Sikkerhet i EDIFACT- meldingen - MEDRUC
Oppgjørskrav til Rikstrygdeverket

Signatur og krypteringsløsning

Teknisk beskrivelse

Sertifikater og Tiltrodde Tredje Part

Versjon 1.3
Mai 2004

Rikstrygdeverket

INNHOLDSFORTEGNELSE

1. INNLEDNING 3

2. SIKKERHETSPROFIL FOR MEDRUC 3

2.1 OVERORDNET PROSEDYREBESKRIVELSE 3
2.1.1 Avsender (Sykehus/Poliklinikk/Laboratorium/Apotek/Ortopedisk verksted) 3
2.1.2 Mottaker (RTV) 4
2.2 IMPLEMENTASJON FOR INKLUDERING AV DIGITAL SIGNATUR 4
2.2.1 Funksjonsbeskrivelse 4
2.2.2 Notasjon 5
2.2.3 Meldingsoversikt "signaturforsterket" MEDRUC 5
2.2.4 Segmentdiagram 6
2.2.5 Segmentspesifikasjon 6
UST – Sikkerhetshale 8
USR – Sikkerhetsresultat 8
2.2.6 Eksempler på signaturforsterket MEDRUC-melding 8
2.2.6.1 Eksempel 1 8
2.2.6.2 Eksempel 2 9
2.2.6.3 Eksempel 3 (Utgår) ..... **Feil! Bokmerke er ikke definert.**
2.3 KRAV TIL SIKKERHET I SIGNATURPROSESSEN 10
2.3.1 Maskin/programvare 10
2.4 IMPLEMENTASJON AV KRYPTERING (CIPHER) 10
2.4.1 Funksjonsbeskrivelse 10
2.4.2 Meldingsoversikt CIPHER 10
2.4.3 Segmentdiagram 11
2.4.4 Segmentspesifikasjon 11
2.4.5 Eksempel på CIPHER-melding med mottakers offentlige nøkkel fra sertifikat utstedt av RTV CA (Utgår) 14
2.4.6 Eksempel på CIPHER-melding med mottakers offentlige nøkkel fra sertifikat utstedt av Posten SDS CA ***Feil! Bokmerke er ikke definert.***
*2.4.7 Forklaring til eksempelet ..... **Feil! Bokmerke er ikke definert.***

3. SERTIFIKATER OG NØKLER 14

3.1 DAGENS SERTIFIKATER / TTP 14
3.2 VISING AV SERTIFIKATINFORMASJON 14
3.2.1 Listing av sertifikat lagret i pem-format vha OPENSSL 14
3.2.2 Listing av sertifikat lagret i DER-format vha OPENSSL 15
3.3 KOBLING MELLOM KONTROLLPROGRAM OG SERTIFIKAT 17

Versjonshistorie

Versjon 1.0	15.08.1998	Første versjon.
Versjon 1.1	21.01.2000	Retting av feil på element 0516 i USH, endring av lengde på element 0511 fra 17 til 256 tegn, samt diverse utdypinger.
Versjon 1.2	03.02.2000	Rettet feil på initialiseringsvektor, samt feil i USB-segmentet (elementverdi "X"). Rettet eksempel i punkt 2.4.5 og forklarende tekst i punkt 2.4.6. Lagt til eksempel på MEDRUC-melding.
Versjon 1.3	09.05.2004	

1. Innledning

Dette dokumentet inneholder en beskrivelse av sikkerheten i den EDIFACT baserte meldingen MEDRUC, som brukes ved forsendelse av oppgjørskrav til Rikstrygdeverket. Implementeringen av løsningen er laget i henhold til KITH's spesifikasjoner i "Håndbok for sikkerhet i EDIFACT-baserte meldinger MEDRPT/MEDPRE/LEGOPP" endelig versjon av 4. oktober 1995.

2. Sikkerhetsprofil for MEDRUC

Normkravene forutsetter følgende:

- Det er kun hele oppgjørskravet som skal signeres av en eller flere ansvarlige for den aktuelle institusjon/firma. Dette kan f.eks. være økonomi/regnskaps-personer.
- Hver enkelt melding eller utveksling (avhengig av hva som skal inkluderes i en enkelt X.400-meldingskropp for sending til en gitt mottaker) skal krypteres. Dette innebærer at dersom flere meldinger settes sammen til en utveksling før denne inkluderes i en X.400-meldingskropp og sendes til mottaker, skal utvekslingen og ikke hver enkelt melding krypteres.
- Sikkerhetstjenestene kan etableres enten av EDIFACT-konverteren selv, eller av en tilhørende sikkerhetsmodul som bygger inn sikkerhetselementene etter ordinær EDIFACT-konvertering til MEDRUC. Det forutsettes at valg av løsning ikke påvirker meldingens utforming, slik at ulike sikkerhetsmoduler og løsninger med sikkerhetsfunksjonalitet integrert i EDIFACT-konverteren er interoperable.

2.1 Overordnet prosedyrebeskrivelse

Dette kapitlet gir en gjennomgang av de prosedyrene som vil forekomme hos en avsender og en mottaker av en MEDRUC-melding som både er signert og kryptert.

2.1.1 Avsender (Sykehus/Poliklinikk/Laboratorium/Apotek/Ortopedisk verksted)

0. Avsender har fått / kjøpt sertifikat / sertifikatpar skal benyttes ved signeringsprosessen. Ved sertifikatpar skal sertifikatet som har attributtet 'ikke-benekt' benyttes. Avsender har også mottatt eller må hente sertifikatutstederens og RTV's sertifikater for krypteringsnøkler.
1. Aktuell applikasjon i institusjonen genererer en melding i mellomformat, som aktuelt kontrollprogram leser inn.
2. Avsender bruker aktuelt kontrollprogram for å lese inn, kontrollere og genererer oppgjør for sending. Institusjonen gjør en aktiv handling som innebærer at dette elektroniske

