
AWS
re:Invent

SEC 305

The busy manager's guide to encryption

Spencer Janyk

Senior Product Manager, Tech

AWS

AWS re:Invent

Agenda

Security and defense in depth

Envelope encryption

Asymmetric permissions

Client-side encryption

Building an application

Related session

https://www.youtube.com/watch?v=-ObImxw1PmI

What is security?

Goal

Reduce risk

- Data exposure
- Loss of control

What is security?

Goal

Reduce risk

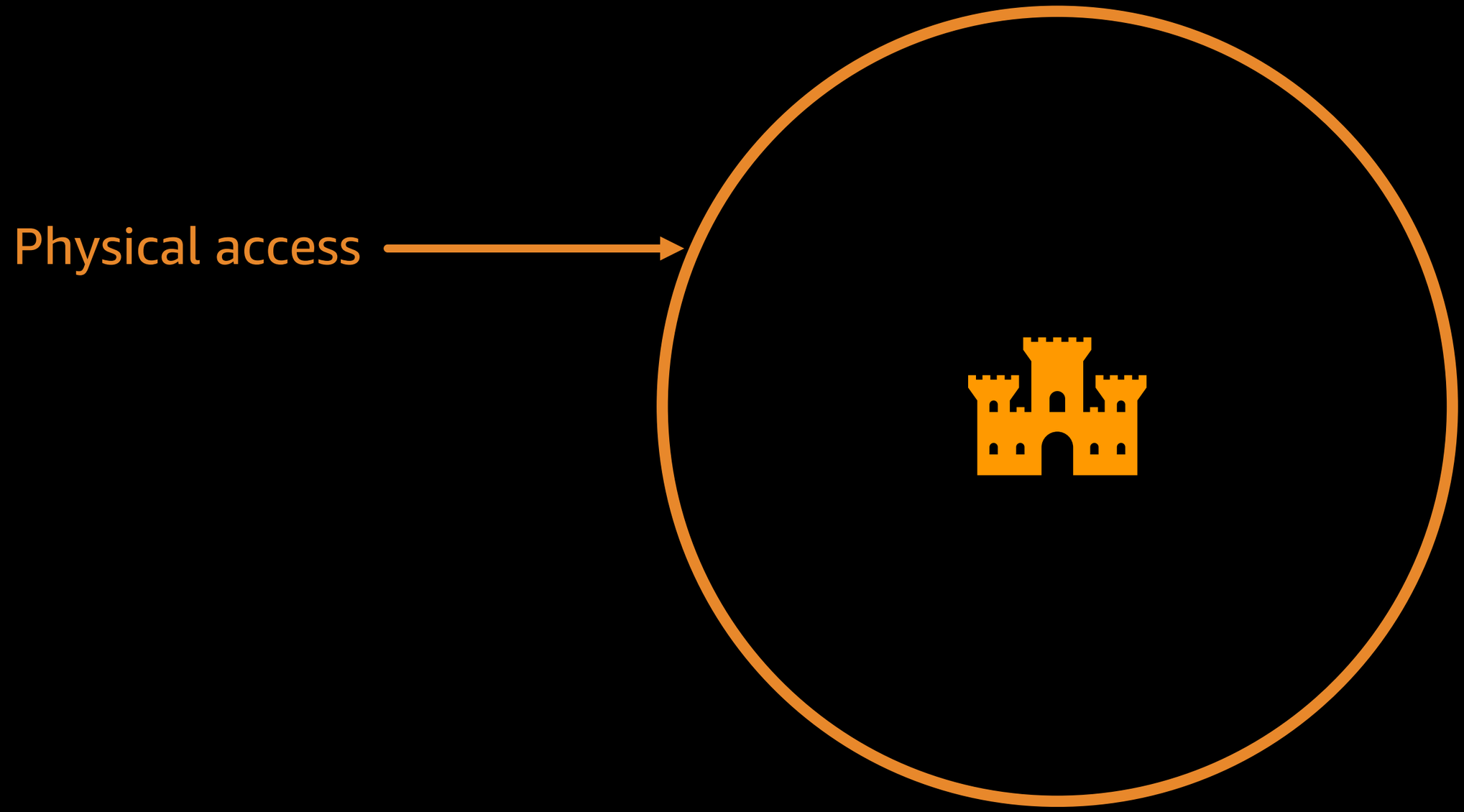
- Data exposure
- Loss of control

Risk types

- Inadvertent
- Malicious

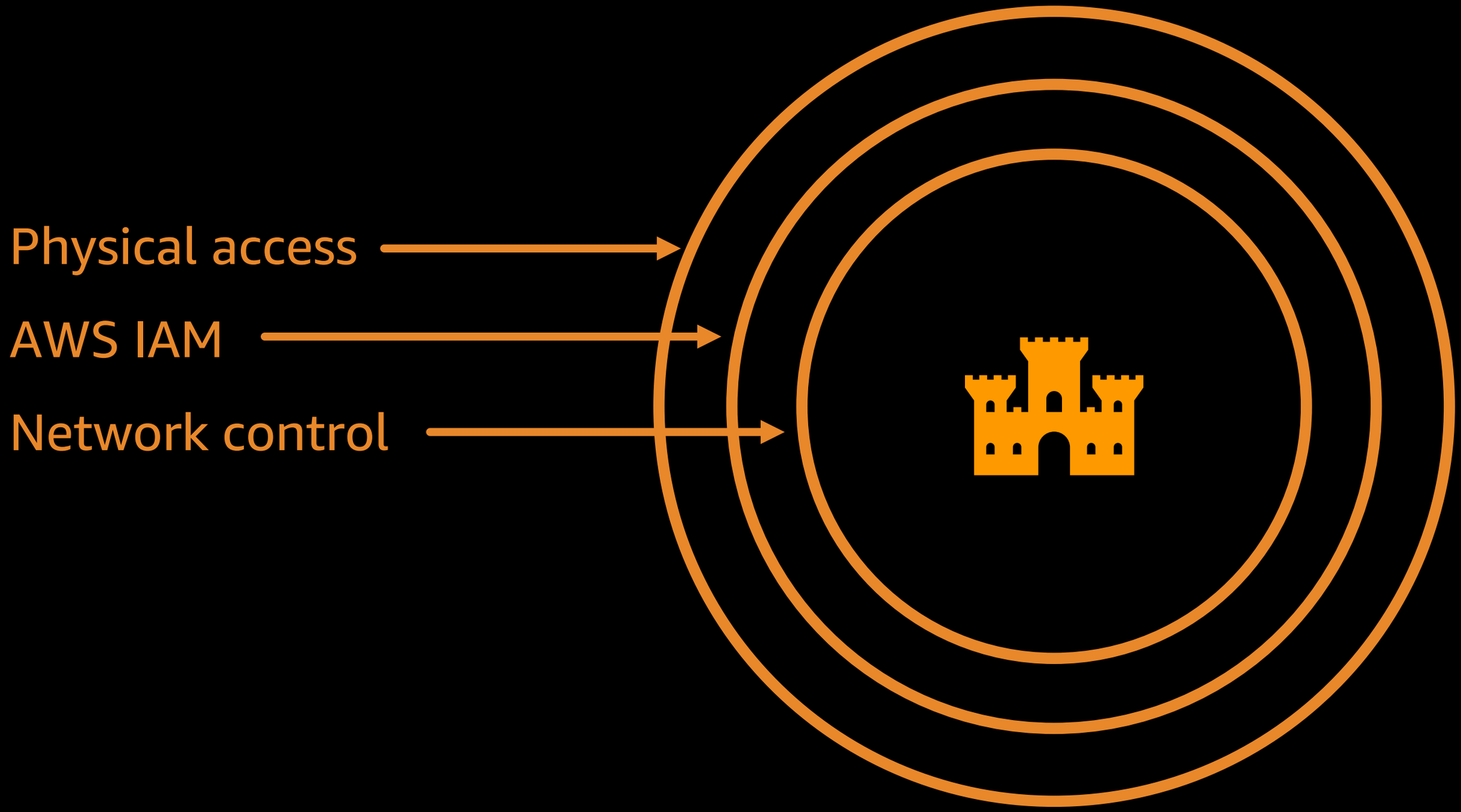
Defense in depth

Defense in depth

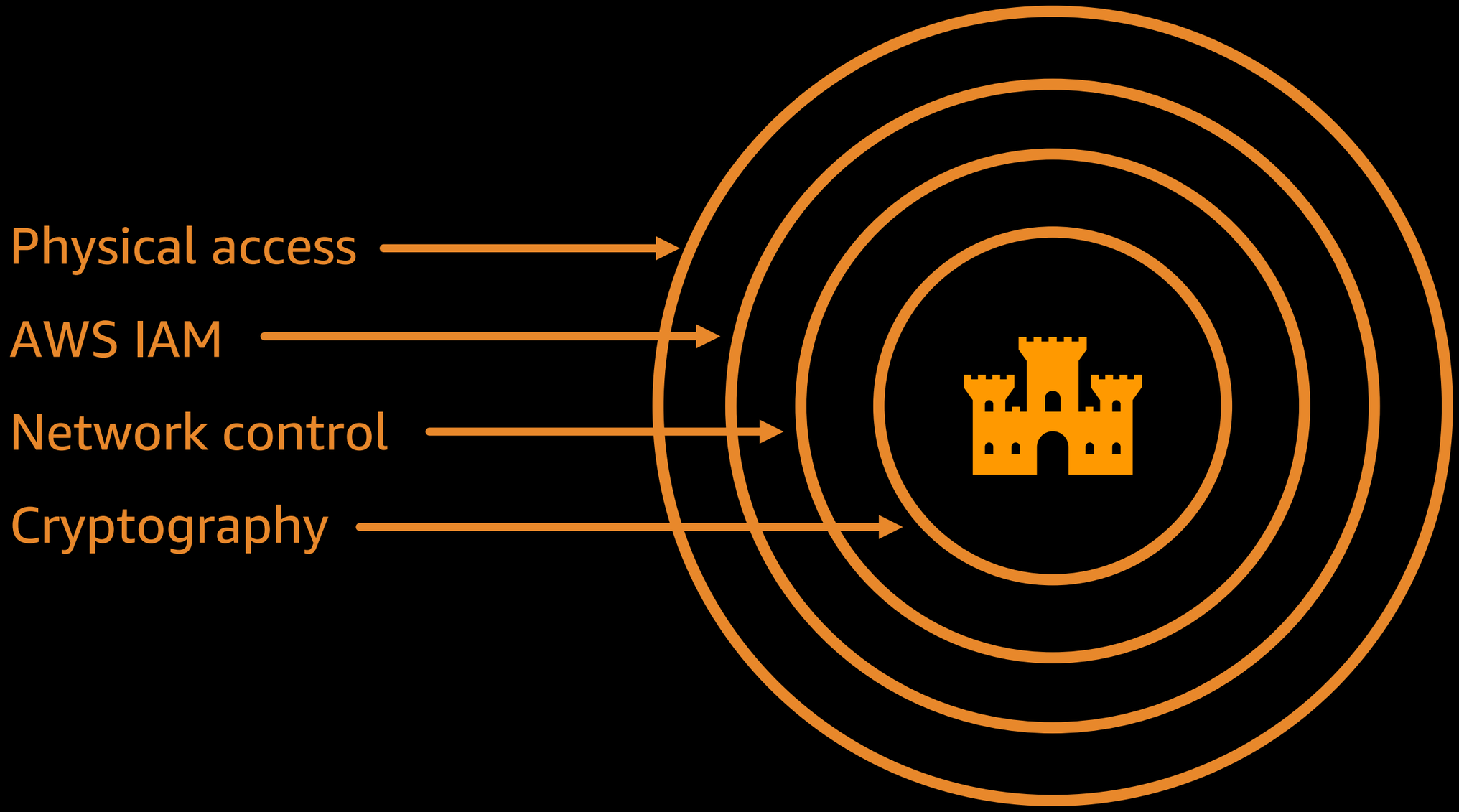


Defense in depth

Defense in depth



Defense in depth



Defense in depth

Why encrypt?

- Keep data confidential
- Demonstrate compliance
- Improve agility

Paving the trusted path

AWS re:Invent

Paving a trusted path

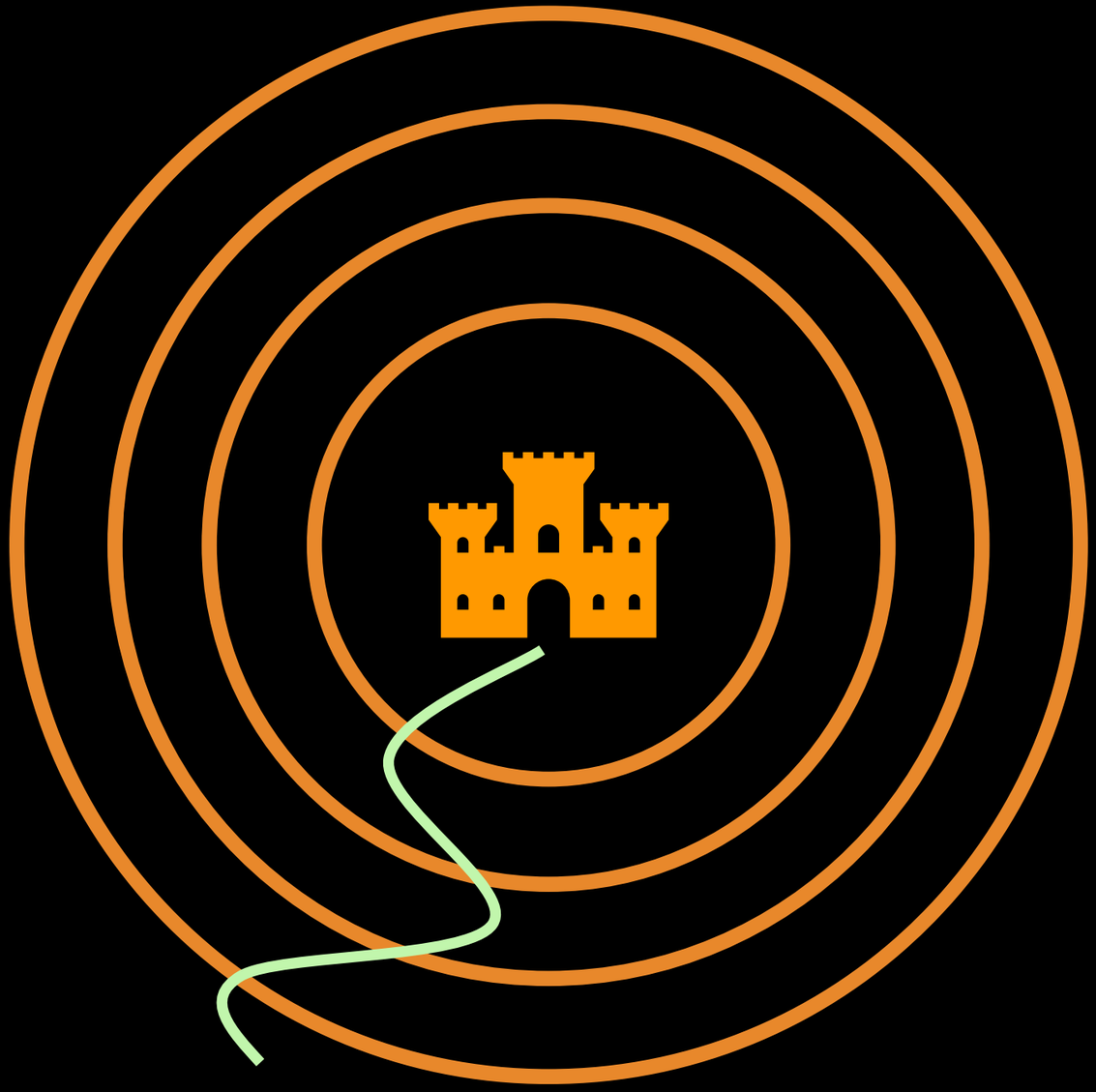
You need to access data (often)

