Service Mesh

Call to Action

After learning about service mesh, let's put it to action using this Call to Action document.

In this document you can find actionable tasks that will help you use service mesh securely in your system.

1. Decide whether to use service mesh in your system

   Service mesh is recommended in a rich communication system. If your system has a lot of services talking to each other, you should definitely consider service mesh. If not, for example – if most calls to the services originate from the front end – then it might not be a good idea to use service mesh.

   Are you going to use service mesh in the system (Y/N)? ____

2. Decide on the specific service mesh to use

If you decided to use service mesh, the next step is to decide on the specific service mesh to use. There are a lot of factors to consider here, mainly the platform used for the services and the type of service mesh required (sidecar vs in-process). Services deployed in Kubernetes will usually go for Istio. Other platforms – will use other service mesh.

Conduct a thorough research and decide on the service mesh to use.

The service mesh in the system will be _____

3. Map the security capabilities of the service mesh

Service mesh engines were not born equal, and each one has its own capabilities. That holds true also for security capabilities.

For the selected service mesh implementation, write down the security capabilities offered out-of-the-box, which will free the services the handle themselves.

Capability	**Supported?**
Secure communication	
Authentication	
Logging and monitoring	

Print this document and use it for running the security tasks.

Good luck!

Memi