# X.509 Certificate EKU for JOSE/COSE

draft-reddy-lamps-jose-eku-01

**IETF116, March 2023**

**T. Reddy** (Nokia)
J. Ekman (Nokia)
D. Migault (Ericsson)

# Problem

- Restrict the purpose of EE certificate to prevent misuse
- No extended key purpose identifiers for
  - Javascript Object Signing and Encryption: JSON Web Signature (JWS), JSON Web Encryption (JWE)
  - CBOR Object Signing and Encryption: CBOR Web Signature (CWS), CBOR Web Encryption (CWE)

# Use case

- Network Functions (NFs) as part of the service-based architecture within the 5G System.
- Certificate (issued by internal CA) can be misused for tasks that 5G NF is not entitled to perform.
  - Certificates for signing Client Credentials Assertion (CCA) tokens using JWS (Section 13.3.8.2 of [TS33.501])
  - Certificates for encrypting JSON objects in HTTP messages between Security Edge Protection Proxies (SEPPs) using (Section 13.2.4.4 of [TS33.501]) and Section 6.3.2 of [ TS33.210])
  - Certificates for signing access tokens for service access authorization in intra-domain (within the PLMN) and/or inter-domain (in roaming scenarios) Service Based Architecture (SBA) scenarios using JWS (Section 13.4.1 of [TS33.501])

# Solution

- Define extended key purpose identifiers for JWS, JWE, CWS and CWE.

```
id-kp  OBJECT IDENTIFIER  ::= {
       iso(1) identified-organization(3) dod(6) internet(1)
       security(5) mechanisms(5) pkix(7) kp(3) }

id-kp-jws OBJECT IDENTIFIER ::= { id-kp TBD1 }
id-kp-jwe OBJECT IDENTIFIER ::= { id-kp TBD2 }
id-kp-cws OBJECT IDENTIFIER ::= { id-kp TBD3 }
id-kp-cwe OBJECT IDENTIFIER ::= { id-kp TBD4 }
```

# Discuss: Multiple EKU

- 2 EKU (JOSE, COSE) + keyUsage bits
- 4 EKU (JWS, JWE, CWS, CWE)
  - RFC5280, key usage extension and extended key usage extension must be processed independently.
    - The certificate can be used provided the purpose is consistent with both extensions.
  - JWS and JWE are used for JWT claims
  - **No need to add a processing rule to check if both the extensions are consistent or not.**

# Next Step

- Presented in 3GPP SA3 meeting at Athens
  - TR (solution #10 of TR 33.876 v.0.6.0) which addresses the KI#7
  - KI#7: Investigate the possibility to adopt the extensions introduced in IETF draft-reddy-lamps-jose-eku-00, which is work in progress in IETF at the time of writing
- Comments and suggests are welcome
- Consider for WG adoption