- Read path
- Write path

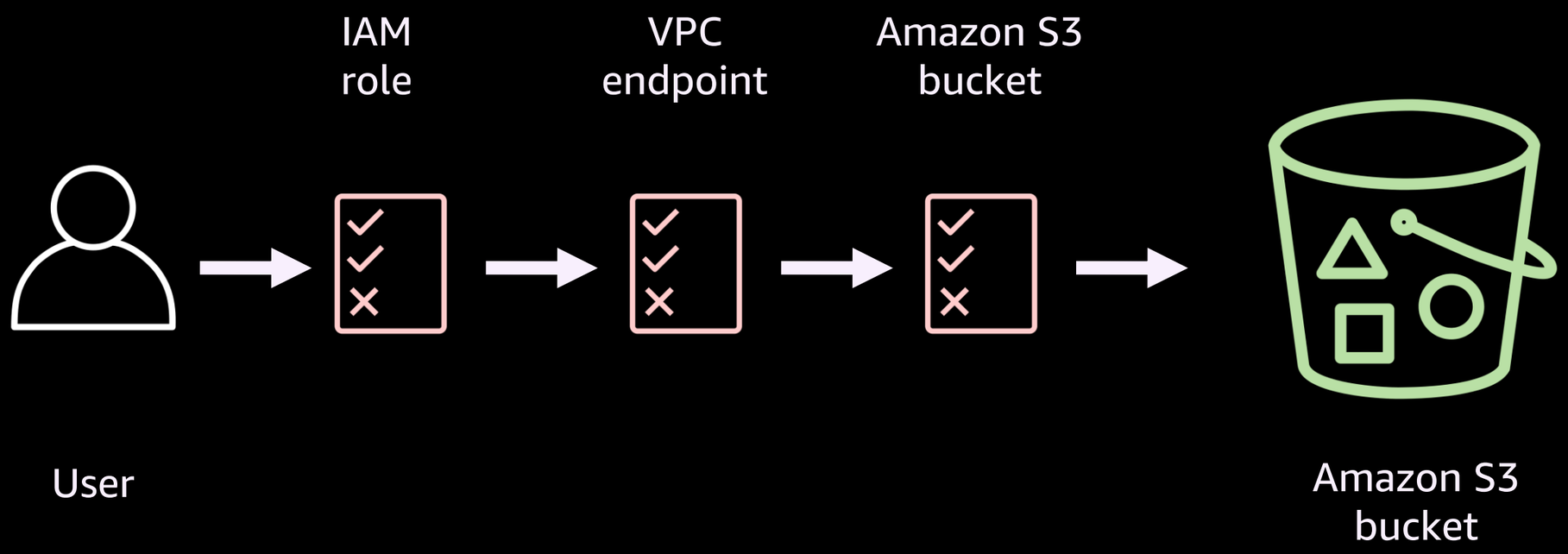
Paving a trusted path

You need to access data (often)

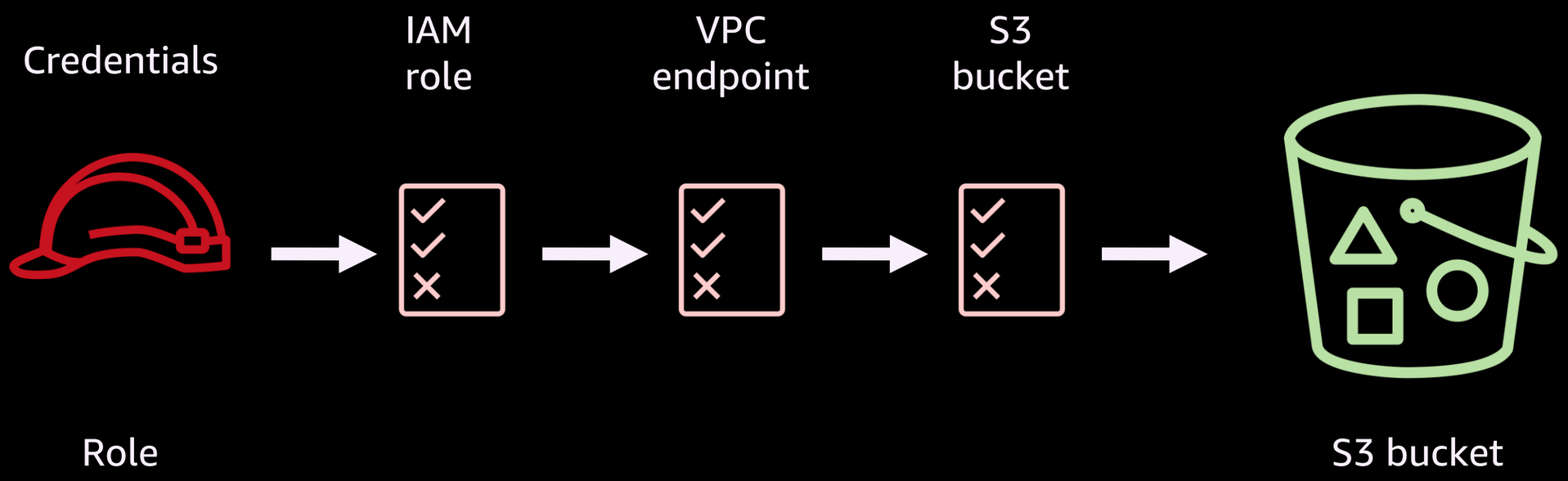
- Read path
- Write path



Defense in depth



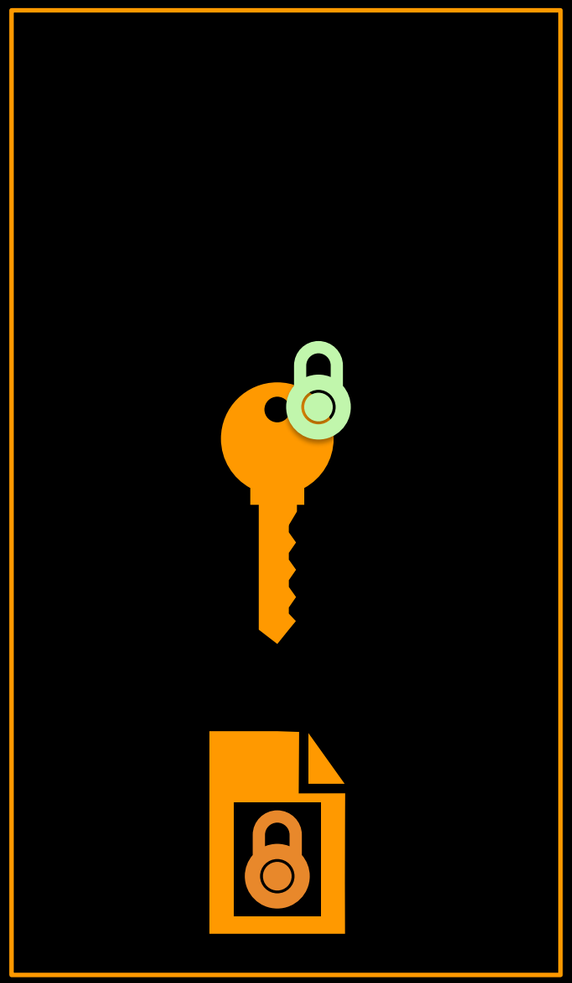
Defense in depth



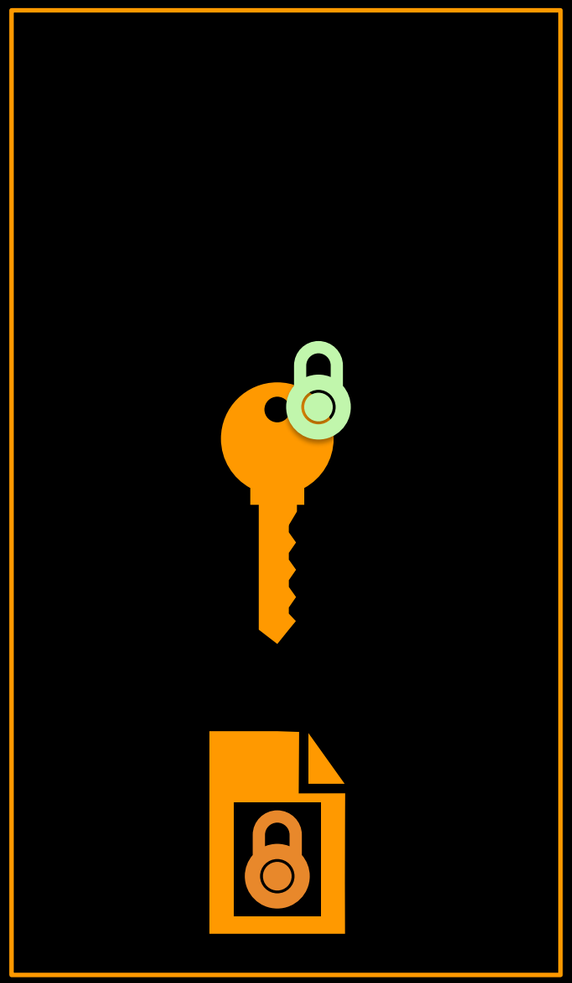
	Permission model	Logging	Complexity
SSE-S3	S3	S3	Low

Envelope encryption

Envelope encryption

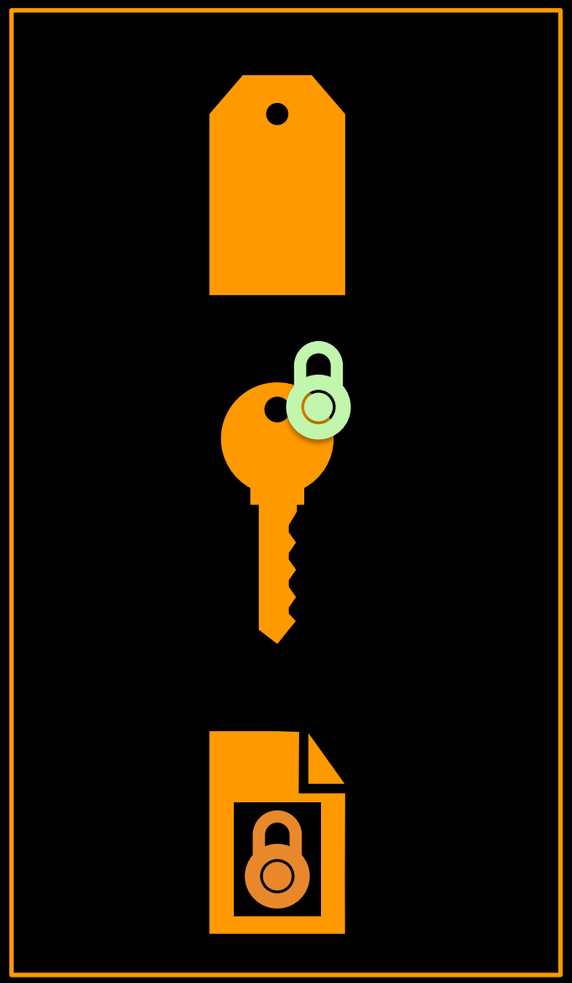


Envelope encryption

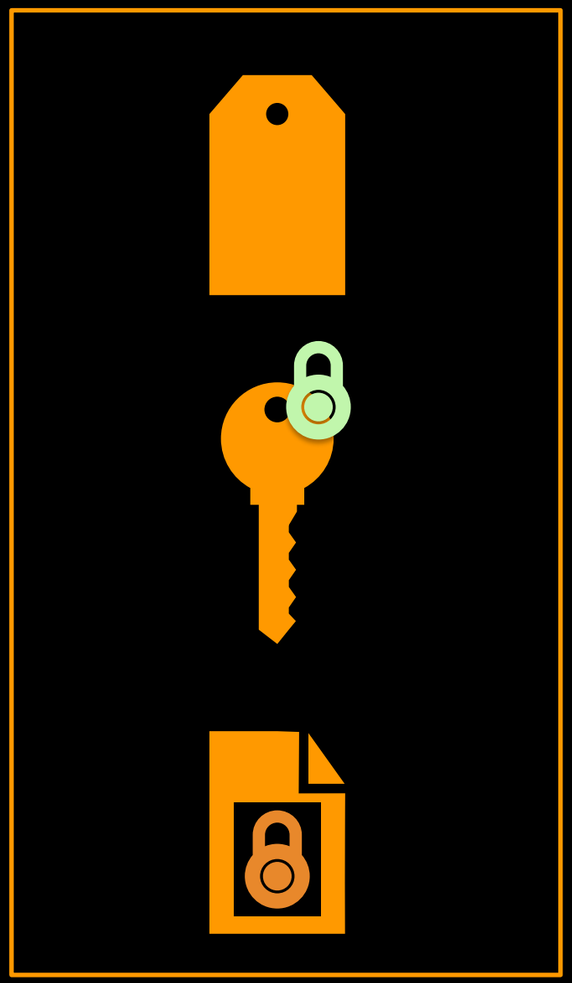


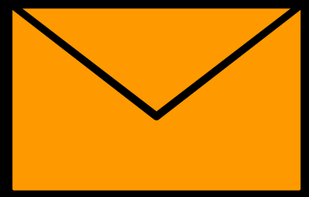
Which key was used to encrypt this key?

