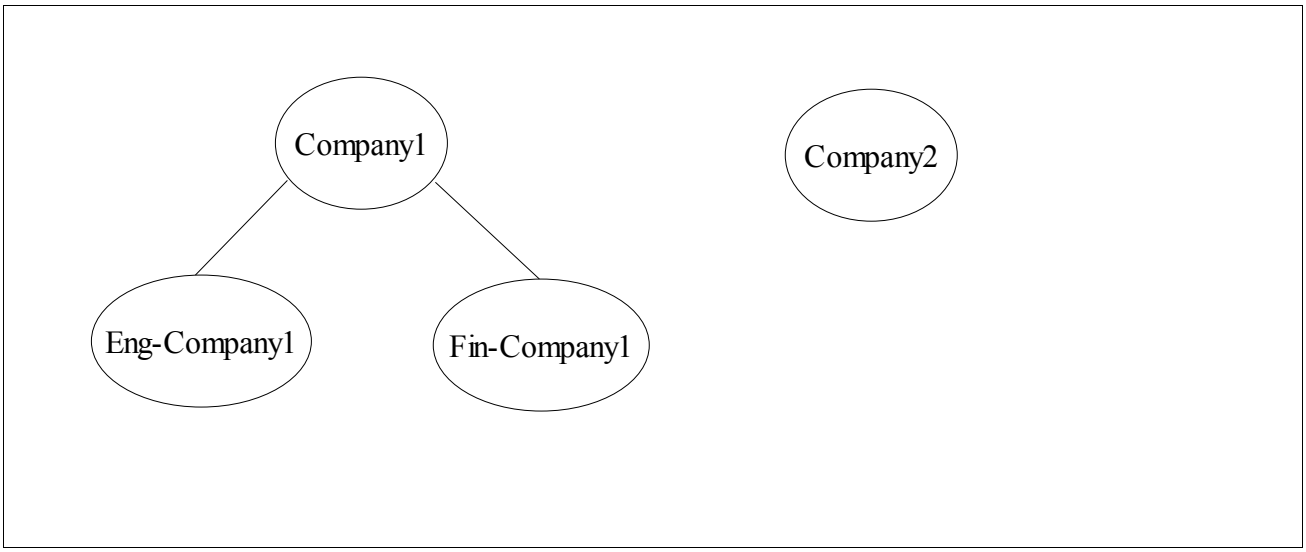
PKI Class Exercise

CS461 September 25, 2009

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 certificate it has signed. In addition, each CA will hold a copy of the certificate of the CA that signed it's certificate.

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 of the host certificates is faulty. How could this happen?