4. Sikkerhed i EDIFACT

1. Indledning 2
2. Kravene til sikkerhed 2
3. Standardisering 2
4. TeleSeC 3
    4.1 Formål 3
    4.2 TeleSeC-egenskaber 3
    4.3 TeleSeC-opbygning 4
    4.4 Certifikater 5
5. Nye forslag til sikkerhed 7
    5.1 Digital signatur 7
    5.2 “Header og trailer” metoden 8
    5.3 AUTACK 8

1. Indledning

Der er flere årsager til, at sikkerhed er relevant for deltagerne i dataudveksling. Det er relevant, hvad enten udvekslingen sker i EDIFACT eller andre formater, men specielt for EDIFACT er det af stor betydning, at de anvendte løsninger fungerer efter de samme principper.

2. Kravene til sikkerhed

En optimal EDIFACT-dataudveksling skal kunne sikres på et niveau, der gør det muligt at udveksle og edb-behandle meddelelser uden overflødige, manuelle kontroller. Det skal f.eks. være muligt at gennemføre pengeoverførsler til 3. part alene på baggrund af selve EDIFACT-dataudvekslingen.

De forhold som gør sig gældende, og som man er nødt til at forholde sig til ved dataudveksling med f.eks. et pengeinstitut er følgende:

- Forsendelsen kan gå tabt.

- Forsendelsen kan utilsigtet blive genfremsendt.

- Indholdet af forsendelse kan sikres mod ændringer, inden den når frem til modtageren (pengeinstituttet). Dette sikkerhedselement betegnes som integritet.

- Der skal være sikkerhed for, at afsenderen af forsendelse ikke er en anden, end denne udgiver sig for (autenticitet).

- Der skal være sikkerhed for, at den rigtige afsender eller modtageren ikke nægter et efterfølgende kendskab til forsendelsen. Dette sikkerhedselement betegnes som uafviselighed.

- Forsendelsen eller dele heraf må ikke kunne læses af uvedkommende.
  Dette sikkerhedselement betegnes som hemmeligholdelse eller konfidentialitet.

En række af de ovennævnte forhold, har naturligvis altid været gældende ved almindelig kendt udveksling af papirdokumenter. Den væsentlige forskel mellem papirdokumenter og EDIFACT er imidlertid, at genereringen og udvekslingen af EDIFACT-meddelelser og forsendelser indgår i en automatiseret edb-proces. I en sådan proces, hvor høj effektivitet og hastighed er nøgleord, kan den menneskelige kontrolfaktor vanskeligt indgå på samme niveau som ved papirdokumenter.

Sikkerhedsmekanismerne ved EDIFACT skal derfor virke fuldt automatiseret, uden samtidig at reducere selve sikkerhedsniveauet.

3. Standardisering

I regi af UN/EDIFACT er der endnu ingen vedtagne standarder for sikkerhedsprincipper og tilhørende -mekanismer. Finansrådet har dog deltaget aktivt i en særlig arbejdsgruppe for sikkerhed i EDIFACT (Security Joint Working Group - SJWG). Gruppen har udarbejdet en række forslag, som indtil videre er godkendt til testbrug.

Pengeinstitutternes BetalingsSystemer (PBS) har udviklet et fælles koncept for sikkerhed kaldet TeleSeC. Dette koncept er for tiden under implementering i pengeinstitutterne, og vil som en helhed opfylde de krav, som blev nævnt i afsnittet ovenfor. TeleSeC leveres som en nøglefærdig løsning til sikring af EDIFACT-meddelelser og forsendelser mellem pengeinstitutterne og deres kunder.

TeleSeC følger princippet i de forslag, som SJWG er fremkommet med. Der er dog den forskel, at Tele-SeC selv har defineret egne meddelelser, segmenter og kodelister for EDIFACT-strukturen. Når forslagene fra SJWG med eventuelle ændringer ophøjes til standarder, vil TeleSeC som konsekvens heraf efterfølgende tilpasses disse.

