

**Assignment 1**

**Assistive Technology Passport System**

**Systems Architectures - TU059**

KANISHKAR THIRUNAVUKKARASU (D23124630)

DATE : 03/03/2024

# System Overview

Assistive Technology revolutionizes accessibility, allows individuals with disabilities to overcome barriers and achieve greater independence in daily life. In this project we will explore the non-cloud-based architecture of the same and analyze its strengths and weaknesses.

**Application Roles**: Users, Organization, Admin

**User Role Flow**:

* User can create an account with documents supporting their disability, age, residence documents.
* Users can update their profile by updating school, college, work, medical documents, and tool accessibility required details.
* Users can manage their documents and share the documents with the organizations.

**Organization Role Flow**:

* An organization can only be of one kind - school, college, hospital, or workplace.
* Each organization can manage their current users.
* Organization can request users to share their information partial/complete data in a document.

**Admin Role Flow**:

* Admins are authorized personnel who background checks the new account creation.
* Admins can block/remove an account.
* Admins have role-based access control (RBAC) to database.

**Data Involved**:

* Health information such as medical certificates, scans, medication details, allergies etc..
* Personal data of the user such as name, Personal Public Service (PPS) [1], birth date & contact details.
* Environmental context which covers information about the user’s environment and their dependence on physical environment, like lighting conditions, noise levels etc.
* User feedback data which provides insights on the tool usability and satisfaction level which tool further enhances tool.

**Data management requirements**:

* Securing data to protect the sensitive data for patient by ensuring encryption of data both in transit and at rest, role-based access control in database and regular security audits
* Compliance with relevant data protection regulations such as Health Insurance Portability and Accountability Act (HIPPA) [2] and General Data Protection Regulation (GDPR) [3].
* Data integration which allows real-time and offline data from common data sources.
* Data backup & recovery to prevent data loss or other foreseen events.
* User consent and transparency in obtaining consent from users and sharing the information on which data is collected, how it will be used, and with whom it may be shared.

**Important features**:

* UI /UX Customization - Designing features like Keyboard Navigation, Screen Reader, Color Contrast, Compatibility, Accessible Forms, Resizable Text, Focus Indication [4].
* Upload file - Users can scan and upload their documents related to their disability.
* Download file - Users can download their documents.
* File sharing - Users can share files / parts of the file with an organization.
* Manage Docs - Users / Organizations can manage and organize the files.
* Notifications - Receive a notification if a file is edited, deleted, or shared.
* Training & Support - Users can watch training resources and contact support if any help is needed.

