IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

FESD Sikker epostløsning

Standard

IT- og Telestyrelsen København den 23. august 2006.

FESD-standardisering
Sikker epostløsning. Grænsesnit Version 1.0

Kolofon:

FESD-standardisering. Sikker epostløsning. Grænsesnit Version 1.0

Denne standard kan frit anvendes af alle. Citeres der fra standarden i andre publikationer til offentligheden, skal der angives korrekt kildehenvisning.

Forslag til FESD-standarder udarbejdes af IT- og Telestyrelsen, IT-Arkitektur kontoret, FESD-standardiseringsgruppen i samarbejde med de tre FESD-leverandører Software Innovation A/S, Accenture I/S og CSC Danmark A/S.

Kontaktperson i FESD-standardisering:

Projektleder Tom Bøgeskov, Mail-adresse tob@itst.dk

Telefon 33 37 92 95 (direkte)

Accenture I/S
Lautrupsgade 7
2100 København Ø
Telefon: 72 28 80 00
Web-adresse: http://www.accenture-fesd.dk/

CSC Danmark A/S
Retortvej 8
1780 København V
Telefon: 36 14 40 00
Web-adresse: http://www.fesd-alliancen.dk/

Software Innovation A/S
Nærum Hovedgade 10
DK-2850 Nærum
Telefon: 45 58 88 88
Web-adresse: http://www.softwareinnovation.dk/

Ministeriet for Videnskab, Teknologi og Udvikling
IT- og Telestyrelsen
National IT and Telecom Agency
Ministry of Science, Technology and Innovation

IT-Arkitektur kontoret
Holsteinsgade 63
DK-2100 København Ø
Telf. +45 35 45 00 00
Fax. +45 35 45 00 10
http://www.itst.dk
itst@itst.dk

Indholdsfortegnelse

1 Forord

Den offentlige sektors IT-systemer på statsligt, kommunalt og regionalt niveau skal kunne spille sikkert og effektivt sammen. Derfor arbejdes der målrettet på at få gennemført fælles standarder for elektronisk sags- og dokumenthåndtering - den såkaldte FESD-standard. Målet med standardiseringsarbejdet er at fremme digital forvaltning i den offentlige sektor, og midlet er at sikre, at de forskellige elektroniske sags- og dokumenthåndteringssystemer (ESDH) får en fælles kernefunktionalitet, og at det samtidig sikres, at denne kerne videreudvikles ensartet. En fælles kernefunktionalitet skal sikre:

- at der kan foretages sagsbehandling på tværs af flere organisationer
- at myndigheder, der arbejder med åbne sager, kan lægges sammen
- at der kan flyttes opgaver mellem forskellige myndigheder

I forlængelse af FESD-projektkonkurrencen, som havde sin afslutning primo 2004, og hvor der blev fundet tre FESD-leverandører, blev det i forbindelse med kontraktforhandlingerne besluttet at starte en standardiseringsproces – den såkaldte FESD-standardisering.

For at sikre interoperabiliteten, både til andre systemer, men også så tredjepart kan udvikle moduler til systemet, blev det anset for afgørende, at der udvikles en fælles offentlig datamodel samt andre standarder på ESDH-området.

Koordinering af FESD-standardiseringen er efterfølgende lagt i IT- og Telestyrelsen (ITST). Den konkrete udarbejdelse af forslag/udkast til standarder foregår i et samarbejde mellem de tre FESD-leverandører og en FESD-standardiseringsgruppe i ITST.

Arbejdet med forslag/udkast til standarder tager udgangspunkt i Noark 4's datamodel og databeskrivelser samt leverandørernes løsninger. Standarderne kan afvige fra Noark 4 på de områder, hvor det er nødvendigt for at understøtte dansk forvaltningspraksis, eller hvor parterne i FESD-standardiseringen kan opnå enighed om en afvigelse.

Udkast/forslag sendes herefter i offentlig høring i ca. 1 måned. FESD-standardiseringsgruppen tilretter og færdiggør på baggrund af høringen de endelige "Forslag til standarder".

Standardforslagene forelægges herefter OIO-Datastandardiseringskomiteen til godkendelse. Godkendte standarder forelægges efterfølgende OIO-IT-Arkitekturkomiteen med henblik på accept af publicering via OIO-Kataloget.

Efter den samlede godkendelse bliver standarderne således offentliggjort og indgår i IT- og Telsestyrelsens "OIO-Katalog", som indeholder en oversigt over godkendte og anbefalede standarder til digital forvaltning i det offentlige.

I standarden kan forekomme brug af særligt ordvalg. Følgende termer anvendes konsekvent i den følgende betydning:

- "**skal**"/"**obligatorisk**": betyder, at den nævnte metode/element/mulighed/etc. skal benyttes eller skal forefindes – dvs. må ikke udelades.
- "**må ikke**": betyder, at den nævnte metode/element/mulighed/etc. ikke må forefindes eller må ikke benyttes.
- "**bør**"/"**anbefalet**": betyder, at det i høj grad anbefales, at den nævnte metode/element/mulighed/etc. benyttes eller forefindes. Der skal være tungtvejende grunde til at udelade.
- "**kan**"/"**optionel**": betyder, at den nævnte metode/element/mulighed/etc. er en valgmulighed og derfor valgfri at medtage.

2 DEL A

2.1 Indledning

Det er besluttet, at som et led i FESD-standardiseringsarbejdet, skal der gennemføres en standardisering vedrørende digitale signaturer, der dækker den anvendelse, der i dag finder sted i det offentlige.

I standardiseringsarbejdet har der været en dialog med en gruppe sikker epost leverandører på markedet og IT- og Telestyrelsens IT-sikkerhedskontor.

Alle klasse- og attributreferencer i diagrammerne i denne standard er på engelsk. Den danske reference kan findes i tabellerne i Del C (attribut dan., klasse dan.). Det danske attributnavn er en oversættelse af det tilsvarende engelske attributnavn.

2.2 Formål

Denne standard omhandler integration af sikker epostløsninger med ESDH-systemer med det formål at understøtte udveksling af sikker epost mellem en organisation og dens eksterne parter.

Sikker epostløsninger også kaldet ”Mail sweepere” eller ”Mail gateways” er løsninger, der håndterer en organisations fælles certifikater og sørger for kommunikation med certifikater.

I en udvekslingssituation er det sikker epostløsningens rolle at håndtere signering og kryptering i forhold til virksomhedscertifikater og at validere informationer omkring forsendelsen.

ESDH-systemets rolle i relation til en brevudveksling er først og fremmest at være arkiv for de dokumenter og informationer, der udveksles, og dernæst at være en sikker container for oplysningerne omkring forsendelsen.

Der er derfor allerede lavet en række løsninger, hvor sikre epostløsninger er integreret med ESDH-systemet, i den forbindelse er der aftalt sikkerhedsprocedurer og den tekniske integration for løsningerne individuelt for hver implementering.

Det, at der ikke findes nogen standard for eller vejledning i, hvordan denne type af integrationer skal laves, betyder en væsentlig fordyrelse af den enkelte integration. Både ESDH-leverandøren og leverandøren af sikker epostløsningen skal lave specialtilpasninger – og det er typisk myndigheden selv, der har ansvaret for, at løsningen som helhed fungerer. Derudover er der en risiko for, at den integration, der aftales lokalt, ikke er sikkerhedsmæssigt i orden, således at myndigheden står svagt, hvis der skal føres bevis for, at en konkret epost kommunikation har fundet sted.

2.3 Grænseflader og afgrænsninger

Den her beskrevne standard er afgrænset til epost og har ikke fokus på andre anvendelser af certifikater til sikker kommunikation, der evt. skal dokumenteres i ESDH-systemer.

Standarden kan på et senere tidspunkt udvides til at omhandle andre anvendelser af certifikater til sikring af levering af meddelelser eller dokumenter til eller fra ESDH-systemer, så den eksempelvis kunne udvides til at dække, hvordan et Content Management system afleverer en signeret blanket til et ESDH-system.