Envelope encryption

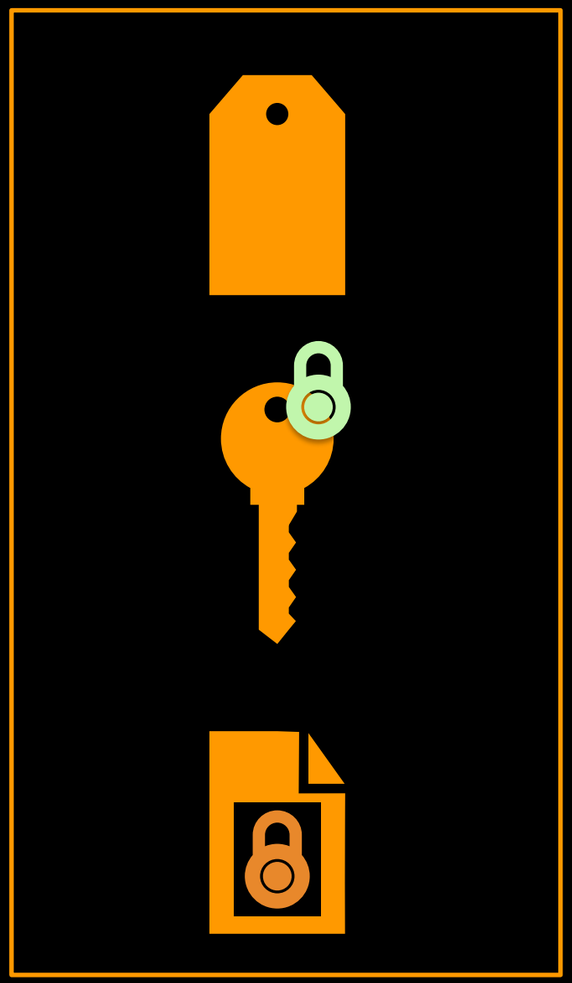


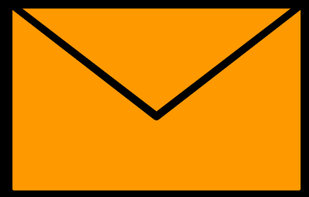
Envelope encryption





Envelope encryption

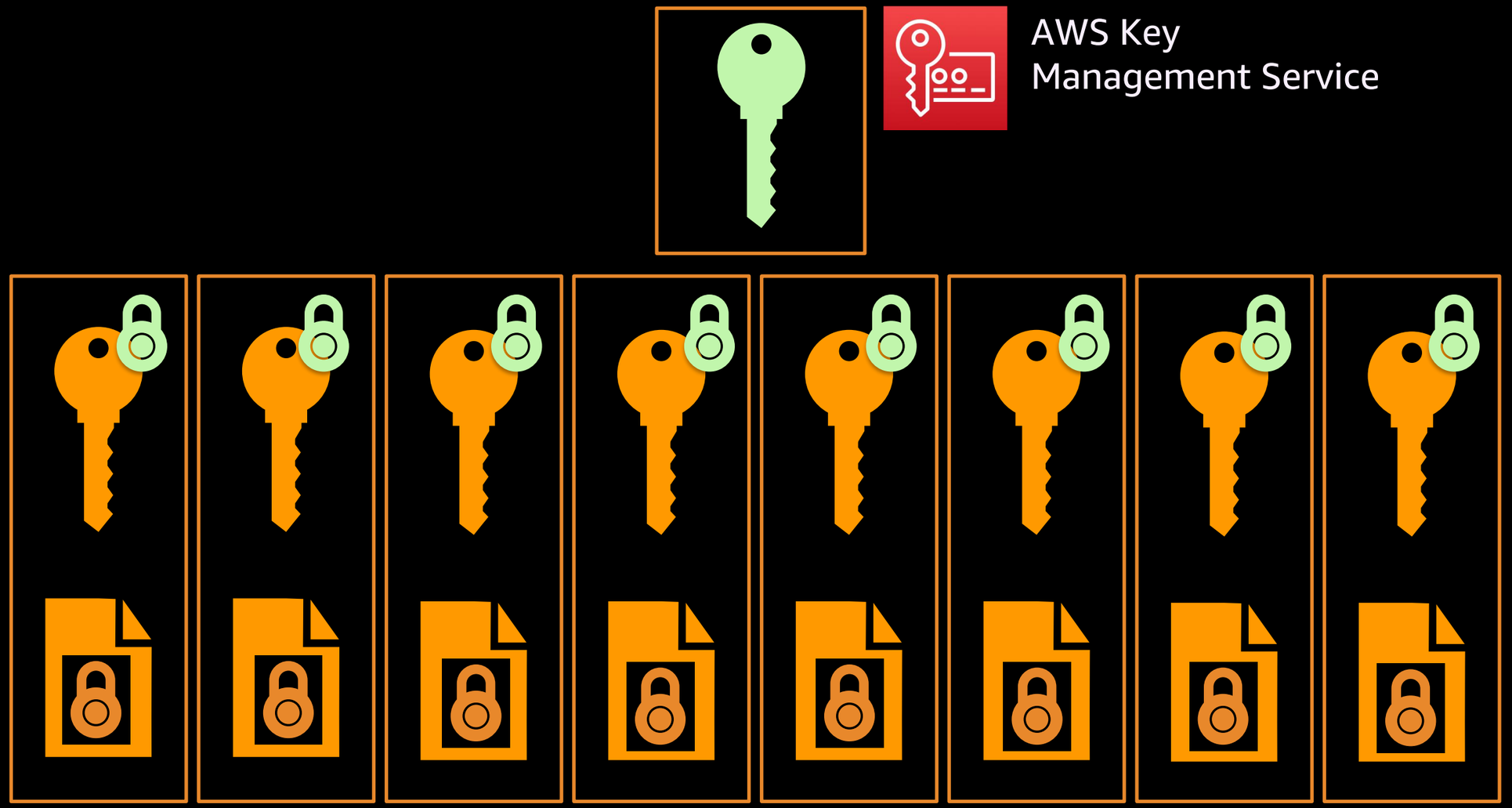




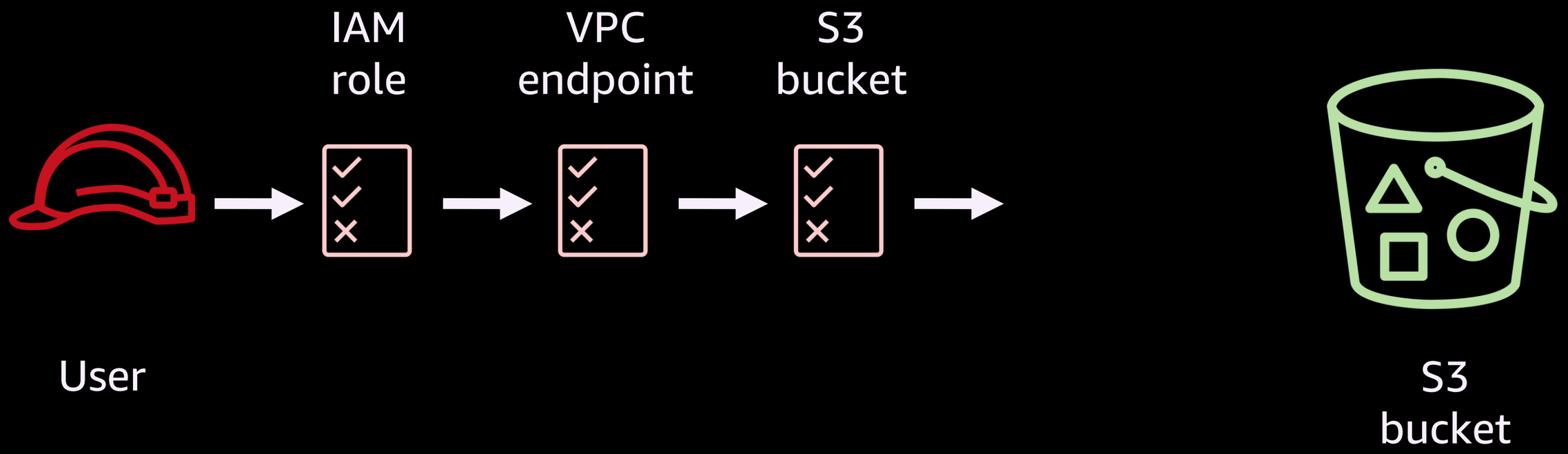
(Not to scale)

Key hierarchy

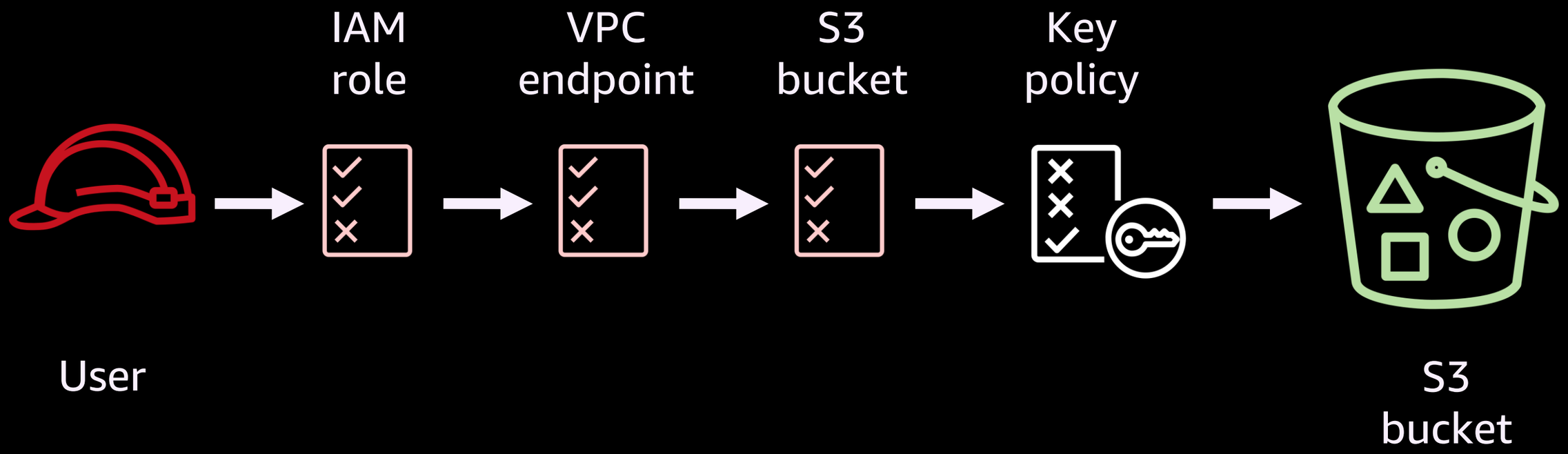
Key hierarchy



Defense in depth



Defense in depth



	Permission model	Logging	Complexity
SSE-S3	S3	S3	Low
SSE-KMS	S3 + KMS	S3 + KMS	Medium

Asymmetric permissions

Policies

IAM policy

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases"
          ],
    "Resource": "*"
     }
}
```

Key policy

Policies

IAM policy

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases"
          ],
    "Resource": "*"
     }
}
```

Key policy

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases"
          ],
    "Resource": "*"
     }
}
```

Policies

Administer

```
"Action": [
            "kms:ListAliases",
            "kms:Create*",
            "kms:Describe*",
            "kms:Enable*",
            "kms:List*",
            "kms:Put*",
            "kms:Update*",
            "kms:Revoke*",
            "kms:Disable*",
            "kms:Get*",
            "kms:Delete*",
            "kms:TagResource",
            "kms:UntagResource",
            "kms:ScheduleKeyDeletion",
            "kms:CancelKeyDeletion"
]
```

Policies

Use

```
"Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
]

