Tullverket

Riktlinjer och anvisningar avseende säkerhet vid informationsutbyte via EDI

Version 2.0

2011-06-16

Innehållsförteckning

1 Inledning ... 5
1.1 Tullverkets säkerhetskoncept för EDI ... 5
1.2 Dokumentets syfte, avgränsning och användning ... 6
1.3 Juridisk bakgrund ... 6
1.4 Ansvar för uppgiftslämnandet ... 7
1.5 Kategorier av elektroniska dokument ... 7
1.6 Några använda begrepp ... 8

2 Översiktlig beskrivning av säkerhetskonceptet ... 9
2.1 Konceptuell beskrivning ... 9
2.2 Elektronisk signatur ... 11
2.3 PKI ... 12
2.4 Signeringscertifikat ... 12
2.5 Certifikatutfärdare (CA) ... 12

3 Anmälan av kontaktperson för signeringscertifikat ... 14

4 Beställning, leverans och spärrning av signeringscertifikat ... 15
4.1 Beställning och leverans ... 15
4.2 Underlag för skapande av CSR-fil ... 17
4.3 Spärrning ... 18

5 Krav på företagets tullsystem ... 19
5.1 Hantering av signeringsnyckel ... 19
5.2 Användaridentifiering och behörighetskontroll ... 19
5.3 Godkännande och signering av uppgiftslämnandet ... 20
5.4 Signaturkontroll vid mottagning ... 21

6 Säkerhetsimplementering för EDIFACT-formatet ... 22
6.1 Signeringsprocessen ... 22
6.2 Algoritmer för checksumma och elektronisk signatur ... 24
6.3 Att tänka på vid hantering av binära tal ... 24

7 Bilaga A: Certifikat - teknisk beskrivning ... 25
7.1 Certifikathierarki ... 25
7.2 Rotcertifikat ... 26
7.3 CA-certifikat ... 27
7.4 Signeringscertifikat ... 28
7.5 authorityKeyIdentifier ... 29

8 Bilaga B: CSR-fil – Beskrivning och exempel ... 30
8.1 OpenSSL ... 31
8.2 Windows certreq ... 34
8.3 Java ... 35

9 Bilaga C: Hexadecimal- och Base64-kodning ... 36
9.1 Hexadecimal kodning ... 36
9.2 Base64-kodning ... 36

Uppdateringar från version 1.0 till 2.0 av dokumentet

AVSNITT	KOMMENTAR
Avsnitt 1.5	Text för kategori 2 har uppdaterats.
Avsnitt 4.1	Redigering och förtydliganden.
Avsnitt 4.2	En förklaring har införts via fotnot avseende certifikatfältet ”serialNumber”.
Avsnitt 5.1	Nytt stycke har tillkommit i slutet av krav 1. Fotnoten avseende tvåfaktorslösning har förtydligats.
Avsnitt 6	Avsnitt 6 har redigerats och förtydligats, bland annat angående nyckellängd, referenser till RFC 3447 samt delfält keyIdentifier till authorityKeyIdentifier.
Bilaga A	Bilaga A har kompletterats med beskrivning, format och innehåll för certifikaten.
Bilaga B	Bilaga B har kompletterats med exempel på hur CSR-fil kan skapas från några vanliga datormiljöer.

1 Inledning

1.1 Tullverkets säkerhetskoncept för EDI

Säkert informationsutbyte via EDI[1] innebär att utfärdaren av informationen säkert kan identifieras och att informationen kan skyddas mot förändringar och transporteras via säker kommunikation[2].

För det elektroniska informationsutbytet via EDI har Tullverket sedan början av 1990-talet använt ett säkerhetskoncept baserad på Säkdatas sigillmetod (senare benämnd Nexus Elektroniska Sigill) för att ersätta personlig namnteckning. Till denna finns även regelverk med riktlinjer och anvisningar som styr användningen[3].

Från och med år 2010 har Tullverket ett PKI-baserat säkerhetskoncept för det elektroniska informationsutbytet via EDI. Det PKI-baserade säkerhetskonceptet för EDI, i dokumentet förkortat till ”säkerhetskonceptet”, kommer att införas successivt och till en början kan den gamla lösningen användas parallellt med den PKI-baserade lösningen.

Några utmärkande skillnader mellan de båda lösningarna beskrivs nedan:

PKI-baserad lösning	**Äldre lösning (Nexus Elektroniskt Sigill)**
Låsning av uppgifterna via en signatur utifrån PKI-baserad asymmetrisk krypteringsmetod där endast utställaren har tillgång till den hemliga nyckeln.	Låsning av uppgifterna via ett sigill[4] utifrån symmetrisk krypteringsmetod, där både utställare och mottagare har tillgång till den hemliga nyckeln.
Metod baserad på allmänt spridda standarder.	Leverantörsberoende metod.
Företagen kan själva, utifrån Tullverkets riktlinjer, välja metod för identifiering av användare i företagets system för uppgiftslämning.	Tullverket har konkreta krav på metod för identifiering av användare i företagets system för uppgiftslämnande.
Företagsorienterad nyckel används för signering. Detta innebär att Tullverket säkert kan identifiera företaget men inte direkt utifrån signaturen avläsa individ. Företaget skall dock i vissa fall vid begäran från Tullverket kunna lämna uppgifter om den individ som godkänt det elektroniska dokumentet.	Individorienterad nyckel används för sigillering. Tullverket kan därigenom direkt utifrån sigillet avläsa individ vid förtaget.

