**T-110.4206 Information security technology**
**Examination 2014-05-15**
Lecturer: Tuomas Aura
No electronic equipment or reference material allowed in the examination.

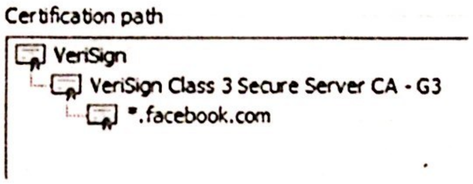
*Answer only 5 of the 6 problems. If you answer them all, only problems 1–5 will be marked.*

1. **Security terminology**

   Analyze the relationship between the following security goals: confidentiality, authentication, and access control.

2. **PKI**

   Explain in detail how the user and web browser verify the authenticity of the web page https://www.facebook.com/, which has the following certificate chain:



Certification path

- VeriSign
  - VeriSign Class 3 Secure Server CA - G3
    - *.facebook.com

   Note: It is not necessary to list or explain the SSL protocol messages. Explain only the certificate chain verification and user actions.

3. **Passwords**

   An online service authenticates its one thousand users with 6-digit PIN codes (e.g. "402730"), which are selected randomly by the service. The service stores the PIN codes in a database as hash values. The hash function is SHA-256, which is computed on the server name, username and password:

   *hash = SHA-256 (service domain name | username | password)*

   (a) How many bit of entropy does one PIN code have?

   (b) The attacker has fancy graphics card that can compute 500 million SHA-256 hashes in a second. If the attacker manages to read the hash values from the database, e.g. with SQL injection, how long does it take to crack at least one password?

   Note: Since you have no electronic calculator, it is ok to make approximations in the calculations, but please show clearly what approximations are made.

   (c) Would you recommend adding a salt field to the password database? Why?

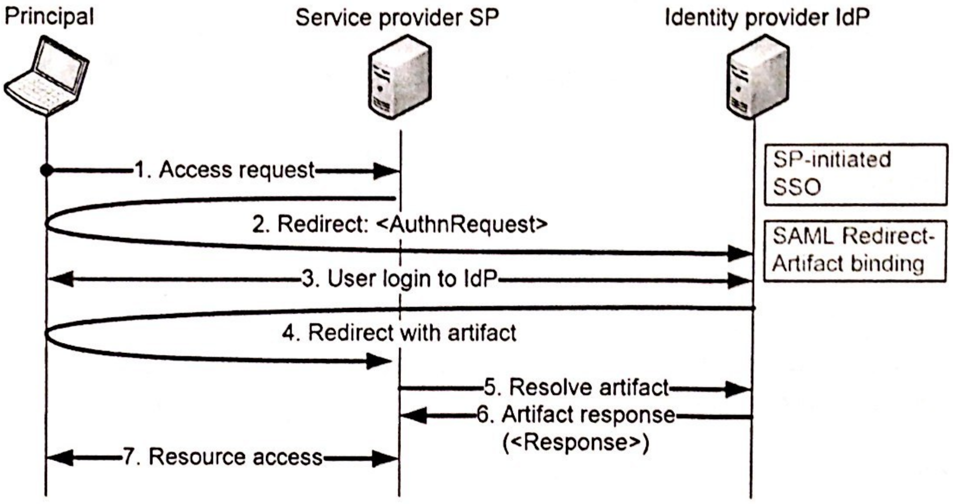
Please turn the paper over for problems 4-6.

**2. PKI**

Aalto University uses Sonera, a commercial CA, for certifying university servers. Thus, the university has to pay for server certificates. If the university decided to set up its own CA instead, it would not need to pay for the certificates and, thus, it could flexibly certify any number of servers. What costs and other disadvantages could that decision have?

**4. Identity management**

The picture below illustrates SAML authentication for web-browser-based SSO (for example, Shibboleth). The Response in message 6 is signed by the IdP. Moreover, SSL is typically used to protect all the connections.



How and why is the security of the protocol affected if SSL is not used between

a. the client and the SP
b. the client and the IdP
c. the SP and the IdP

**5. Threat analysis**

An amusement park uses wrist band tickets. They can be bought at the park gate or ordered online. The ticket is valid for unlimited rides during one day within a year from the purchase. Tickets are read with a bar code scanner before each ride. What security threats and potential vulnerabilities are there in this system? Which are the top-priority threats from the point of view of the amusement park business?