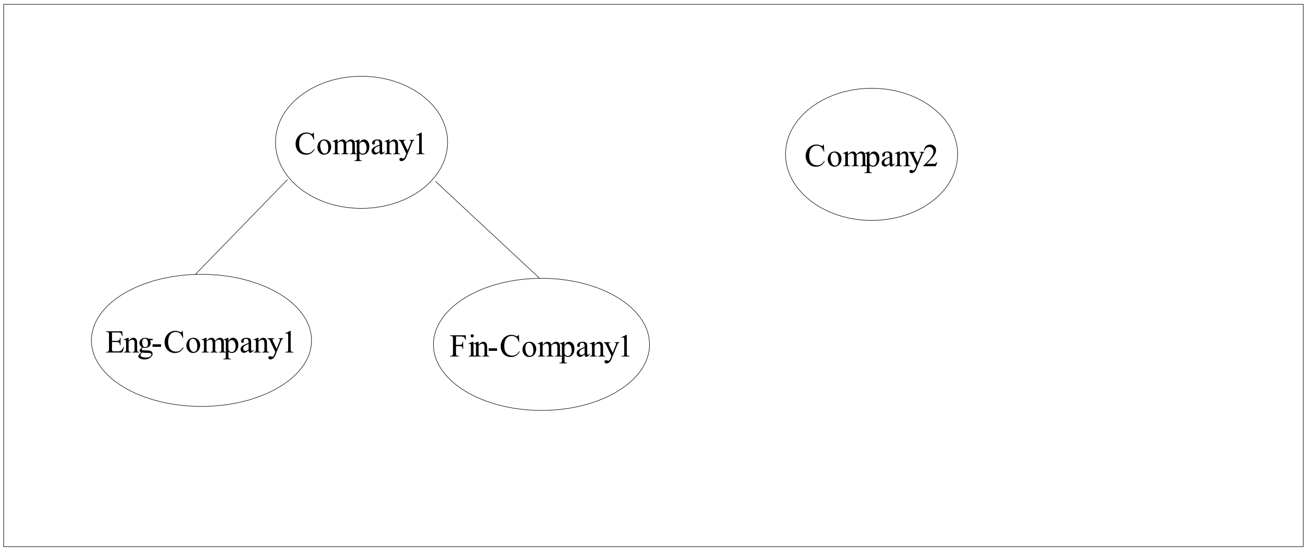
# PKI Class Exercise

*CS461 September 27, 2010*

Today you will role play through a public key infrastructure (PKI) scenario. The Certificate authorities (CAs) are shown below. In addition, there are 5 hosts signed by these CAs.



You will divide into groups. Assign people to act as each of the CA's. Each CA will hold a copy of the certificates it has signed.

The RSA algorithm is used for signing operations. The actual hash algorithm is unimportant. Somehow the hash value was computed and is noted on each certificate. The signature in the certificate is the hash value encrypted by the signer's private key.

Run through scenarios with the certificates for Hosts 1 through 5. An individual receives a certificate (from a web browser or some other initial secure communication authentication). The individual needs to validate the certificate. What root certificate is needed? Can any of the CA certificates act as the root certificate the individual uses to validate the certificate he received? Why is a root certificate needed to validate other certificates?

Hopefully, we have enough computers available so you can actually validate the signatures. The builtin calculator functions on Windows or Linux have sufficient precision. One or two of the host certificates are faulty. How could this happen?