[1] Med informationsutbyte via EDI avser vi i detta dokument ett informationsutbyte system till system.

[2] Kommunikationsprotokoll och säkerhet kopplat till dessa ligger utanför Tullverkets säkerhetskoncept för EDI och behandlas inte i detta dokument.

[3] Se bland annat *Säkerhetsfrågor i Tullverkets EDI-system*, 2006-10-04, version1.0

[4] Historiskt har *sigillering* används som begrepp för låsning av informationen via symmetrisk kryptonyckel där både avsändare och mottagare har kännedom om den hemliga nyckeln medan signering används som begrepp för låsningen i den PKI-baserade lösningen.

1.2 Dokumentets syfte, avgränsning och användning

Dokumentet riktar sig till systemleverantörer av standardsystem för informationsutbyte via EDI till Tullverket, företag med motsvarande egenutvecklade tullsystem samt företag som väljer att köpa standardsystem från systemleverantör. Vid systemval och implementering ansvarar det uppgiftslämnande företaget för att uppfylla Tullverkets krav.

Dokumentet omfattar Tullverkets EDI-baserade informationsutbyte system till system och inkluderar inte informationsutbyte individ till system via t ex ett webbgränssnitt. Import- och exportdeklarationer är exempel på vanligt förekommande informationsutbyten via EDI.

Dokumentet beskriver användningen av det PKI-baserade säkerhetskonceptet för informationsutbyte via EDI och har ett fokus på säkerhet och teknik. I dokumentet ställs krav på företagets implementering av tullsystemet för att garantera att överförda elektroniska dokument skyddas och att företaget, samt i vissa fall även godkännande användare, kan identifieras på ett trovärdigt sätt.

Dokumentet innehåller såväl teknikorienterade anvisningar för den tekniska implementeringen som riktlinjer för att skapa tillit till gjord implementering. De teknik-orienterade anvisningarna är uppdelade i en formatoberoende huvuddel samt en formatspecifik del för de olika formaten, inledningsvis EDIFACT.

Val av kommunikationsprotokoll och i kommunikationsprotokollet inbyggd säkerhet i form av kryptering etc. är även viktigt, men beskrivs inte i detalj i detta dokument.

1.3 Juridisk bakgrund

Skriftliga tulldeklarationer ska enligt tullkodex[5] vara undertecknade. När det gäller elektroniska tulldeklarationer ska enligt tillämpningskodex[6] tullmyndigheterna bestämma reglerna för ersättning av den handskrivna namnteckningen. Det ska bl.a. inkludera åtgärder för att kontrollera källan till data och för att skydda data mot risken för obehörig åtkomst, förlust, ändring eller förstörelse. Detta uttrycks i tullagen[7] som att ett elektroniskt dokuments innehåll och utställare ska kunna verifieras genom ett visst tekniskt förfarande.

I den moderniserade tullkodexen[8] sägs att tulldeklarationer som upprättas med hjälp av elektronisk databehandlingsteknik ska innehålla en elektronisk signatur eller annan typ av autentisering.

Andra elektroniska dokument kan komma i framtiden, styrda av annan lagstiftning, vilket kan ställa andra krav på elektronisk signering.

[5] Artikel 62 i förordning (EEG) 2913/92
[6] Artikel 4b i förordning (EEG) 2454/93
[7] 2 kap 2§ i SFS 2000:1281
[8] Artikel 108 i förordning (EG) 450/2008

1.4 Ansvar för uppgiftslämnandet

Om uppgiftslämnaren är en juridisk person undertecknas deklarationen av en firmatecknare eller någon som fått fullmakt att göra detta. Som huvudregel är det styrelsen som tecknar bolagets firma. Verkställande direktören tecknar firman i den löpande verksamheten där inlämnandet av tulldeklarationer får anses ingå. Utöver det kan fullmakt ges för att teckna firma i särskilda fall, t.ex. för att lämna tulldeklaration. En sådan fullmakt kan ges skriftligen, muntligen eller underförstått genom en ställningsfullmakt. Med ställningsfullmakt menas en sådan förtroendeställning som följer med en viss anställning hos företaget.

Legala företrädare för en verksamhet har ett direkt företagaransvar och ansvarar då fullt ut även för sin passivitet. Ansvaret gäller för den tid man är företrädare. Om arbetsuppgifter och befogenheter delegeras kan ansvaret under vissa förutsättningar följa med. En eventuell bedömning av ansvarsfrågan i sådana fall görs utifrån det enskilda fallet.

1.5 Kategorier av elektroniska dokument

I säkerhetskonceptet definieras två kategorier av elektroniska dokument för informationsutbyte mellan företag och Tullverket. Det framgår av respektive tillstånd för informationsutbyte vilken kategori det elektroniska dokumentet tillhör.

Kategori 1 – utan krav på att kunna identifiera fysisk person

Avser elektroniska dokument som inte omfattas av krav på att en behörig användare skall godkänna uppgifterna innan överföring och avsändaren inte vid överföring eller i efterhand behöver identifiera en behörig fysisk person.

