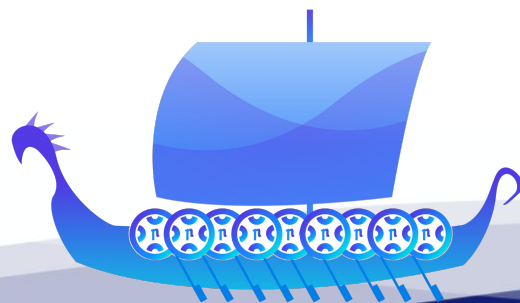




# Rönd

Open Source Security Enforcement  
over your APIs



# The importance of securing an API Platform

Rönd



Strong and reliable authentication and authorization mechanisms are essential tools to build efficient digital platforms and **protect companies' digital assets**.

As APIs are the **entrance of companies' network or application**, it is extremely important to secure their access



API Gateways are not enough in today's context, companies need to **set up reliable processes for their whole platform** ecosystem

# A Stronger Approach: Role Based Access Control

Rönd



When it comes to managing enterprise data in a platform used by many different people, you need to have these **people work on a restricted set of data with a different set of capabilities**.

- RBAC is an authorization mechanism that defines the concepts of **Roles**, **Permissions**, and **User Groups** as building blocks.
- The system is a true **mirror of your organization**, reflecting the **actual role** people have and the **specific actions** they may perform.



OPA is the CNCF open-source, general-purpose policy engine that unifies policy enforcement across the stack.

# Rönd: your open source solution

Rönd



Rönd is a lightweight container that allows you **define your own security policies** and **distribute them across your application**.

- Prevent **undesired API accesses**
- **Generate queries** to be applied to requests based on user permissions
- Manipulate responses to **remove sensitive information**



# How Rönd works

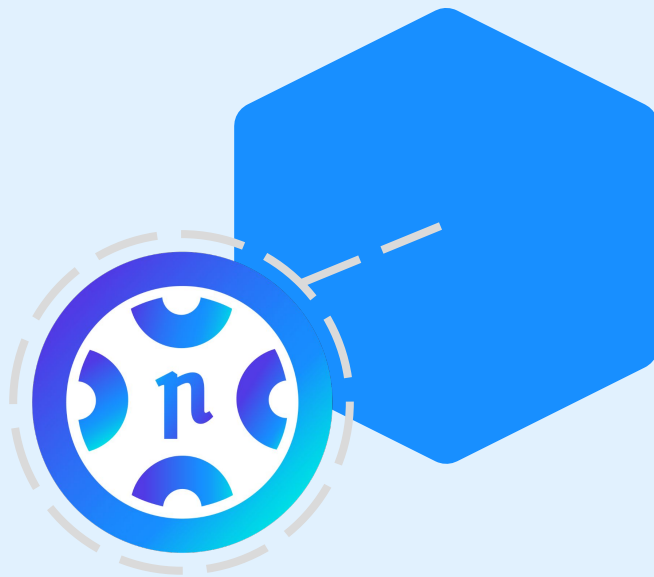
Rönd



It runs in Kubernetes cluster as a **sidecar container alongside the Pods**, meaning that each pod has an **extra container in charge of implementing the authorization controls**.

Rönd **intercepts the API traffic** and applies the policies to the API requests:

- **If policy requirements are satisfied**, Rönd forwards the request to the actual microservice.
- **If requirements are not met**, Rönd rejects the API invocation and the API call never reach the service itself, so it's more secure.



# Use Case - Financial Institution

Rönd



This advanced Access Control is an efficient tool specially for **Banking, Insurance and other Financial Institutions**, which manage a lot of sensitive data such as **Personally Identifiable Information (PII) and Payment Card Industry (PCI)** data.