…

"Sid": "Allow attachment of
persistent resources",
"Action": [
      "kms:CreateGrant",
      "kms:ListGrants",
      "kms:RevokeGrant"
]
```

Policies

Encrypt

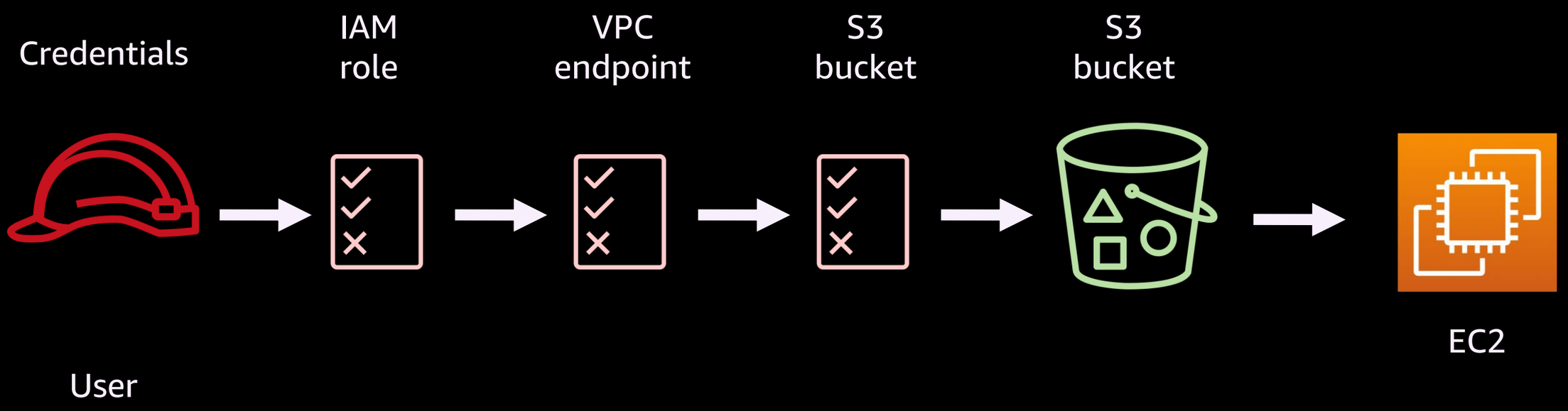
```
"Effect": "Allow",
"Action": [
     "kms:Encrypt",
     "kms:Decrypt",
     "kms:ReEncrypt*",
     "kms:GenerateDataKey*",
     "kms:DescribeKey"
     ]
```

Decrypt

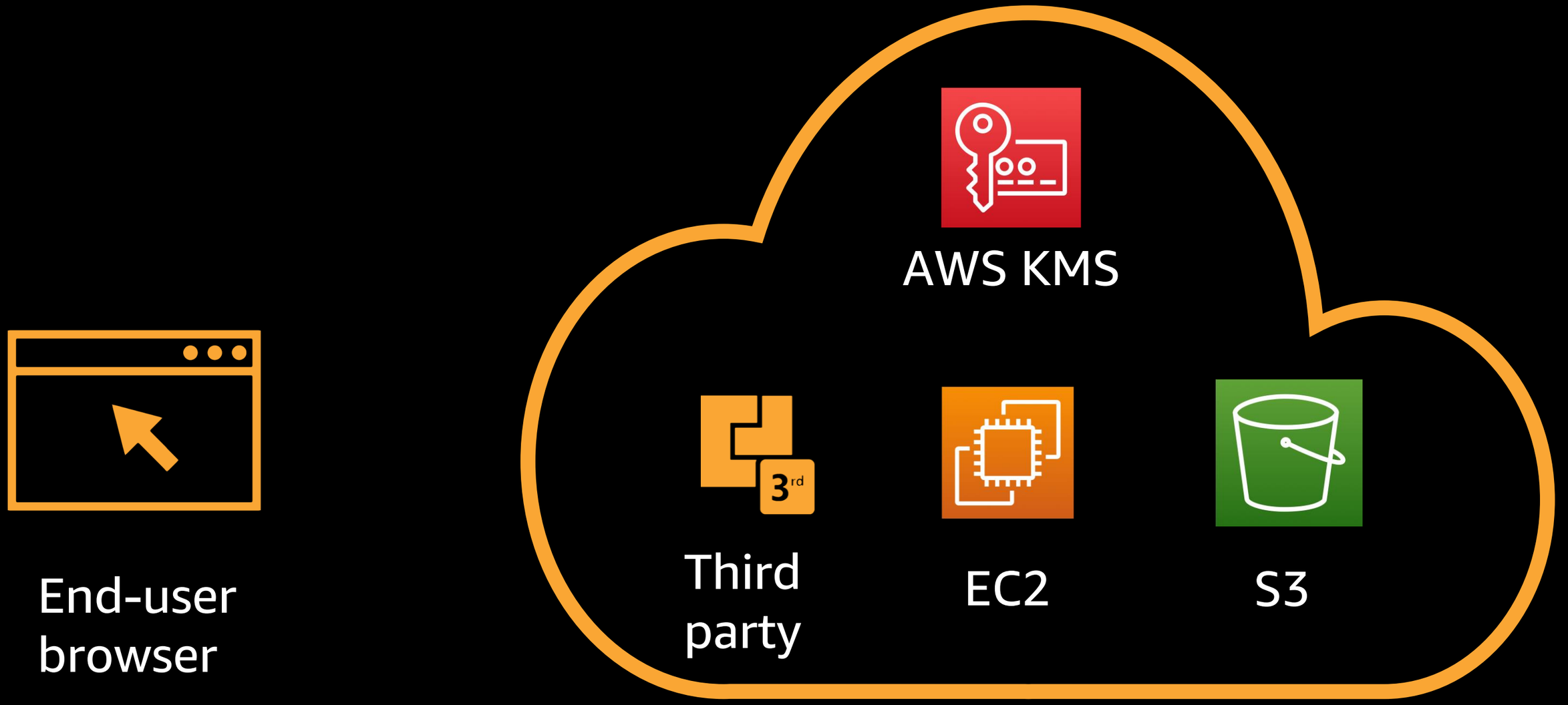