# Architecture Diagram & Design Choices

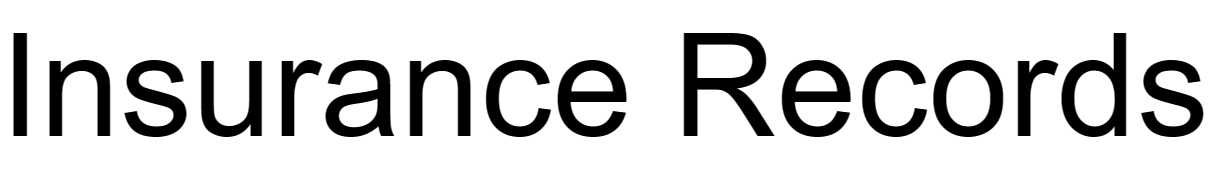
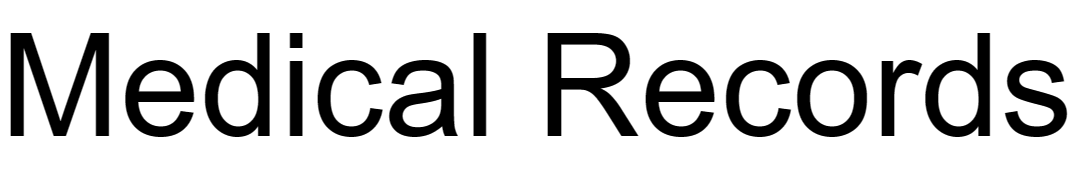
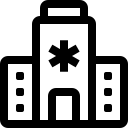
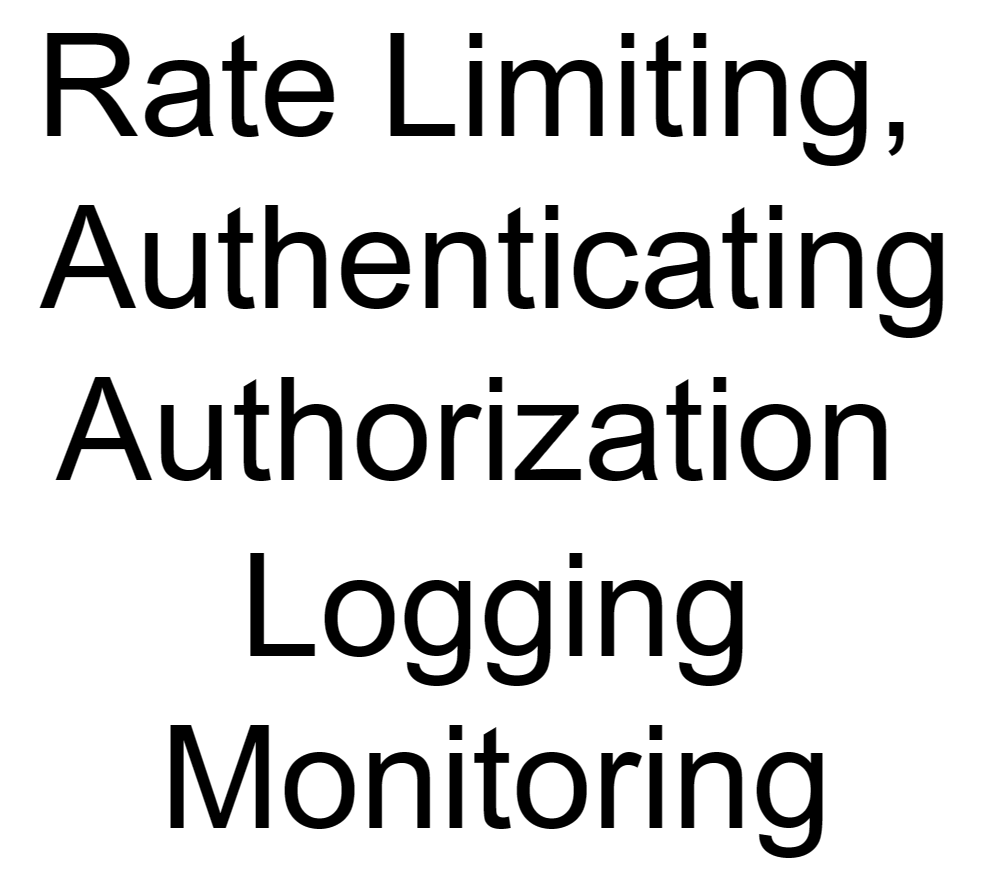
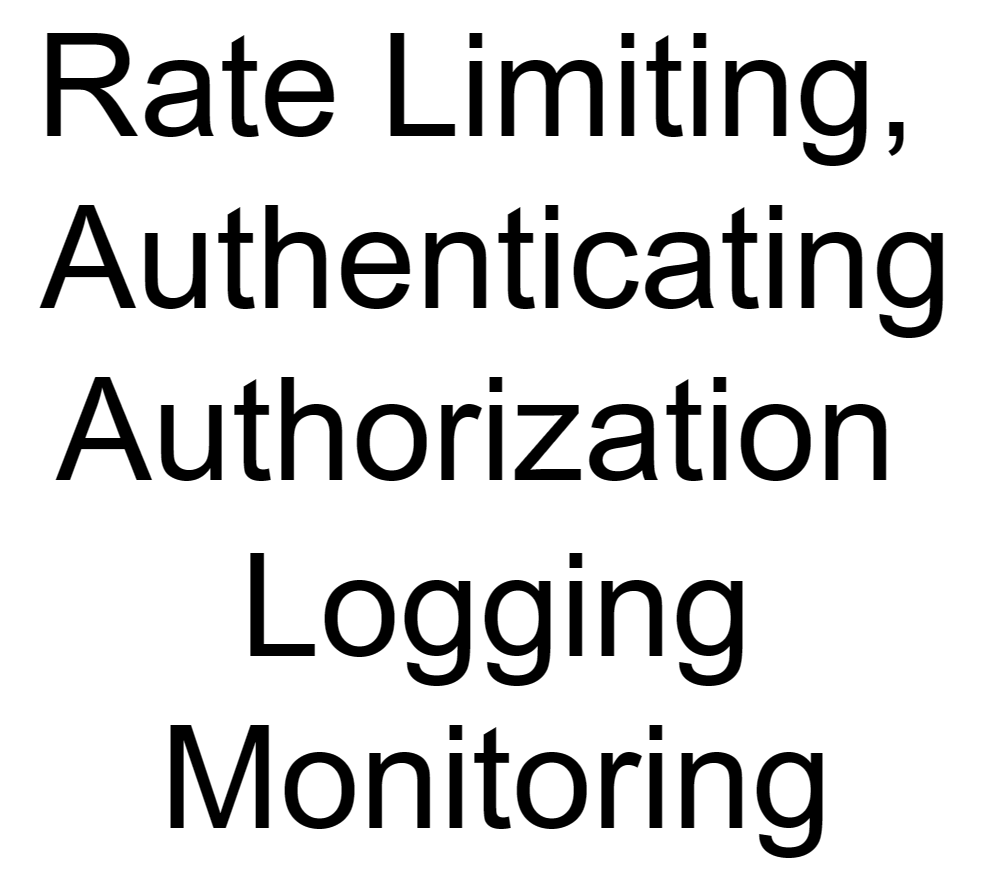
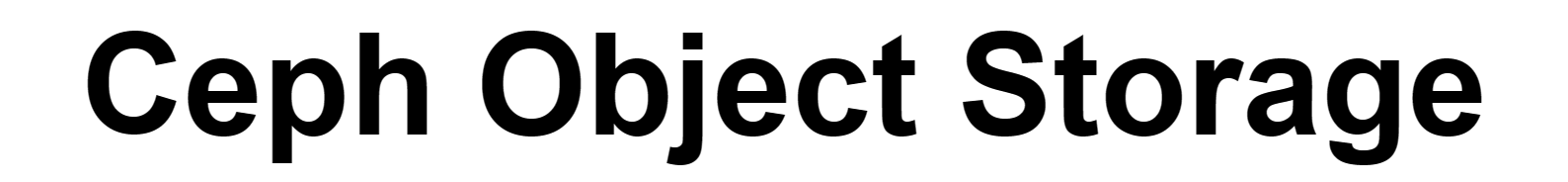
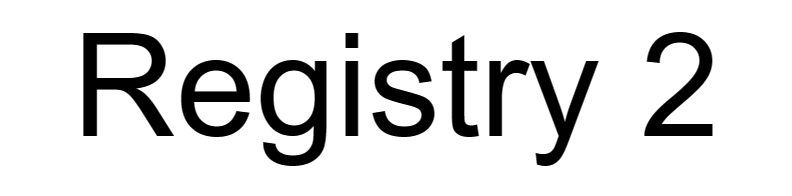
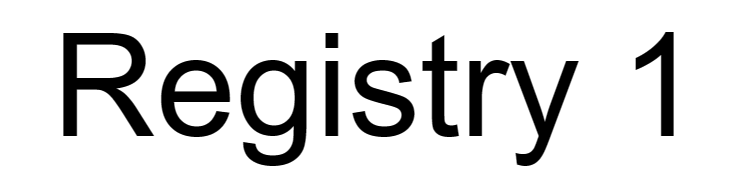
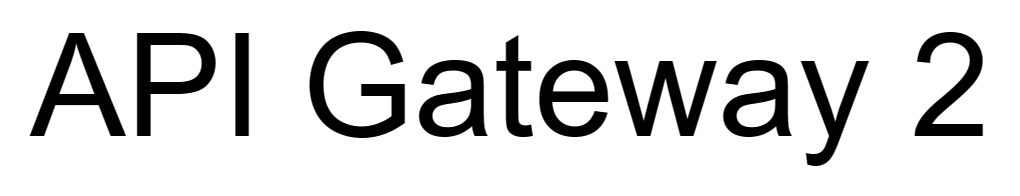
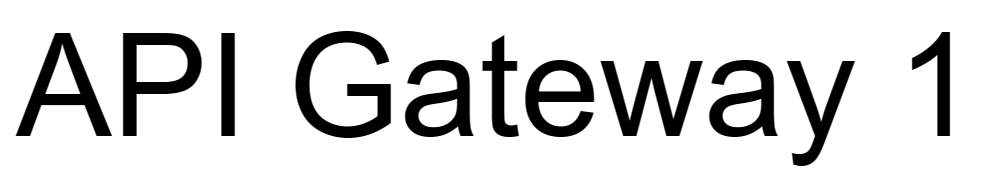
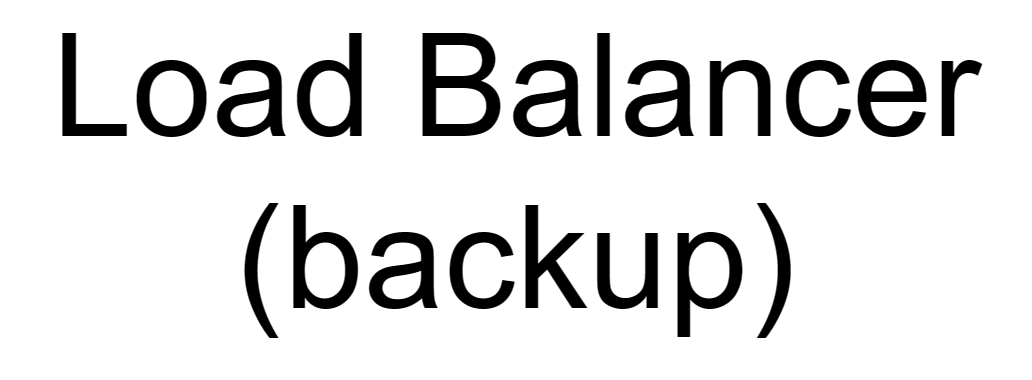
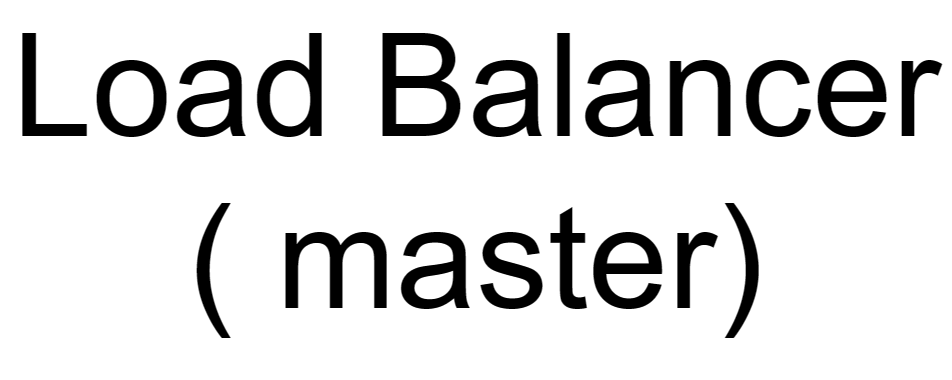