En mere detaljeret beskrivelse af TeleSeC-konceptet fremgår af afsnittet *TeleSeC.*

Pengeinstitutternes kunder benytter en række forskellige tekniske platforme, og de enkelte penge-institutter har tilsvarende forskellige sikkerhedsprincipper. Der kan derfor også fremover i nogle tilfælde være behov for ikke-standardiserede sikkerhedsprincipper i de enkelte pengeinstitutter.

I afsnittet "Nye forslag til sikkerhed" beskrives relevante løsningsforslag fra SJWG. For yderligere informationer f.eks. i relation til en aktuel implementering henvises til det aktuelle pengeinstitut.

4. TeleSeC

4.1 Formål

TeleSeC er et sikkerhedssystem, som har til formål at sikre datakommunikation f.eks. i forbindelse med office banking systemer. Denne sikring sker ved at opfylde nedenstående 4 krav.

- **Autenticitet**
  Vished for hvem der er afsender og modtager af data.

- **Uafviselighed**
  Hverken afsender eller modtager kan afvise at have sendt henholdsvis modtaget data.

- **Integritet**
  Sikkerhed for, at data er intakte og ikke forvanskede.

- **Konfidentialitet**
  Sikkerhed for, at data hemmeligholdes for uvedkommende under transmissionen.

Ved hjælp af avanceret kryptografi er det muligt at fremstille en elektronisk underskrift, som kaldes en digital signatur.

TeleSeC-systemet er et standardiseret sikkerhedssystem, som danner digitale signaturer baseret på konceptet Public Key systemer.

TeleSeC anvender RSA (**R**ivest, **S**hamir og **A**dleman) krypteringsalgoritme med en nøglelængde på 512 bits til fremstilling af digitale signaturer.

Til hemmeligholdelse af transmissioner anvendes DES-krypteringsalgoritme med en nøglelængde på 64 bits.

TeleSeC giver mulighed for at fremstille/verificere digitale signaturer i EDI/EDIFACT, således at modtageren af et dokument får bevis for, at dokumentet kommer fra den afsender, som er indikeret i dokumentet.

Systemet giver afsenderen bevis for, at modtageren rent faktisk har modtaget dokumentet, ved at brugeren returnerer en kvittering med digital signatur .

4.2 TeleSeC-egenskaber

Med TeleSeC-systemet har man mulighed for at sikre kommunikationen, dels ved en enkel form mellem en bruger og en edb-central og dels ved en mere åben kommunikation, hvor kunder kommunikerer indbyrdes.

Sikrer data i et åbent net
TeleSeC er designet til sikring af datakommunikation i et åbent net. Med anvendelse af certifikater sikres en entydig relation mellem en brugers offentlige nøgle og dennes identifikation.

EDI og EDIFACT
TeleSeC kan anvendes til sikring af EDI- og EDIFACT-transmissioner både med anvendelse af digitale signaturer og med hensyn til hemmeligholdelse af dataindholdet.

TeleSeC og 3270-online-kommunikation
TeleSeC kan anvendes til sikring af 3270 online kommunikation. Det betyder, at skærmbilleder, som sendes fra en PC, der emulerer en 3270-terminal, kan sikres med en digital signatur.

TeleSeC er uafhængig af kommunikationsform
Der er implementeret forskellige konverterings- og filterfunktioner i TeleSeC, som sikrer en stor uafhængighed til den valgte kommunikationsform.

TeleSeC er uafhængig af brugergrænsefladen
TeleSeC er udelukkende et sikkerhedsmodul, som kan integreres i en given forretningsapplikation via en veldefineret programmeringsgrænseflade (API). Brugergrænsefladen defineres af applikationen.

TeleSeC på forskellige platforme
TeleSeC er primært implementeret i "C", hvilket sikrer en meget høj grad af portabilitet. Enhver platform, som kan afvikle C-programmer, kan i princippet benytte TeleSeC.

Det kritiske element i anvendelse af ethvert kryptografisk system er hemmeligholdelsen af den kryptografiske nøgle. Derfor kan TeleSeC med fordel implementeres som en "client-server"-løsning, hvor TeleSeC installeres på en dedikeret "server", som beskyttes yderligere.

TeleSeC kan også leveres i forskellige assembler versioner, der er specielt udviklet til forskellige processortyper såsom 8086 og 80386. Herved opnås en betydelig forbedret performance.

