EUROPEAN CLOUD SUMMIT 2024

Securing access to your Azure environments

Henry Been

Independent DevOps & Azure Architect

Microsoft MVP | Pluralsight & A Cloud Guru Author

EUROPEAN CLOUD SUMMIT

MANAGING ACCESS
TO YOUR ENVIRONMENTS

A different talk

Not about a technology

More of a Case Study

Based on **lessons-learned** across different customers

MANAGING ACCESS
TO YOUR ENVIRONMENTS

1. Challenge

- In general
- Specific use case

2. Requirements

3. Solution

- Microsoft Entra ID

  Access Packages & PIM demo
- Design

4. Results & experiences

Challenge

Challenge

Traditional **trade-off** between two important requirements

Engineers need access to do their work

Preventing unauthorized access

Preventing phishing, mistakes, misuse of compromised accounts

Challenge

More traditional organizations

Developer-only organizations

Challenge – In general

Actual situation in many companies is complex and can be incomplete

- A **complex structure** of nested Entra ID groups for allocating authorizations has become the defacto standard
- Changes to that structure are difficult
- End-to-end overview can be lacking
- User – group membership is rarely reviewed
- Group – group nesting is even rarer to be reviewed

Challenge – In developer-only situations

Lack of systematic approach in **developer-only** situations with a high focus on Getting Things Done ™

Authorizations are assigned case by case

- On a **per-user** basis
- In response to **specific situations**
- In practice **never revoked**

There is no **governance**, with things like

- Design
- Review
- Auditlog

Requirements

for a better design

Requirements for a better design

- Engineers should have (or can easily acquire) the permissions they need to do their job.
- Provable in control of who has which permissions, and why.
- **Permissions are given out by the PO, not by some administrator or the team itself.**
- Compliant with ISO27001, enforced through technology, requiring no additional process.
- Understandable design that is extensible and can be implemented by any engineer in the team.
- Useable for managing access to Microsoft Entra ID, Azure Cloud, Azure DevOps and more

Solution

Solution

Three **ingredients:**

Access Packages

Group of authorizations combined with request, approval and review rules

Privileged Identity Management

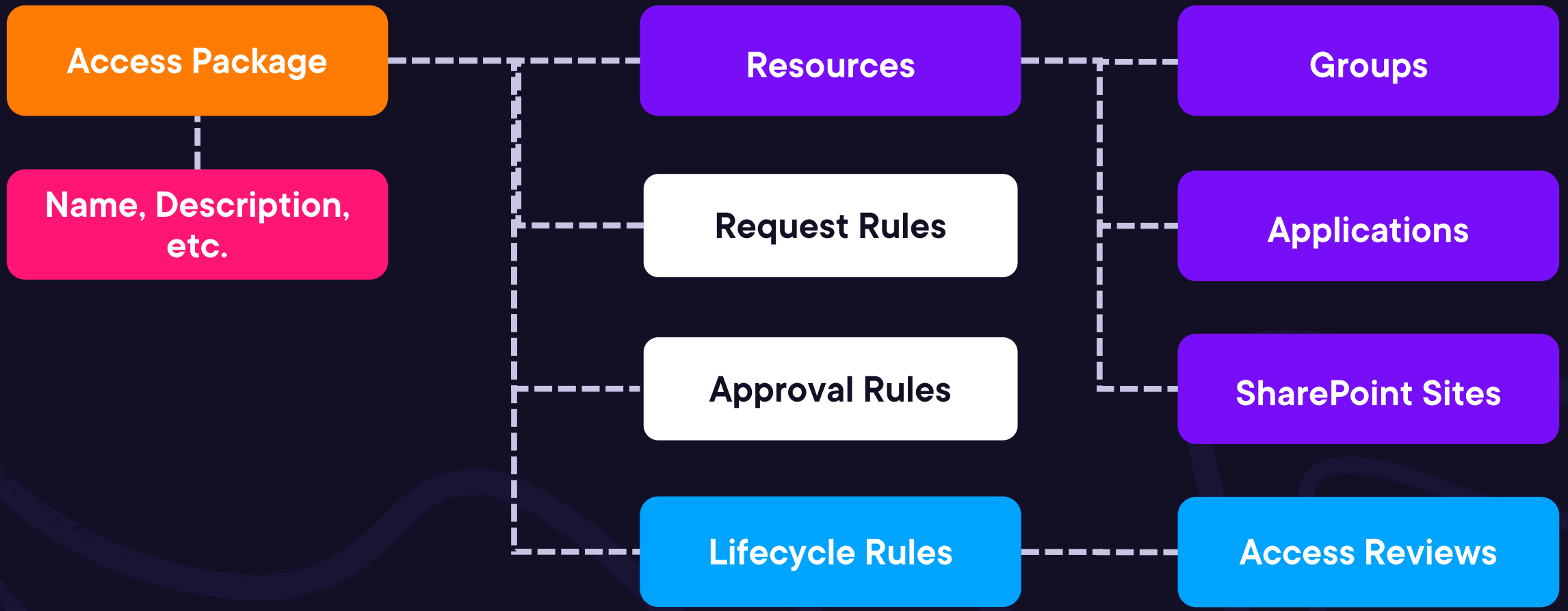
Capability to assign roles and groups as eligible instead of permanent