dokumentet signeres (og sendes til mottaker). Det forutsettes at avsender ser / har sett de sentrale informasjonselementene i meldingen før signering og sending er mulig.
3. Denne meldingen EDIFACT-konverteres til en MEDRUC.
4. EDIFACT-konverteren (eller en tilhørende sikkerhetsmodul) inkluderer en del nødvendige sikkerhetsparametre (et sikkerhetshode) og genererer så en såkalt hashverdi av meldingen[1]. Hashverdien sendes til programvare[2], blir signert der og sendes i retur.
5. EDIFACT-konverteren (eller en tilhørende sikkerhetsmodul) inkluderer signaturen i meldingen[3]. (Den meldingen som nå foreligger omtales som en signaturforsterket MEDRUC-melding.
6. EDIFACT-konverteren (eller en tilhørende sikkerhetsmodul) genererer en tilfeldig DES-krypteringsnøkkel, for deretter å *komprimere, kryptere og filtrere*[4] den signaturforsterkede meldingen (evt en utveksling av flere meldinger til samme mottaker).
7. EDIFACT-konverteren (eller en tilhørende sikkerhetsmodul) genererer en CIPHER-melding og inkluderer i denne den komprimerte/krypterte/filtrerte meldingen, samt DES-nøkkelen kryptert under mottagers offentlige RSA krypteringsnøkkel.
8. CIPHER-meldingen inkluderes i en X.400-forsendelse til mottaker (RTV).

2.1.2 Mottaker (RTV)

0. RTV har generert eller fått tildelt et par (en offentlig og en privat) av asymmetriske RSA-nøkler som kalles krypteringsnøkler og benyttes til dekrypteringsprosessen. RTV har installert sertifikatet til sertifikatutsteder av avsenders sertifikater.
1. CIPHER-meldingen pakkes ut av X.400-forsendelsen fra avsender (sykehuset).
2. EDIFACT-konverteren (eller en tilhørende sikkerhetsmodul) dekrypterer den krypterte DES-nøkkelen med mottagers private RSA dekrypteringsnøkkel, for deretter å defiltrere, dekryptere og dekomprimere innholdet i CIPHER-meldingen (sammensettingen av USE-segmentene).
3. EDIFACT-konverteren (eller en tilhørende sikkerhetsmodul) innhenter om nødvendig avsenders X509-sertifikat og eventuelt fornyet revokeringsliste fra aktuell sertifikatutsteders distribusjonspunkt. Sertifikat og revokeringsliste verifiseres ned til installert tiltrodd rotsertifikat for aktuell sertifikatutsteder. Dersom oppgitt x509-sertifikat aksepteres som gyldig brukes dette (dets offentlige RSA-nøkkel) til å verifisere meldingens signatur.
   Dersom verifiseringen av sertifikat eller meldingssignatur feiler, avvises medlingen.
4. Den resulterende MEDRUC-meldingen konverteres via et mellomformat til RTV's lokalformat og behandles videre der.

2.2 Implementasjon for inkludering av digital signatur

Bruk av digital signatur (DS) er påkrevet.

2.2.1 Funksjonsbeskrivelse

Signaturen skal påføres av en/flere ansvarlige hos avsender, vha software signatur. Digital signatur sikrer både integritet av meldingsinnhold, opphavsautentisering og ikkebenekting

[1] D.v.s alle segmenter foruten UNH og UNT i den opprinnelige meldinge, med tillegg av USH, USA og USC, beskrevet nedenfor.

[2] Jfr kapittel 2.3.

[3] D.v.s legger til segmentene UST og USR.

[4] Komprimering gjennomføres valgfritt for å redusere datavolumet som skal krypteres og overføres. Filtreringen skjer for å overholde EDIFACT-syntaks.

(disse sikkerhetstjenestene er definert i ISO 7498-2). Digital signatur inkluderes i hver enkelt MEDRUC-melding før evt sammensetting i en utveksling og før komprimering/kryptering. Signering gjennomføres ved bruk av den asymmetriske kryptoalgoritmen RSA. De offentlige RSA-nøklene som benyttes til verifisering av signaturer, forutsettes å være sertifisert av en TTP (Tiltrodd Tredje Part) gjennom utstedelse av et nøkkelsertifikat (signert av TTP-en).

2.2.2 Notasjon

For hvert enkelt dataelement i et segment er det angitt følgende opplysninger:

- Dataelementets nummer (i.h.t EDIFACT-standarden)
- Dataelementets navn (på engelsk)
- Representasjon av dataelementet (i.h.t EDIFACT-standarden)
  - n2 = Numerisk, 2 tegn
  - a..3 = Alfabetisk, opptil 3 tegn
  - an..35 = Alfanumerisk, opptil 35 tegn
  - o.s.v.
- Bruk av dataelementer:
  - M Påkrevet (Mandatory) - Må forefinnes i.h.t EDIFACT-syntaks.
  - R Skal brukes (Required) - Må forefinnes for å oppfylle krav.
  - D Avhengig (Depending) - Bruk av segmentet/elementet avhenger av gitte omstendigheter. Disse er gitt i beskrivelsen av segmentet/elementet.
  - A Anbefalt (Advised) - Det anbefales at segmentet/elementet brukes, men det er ikke påkrevet. Mottakeren må kunne håndtere dette feltet.
  - O Valgfritt (Optional) - Dette feltet kan være med. Avsenderen kan avgjøre om feltet skal brukes eller ikke og mottakeren må kunne håndtere det.
  - N Ikke anbefalt (Not recommended) - Segmentet/elementet bør ikke brukes i denne meldingen. Mottaker kan velge å ignorere informasjonen i et slikt segment/element. Mottaker kan ikke betrakte bruk av segmentet/elementet som en feil.
  - X Brukes ikke (Not used) - Skal ikke brukes. Mottaker kan betrakte bruk av segmentet/elementet som en feil. Der hvor det er angitt at et sammensatt dataelement ikke skal brukes (X) vil kolonnen for bruk av delelementene være tom.