Denna kategori av elektroniskt dokument kan således skapas och överföras helt automatiskt i datasystem.

Kategori 2 – med krav på att kunna identifiera fysisk person

Avser elektroniska dokument som omfattas av krav på att en behörig användare skall godkänna uppgifterna innan överföring och Tullverket skall, inte vid överföring men i efterhand, kunna få besked om vilken fysisk person som godkänt uppgifterna.

Metoden för behörighetskontroll, identifiering av behörig användare samt loggning med koppling till användaren och uppgifterna i det elektroniska dokumentet skall uppfylla kraven från Tullverket.

Uppgifterna måste låsas under processen då uppgifterna granskas och godkänns av en fysisk person vars ansvar knyts till uppgifterna som överförs i det elektroniska dokumentet. Denna kategori av elektroniskt dokument kan således inte skapas och överföras helt automatiskt i datasystem.

1.6 Några använda begrepp

	Beskrivning
Firmatecknare	Firmatecknaren i form av t ex VD har det övergripande ansvaret. Vilka som är behöriga firmatecknare, framgår av företagets registreringsbevis. Firmatecknaren kan delegera visst ansvar via fullmakt. Den som delegeras ansvar för tullhantering kallas ibland för tullansvarig. I detta dokument likställs tullansvarig i den fortlöpande texten med en firmatecknare.
Behörig användare	Detta är den person som är behörig att godkänna (elektroniskt underteckna) elektroniska dokument innan de skickas.
Kontaktperson för signeringscertifikat	Är den som beställer, mottar och fortlöpande hanterar signeringscertifikat för informationsutbyte via EDI
Elektroniskt dokument	Med elektroniskt dokument menas här en verksamhetsorienterad vy av dess innehåll utan fokus på dess tekniska format (EDIFACT, XML etc.). Det som signeras är dock det tekniska formatet.

2 Översiktlig beskrivning av säkerhetskonceptet

Det PKI-baserade säkerhetskonceptet innebär att informationsutbytet mellan Tullverket och företagen alltid sker via signerade elektroniska dokument. Vid informationsflöde från företaget till Tullverket används signeringscertifikat utställt på företaget för signering. Vid flöde i motsatt riktning används signeringscertifikat utställt på Tullverket.

Traditionellt ställer ett säkert informationsutbyte via EDI krav på att:

1. det elektroniska dokumentet inte skall kunna förvanskas utan upptäckt
2. ingen skall kunna sända det elektroniska dokumentet i annans namn, avsiktligt eller oavsiktligt utan upptäckt
3. avsändaren inte skall kunna förneka sitt utfärdande och sin sändning av det elektroniska dokumentet
4. mottagaren inte skall kunna förneka sin mottagning av det elektroniska dokumentet
5. det elektroniska dokumentet inte skall kunna läsas av obehöriga

Punkt 1 – 3 hanteras av det PKI-baserade säkerhetskonceptet, punkt 4 löses med krav på signerade kvittenser och punkt 5 löses med krav på kryptering av kommunikationen.

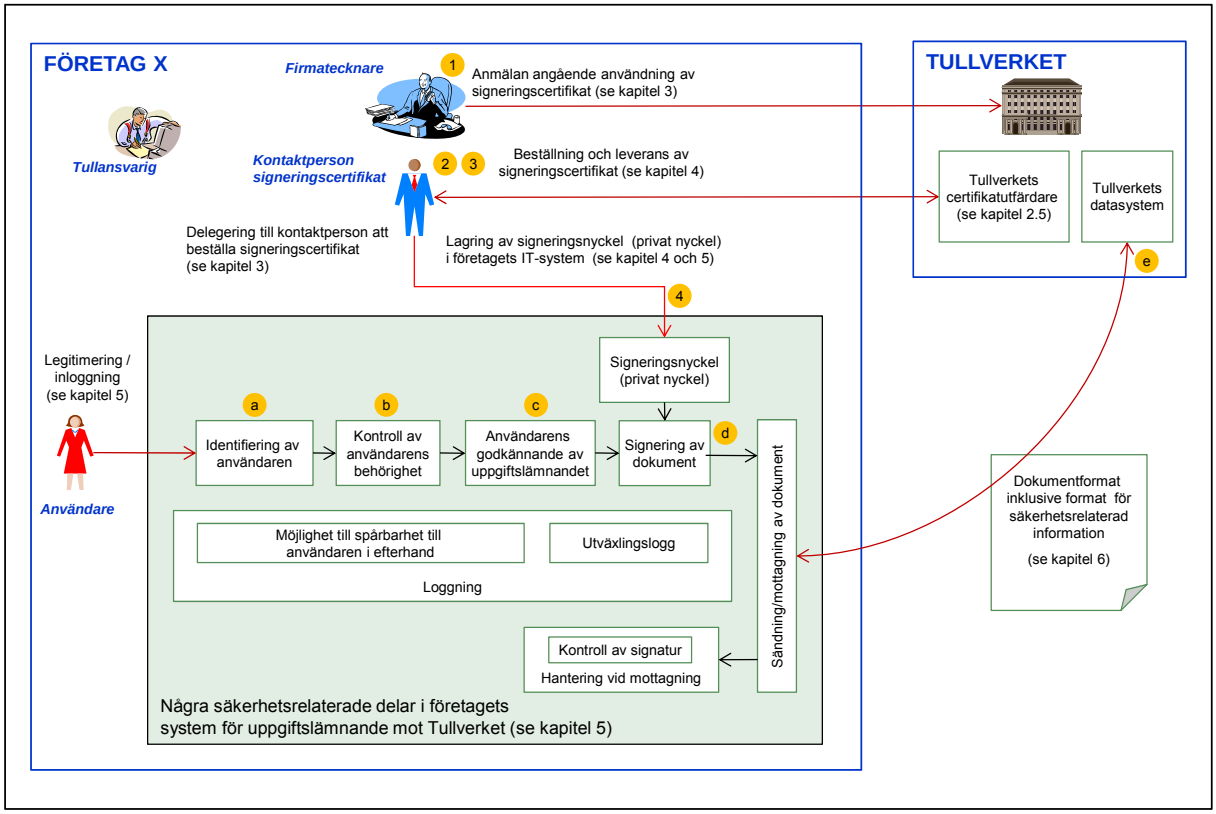
Utöver dessa traditionella EDI-krav ställer Tullverket, för elektroniska dokument av kategori 2, även krav på att identifiera fysisk person.

