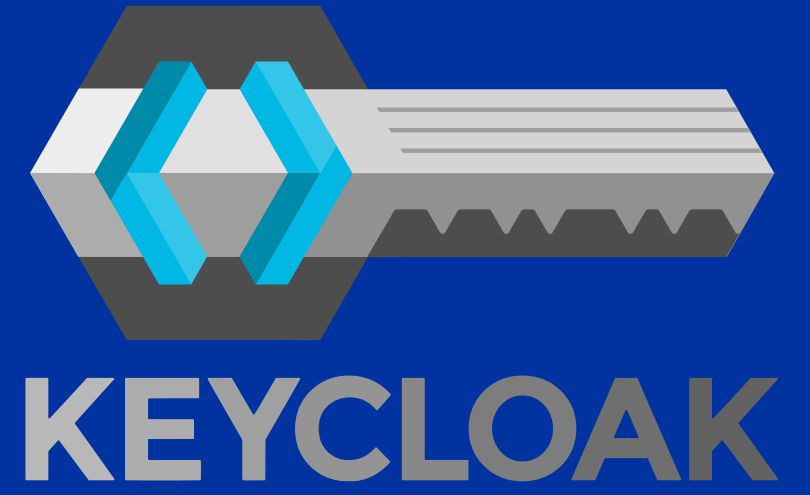




Twelve!

Six months of Single Sign-On on Kubernetes



Authors: Antonio Nappi, Sebastian Lopienski, Paul Van Uytvinck, Hannah Short
Presenter: Ismael Posada Trobo

Why SSO

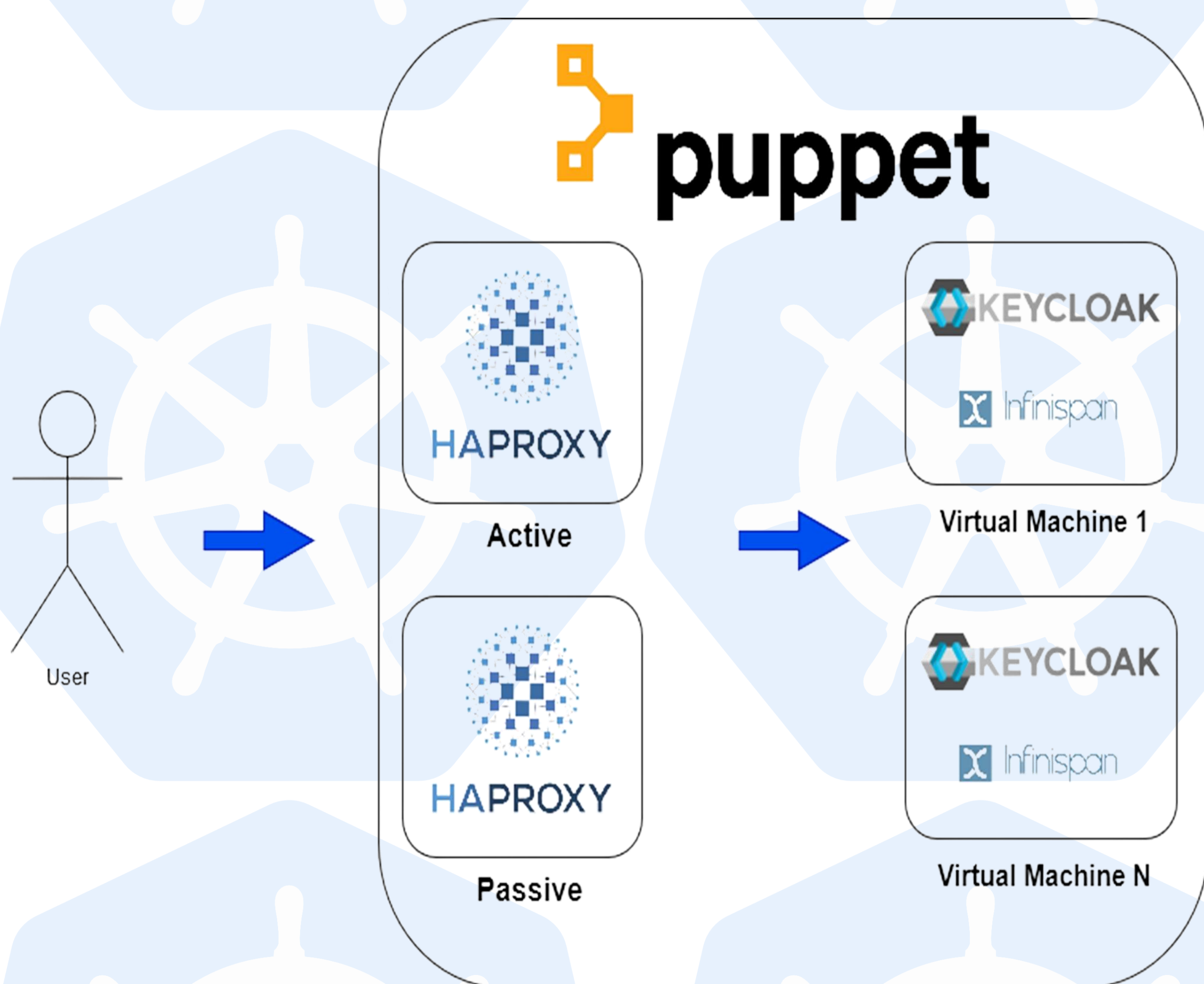
The Single Sign-On is one of the most critical services at CERN. It helps to