2.2.3 Meldingsoversikt "signaturforsterket" MEDRUC

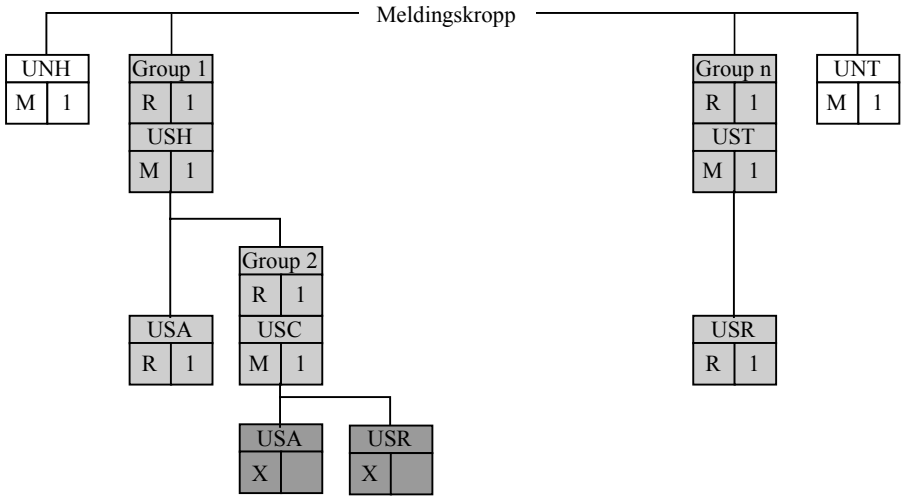
Segmenttabellen under viser hvordan EDIFACT-segmentene i signaturforsterket MEDRUC er brukt. Bruk av dataelementene i denne norske implementasjonen er vist i parentes. Av den "opprinnelige" MEDRUC-meldingen er kun UNH-, BGM-, AUT- og UNT-segmentene angitt.

TAG	Engelsk navn	Forklaring	Kval	Antall
UNH	Message Header (MEDRUC)	Meldingshode	M	1 (M 1)
----- Segmentgruppe 1 -- Sikkerhetsmekanismer ----------			C	9 (R 1)
-				
USH	Security Header	Sikkerhetshode	M	1 (M 1)
USA	Security Algorithm	Sikkerhetsalgoritme	C	1 (R 1)

----- Segmentgruppe 2 -- Valideringsmekanismer ----------			C	2 (R 2)
--				
USC	Certificate	Sertifikat	M	1 (M 1)
USA	Security Algorithm	Sikkerhetsalgoritme	C	3 (X)
USR	Security Result	Sikkerhetsresultat	C	1 (X)
----- UNSM-kropp (MEDRUC) ----------				
BGM	Beginning of message	Meldingsstart	M	1 (M 1)
...				
AUT/CNT	Authentication Result/Control Total	Autent.kode/Antall legeregn	C/M	1/1 (X/R)
----- Segmentgruppe n -- Binding til segmentgruppe 1 ----------			C	9 (R 9)
UST	Security Trailer	Sikkerhetsavslutning	M	1 (M 1)
USR	Security Result	Sikkerhetsresultat	C	1 (R 1)
UNT	Message Trailer (MEDRUC)	Meldingsavslutning	M	1 (M 1)

2.2.4 Segmentdiagram

Segmenter i UNSM-kropp er utelatt. Sikkerhetssegmentene som legges til "opprinnelig" MEDRUC-melding, er gjengitt gråtonet.



2.2.5 Segmentspesifikasjon

Segmentgruppe 1 (R 1)

USH – Sikkerhetshode (M 1)

Ref	Navn	Format	Kval	Bruk av element
0552	SECURITY STRUCTURE VERSION NUMBER	an..3	M	"94W"
0501	SECURITY FUNCTION, CODED	an..3	M	"1" (NRO)
0534	SECURITY RESULT LINK	n2	M	"1"
0541	SCOPE OF SECURITY APPLICATION, CODED	an..3	R	"1" (SHM)
0503	RESPONSE TYPE, CODED	an..3	X	Brukes ikke[5]
0505	FILTER FUNCTION, CODED	an..3	R	"2" (HEX)
0507	CHARACTER SET ENCODING, CODED	an..3	R	"2" (AS8)
0509	ROLE OF SECURITY PROVIDER, CODED	an..3	X	Brukes ikke
S500	SECURITY IDENTIFICATION DETAILS		X	Brukes ikke
0516	SECURITY REFERENCE NUMBER	an..35	R	”0”[6]

[5] Merk at Edifact-standarden sier at ubrukte attributter må være tomme dersom de etterfølges av attributter med verdi innen samme segment eller kompositt-attributt.

[6] Elementet er påkrevet, men settes til verdien 0 da det ikke er i praktisk bruk.

S501	SECURITY DATE AND TIME		R	
0517	Date and time qualifier, coded	an..3	M	"1"
0502	Date	n8	R	"YYYYMMDD"
0504	Time	n6	R	"HHMMSS"
0506	UTC offset	an..5	X	Brukes ikke[7]

USA – Sikkerhetsalgoritme (R 1)

Ref	Navn	Format	Kval	Bruk av element
S502	SECURITY ALGORITHM		M	
0523	Use of algorithm	an..3	M	"1" (OHA)
0525	Cryptographic mode of operation, coded	an..3	R	"0" (NUL)
0533	Mode of operation code list identifier	an..3	X	Brukes ikke
0527	Algorithm coded	an..3	R	"6" (MD5)
0529	Algorithm code list identifier	an..3	X	Brukes ikke
S503	ALGORITHM PARAMETERS		X	Brukes ikke

Segmentgruppe 2 (R 1)

USC	Sertifikat – Certificate	M	1
USA	Sikkerhetsalgoritme – Security Algorithm	X	Brukes ikke
USR	Sikkerhetsresultat – Security Result	X	Brukes ikke

USC – Sertifikat (M 1)