2.1 Konceptuell beskrivning

I nedanstående bild visas som exempel viktiga delar i säkerhetskonceptet för ett informationsutbyte med elektroniska dokument av kategori 2. Kategori 1 innebär vissa förenklingar eftersom ingen fysisk person behöver identifieras.

Företaget önskar i exemplet deklarera import- eller export elektroniskt till Tullverket och har sökt tillstånd för detta. För att kunna starta det elektroniska uppgiftslämnandet krävs dock tillgång till ett signeringscertifikat.

Hanteringen kan grupperas i en administrativ del för hantering av signeringscertifikat samt en del för användningen av signeringscertifikat i uppgiftslämnandet med Tullverket.



2.1.1 Administrativ hantering av signeringscertifikat

För att kunna starta det elektroniska uppgiftslämnandet krävs tillgång till ett signeringscertifikat vilket möjliggörs via anmälan till Tullverket.

1) I anmälan anges en eller flera kontaktpersoner ut för de fortsatta kontakterna med Tullverket angående signeringscertifikat.

2) Kontaktpersonen beställer signeringscertifikat från Tullverkets tjänst för certifikatutfärdande (CA).

3) Kontaktpersonen ser till att en privat (hemlig) nyckel genereras av företaget och kopplas till certifikatet (se kapitel 4).

4) Den privata nyckeln lagras i företagets system på ett säkert sätt.

För att skapa tilltro krävs att företagets tullsystem har en tillräcklig totalsäkerhet. Detta innefattar bland annat en säker hantering och lagring av privat nyckel kopplad till signeringscertifikatet.

Systemet måste även tillhandahålla spårbarhet via loggning (kategori 2) så att den användare som signerat ett elektroniskt dokument i efterhand kan pekas ut med tillräcklig säkerhet (se kapitel 5).

2.1.2 Användande av signeringscertifikat i uppgiftslämnandet

Hanteringen av uppgiftslämnandet skiljer sig mellan elektroniska dokument av kategori 1, utan krav på att identifiera fysisk person, och kategori 2 med sådant krav.

För elektroniska dokument av kategori 2 gäller:

a) att personen först identifieras

b) att kontroll sedan görs att personen är behörig utifrån dess identitet

c) att det elektroniska dokumentet måste godkännas av den behörige användaren före signering

För båda kategorierna av elektroniska dokument gäller:

d) att det elektroniska dokumentet signeras med företagets signeringsnyckel

e) att kontroll sker av signaturen vid mottagning hos Tullverket

Då Tullverket skickar ett signerat elektroniskt dokument till företaget skall signaturen kontrolleras hos företaget.

2.2 Elektronisk signatur

En signatur på papper kan ha olika innebörd utifrån vad som undertecknas. I sin enklaste form innebär signaturen enbart en markering att en person tagit del av ett dokument. I andra sammanhang, t ex vid ett fastighetsköp, har signaturen/underskriften en betydligt tyngre innebörd i form av oavvislighet. Oavvislighet innebär att personen i efterhand inte kan neka att den via sin underskrift godkänt en transaktion etc.

Den elektroniska signaturen är den elektroniska världens motsvarighet till pappersbaserad signatur eller underskrift. På samma sätt som den pappersbaserade signaturen eller underskriften kan den elektroniska motsvarigheten ha olika funktion beroende på de krav som finns på det elektroniska dokumentet. En synonym till elektronisk signatur är *digital signatur*.

Utmärkande för den signatur som används i Tullverkets PKI-baserade säkerhetskoncept är att den endast är kopplad till företaget, d v s den har ingen direkt koppling till den användare som godkänt uppgifterna. Företaget ska dock för elektroniska dokument av kategori 2 alltid kunna redogöra för vilken fysisk person som har godkänt detta samt, vid begäran från Tullverket, kunna lämna ut uppgift om denna person.