Epost kommunikation mellem organisationer er også temaet for standarden vedrørende ’FESD-udvekslingspakke’ trin 1, der er en protokol til udveksling af dokumenter mellem ESDH-systemer via epost. Standarden vedrørende ’FESD-udvekslingspakke’ beskæftiger sig i trin 1 ikke med sikkerhed eller autenticitet (kryptering eller signering) ved udvekslingen, men beskæftiger sig med hvordan en epost opbygges af dokumenter, der skal udveksles, og hvordan metadata beskrives i en vedhæftet efølgeseddel i dokform-format. Den her beskrevne standard er komplementær til standarden vedrørende ’FESD-udvekslingspakken’ trin 1 - idet det er forskellige aspekter af en forsendelse de to standarder beskæftiger sig med.

Der er planlagt et trin 2 til standarden 'FESD-udvekslingspakken', som sigter på at beskrive en udvekslingspakke udelukkende i XML-format – uden epost-indpakningen af dokumenter og følgeseddel. Trin 2 kan evt. også indeholde muligheden for at signere eller kryptere dele af udvekslingspakken. Det kan derfor være, at Trin 2 vil være funktionelt overlappende i forhold til denne standard, idet der tilbydes en anden måde at kommunikere sikkert mellem to organisationer med ESDH-systemer.

2.3.1 eDag2

Den 1. februar 2005 var det eDag2. Med eDag2 har alle myndigheder forpligtet sig til at have en officiel sikker epost adresse, der som noget nyt muliggør sikker og fortrolig epost kommunikation med den offentlige sektor. Efter den dato har alle offentlige myndigheder i stat, amt og kommune som udgangspunkt ret til at sende breve og dokumenter med følsomme og fortrolige oplysninger fuldt elektronisk til andre myndigheder og droppe papirversionen. Tilsvarende har de også ret til at kræve, at andre myndigheder sender fuldt elektronisk til dem. Endvidere har borgere og virksomheder efter denne dato ret til at sende sikker epost til det offentlige.

2.3.1.1 Baggrund

eDag2 er en fortsættelse af eDag. Den første eDag gav myndighederne ret og pligt til at kommunikere digitalt, men undtog dokumenter med følsomme og fortrolige oplysninger, idet disse ikke måtte sendes over det åbne Internet, med mindre de var krypteret. Det var et ufravigeligt krav til offentlige myndigheder for så vidt angår personoplysninger. Endvidere var kommunikation med borgere og virksomheder ikke omfattet af den første eDag.

Såvel eDag som eDag2 var aftalt mellem Regeringen, KL, Amtsrådsforeningen, Københavns Kommune og Frederiksberg Kommune efter anbefaling fra Den Digitale Taskforce. De involverede parter havde aftalt datoen for eDag2 og det nærmere omfang af rettigheder og pligter. eDag2-initiativet var endvidere forankret i regeringens moderniseringsprogram og i strategien for Digital Forvaltning.

2.3.1.2 Formålet

Formålet med eDag2 var at skabe en mere effektiv offentlig sektor gennem optimal udnyttelse af digitale værktøjer. eDag2 ville medføre, at en stor del af det offentliges brevpost kunne omlægges til fuldt digitale arbejdsgange, og dermed spare ressourcer til posthåndtering, scanning, kopiering og porto samt give en hurtigere sagsbehandlingstid.

2.3.1.3 eDag2 og digital signatur

Videnskabsministeriet udarbejdede i forbindelse med eDag2 aftalen i samarbejde med Den Digitale Taskforce, KL og Amtsrådsforeningen en række minimumskrav til sikker epost løsninger, som blev anbefalet til alle, der skulle implementere eDag2. Minimumskravene blev udarbejdet med udgangspunkt i konsulentfirmaet Devoteam Fischer & Lorenzes vejledning om implementering af digital signatur i kommunerne og med deltagelse af bl.a. Kommunernes Revision (KR).

Et væsentligt krav til myndighederne i forbindelse med eDag2 var, at de kunne sende sikker epost til og modtage svar på samme vis fra borgere, virksomheder og andre myndigheder.

Sikker epost har til formål at håndtere følgende tre sikkerhedselementer i forbindelse med digital kommunikation:

- Autenticitet, der giver modtageren af en meddelelse garanti for, at den kommer fra den person, som påstår at have sendt den
- Integritet, der giver sikkerhed for, at en modtaget meddelelse er identisk med den meddelelse, som afsenderen sendte
- Fortrolighed, der giver sikkerhed for, at uvedkommende ikke kan få kendskab til meddelelsens indhold

I praksis tilgodeses disse sikkerhedselementer ved, at afsenderen signerer eposten med sit eget digitale certifikat (dette sikrer autenticiteten og integriteten af eposten) og krypterer eposten med den offentlige del af modtagerens digitale certifkat (dette sikrer fortroligheden). For at kunne signere og kryptere en epost kræves altså en digital signatur hos både afsender og modtager. Der vil ikke altid være behov for både at signere og kryptere eposten, men for at leve op til eDag2 skulle sikker epostløsningen kunne håndtere begge dele.

eDag2 baserede sikker epost på det offentliges standard for digital signatur, den såkaldte OCES standard, hvor OCES er en forkortelse for Offentlige Certifikater til Elektronisk Service. Udstedelse, indhold, håndtering og anvendelse af OCES certifikater er beskrevet i OCES certifikatpolitikkerne, som kan læses og downloades på www.signatursekretariatet.dk. En detaljeret beskrivelse af eDag2 minimumskravene kan findes på www.digitalsignatur.dk.

2.3.2 Signering og kryptering i relation til ESDH-systemer

Teknologien og infrastrukturen der knytter sig til certifikater, kan anvendes til at sikre autenticitet, integritet og fortrolighed i forbindelse med forsendelsen af meddelelsen.

Når meddelelsen først er nået frem til modtageren og er lagret i et ESDH-system, er informationerne underkastet ESDH-systemets sikkerhedssystem og dermed sikret både mht. autenticitet, integritet og adgangsbeskyttelse.

De tekniske elementer, der indgår i beviset for fremsendelsen det vil f.eks. sige:

- Certifikatet der er brugt til at signere med
- Signaturen der er tilknyttet eposten
- Spærrelisten der er brugt til at verificere, at afsenderens certifikat var validt på modtagelsestidspunktet

er kun interessante på modtagelsestidspunktet – herefter er deres validitet ikke af betydning.

Derfor er det vedtagne udgangspunkt for dette standardiseringsarbejde, at når en forsendelse er modtaget eller afsendt fra en organisation og lagret i ESDH-systemet, er det kun informationer *om* sikkerhed og autenticitet, der er anvendt og indhentet ved forsendelsen, der lagres i ESDH-systemet - og *ikke* selve de tekniske elementer, der indgår i beviset.

2.3.3 Anvendelse af ”medarbejdersignatur avanceret”

Med anvendelse af ”medarbejdersignatur avanceret” bliver det ikke længere nødvendigt, at løsninger kan håndtere krypteret epost, der sendes direkte til personlige postkasser i en organisation. Det forudsættes i standardiseringsarbejdet, at der kun anvendes ”medarbejdersignatur avanceret” i de organisationer, der ønsker at implementere integrationen mellem sikker epostløsningen og ESDH-systemet.

2.3.3.1 Baggrund for ”medarbejdersignatur avanceret”

Modtagelse og afsendelse af sikker epost med kryptering har typisk været en udfordring for virksomheder, som har centrale løsninger til kontrol af epost for virus og spam. Samtidig har krypteret epost, sendt direkte til medarbejdere, også kunnet give problemer i forhold til tilgængelighed af data for andre medarbejdere.