Ref	Navn	Format	Kval	Bruk av element
0536	CERTIFICATE REFERENCE	an..35	R	"nnnnn...n"[8]
S500	SECURITY IDENTIFICATION DETAILS		R	
0577	Security party qualifier	an..3	M	"4" (AX)
0538	Key name	an..35	X	Brukes ikke
0511	Party Identification	an..256	R	Sertifikatutsteders navn[9]
0527	Code list qualifier	an..3	X	Brukes ikke
0529	Code list responsible agency	an..3	X	Brukes ikke
0586	Party name	an..35	X	Brukes ikke
0586	Party name	an..35	X	Brukes ikke
0586	Party name	an..35	X	Brukes ikke
S500	SECURITY IDENTIFICATION DETAILS		X	Brukes ikke
0544	FORMAT CERTIFICATE VERSION	an..3	X	Brukes ikke
0505	FILTER FUNCTION CODED	an..3	X	Brukes ikke
0507	CHARACTER SET ENCODING, CODED	an..3	X	Brukes ikke
0543	CHARACTER SET REPERTOIRE, CODED	an..3	X	Brukes ikke
0546	USER AUTHORISATION LEVELS	an..35	X	Brukes ikke
S505	SEPARATOR FOR SIGNATURE		X	Brukes ikke
S501	SECURITY DATE AND TIME		X	Brukes ikke

Hashverdi (for signering av sertifikater):

Ref	Navn	Format	Kval	Bruk av element
S502	SECURITY ALGORITHM			
0523	Use of algorithm, coded	an..3	R	"4" (IHA)
0525	Cryptographic mode of operation	an..3	R	"0" (NUL)
0527	Algorithm, coded	an..3	R	"6" (MD5)

Signatur (på sertifikater):

Ref	Navn	Format	Kval	Bruk av element

[7] Tolkes som "offisiell norsk tid".

[8] Serienummer (unikt) hentet fra det aktuelle sertifikatet. (Certificate.serialNumber) NB: Desimalt

[9] Sertifikatutsteders hentet fra "Distinguished name" i sertifikatet. (Certificate.issuer.)

S502	SECURITY ALGORITHM			
0523	Use of algorithm, coded	an..3	R	"3" (ISG)
0525	Cryptographic mode of operation	an..3	R	"16" (DSMR)
0527	Algorithm, coded	an..3	R	"10" (RSA)
S503	ALGORITHM PARAMETER			
	Algorithm parameter value	an..512		"1024"
	Algorithm parameter qualifier, coded	an..3		"14"

Signatur (på meldinger):

Ref	Navn	Format	Kval	Bruk av element
S502	SECURITY ALGORITHM			
0523	Use of algorithm, coded	an..3	R	"6" (OSG)
0525	Cryptographic mode of operation	an..3	R	"16" (DSMR)
0527	Algorithm, coded	an..3	R	"10" (RSA)
S503	ALGORITHM PARAMETER			
	Algorithm parameter value	an..512		"512"
	Algorithm parameter qualifier, coded	an..3		"14"

Segmentgruppe n (R 1)

UST	Sikkerhetshale – Security Trailer	R	1
USR	Sikkerhetsresultat – Security Result	R	1

UST – Sikkerhetshale

Ref	Navn	Format	Kval	Bruk av element
0534	SECURITY RESULT LINK	n2	M	"1"

USR – Sikkerhetsresultat

Ref	Navn	Format	Kval	Bruk av element
S508	VALIDATION RESULT		M	
0560	Validation value	an..256	M	Digital signatur[10]
0560	Validation value	an..256	X	Brukes ikke

2.2.6 Eksempler på signaturforsterket MEDRUC-melding

2.2.6.1 Eksempel 1

Signert med avsenders hemmelige nøkkel fra sertifikat utstedt av ZebSign – nytt CA

```
UNH+1001+MEDRUC:D:93A:UN:RTVPO0'
USH+94W+1+1+1++2+2+++0+1:20040311:144400'
USA+1:0::6'
USC+1234+4::CN=First ZebSign Community ID CA, O=ZebSign - 983163432, C=NO'
BGM+POL::ZZ3+A11B22C33D44E55'
DTM+137:20030603:102'
..
UST+01'
USR+9BC4F9E2A66FCFBFE573DDD5B2353BC9158745BC70555CF63E07A89F41BA0AAEBB80BCC
0394650BABFCA4F52B8644A9223527AA3B1828B4E3660D91332C7D1D982673796EC3EC264F4
6C541804AE55E3DEFFA0D8511DCED4565F6DB6D60539D19B2E5B98EC3AE24887E1693D1D42C
EAEBC8E3F0EB9B587068F452C95777D4CCC'
UNT+195+1001'
```

UNH: Referansenummer til denne meldingen er 1001.

[10] Filtrert (i.h.t. dataelement 0505, filterfunksjon i USH) signatur. Lengden er 512 biter før filtrering.

USH: Sikkerhetsstrukturen er versjon 94W, sikkerhetstjenesten er ikkebenekting (kode 1), sikkerhetslenken er 1, filterfunksjonen er HEX-filtrering (kode 2) og 8-bits ASCII-tegn benyttes i meldingen (kode 2). Sikkerhetsdato og tid er (kvalifikator 1): Dato: 2004-03-11, tid: 14.44.00.
USA: Avsender benytter hashfunksjon MD5.
USC: Sertifikatet som RTV skal benytte for å verifisere signaturen har serienummer 1234 og er utstedt av (issuer)

```
CN=First ZebSign Community ID CA, O=ZebSign - 983163432, C=NO
```

.
UST:
USR: Signaturen på denne meldingen.
UNT: Det er i alt 195 segmenter i denne meldingen med referansenummer 1001.

2.2.6.2 Eksempel 2

Signert med avsenders hemmelige nøkkel fra sertifikat utstedt av ZebSign – gammelt CA

Nr	Datasegment	Melding
1	Meldingshode	UNH+1148+MEDRUC:D:93A:UN'
2	Sikkerhetshode	USH+94W+1+1+1++2+2+++0+1:20000129:160700'
3	Sikkerhetsalgoritme	USA+1:0::6'
4	Sertifikat	USC+3437+4::CN=Norway Post Organizational CA, O=CA, C=NO'
5	Meldingsstart	BGM+POL::ZZ3+000129160701'
...		
34	Trygdekontor	PNA+TK+0425:ZZ3'
35	Avsender	PNA+BQ2+11177+111111111::ENH+++1:TESTSYKEHUS+2:TEST POLIKLINIK77'
...		
80	Sikkerhetshale	UST+01'
81	Sikkerhetsresultat	USR+B3B4285332914D9BAEE07DB88CA024587BC047965A4FBAE6125ECCF20D2EEEE66D0D58FF6B1FD9B0A344FEB20B982447E390720183CF63F2C510D13C53CB9113197F42F437124F1A43767BF71F5A0405620B32749B48EEC9D007688BD458D5166E93E1EC00AD222BFD8945E468D21A164F3BDAC013ADAEB469DDEAA7EC11DD9A'
82	Meldingsavslutning	UNT+361+1148'

