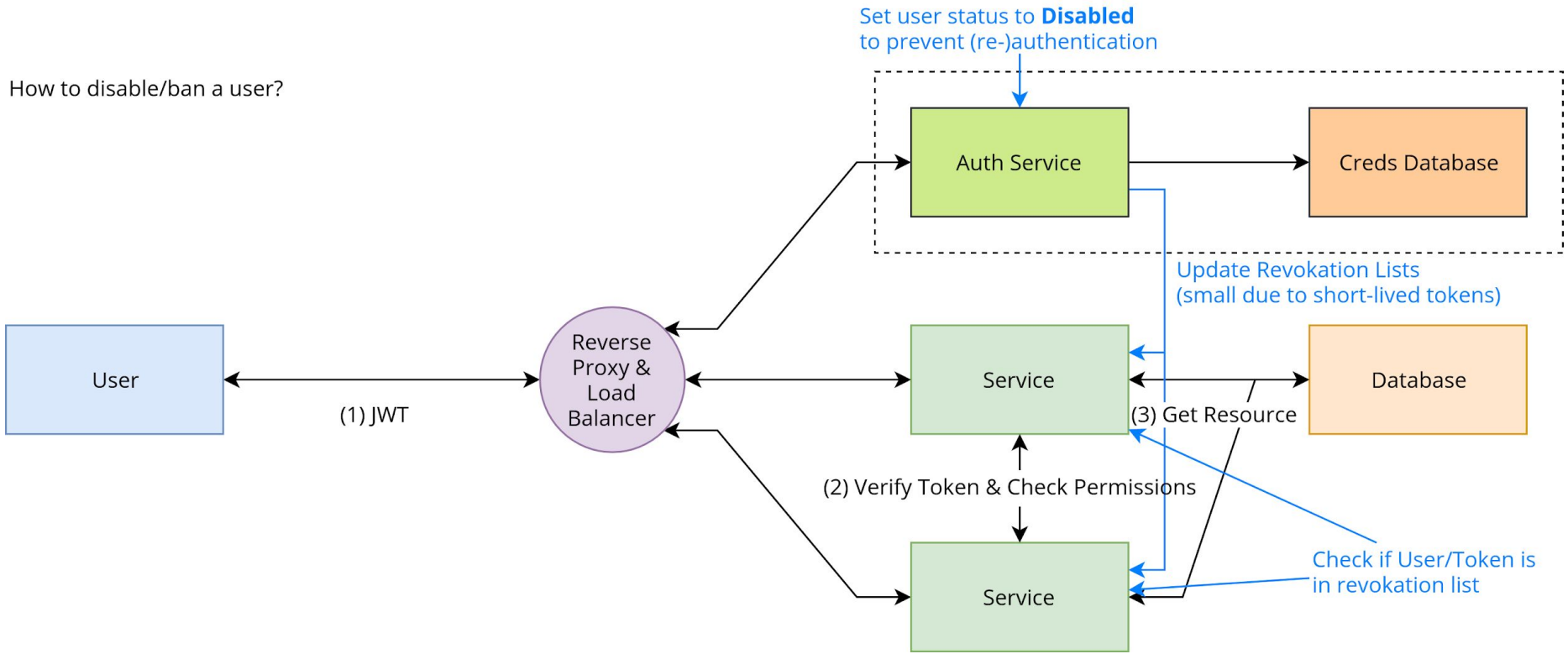

Auth Service
Creds Database
Update permissions
User
Reverse Proxy & Load Balancer
Service
Database
(1) JWT
Add version of permission
Verify Token & Check Permissions
Check if version number matches
Service