Problemet med krypteret epost til en given medarbejder har hidtil været løst ved, at afsenderen udenfor organisationen skulle sende epost adresseret til den enkelte medarbejder og Cc: til en central indholdsscanner (fælles postkasse) med efterfølgende manuel postdistribution internt. Disse løsninger har forskellige anvendelsesmæssige svagheder. For at undgå ovenstående svagheder er der etableret en ny form for medarbejdercertifikater kaldet for ”medarbejdersignatur avanceret”.

2.3.3.2 Funktion

Virksomheden har mulighed for at bestille ”medarbejdersignatur avanceret” igennem virksomhedens LRA enhed (Lokal Registrerings Autoritet er den autoritet i en virksomhed, der administrerer virksomhedens interne certifikater). For at kunne udstede ”medarbejdersignatur avanceret” skal der i forvejen være adgang til

et virksomhedscertifikat. Når virksomhedens LRA opretter en medarbejder med ”medarbejdersignatur avanceret”, vil der genereres to certifikater med hver sit nøglepar. Det ene er et certifikat, der kan anvendes til at logge sig på systemer og generere digital signatur på epost, men det kan ikke anvendes til kryptering. Dette certifikat placeres lokalt sammen med den tilhørende private nøgle hos den enkelte medarbejder på dennes PC som en standard software signatur eller i en HW-token (USB eller smartcard).

Det andet certifikat udstedes, så det udelukkende kan anvendes til kryptering og ikke til signering. Dette certifikat placeres centralt i organisationen sammen med den tilhørende private nøgle uden for den enkelte medarbejders kontrol. Da disse "kolde" krypteringscertifikater (og især de tilhørende private nøgler) således ikke kommer til medarbejdernes kendskab, anvendes samme nøgle til alle medarbejdere. Krypteringscertifikaterne placeres i et offentligt tilgængelig directory.

Når en person udenfor virksomheden vil sende direkte til en medarbejder, fremsøges medarbejderens krypteringscertifikat som vanligt, eposten krypteres direkte til medarbejderen, og eposten afsendes. Når den krypterede epost modtages af virksomhedens centrale epostapplikation (som har adgang til den private RSA nøgle til dekryptering), dekrypteres eposten, inden den sendes ukrypteret videre internt i virksomheden.

Når en medarbejder ønsker at sende til en person udenfor virksomheden, kan signering påsættes lokalt, og kryptering kan foretages centralt.

Spærring og fornyelse håndteres parallelt med signeringscertifikater i stil med, hvordan det håndteres i øvrige to-nøglepar løsninger.

2.3.4 Noark

FESD-standardisering har normalt Noark 4 standarden som udgangspunkt På området vedrørende digital signatur, har Noark et andet udgangspunkt end denne standard. Det har derfor ikke været muligt at anvende Noark som grundlag for denne standard.

Noark opererer ikke med en opdeling mellem et ESDH-system og en sikker epostløsning, og de grænseflader, der er i en sådan løsning. Noark arbejder i stedet med en model, hvor ESDH-systemet lagrer signaturer i ESDH-systemets database.

I Noarks datamodel er der defineret en tabel ’DIGISIGN’ digitale signaturer. Denne tabel bliver ikke inkluderet i FESD-datamodellen, men erstattes af de datamodelsudvidelser, der defineres som følge af denne standard.

2.3.5 Afgræsninger

2.3.5.1 S/MIME

Denne standard vedrører kun håndtering af S/MIME-mail.

2.3.5.2 Registrering af afsender- og modtageroplysninger.

Standarden forholder sig ikke til selve dokumentregistreringen i ESDH-systemet. Der tilvejebringes en række informationer, som kan benyttes i forbindelse med registreringen, men myndigheden vil fortsat skulle sikre en forsvarlig registrering af dokumenter, herunder at på- og/eller tilføre de almindelige afsender-/modtageroplysninger.

2.4 Sikkerhed

I forbindelse med udarbejdelsen af denne standard har der været stor fokus på at finde det rigtige niveau for sikkerheden i de løsninger, der bygger på standarden. Sikkerheden har specielt været koncentreret om 3 områder:

1. Bevisværdi – hvis en myndighed har implementeret standarden, skal det sikre bevisværdien i forbindelse med myndighedens epost kommunikation.

2. Eksterne parter: Som følge af pkt. 1 skal det kunne godtgøres, at ingen uden for myndigheden har en teoretisk mulighed for at registrere epost i ESDH-systemet med falske autenticitets informationer.
3. Oplysninger, der er fortrolige, skal være beskyttet også mod, at en medarbejder uforvarende kommer til at videregive dem.

2.4.1 Bevisværdi

ESDH-systemet har traditionelt set ikke nogen rolle i en epost/brevudveksling, idet ESDH-systemets primære rolle har bestået i at være lager for indholdet af den kommunikation - og dernæst oplysningerne omkring kommunikationen.

Når det gælder udveksling af dokumenter mellem offentlige myndigheder ved hjælp af ikke elektronisk post, indeholder ESDH-systemet typisk brevet eller rettere en indskannet kopi af brevet. Hvis der opstår tvist om, hvorvidt en myndighed har modtaget et brev fra en modtager, vil myndigheden i ESDH-systemet kunne dokumentere modtagelsen ved at kunne producere en kopi af brevet (evt. med en håndskrevet underskift) og de hertil knyttede metadata, såsom modtagelsestidspunkt og identifikation af hvem, der har foretaget skanningen og registreringen af brevet. Bevisværdien opnås ved at underbygge denne dokumentation med de it-sikkerhedsmæssige procedurer i organisationen og vil i en tvist kunne sandsynliggøre, hvilken kommunikation, der har fundet sted.

Sikkerheden, når det gælder bevislighed af epost kommunikation, skal som minimum være på højde med den, der gælder for den øvrige brevudveksling. Dvs. at der skal registreres oplysninger i ESDH-systemet, der kan sandsynliggøre hvilken kommunikation, der har fundet sted, men bevisværdien vil altid tillige være baseret på myndighedens it-sikkerhedsmæssige procedurer og dokumentationen for, at disse bliver overholdt.

2.4.2 Eksterne parter

Det må ikke kunne lade sig gøre, at en part uden for organisationen kan fremsende epost, der bliver registreret i ESDH-systemet, som om de var troværdige uden at være det. Løsningen bygger på, at oplysningerne fra certifikaterne bliver ekstraheret og registreret som metadata i ESDH-systemet. Standarden skal sikre, at en ekstern part, der kender myndighedens opsætning og kender de interne dataformater for udveksling i løsningen, ikke kan levere data, der bliver registreret med en falsk autenticitet i ESDH-systemet.

2.4.3 Beskyttelse af fortrolige oplysninger

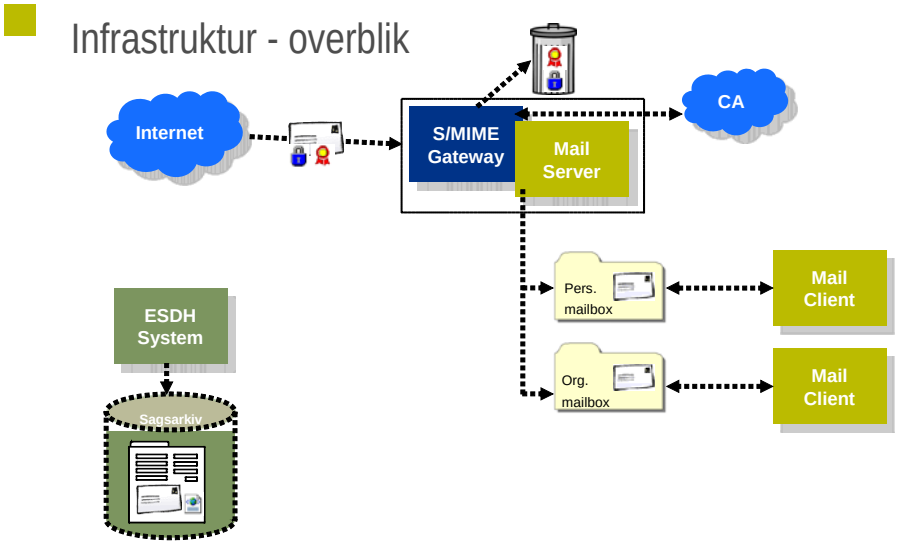
Håndtering af smime-epost involverer kryptering og dekryptering af informationer der under fremsendelsen er beskyttet mod, at udenforstående kan se dem. De grænseflader, der er mellem sikker epostløsningen, må ikke kompromittere denne sikkerhed.