1. Referansenummeret til denne poliklinikkmeldingen er 1148.
2. Sikkerhetsstrukturen er versjon 94W, sikkerhetstjenesten er ikkebenekting (kode 1), sikkerhetslenken er 1, filterfunksjonen er HEX-filtrering (kode 2) og 8-bits ASCII-tegn benyttes i meldingen (kode 2). Sikkerhetsdato og tid er (kvalifikator 1): Dato: 2000-01-29, tid: 16.07.00.
3. Avsender benytter hashfunksjon MD5.
4. Sertifikatet som RTV skal benytte for å verifisere signaturen har referansenummer 3437 og er utstedt av
   CN=Norway Post Organizational CA, O=CA, C=NO.

5-79. Ikke sikkerhetsrelevante segmenter.

80. Lenken til tilsvarende sikkerhetshode er 1 (segment 2).
81. Selve signaturen på denne poliklinikkmeldingen.
82. Det er i alt 361 segmenter i denne meldingen med referansenummer 1148.

2.2.6.3 Eksempel RTV-CA

Eksempel med sertifikat fra RTV-CA utgår; det skal ikke benyttes av nye partnere og skal utfases

2.3 Krav til sikkerhet i signaturprosessen

Selve signeringen kan foregå i maskin/programvare.
Merk at sertfifikat med attributt 'ikke-benekt' skal benyttes for signeringen.

2.3.1 Maskin/programvare

Programvareløsninger må sikre følgende:

- Private nøkler skal lagres kryptert på disk. Ved bruk skal autorisert person autentiseres med passord som også benyttes til å "åpne" den krypterte nøkkelen.
- På lik linje med PIN-koder til smartkort vil det være nødvendig å sikre mot systemfeil/ misbruk dersom passord ikke kreves oppgitt ved hver enkelt signering.
- Under selve signaturberegningen finnes brukerens hemmelige nøkkel seg i klartekst i datamaskinens prosessor. For å sikre mot kompromittering av nøkkelinformasjonen, blir alle prosessorens aktuelle internminner o.l slettes (overskrives) etter signaturberegningen.

2.4 Implementasjon av kryptering (CIPHER)

Kryptering er påkrevet.

2.4.1 Funksjonsbeskrivelse

Kryptering kan gjøres på enten meldinger eller utvekslinger, avhengig av hva som skal legges inn i en enkelt X.400 meldingskropp og sendes til en gitt mottaker. Kryptering sikrer konfidensialitet.
Kryptering gjennomføres ved bruk av den symmetriske krypteringsalgoritmen DES. De symmetriske nøklene som benyttes til krypteringen genereres tilfeldig på nytt ved før kryptering av hver ny melding eller utveksling. DES-nøklene utveksles i CIPHER-meldingen kryptert med mottagers offentlige RSA-nøkkel (såkalt hybrid nøkkelutveksling). De offentlige RSA-nøklene som benyttes til krypteringen av DES-nøklene forutsettes sertifisert av en TTP gjennom utstedelse av et nøkkelsertifikat (signert av TTP-en). Det forutsettes at meldingen eller utvekslingen som skal krypteres, komprimeres før kryptering og filtreres etter kryptering, se nedenfor.

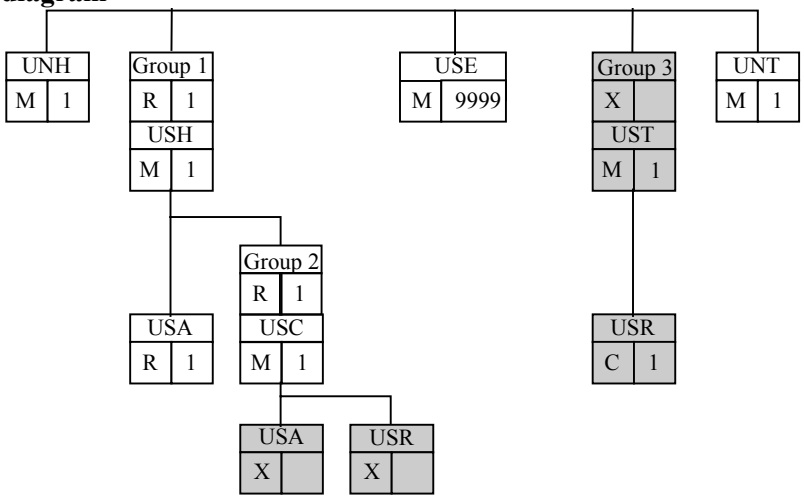
2.4.2 Meldingsoversikt CIPHER

Segmenttabellen under viser hvordan EDIFACT-segmentene i CIPHER er brukt. Bruk av dataelementene i denne norske implementasjonen er vist i parentes.

TAG	Engelsk navn	Forklaring	Kval	Antall
UNH	Message Header	Meldingshode	M	1 (M 1)
----- Segmentgruppe 1 -- Sikkerhetshodegruppe ----------			C	9 (R 1)
--				
USH	Security Header	Sikkerhetshode	M	1 (M 1)
USA	Security Algorithm	Sikkerhetsalgoritme	C	1 (R 1)
----- Segmentgruppe 2 -- Sertifikatgruppe ----------			C	2 (R 1)
--				
USC	Certificate	Sertifikat	M	1 (M 1)

USB	Beginning of security message	Sikkerhetsmeldingsstart	M	1 (X)
USE	Encryption	Kryptert melding	M	9999 (M 9999)
----- Segmentgruppe 3 -- Sikkerhetsavslutningsgruppe ----------			C	9 (X)
--				
UNT	Message Trailer	Meldingsavslutning	M	1 (M 1)

2.4.3 Segmentdiagram



2.4.4 Segmentspesifikasjon

UNH – Meldingshode (M 1)