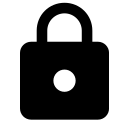
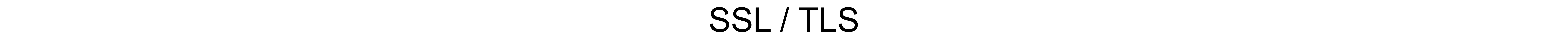
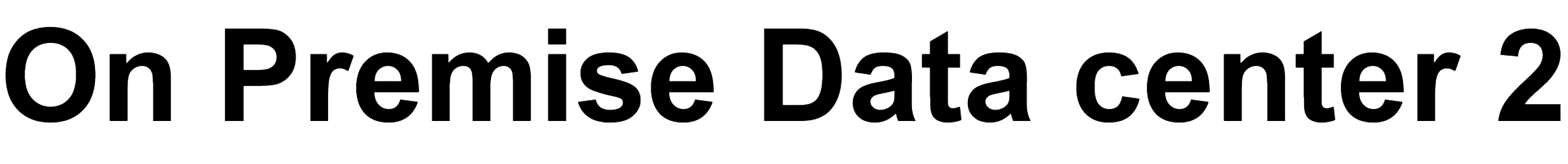
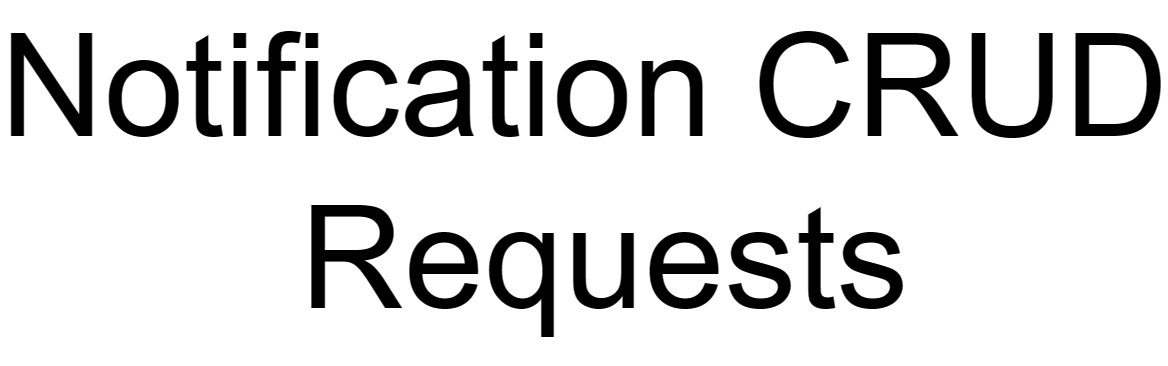
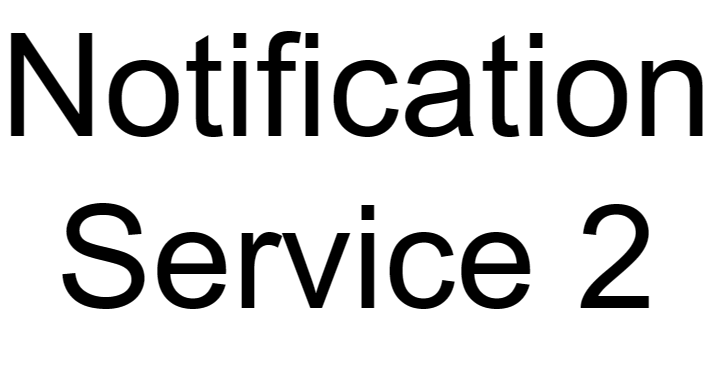
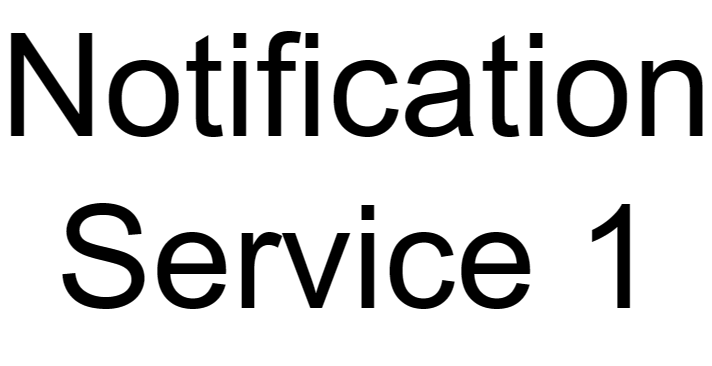
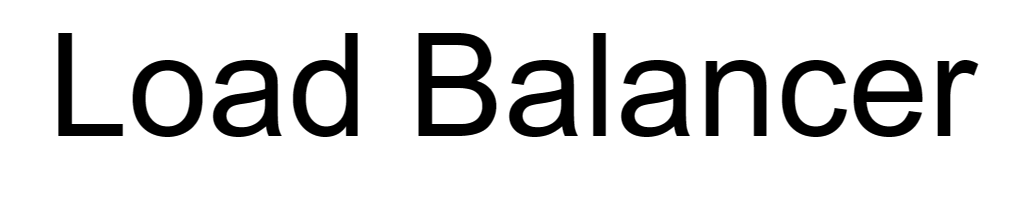
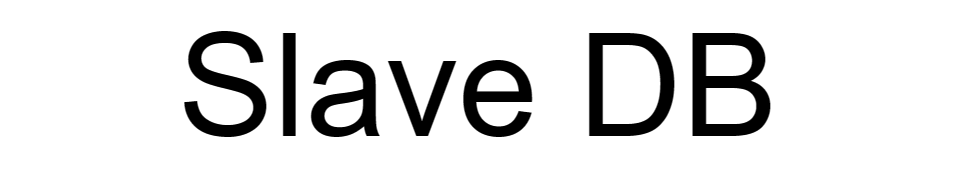
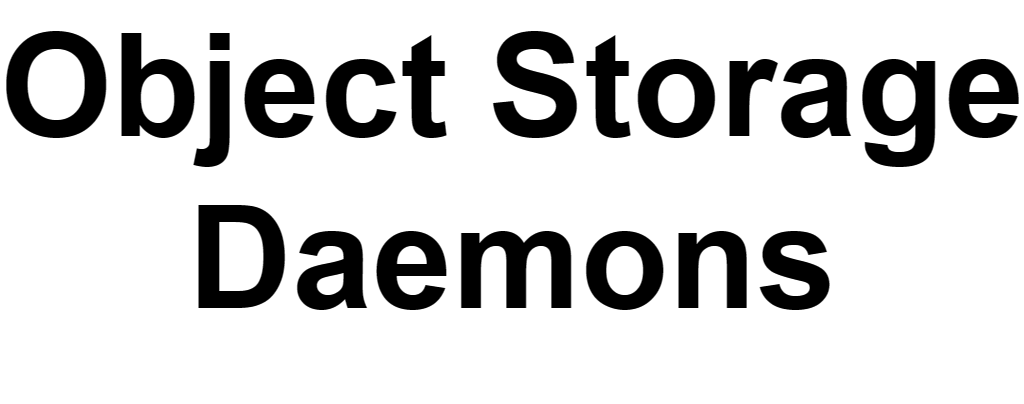
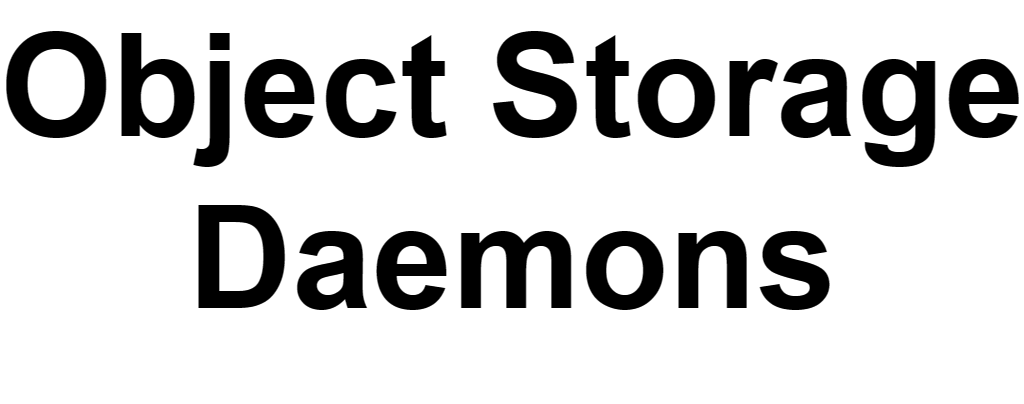
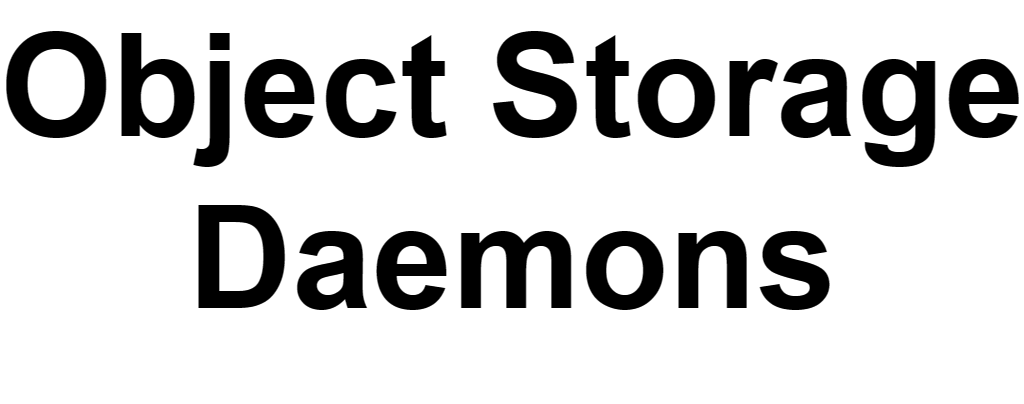
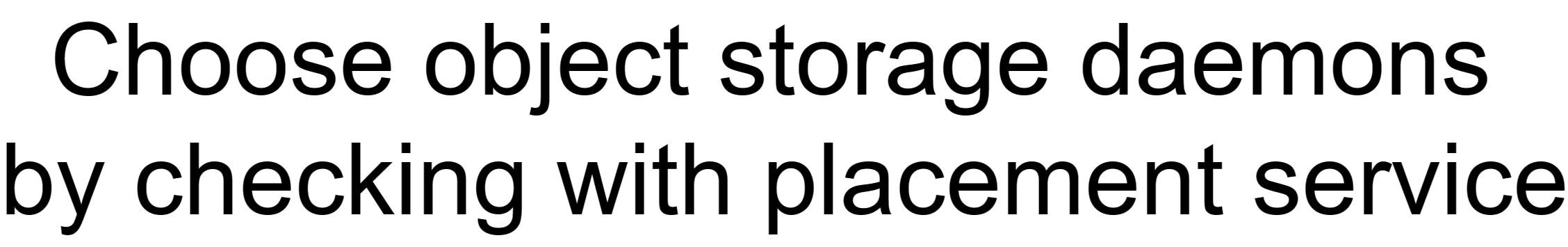