```
"Effect": "Allow",
"Action": [
     "kms:Decrypt",
     "kms:DescribeKey"
     ]
```

Client-side encryption

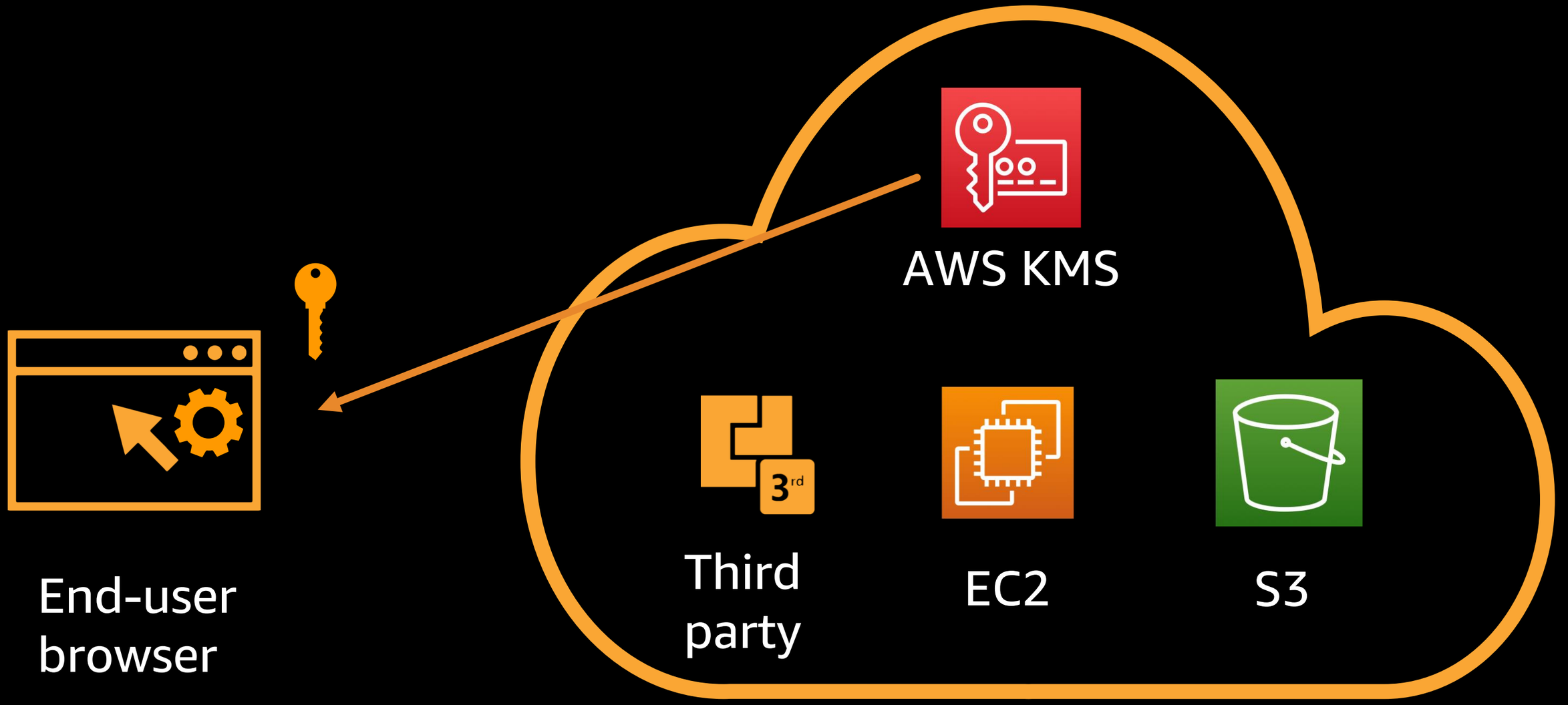
Client-side encryption



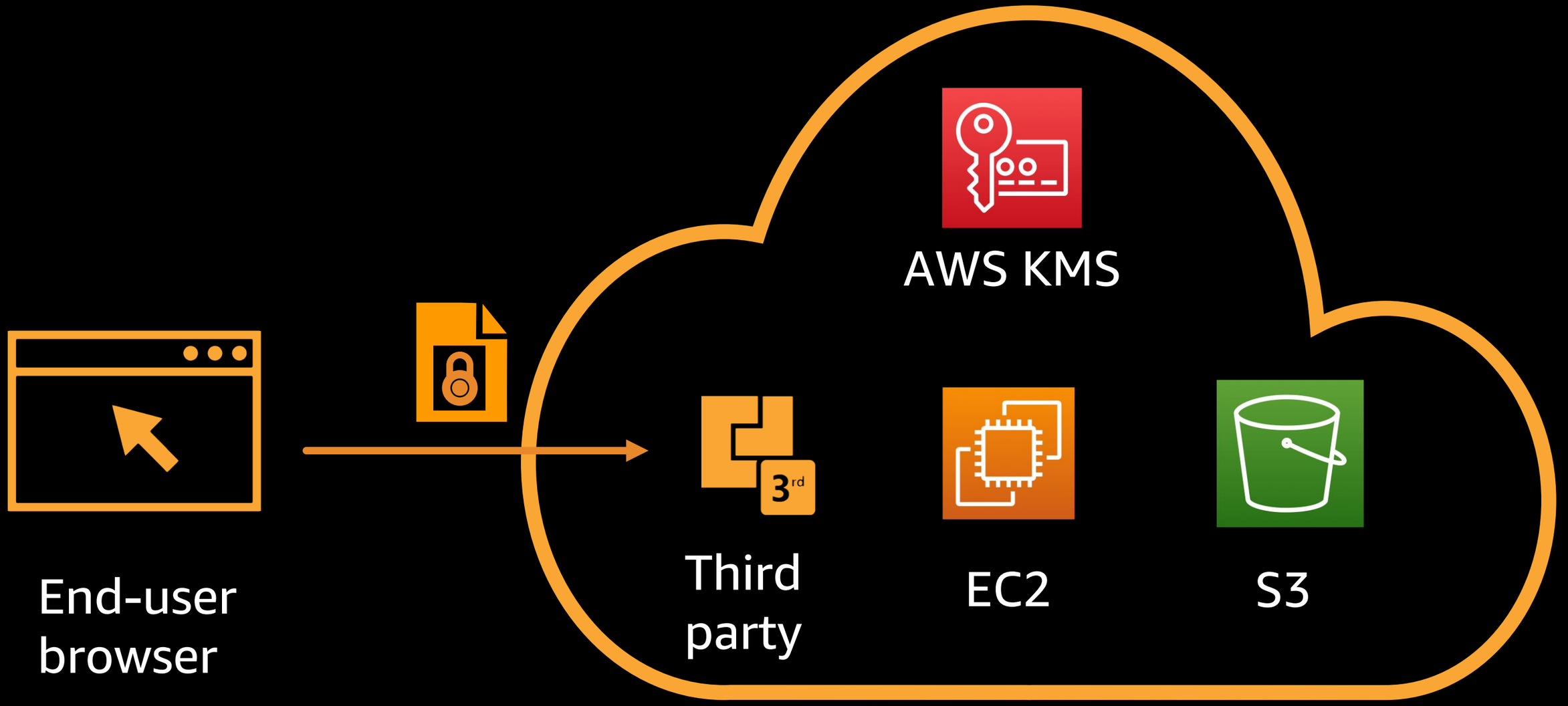
Client-side encryption – Use-case



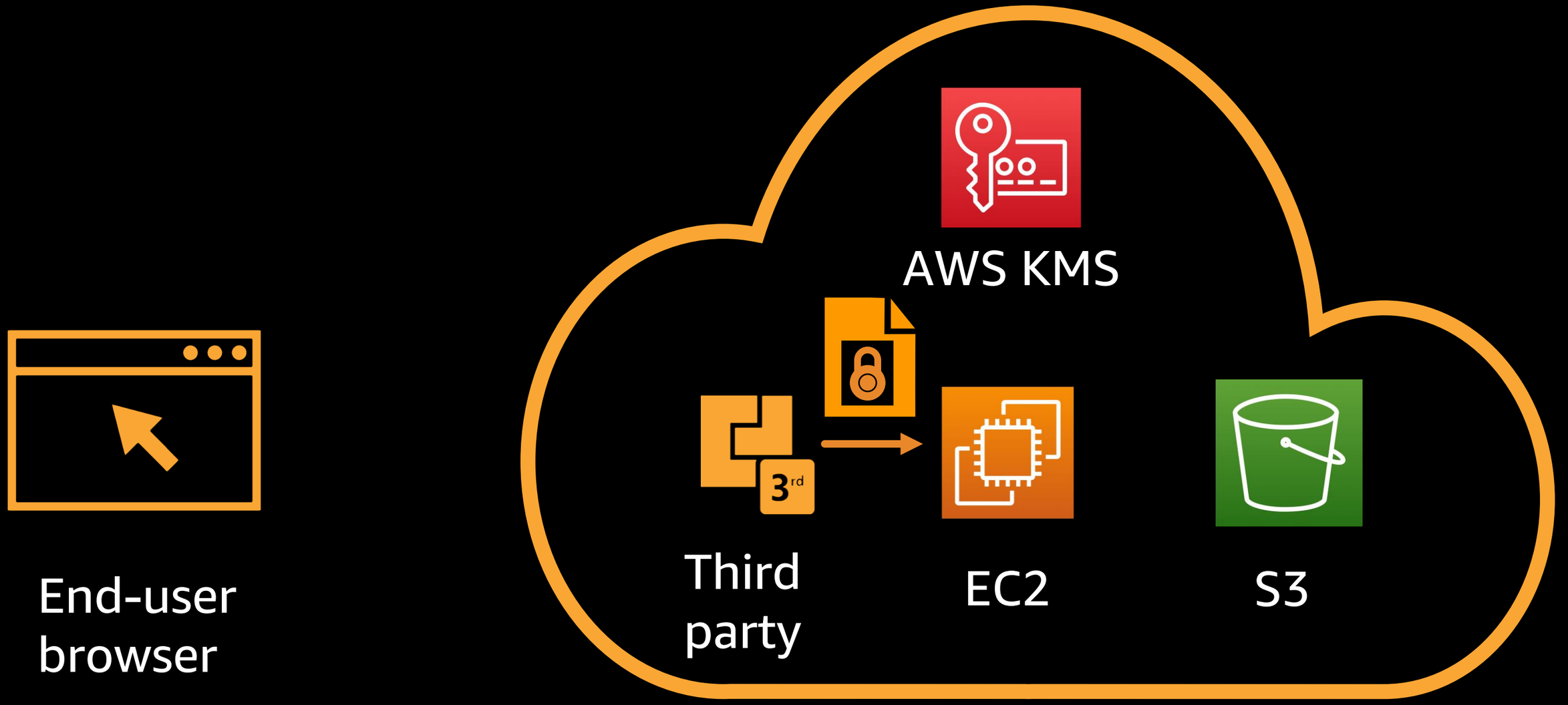
Client-side encryption – Use-case



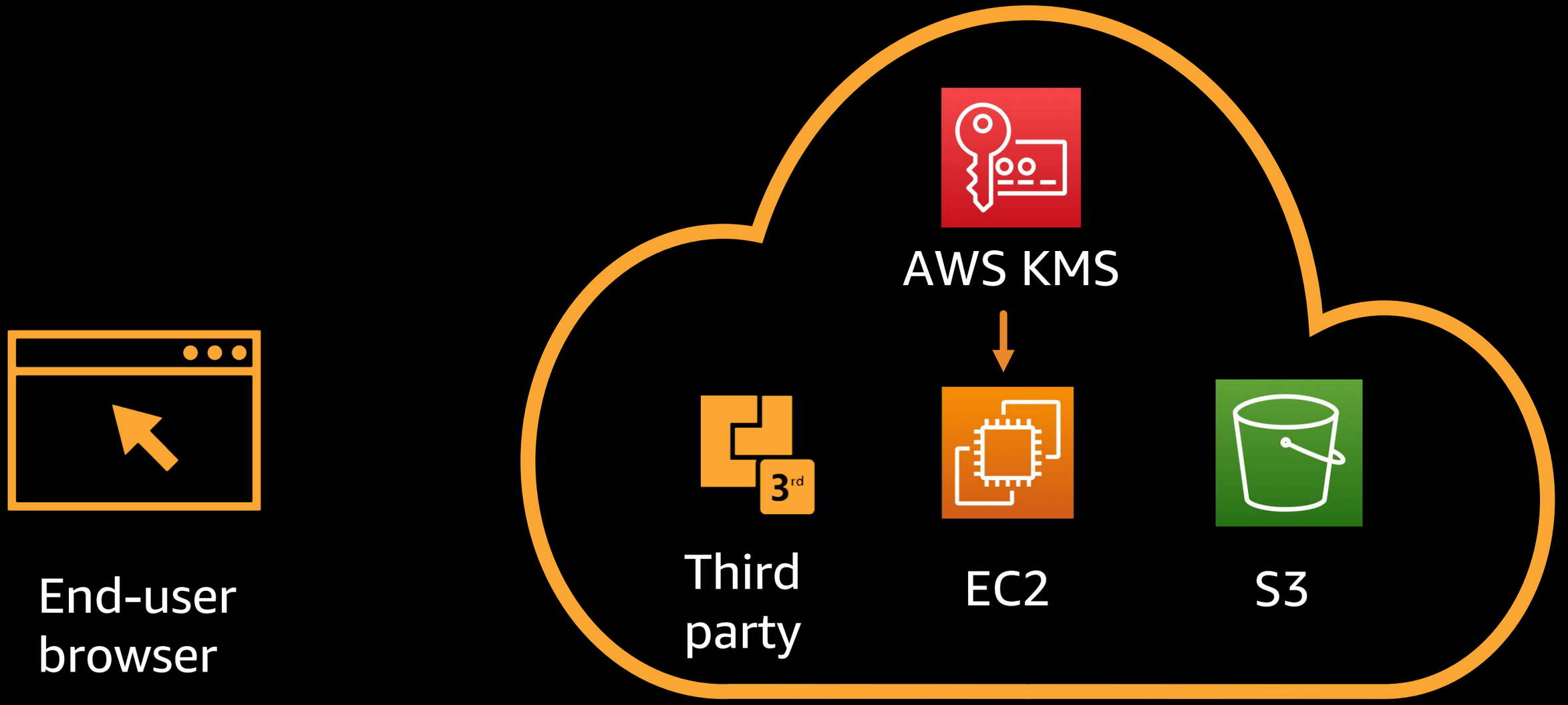
Client-side encryption – Use-case