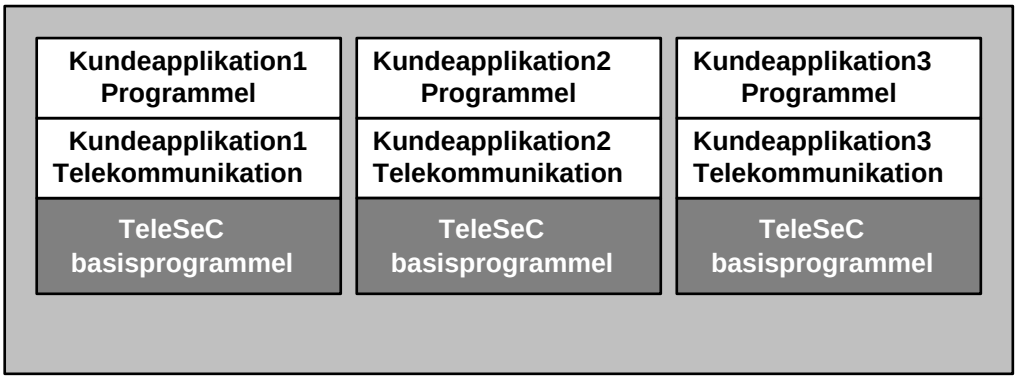
4.3 TeleSeC-opbygning

TeleSeC er en totalløsning, som omfatter dels en overordnet sikkerhedsarkitektur med protokoller, der understøtter oprettelses- og certificeringsproceduren, dels softwaremoduler, der fremstiller de nødvendige sikkerhedsservices, men også et komplet sæt af retningslinier og procedurer for, hvorledes sikkerhedssystemet skal administreres.

TeleSeC er velegnet til at beskytte alle former for data, hvor en høj sikkerhed er påkrævet. TeleSeC kan anvendes i alle brancher, hvor man i dag tillægger den almindelige håndskrevne underskrift og dokumenternes ægthed en stor værdi. Som eksempler kan nævnes finansielle transaktioner, personlige oplysninger i den offentlige forvaltning, handelstransaktioner og dokumenter samt regnskabsoplysninger.

TeleSeC er udviklet med udgangspunkt i den finansielle sektor, men der er intet i det aktuelle design, som begrænser systemet til denne sektor. TeleSeC er i meget vid udstrækning udviklet på baggrund af nationale og internationale standarder.

TeleSeC-basisprogrammel udgør TeleSeC's sikkerhedsmoduler, som anvendes af brugerapplikationerne via standardiserede API-funktioner (grænseflade-funktioner). Standard-kommunikationsprogrammellet vil variere afhængigt af den enkelte installation (Fig. 1). Brugerapplikationer og kommunikationsprogrammel er ikke en integreret del af TeleSeC-konceptet.



4.4 Certifikater

Certifikatets formål

Ved en elektronisk meddelelse medsendes certifikatet som en bekræftelse på afsenderes identitet. Et certifikat er nøglecentrets bekræftelse på oprettelsesinstansens oplysninger om overensstemmelse mellem en brugers identitet og hans elektroniske signatur. Certifikatet vil især finde anvendelse i åbne netværk med kunde-til-kunde kommunikation. I TeleSeC-systemet er anvendelse af certifikater tillige en forudsætning for, at brugerne kan hemmeligholde transmissionen indbyrdes.

Dannelse af certifikat

Certifikatet bliver dannet i forbindelse med oprettelse af en bruger. Oprettelsesinstansen transmitterer brugeroplysninger (akkreditiver) herunder bl.a. en nøglekontrolværdi for den offentlige nøgle til nøglecentret, hvorefter nøglecentret underskriver med sin hemmelige nøgle. Hermed er certifikatet dannet, og nøglecentret transmitterer det tilbage til oprettelsesinstansen, hvorefter brugeren afhenter det elektronisk.

Certifikatets anvendelse

Når en afsender af en meddelelse anvender TeleSeC-programmet, påhæftes afsenderens certifikat automatisk til meddelelsen. Modtageren har dernæst mulighed for at kontrollere certifikatets gyldighed ved at forespørge hos nøglecentret via oprettelsesinstansen. Oprettelsesinstansen får løbende opdateret meddelelser om afmeldinger fra nøglecentret.

