SÄKERHETSFRÅGOR I TULLVERKETS EDI-SYSTEM

1 Loggning

All information som går via TMF (Tullverkets Mottagningsfunktion) loggas där och blir sökbar inom vissa gränser.

TMF för en noggrann journal över alla trafikhändelser. Journalen är främst till för att kunna hjälpa uppgiftslämnare i situationer där det uppstått oklarhet i vad som skett i kommunikationen med TES (Tullverkets EDI-system).

Direkt efter det att en fil mottagits av TMF, sker en säkerhetsarkivering av filen. Arkivet är tekniskt utformat för maximalt skydd mot förlust eller förvanskning av innehållet.

Arkivets uppgift är att utgöra en referenspunkt vid en eventuell tvist om vad som skickats till eller från Tullverket (juridiskt gränssnitt mot Tullverket). Loggning hos företaget är inte något krav. Den loggning som sker hos TMF och åsättande av sigill anses uppfylla de krav på bevisning som kan komma att ställas vid en eventuell tvist.

Däremot kan företaget ha intresse för att skapa en händelselogg av vilken framgår vilka tull/transitärenden (tullid) som ingått i respektive dataöverföring.

2 Sigillering, allmänt

Den personliga namnteckningen på ett enhetsdokument ska i det elektroniska dokumentet ersättas av ett "elektroniskt sigill". Sigillet ska produceras genom en metod som är godkänd av Tullverket.

Föreskrift om detta finns i 12 § tullagen (1994:1550). För tillämpningen av denna föreskrift gäller följande fyra grundregler.

A. Dokumentets innehåll måste låsas genom en teknisk metod.

B. Dokumentets utställare (personanknutet) måste kunna identifieras med en teknisk metod.

C. Enbart lösenord ger inte ett tillräckligt äkthetsskydd för dokument i TES, vilket ställer krav på ett kortbaserat BKS (BehörighetsKontrollSystem) hos företagen.

D. Utställaren måste ha möjlighet att kontrollera innehållet i dokumentet innan han åsätter det elektroniska sigillet samt vidtaga någon medveten fysisk åtgärd när han godkänner densamma (t.ex. knapptryckning).

Det ankommer på respektive företag att svara för att ifrågavarande krav uppfylls.

Den teknik som f n tillämpas är elektroniskt sigill. Det elektroniska sigillet (utställarsigillet) är en sifferkombination som erhålls genom att med hjälp av en **hemlig** utställarsigillnyckel kryptera en meddelandekontrollsumma (dokumentsigill). Dokumentsigillet beräknas med hjälp av en **öppen** nyckel. Vilka delar av meddelandet som används för att skapa ett dokumentsigill preciseras närmare i punkt 5, Beräkning av dokumentsigill. Sigillet består efter komprimering, från 18 numeriska tecken, av 6 numeriska tecken.

3 Sigilleringsprocedurer

Tillvägagångssättet för att anbringa sigill kan variera med hänsyn till sigilleringsfrekvensen hos företagen, t.ex.

- Manuell knappning av sigillinformation via en fristående sigillator.
- Inbyggd sigillering kombinerad med BKS och engångslösen, beräknat i fristående sigillator.
- Inbyggd sigillering och terminal försedd med kortläsare samt tillfredsställande BKS.

Det enklaste sättet att använda sigilleringsfunktionerna är att ha en fristående sigillator i anslutning till datorn där arbetet utförs. Förfarandet innebär dock att för varje ärende dokumentsigill och utställarsigill på vardera 6 tecken knappas in . Vid stor ärendemängd är denna procedur betungande.