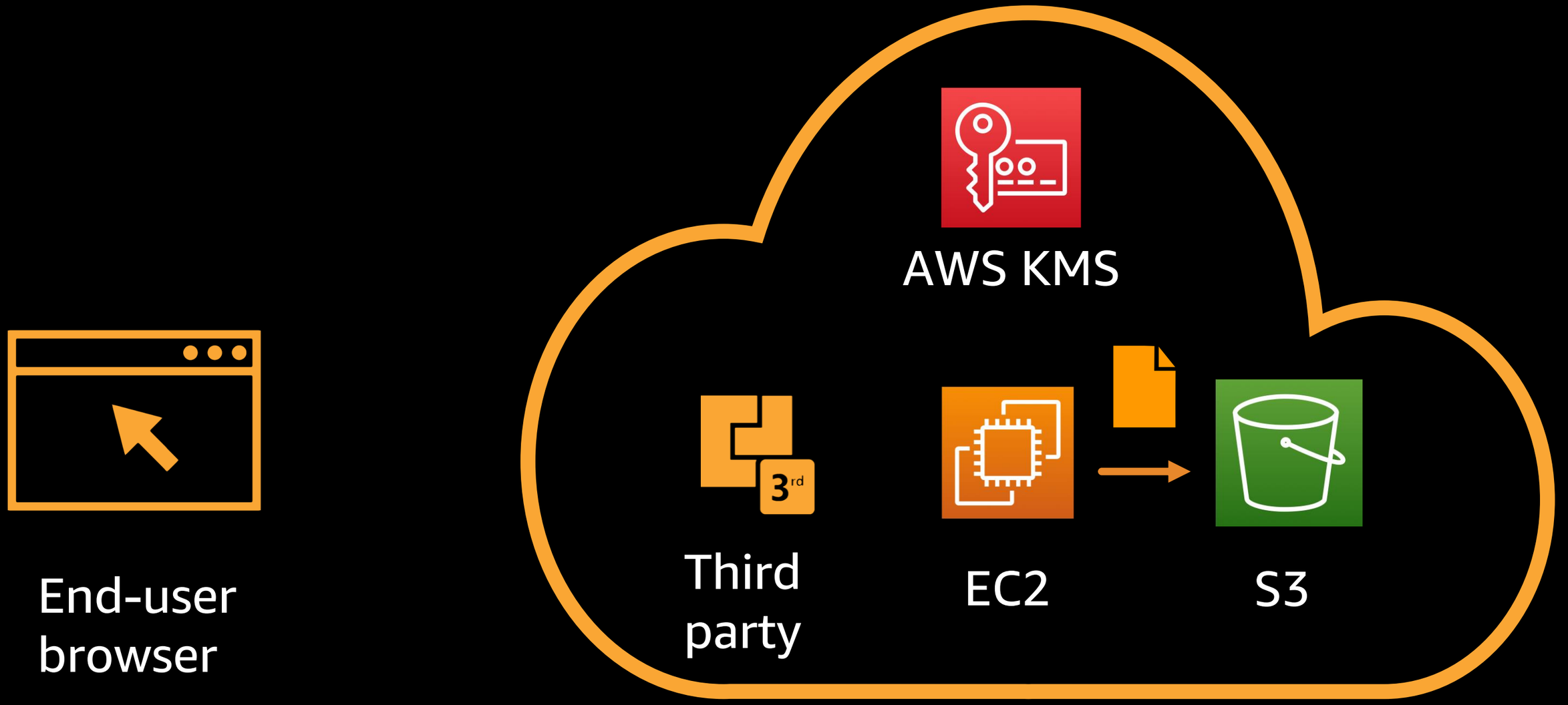
Client-side encryption – Use-case



Client-side encryption – Use-case



Client-side encryption – Use-case

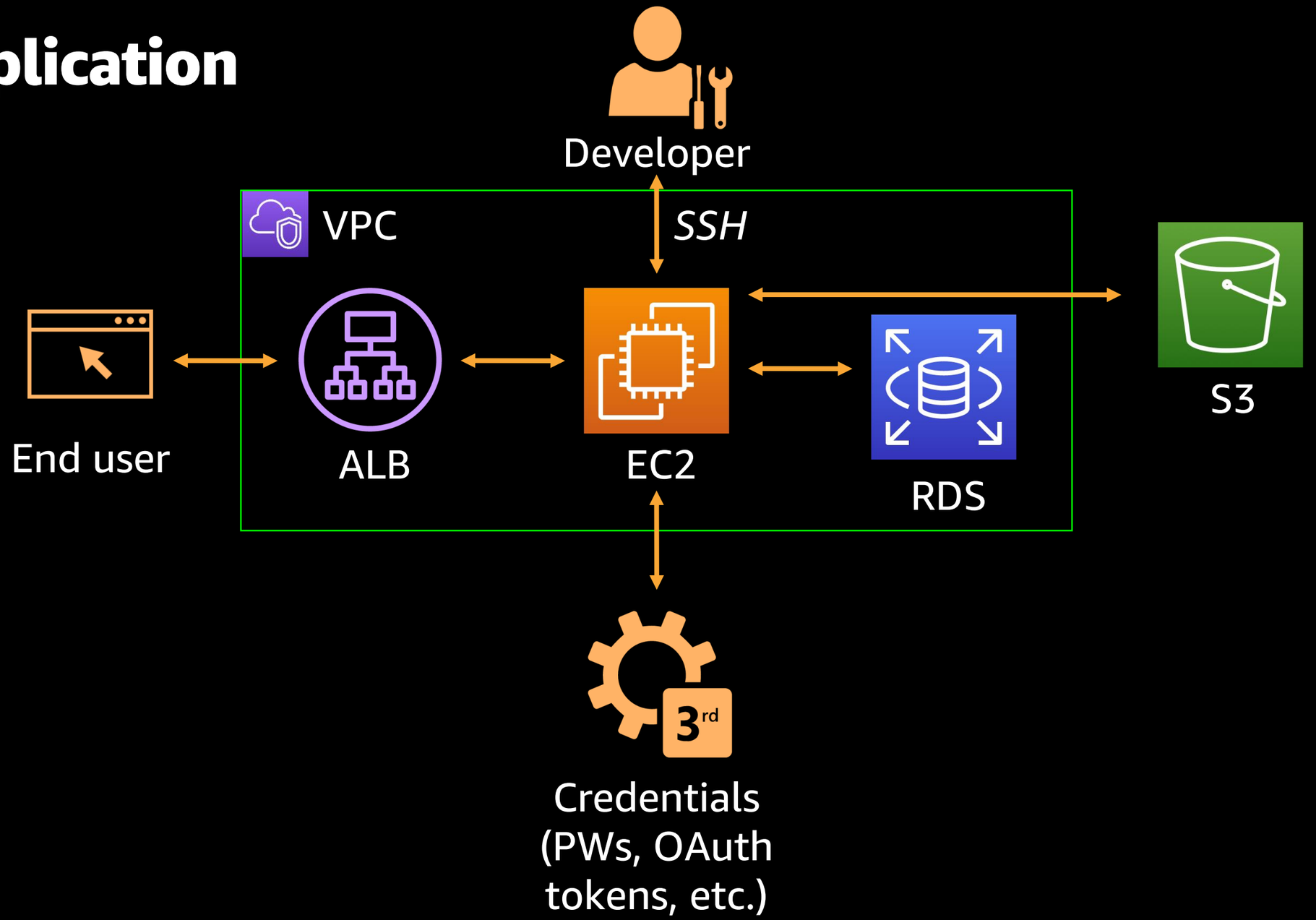


	Permission model	Logging	Complexity
SSE-S3	S3	S3	Low
SSE-KMS	S3 + KMS	S3 + KMS	Medium
SSE-KMS + CSE	S3 + KMS + your app	S3 + KMS + your app	High

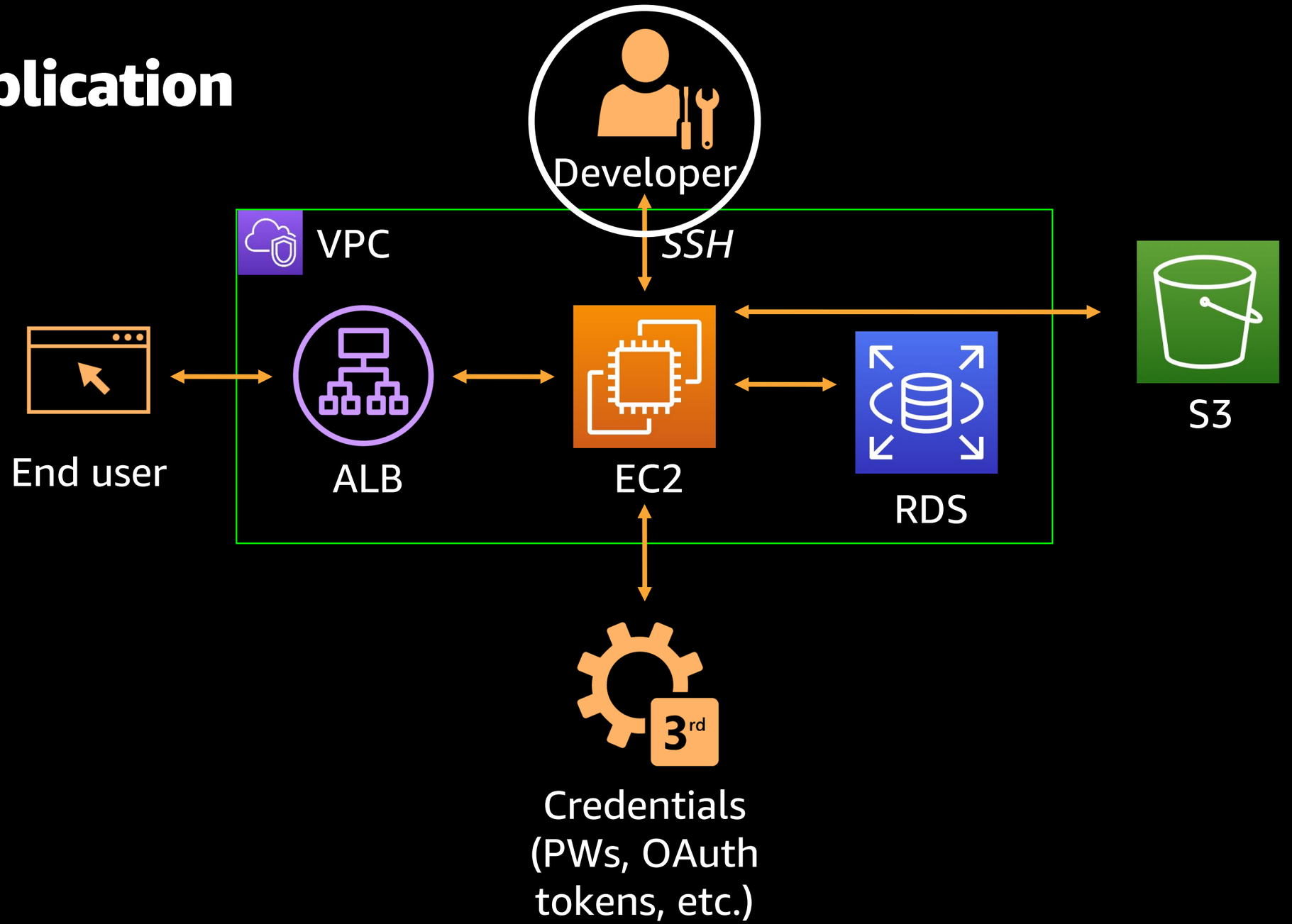
Building an application