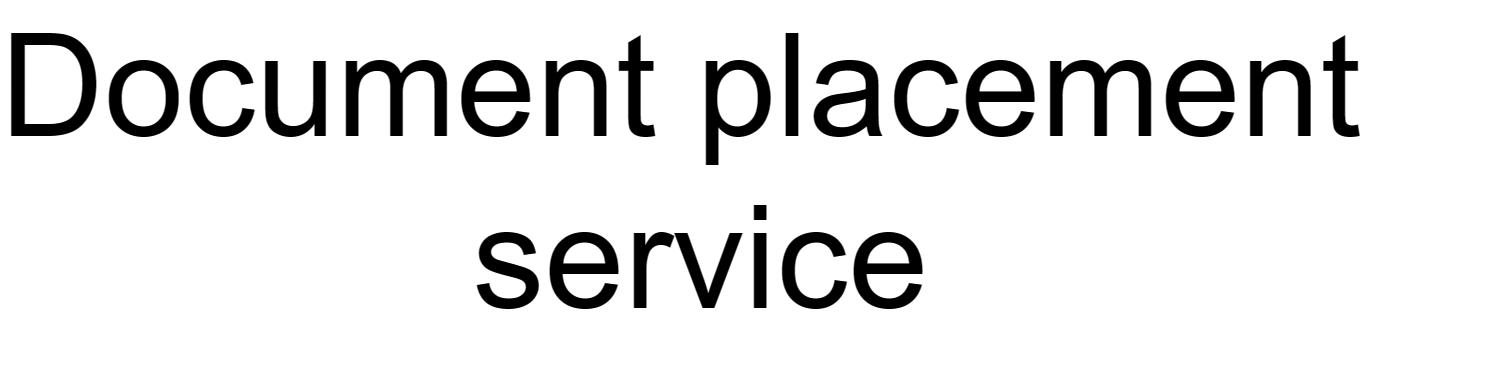
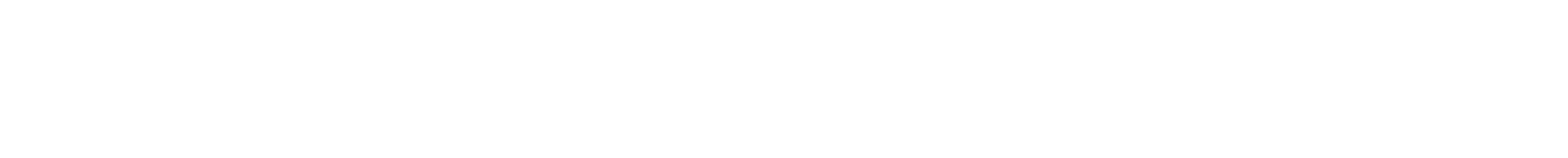
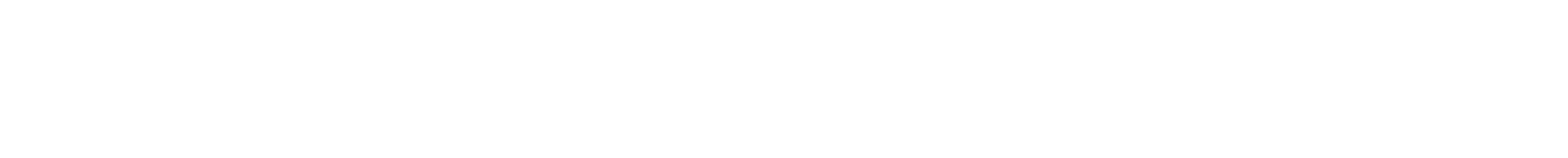
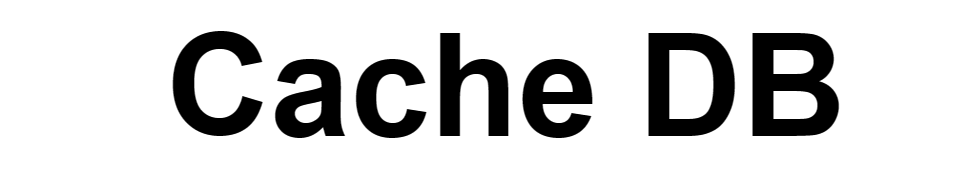
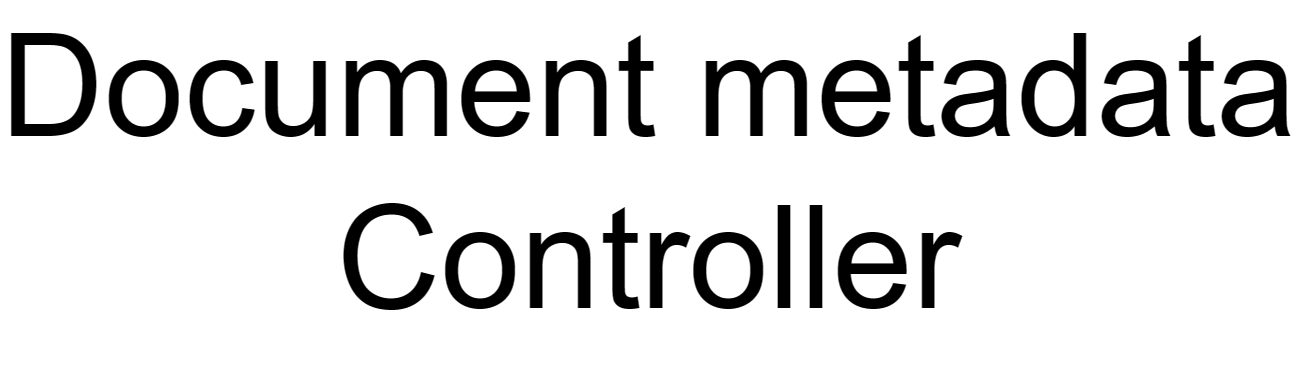
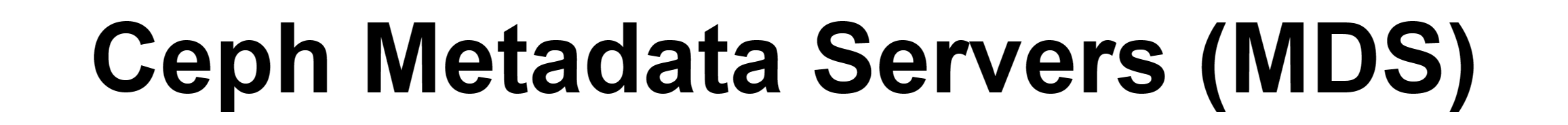
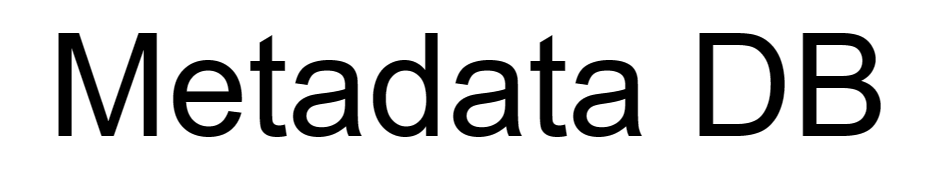
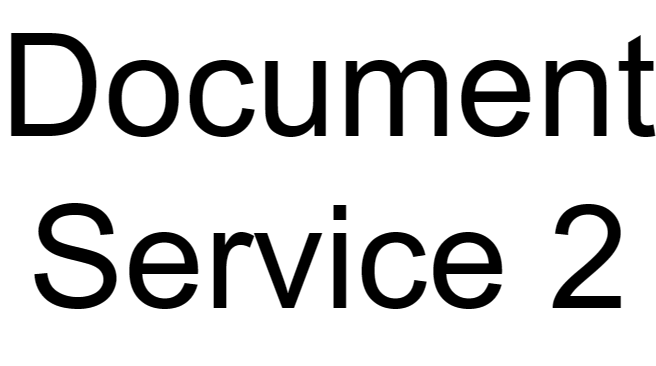
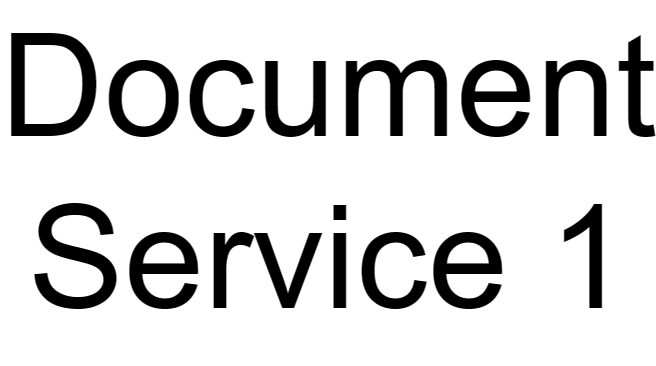
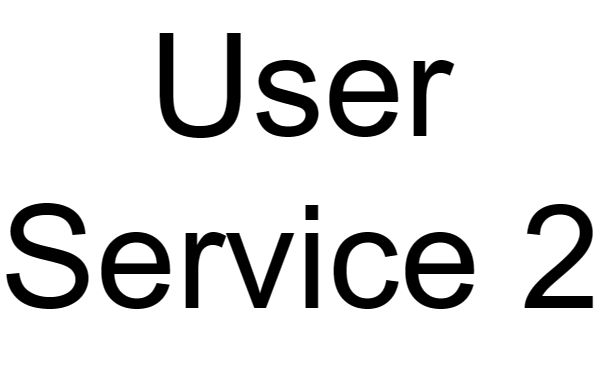
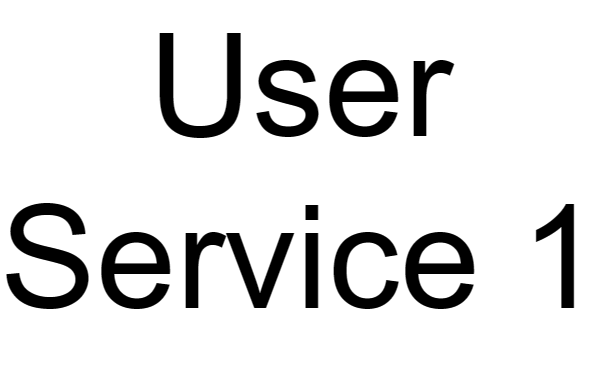
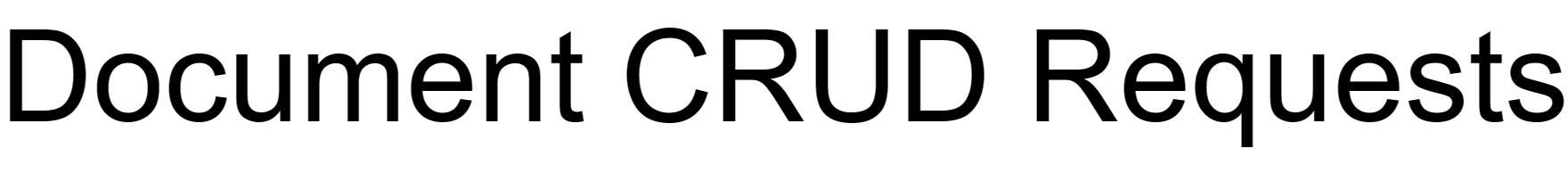
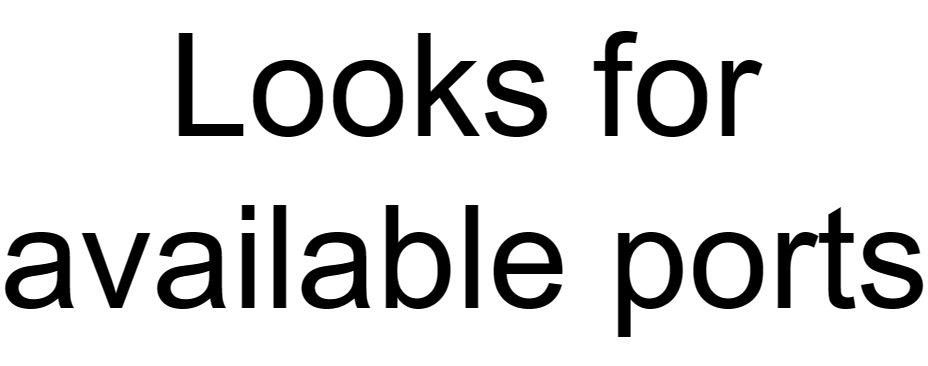