3 DEL B

3.1 Infrastruktur i organisationen

ESDH-systemer kan have funktionalitet indbygget til at håndtere sikker epost, men det er ikke ESDH-systemets opgave at håndtere al epost, der sendes til eller fra organisationen.

Forretningslogikken vedrørende styring af certifikater, opslag i spærrelister mv. er ikke en naturlig del af ESDH-systemet, men en del af organisations mere basale infrastruktur og skal derfor ikke være en del af organisationens ESDH-løsning.



Figur 1: Overblik over infrastruktur

Figur 1 viser forudsætningerne for infrastrukturen i organisationen. Det forudsættes, at der er en sikker epostløsning, der implementerer en S/MIME-Gateway. S/MIME Gateway'en har ansvaret for at modtage og afsende S/MIME mails, således at den fysiske kryptering og signering fjernes fra mails, inden de kommer ind i organisationen – det er illustreret med skaldespanden øverst. De løsninger, der findes på markedet i dag, er meget forskellige, hvad angår deres integration til organisationens øvrige epost servere. Nogle gateway's er selvstændige servere, der har en klar grænseflade til en epost server, mens andre er en udbygning af epost serverens funktionalitet. Standarden antager ikke noget om, hvordan grænsefladen mellem epost serveren og gatewayen er, men antager blot, at det samlede epostsystems funktionalitet er udvidet med S/MIME håndtering.

Indgående epost kan enten være direkte til sagsbehandlere eller til virksomhedens generelle epostkasse. Arbejdet med epost sker via epostklienter, og der vil typisk være en hel del epost, der ikke skal registreres i ESDH-systemet. Standarden tager derfor udgangspunkt i, at der i organisationen findes en sikker epostløsning, og at der er et tillidsforhold mellem sikker epostløsningen og ESDH-systemet, således at:

- Epost, der er verificeret af sikker epostløsningen, ikke behøver at blive genverificeret af ESDH-systemet
- ESDH-systemet kan bestille sikker epostløsningen til at signere udgående epost ved at anvende f.eks. virksomheds certifikater

3.2 Brugsscenarier

De brugsscenarier, standarden fokuserer på, er dem, der udspringer af sikker epost kommunikation mellem en medarbejder i en organisation og en for organisationen ekstern part. Den eksterne part kan i princippet være medarbejder i en anden organisation, men fokus er ikke på epost udveksling mellem to organisationer. Standarden håndterer således ikke scenarier med epost krypteret i en End-to-End S/MIME løsning, hvor modtageren selv har dekrypteringsnøglen, og hvor epost således ikke dekrypteres af S/MIME gateway'en.

Epost kommunikationen vil typisk være initieret af den eksterne part – f.eks. i en situation, hvor en borger henvender sig til en myndighed for at ansøge om en tilladelse, et tilskud eller lignende – men kommunikationen kan også være initialiseret af en medarbejder i organisationen, som f.eks. ved en nabohøring.

I de næste afsnit beskrives, hvordan ind- og udgående epost kommunikation skal håndteres generelt – i del C beskrives den konkrete informationsarkitektur og krav til henholdsvis ESDH og sikker epostløsning.

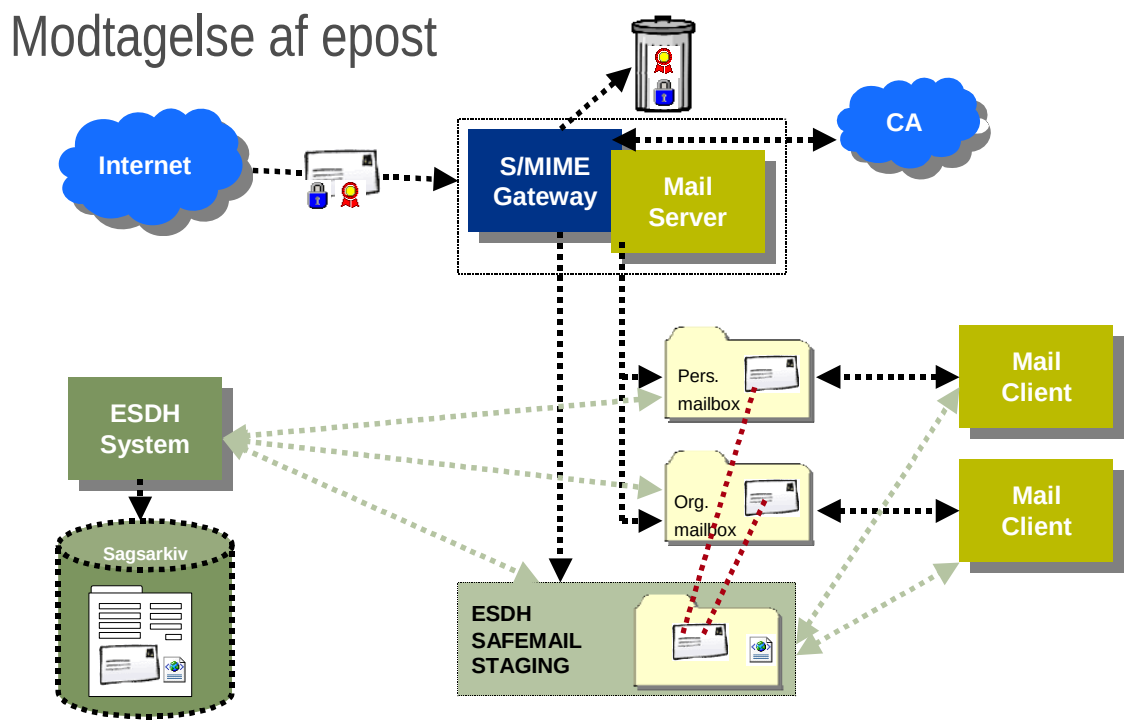
3.2.1 Modtagelse af epost i organisationen

3.2.1.1 Case

Den eksterne part har enten kendskab til epostadressen (og certifikat) på organisationens generelle epostkasse eller har kendskab til en konkret medarbejders epostadresse (og certifikat), således at parten kan danne en epost, der er krypteret og/eller signeret og fremsende den til epostadressen.

I organisationen modtages eposten enten direkte af en medarbejder eller i den centrale epostkasse og videre-fordeles til en medarbejder, der skal behandle eposten. Indholdet af eposten registreres herefter i ESDH-systemet sammen med oplysninger om kommunikationen. Medarbejderen kan så initiere en ny eller fortsætte en igangværende sagsbehandling på baggrund af indholdet.

3.2.1.2 Løsningsscenarie



Figur 2: Modtagelse af epost

Figur 2 viser, hvordan en epost bliver modtaget i organisationen. Første led er S/MIME Gatewayen (1) (sikker epostløsningen), der opfattes som en udvidelse af epost serverens funktionalitet.

Gateway'en behandler indgående epost, der er S/MIME encoded – dvs. epost, der er krypteret, signeret eller begge dele. Gateway'en behandler S/MIME-mails ved at verificere, at de er korrekte. Dvs. at en vedhæftet signatur er relateret til indholdet af eposten, og at certifikater, der er anvendt, er valide, og der indhentes evt. ekstra oplysninger om indehaveren.

Gateway'en danner et indgående signaturbevis, der indeholder oplysninger om signatur, certifikat og certifikatholderen samt nogle forsendelsesoplysninger. Det indgående signaturbevis er nærmere beskrevet i Del C.