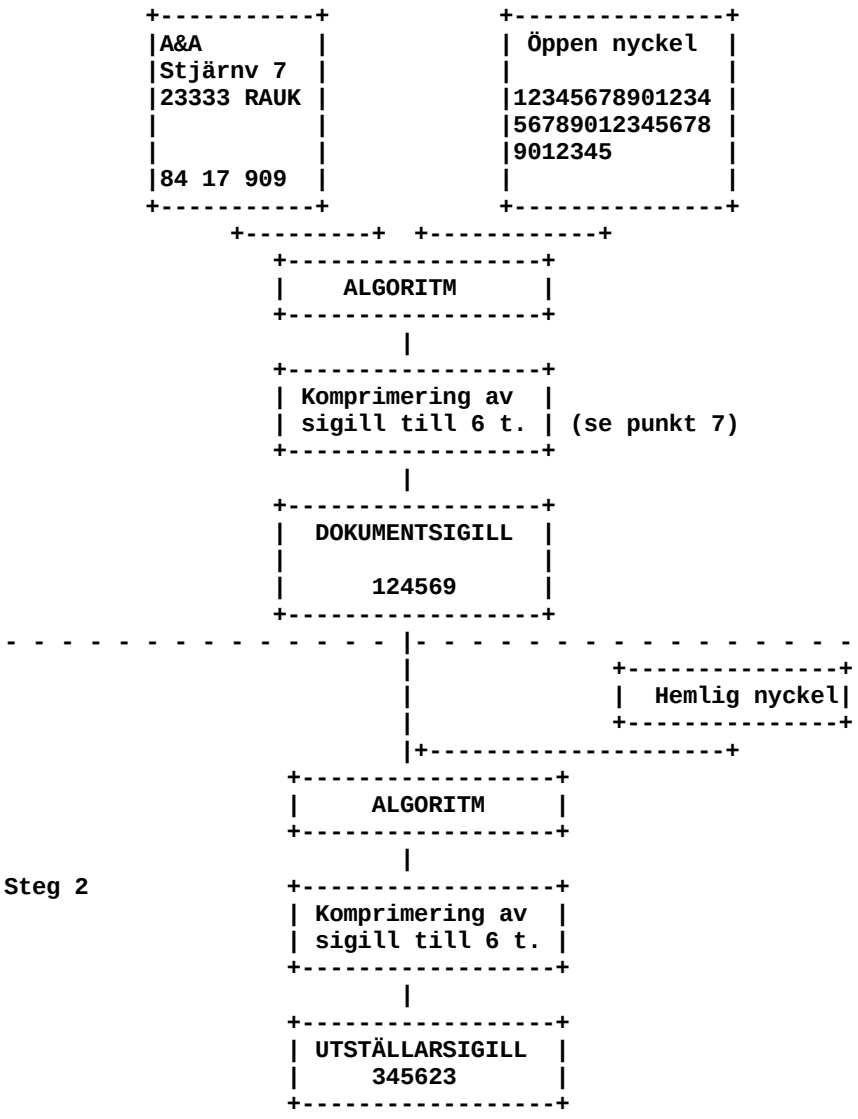
"Inbyggd sigillering med engångslösen" - med hjälp av en sigillator och ett smartcard vid inloggningen kan den personliga koden läsas in till systemet och utnyttjas tills utloggning sker. Detta alternativ är mer praktiskt. De behörighetskort som tillhandahålls av Tullverket kan utnyttjas.

Det finns terminaler med funktion att läsa kort. I kombination med ett betryggande BKS är detta en framkomlig väg. Det bör dock noteras att Tullverket endast tillhandahåller behörighetskort som kan läsas av sigillatorer av typen Safepad. Andra typer av kort måste företaget själv bekosta.

Beskrivning steg för steg

Steg 1. Dokumentsigill beräknas. Det utgör en kontrollsumma som beräknas med hjälp av en algoritm och innehållet i ett meddelande, se punkt 5.

Steg 2. Utställarsigillet beräknas. Det utgör en kontrollsumma som beräknas med hjälp av det 6-ställiga dokumentsigillet, den hemliga sigillnyckeln och en algoritm.



4 Utrustning för sigillering

4.1 Sigillprogramvara

För att kunna genomföra sigilleringen behöver företaget en speciell sigillprogramvara som kan köpas genom den ordinarie leverantören. Sigillprogramvaran ska vara avsedd för sigillering enligt ovan beskriven procedur. SÄKDATA:s sigillmetod är godkänd av Tullverket och implementerad i TES. Sigillprogramvara tillhandahålls av Technology Nexus AB (nexus.se) företag som är intresserade av denna sigillprogramvara bör vända sig direkt till Nexus och kan ta kontakt via e-post (info.sigillet@nexus.se) eller telefon (013-35 74 00).

