De berørte organene må ha en egen instruks med rutiner for hvordan de velger å bruke funksjonene basert på utvekslingsformatet.

6.3.2 Kryptering og elektronisk signatur

Ved elektronisk kommunikasjon er det nødvendig å kunne angi krav til sikkerhet. Dette innebærer krav til kryptering og elektronisk signatur, samt dokumentasjon av sikkerheten til dokumenter som er sendt eller mottatt i elektronisk form. Man må også kunne angi krav til sikkerhet på forskjellige nivå i arkivstrukturen.

Løsninger som er konfigurert for å lagre kryptert, vil typisk stå overfor to mulige alternativer for rekryptering:

1) Lagre med *samme kryptering* som var påført ved mottak eller ved utsendelse. Det vil innebære at man bare kan lese et mottatt/ekspedert dokument ved å bruke avsenderes offentlige nøkkel. Slike nøkler er i praksis "ferskvare", og svært vanskelig å administrere pålitelig over lenger tid enn noen få år. Det kan imidlertid tenkes at noen har behov for å lagre kryptert innhold på den måten, for å oppnå høy grad av bevisbarhet for at avsender har sendt det angitte innholdet ("ikke-benekting").
2) Åpne det mottatte eller ekspederte dokumentet, og påføre en ny kryptering som man lagrer det med. En slik ny kryptering kan være av en annen type (for eksempel symmetrisk kryptering), eller kryptert med organets eget virksomhetssertifikat. Dette vil bidra til at det blir betydelig enklere å sikre tilgjengeligheten over tid. På den annen side vil ikke-benektbarheten svekkes noe, og bevisbarheten vil i større grad hvile på troverdige rutiner for verifisering og logging av hva som skjer med dokumentene etter mottak.

I tilfelle 2 bør endringer logges: Type kryptering/sikkerhetsnivå dokumentet på mottakstidspunktet, type kryptering/sikkerhetsnivå ved re-kryptering med, hvem som har utført endringen.

Metadata for verifisering av elektronisk signatur

Metadata for verifisering av elektronisk signatur skal kunne grupperes inn i metadata for journalpost og dokumentbeskrivelse. Det skal være mulig å ha ulikt sikkerhetsnivå på de ulike dokumentene.

Nr.	Navn	Type	Forek.	Avl.	Merknad
M507	elektroniskSignatur Sikkerhetsnivaa	B	En	A	Obligatorisk når det er foretatt verifisering av elektronisk signatur.
M508	elektroniskSignaturVerifisert	B	En	A	Obligatorisk når det er foretatt verifisering av elektronisk signatur.