How to make use of the X.509 extensions for alternate signature schemes in IKEv2?

Leonie Bruckert (secunet AG)

Heike Hagemeier (BSI)

@IETF 110

ISO/IEC 9594-8 (2020) defines three extensions

`subjectAltPublicKeyInfo`	alternative public key information
`altSignatureAlgorithm`	alternative digital signature algorithm
`AltSignatureValue`	alternative signature

… to be used *instead* of the native fields (if present)

→ Allows for a smooth migration of a PKI to a new signature algorithm

→ Does *not* intend hybrid use of algorithms

Question: Do we need a hybrid solution for authentication with regard to PQC?