# Non-human identities

Expose ownerless keys, excessive privileges and rotation dependencies.

Printable workpaper. The detailed guide and all scenario branches are in the Markdown file.

Do not upload production secrets. Record masked identifiers, ownership and permission scope instead of secret values.

## Process and expected evidence

### 1. Assign identity ownership

Identity–workload–owner record

### 2. Constrain privilege and trust

Effective privilege and trust relationship

### 3. Rehearse rotation

Rotation and old-key rejection test

### 4. Monitor the lifecycle

Lifecycle and exception record

## Work record

| |
|---|
| Scope / date: |
| Business / technical owner: |
| Decision and rationale: |
| Evidence reference / retest: |

# Example and closure

Fictional example; not evidence of actual work.

Masked ID: svc-***-21

Workload: Example transfer job

Owner: Data platform owner

Permission: Write to destination only

Consumer: Synthetic batch job

Revocation test: Old identity rejected

## Closure checklist

[ ] No secret values recorded.

[ ] Business and technical owners exist.

[ ] Environment and resource privileges constrained.

[ ] Old-identity revocation verified.

## Official sources

Microsoft — Securing service principals

https://learn.microsoft.com/en-us/entra/architecture/service-accounts-principal

Microsoft — Protect identities and secrets

https://learn.microsoft.com/en-us/entra/fundamentals/zero-trust-protect-identities