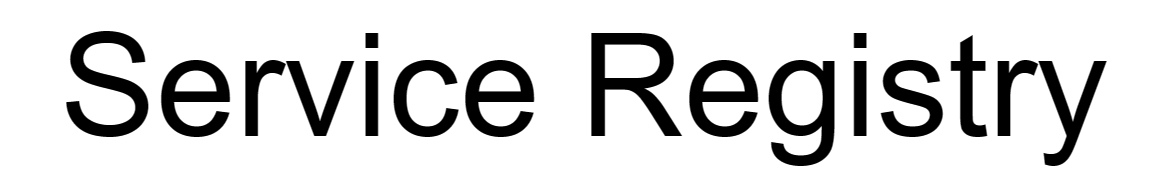
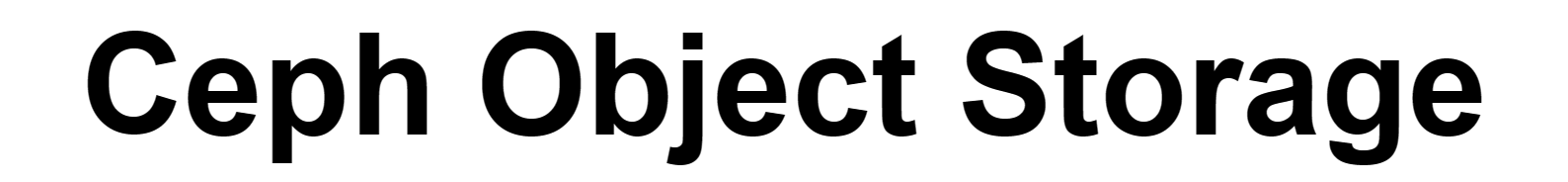
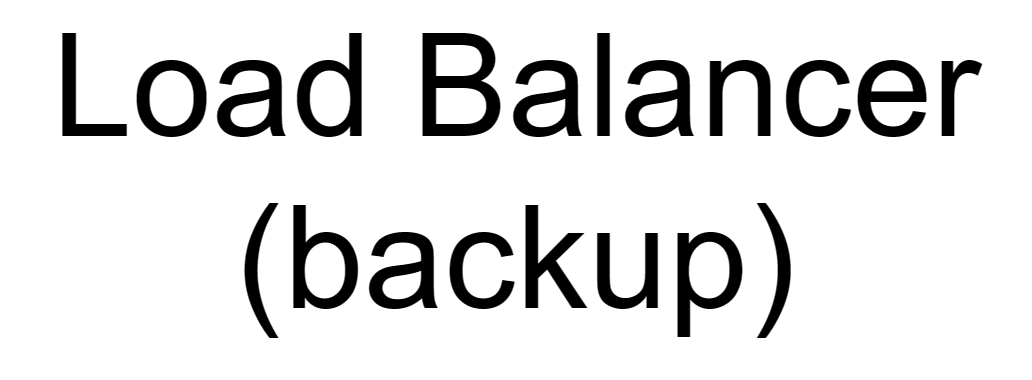
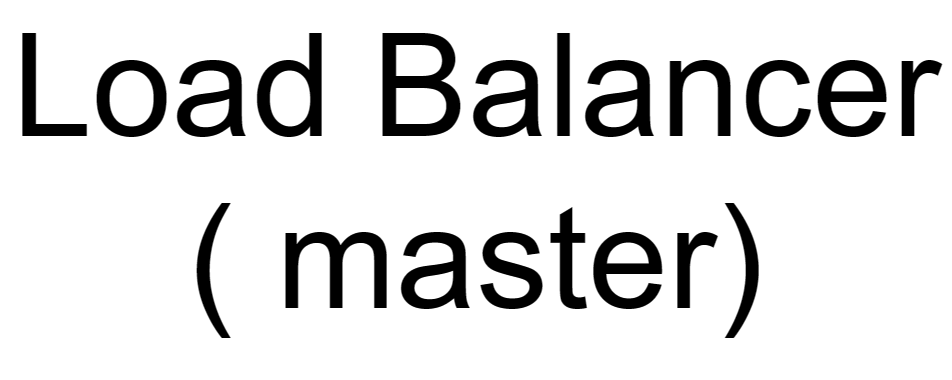
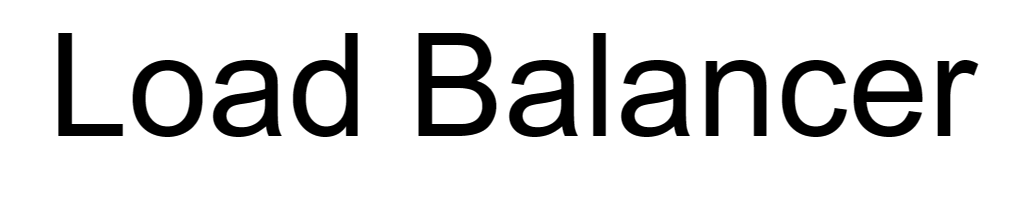
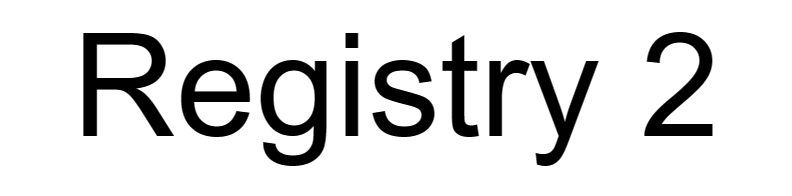
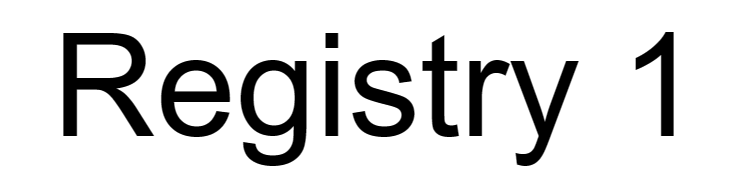
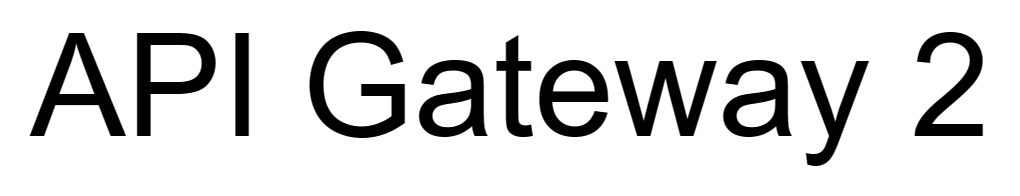
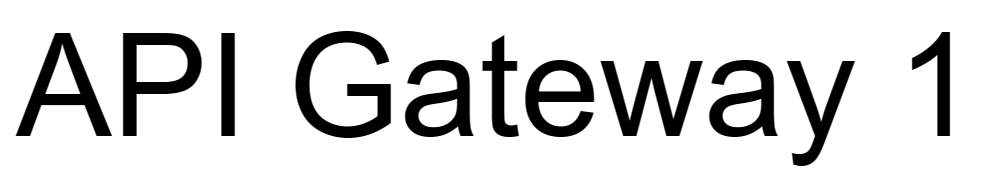
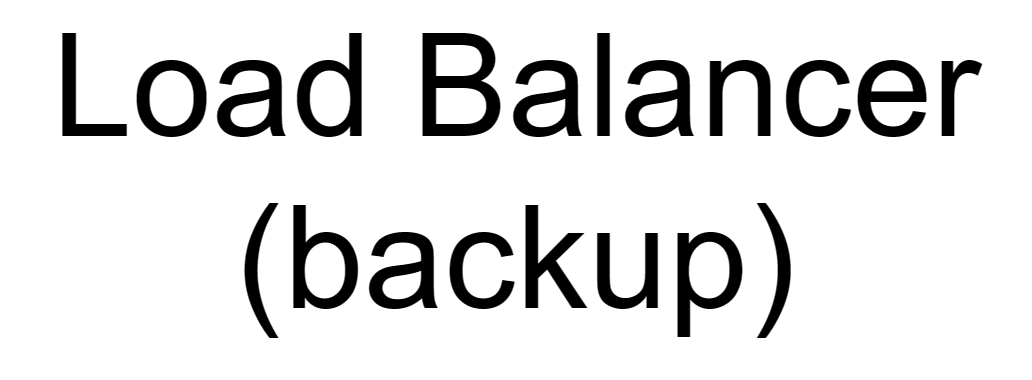
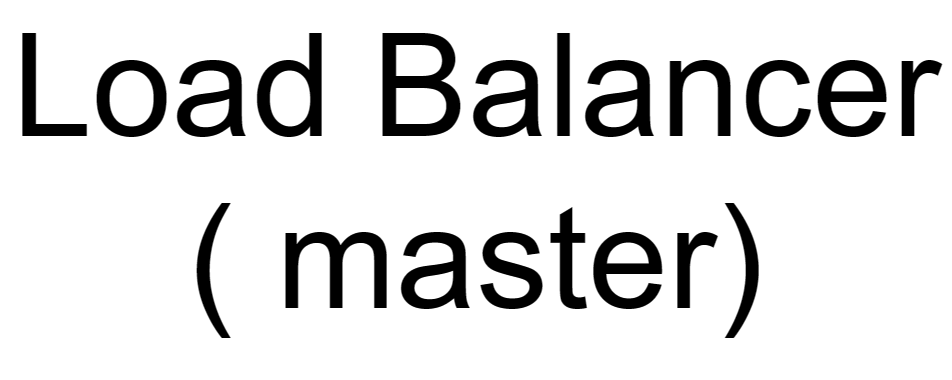
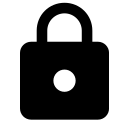
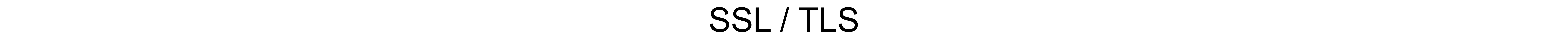
