A-4 How is perfect forward secrecy solved in OTR?

By using Diffie-Hellman as the key exchange protocol for each session. This means that if a session key is compromised this will only compromise the session that that key belongs to and not any other. I believe that this answer is sufficient for the question asked but there is some more detail on how the two parties can verify each others public key fingerprint to ensure that they are not the victims of a man-in-the-middle attack.

A-8 What is an artifact binding?

A SAML message is transmitted from one entity to another either by value or by reference. A artifact in SAML is a reference. The receiver of an artifact resolves the reference by sending a request directly to the issuer of the artifact, who then responds with the actual message referenced by the artifact.

This solution is done to increase security as intermediaries as a HTTP user agent can not sniff on the actual value as well as this lets the communication bypass limitations of intermediaries in the connection path. More detailed information can be found in section 3.6.2 oc the SAML 2.0 bindings specs.

A-9 Name and describe four profiles in SAML. You should be able to provide a more detailed description for one of them

Web browser SSO Profile which defines how the assertions, protocols and bindings are to be used for web based SSO. It uses the SAML Authentication Request protocol together with the HTTP Redirect, HTTP POST and HTTP Artifact bindings. There is no extra requirements on the users web browser other than it being a standard web browser. These are the steps for achieving SSO:

1. The subject tries to access a resource at the SP.
2. The SP determines the correct IdP to use for authentication.
3. The SP sends an authentication request ¡AuthnRequest¿ to the IdP via the subject. This message may be digitally signed.
4. The IdP authenticates the subject in some way. It could be the case that the subject already has an authenticated session with the IdP. Then, no new authentication is needed.
5. The IdP sends a ¡Response¿ message back to the SP with some proof that authentication was successful.
6. The SP verifies that the IdP authenticated the subject and the subject is allowed access to the requested resource.
7.

Enhanced Client and Proxy (ECP) Profile which supports SSO with clients that have more capabilities than plain web browsers.
The Single Logout Profile is used to simultaneously logout from all services that a user has been logged into using SSO.
Identity Provider Discovery Profile is used to discover which IdP to contact in the discovery phase.

A-10 Describe the purpose of RelayState and show how it is used.

If a SAML request message is accompanied by RelayState data, then the SAML responder MUST return its SAML protocol response using a binding that also supports a RelayState mechanism, and it MUST place the exact RelayState data it received with the request into the corresponding RelayState parameter in the response.

RelayState can also be used to coordinate messages and actions of IdPs and SPs, for example, to allow an IdP (with which SSO was initiated) to indicate the URL of a desired resource when communicating with an SP.

A-11 Describe and compare "discovery" in SAML and OpenID.

SAML does not explicitly specify how the SP determines which IdP to contact. SAML has another profile called the SAML identity provider discovery profile that can be used for this, but it can also be achieved in other ways.

OpenID on the other hand uses XRDS or HTML based discovery. This is done by the user actually specifying a User-Supplied Identifier in the form of an XRI or a URL. Depending on the format it then decides whether to use XRDS or HTML based discovery. These two methods are described below in question A-16.

A-15 Briefly explain what an XRI is, and why it is a good idea to use it in the context of OpenID.

An XRI is an E**X**stensible **R**esource **I**dentifier which itself is a generalized version of URI. As the name suggests it is used to identify a resource and these identifiers are domain, location0, application, and transport independent. This means that they can be shared across any number of domains, directories, and interaction protocols.
The XRI resolves to a XRDS document which is a XML document containing the information gathered from the specified XRI.

This is useful in OpenID because the end user(the person who wants to log in) can change between OpenID providers(OPs) while still keeping the same XRI, the actual OP will be resolved in the XRDS document. Therefor the user does not have to create a new identifier at another OpenID provider if he/she

wants to change provider, instead he just specifies his/her XRI and let it resolve to actual OpenID provider.

A-16 Describe how XRDS-based discovery and HTML-based discovery differ. In which context are they used?

The discovery methods are used when the service provider needs to find out what IdP/OP a end user is using. The discovery is based on either finding a XRDS-document containing the necessary information or by finding a HTML page which holds the information.

It starts of by the user supplying a user supplied identifier to the service provider. If this identifier is an XRI or a URL, XRDS based discovery can be used. However if the Yadis protocol fails to resolve the URL to an XRDS document then HTML based discovery has to be used. These two differ in the way that the HTML version the actual OP endpoint URL and OP local identifier is found in the `<HEAD>` section of the page. In the XRDS version there is an actual XRDS document containing the same information.

A-18 In OAuth, explain why the access token must not be cached, and how this is achieved.

The access token is used as a replacement for username and password to authenticate to services. If this is cached, malicious users could get their hands on a token and use it to log in to a service. Since the tokens normally have a long expiry time they must not be cached for the above mentioned reasons. This is achieved by the authorization server specifying the fields `Cache-Control: no-store` and `Pragma: no-cache` in the HTTP response of a authorization request.