

# IY5601 coursework

27th March 2006

1. The OASIS SAML standard defines several types of assertions.

(a) Explain what a SAML assertion is, and describe three types of statements that such an assertion may contain. For each type of assertion, give a short sentence describing an example.

*An assertion is simply a statement, in XML, issued by a SAML authority. The three types of statement that may be carried in a SAML assertion are:*

- *an authentication statement, in which case the assertion is that the issuer has authenticated the subject.*
  - *for example: “The subject has been authenticated by kerberos”*
- *an authorisation statement, where the assertion is that the issuer has granted particular rights to the subject.*
  - *for example: “The subject is authorised to make a purchase”*
- *an attribute statement, where the issuer provides qualifying information about the subject.*
  - *for example: “The subject has a credit limit of £1000.”*

(b) In addition to these statements what other information must a SAML assertion contain.

*All SAML assertions must contain:*

- *a timestamp stating when the assertion was issued*
- *the identity of the issuer*
- *an ID for the assertion, and the version of the SAML standard being used.*

(c) What optional element may a SAML assertion contain to control the use of the assertion. Give a short sentence to describe how this element may be used.

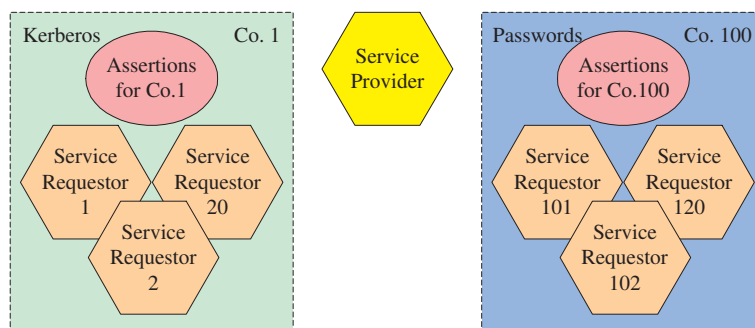
*The optional <Conditions> element may be used to control the use of the assertion. For example, by specifying a validity period for the assertion.*

2. A manufacturer supplies parts to many different companies. The purchasing officer’s job in these companies is a dynamic post, and the identity of this individual changes frequently as employees move around within each company.

- (a) What security problems does this pose to the supplier who wishes to automate his sales procedures using the Internet.

*The identity of each purchasing officer is not stable, therefore managing authentication of this individual from outside the company is difficult. New identities and authentication credentials will need to be created as new purchasing officers enrol with the system, and the credentials of individuals no longer authorised to make purchases need to be removed. The authentication mechanisms supported by each company may differ and the supplier will either have to support all of these, or insist that each company uses a particular mechanism.*

- (b) Assuming that the supplier trusts one entity in each company explain, with the aid of a diagram, how SAML can be used to simplify the problem of authentication and authorisation for this supplier.



*A single trusted entity within each security domain may issue a SAML assertion describing authorisation, authentication, and attribute statements on behalf of an organisation or company. All credential management for purchasing officers is dealt with within the particular company or security domain. The service provider does not have to get involved with local credential management. The service provider now only has to trust a single SAML authority within each company who issues the assertions. If the service provider shares a key with each SAML authority (or holds a certificate containing a public key for each SAML authority) then the assertions can be signed by the issuing authority and validated by the service provider. Since the SAML authorities are stable (as opposed to the dynamic behaviour of individuals) this may make it feasible to use a TTP to authenticate previously unknown SAML authorities.*

3. The OASIS WS-Security standard provides support for security tokens in SOAP messages.

- (a) Where would a security token be found in a SOAP message, and what would the information contained in this token be used for.

*A security token would be found within the <wsse:security> element of the SOAP header block. It contains information used for authentication, authorisation, or both.*

- (b) List three types of security tokens supported by WS-Security.

*Username tokens, binary tokens, and XML tokens*

- (c) How could an X.509 BinarySecurityToken be used for authentication in a WS-Security message?

*The sender must sign something in the message using the private key corresponding to the public key carried in the security token. This signature binds the data to the key carried in the token and may be verified by the receiver. The X.509 certificate must be signed by a CA that is trusted by the receiver. The signature of the CA binds the asymmetric key pair to a user ID, and may be verified by the receiver. Thus the receiver can verify that the data in the message was signed by the entity with the ID contained in the X.509 certificate, providing authentication of the data origin. If this signed data is a nonce that the receiver had recently generated and sent as a challenge, then the signature on this nonce can be used to authenticate the entity involved in this run of the challenge-response protocol.*

- (d) How could an SAML BinarySecurityToken be used in a WS-Security message?

*As with the X.509 example, the token must be used to sign something in the message. This signature binds the data to a particular key. In the case of a SAML token, the subject of a SAML assertion identifies the signing party. If the <SubjectConfirmation> element has the “holder-of-key” attribute, with a key contained (or referenced) in a <KeyInfo> sub element, then this key is associated with the subject of the assertion. This key may then be used to create the signature on the message data, thus binding the key contained (or referenced) in the SAML token to the data. If the SAML authority issuing the assertion also signs the assertion, then this signature binds the key to the subject of the assertion. The receiver can then use the key carried in the <SubjectConfirmation> element to verify the signature on the data in the message. The receiver can then verify the SAML authority’s signature on the assertion. Hence the receiver can be sure that the data in the message was signed by the subject of the assertion, providing authentication of the data origin. If this signed data is a nonce that the receiver had recently generated and sent as a challenge, then the signature on this nonce can be used to authenticate the entity involved in this run of the challenge-response protocol.*