- Improve **usability**
 - One password for access to all organization's computing resources
 - Daily login with per-browser session valid up to 12 hours
- Improve **security**
 - Centralized place to enforce policies at organization level (e.g. 2FA)
 - Less risk of password leaking

Why modernize

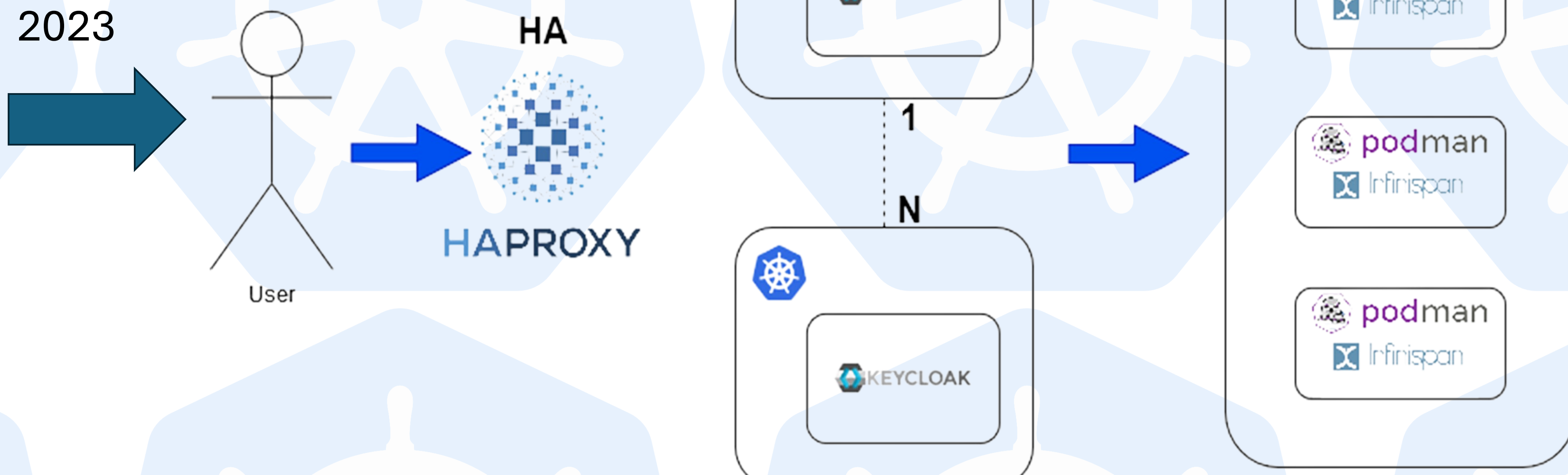
- Stability issues caused by performance bottlenecks and operational inefficiencies
- Puppet Module maintained by 1 person
- Scalability issues
- Inefficient personnel allocation
 - Service Managers were maintaining infrastructure as well as expertise in authentication
- Identity Server (Keycloak) and Cache (Infinispan) sharing the same process
 - Impossible to scale and monitor separately