Gateway'en fjerner det certifikat, der er påført eposten ved modtagelsen, og dekrypterer eposten, såfremt den er krypteret med virksomhedscertifikatets nøgle. Hvis eposten er krypteret med en anden nøgle, kan gateway'en ikke behandle eposten, og opfatter dette som en fejlsituation (hvis virksomheden anvender "medarbejdersignatur avanceret", vil det være virksomhedscertifikatets offentlige krypteringsnøgle, der ligger i de enkelte medarbejdercertifikater, og dermed vil det være muligt for gatewayen at dekryptere en mail, der er krypteret til en specifik medarbejder).

Gateway'en danner endvidere en ny unik id i form af en UUID, der tilføjes epostens mailheader.

Gateway'en videresender to kopier af eposten :

1. Direkte til modtageren (2). Hvad enten det er en personlig epostkasse (2-1) eller en virksomhedsepostkasse (2-2), fremsendes en kopi af eposten direkte. Denne kopi af mailen skal behandles af brugeren i den mailklient, som brugeren anvender. Gatewayen kan derfor ikke stille specielle krav til mailklienten

2. Til ESDH-systemets postkasse (3) fremsendes en kopi af eposten, der har vedhæftet det dannede signaturbevis.

De to eposter knyttes til hinanden ved hjælp af nogle ekstra metadata, der tilføjes til MIME-headeren, der indeholder den unikke ID, gateway'en har tildelt.

Modtagelse af eposten (4) sker i modtagerens indbakke – hvad enten modtageren er en medarbejder eller en virksomhedspostkasse. Den version af eposten, der ses i mailklienten, er ikke tilknyttet et signaturbevis, og brugeren kan altså frit besvare eller videresende denne epost uden at skulle fjerne et tilknyttet signaturbevis. Dermed er risikoen for, at brugeren uforvarende kommer til at videresende et signaturbevis med afsenderens CPR-nummer, minimeret.

ESDH-systemets postkasse (ESDH Safemail staging på figur 2) er en særlig postkasse (3), der er oprettet til integrationen. Denne postkasse skal opsættes, så kun MailGateway'en og ESDH-systemet har adgang til den. Denne sikkerhedsopsætning er central for sikkerheden i løsningen, idet den sikrer, at der ikke kan lagres forvanskede data i ESDH-systemet. Hvordan denne opsætning skal foretages, afhænger af sikker epost-løsningen og ESDH-systemet.

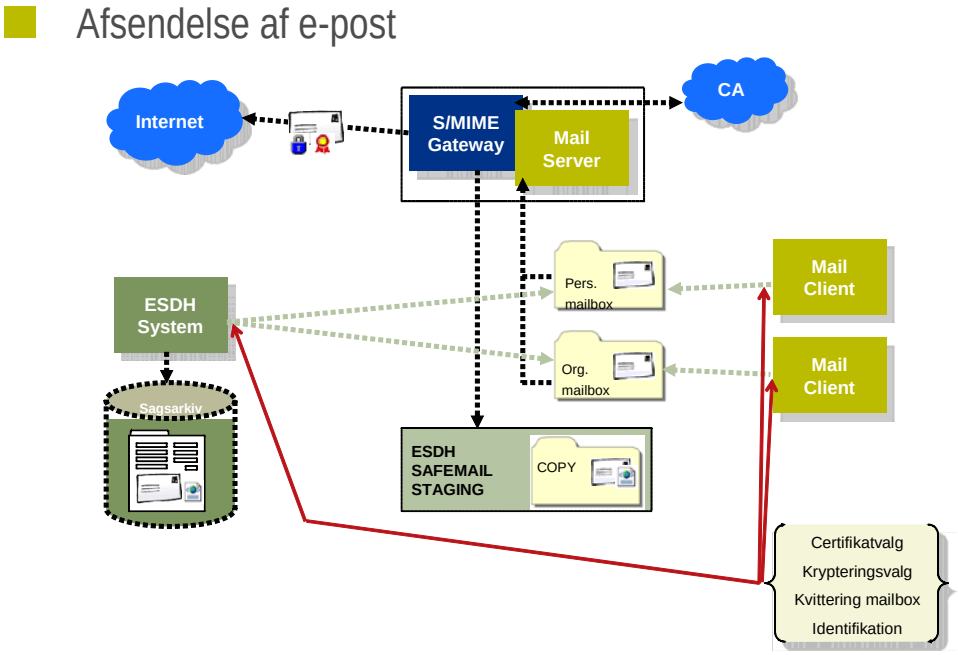
ESDH-systemets funktionalitet omfatter en integration med postklienten, der giver mulighed for at arkivere epost i ESDH-systemet. Når epost gemmes i ESDH-systemet (5), undersøger logikken, om der eksisterer en kopi af eposten i "safemail staging postkassen". Hvis der findes en sådan kopi, er det denne (og ikke eposten i brugerens indbakke), der arkiveres i ESDH-systemet. Når eposten gemmes i ESDH-systemet, er det i form af en journalpost med tilknyttede dokumenter. Journalposten tilknyttes endvidere et signaturbevis, der er en tabel i ESDH-systemets datamodel (en udvidelse til FESD-datamodellen). Denne funktionalitet kan være implementeret på forskellig vis i de forskellige ESDH-systemer og epostklienter.

3.2.2 Afsendelse af epost

3.2.2.1 Case

Medarbejderen har i forbindelse med en sagsbehandling behov for kommunikation med en ekstern part. Medarbejderen kender eller får kendskab til partens epost-adresse, certifikat og seneste kommunikation med organisationen for at afgøre, hvordan parten skal kontaktes. Medarbejderen danner en epost og anvender organisationens certifikat til at sikre kommunikation og autenticitet. Efter afsendelse registreres i ESDH-systemet, at eposten er afsendt, ligesom der registreres informationer om, hvordan epost afsendelsen er sket.

3.2.2.2 Løsningsscenarie



Figur 3: Afsendelse af epost

Afsendelsen af epost foregår fra epostklienten (1). Epostklienten beriges med noget afsendelses funktionalitet, som gør det muligt for brugeren at vælge, om eposten skal signeres med et virksomhedscertifikat og/ eller krypteres (2). I organisationer med flere virksomhedscertifikater, kan det endvidere være hensigtsmæssigt, at medarbejderen kan vælge hvilket virksomhedscertifikat, der skal avendes til signeringen.

Denne afsendelses funktionalitet leveres i dag normalt af samme leverandør, som leverer sikker epostløsningen (typisk i form af en 'Send sikkert'-knap i epostklienten), men kunne også leveres med ESDH-systemet eller af en tredje parts leverandør. Standarden beskæftiger sig ikke med, hvordan eller af hvem funktionaliteten er udviklet, men beskriver udelukkende grænsefladen mellem epostklienten og sikker epostløsningen.

Grænsefladen, som konkretiseres i DEL C, indbefatter, at den epost, der videresendes fra epost klienten til sikker epostløsningen (3), forsynes med op til fire ekstra oplysninger (header oplysninger eller evt. udvidelse af subjectfeltet):

1. Certifikat der skal anvendes til signering.
2. Kryptering – skal kryptering foretages?
3. Epostadresse på ESDH-systemets 'Safemail staging'-epostkasse.
4. En frivillig identifikatorstreng, der identificerer eposten overfor ESDH-systemet.

Hvis medarbejderen vælger at signere eposten direkte i epostklienten med medarbejderdelen af "medarbejdersignatur avanceret", udelades oplysningen vedrørende certifikat.

Gatewayen agerer på udgående epost, der har tilknyttet de ekstra oplysninger, således at :

- Epost, der har certifikat-oplysningen, bliver signeret med det pågældende certifikat, og at afsenderadressen på eposten ændres fra medarbejderens til virksomhedens.
- Epost, der har krypterings-oplysningen (true), bliver krypteret med modtagerens certifikat.