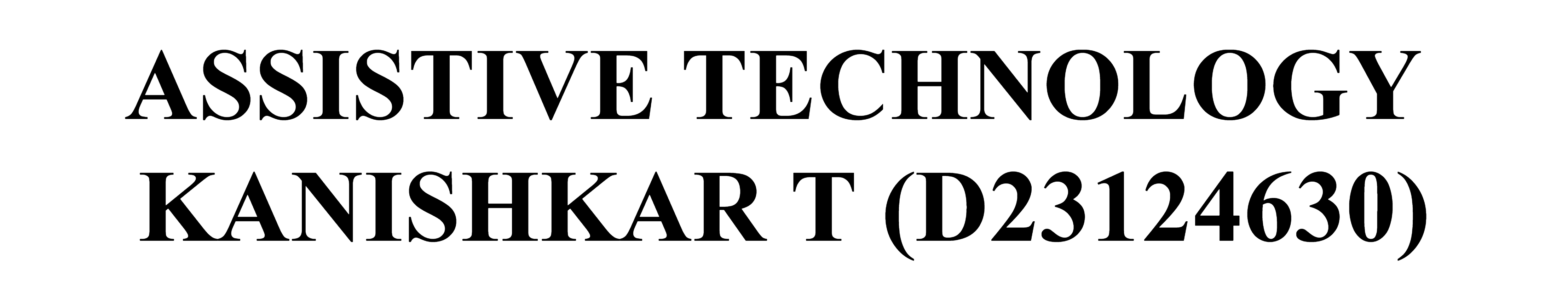
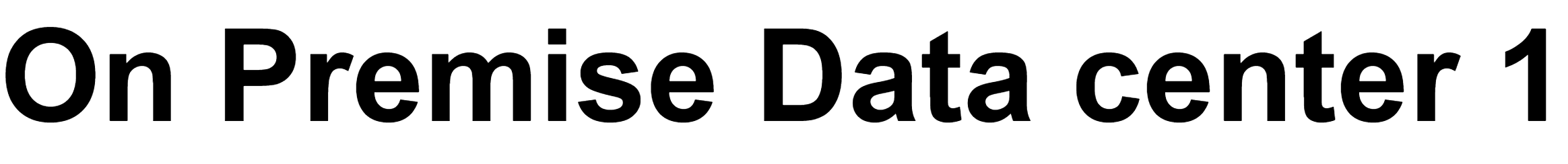
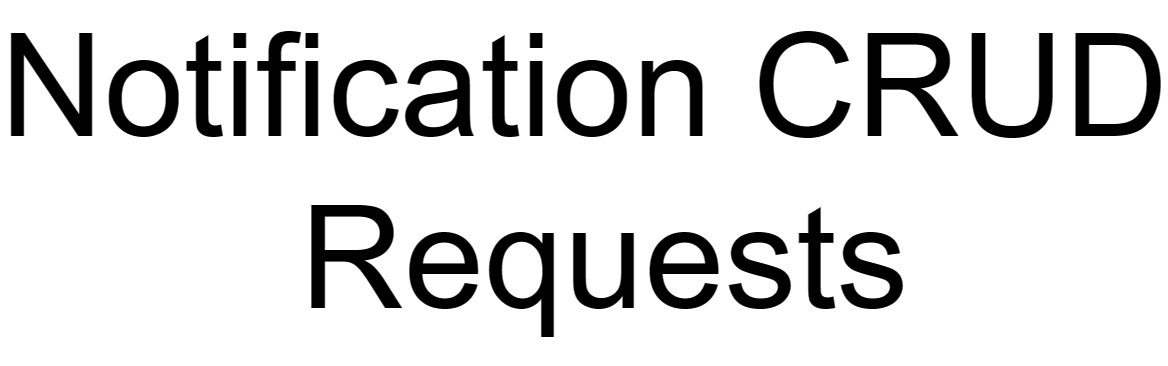
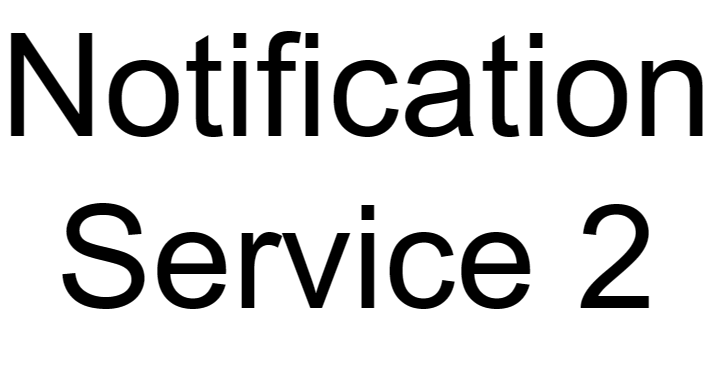
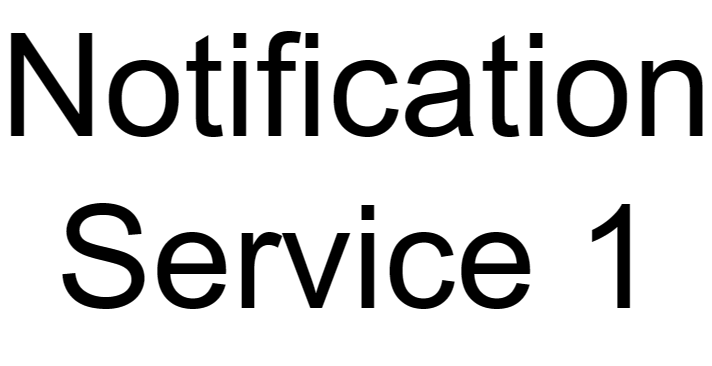
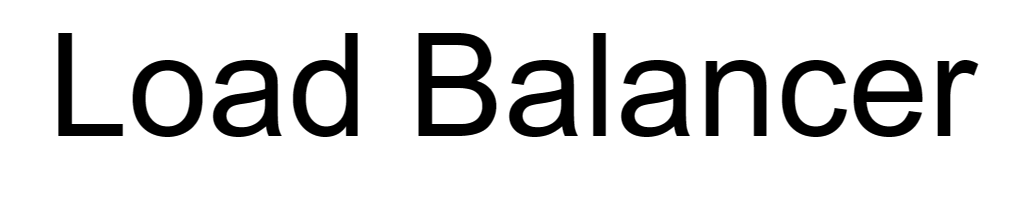
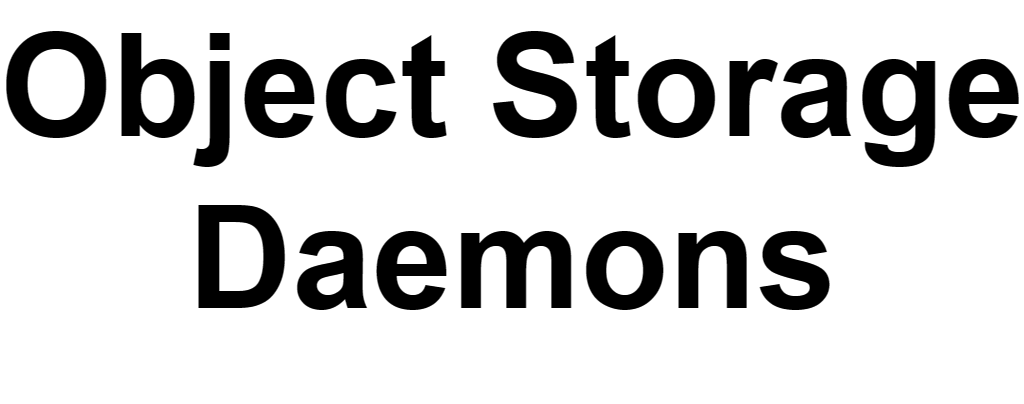
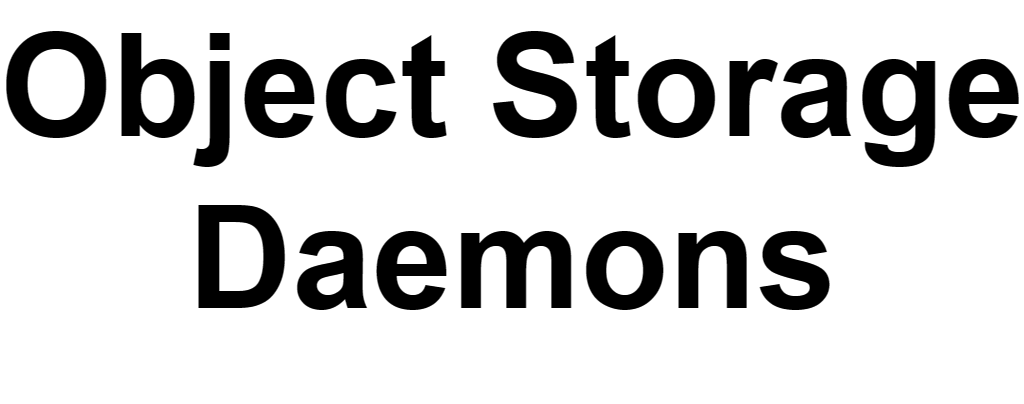
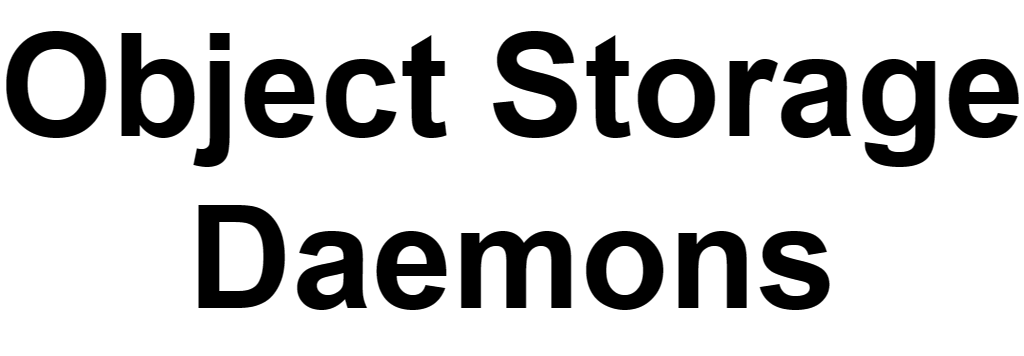
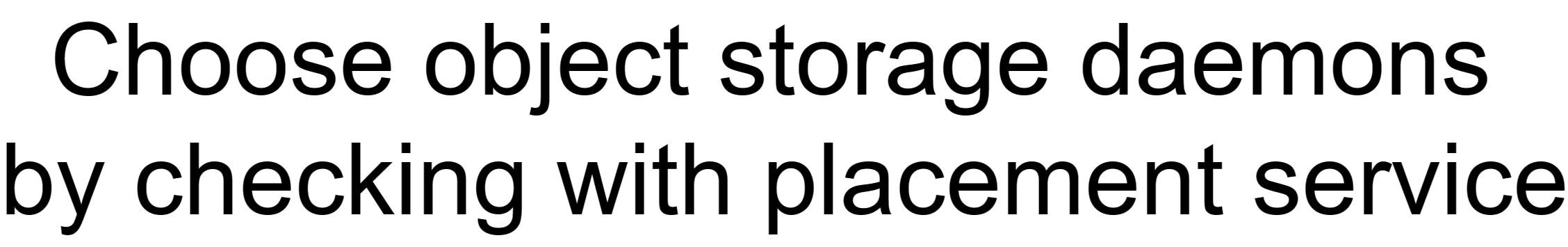
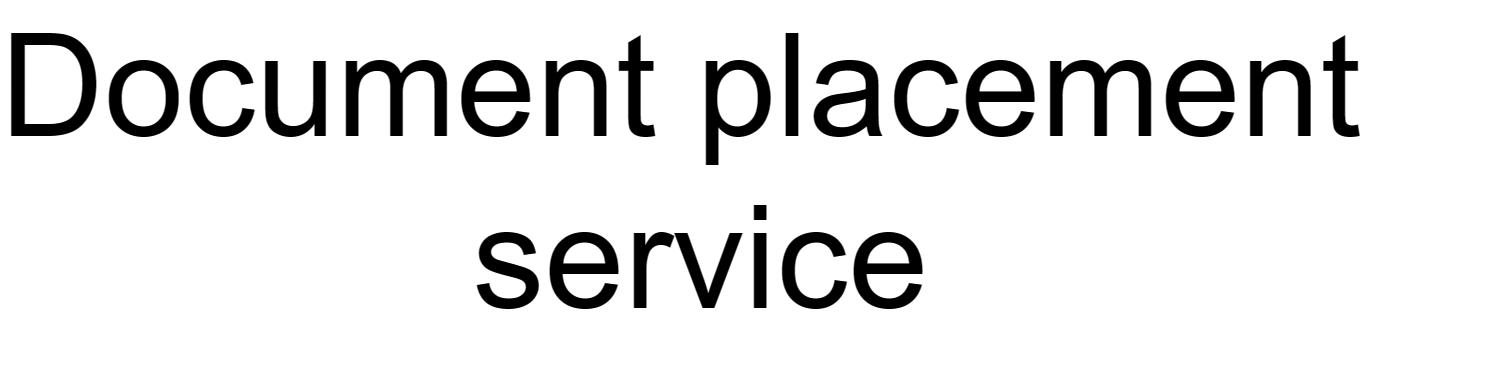
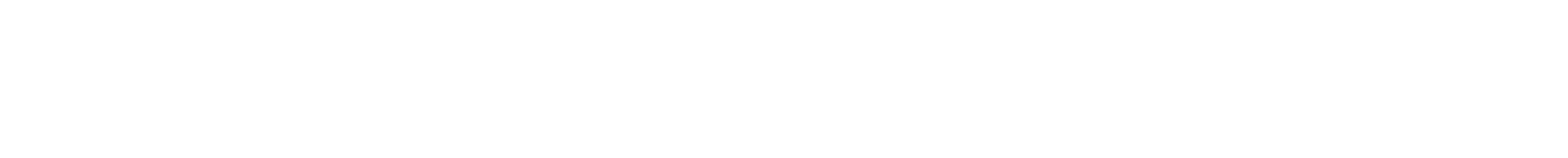