Ref	Navn	Format	Kval	Bruk av element
0062	MESSAGE REFERENCE NUMBER	an..14	M	Sekvensnummer 0-999
S009	MESSAGE IDENTIFIER		M	
0065	Message type identifier	an..6	M	"CIPHER"
0052	Message type version number	an..3	M	"1"
0054	Message type release number	an..3	M	"931"
0051	Controlling agency	an..2	M	"UN"

Segmentgruppe 1 (R 1)

USH – Sikkerhetshode (M 1)

Ref	Navn	Format	Kval	Bruk av element
0552	SECURITY STRUCTURE VERSION NUMBER	an..3	M	"94W"
0501	SECURITY FUNCTION, CODED	an..3	M	"4" (ENC)
0534	SECURITY RESULT LINK	n2	X	Brukes ikke
0541	SCOPE OF SECURITY APPLICATION, CODED	an..3	X	Brukes ikke
0503	RESPONSE TYPE, CODED	an..3	X	Brukes ikke
0505	FILTER FUNCTION, CODED	an..3	R	"2" (HEX)
0507	CHARACTER SET ENCODING, CODED	an..3	R	"2" (AS8)
0509	ROLE OF SECURITY PROVIDER, CODED	an..3	X	Brukes ikke
S500	SECURITY IDENTIFICATION DETAILS		X	Brukes ikke
0516	SECURITY REFERENCE NUMBER	an..35	R	Brukes ikke
S501	SECURITY DATE AND TIME		R	Dato og tid for kryptering
0517	Date and time qualifier, coded	an..3	M	"1"
0502	Date	n8	R	"YYYYMMDD"
0504	Time	n6	R	"HHMMSS"
0506	UTC offset	an..5	X	Brukes ikke

USA – Sikkerhetsalgoritme (R 1)

Ref	Navn	Format	Kval	Bruk av element
S502	SECURITY ALGORITHM		M	
0523	Use of algorithm	an..3	M	"2" (OSY)
0525	Cryptographic mode of operation,	an..3	R	"2" (CBC)[11]
0533	coded	an..3	X	Brukes ikke
0527	Mode of operation code list identifier	an..3	R	"1" (DES) eller "999" (GZIP før DES) [12]
0529	Algorithm coded	an..3	X	Brukes ikke
	Algorithm code list identifier			
S503	ALGORITHM PARAMETER		R	
0532	Algorithm parameter value	an..512	R	RSA-kryptert DES-nøkkel[13]
0531	Algorithm parameter qualifier	an..3	R	"6" (KYP)

Segmentgruppe 2 (R 1)

USC	Sertifikat – Certificate	M	1
USA	Sikkerhetsalgoritme – Security Algorithm	X	Brukes ikke
USR	Sikkerhetsresultat – Security Result	X	Brukes ikke

USC – Sertifikat (M 1)

Gir referanse til sertifikatet tilhørende den offentlige nøkkelen som ble benyttet til å kryptere DES-nøkkelen.

Ref	Navn	Format	Kval	Bruk av element
0536	CERTIFICATE REFERENCE	an..35	R	"nnnnn...n"[14]
S500	SECURITY IDENTIFICATION DETAILS		R	
0577	Security party qualifier	an..3	M	"4" (AX)
0538	Key name	an..35	X	Brukes ikke
0511	Party Id identification	an..256	R	Sertifikatutsteders navn[15]
0527	Code list qualifier	an..3	X	Brukes ikke
0529	Code list responsible agency	an..3	X	Brukes ikke
0586	Party name	an..35	X	Brukes ikke
0586	Party name	an..35	X	Brukes ikke
0586	Party name	an..35	X	Brukes ikke
S500	SECURITY IDENTIFICATION DETAILS		X	Brukes ikke
0544	FORMAT CERTIFICATE VERSION	an..3	X	Brukes ikke
0505	FILTER FUNCTION CODED	an..3	X	Brukes ikke
0507	CHARACTER SET ENCODING, CODED	an..3	X	Brukes ikke
0543	CHARACTER SET REPERTOIRE, CODED	an..3	X	Brukes ikke
0546	USER AUTHORISATION LEVELS	an..35	X	Brukes ikke
S505	SEPARATOR FOR SIGNATURE		X	Brukes ikke
S501	SECURITY DATE AND TIME		X	Brukes ikke

Det forutsettes altså bruk av lokalt lagrede sertifikater som det kun refereres til i USC-segmentet. Sertifikatets format er ikke spesifisert fullt ut, men *skal* være i henhold til beskrivelsene under USC i kapittel 0.0.0.

USB – Begynnelse av sikkerhetsmelding (X)

---

11 Initialiseringsvektoren (startvariabelen) IV = 0F 0F 0F 0F 0F 0F 0F 0F.

12 Ved "1" krypteres meldingen med DES i CBC-modus uten forutgående komprimering. Ved "999" forutsettes at meldingen komprimeres før kryptering med DES i CBC-modus. Kompresjonsalgoritmen som *skal* benyttes er algoritmen GZIP versjon 1.2.4. GZIP (GNU ZIP) versjon 1.2.4 er tilgjengelig via anonym ftp fra f.eks ugle.unit.no (katalogen pub/gnu) eller hos KITH. GZIP finnes for de fleste plattformer inkludert UNIX og DOS.

13 DES-nøkkelen er kryptert under mottakers offentlige krypteringsnøkkel og filtrert i h.h.t. filtreringsfunksjonen angitt i dataelement 0505 i USH.

14 Serienummer (unikt) hentet fra det aktuelle sertifikatet. (Certificate.serialNumber)

15 Sertifikatutsteders domenenavn hentet fra "Distinguished name" i sertifikatet. (Certificate.issuer.addmd)

Ref	Navn	Format	Kval	Bruk av element
	START OF SECURITY MESSAGE	an..1	M	"X"

USE – Kryptert melding/utveksling (M 9999)

Ref	Navn	Format	Kval	Bruk av element
0522	ENCRYPTED STRING	an..512	M	512-tegns kryptert blokk[16]

Segmentgruppe 3 (X)
UNT – Meldingsavslutning (M 1)

Ref	Navn	Format	Kval	Bruk av element
0074	NUMBER OF SEGMENTS IN A MESSAGE	n..6	M	
0062	MESSAGE REFERENCE NUMBER	an..14	M	Som 0062 i UNH

Meldingen som er komprimert, kryptert og inkludert i CIPHER-meldingen, er den som er vist i eksempelet i kapittel 2.2.6.1.