Gyldighedsperioden for et certifikat er to år, hvorefter brugeren ved transmission til oprettelsesinstansen kan forny certifikatet.

A- og B-certifikater

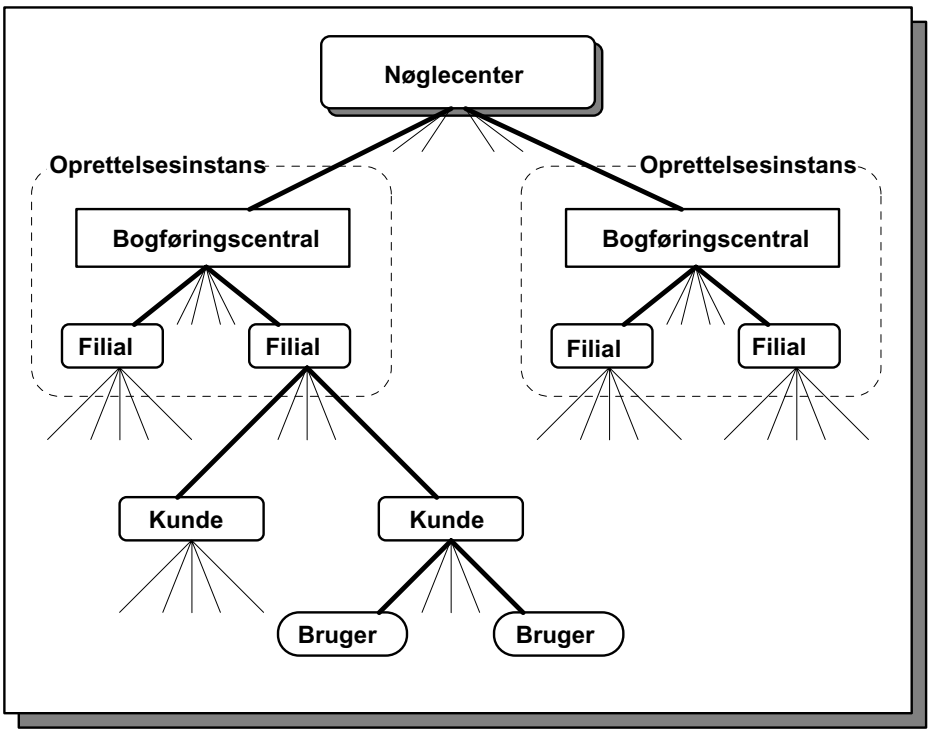
I TeleSeC er defineret to typer af certifikater. Et A-certifikat, som giver mulighed for sikring af kommunikation i et åbent net, og et B-certifikat, som udelukkende kan anvendes mellem en bruger og en oprettelsesinstans.

Hvem skal certificeres?

En virksomhed, som indgår en kontrakt om TeleSeC, vil typisk have et vist antal medarbejdere, som foretager transaktioner med TeleSeC. Der skal oprettes et certifikat til hver enkelt bruger.

TeleSeC-organisation

Hierarkisk set er nøglecentret placeret i toppen af TeleSeC-organisationen. Til nøglecentret er knyttet en række oprettelsesinstanser med tilhørende filialer. Kunden vil typisk være en erhvervsvirksomhed, hvor de enkelte medarbejdere vil være de egentlige TeleSeC-brugere.



TeleSeC-nøglecenter

Nøglecentret er den certificerende myndighed, som har ansvar for at certificere TeleSeC-brugere og administrere certifikater. Nøglecentrets funktioner er:

- Fremstilling og fremsendelse af certifikater
- Fornyelse af certifikater
- Modtagelse af spærringer på certifikater
- Fremsendelse af liste over spærrede certifikater til oprettelsesinstanser
- Fremsendelse af svar på forespørgsler på certifikater
- Opbevaring af softwareprogrammer, som oprettelsesinstanserne har distribueret til brugerne.
- Distributør af TeleSeC-kontrolprogram

TeleSeC-oprettelsesinstans

Oprettelsesinstansen er den myndighed, som har ansvar for registrering og godkendelse af TeleSeC-brugere på vegne af nøglecentret. Oprettelsesinstansens funktioner er:

- Registrering og godkendelse af brugere som TeleSeC-brugere.
- Kommunikationsforbindelse mellem en bruger og nøglecentret.
- Distributør af TeleSeC-programmer til brugere.

