A KGYHSZ OCSP válaszadás szolgáltatás elérhetősége és jellemzői

- A szolgáltatás címe: http://ocsp.kgyhsz.gov.hu/ocsp/ vagy https://ocsp.kgyhsz.gov.hu/ocsp/.
- A szolgáltatás igénybevételéhez authentikáció nem szükséges.
- Az OCSP szolgáltatás az RFC 2560 4.2.2.2 pontja szerinti "Authorized Responder" esetnek felel meg.
- Az OCSP választ aláíró tanúsítványt a KGYHSZ bocsátja ki 30 napos gyakorisággal és 60 napos érvényességgel.
- Az OCSP választ aláíró tanúsítvány tartalmazza az *id-kp-OCSPSigning* (1.3.6.1.5.5.7.3.9) jelzést az *extendedKeyUsage* kiterjesztésében.
- Az OCSP választ aláíró tanúsítvány tartalmazza az *id-pkix-ocsp-nocheck* (1.3.6.1.5.5.7.48.1.5) kiterjesztést.
- Az OCSP választ aláíró tanúsítvány aláírási algoritmusa: SHA256withRSA.
- A válaszadó az OCSP kéréseket nonce kiterjesztéssel és anélkül egyaránt elfogadja.
- Az OCSP kérés *CertID* elemében az alábbi lenyomatképző algoritmusok elfogadottak: SHA-1, SHA256, SHA384, SHA512. A válaszban mindig a kérésben levő elemmel azonos algoritmusú elem fog szerepelni.
- A válaszadó aláírt és aláíratlan OCSP kéréseket egyaránt elfogad. Az aláírt OCSP kérés akkor kerül elfogadásra, ha az aláírás érvényes, és az aláírói tanúsítvány tanúsítási útvonala a KGYHSZ-re vezethető vissza.