Resources, Groups and Packages Design

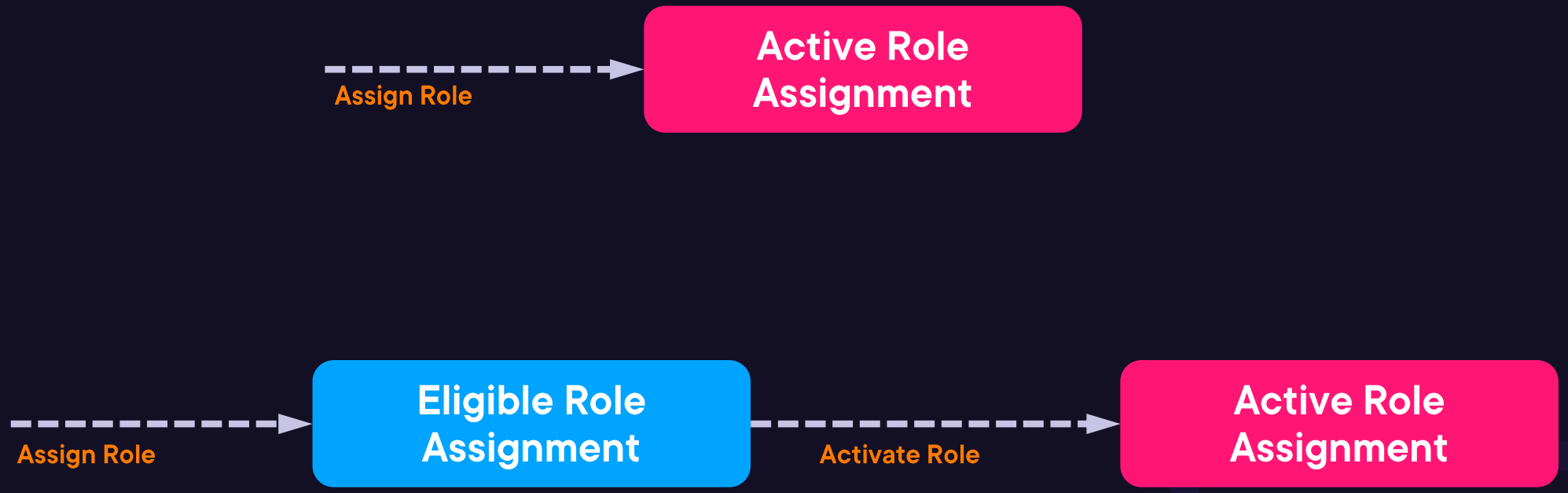
Customer specific design for applying these capabilities

Working with Access Packages

An access package is a grouping of **authorizations and everything around those authorizations** to govern their usage.