2.3 PKI

PKI i Tullverkets PKI-baserade säkerhetskoncept står för Public Key Infrastructure. Grundläggande för ett PKI-baserat säkerhetskoncept är att mottagande part för sin verifiering inte behöver ha den nyckel som avsändaren använt vid sin signering av det elektroniska dokumentet. För att klara detta har varje part som deltar i informationsutbytet ett unikt nyckelpar med *privat nyckel* som måste hållas hemlig och *publik nyckel* vilken kan publiceras till samtliga parter.

En stark matematisk koppling finns vidare mellan privat nyckel och publik nyckel. Denna koppling gör att en mottagare av ett elektroniskt dokument via den publika nyckeln kan verifiera om det elektroniska dokumentets signatur är framställd av den tillhörande privata nyckeln.

2.4 Signeringscertifikat

Det vi här avser med certifikat är vad som definieras av den internationella standarden X.509. Certifikatet kopplar samman företagets publika nyckel (se 2.3) med företagets namn och annan identitetsinformation. Kopplingen görs av certifikatutfärdaren (se 2.5). För att kopplingen inte ska kunna ändras i efterhand låser utfärdaren certifikatet via en signatur.

Då företaget sänder ett signerat elektroniskt dokument kan Tullverket via företagets publika nyckel verifiera att signaturen verkligen är gjord med företagets privata (hemliga) nyckel. Om så är fallet kan Tullverket via företagets publika nyckel och dess koppling till identitetsinformation i certifikatet säkert veta vilket företag som utfärdat det elektroniska dokumentet. Detta ger möjlighet till oavvislighet för informationsutbyten som kräver detta. På samma sätt kan företagen säkerställa elektroniska dokument som kommer från Tullverket via Tullverkets signatur.

De signeringscertifikat som används vid informationsutbytet mellan företag och Tullverket saknar koppling till individ. Signeringscertifikatet ger endast en koppling till företaget. Denna typ av organisationsorienterat signeringscertifikat brukar även benämnas stämpelcertifikat.

2.5 Certifikatutfärdare (CA)

Tullverket kommer inledningsvis själv att vara certifikatutfärdare (CA) för det PKI-baserade säkerhetskonceptet. Ett motiv till detta är att marknaden idag inte täcker upp hela behovet av utfärdande mot alla företag med önskad funktionalitet. De av Tullverket utfärdade certifikaten är enbart avsedda för signering av elektroniska dokument vid informationsutbyte med Tullverket.

Som angivits ovan i 2.4 är en viktig uppgift för certifikatutfärdaren att koppla samman företagets publika nyckel med företagets namn och annan identitetsinformation samt låsa denna information via en signatur.

För att skapa tilltro måste certifikatutfärdaren även se till så att de uppgifter som läggs på certifikatet verkligen är korrekta. Vid uppgiftslämnandet till Tullverket är det företaget som förser certifikatutfärdaren med dessa uppgifter. Certifikatutfärdaren måste dock förvissa sig om att uppgifterna kan härledas till behörig person (firmatecknare) samt att de oförvanskat når certifikatutfärdaren tillsammans med uppgift om företagets publika nyckel.

3 Anmälan av kontaktperson för signeringscertifikat

Användning av det PKI-baserade säkerhetskonceptet kräver tillgång till signeringscertifikat för signering av företagets elektroniska dokument till Tullverket. Via anmälan ger företaget behörighet till en eller flera kontaktpersoner vid företaget att beställa och administrera signeringscertifikat. Beställning av signeringscertifikat beskrivs i avsnitt 4.

För att få signeringscertifikat krävs att företaget har eller ansöker om tillstånd för visst elektroniskt uppgiftslämnande.

Blankett för anmälan kan hämtas från Tullverkets webbsida. På blanketten skall anges den eller de kontaktpersoner som skall ha rätt att beställa och administrera signeringscertifikat. Blanketten kan även användas för att lägga till nya kontaktpersoner eller ta bort tidigare angivna kontaktpersoner.

Anmälan skall vara underskriven av firmatecknare eller person med fullmakt. Tullverket kan komma att göra kontroll mot Bolagsverkets register eller motsvarande utländska register eller på annat sätt förvissa sig om att anmälan görs av behörig person.