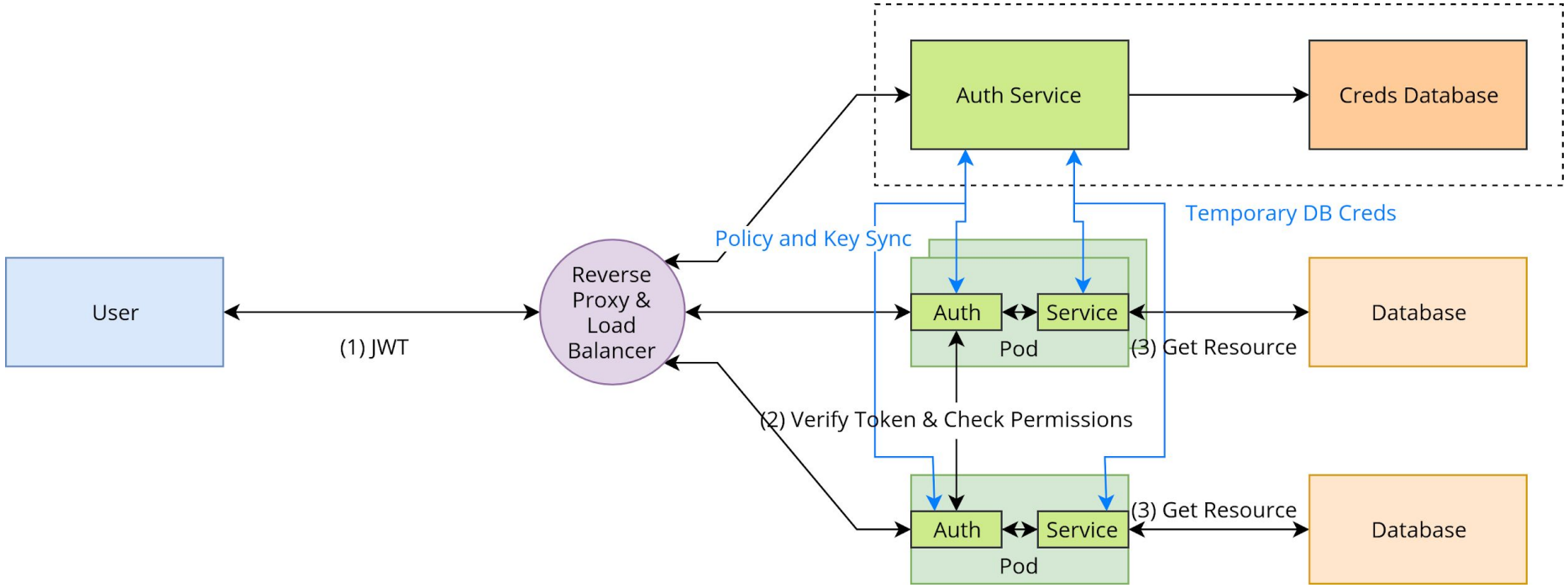

Auth Service
Creds Database
User
Reverse Proxy & Load Balancer
Service
Database
(1) JWT
(3) Get Resource
(2) Verify Token & Check Permissions
Service

How to add/remove permissions to a user/group?