Active vs. Eligible Role Assignments



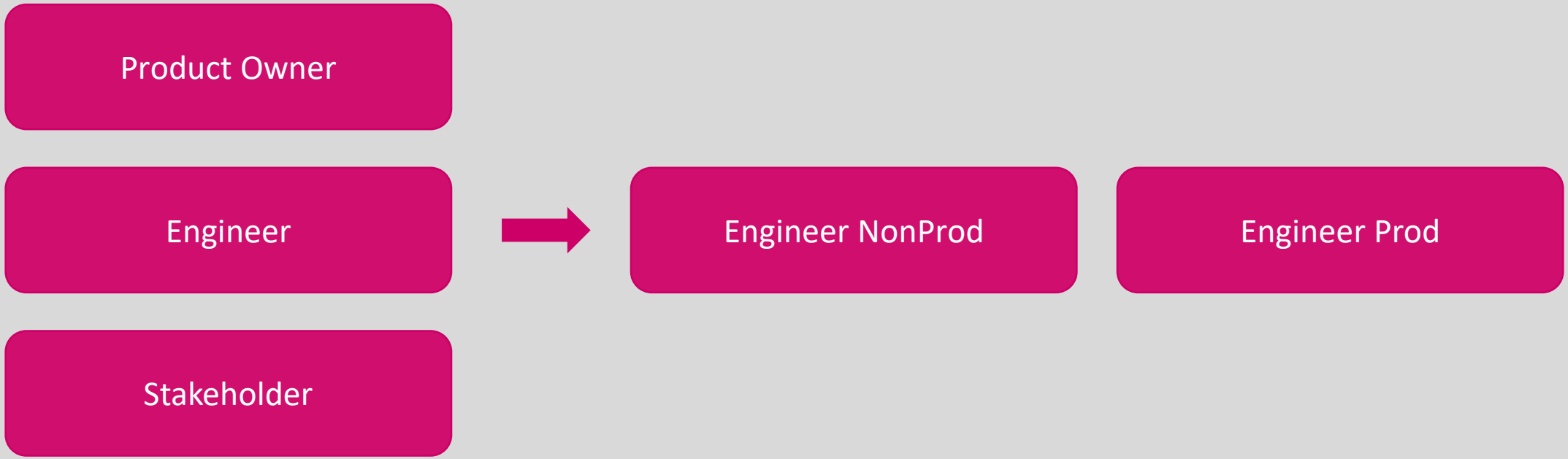
From: Introduction to Microsoft Entra ID (A Cloud Guru)

Want a DEMO?

Design

Design – Roles

There are different roles someone can have in a team.
Depending on your role you have responsibilities
Responsibilities require certain authorizations.



Design – Roles

Product Owner	Owns the product, builds the backlog, no technical access, manages team members.
Engineer NonProd	Read code, open/approve pull requests, can read/write non-production environments, work on the backlog.
Engineer Prod	Can read production environments.
Stakeholder	Can read the backlog, dashboards, documentation, etc.
Administrator	Can read and write in production. *Special

Design – Products

We have different products. Not every engineer works on every product. Roles should be scoped to products.

Product 1

Product 2

Product 3

* Use meaningful names instead, these are examples

Design – Access Packages

One access package should provide all authorizations for a role in the organization.

We need an access package for each product/role combination.

Product / **Role**	Product 1	Product 2	Product 3
Product Owner	Product 1 – Product Owner	Product 2 – Product Owner	Product 3 – Product Owner
Engineer NonProd	Product 1 – Engineer NonProd	Product 2 – Engineer NonProd	Product 3 – Engineer NonProd
Engineer Prod	Product 1 – Engineer Prod	Product 2 – Engineer Prod	Product 3 – Engineer Prod
Stakeholder	Product 1 – Stakeholder	Product 2 – Stakeholder	Product 3 – Stakeholder
Administrator	All Products - Administrator		

Design – Authorizations

Use Entra ID groups as an indirection for assigning authorizations.