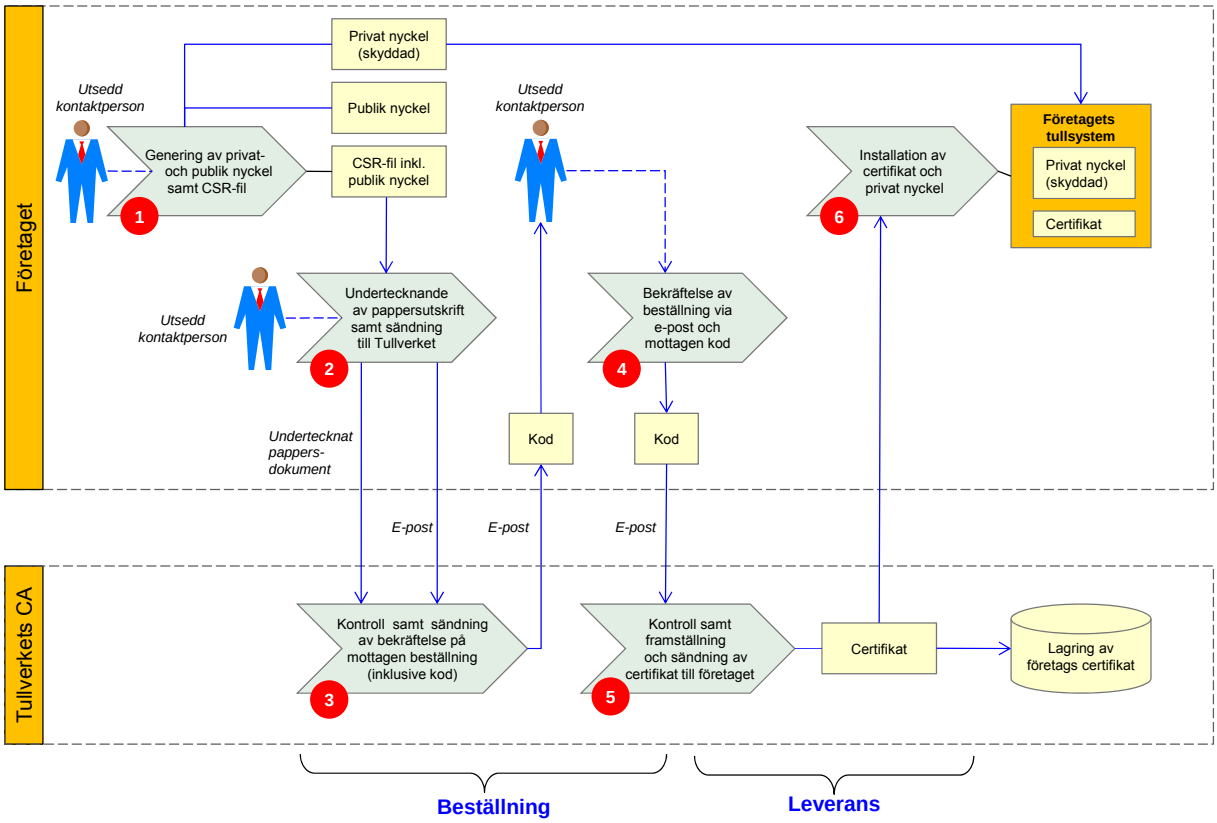
Efter hantering av anmälan sänder Tullverket bekräftelse till företaget på mottagen anmälan och utförda åtgärder.

4 Beställning, leverans och spärrning av signerings-certifikat

De av Tullverket utfärdade certifikaten är enbart avsedda för signering av elektroniska dokument vid informationsutbyte med Tullverket.

Giltighetstid för ett signeringscertifikat är begränsad. Företaget ansvarar självt för att i god tid före giltighetstidens utgång beställa ett nytt certifikat. Överlappande giltighetstider är tillåtet och rekommenderas. Nedanstående beskrivna rutin gäller för såväl nybeställning som efterföljande beställningar.

4.1 Beställning och leverans



Steg 1
Utsedd kontaktperson vid företaget genererar ett nyckelpar med privat och publik nyckel via för detta avsedd programvara. Hanteringen av den privata nyckeln skall ske med beaktande av säkerhetskrav enligt avsnitt 5.

I samband med nyckelgenereringen skapas även en CSR-fil (Certificate Signing Request) innehållande den publika nyckeln och övriga nödvändiga uppgifter.

Steg 2
Kontaktperson för signeringscertifikat ska kopiera in hela texten från CSR-filen in i ett e-postmeddelande och sända det till edi.certifikat@tullverket.se. Företagets namn och EORI-nummer ska anges i e-postmeddelandets ämnesrad.

Hela texten från CSR-filen ska även kopieras in i ett dokument med rubriken "Beställning av signeringscertifikat". Företagets namn och EORI-nummer ska även anges i dokumentet. Dokumentet ska undertecknas av kontaktperson för signeringscertifikat (inklusive namnförtydligande) och skickas per brev till:

Tullverkets IT-avdelning
EDI-certifikat
Aurorum 3
977 75 LULEÅ

Det undertecknade brevet är nödvändigt för att juridiskt kunna koppla kontaktpersonen till det utfärdade signeringscertifikatet.

Det är möjligt för företaget att sända utskriven CSR-fil i samma brev som anmälan enligt avsnitt 3.

Steg 3
Tullverket gör kontroll mot tidigare anmälan angående användning av signeringscertifikat. En bekräftelse av mottagning sänds därefter per e-post till i anmälan tidigare registrerad e-postadress för angiven kontaktperson. I bekräftelsen anger Tullverket kod som ska användas av företaget för att bekräfta beställningen.

Steg 4
I beställningen angiven kontaktperson vid företaget bekräftar per e-post beställningen genom att ange den från Tullverket mottagna koden.

Steg 5
Då Tullverket mottar en korrekt bekräftelse av beställningen från företagets kontaktperson skapar och signerar Tullverket ett X.509-certifikat giltigt från tillverkningstidpunkten och 14 månader framåt utifrån den i CSR-filen mottagna informationen. Certifikatet sparas hos Tullverkets CA samt sänds per e-post till företagets kontaktperson med användning av den i anmälan registrerade e-postadressen.