2.4.5 Eksempel på CIPHER-melding med mottakers offentlige nøkkel fra sertifikat utstedt av Posten SDS CA

Nr	Datasegment	Melding
1	Meldingshode	UNH+1149+CIPHER:1:931:UN'
2	Sikkerhetshode	USH+94W+4++++2+2+++000000+1:20000129:160719'
3	Sikkerhetsalgoritme	USA+2:2::999+6CF68C083FBD9E4EBA142DF0D76677D44B8385AEF40D1CEF7B591DB321B6914B91AFFB807DC81B169E439FD17F512580EF1A8E22B9A6F02A8C9E38444CD19E042BB61EA80D26BB0AB8615EB47841A5886E88069F9B67D1B00EA3199C98978764DA0416352E01B093D03D8C61E7198E7D87D5E006DD9059A562828EB2F01C50B8:6'
4	Sertifikat	USC+44260+4::CN=Norway Post Organizational CA, O=CA, C=NO'
5	Begynnelse av sikkerhetsmelding	USB+X'
6	Kryptert melding	USE+0CFAD75B44EC657A1E9AE823BA8394EFC750CED756C1685838A0432655B093C196DB217503854970149E575C6FBD8D202FD7700075B506916DF3B6B3BDB051057FA3C03B37EC01EC565B27F4F19DBCBDDB98A77DA9AC743CE06C2FFF02409247490DB6DF8DE7AF264781F7D5827B6DB2A9D9D9438A8AA4A1078DD70DDA9691A9'
...		
14	Kryptert melding	USE+3037A28325EB7F7A9C075D51B22A1EF46FB651CD3244A86D7C4130E868D7DCC6EBF750A7172478F2033715C44662DC7C212F734B5AB814719717A19717AF750A7172478F2033715C44CF734B5AB8162DC7C212F73462DC7C212'
15	Meldingsavslutning	UNT+14+1149'

1. Referansenummeret til denne CIPHER-meldingen (krypterte oppgjørsmeldingen) er 1149.
2. Sikkerhetsstrukturen er versjon 94W, sikkerhetstjenesten er kryptering (kode 4), filter-funksjonen er HEX-filtrering (kode 2) og 8-bits ASCII-tegn benyttes i meldingen (kode 2). Sikkerhetsdato og tid er (kvalifikator 1): Dato: 2000-01-29, tid: 16.07.19.
3. Meldingen er først komprimert med GZIP (fast definert - reflekteres ikke i meldingen), deretter kryptert med DES (kode 999, GZIP og DES sammen) i CBC-modus (kode 2).

[16] Etter filtrering i h.h.t. filtreringsfunksjonen angitt i dataelement 0505 i USH. Siste blokk kan være mindre enn 512 tegn.

Deretter følger DES-nøkkelen kryptert under mottakers offentlige RSA-nøkkel og HEX-filtrert.

4. Sertifikatet (tilhørende RTV) som sykehuset/poliklinikken har benyttet til å kryptere har referansenummer 44260 og er utstedt av
   CN=Norway Post Organizational CA, O=CA, C=NO.
5. Segment USB som angir begynnelse av sikkerhetsmelding er påkrevet, men ikke i bruk. Denne settes derfor til "X"

6-14. Komprimert, kryptert og filtrert poliklinikkmelding som er delt opp i blokker på 512 tegn.

15. Det er totalt 14 segmenter i meldingen. Meldingens referansenummer er 1149.

2.4.6 Eksempel på CIPHER-melding med mottakers offentlige nøkkel fra sertifikat utstedt av RTV CA

Eksempel med sertifikat fra RTV-CA utgår; det skal ikke benyttes av nye partnere og skal utfases

3. Sertifikater og nøkler

3.1 Dagens sertifikater / TTP

Pr. i dag er det bare ZebSign som er godtkjent av RTV for utstedelse av nye sertifikater.
Avsender er selv ansvarlig for å bestille sertifikat herfra.
Ved spørsmål kontakt EDI-leverandør.

3.2 Vising av sertifikatinformasjon

3.2.1 Listing av sertifikat lagret i pem-format vha OPENSSL

```
C:\ openssl x509 -in cert.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 14425 (0x3859)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=NO, O=ZebSign - 983163432, CN=First ZebSign Community ID CA
        Validity
            Not Before: Sep 23 08:47:14 2003 GMT
            Not After : Sep 23 08:47:14 2005 GMT
        Subject: C=NO, O=Visma Software ASA-980858073, CN=Visma Software ASA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
..
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                4D:87:17:DF:BA:AD:F1:FD
            X509v3 Certificate Policies:
```