Let's start with something easy…

All Products – EntraID – Global Administrators

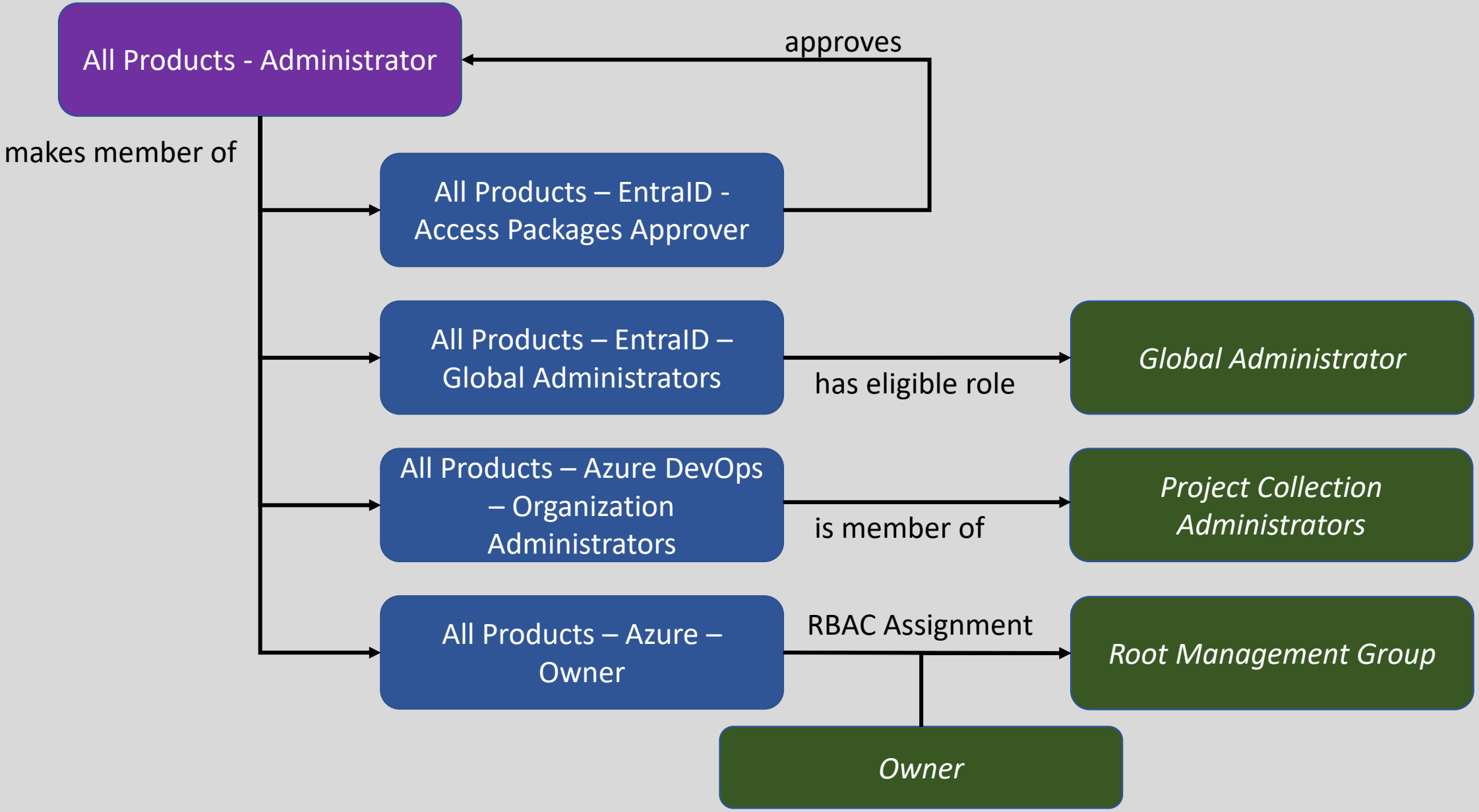
All Products – Azure DevOps – Organization Administrators