Customers as final users  
can **read and write only  
their own data**



Employees are able to  
**access enough  
information** to perform  
specific tasks



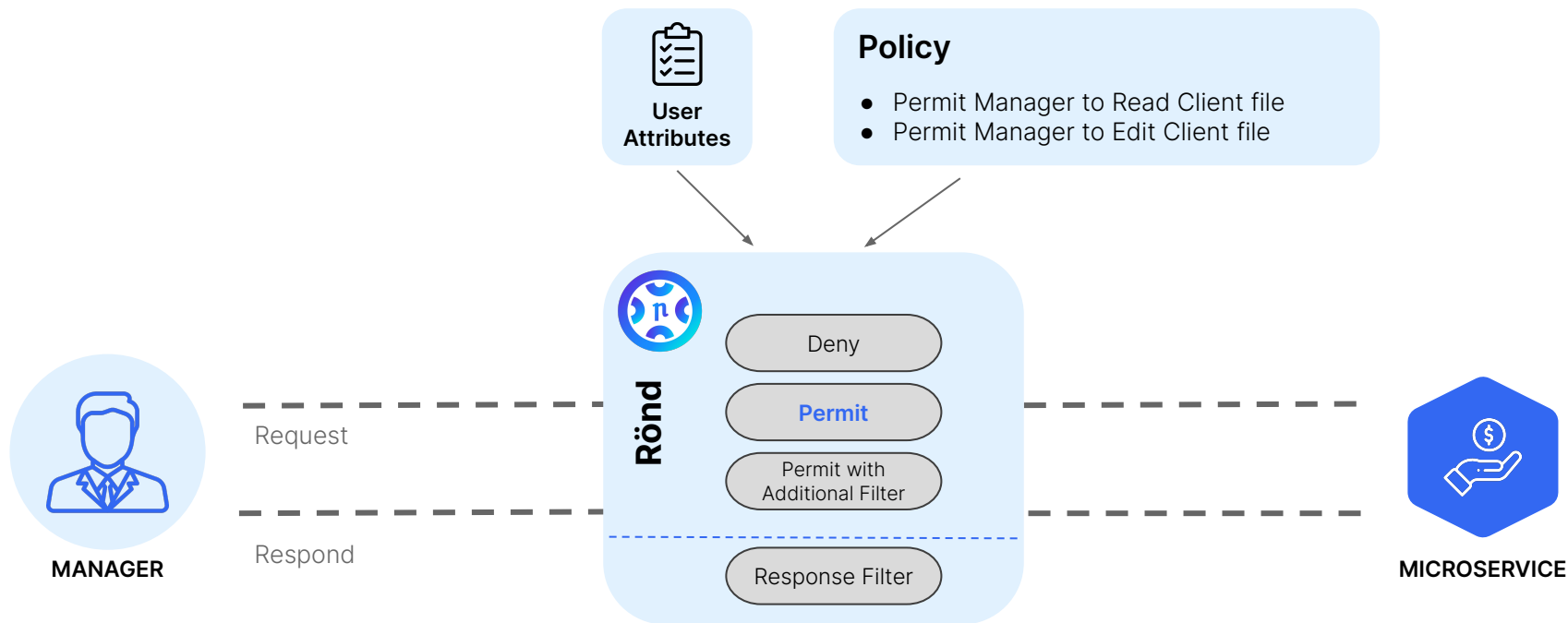
Managers can **access  
more sensitive data**  
compared to lower level  
employees

# Use Case - Financial Institution

Rönd



The branch manager has permission to read all data of client of the same branch he manages.



# Use Case - Retail Company

Rönd



This advanced Access Control is an efficient tool specially for **Banking, Insurance and other Financial Institutions**, which manage a lot of sensitive data such as **Personally Identifiable Information (PII) and Payment Card Industry (PCI)** data.