4.2 Sigillator

Sigillatorn är en fristående enhet som kan användas för beräkning av utställarsigill eller engångslösen. Sigillatorer tillverkas av Steria AB (Tel. +46 8 622 42 00 Fax. +46 8 622 42 23). Vid beställningen måste det anges att sigillatorn ska användas för framställning av "tullsigill". Sigillatorn är en enhet till vilken man använder ett aktivt behörighetskort.

4. 3 Behörighetskort (Smartcard)

Den hemliga sigillnyckeln levereras från Tullverket i ett "aktivt" behörighetskort, s.k. smartcard, i skriftlig form eller i skriftlig form och i kort. Behörighetskort tillhandahålls utan avgift från Tullverket. Smartcard skiljer sig från andra typer av behörighetskort genom att de är försedda med beräkningskapacitet i den mikroprocessor som finns i kortet. Kortet innehåller bl.a. den hemliga sigillnyckeln som beskrivs nedan.

Den typ av behörighetskort som tillhandahålls av Tullverket kan läsas av sigillatorer av typen Safepad. Ytterligare specifikation på korttyp kan erhållas av Interna System hos Tullverkets IT-avdelning.

5 Beräkning av dokumentsigill

För beräkning av dokumentsigill finns två varianter, där skillnaderna består i vilka delar av meddelandet som används för att beräkna dokumentsigillet. Olikheterna beror på den utveckling som skett inom standardiseringen för applicering av digitala signaturer.

5.1 För TDR041 gäller

- Beräkning av dokumentsigill ska göras på **all** tullinformation som finns lagrad i ärendet på EDIFACT-format. Informationen ska omfatta segment UNH till UNT (dvs UNT ska inte ingå). Exakt den tullinformation som finns i EDIFACT-formatet ska gälla.

- Beräkningen ska inte omfatta information som hör till EDIFACT-syntaxen, dvs segmentnamn och EDIFACT-avskiljningstecken. Kvalificerare som definieras i tullmeddelanden, t ex "EX" för exportör ska inkluderas i den information som sigilleras.

- Före beräkningen av dokumentsigill, ska utrymmet för dokumentsigill (6 tecken) och utrymmet för utställarsigill (6 tecken) vara nollutfyllda. De ingår i sigillberäkningen.

5.2 För TDR007, TDR050 och Transit gäller

- Beräkning av dokumentsigill ska göras på **alla** tecken som ingår i meddelandet på EDIFACT-format mellan en start- och stopp-punkt i meddelandet.
- Start- och stopp-punkt för dokumentsigillets beräkning specificeras med kvalificerare i EDIFACT- dataelementet USH/0541 (Scope of security application, coded), se relevant regelverk.

5.3 För båda varianterna gäller

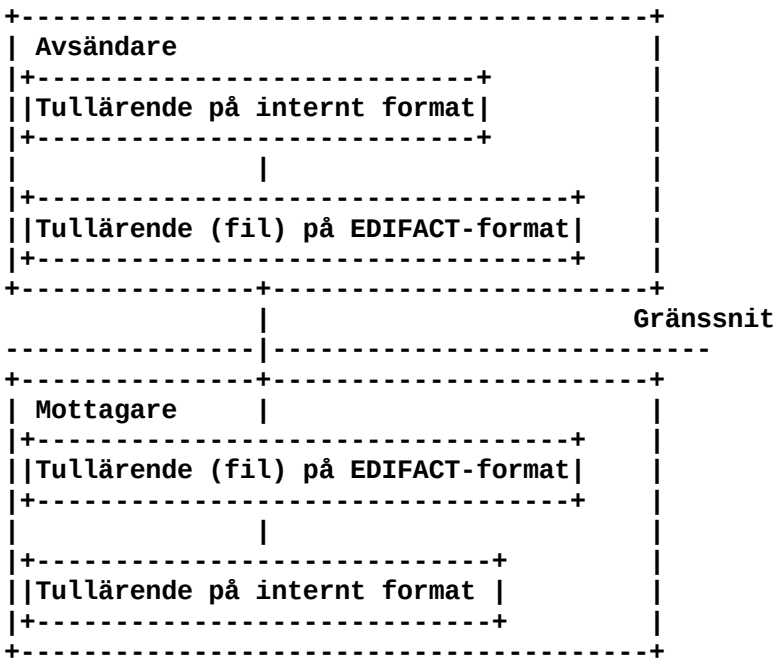
- Vid beräkningen gäller ordningsföljden för informationen enligt den aktuella EDIFACT-filen som den är definierad i regelverket.