- Epost der har ESDH-epostkasse-oplysningen behandles ved, at der
    - Dannes en udgående følgeseddel
    - Dannes en kopi af eposten
    - Fremsendes en kopi med følgesedlen tilknyttet til ESDH-systemets 'Safemail staging'-epostkasse (4).
- Epost der har en identifikatorstrengs-oplysning får identifikatorstrengen indsat i den udgående følgeseddel, såfremt der også er tilknyttet en ESDH-epostkasse-oplysning.

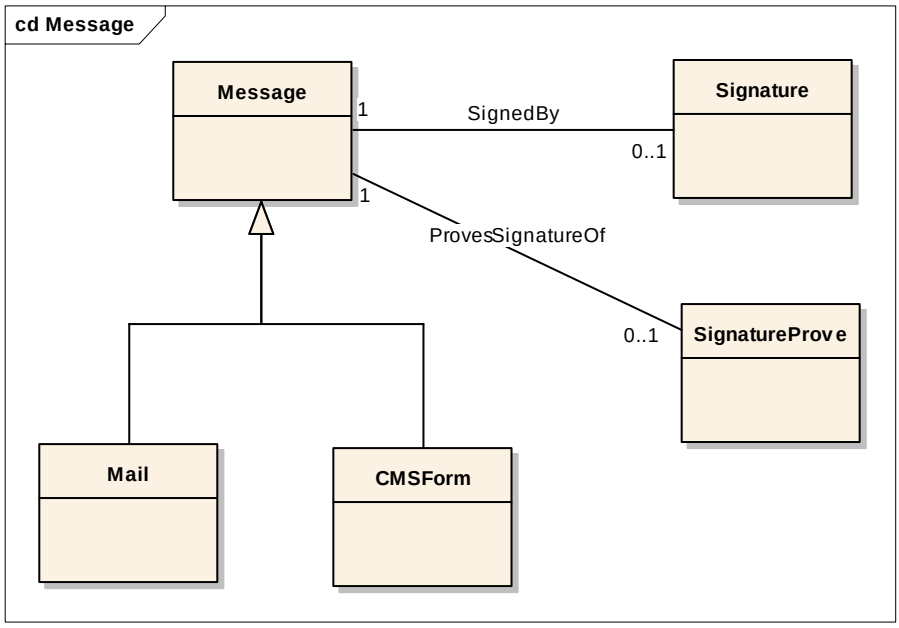
Når medarbejderen har afsendt eposten, vil der med en tidsforsinkelse blive sendt en kopi af eposten til ESDH-systemets safemail staging epostkasse, såfremt Gateway'en kan verificere modtageren og foretage en korrekt afsendelse af eposten.

Medarbejderen kan nu arkivere eposten i ESDH-systemet fra epost klienten vha. ESDH-systemets epostintegration (5). Medarbejderen kan genfinde eposten i folderen med afsendte epost og vælge at gemme den i ESDH-systemet. ESDH-systemets epostintegration genkender epost, der har påført ESDH-epostkasse-oplysningen og tillader, at disse lagres i ESDH-systemet, når der er modtaget en kopi af eposten i ESDH-epostkassen – og som ved indgående post er det kopien fra ESDH-epostkassen, der gemmes i ESDH-systemets arkiv.

4 DEL C

4.1 Logisk model

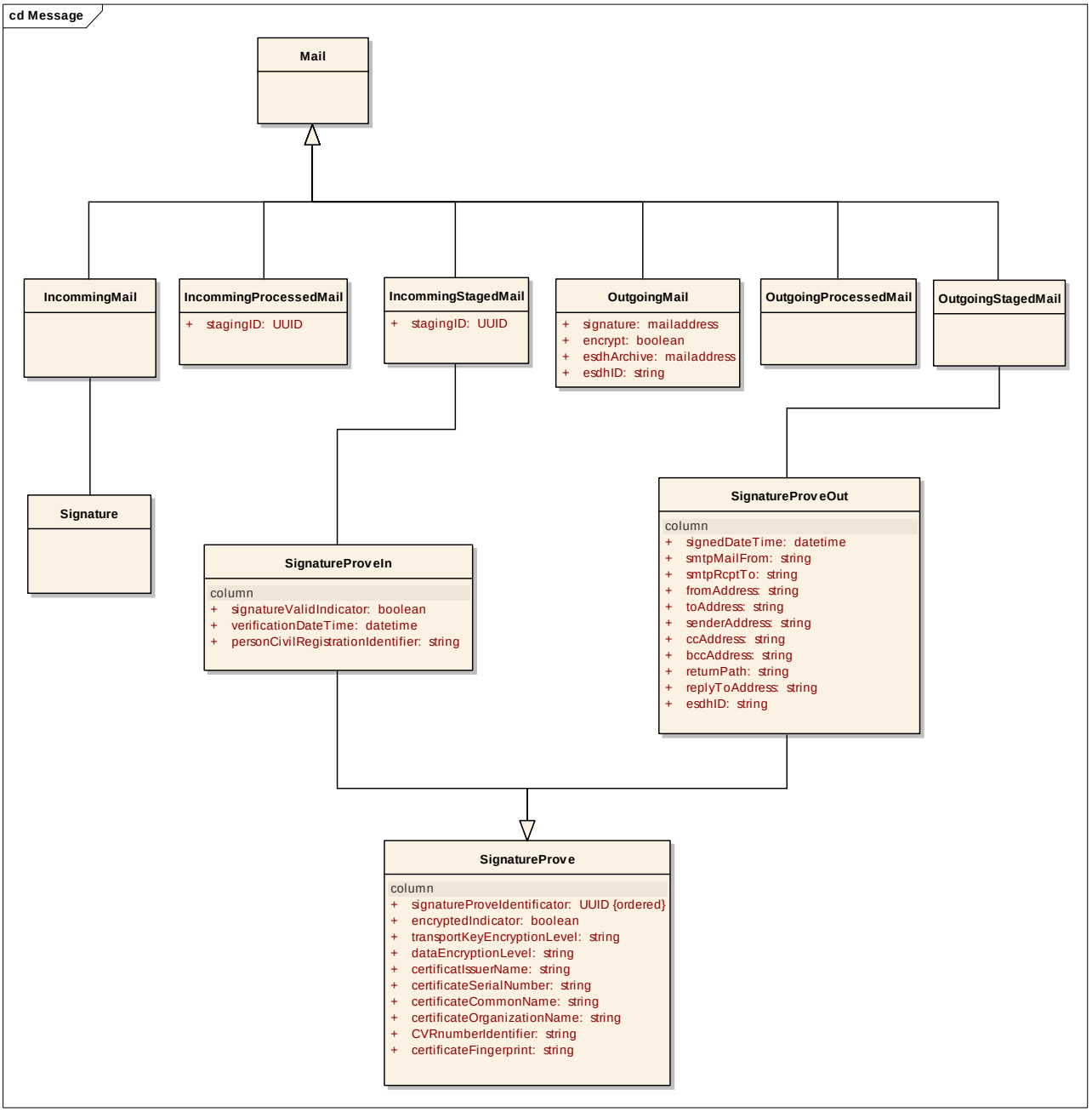
4.1.1 Epost Message



Figur 4

En ’Message’ er et generelt begreb for meddelelser, der kan sendes til et ESDH-system. Denne standard omfatter kun epost, men på et senere tidspunkt kan standarden revideres, så andre typer af meddelelser også understøttes. På klassediagrammet er vist en CMSForm som eksempel på en udvidelse.