Der kan tilsluttes et vilkårligt antal oprettelsesinstanser til TeleSeC nøglecenter.

TeleSeC-bruger
TeleSeC-brugeren er den medarbejder i virksomheden, som er blevet godkendt til at foretage transaktioner på firmaets vegne med brug af TeleSeC. Brugerens funktioner er:

Generel administration af nøgler (certifikater).
Sikring af datakommunikation med digital signatur og kryptering.

Der kan tilsluttes et vilkårligt antal TeleSeC-brugere i certificeringsorganisationen.

5. Nye forslag til sikkerhed

5.1 Digital signatur

Det primære element i SJWG's forslag er anvendelse af digital signatur, som har en række sikkerhedsmæssige egenskaber, der gør den særligt velegnet til EDIFACT.

Modtageren af en forsendelse kan på baggrund af den digitale signatur, éntydigt afgøre afsenderens identitet, og kontrollere at indholdet af forsendelsen er korrekt.

Signaturen kan yderligere kontrolleres af en uvildig 3. part og derved indgå i en eventuel tvist ved bevisførelse. Både afsender og modtager kan bevise, hvad der præcist henholdsvis er sendt og modtaget mellem parterne.

I forbindelse med prokuraforhold som ofte anvendes ved kvittering af betalingstransaktioner m.v., åbner standarden endvidere mulighed for, at en forsendelse kan indeholde flere digitale signaturer. De enkelte medarbejdere skal i givet fald hver have en digital signatur.

Princippet i SJWG's forslag består af to forskellige implementeringsmuligheder. Enten kan den eksisterende EDIFACT-forsendelse udbygges med sikkerhedsinformationer i form af nye segmenter med den såkaldte “header og trailer” metode, eller også kan signatur og EDIFACT-forsendelsen sendes uafhængigt af tid i to separate forsendelser ved hjælp af servicemeddelelsen AUTACK.

5.2 "Header og trailer" metoden

Forsendelses-header (UNB) Sikkerheds-header (USH) Meddelelses-header (UNH) *Én eller flere meddelelser, f.eks. PAYEXT* Meddelelses-trailer (UNT) Sikkerheds-trailer (UST) Forsendelses-trailer (UNZ)

Sikkerhedsinformationerne i en EDIFACT-forsendelse placeres i dette tilfælde efter den såkaldte "header og trailer" metode. Fordelen ved denne løsning er, at den kan implementeres uden ændringer i de eksisterende meddelelser.

Sikkerheds-headeren indeholder information om f.eks. afsenders identitet, anvendte sikkerhedsmekanismer og -algoritmer samt verifikationsidentifikationer for sikkerhed.

Sikkerheds-traileren indeholder information om f.eks. den digitale signatur og hash-værdi.

5.3 AUTACK

Med denne servicemeddelelse kan afsenderen henvise til en specifik EDIFACT-forsendelse og foretage en godkendelse/kvittering af denne.

Servicemeddelelsen kan indeholde digitale signaturer og andre sikkerhedsinformationer. Meddelelsen kan enten før, samtidig med eller efter forsendelsen afsendes til pengeinstituttet. Fremgangsmåden med separat forsendelse af AUTACK kan anvendes, hvis afsenderen f.eks. ønsker at afsende sine EDIFACT-betalingstransaktioner på et tidspunkt, hvor de endnu ikke er prokuramæssigt godkendt. Efterfølgende kan de nødvendige digitale signaturer m.v. for det gældende prokuraforhold afsendes, hvorefter betalingstransaktionerne godkendes til videre ekspedition i pengeinstituttet.

AUTACK er ikke beskrevet i denne vejledning, fordi meddelelsen har nogle mangler.

Der kan ikke sikres:

- hemmeligholdelse
- kompression
- nøgleadministration samt nøgleudveksling
- afmelding af certifikater