- Det 18-siffrors sigill som produceras av sigillprogramvaran ska komprimeras till 6 siffror, se punkt 7.

6 Gränssnitt avsändare/mottagare

I praktiken kommer avsändarens tull/transitärende i regel först att finnas på ett internt format. Detta format omvandlas före överföring till EDIFACT-format varefter mottagaren tar emot filen på EDIFACT-format och omvandlar den tillbaka till ett internt format.

För att få ett sigilleringsförfarande som är tillfredsställande ur såväl juridisk som teknisk synpunkt måste ett klart gränssnitt finnas mellan avsändare och mottagare där det definieras vilken information som ska omfattas av dokumentsigillet.



Gränssnittet mellan avsändare och mottagare är de EDIFACT-formaterade ärenden som överförs mellan dessa. Avsändaren vet exakt vad han sänder iväg och mottagaren erhåller exakt vad som sänds (före teckenomvandling). Vid eventuell diskussion om vilken part som har gjort en felaktig implementering kan båda parter utgå från exakt samma information.

För TDR041 kan det vara värt att notera att gränssnittet inte lägger några synpunkter på var och hur dokumentsigillet beräknas vid överföring. Genom att ingen EDIFACT-syntax ingår i informationen att sigillera, finns t.ex. möjligheter att göra sigillberäkningarna mot ett eget internt format, i stället för EDIFACT-formatet. Korrigeringar av elementinnehåll kan då vara nödvändiga innan elementet lämnas till sigillering, eftersom EDIFACT-produkterna i vissa

fall tillför/tar bort inledande nollor, avslutande blanktecken mm för element som definierats med variabel elementlängd.

När dokumentsigillet beräknats erhålls ett dokumentsigill som består av 18 tecken. Dessa 18 tecken ska sedan komprimeras till 6 tecken och föras på dokumentet. Samma förhållande gäller utställarsigillet, som beräknas på dokumentsigillets 6 siffror.

7 Komprimering av sigill

Det 18-ställiga sigillet ska komprimeras till 6 tecken

Följande gäller för komprimering av såväl dokumentsigill som utställarsigill.

Algoritm för komprimering

Tag de tre första (pos 1-3) siffrorna i sigillet och lägg dessa i en arbetsarea.
Addera de 6 nästa (pos 4-9) siffrorna i sigillet till arbetsarean.
Om resultatet blev större än 999 999 subtrahera då 1 000 000 från arbetsarean.
Addera därefter de 6 nästa (pos 10-15) siffrorna i sigillet till arbetsarean.
Om resultatet blev större än 999 999 subtrahera då 1 000 000 från arbetsarean.
Addera till sist de tre sista (pos 16-18) siffrorna i sigillet till arbetsarean.
Om resultatet blev större än 999 999 subtrahera då 1 000 000 från arbetsarean.
De 6 sista positionerna i arbetsarean innehåller nu det komprimerade sigillet.

8 Sigilleringsnycklar

Den hemliga sigillnyckeln som distribueras av Tullverket är av två olika slag beroende på sigillberäkningsmetod. Den finns antingen i klartext på papper eller inlagd i ett behörighets-kort. Det ankommer på företaget att se till att sigillnycklarna hålls hemliga och inte vid något tillfälle kan komma till obehörigs kännedom. Nycklarna har en begränsad giltighetstid. Tullverket distribuerar nya nycklar före utgången av giltighetsdatum för de gamla.

Utskrivna nycklar skickas med post till säkerhetskontaktpersonen hos företaget. De aktiva korten sänds till utställaren i ett brev och den personliga koden i ett annat brev med några dagars mellanrum.

Den "öppna" nyckeln, som för närvarande används för beräkning av dokumentsigill, har formatet n35 och är: 12345678901234567890123456789012345 (se exempel sid 4). Den hemliga utställarsigillnyckeln har också formatet n35.

Behörighetskort

Behörighetskort innehåller den hemliga nyckeln och innehavarens identitet (anställnings-nummer eller motsvarande). Nyckeln finns gömd på kortet och är skyddad av en personlig kod (PIN-kod) om måste knappas in innan sigillnyckeln kan läsas av sigillatorn. Kortet är obrukbart utan kod. Den PIN-kod som satts på kortet av tullverket bör snarast bytas av innehavaren.