En Message kan være signeret med en digital signatur, og en løsning kan evt. have verificeret signaturen og erstattet signaturen med (eller blot tilføjet) et signaturbevis. Signaturbeviset indeholder oplysninger i XML-format, der beskriver, hvordan eposten er signeret.


cd Message
Mail
IncommingMail
IncommingProcessedMail
+ stagingID: UUID
IncommingStagedMail
+ stagingID: UUID
OutgoingMail
+ signature: mailaddress
+ encrypt: boolean
+ esdhArchive: mailaddress
+ esdhID: string
OutgoingProcessedMail
OutgoingStagedMail
Signature
SignatureProveIn
column
+ signatureValidIndicator: boolean
+ verificationDateTime: datetime
+ personCivilRegistrationIdentifier: string
SignatureProveOut
column
+ signedDateTime: datetime
+ smtpMailFrom: string
+ smtpRcptTo: string
+ fromAddress: string
+ toAddress: string
+ senderAddress: string
+ ccAddress: string
+ bccAddress: string
+ returnPath: string
+ replyToAddress: string
+ esdhID: string
SignatureProve
column
+ signatureProveIdentificator: UUID {ordered}
+ encryptedIndicator: boolean
+ transportKeyEncryptionLevel: string
+ dataEncryptionLevel: string
+ certificatIssuerName: string
+ certificateSerialNumber: string
+ certificateCommonName: string
+ certificateOrganizationName: string
+ CVRnumberIdentifier: string
+ certificateFingerprint: string

Figur 5

4.1.2 Signaturbevis

4.1.2.1 Generelt for ind- og udgående signaturbevis

Klassen indeholder attributter, som skal været tilstede i både ind- og udgående signaturbeviser.

Attribut **Dan**	**Attribut** **Eng**	**Type**	**Kardinalitet**	**Beskrivelse**	**Mapning til NOARK4**
krypteret	encryptedIndicator	boolean	[1]	Tekst der angiver, om en modtagen epost meddelelse har været krypteret eller ej.	
transportNøgleKrypteringsNiveau	transportKeyEncryptionLevel	char(255)	[1]	Indeholder information om den modtagne eller afsendte meddelelses transportnøglekrypteringsniveau. Anvendes til at angive hvilken krypteringsalgoritme og hvilken nøglelængde, der er anvendt. F.eks. RSA 1024 bit.	
dataKrypteringsNiveau	dataEncryptionLevel	char(255)	[1]	Indeholder information om den modtagne eller afsendte meddelelses datakrypteringsniveau. Anvendes til at angive hvilken krypteringsalgoritme og hvilken nøglelægde, der er anvendt. F.eks. 3DES 168 bit.	
certifikatUdsteder	certificateIssuerName	char(50)	[1]	Indeholder information om hvem der er udsteder af den digitale signatur. Anvendes til at angive udstederen (certificeringscentret) af den digitale signatur. Tekst, der angiver udstederen af et givent certifikat, og som direkte kan tages fra certifikatfeltet ”Udsteder” eller ”Issuer”. F.eks.: TDC OCES CA, TDC, DK	

Attribut Dan	Attribut Eng	Type	Kardinalitet	Beskrivelse	Mapning til NOARK4
certifikatSerieNummer	certificateSerialNumber	char(60)	[1]	Indeholder information om certifikatets serienummer. Anvendes til at angive serienummeret i certifikatet. Entydigt felt i certifikatet, som indeholder forskellige oplysninger, alt afhængig hvilken certifikattype, der bruges. **For personcertifikater** Kvalifikator PID: konkateneret med løbenummer. Se DS 843-1 Personspecifikke identifikationsnumre (PID). **For medarbejdercertifikater** CVR:cvrnummer-RID:medarbejderId. **For virksomhedscertifikater** Kvalifikator CVR:konkateneret med cvrnummer og evt. en af følgende kvalifikatorer:UID:, SE:, P: konkateneret med et ID, se DS 844, pkt. 6.1 Eksempler: serialNumber= PID:9208-2001-3-279815395,serialNumber=CVR:12345678-RID:medarbejderId serialNumber=CVR:12345678-UID:Skatteforvaltningen	

Attribut Dan	Attribut Eng	Type	Kardinalitet	Beskrivelse	Mapning til NOARK4
certifikatAnvenderNavn	certificateCommonName	char(50)	[1]	Anvendes til at angive CommonName-feltet i certifikatet. Entydigt felt i certifikatet, som indeholder forskellige oplysninger, alt afhængig hvilken certifikattype, der anvendes. Personens fulde navn eller pseudonym. Medarbejderens fulde navn eller registrerede pseudonym, evt. inkl. Titel. Certifikatindehaverens navn plus evt anden tekststreng adskilt af ”-” Eksempler: commonName= Test Testesen commonName= Projektleder Jens Madsen, commonName=Virksomhed A/S-tekststreng	

Attribut Dan	Attribut Eng	Type	Kardinali-tet	Beskrivelse	Mapning til NOARK4
certifikatOrganisationNavn	certificateOrganizationName	char(50)	[0..1]	Anvendes til at angive Organisationsfeltet i certifikatet. Entydigt felt i certifikatet, som indeholder forskellige oplysninger alt afhængig hvilken certifikattype, der anvendes. "Ingen organisatorisk tilknytning". Virksomhedens fulde navn, evt. inkl. CVR-nummer.	
certifikatOrganisationEnhedNavn	certificateOrganizationUnit-Name	char(50)	[0..1]	Navn på den organisatoriske enhed.	
cvrNr	CVRnumberidentifier	int(8)	[0..1]	Indeholder CVR-nr. (Kun relevant ved medarbejder- og virksomhedscertifikater). Indeholder CVR-nr. Anvendes til at angive CVR-nummeret i certifikatet (kun relevant ved medarbejder- og virksomhedscertifikater). Xxxxxxxx - f.eks.12345678.	

Attribut Dan	Attribut Eng	Type	Kardinali-tet	Beskrivelse	Mapning til NOARK4
certifikatFingeraftryk	certificateFingerprint	char(255)	[0..1]	Anvendes til at angive certifikatets fingerprint, som er en ”digest” (en hashfunktion) af cerftifikatet i X.509 binært format. Den kan udregnes ved hjælp af forskellige algoritmer, f.eks. SHA1 (Internet Explorer) eller MD5 for andre browsere Xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx F.eks i SHA1: 78:e9:dd:06:50:62:4d:b9:cb:36:b5:07:67:f2:09:b8:43:be:15:b3	

De konkrete krav for indholdet af nogle af felterne er uddybet i certifikatpolitikkerne på www.signatursekretariatet.dk

4.1.2.2 Specifikt for indgående signaturbevis

Klassen indeholder attributter, som skal været tilstede ved indgående signaturbeviser.

Attribut **Dan**	**Attribut** **Eng**	**Type**	**Kardinalitet**	**Beskrivelse**	**Mapning til NOARK4**
signaturGyldig	signatureValidIndicator	boolean	[1]	Indeholder information om en signeret meddelelses digitale signatur er gyldig eller ej. Tekst der angiver, om en digital signatur på en modtaget sikker epost er gyldig eller ej.	
verificeringsDatoTidspunkt	verificationDateTime	datetime	[1]	Indeholder information om tidspunktet for verificering af den digitale signatur. Dato der angiver, hvornår den digitale signatur er blevet valideret. F.eks. Mon, 6 Oct 2005 14:07:35 +0200 (CEST),	
cprNr	personCivilRegistrationIdentifier	int(10)	[0..1]	Anvendes til at angive CPR-nr. Entydigt nummer.	

4.1.2.3 Specifikt for udgående signaturbevis

Klassen indeholder attributter, som skal være tilstede ved udgående signaturbeviser.