All Products – Azure – Root Managementgroup Owner

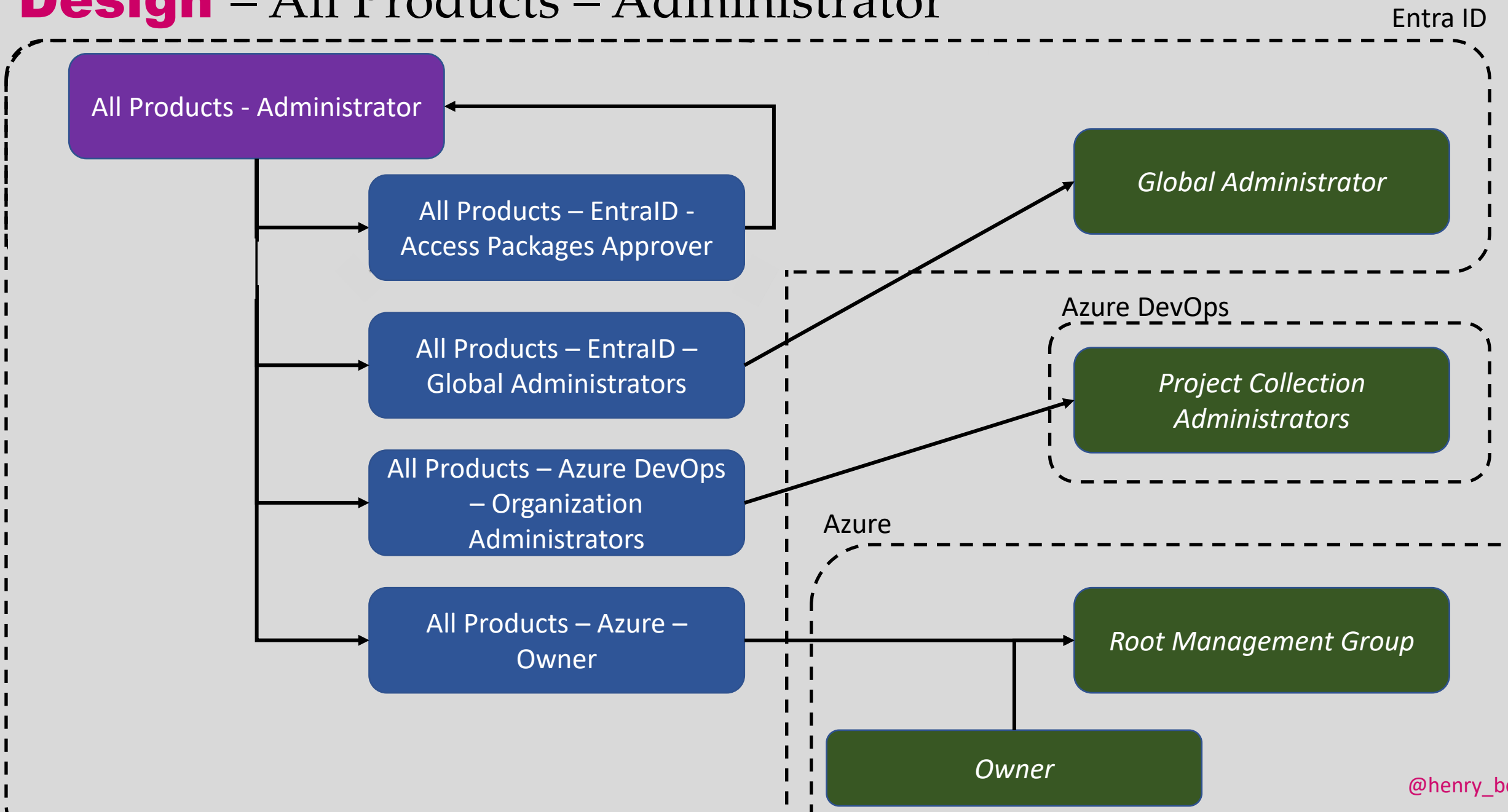
All Products – EntraID - Access Packages Approver