Steg 6
Företaget installerar mottaget certifikat samt företagets privata nyckel via en process som uppfyller ställda krav i avsnitt 5.

4.2 Underlag för skapande av CSR-fil

I den i föregående avsnitt beskrivna beställningen av signeringscertifikat ska företaget via ett ”Certificate Signing Request” lagrad i CSR-fil förse Tullverket med korrekta identitets-uppgifter. Skapandet av CSR-fil följer vedertagen standard (RFC 2986) och finns implementerad i utvecklingsverktyg för olika datormiljöer såsom Windows, Java etc. Utifrån mottagen CSR-fil framställer Tullverket företagets signeringscertifikat. Signeringscertifikatet lagras hos Tullverket samt sänds till företaget.

I samband med skapandet av CSR-fil genererar företaget sin publika och privata nyckel. Genereringen av signeringsnycklar skall ske på sådant sätt att den privata signeringsnyckeln skyddas mot obehörig åtkomst (se avsnitt 5).

Företagets tullsystem bör tillhandahålla ett användarvänligt gränssnitt för framställning och sändning av CSR-fil så att kontaktpersonen kan hantera detta utan krav på djupa tekniska kunskaper.

CSR-filen ska innehålla följande uppgifter avseende företagets identitet (”subject”):

Attribut	Max längd	Kommentar
countryName	2	Landskod för företaget
organizationName	64	Företagets namn
organizationalUnitName	64	Avdelning inom företaget (frivilligt)
serialNumber[9]	64	Företagets EORI-nummer
commonName	64	Företagets namn i kortare form (frivilligt)

Förutom ovanstående uppgifter ingår även företagets publika nyckel. Se bilagorna A och B för mer information och konkreta exempel.

[9] Observera att ”serialNumber” i tabellen ovan inte avser certifikatets serienummer utan är en del av beskrivningen av den organisation för vilket certifikatet är utställt (”subject”).
Se RFC 5280, avsnitt 4.1.2.4, för ytterligare beskrivning av det i tabellen ovan angivna ”serialNumber”.
I X.520 finns ”serialNumber” definierad med objektidentifierare 2.5.4.5 och typen ”Printable string” (till skillnad från certifikatets serienummer som är av typen ”Integer”).

4.3 Spärrning

Möjlighet finns att spärra certifikat.

4.3.1 Spärrning på initiativ av företaget

Om företaget vet eller misstänker att den privata nyckeln har blivit tillgänglig för andra än behörig inom företaget skall företaget snarast begära att certifikatet spärras.

Företaget har möjlighet att begära spärrning av certifikat utfärdade för företaget genom

- e-post
- fax
- telefon
- brev

Kontaktuppgifter framgår av Tullverkets hemsida, www.tullverket.se
Innan certifikatet spärras kontaktar Tullverket företaget för att verifiera begäran om spärrning.

4.3.2 Spärrning på initiativ av Tullverket

Tullverket har möjlighet att spärra certifikat som Tullverket utfärdat för företag.

Anledning till spärrning kan exempelvis vara misstanke om felaktighet eller att andra tillstånd som informationsutbytet är beroende av dras in.

4.3.3 Publicering av spärrade certifikat

Tullverket kommer att publicera spärrlistor för spärrade certifikat utfärdade av Tullverket. Detta gäller både certifikat utfärdade för Tullverket och för företag.

5 Krav på företagets tullsystem

Företaget skall använda en implementering av det PKI-baserade säkerhetskonceptet i sitt tullsystem för att ge god totalsäkerhet. I detta ingår bland annat att följa nedan angivna krav. Dessa omfattar såväl sändningen av information till Tullverket som mottagningen av information från Tullverket.

Kraven på företagets tullsystem beror på de kategorier av elektroniska dokument som ska överföras. I nedanstående krav anges i kravrutorna via symbolerna ❶ (kategori 1) och ❷ (kategori 2) den/de kategorier som kravet avser. Kategorierna definieras i avsnitt 1.5.

5.1 Hantering av signeringsnyckel

Det elektroniska dokumentets signatur är grunden för såväl dokumentskyddet som en säker identifiering av företaget.

Krav 1 ❶ ❷	Generering och användning av signeringsnycklar skall ske på sådant sätt att den privata signeringsnyckeln skyddas mot obehörig åtkomst. Nya signeringsnycklar skall genereras för varje nytt certifikat och skapas via parametrar som tillgodoser krav på nycklarnas kvalitet. Nyckellängd för RSA-nycklar skall vara enligt bilaga A.

5.2 Användaridentifiering och behörighetskontroll

Utifrån Tullverkets krav väljer företaget självt en säker lösning för identifiering av de användare som avser att godkänna uppgifter för signering. Identifiering är en förutsättning för såväl behörighetskontroll som spårbarhet till användaren i efterhand.

Identifiering

Krav 2 ❷	Användaren, som avser godkänna uppgifter för signering, skall vara identifierad i företagets tullsystem med god säkerhet, vilket innebär krav på minst en tvåfaktorslösning[10].