Attribut **Dan**	**Attribut** **Eng**	**Type**	**Kardinalitet**	**Beskrivelse**	**Mapning til NOARK4**
signeringsDatoTidspunkt	signatureDateTime	datetime	[1]	Indeholder information om, hvornår den afsendte meddelelse er blevet signeret. Anvendes til at angive tidspunktet for signeringen af den afsendte epost meddelelse. F.eks. Mon, 6 Oct 2005 14:07:35 +0200 (CEST).	
smtpEpostFra	smtpMailFrom	char(255)	[1]	Indeholder informationer, som SMTP-serveren har behov for at vide. Anvendes til at angive til SMTP-serveren, at der starter en ny e-mail transaktion- MAIL FROM er det første skridt i en MAIL kommando. MAIL FROM:<reverse-path> [SP <mail-parameters>] <CRLF> f.eks. MAIL FROM:<userx@y.foo.org> De konkrete krav til formatet kan findes i RFC 2821.	

Attribut Dan	Attribut Eng	Type	Kardinalitet	Beskrivelse	Mapning til NOARK4
smtpRcptTil	smtpRcptTo	char(255)	[1]	Indeholder informationer, som SMTP-serveren har behov for at vide. Anvendes til at angive en ”forward-path” (recipient RCPT TO er det andet skridt i en MAIL kommando RCPT TO:<forward-path> [SP <rcpt-parameters>] <CRLF> f.eks.: RCPT TO:<@hosta.int,@jkl.org:userc@d.bar.org> De konkrete krav til formatet kan findes i RFC 2821.	
fraAdresse	fromAddress	char(255)	[1]	Indeholder information om, hvem epost meddelelsen kommer fra. Anvendes til at angive ”Fra”-headeren i en epost meddelelse. ”Fra”-headeren er specificeret i RFC 2822.	
tilAdresse	toAddress	char(255)	[1]	Se ovenfor	
afsenderAdresse	senderAddress	char(255)	[1]	Se ovenfor	
ccAdresser	ccAddresses	char(255)	[1]	Se ovenfor	
bccAdresser	bccAddresses	char(255)	[1]	Se ovenfor	
returSti	returnPath	char(255)	[1]	Se ovenfor	
svarTilAdresse	replyToAddress	char(255)	[1]	Se ovenfor	
elementIdentifikatorStreng	itemIdentificatorString	char(255)	[1]	Indeholder den ID-streng, som er vedhæftet udgående mail (svarer til X-ESDH-ID i den udgående mail). Kan anvendes af ESDH-systemet til at påhæfte ekstra ID-oplysninger ved en forregisterring af mailen, som kan genfindes i kvitteringsmailens tilknyttede signaturbevis. Ingen krav til syntaks af strengen. Kan defineres af det enkelte ESDH-system.	

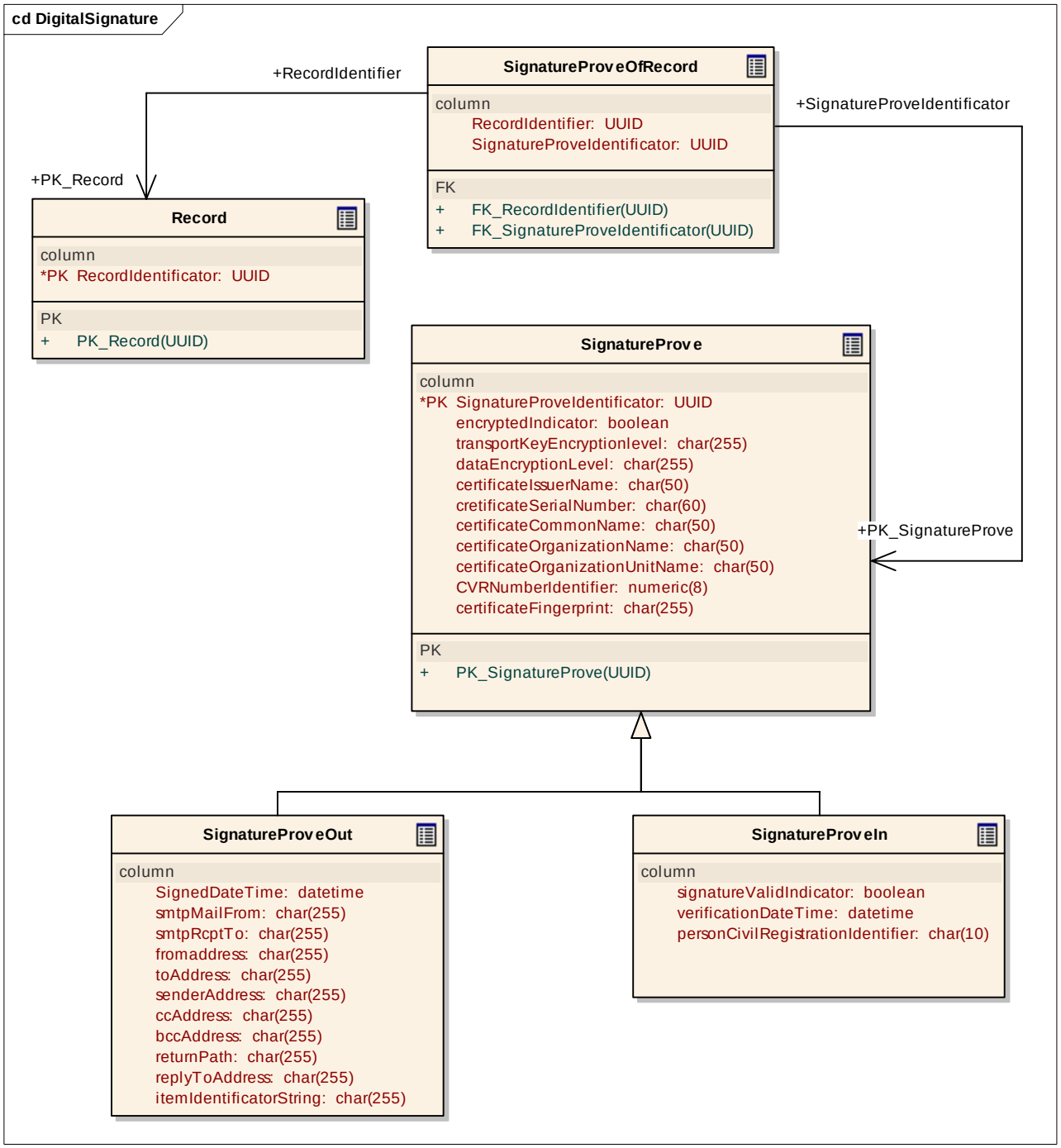
4.1.3 Epost headere for udgående epost

Ved afsendelse af epost anvendes følgende mimeheadere til at markere og kommunikere med S/MIME-gateway'en:

- X-Sign: Signering [certifikatnavn] (bruges kun til virksomhedscertifikat)
- X-Encrypt: Kryptering Boolean
- X-Archive: ESDH Arkiv [epostkasse]
- X-ESDH-ID: ID, der videreføres til ESDH-systemet.

Da ikke alle epostklienter tillader programmatisk adgang til mimeheadere, bør sikker epostløsningerne tilbyde en metode til at encode oplysningerne ind i subjectfelterne.

4.2 Udvidelse af FESD-datamodel



Figur 6

Registrering af sikkerheden via forsendelser foretages i 2 nye tabeller, der navngives:

- SignatureproveIn
- SignatureproveOut

Tabellerne indeholder oplysningerne fra de ind- og udgående signaturbeviser med retningsangivelse.

Derudover udvides datamodellen med en relationstabel:

- signatureProveOfRecord

mellem record og Signatureprove-tabellen, således at journalposter, der repræsenterer en sikker email, kan tilknyttes et signaturbevis.

Udvidelsen giver således mulighed for, at der på et senere tidspunkt kan tilknyttes signaturbeviser til andre entiteter i datamodellen (f.eks. dokumenter, der repræsenterer formularer fra et CMS-system).

Denne udvidelse indarbejdes ved næste konsolidering af FESD-datamodellen.

Grundet drøftelse mellem ITST og KL om anvendelse af dansk eller engelsk sprog i XML-skemaer er disse ikke medtaget i standarden. Udformning af XML-skemaer vil blive gennemført på et senere tidspunkt og vil efter godkendelse blive publiceret.