Customers as final users  
can **read and write only  
their own data**



Employees are able to  
**access enough  
information** to perform  
specific tasks



Managers can **access  
more sensitive data**  
compared to lower level  
employees

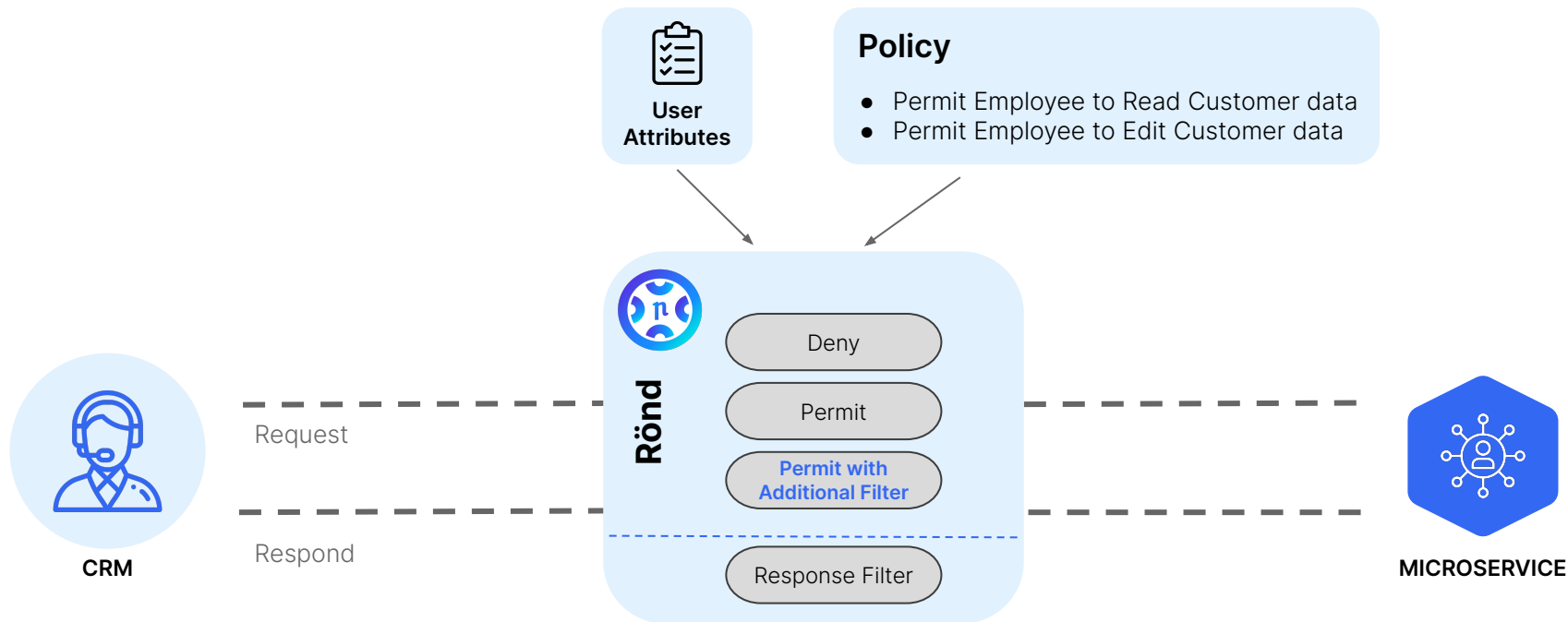


# Use Case - Retail Company

Rönd



The CRM assistant has permission to read Customer Data with additional filter for credit card number.



# Use Case - Healthcare Provider

Rönd



This advanced Access Control is an efficient tool specially for **Banking, Insurance and other Financial Institutions**, which manage a lot of sensitive data such as **Personally Identifiable Information (PII) and Payment Card Industry (PCI)** data.