{Product} – {TargetSystem} – {TargetSystemAuthorizations}

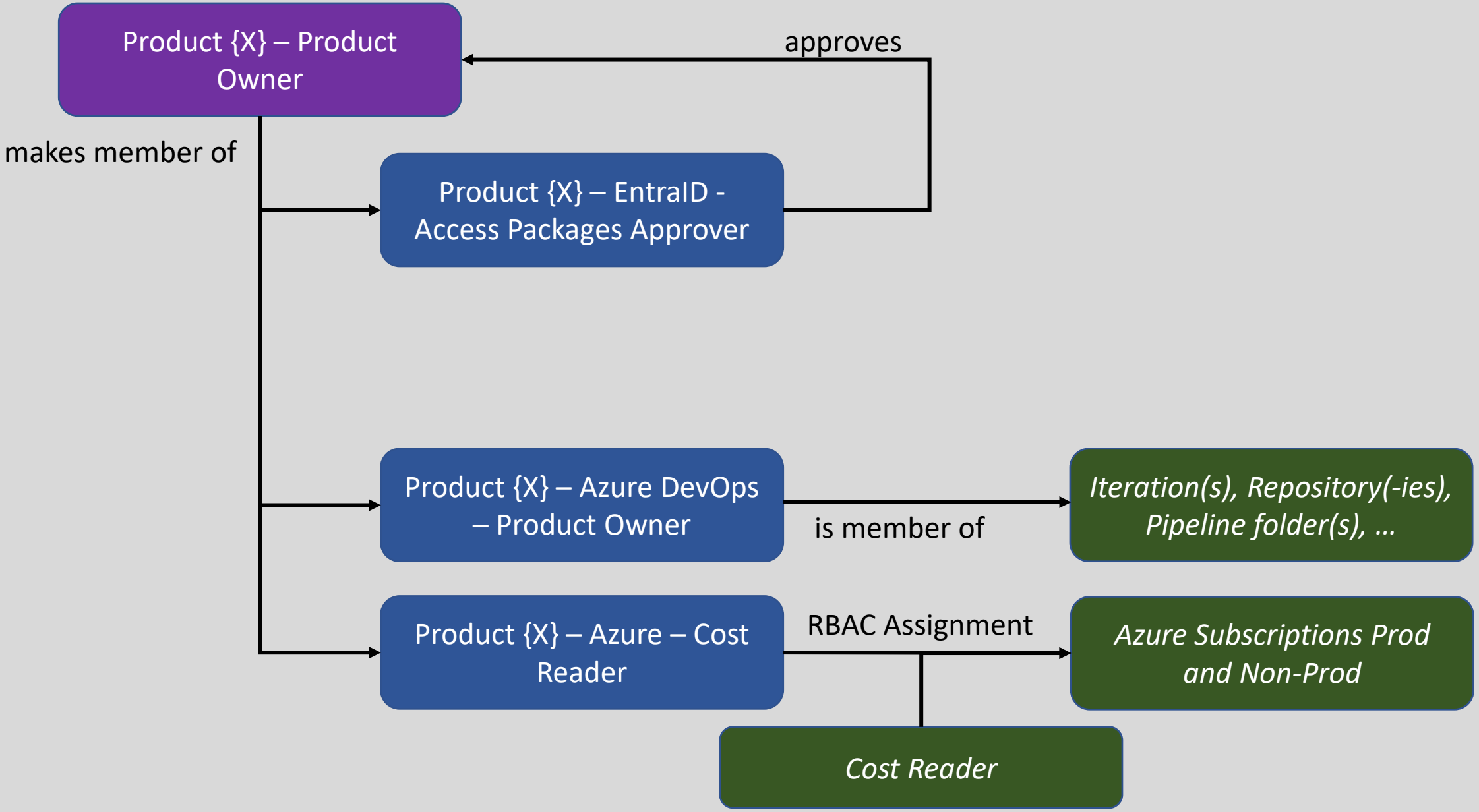
Design – All Products – Administrator



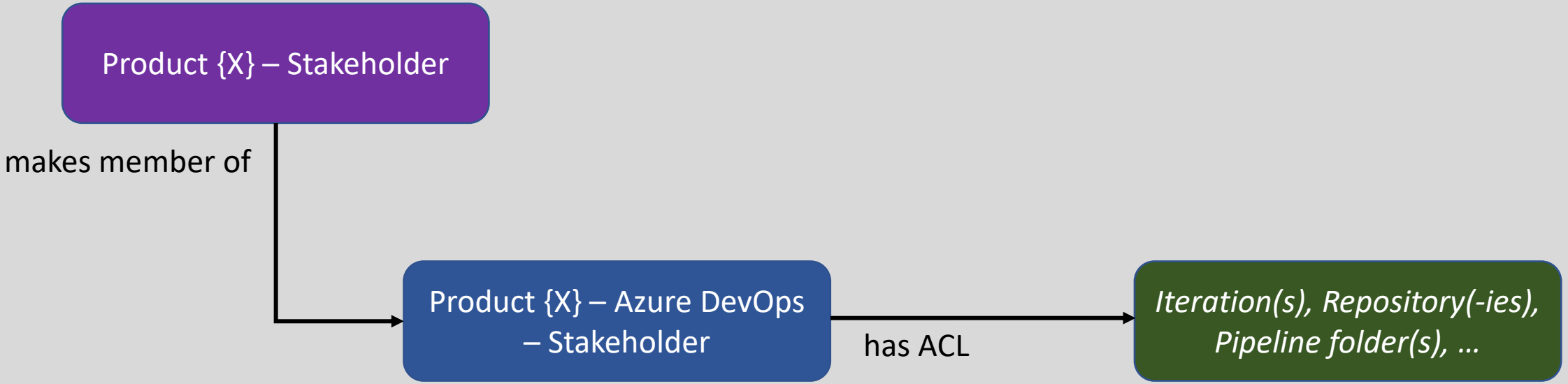
Design – All Products – Administrator



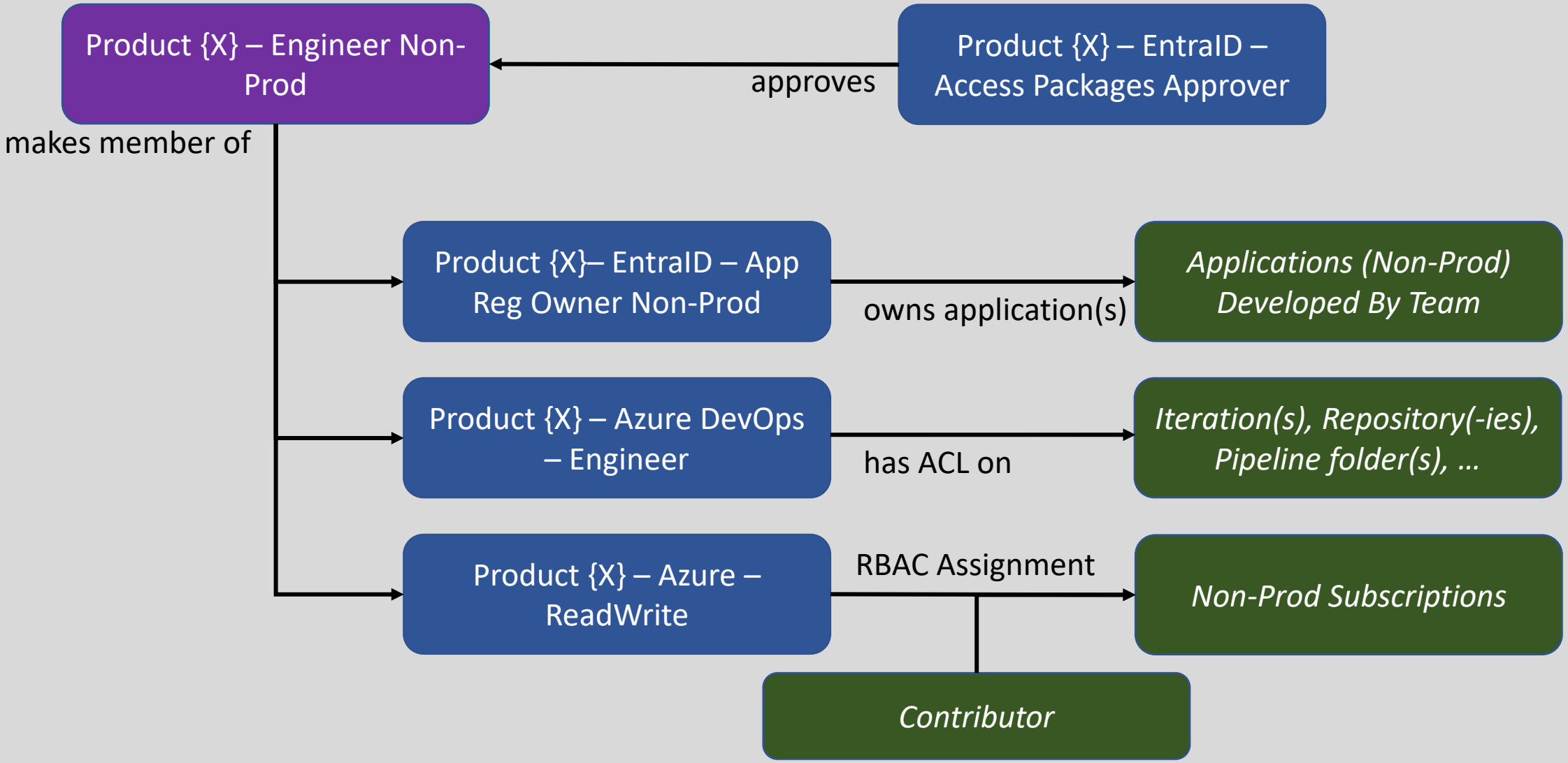
Design – All Products – Product Owner



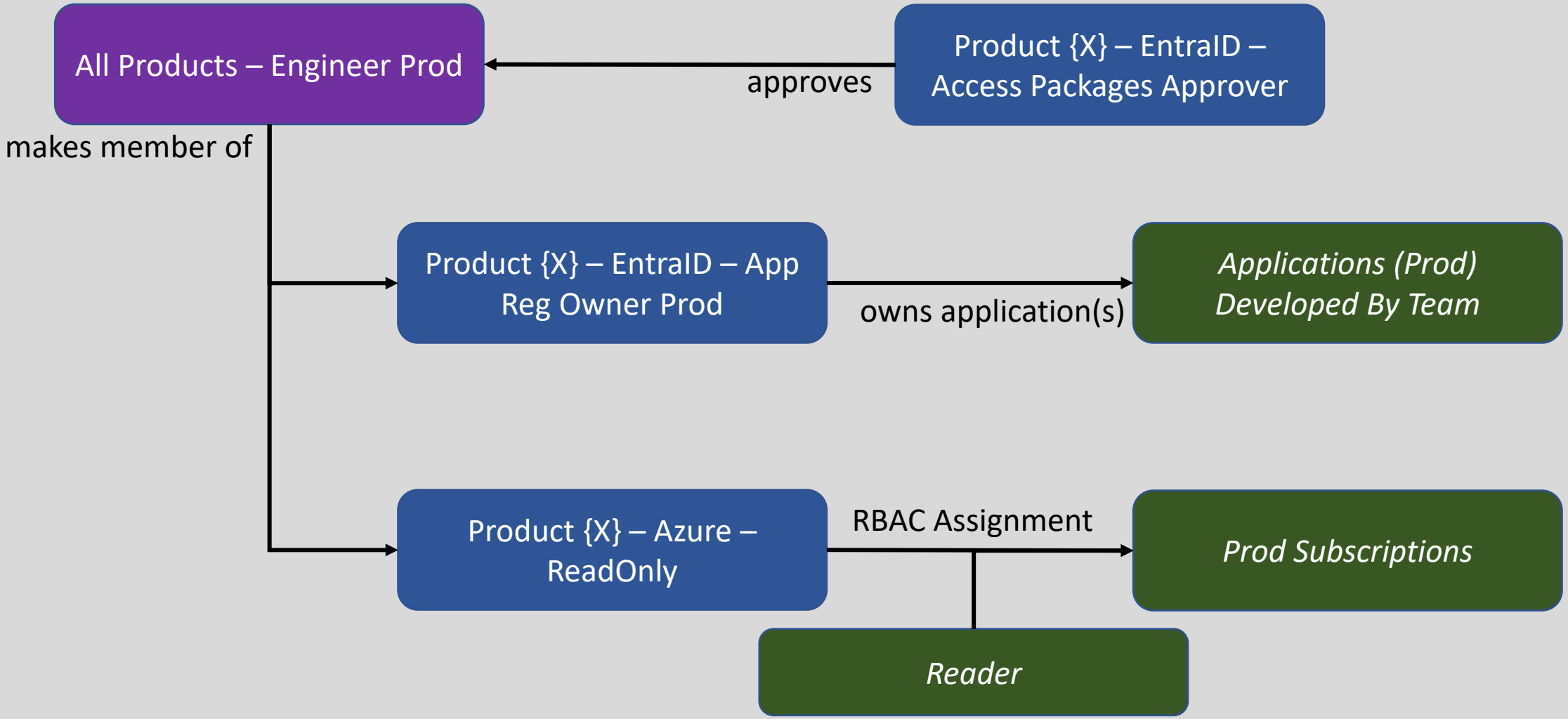
Design – All Products – Stakeholder



Design – Product {X} – Engineer Non-Prod



Design – Product {X} – Engineer Prod



Results

& Experience

Results & Experiences

Positive **experiences** & **outcomes**