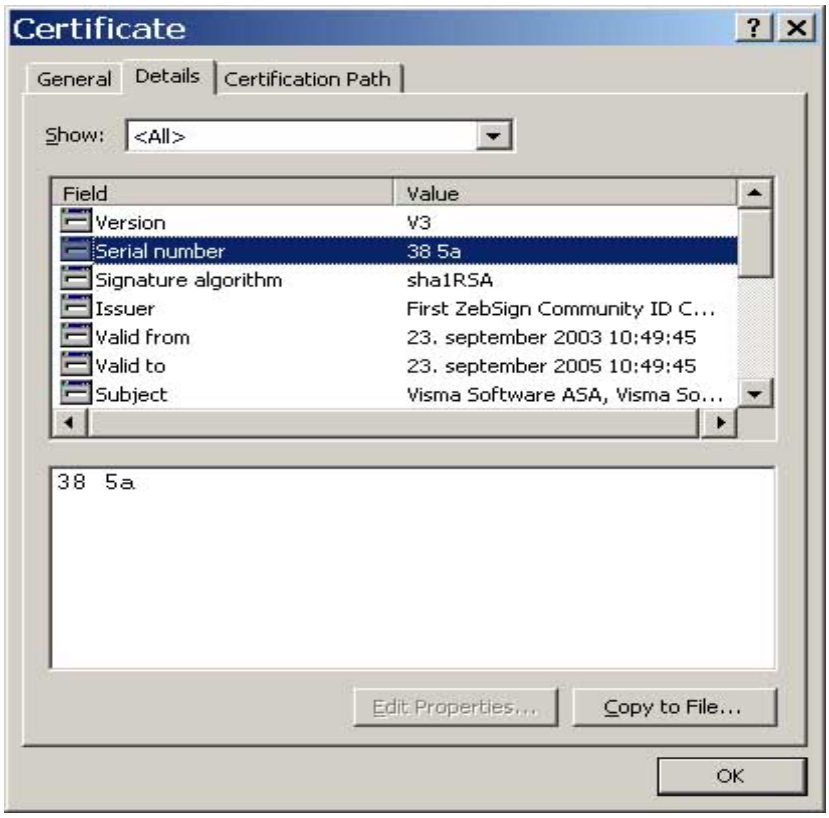
```
                Policy: 2.16.578.1.9.4.1.5

            X509v3 Authority Key Identifier:
                keyid:4F:FD:12:79:92:93:FB:E6

            Authority Information Access:
                OCSP - URI:http://ocsp.zebsign.com/zebsign/ocsp/

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment, Key
Agreement
..
```

Merk at dette sertifikatet IKKE har ”key usage” Non Repudiation; og dette skal derfor ikke benyttes til signering

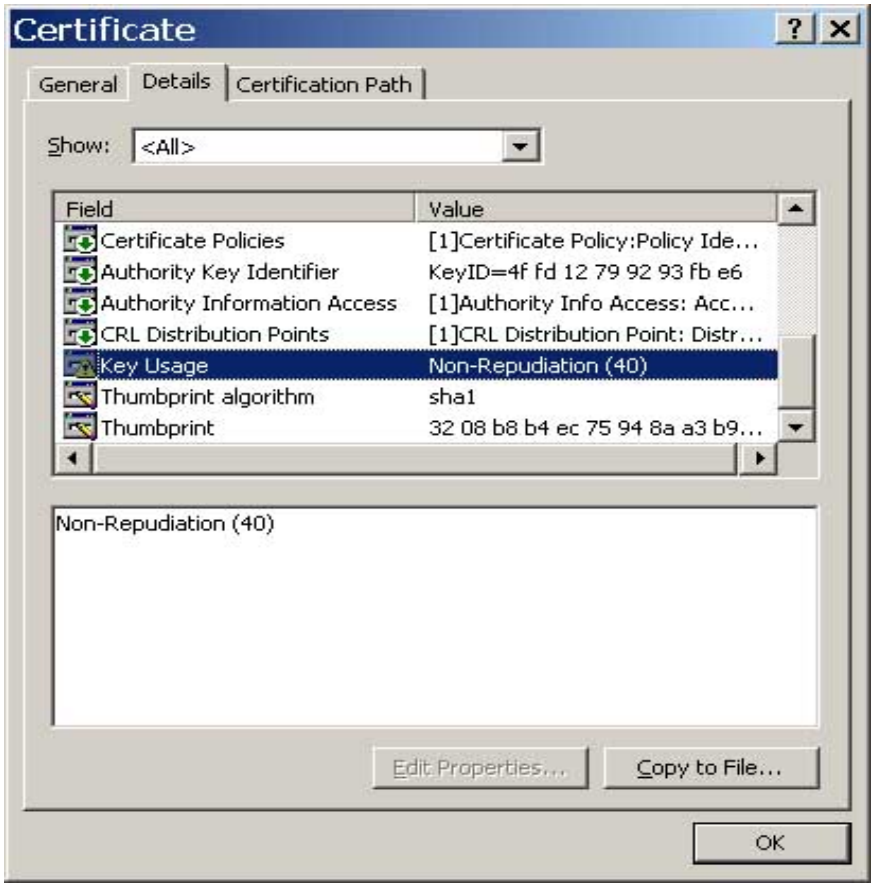
3.2.2 Listing av sertifikat lagret i DER-format vha OPENSSL

```
openssl x509 -in cert.crt -inform DER -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 14426 (0x385a)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=NO, O=ZebSign - 983163432, CN=First ZebSign Community ID CA
        Validity
            Not Before: Sep 23 08:49:45 2003 GMT
            Not After : Sep 23 08:49:45 2005 GMT
        Subject: C=NO, O=Visma Software ASA-980858073, CN=Visma Software ASA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
  ..
      X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                46:CC:48:5E:8A:8E:D0:8E
            X509v3 Certificate Policies:
                Policy: 2.16.578.1.9.4.1.5

            X509v3 Authority Key Identifier:
                keyid:4F:FD:12:79:92:93:FB:E6

            Authority Information Access:
                OCSP - URI:http://ocsp.zebsign.com/zebsign/ocsp/

            X509v3 Key Usage: critical
                Non Repudiation
            X509v3 CRL Distribution Points:
               ..
```

3.2.3 Visning av sertifikat i Windows ”Crypto Shell Extensions”



Merk at serienummer her vises i hex-form; i Meldingen skal imidlertid desimalverdien brukes.



3.3 Kobling mellom kontrollprogram og sertifikat

I programmet for Kontroll av regninger (POLK/LABR/ORTOK/APOK) starter man forsendelsen av MEDRUC meldingen til RTV. For å starte forsendelsen må man oppgi sertifikat identifikasjon og passord (PIN-kode). Det er dette som initierer selve signerings prosessen av meldingen. Disse opplysningene blir overført til EDI-serveren som sjekker sertifikat identifikasjon og passordet med sertifikatopplysningene som ligger lagret kryptert på serveren. Under selve signerings beregningen gjøres brukerens hemmelig nøkkel lesbar i klartekst i EDI-serverens prosessor (se kap.2.4.1).

Sertifikat identifikasjon og passord får brukeren fra sertifikat utsteder (CA) i forbindelse med at sertifikatene blir sendt ut.