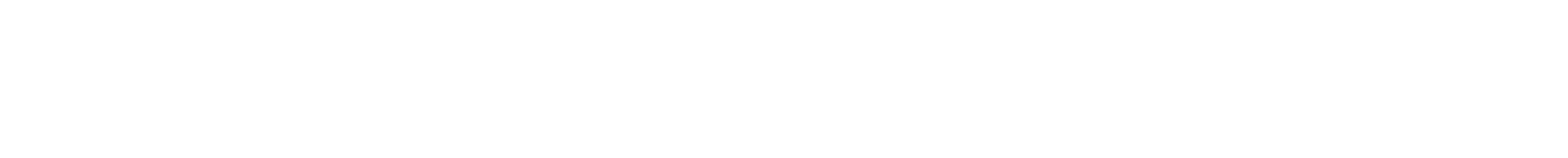
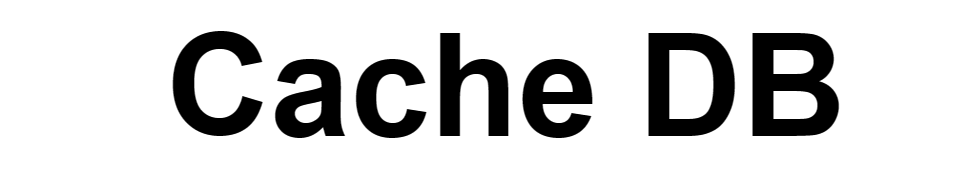
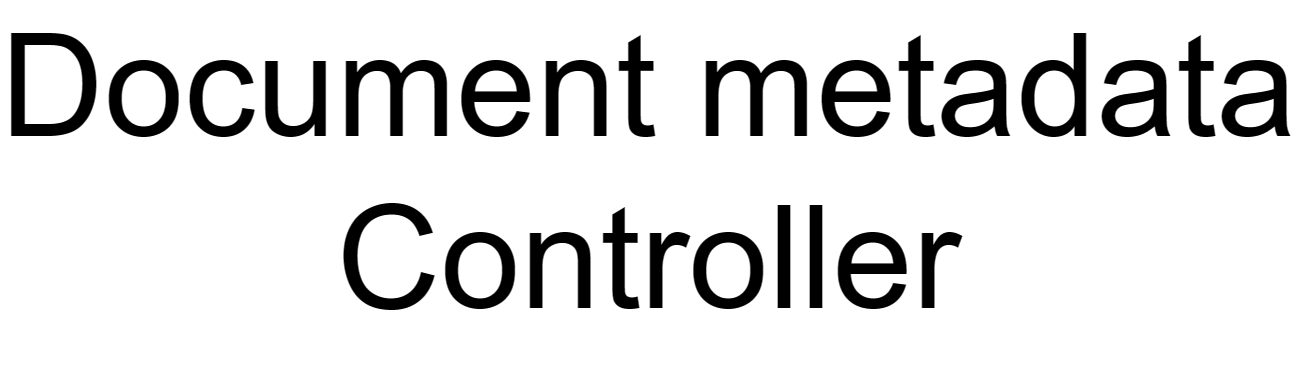
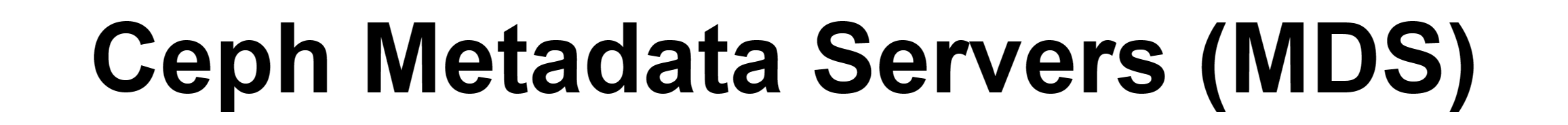
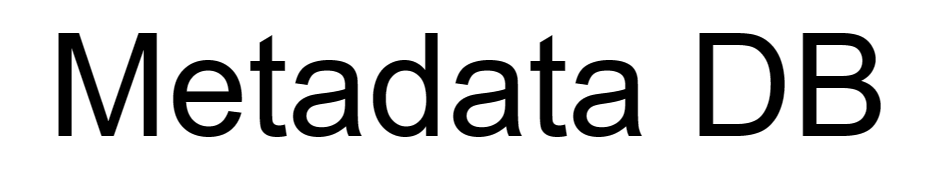
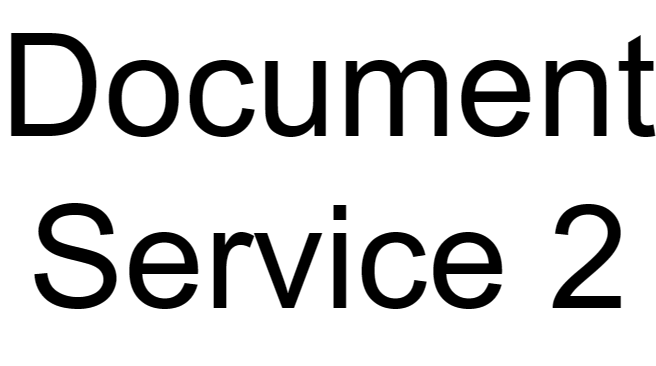
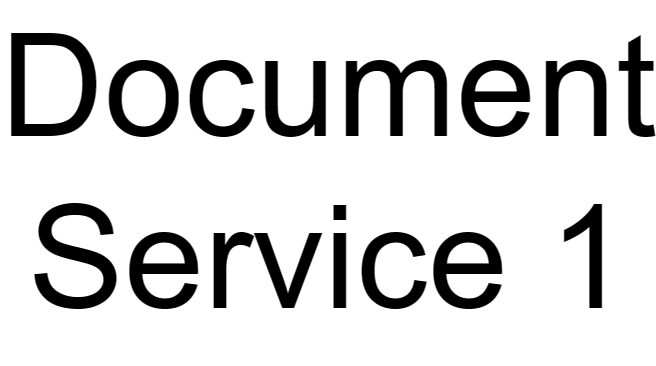
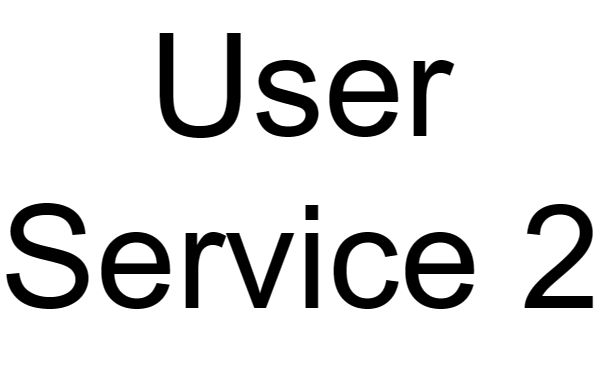
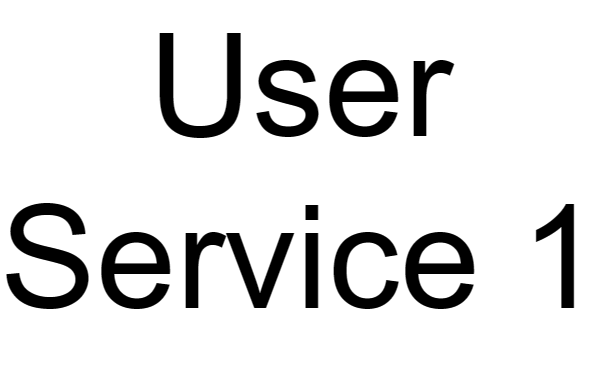
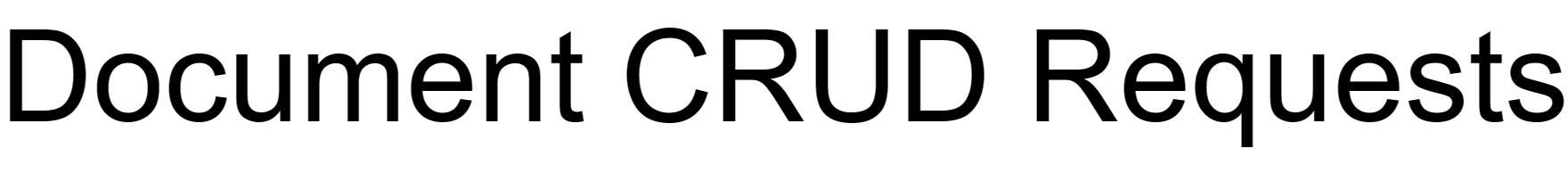
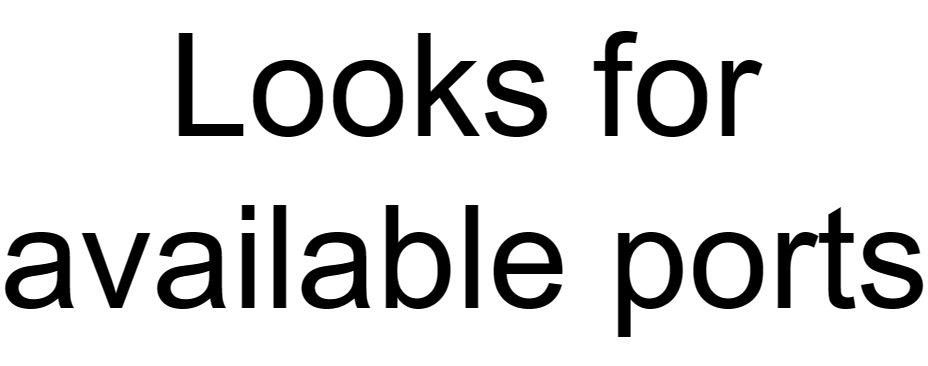
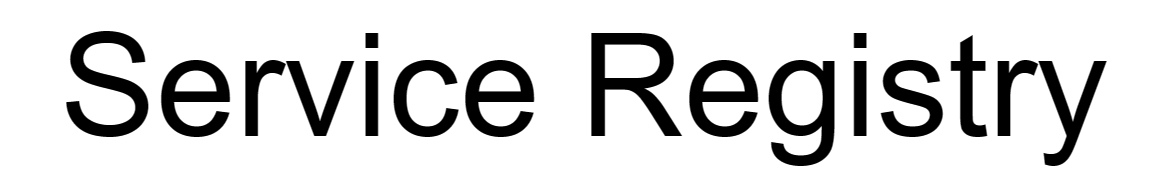
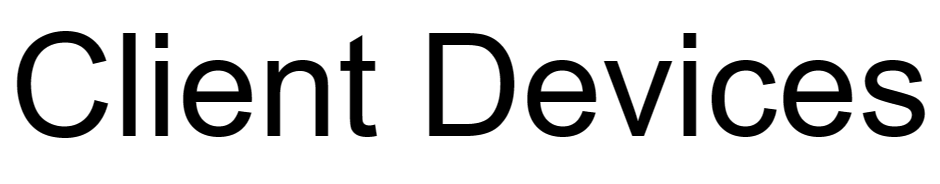


