

IY5601 Coursework D (2005–2006)

Identity management

1. Define and distinguish between the terms anonymity, pseudonymity and unlinkability.
2. List two advantages of the use of a single sign-on (SSO) system. What disadvantages might arise from the use of an SSO system?
3. Distinguish between local and proxy-based SSO, and also between pseudo and true SSO. Where does InfoCard fit into this taxonomy?
4. Give an estimate of how long it would take to discover a poorly chosen password if an attacker intercepts the initial Kerberos message exchanges. Use your own estimates for the number of possible passwords, and how long it takes to perform any necessary cryptographic operations.
5. Sketch the message flows for a Liberty SSO procedure, assuming that the user has not previously logged on with the Identity Provider (IP).
6. Discuss a possible attack on Liberty via the web redirection procedure.
7. Sketch the message flows for InfoCard.
8. How does InfoCard differ from Liberty?