- Business (PO) in control of access & authorizations
- Access Reviews are enforced
- Workable solution for engineers
- Provable in control of authorizations
- Justification for all changes are logged
- Privilege escalation is always logged

Results & Experiences

Open **issues** & **requests**

Review results are not immediate

Multiple reviewers cannot see each others' actions

No support for App Registrations as Access Package resource

Approvers cannot revoke authorizations effective immediate

DO TRY THIS **AT HOME!**

HENRY BEEN
Independent Devops & Azure Architect

E: henry@azurespecialist.nl
T: @henry_been
L: linkedin.com/in/henrybeen
W: henrybeen.nl

QUESTIONS?

NOW IS THE TIME!

DO TRY THIS AT HOME!

HENRY BEEN
Independent Devops & Azure Architect

E: henry@azurespecialist.nl
T: @henry_been
L: linkedin.com/in/henrybeen
W: henrybeen.nl

Use ECS Coins for Swag!

Top 3 win an Atari 2600+

1. Get the app
2. Visit sessions and sponsors, rate sessions
3. Earn ECS Coins
4. Spend ECS Coins

csmmt.eu/app

run events

THANK YOU,
YOU ARE AWESOME ❤️

PLEASE RATE THIS SESSION IN THE MOBILE APP.

Henry Been | @henry_been | linkedin.com/in/henrybeen