AWS re:Invent

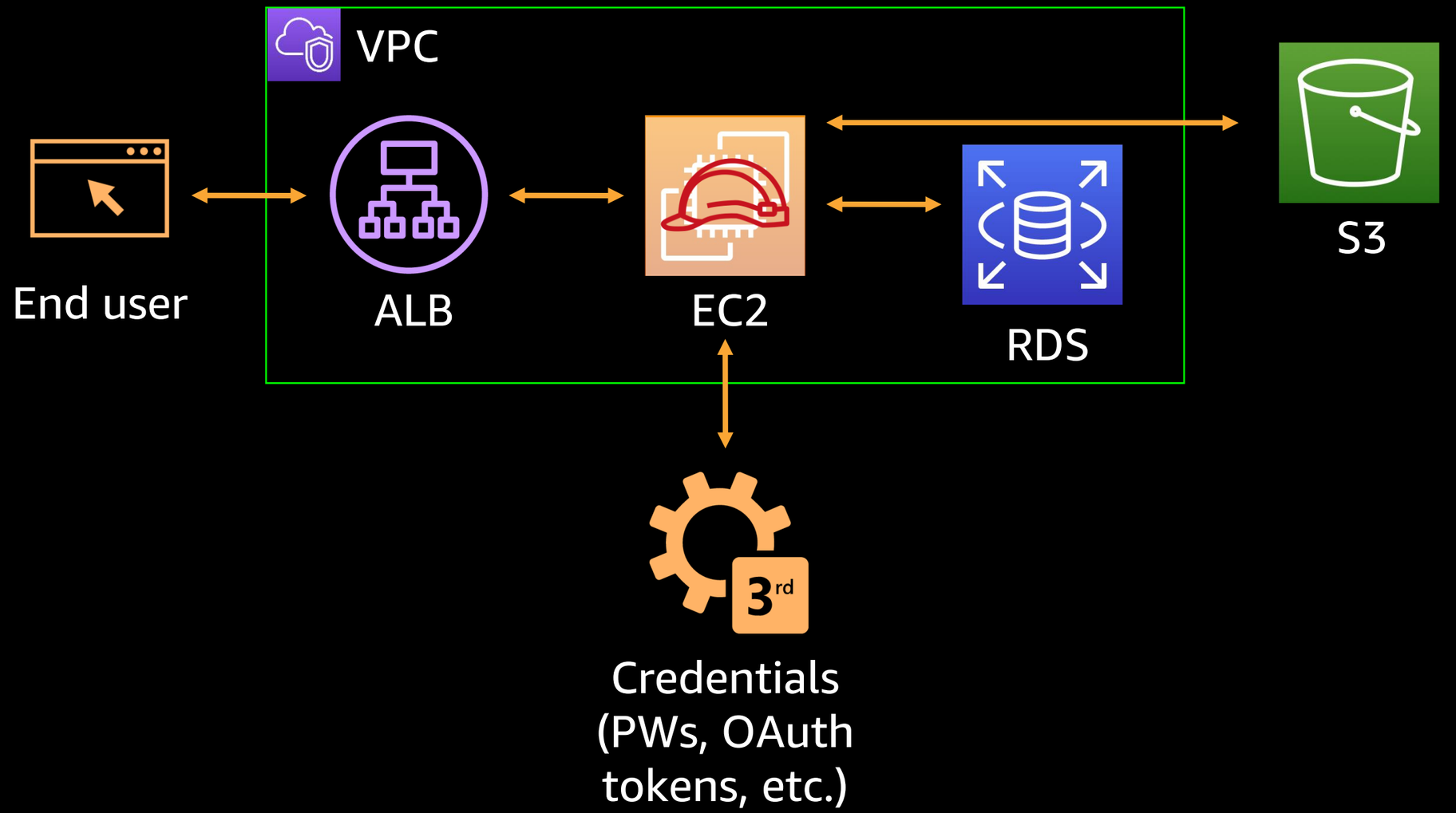
Application



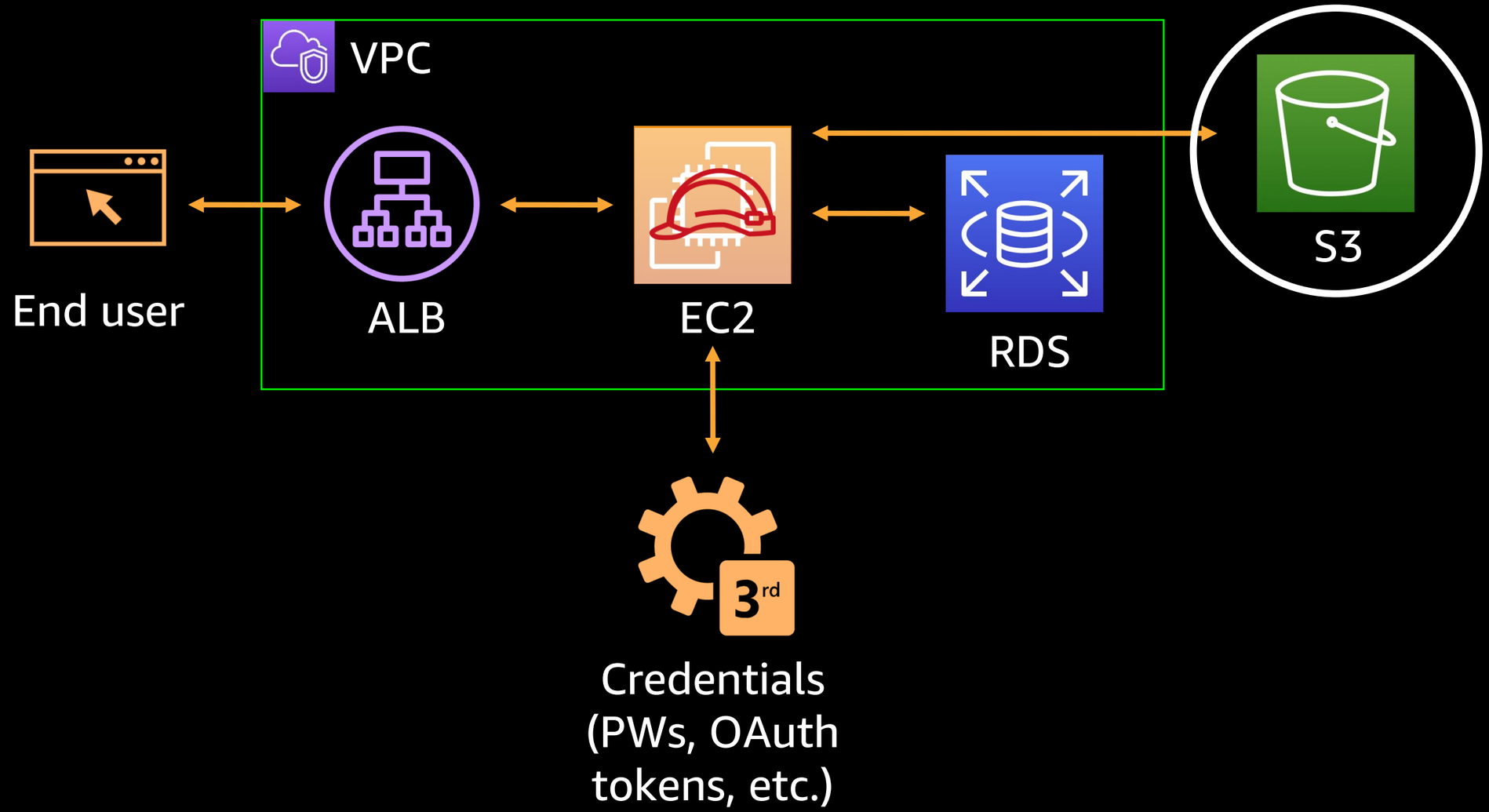
Application



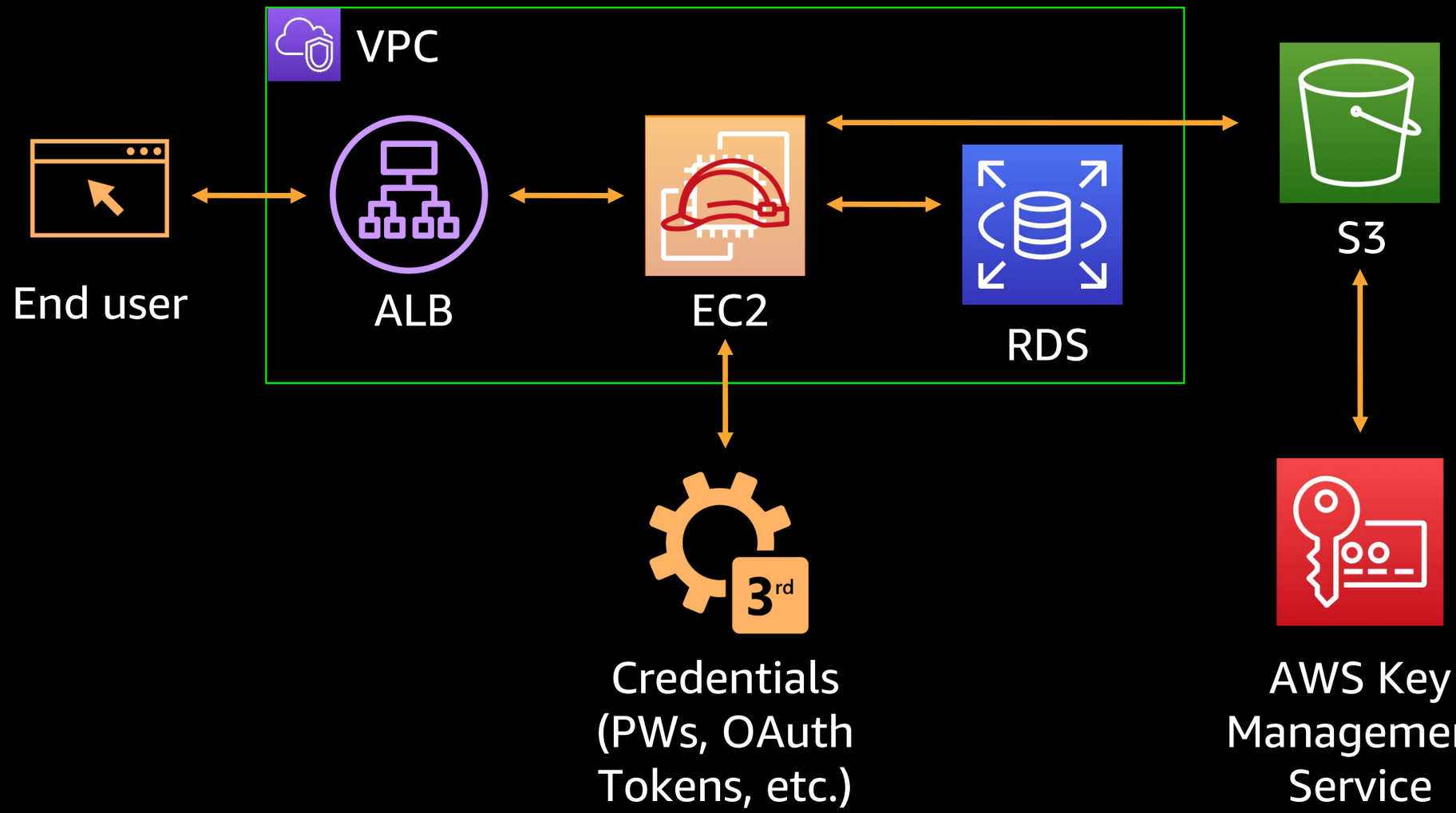
Application



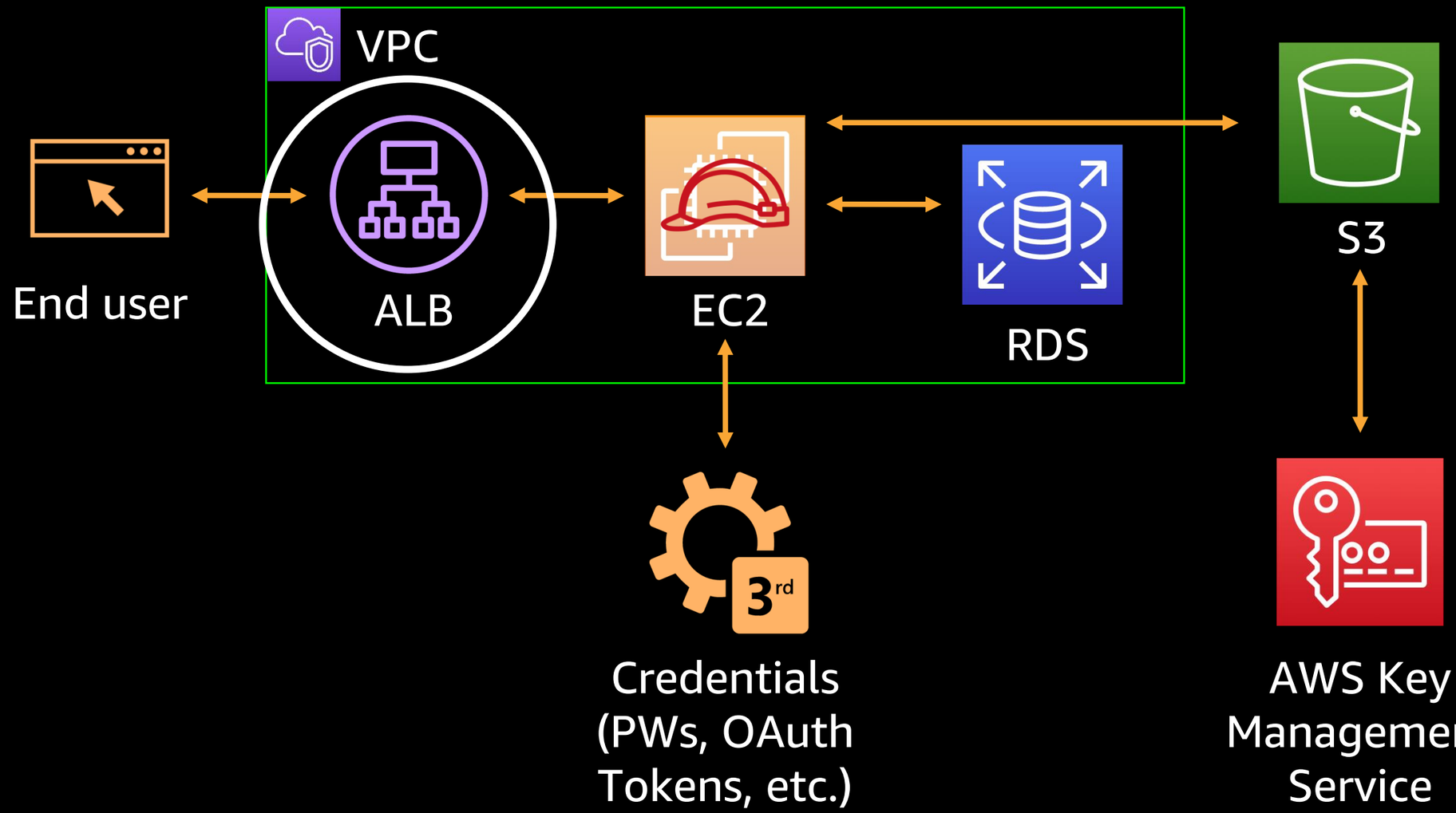
Application



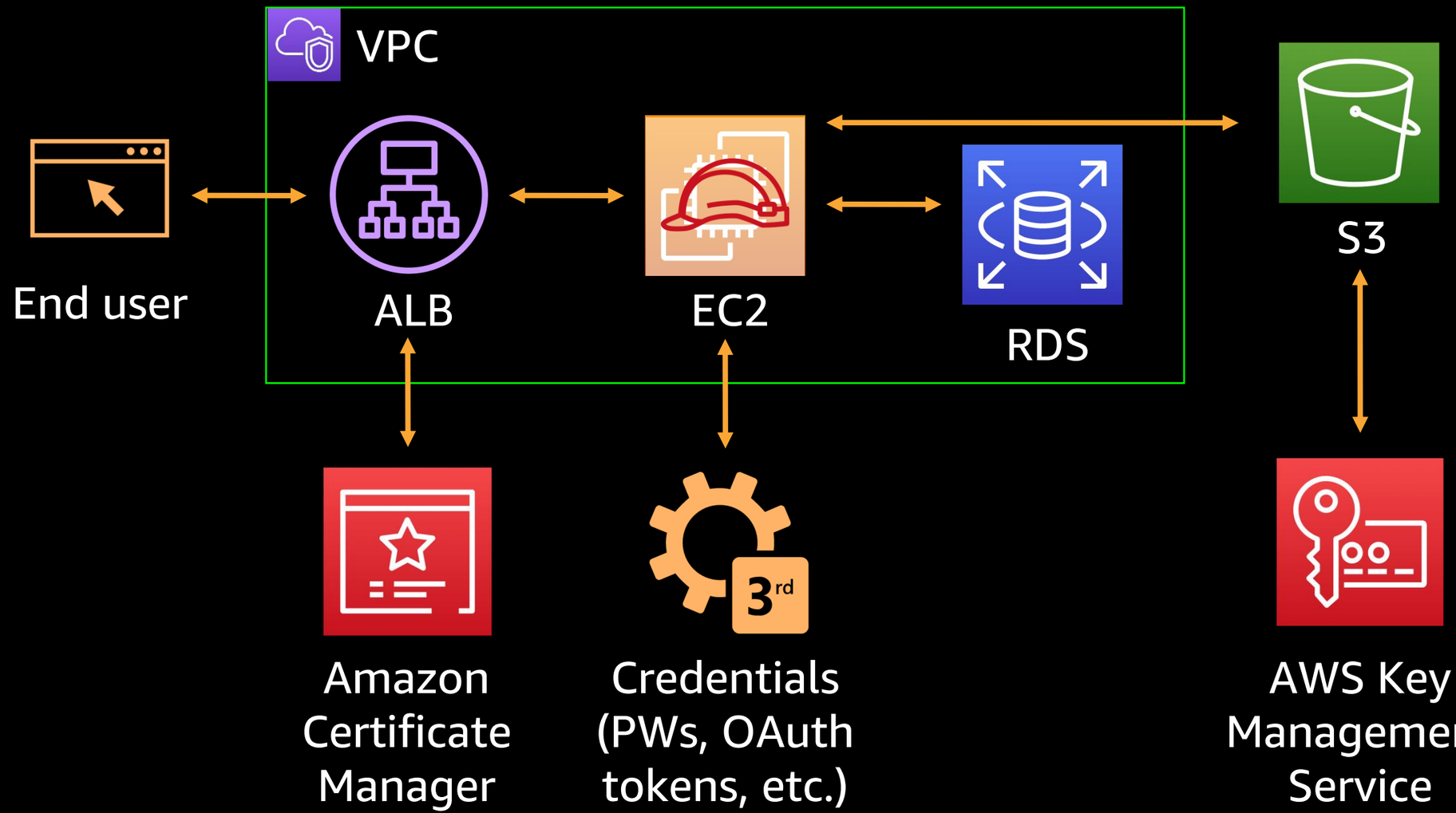
Application



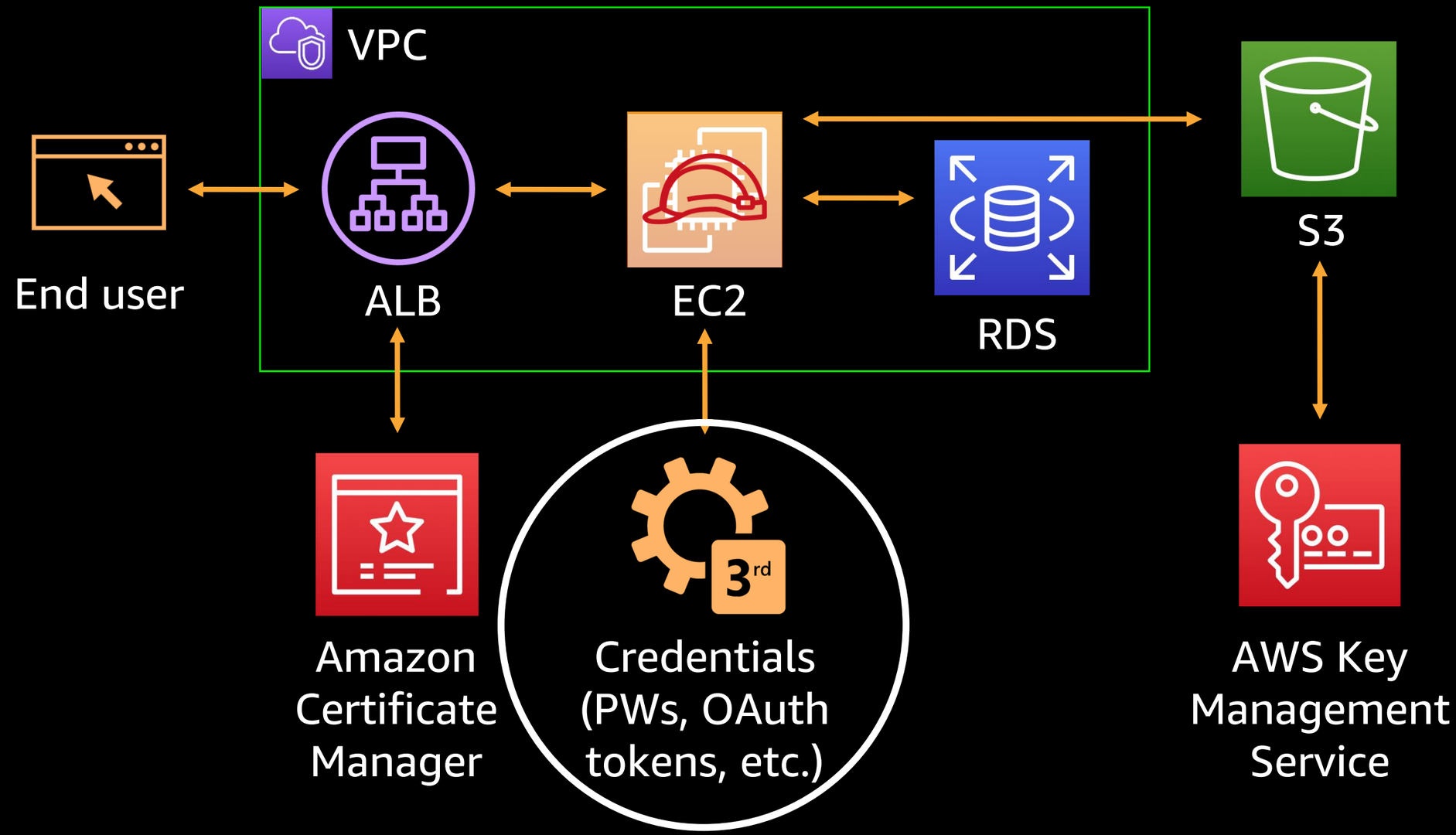
Application



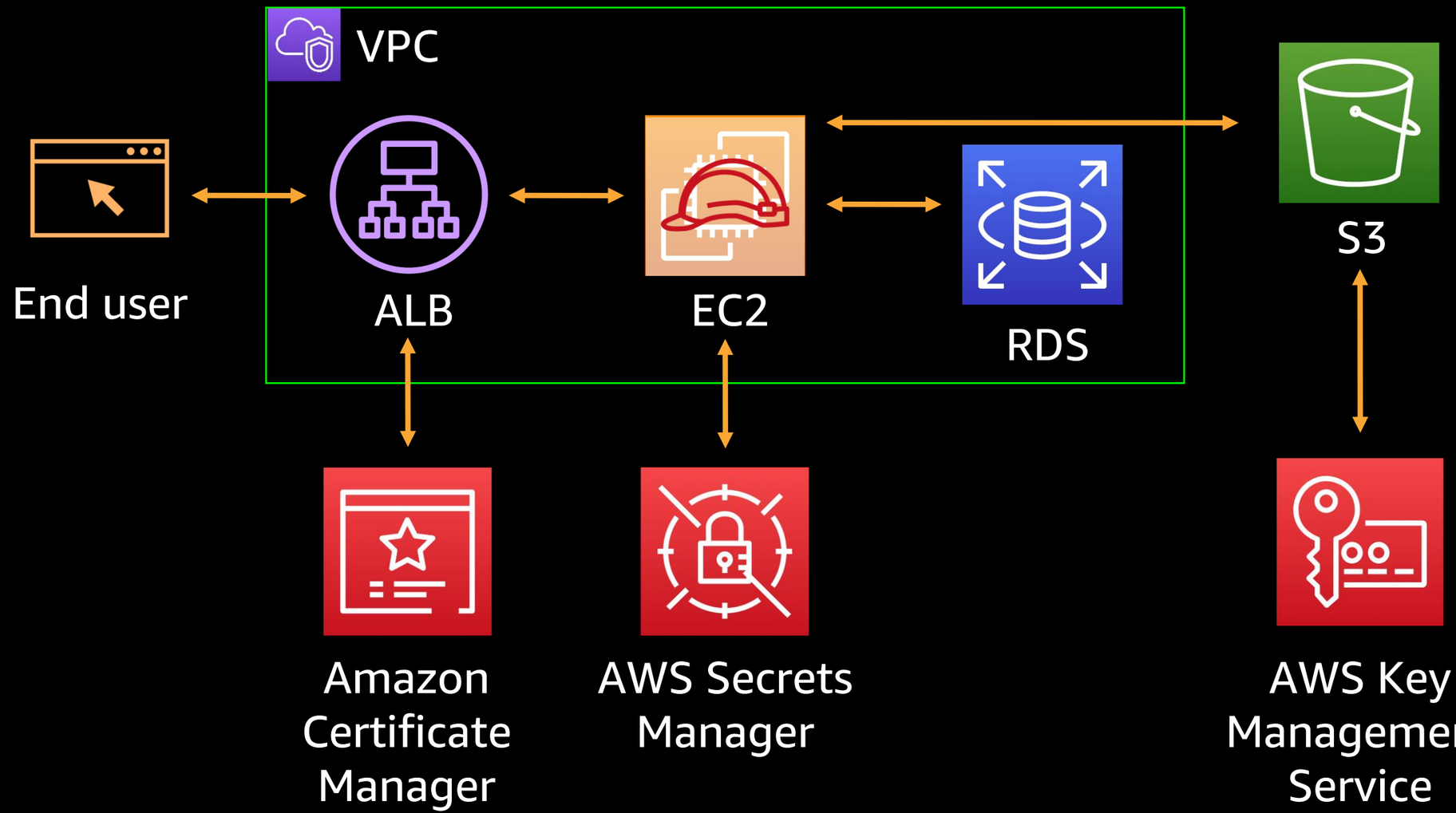
Application



