1. Task: Fix the PKI architecture we will model in OPNET:
   • Candidates are: SPKI, PKIX (X.509), PGP, etc.
   • We finally agree to model PKIX. But we are not pursuing a complete model in OPNET. Instead, we will find basic components in PKIX and implement them step by step.

2. Task: Fix the application that we will model in OPNET at the first stage:
   • Candidates are: E-mail, database transactions, HTTP, etc.
   • We finally agree to model e-mail applications first. The main reason is that it is the simplest application to model and it might be easy to add PKI onto it.

3. Decide the basic building blocks that we need to implement in OPNET for e-mail applications using PKI.
   • Certificate Authority (CA): 1 at first, maybe multiple (CA trees) later.
   • Email clients and servers: We figure out that extra work need to be done on the client side because it has to handle key management, encryption, decryption, etc. However, the server side can be dumb – it is very likely that we will be able to use the existing model in OPNET for email servers.
   • Certificate Revocation List (CRL): This is inevitable.
   • Directories: store and provide certificates to clients.

4. How do we model the interactions among these building blocks?
   • We come up with the following diagram to describe the interactions we want to model soon. In this diagram, we assume the email client A wants to send an email to email client B.
5. Tasks for next week:

- Get more knowledge about the basic components that we want to model for PKIX.
- Get data for metrics, such as:
  - request size
  - response size
  - processing times for: checking a certificate against a CRL, lookup in PKC, encryption and decryption delays, etc.
- Get a more precise model for email systems that use PKI.—Jun
- OPNET modeling issues: how to model a new application (for example, how to model the email system that uses PKI)? – Suvda
- Email Kelley R. Klepzig, ask him for his OPNET models for PKI applications. (What is his email address? We need to find it out. – Jun)
- Webpage: Jun has already finished the webpage. He will ask around and find a way to post it somewhere at NCSA.
- Progress report – Jun will try his best to write a progress report.
- What is Zahid’s task? Sorry, I forgot.