~~Best Practices for CMS SignedData with Regards to Signed Attributes~~
Best Practices for Signed Attributes in CMS SignedData

draft-ietf-lamps-cms-euf-cma-signeddata-02

Daniel Van Geest, Falko Strenzke

IETF 125 – LAMPS

Since WG Adoption

- New mimeData content type
- Best Practices
  - New uses of CMS SignedData MUST NOT use id-data
  - New uses where content is MIME encoded SHOULD use mimeData
  - -bis documents SHOULD deprecate id-data or provide rationale for not doing so
  - -bis documents keeping id-data SHOULD specify that signedAttrs is always required or forbidden
  - Recipients SHOULD perform expected content type and signedAttrs verification
- id-data mitigations remain the same

Since WG Adoption

- Security Considerations
  - Updated for case of signing+encryption
  - Point out that using signedAttributes loses the independence from the assumption of collision resistance in some signature schemes (SLH-DSA, LMS, XMSS)
- + simple ASN.1 Module
- + IANA Considerations

Next

- Minor updates + request WGLC