Fig 1 : AT Passport architecture diagram

# System Reliability

**Distributed Architecture**: The assumption of the design was made that it will be used by millions of people[5] and to handle the high volume of usage the AT Passport system is deployed in two datacenters[6] [7] so, If there are any unforeseen circumstances in one datacenter, all requests will be routed to other datacenter.

**Load Balancers**: To avoid Single point of failure SPOF[8] the design has backups for load balancers using Active-Passive Clustering and it also manages service based on user location and redirects the requests to nearest available datacenter.

**Caching Mechanisms & Messaging Queues**: To reduce latency, the system has a caching mechanism which helps in accessing data faster instead of fetching each data from database. Asynchronous requests to continue with other tasks while waiting for certain operations to complete which can be achieved by message queues.

# Architectural choices

The architecture employs microservices for loose coupling and scalability, containerized with Docker [9]. Kubernetes [10] automates scaling and management. Data management utilizes a hybrid Ceph storage system [11][12] for redundancy and fault tolerance, combining replication and object sharding to ensure data accessibility and protection, the inspiration to have a system like S3 object storage [13] [14].

# Privacy & Security

* For secure connection with database the system is designed by keeping encryption at rest and in transit in mind by using secure sockets layer and transport layer security (SSL/TLS) [15] meeting encryption requirements under GDPR and HIPAA. In database salted secure hashing algorithm is used wherever necessary to store sensitive data like passwords, health information etc.
* Access control and authentication using cephx [16], to authenticate user services accessing the cluster integrated with external authentication systems like LDAP(Lightweight Directory Access Protocol) which ensures data meeting access control under GDPR and HIPAA.
* Using Ceph’s data placement policies to ensure that healthcare data remains within appropriate geographic regions or data residency according to GDPR. Auditing and Logging using Ceph logging [17] to meet compliance with GDPR and HIPPA’s requirement for audit trails and accountability.
* Employee Training on how to protect their access credentials, safeguard their devices and be mindful of cyber threats.

# System Management

The System will be managed by a dedicated team comprising system administrators, UI/UX developers, DevOps engineers, security specialist, and database administrators. Skills include proficiency in containerization, full-stack development, networking, security protocols, and compliance regulations. Resources include servers, networking equipment, security tools and training materials. The proposed microservice architecture facilitates easier management, scalability, and maintenance through automation and scaling of components.

# Green Computing

* Using containerization reduces the physical hardware footprint, leading to lower energy consumption and reduced cooling requirements [18].
* Power management policies at the system level to control power usage during periods of inactivity or low demand [19]. Implementing energy-aware routing algorithm to optimize network traffic [20].
* As Fig 1 clearly states the system is deployed on dual data center deployment which was implemented to make system always available which can be costly in terms of energy consumption like infrastructure costs, maintenance etc.. Replication Strategies can lead to increased storage costs and computational costs.

# References

[1] <https://www.citizensinformation.ie/en/social-welfare/irish-social-welfare-system/personal-public-service-number/#:~:text=Your%20Personal%20Public%20Service%20(PPS,is%20sometimes%20called%20a%20PPSN>.

[2]<https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge>

[3] <https://gdpr-info.eu/>

[4] <https://www.w3.org/WAI/people-use-web/>

[5] <https://bytebytego.com/courses/system-design-interview/scale-from-zero-to-millions-of-users>

[6] <https://nickcraver.com/blog/2013/11/22/what-it-takes-to-run-stack-overflow/>

[7] <https://netflixtechblog.com/active-active-for-multi-regional-resiliency-c47719f6685b>

[8] <https://en.wikipedia.org/wiki/Single_point_of_failure>

[9] <https://en.wikipedia.org/wiki/Docker_(software)>

[10] <https://en.wikipedia.org/wiki/Kubernetes>

[11] <https://en.wikipedia.org/wiki/Replication_(computing)>

[12] <https://www.usenix.org/legacy/event/osdi06/tech/full_papers/weil/weil.pdf>

[13] <https://www.ibm.com/blog/object-vs-file-vs-block-storage/>

[14] <https://www.dataversity.net/nine-key-benefits-of-metadata-management/>

[15] <https://aws.amazon.com/what-is/ssl-certificate/#:~:text=SSL%2FTLS%20stands%20for%20secure,using%20the%20SSL%2FTLS%20protocol>.

[16] <https://docs.ceph.com/en/quincy/dev/cephx/>

[17] <https://docs.ceph.com/en/latest/rados/troubleshooting/log-and-debug/>

[18] <https://increment.com/containers/containers-for-sustainable-software-engineering/>

[19] <https://www.linuxfoundation.org/wp-content/uploads/2019/10/Power-Management-Guide_Linux-Foundation.pdf>

[20] Bianzino, A. P., Chaudet, C., Larroca, F., Rossi, D., & Rougier, J.-L. (2010). Energy-aware routing: A reality check. 2010 IEEE Globecom Workshops, 1422–1427. <https://doi.org/10.1109/GLOCOMW.2010.5700172>