Addressing Synchronization Problem in Next Generation Certificate Transparency (CTng) Local Testing Environment.

CTng is a re-design of traditional certificate transparency proposed by Professor Amir Herzberg and the goal is to achieve transparency of certificate and revocation status, with no trusted third-party principle, while allowing offline validation and protecting against Denial-of-Service attacks.

The interations between different entites can be represented as the graph below

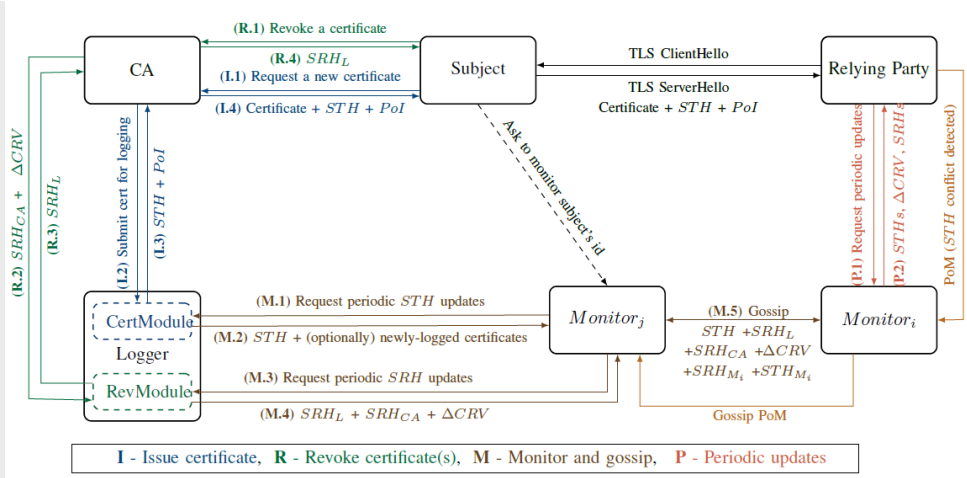
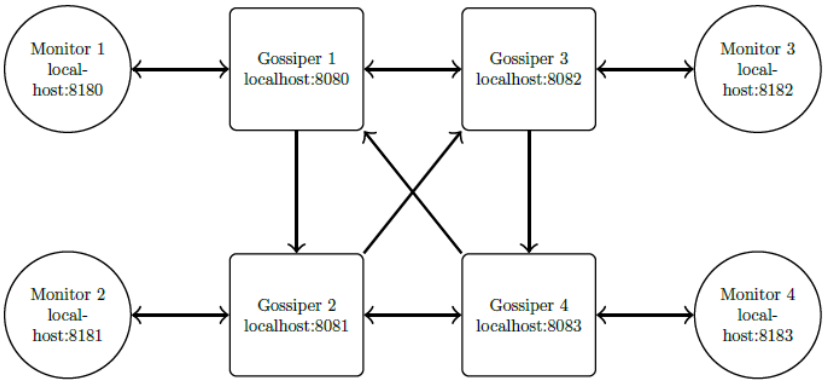


Fig. 1: CTng: entities and interactions. See §IV-A for an overview and Table II for notation.

In this project, we are looking into a simplified model, with the primary focus on the gossipers and the monitors. The testing will be done locally utilizing different port numbers to simulate different machines in a real world scenario and the loggers/CAs will be “fake loggers/CAs” that do not have an API core to realistically issue/revoke certificates. The topolgy looks like the graph we have below:



Our goal is to ensure monitor synchronization in terms of both operation and storage such that correct information can be served to the relying party (client for the system). We will also discuss some potential problems caused by monitor desycronization and what the client can do under those circumstances.