PUBLIC KEY CERTIFICATES Module 3

PUBLIC KEY CERTIFICATES

SUMMERY

Matched Branch:	0
Partially Matched Branch:	0
Mismatched Branch:	7
Extra Branch:	4
Total Match:	20.0 %
Concept Match:	22.22 %
Link. Phr. Match:	0.0 %
Misconception:	100.0 %
Hierarchy Match:	0.0 %

Grade: 6.6%

key steps summarized as

- Client may provide the signed certificate to any other user
- User software (client) creates a pair of keys: one public and one private
- Client prepares an unsigned certificate that includes the user ID and code of public key
- User provides the unsigned certificate to a Certificate Authority in some secure manner
- Any user may verify for certificate validity by calculating the hash code of certificate without the signature, decrypting the signature using the Certificate Authority ’s known public key, comparing the result for a match
- Certificate Authority creates a signature using a hash function to calculate the hash code of the unsigned certificate, and encrypts the hash code with the Certifictae Authority’s private key
- Certificate Authority attaches the signature to the unsigned certificate to create a signed certificate and Certificate Authority returns the signed certificate to client