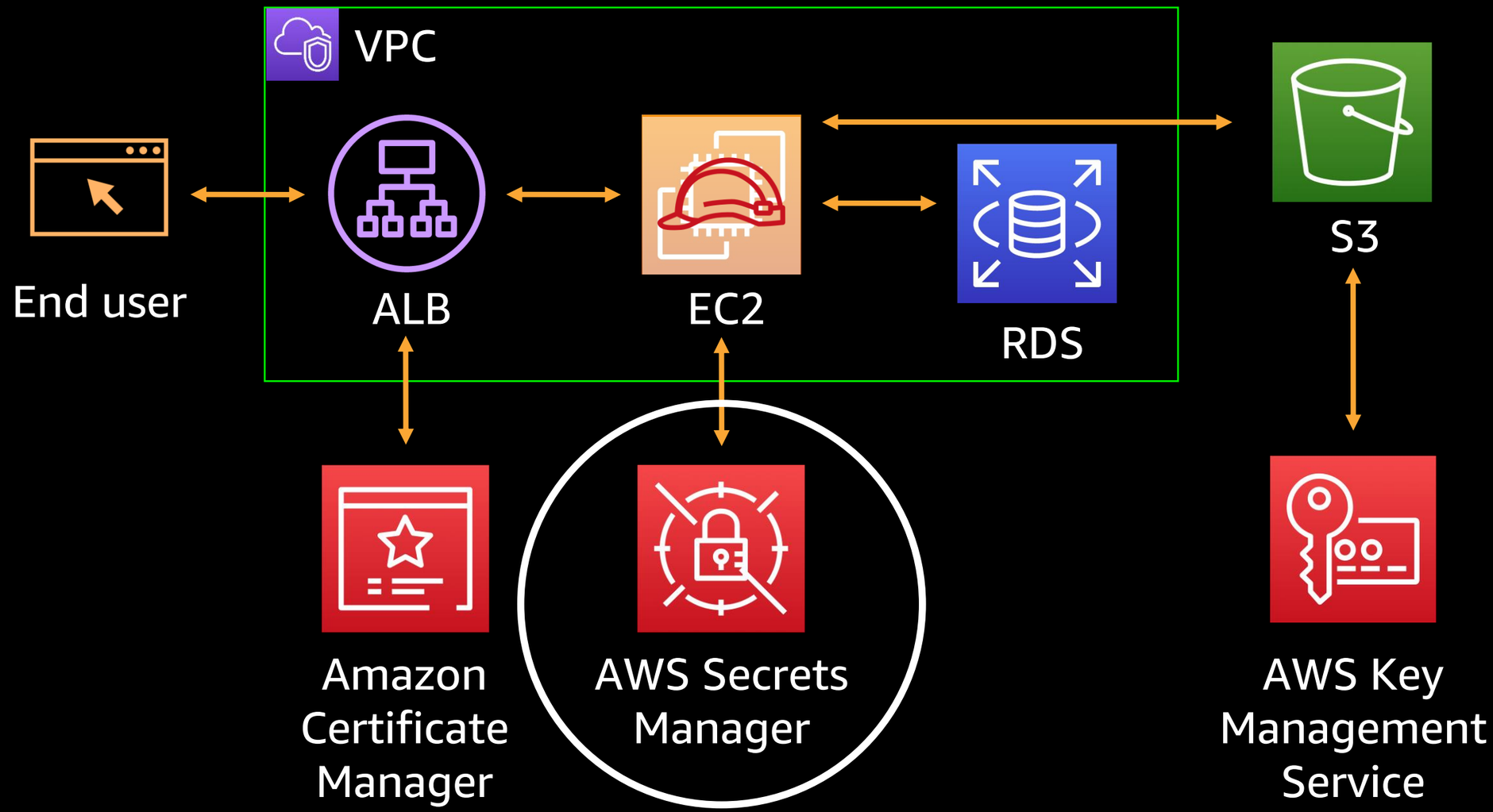
Application



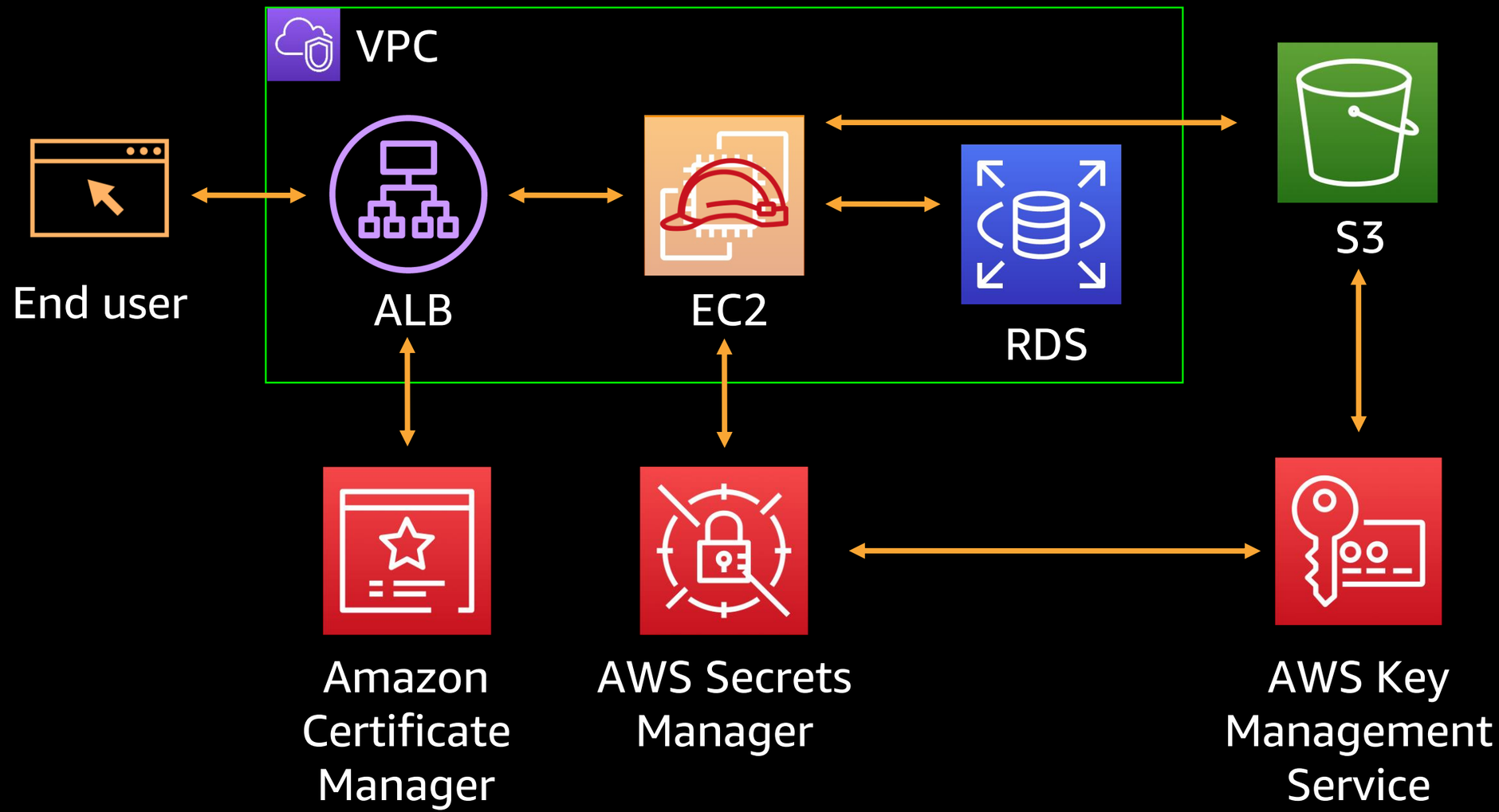
Application



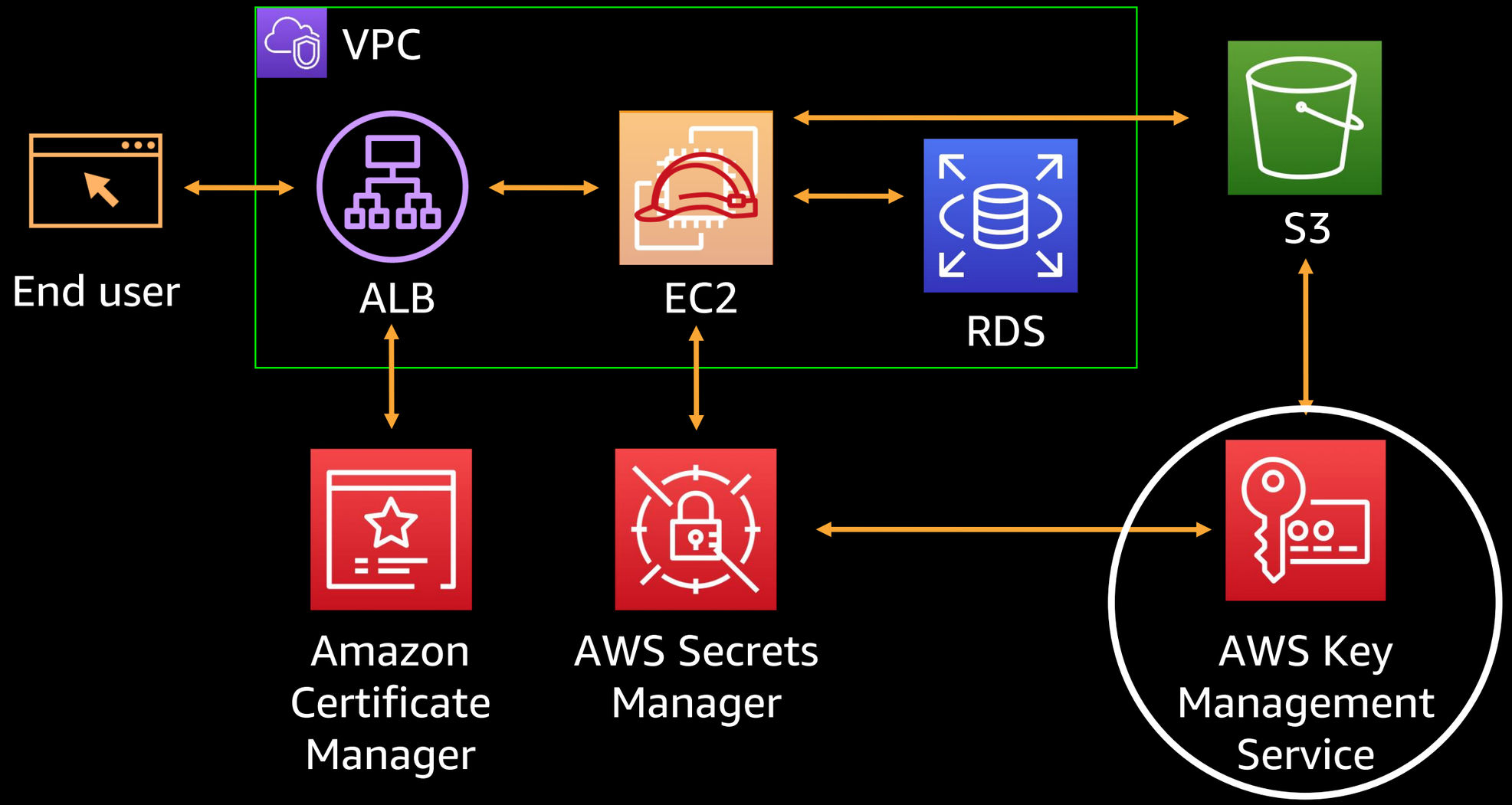
Application



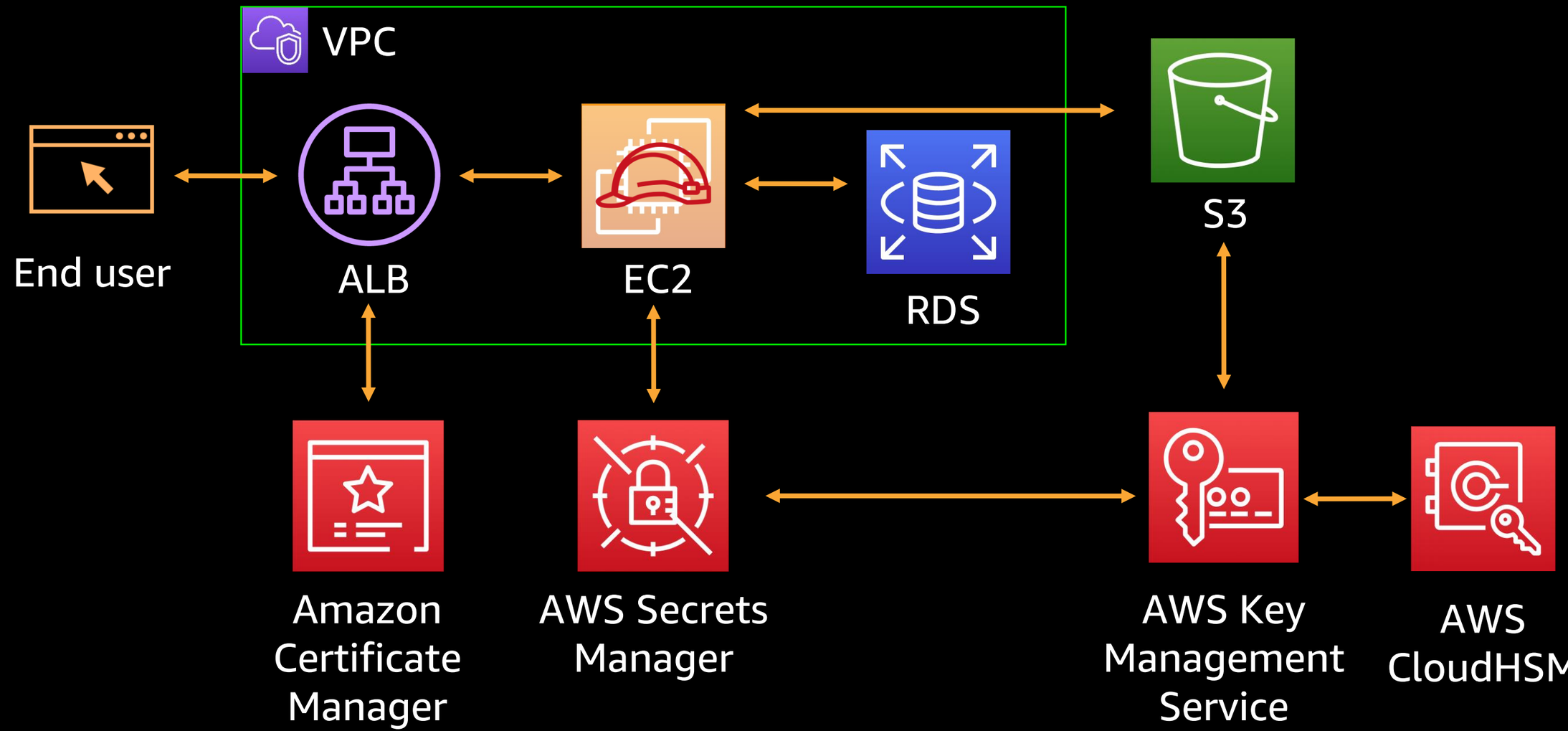
Application



Application



Application



“Nothing is wholly obvious without becoming enigmatic.”

Jean Baudrillard

EGS

AWS re:Invent

Thank you!

AWS re:Invent

Please complete the session survey

AWS re:Invent