Patients as final users  
can **read and write only  
their own data**



Medical staff is able to  
**access enough  
information** to perform  
specific tasks



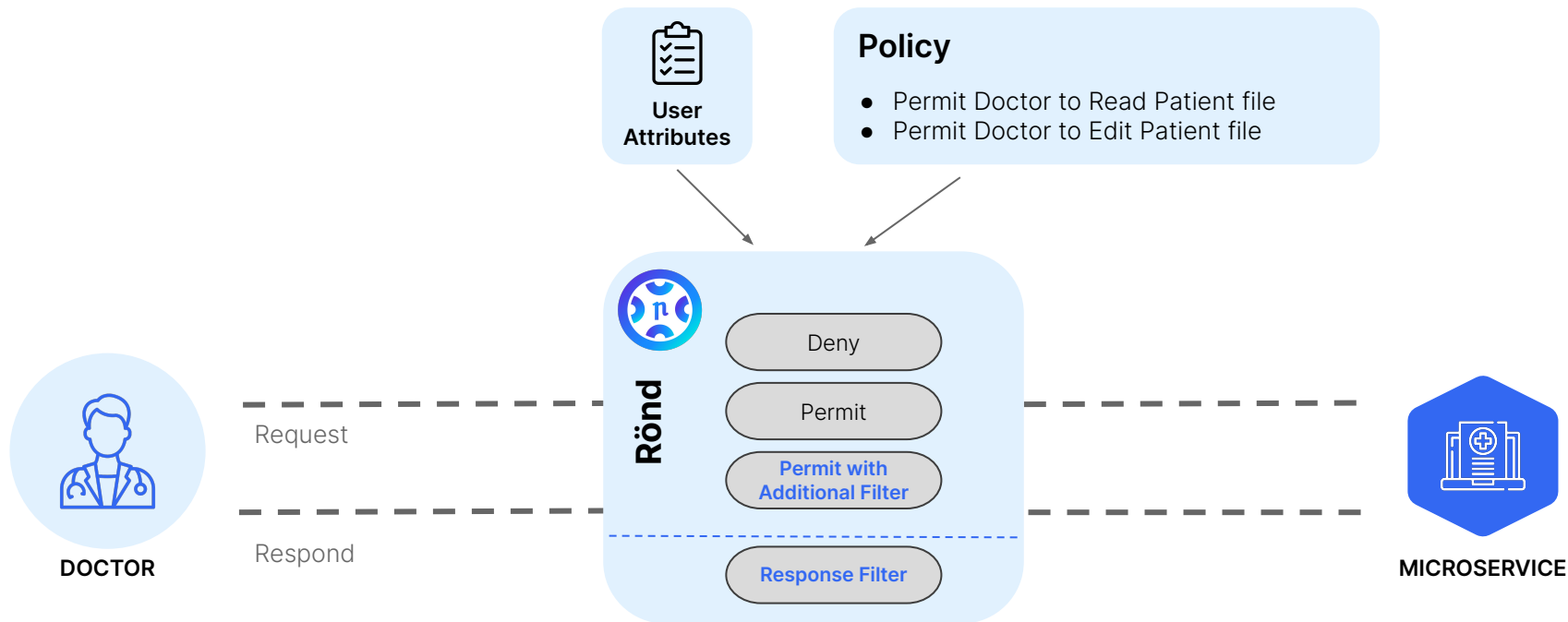
Doctors can **access  
more sensitive data**  
compared to lower level  
employees

# Use Case - Healthcare Provider

Rönd



The Doctor has permission to read patient's medical records from all hospitals of the state.



# Benefits

Rönd



## Higher levels of access security

Access based on attributes  
to avoid undesired access to critical  
resources



## 360-degree permission governance

Improve data and API security  
with a centralized and independent  
access to resources



## No single points of failure

Rely on sidecar container pattern for all  
your pods to enable strong and secure  
authorization processes



## Language independence

Adopt the solution independently  
to the language used to write the  
microservices



## Security management simplification

Rely on centralized policies  
distributed throughout all your  
authorization blocks



## Modular Approach

Enjoy incremental adoption  
among your services to test the  
reliability of the technology



# Thank You!