

# Klargjør sjekksumalgoritme-verdi og referanse

---

Prosjekt	NOARK 5 Tjenestegresesnitt
Kategori	Versjon 1.0 beta
Alvorlighet	kommentar
Meldingstype	trenger klargjøring
Brukerreferanse	pere@hungry.com
Dokumentdel	7.2.1.7
Sidenummer	106
Linjenummer	n/a
Innsendingsdato	2017-06-12

---

Denne teksten er del av en samling innspill til NOARK5-standarden tilgjengelig fra <https://github.com/petterreinholdtsen/noark5-tester/>.

## Beskrivelse

Gjelder også side 61 i Noark 5 versjon 4.0 vedlegg nr. 1 Metadatakatalog.

Det fremgår ikke klart fra tjenestegresesnittet og Noark 5-standarder hvilke verdier som er gyldige i metadatafeltet M706 sjekksumAlgoritme. Tjenestegresesnittet forklarer at algoritmen som skal brukes i dag er SHA 256, men sier ikke noe om hvilken verdi selve feltet skal ha når det gjøres.

Betingelsen for M706 i metadatakatalogen til Noark 5 versjon 4.0 på side 61 sier

Betingelser: Kan ikke endres. Algoritmen som skal brukes inntil videre er SHA256.

Spesifikasjonen for tjenestegresesnittet del 7.2.1.7 (Dokumentobjekt) i listen med restriksjoner på side 106 sier:

M706 sjekksumAlgoritme: Algoritmen som skal brukes inntil videre per SHA256.

En kunne ut fra dette anta at verdien som skal brukes er «SHA256», men «[Eksempel på innhold i malen for arkivuttrek.xml for Noark 5 versjon 4.0](#)» bruker verdien «SHA-256» med bindestrek. Det er dermed minst to ulike tolkninger av lovlig verdi for dette feltet. Det bør være entydig definert i tjenestegresesnittet hvilken verdi som vil bli gjenkjent av klient og tjeneste. Gitt at verdien «SHA-256» allerede er brukt i et eksempeluttrekk, foreslår jeg at denne varianten velges som lovlig verdi for metadatafelt M706.

Jeg har ikke klart å finne en referanse i spesifikasjonen for tjenestegresesnitt eller i Noark 5-spesifikasjonene forøvrig til hva som konkret menes med sjekksumalgoritmen SHA 256, hverken i spesifikasjonen for Noark 5 versjon 4.0 eller i spesifikasjonen for Noark 5 Tjenestegresesnitt versjon 1.0 Beta. Algoritmen er velkjent, men det kunne med fordel refereres til en spesifikasjon der SHA 256 er forklart. En slik mulig referanse er [IETF RFC 4634](#). Jeg foreslår at denne legges inn i tjenestegresesnitt-spesifikasjonen under del 2 (Normative referanser) i tjenestegresesnittspesifikasjonen.

## Ønsket endring

Endre del 2 (Normative referanser), legg inn nytt punkt på slutten:

SHA-256 er definert i IETF RFC 4634 - <https://tools.ietf.org/html/rfc4634>.

Endre spesifikasjonen for tjenestegresesnittet del 7.2.1.7 (Dokumentobjekt), bytt ut denne tekst i listen med restriksjoner på side 106

M706 sjekksumAlgoritme: Algoritmen som skal brukes inntil videre er SHA256.

med denne teksten:

M706 sjekksumAlgoritme: Algoritmen som skal brukes inntil videre er SHA-256. Obligatorisk verdi:  
«SHA-256»

Endre betingelsen for M706 i metadatakatalogen for Noark 5, bytt ut

Algoritmen som skal brukes inntil videre er SHA256»

med

Algoritmen som skal brukes inntil videre er SHA-256».

Obligatorisk verdi:

- «SHA-256»