Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

Notat

Dato:	26.3.2021	**Saksnr:**	21/00208-9

Til:	
Fra:	Seksjon for strategi og tjenesteutvikling
Saksbehandler:	Sindre Børsheim Ramung

PAdES valideringsfeil ift. arkivstandard

Oppsummering

Fellestjenestene eSignering har en valideringsfeil i malene som brukes for å generere arkivkompatible PAdES-dokumenter (avansert signerte PDFer). Feilen knytter seg til selve PAdES-signaturen, som blir for stor ift. PDF/A-(3b-) spesifikasjonen. Feilmeldinger som kan oppleves ved validering kan være:

- *Implementation limit: String too long,*
- *A string length exceeds the limit defined by the standard,*
- *o.l.*

Feilen har oppstått høsten 2020 fordi vi nå inkluderer mere langtidsvalideringsdata i signaturen enn tidligere. Vi ser at PAdES- og PDF/A-spesifikasjonene ikke er helt samkjørte på dette punktet og at PAdES-signaturene derfor skaper problemer ved validering ift. PDF/A.

Avviket gjelder et usynlig felt i PAdES og påvirker verken autentisiteten til det signerte dokumentet eller brukeropplevelsen ved behandling av dokumentet eller signaturen.

Digitaliseringsdirektoatet har varslet Arkivverket om det spesifikke avviket fra arkivstandarden. Arkivverket svarer at de aksepterer avviket, fordi avviket ikke påvirker de egenskapene ved PDF/A-dokumenter som er viktige ifm. avlevering. Aksepten gjelder altså alle PAdES-filer som er framstilt i fellestjenesten siden høsten 2020, og som offentlige virksomheter avleverer til Riksarkivet.

Likevel ønsker Arkivverket at det blir gjort oppmerksom avviket og årsakene til det ifm. avlevering. Digitaliseringsdirektoratet ser at forventningen om at arkiveieren varsler om avviket ifm. avlevering er problematisk for arkiveierne, og beklager dette.

Vi jobber sammen med leverandøren om å få rettet feilen i løpet av 2. kvartal 2021.

Utfyllende beskrivelse av problemet og bakenforliggende årsak

Problem

Ved generering av arkivkompatible PAdES i eSignering er det observert avvik fra forventet PDF/A standard for resultatdokumentene. Forventet resultat skal være PDF dokumenter, påført avansert signatur (PAdES), kompatible med PDF/A-3b standarden.

Avviket som er observert gjelder brudd på seksjon 6.4.3 i underliggende standard ISO 19005 (PDF/A-3), som igjen refererer PDF 32000-1:2008, Annex C.1, “Maximum length of a string, in bytes = 32,767”.

Årsak

Feltet med tekststrengen som blir for lang er Contents feltet med den digitale signaturen (forseglingen), og oppstår når det inkluderte langtidsvalideringsmaterialet (LTV) er for omfattende. Contents-feltet tolkes som et tekstfelt i PDF/A standarden.

Dette langtidsmaterialet består av involverte sertifikatskjeder, samt revokeringsinformasjon for disse på signeringstidspunktet, typisk signerte OCSP responser og/eller signerte revokeringslister (CRL). Det er sistnevnte som skaper problemer dersom innholdet av listen blir stort, noe som kan skje for “gamle” CAer der også intermediate røttene er “gamle” og mange sertifikater utstedt av denne intermediate roten har utløpt og eller har blitt revokert.

Dagens implementasjon er gjort iht. ETSI TS 102 778-3 og ETSI TS 102 778-4, og er i tråd med Adobe’s støtte for PKCS#7 strukturerte digitale signaturer.

Konsekvens

Rent bortsett fra at dette er et avvik fra PDF/A-3b standarden, så vil den praktiske konsekvensen være ubetydelig fordi det relevante feltet ikke er et synlig felt, og dermed ikke vil påvirke fremvisning av innholdet i PDF dokumentet.

Premisset for dette resonnementet er at hensikten med PDF/A er å sikre korrekt fremvisning av innholdet i PDF dokumentet i fremtiden uavhengig av tilgjengelighet av eksterne ressurser slik som fonter.

Selve tolkingen av den digitale signaturen med LTV materiale, er uavhengig av PDF/A standarden og vil ikke påvirkes av dette avviket.

Plan for utbedring

Permanent utbedringen av dette problemet er en del av planlagt overgang til nytt signaturbibliotek på kodenivå. Metodikken som benyttes der vil plassere LTV materiale i egne “dictionary” elementer i PDF dokumentet, slik at disse ikke innbefattes i Contents feltet til signaturen.

Dette arbeidet er i gang hos leverandøren, Signicat.

Eventuelle spørsmål kan rettes til servicedesk@digdir.no