men hvor innholdet har en felles kjent form og struktur. Det vil ofte gjelde kommunikasjon mellom et organ og deres brukere, der innholdet for eksempel er søknadsskjemaer eller annen strukturert informasjon. Tredje og fjerde kategori er kommunikasjon der innholdet har ukjent form og struktur (for eksempel brev), mellom henholdsvis kjente og ukjente aktører. For disse to kategoriene bør hensiktsmessig journalføring og arkivering baseres på Noark 5 *utvekslingsformat. Se kapitlene 6.3.1* E-post *og 8 E-postløsninger.*

	Innhold med kjent form og struktur	Innhold med ukjent form og struktur
Kjente aktører	Bilaterale avtaler evt. også felles programvare o.l.	Utvekslingsformat, e-post etc. Lave krav til sikkerhet i kommunikasjonen
Ukjente aktører	Helhetlige rammeverk for kommunikasjon f.eks. sikre web-skjemaer, ebXml e.l.	Utvekslingsformat, e-post etc. Høye krav til sikkerhet i kommunikasjonen

Ulike grunnlag for tillit til elektronisk avsendte og mottatte dokumenter

For første kategori vil det være få tekniske sikkerhetskrav, ettersom partene kan avtale sikkerhetsnivå og relevante sikkerhetsmekanismer seg i mellom.

For de tre øvrige kategorier gjelder de grunnleggende prinsippene i eForvaltningsforskriftens § 4: Hovedprinsippet er at enhver kan henvende seg til et forvaltningsorgan ved bruk av elektronisk kommunikasjon uten bruk av sikkerhetstjenester eller -produkter. Dersom det er nødvendig, etter nærmere kriterier i eForvaltningsforskrifen eller annen lov, kan imidlertid forvaltningsorganet kreve bruk av sikkerhetstjenester eller -produkter som de gjør tilgjengelig.

eForvaltningsforskriften, særlig kapittel forskriftens 6, supplerer arkivlovas og arkivforskriftens regler om organets behandling av meldinger som er kryptert eller *elektronisk signert*. Det er i utgangspunktet mulig å velge mellom ulike strategier for behandling av krypterte eller signerte meldinger. De obligatoriske kravene er basert på en strategi som kan sies å ha lavt ambisjonsnivå. Den går ut på at organet dekrypterer meldingen ved mottak, deretter tilføres registreringen og dokumentbeskrivelsen metadata om forsendelsen. Det mottatte dokumentet lagres i ukryptert form i Noark 5-kjernen. Senere bruk av dokumentet innenfor organet vil kun være basert på den ordinære tilgangskontrollen i Noark-løsningen.

Det er lite metadata på dette området som skal lagres internt i Noark 5-løsningen. Detaljerte verifikasjonsdata skrives i den utstrekning det er behov for til logger, jf. kapittel *13 Logg- og sporingsløsninger*.

Krav nr.	Krav til metadata for dokumenter mottatt eller sendt med elektronisk signatur	Type	Merknad
12.4.1	Hvis et inngående kryptert dokument er signert elektronisk av en annen enn den som er oppgitt som avsender, bør Noark 5-løsningen varsle om dette	V	