Om ett behörighetskort förkommer eller förstörs på grund av upprepat felaktig PIN-kod eller på annat sätt ska företaget omedelbart kontakta Tullverket Huvudkontoret/Tullprocedursektionen, tfn 0771-520 520. När användaren ska ta ett nytt behörighetskort i bruk är det viktigt att anvisningarna från leverantören följs i detalj. Bl.a. gäller för sigillatorn att användaren som första åtgärd ska byta "PIN-kod". Det är också mycket viktigt att inte ta ut kortet för tidigt ur apparaten. Kortet kan då bli blockerat.

Ansvar för kort och lämnade uppgifter

Den som innehar behörighetskort för tull/transitändamål är ansvarig för att kortet inte används av annan person än han själv. Var och en som erhåller behörighetskort ska vara medveten om detta.

9 Sigillering kombinerad med engångslösen

9.1 Syfte

Många företag med olika ADB-system avses samverka med TES. Tullverket kan inte ta fram konkreta lösningar för dessa, utan det ankommer på företagen att utforma sina egna detaljlösningar.

Nedan ges ett exempel på en praktisk lösning för sigillering av tull/transitdokument. Exemplet innebär små investeringar i utrustning och liten påverkan på företagets normala rutiner. Avsikten är att detta exempel bör kunna tjäna som utgångspunkt för företaget när det ska utarbeta en egen specifik lösning.

Det förutses att företagen kommer att behöva modifiera den föreslagna lösningen, och exemplet pekar därför särskilt på några områden där vi förutser variationer.

9.2 Exempel på hur inbyggd sigillering kan utformas

För detta exempel förutsätts att:

- Företagets BKS-system använder endast lösenord eller annan enkel användaridentifiering, men att BKS-systemet modifieras för att klara nedanstående beskrivning

- Företaget anskaffar fristående sigillator, som kan utnyttjas en gång per påloggningstillfälle, varför varje medarbetare som arbetar med tull/transitgodkännande bör ha en sådan sigillator inom "gångavstånd"

- Företaget har ett väl dokumenterat totalt ADB-säkerhetsskydd som uppfyller allmänt accepterade krav

- Företaget utnyttjar TES sigilleringsprinciper, sigillprogramvara och behörighetskort för att höja säkerhetsnivån när det gäller användarverifiering

- Företaget har en funktion med automatisk avloggning när användaren är inaktiv i systemet. Tidsparametern för denna avloggningsfunktion ska inte vara längre än 30 minuter.

9.3 Handläggarintroduktion

När ny handläggares utställarnyckel ska införas i ADB-systemet bör detta ske i en rutin som utförs av säkerhetsansvarig tillsammans med ett vittne. Det är en fördel om den nye handläggaren själv fungerar som vittne. Rutinen bör genomföras på terminal som har en från obehörig avlyssning skyddad förbindelse med datorn, s k konsolterminal. Den säkerhetsansvarige medför det av Tullverket förseglade kuvertet med utställarsigillnyckel. Behörighetskort har samtidigt distribuerats direkt till handläggaren från Tullverket.

Den säkerhetsansvarige verifierar sin identitet på en terminal och ger sedan transaktionskoden för "ny hemlig nyckel". Säkerhetsansvarig anger handläggarens användaridentitet.

Vittnet öppnar kuvertet och matar in den hemliga utställarsigillnyckeln och utställarens identifieringsnummer till datorn. ADB-systemet skriver sedan över eventuella temporärlagringsareor.

Inläggning av utställarsigillnyckel noteras med anteckning om tid och närvarande personer i ett enkelt protokoll som undertecknas av de närvarande. Kuvertet med utställarsigillnyckel förstörs eller återförseglas för förvaring på säker plats. I det senare fallet bör åtkomstrutinen kräva två personers närvaro för att ett kuvert ska vara åtkomligt.

Berörd handläggare ska, i den mån han ej är närvarande vid inläggningen, underrättas om att hans utställarsigillnyckel lagts in i systemet.

