**Answers and grading comments for Assignment 7 – Week 9**

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**

**(1) The Internet requires that every host has a domain name.**

a) true  
b) false

**ANS: b**  
Each machine on the Internet is required to have an IP address. If it doesn't have a domain name it can still be accessed by typing the IP address into the browser.

**(2) What is the difference between a CA authentication policy and a CA issuance policy?**

**ANS:** The difference between these two policies is that the first simply establishes the level of proof of identity needed for the CA to accept the principal's claim of identity whereas the second answers the question, "Given the identity of the principal, will the CA issue a certificate?"

**(3) What do you mean by a distinguished name?  Explain with an example.**

**ANS:**A distinguished name identifies a principal.  It consists of a series of fields, each with a key and a value.  
/O=IBM/OU=Quality Assurance/CN=Jack Davis/

**(4) Which of the following are true about cookies?**

a) permanent cookies are stored on the server  
b) temporary cookies are stored on the client machine which is running the browser.  
c) a cookie is encrypted if SSL is used.  
d) the value of a cookie can be the serialization of a C# object (i.e., binary data)  
e) a temporary cookie is deleted after the browser sends it to the server.

**ANS: b,c**  
Most students were unaware that SSL encrypts cookies. This is because the entire HTTP request is encrypted and cookies are defined in the HTTP request. Also the value of a cookie cannot be binary; HTTP is a ASCII-based protocol.

**(5) A principal is represented in computer memory by an identity.**

a) true  
b) false

**ANS: a**

**(6) The same principal may have many different identities.**

a) true  
b) false

**ANS: a**

**(7) What are the different types of certificates?**

**ANS:**

1. Site certificates (e.g, www.cs.mum.edu)  
2. Personal certificates (e.g. used if the server wants to authenticate the client. You can install a personal certificate in your browser.)  
3. Software vendor certificates (e.g. used when software is installed. Often when you run a program, a dialog box appears warning that "The publisher could not be verified. Are you sure you want to run this software?". This is caused either because the software does not have a software vendor certificate or because you do not trust the CA who signed the software vendor certificate).  
4. Anonymous certificates, e.g., used by a whistle blower to indicate that the same person sent a sequence of messages. But don't know who that person is.

**(8) List two things that an identity is used for.**

**ANS: access control and accountability**

Identity is not used for authentication, it is created after the principal is authenticated. I also accepted the answer that an identity is used to represent a principal.  
 **(9) What is a principal and what is an identity?**

**ANS:** A principal is a unique entity.  An identity specifies a principal. Identity is simply a computer’s representation of an entity.

**(10) What’s the goal of a certificate in regards to identity?**

**ANS:** Bind correct identity to DN

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**