COSE HPKE

draft-ietf-cose-hpke-02

Hannes Tschofenig, Russ Housley, Brendan Moran
Public Key Format(s)
What format should we use?

P256 public key (Ilari’s proposal)
{
  / kty => OKP /  
  1: 1,  
  / kid /  
  2: h'1F677209D1C5174C,  
  / crv => -65537 (HPKE P256 with SHA256) /  
  -1: -65537,  
  / Raw public key data, 65 bytes /  
  -2: h'040E271193..69'  
}

P256 public key (COSE)
{
  / kty => EC2 /  
  1:2,  
  / kid /  
  2: h'1F677209D1C5174C',  
  / crv => P-256 /  
  -1:1,  
  / x => x-coordinate /  
  -2:h'0072...85e5c8f42ad',  
  / y => y-coordinate /  
  -3:h'01dc...fe1ea1d9475',  
}
Ciphers without Integrity Protection

• Use case of firmware encryption requires the use of ciphers without integrity protection (such as AES-CTR or AES-CBC).
• Integrity protection is still provided by other means (signature over plaintext payload in the SUIT software encryption case).
• Join SUIT meeting for details

• Idea:
  • Register such algorithms but require them to be used only when integrity protection is offered separate from the encryption.