Old Architecture



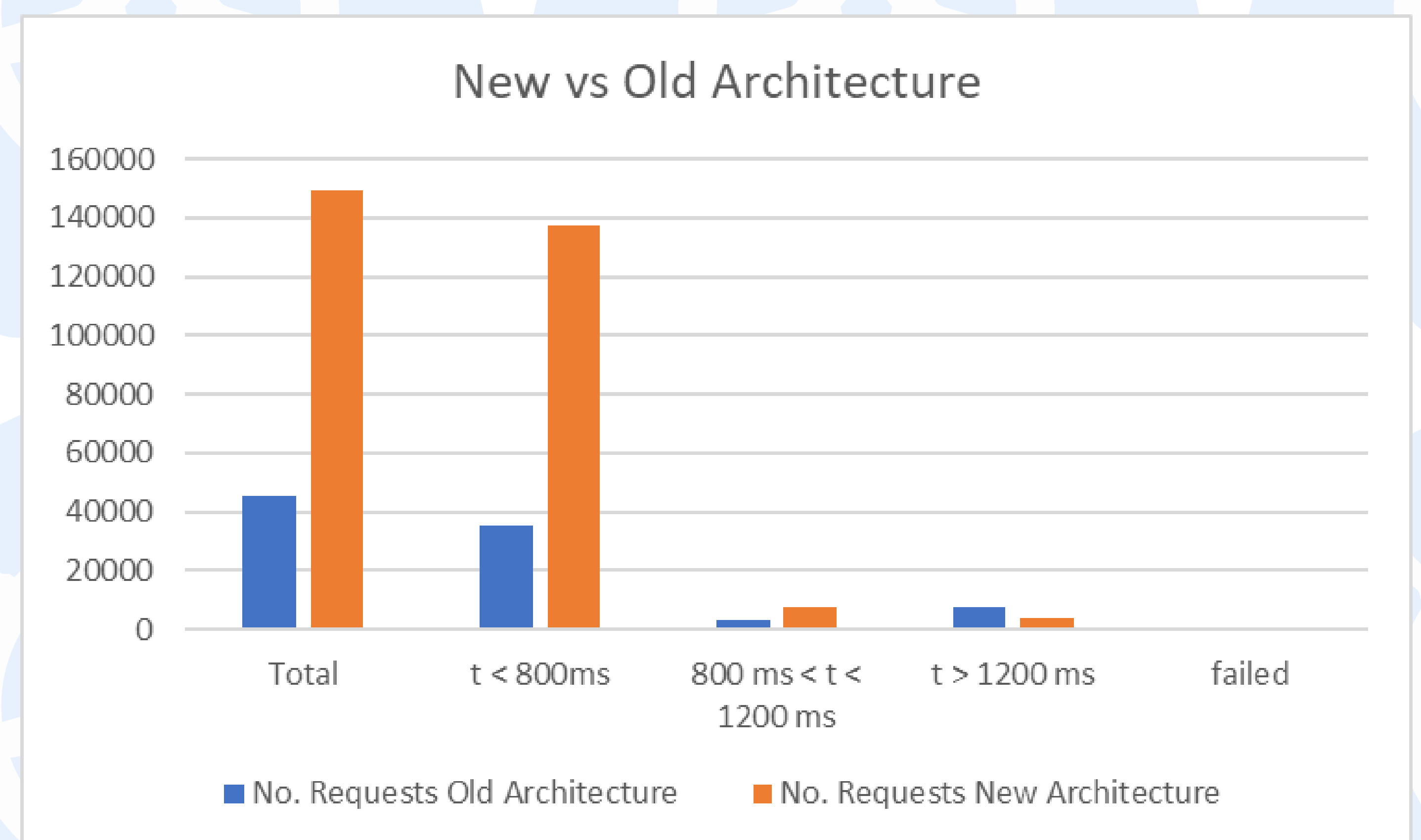
Moved on 11th of September 2023

New Architecture



Benefits

- Performance improved by **300%**!
- Outsourced infrastructure management
- Authentication experts can focus on their own domain
- Reduced infrastructure service incidents by **86%**!
- Kubernetes enabled:
 - Faster and easier operations
 - Keycloak is stateless!
 - Implementation of GitOps principles
 - Versioning and tracking of changes
 - Easy rollback



October 19 - 25, 2024

CHEP 2024