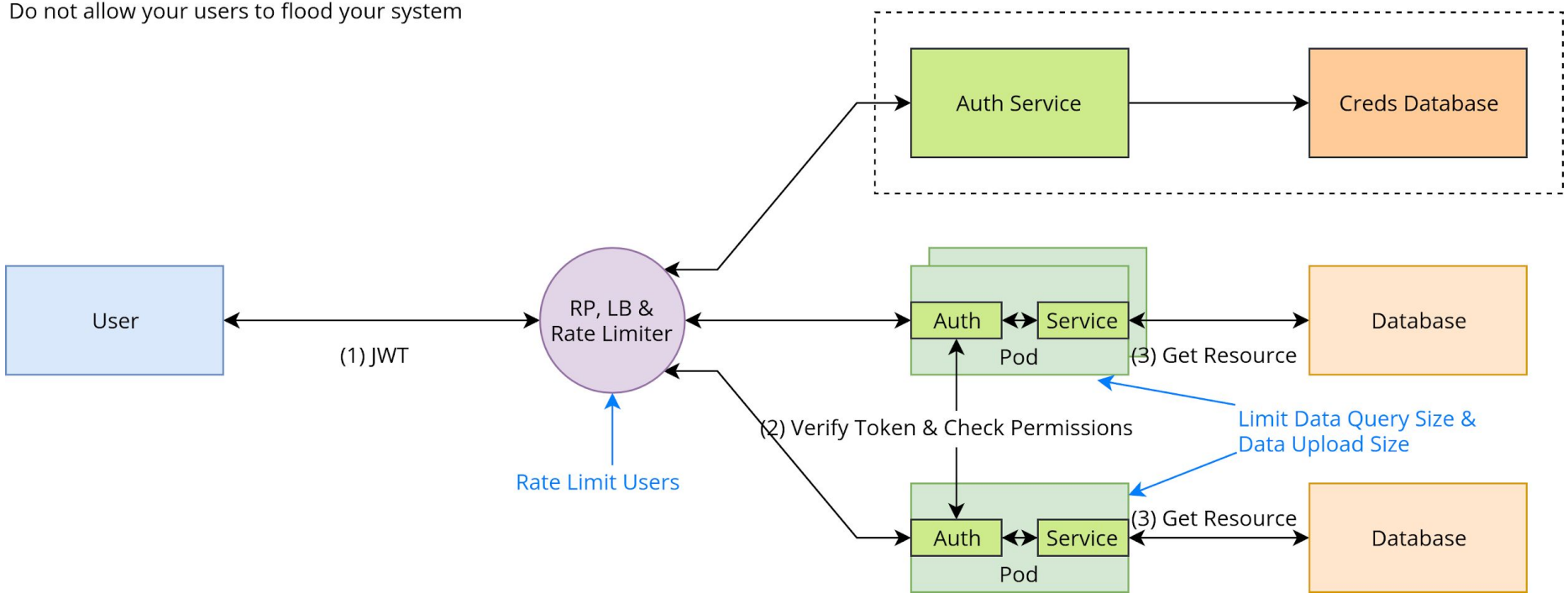


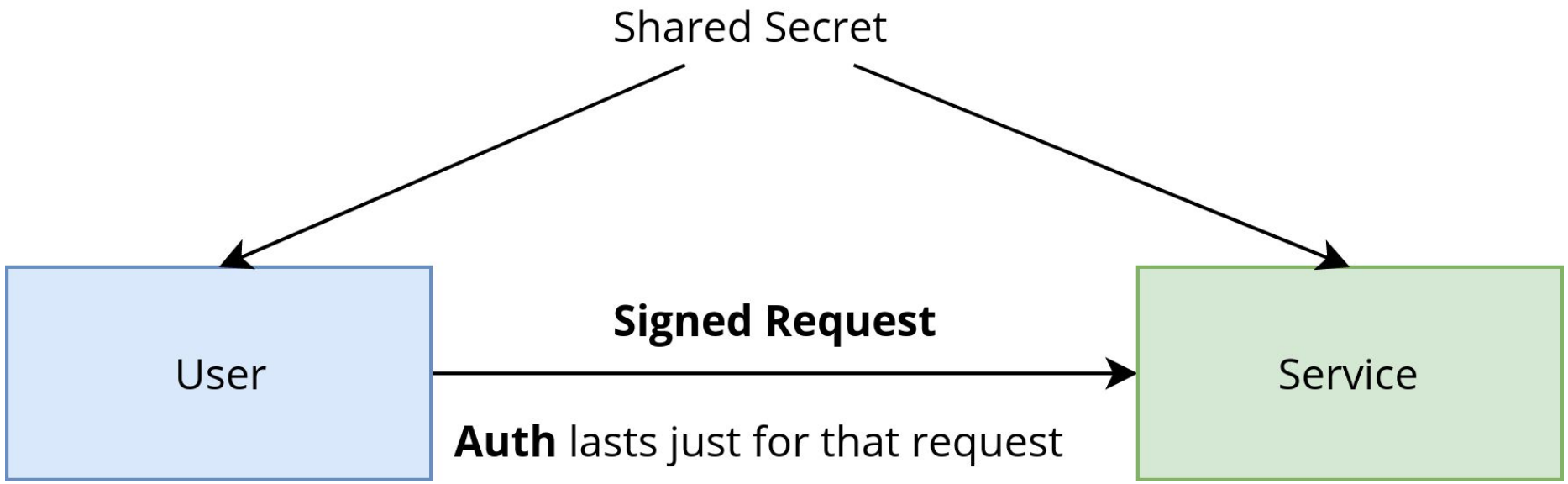
How to disable/ban a user?




Auth Service
Creds Database
Temporary DB Creds
Policy and Key Sync
User
Reverse Proxy & Load Balancer
Auth
Service
Pod
Database
(1) JWT
(3) Get Resource
(2) Verify Token & Check Permissions
Auth
Service
Pod
(3) Get Resource
Database

Do not allow your users to flood your system




Shared Secret
User
Signed Request
Service
Auth lasts just for that request

Resources

1. https://jwt.io/introduction/
2. https://en.wikipedia.org/wiki/JSON_Web_Token
3. https://www.vaultproject.io/
4. https://en.wikipedia.org/wiki/Role-based_access_control
5. https://kubernetes.io/docs/reference/access-authn-authz/rbac/
6. https://auth0.com/docs/authorization/concepts/rbac
7. https://ldapwiki.com/wiki/Neo-Security%20Stack
8. https://19yw4b240vb03ws8qm25h366-wpengine.netdna-ssl.com/wp-content/uploads/securing-the-api-stronghold.pdf
9. https://www.keycdn.com/support/rate-limiting
10. https://cloud.google.com/solutions/rate-limiting-strategies-techniques
11. https://en.wikipedia.org/wiki/Rate_limiting
12. https://tools.ietf.org/id/draft-cavage-http-signatures-08.html
13. https://docs.adobe.com/content/help/en/audience-manager/user-guide/implementation-integration-guides/receiving-audience-data/real-time-outbound-transfers/digitally-signed-http-requests.html
14. https://docs.aws.amazon.com/general/latest/gr/signing_aws_api_requests.html