

COMP3441/9441 Tutorial Week 6

Public Key Infrastructure (PKI)

1. What is the basic purpose of PKI?
2. What are the components of PKI?
3. What name constraints would you put into PKIX certificates to build the anarchy (P2P) model? *[KPS 3]*
4. If there is a revocation mechanism, why do certificates need an expiry date? *[KPS 6]*
5. Why must a CRL be reissued periodically, even when no new certificates have been revoked? *[KPS 5]*
6. Why is it important in a good-list revocation scheme to keep hashes of the valid certificates, rather than just their serial numbers? *[KPS 8]*
7. Compare revocation schemes of verifiers downloading complete CRLs, clients obtaining non-revocation certificates, and verifiers checking individual validity status. Consider in overhead (on bandwidth, verifiers, clients, the OLRs) and revocation timeliness. Consider factors such as how many clients a verifier serves and how many services a client visits. *[KPS 7]*

Questions marked *[KPS n]* are taken from *Kaufman et al., Network Security*, Chapter 15, Section 9.