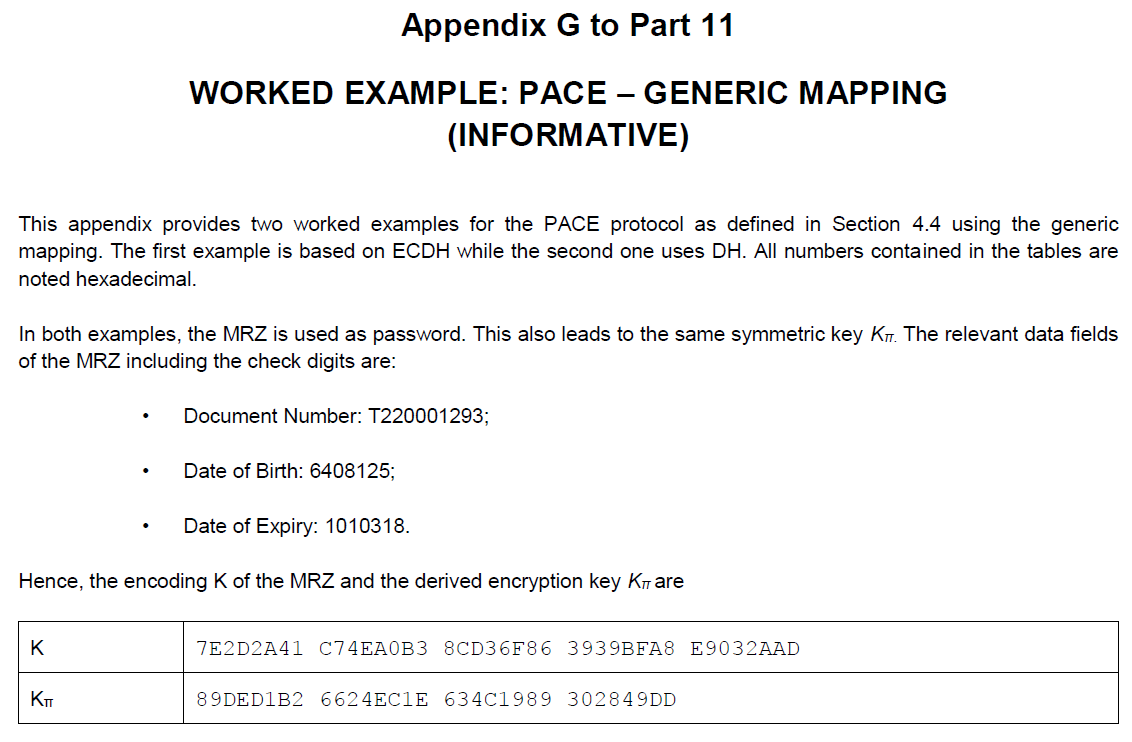


*ECDH (Elliptic curve Diffie-Hellman), which is used for encryption, and ECDSA (Elliptic Curve Digital Signature Algorithm), used for digital signing*.



24bytes: T22000129364081251010318

**1.** K (20 bytes): được tao bởi HASH SHA-1 với đầu vào là 24 bytes (doc number, DOB, DOE).

Generate SHA-1 online: <https://md5decrypt.net/en/Sha1/#answer>

<https://md5hashing.net/hash/sha1>

**2.** Kπ: