Certificates

Step 2 Questions and answers

1. Would a certificate validity for another 5 years be a good idea? It would significantly simplify key handling on servers.
    - Signature algorithm: SHA256 with rsa encription
    - Public key encryption: RSA 4096 bit
    - Validity Dec. 2022 - Marc. 2023 (only a few months)
    - i believe as of know the algorithms and key sizes would be considered to be safe for the next 5 years. However, the possibility cannot be excluded that there are break throughs in science that might render certain algorithms unsafe so the the validity should be not too far in the future.
2. Are the algorithms strong enough for the lifetime of the certificate? If yes, what would you consider an weak algorithm?
    - yes the algorithms are strong enough (keys should also be ok, see https://www.keylength.com but is more about the next question)
    - I would consider MD5 for the hash function to be insecure.
3. Is the key strong enough? If yes, what would be insufficient?
    - yes 4096 bit is strong enough. According to some sources 2048 would still be acceptable. 1024 would be consicdered to insufficient.
4. Would it be okay if the OCSP and CRL info is missing? What would be the impact?
    - not ideal as OCSP and CRL are means to revoke (invalidate) certificates, for example the private key is leaked. Without OCSP and CRL the browser would not know which revocation list to query.
5. Would it be okay if the CA signed the request for the analysed certificate if key usage would also include "Code Signing" or "Email Protection" or "Time Stamping" or "OCSP Signing"?
    - I believe it would be ok. (From how the questions is phrased, I would have guessed that it woulnd't be allowed.. for example the CA cert would have to have the same extended key usage.. however, didnt find any indicator for that)
6. Is there are reason why the basic constraint states CA:FALSE? What if it would be CA:TRUE?
    - CA:true would be for a CA certificate that is used to sign. CA:false means the certificate cannot be used to valide other certificates.

Step 4 Questions and answers

Some differences between server certificate compass-security.com and client certificate created in previous task "Public key infrastructure"

- Client certificate is valid a lot longer (till 2032).
    - Maybe this is due to the tool but maybe client certificates are usually considered less critical as a user maybe has to authenticate via additional means (password)???
- Client certificate key is only 2048 bit
    - maybe the reduced key lenght is due to the tool, but maybe client certificates are considered less critical? (as there are often other means for authentication?)
- No info about revocation list on client certificate
- Extended Key Usage: doonly lists "TLS Web Client Authentication" for the client certificate. (but it is not marked as critical, so from my understanding, it would not be invalid to use it as a server certificate..)

Notes and varia

Some properties of a X.509 certificate

- Issuer
- Expiration time (Validity)
- Common Name
    - Subject
- Subject Alternative Name
    - browsers will also look at the alternative names to validate the domain of an url
- Public Key Algorithm
- Public Key Size
- Signature Algorithm used for the end-entity (leaf, last)
- Signature Algorithm used for root and intermediate CAs
- OCSP Supported
    - OCSP: Online certificate status protocol
    - created as alternative to CRL
    - https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol
    - apparently: chrome doesnt use OCSP but others browsers do
- CRL Supported
    - CRL: Certificate recovation list
    - FF has deprecated CRL in favor of OCSP
- Purpose of the key (extended key usage)
    - "Certificate key usage" Extension "key usage" defined in RFC: https://datatracker.ietf.org/doc/html/rfc5280#section-4.2.1.3
    - "Extended Key Usage":
        - https://help.hcltechsw.com/domino/11.0.0/conf_keyusageextensionsandextendedkeyusage_r.html
    - if extension is marked as critical, certificate may only be used for that particular purpose. If not critical, it can be used for other purposes. If "Certificate key usage" and "Extended Key Usage" are both critical, the purpose must appear in both fields.
- Basic constraint extensions

https://en.wikipedia.org/wiki/X.509 https://www.techtarget.com/searchsecurity/definition/X509-certificate#:~:text=The%20X.,communications%20with%20a%20second%20party.