Deprecate “none” and “RSA1_5”

Neil Madden

draft-ietf-jose-deprecate-none-rsa15

IETF 121, Dublin, 2024–11–04

RSA1_5

RSA encryption with PKCS#1 v1.5 padding

Bleichenbacher’s Attack (BB’98)

Forbidden by NIST/FIPS since end 2023

Replacements now widely implemented (OAEP, ECDH)

“none”

No security at all

Long history of mistakes: (10+ CVEs, many Critical)

Easy to replace (?)

But: some standards use it (OIDC, ISO)

Current status

Draft adopted by WG

WG -00 version just submitted

As original I-D, with changes from WG feedback:

- Clarified algs are *deprecated* not *prohibited*
- Clarified `RSnnn` *signature* algorithms unchanged

  Also fixed some xml2rfc warnings

1.3. Guidance on deprecation

> Both of the algorithms listed above are deprecated for use in JWS and JWE. JOSE library developers SHOULD deprecate support for these algorithms and commit to a timeline for removal. Application developers SHOULD disable support for these algorithms by default. New specifications building on top of JOSE MUST NOT allow the use of either algorithm.

4.2. Updated Review Instructions for Designated Experts

New algorithms must meet standard security goals:

- JWS: EUF-CMA
- JWE key encryption/KEM: IND-CCA2
- JWE content encryption: AEAD

“Reasonably conjectured to meet [the goal]”

Discussion: COSE too?