9.4 Handläggarens inloggning i ADB-systemet (engångslösen)

Handläggaren loggar in i ADB-systemet på normalt sätt. BKS-systemet läser i sin användartabell att handläggaren är godkänd för att arbeta med "tull/transitrutiner". Användaren får ett "6-siffrigt slumptal på skärmen (ett tal som kan bildas av sista siffran i årtal, tresiffrigt dagnummer och hundradelarna i sekunden för påloggningstillfället) eller ett löpnummer.

Om handläggaren inte tänker använda sigilleringsrutiner svarar han/hon med "Enter", och är därmed en vanlig användare utan tillstånd att använda sigilleringsrutiner.

Om handläggaren tänker godkänna tull/transitdeklarationer antecknar han/hon det sexsiffriga talet och beger sig till en (fristående) sigillator, stoppar in kort och anger PIN-kod. Därefter matas det sexsiffriga talet in. Sigillatorn krypterar detta svar och anger resultatet i sifferfönstret.

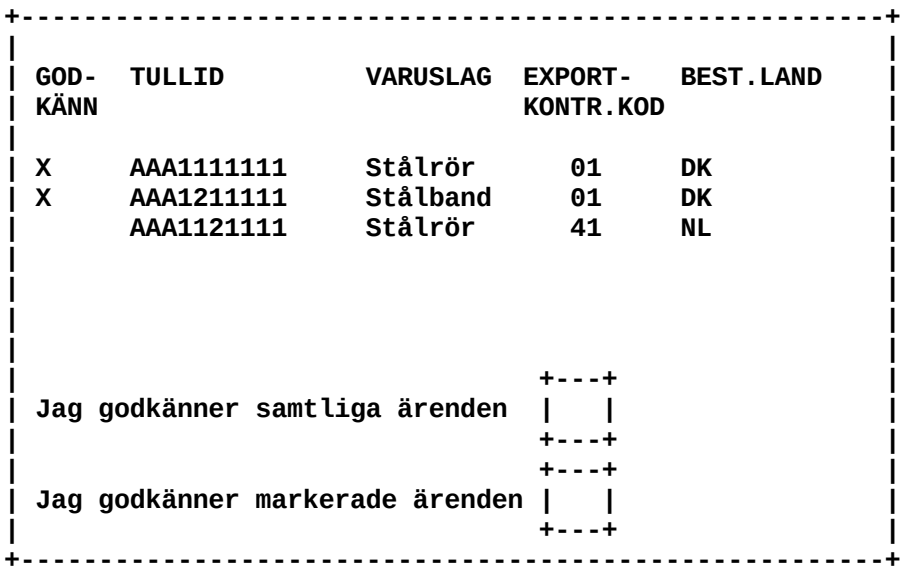
Handläggaren matar in talet på sin dataterminal. ADB-systemet hämtar handläggarens hemliga nyckel ur skyddad area i ADB-systemet och applicerar samma krypteringsalgoritm på det ursprungliga sexsiffriga talet. Om resultatet är samma som användaren matade in godkänns handläggaren med angiven identitet som användare av rutiner för sigillering av tull/transitdokument. Om inte uppmanas han/hon att mata in det krypterade talet en gång till varefter proceduren upprepas.

Den dataterminal som inloggning skett på avses nu användas av identifierad handläggare till dess avloggning sker.

9.5 Handläggarens godkännande av dokument

Den information som ska skickas till TES kan presenteras i samlad form på handläggarens dataterminal, men handläggaren ska ha möjlighet att kunna se ärendet i sin helhet.

Handläggaren kan markera ärende för ärende eller om samtliga ärenden på skärmen godkänns ange detta på lämpligt sätt. (se bild)



9.6 Datorsystemets hantering av godkänt ärende

I direkt anslutning till handläggarens godkännande tillfogar ADB-systemet utställarsigill genom att

- Lägga in handläggaridentitet ur BKS-systemets skyddade användarregister på avsedd plats i ärendet.
- Räkna fram dokumentsigill med hjälp av öppen nyckel.
- Hämta rätt hemlig utställarnyckel ur av BKS-systemet skyddat register, räkna fram utställarsigill och lägga det på avsedd plats.
- Skriva över eventuella temporärt utnyttjade areor så att utställarens hemliga nyckel ej blir åtkomlig för obehöriga.

Dokument överförs till TES via TMF.