EUF-CMA for CMS SignedData

draft-vangeest-lamps-cms-euf-cma-signeddata-01

Daniel Van Geest, Falko Strenzke

IETF 122 – LAMPS

The Problem

ForgedAttributes: An Existential Forgery Vulnerability of CMS and PKCS#7 Signatures, Falko Strenzke, https://eprint.iacr.org/2023/1801.pdf

- Different signing behaviour when SignedAttributes is present allows an existential forgery.

Virtual Interim

- Comments
  - Write a BCP (used signed attributes in new/updated CMS applications)
  - “how critical is it that we retro-fix this? Are there actual practical attacks?”
  - “Worth writing down to use context for new algorithms, worth writing down mitigation/detection for RSA/ECDSA. Whether it's worth revising Ed448, I don't know.”

IETF Uses of id-data

RFC	Signed Attributes Usage
SCEP	Required
SZTP	Silent
S/MIME	Recommends
Bundle Security Protocol	Forbids
IPFIX	Silent
Traceable Anonymous Certificate	Forbids
CAdES	Required
ODETTE	Silent
Electronic Signature Formats	Required

Next Steps?

- The authors are inclined to write a BCP:
  - New uses of CMS should not use *id-data* eContentType.
  - New versions of existing *id-data* uses should try to move away from *id-data*, or require the use of signed attributes.
  - Implementation guidance?
    - If you must use *id-data*, you could do attack detection.
    - Verifiers who see eContentType != *id-data* must fail verification if signed attributes are not present.
  - More?

- Sound good?
- Adopt?