SECRET STORAGE MANAGEMENT VIA TTL VIRTUAL MASKS

ADITYA CHAYAPATHY

EJAZ SAIFUDEEN

BALACHANDAR SAMPATH

ARCHANA RAMANATHAN SESHAKRISHNAN

CURRENT SCENARIO

What are secrets? SSN info, credit card info, etc

Sensitive customer information is provided to 3rd party service providers in its original form with the belief that the 3rd party service providers are secure.

What happens in the background? No one knows! Is my data encrypted? Is my data shared? What if the service provider is breached? What actions to take when data is compromised?

PROPOSAL

- What if I, as a customer, had the opportunity to provide my secret to 3rd party service providers in a secure manner?
- What is secure? A system that lets you mask your secrets which can be used by 3rd party vendors. A system that maintains these virtual masks for a limited time.
- Easier said than done? Or, is it? ;)

USERS INVOLVED

01

Central Authority – Manages all the secrets and the virtual masks

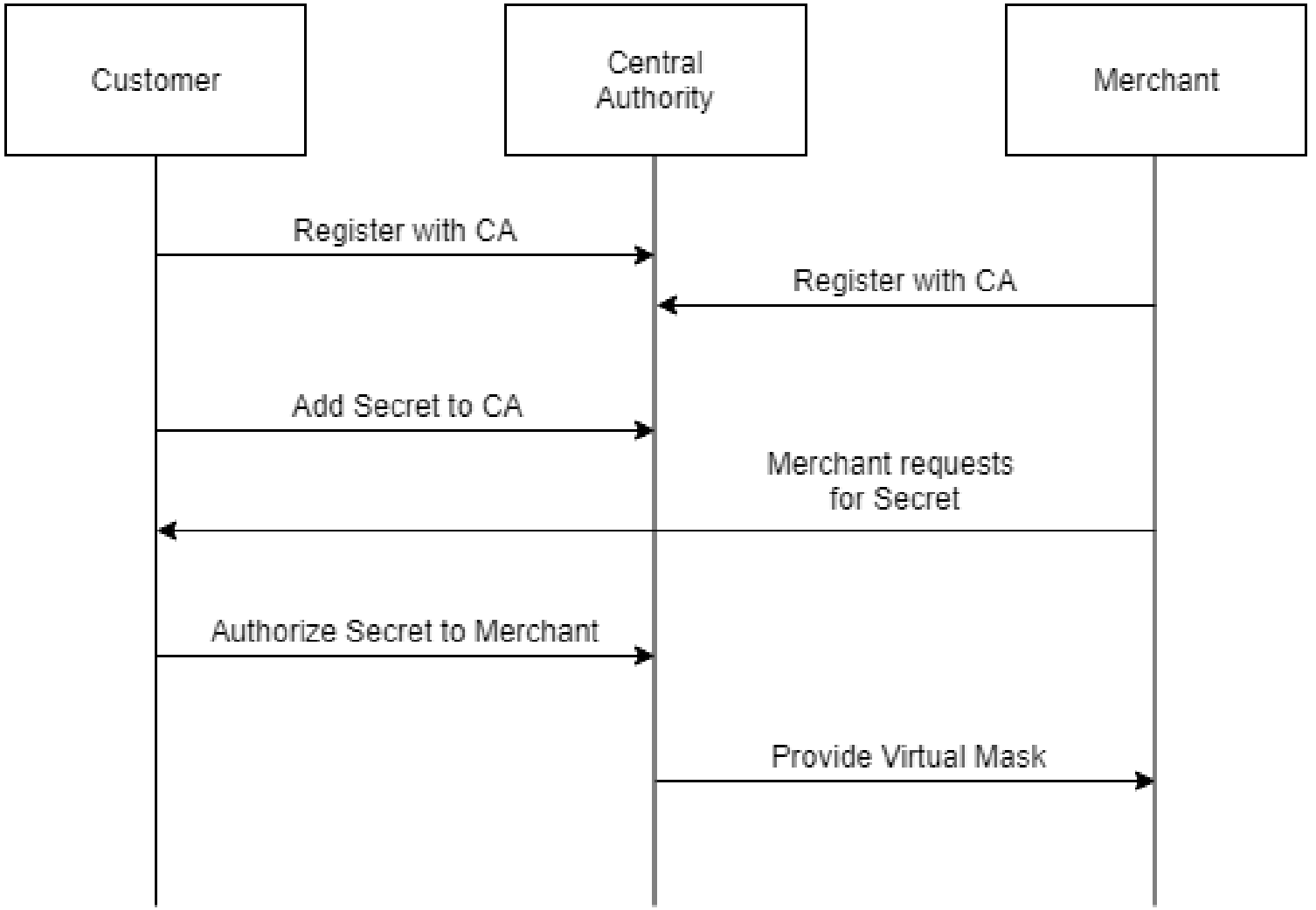
02

Merchants – Use virtual masks for their business logic

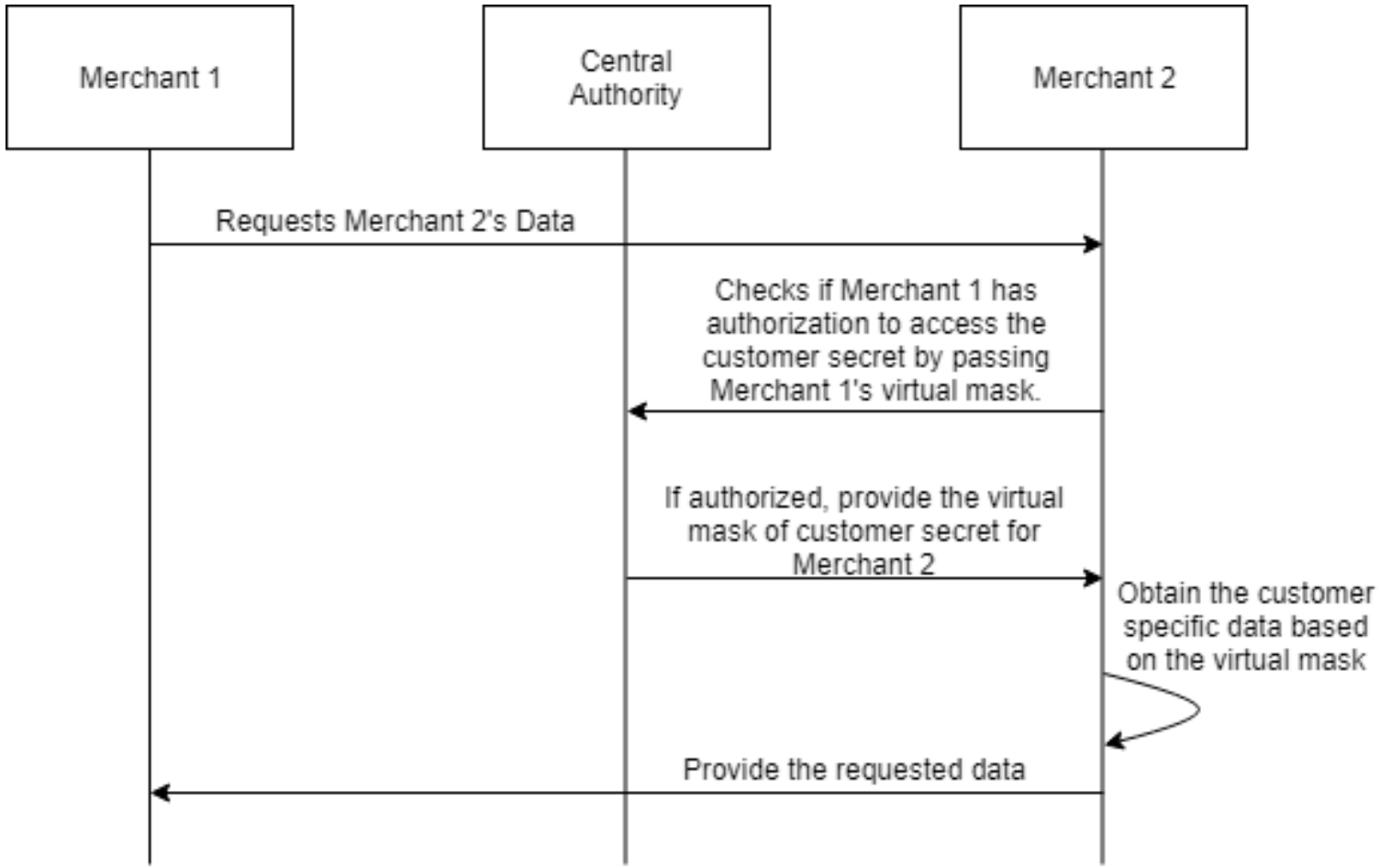
03

Customers – End users who authorize TTL virtual masks to merchants

ARCHITECTURE



INTERACTION AMONG MERCHANTS



SOCIAL IMPACTS

1

Fine grain control of secrets. Virtual masks are short lived. Once they expire, they are no longer valid.

2

Easy to revoke access.

3

3rd party is no longer accountable.

4

Easy to identify suspicious merchants as they will be registering with the central authority.

5

Original secrets are irreproducible using virtual masks.

DEMO

Context: We are attempting to mimic the behavior of central authority by masking SSN information of the customer. Here, we have 2 merchants who interact with each other to exchange data.

How is it achieved?

- Spring boot application which provides CA functionality as a service via REST APIs.
- Mongo is used as the datastore for storing CA data.
- AngularJS is used to create the UI interface.

NOTE: THIS IMPLEMENTATION IS FOR THE PURPOSE OF "PROOF OF CONCEPT" ONLY.

FUTURE IMPROVEMENTS

1

Use a secure secret storage system such as Hashicorp Vault to store Central Authority data.

2

Use SSL certificates to identify merchants.

3

Use RSA public keys to identify customers.

4

Provide token based API access to CA service.

THANK YOU