T-110.4206 Information security technology
Examination 2011-10-27
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 concepts**

   Analyze the relationship between the following security goals: confidentiality, integrity, authentication, availability, authorization, non-repudiation, access control, and privacy. For example, consider which goals may be overlapping, conflicting or supporting one another. Explain why and how. (Hint: Drawing a diagram may help you to get started.)

2. **Cryptography and user authentication**

   What properties and features are needed in a function that is used for computing hash values of user passwords for password storage? Explain why.

3. **PKI**

   Aalto University uses Sonera, a commercial CA, for certifying university servers. Thus, the university has to pay for server certificates. If the university instead decided to set up its own PKI, 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. **Payment systems**

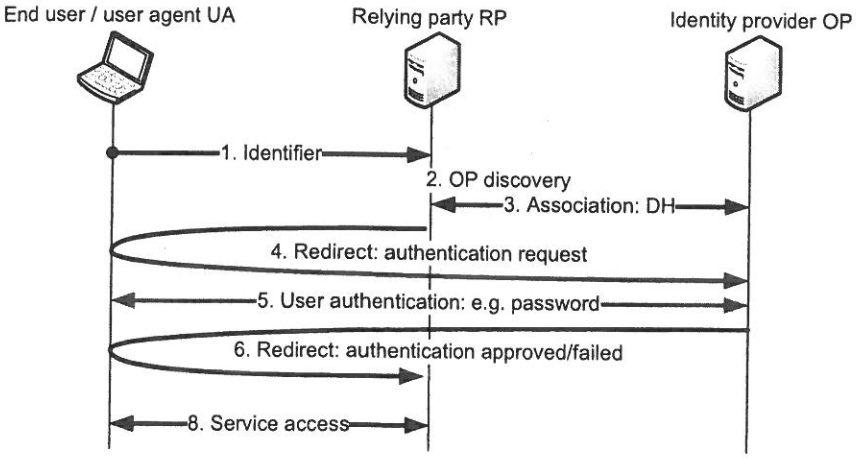
   EMV payments have three different levels of security: static data authentication (SDA), dynamic data authentication (DDA), and combined DDA and application cryptogram (CDA).

   a) What are the differences between these, and when and why would each one be used?
   b) How does the security of these methods compare with the old magnetic stripe cards?

Please turn the paper for problems 5–6.

5. Identity management

The picture below illustrates OpenId authentication. Message 6 is protected with the key created in the key exchange in step 3. SSL may be used for protecting the connections but, originally, the user agent was not required to support SSL.



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

a) UA and RP
b) UA and OP
c) RP and OP

6. Threat analysis

An amusement park uses wrist band tickets. The tickets are priced differently for under and over 15 year olds. 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 there are in this system? Prioritize the threats (approximately) from the point of view of the amusement park business.