

Update on JWS signed Vouchers

JWS signed Voucher Artifacts for Bootstrapping Protocols
draft-ietf-anima-jws-voucher-06

Michael Richardson, Thomas Werner

mcr+ietf@sandelman.ca

thomas-werner@siemens.com

Shepherd: Matthias Kovatsch

IETF 116

ANIMA Working Group

JWS Voucher and options

- RFC 8366 specifies CMS-signed JSON for Voucher artifacts → Draft: JWS signed JSON
- Makes no YANG changes to RFC 8366
- Changes of draft-ietf-anima-jws-voucher-05 --> 06
 - Restructuring and clean-up, preparation for WGLC¶
 - Included feedback from shepherd review¶

JWS Voucher Results from WGLC

- Two major identified points are rather process related
 - JWS-Voucher currently targets an update of RFC 8366, which it should not.
 - It is intended as another form factor next to CMS-voucher
 - Proposal to remove “update” and to include proposed text from review

RFC8366bis defines a "CMS signed JSON Voucher Artefact" (RFC8366, Section 6.5). The voucher is defined via YANG and CMS is the signature format. This document defined a "JWS signed JSON Voucher Artefact" using the voucher YANG definitions of RFC866bis and replacing the CMS signature with a JWS signature.
 - “Todo” included for *typ* value definition “voucher-jws+json” was included to not miss IANA registration
- Remaining comments were related to editorial improvements

JWS Voucher - Next Steps

- Address comments from WGLC
- Interop testing with others welcome 😊
 - Could happen in combination with BRSKI-PRM interop
- Finalization of document, shepherd writeup

BRSKI-PRM: BRSKI with Pledge in Responder Mode (draft-ietf-anima-brski-prm)