[10] Typer av faktorer att välja mellan är: Något man vet (t ex lösenord), något man äger (t ex kort eller inloggningsdosa), något man är (t ex fingeravtryck). Med ”något man äger” avses något som enbart användaren disponerar och bär med sig, som även är svårt att kopiera. Magnetkort, ip-adresser och kopierbar lista över engångslösenord uppfyller inte detta krav. En tvåfaktorslösning innebär att man väljer två olika typer av faktorer.

Krav 3 ❷	För att säkerställa identiteten på användaren som skall godkänna uppgifterna för signering, måste förnyad identifiering (enligt krav 2) utföras efter viss tids inaktivitet. Denna tid för inaktivitet utan förnyad identifiering skall hållas kort för att upprätthålla säkerheten i tullsystemet.
Krav 4 ❷	Företaget skall, på begäran från Tullverket, i efterhand lämna identitetsuppgift om den behöriga användare som godkänt ett visst elektroniskt dokument för signering. Det framgår av respektive tillstånd för informationsutbyte hur långt tillbaka i tiden dessa uppgifter ska kunna lämnas.

Behörighetskontroll

Krav 5 ❷	Ett behörighetssystem skall finnas för tullsystemet så att enbart behöriga användare kan godkänna uppgifter för signering.
Krav 6 ❷	Behörighet skall endast kunna registreras av för ändamålet utsedda personer.

5.3 Godkännande och signering av uppgiftslämnandet

Före sändning till Tullverket godkänner användaren uppgifterna i det elektroniska dokumentet. Godkännandet ska resultera i att uppgiftslämnandet ges en signatur som låser uppgifterna samt gör att företaget kan identifieras på ett säkert sätt av mottagaren. Signeringen kan ske direkt vid godkännandet eller vid ett senare tillfälle.

Krav 7 ❷	Före godkännandet av det elektroniska dokumentet skall användaren ges möjlighet att på ett användarvänligt sätt granska alla ingående uppgifter.
Krav 8 ❷	När användare granskar uppgifterna inför godkännande, skall tullsystemet se till att uppgifter som ska sändas till Tullverket inte kan förändras av andra.
Krav 9 ❷	Ett godkännande av uppgifterna för signering kräver att användaren gör en aktiv handling (t.ex. knapptryckning) och görs medveten om att åtgärden motsvarar en underskrift.
Krav 10 ❷	Om signeringen inte sker i direkt anslutning till användarens godkännande av uppgifterna, skall dessa skyddas mot förändring fram till signeringen.

5.4 Signaturkontroll vid mottagning

Normalt är alla elektroniska dokument från Tullverket signerade. Vid mottagning ska dessa signaturer kontrolleras av företaget.

Krav 11 ❶ ❷	Alla elektroniska dokument från Tullverket skall kvitteras, enligt regelverk för aktuellt flöde, för att bekräfta att de har mottagits.
Krav 12 ❶ ❷	Signaturkontroll skall göras av mottagaren för de elektroniska dokument som enligt regelverk för aktuellt flödet ska innehålla signatur.
Krav 13 ❶ ❷	Felaktig signatur eller avsaknad av signatur där sådan förväntas enligt regelverk för det aktuella flödet skall kvitteras med felmeddelande.

6 Säkerhetsimplementering för EDIFACT-formatet

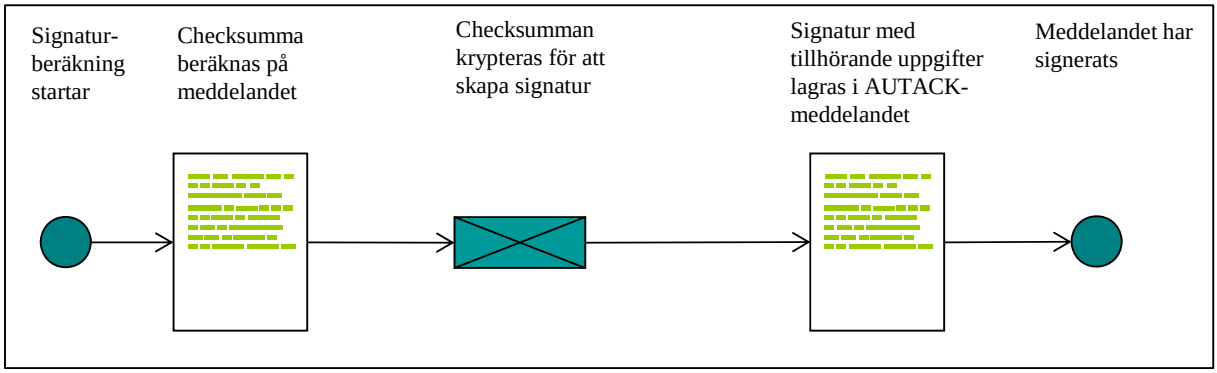
För EDIFACT-formatet gäller att AUTACK-meddelandet används för paketering av signatur-relaterad information.

Regelverk SCTS-SC, som nås via Tullverkets hemsida, beskriver mer utförligt hur den signaturrelaterade informationen hanteras och lagras i AUTACK-meddelandet.

I och med att säkerhetskonceptet är baserat på allmänt stödda standardiserade säkerhets-algoritmer finns i regel bra stöd i alla datormiljöer för implementering av signatur. Implementeringen kan dock se olika ut för olika utvecklingsverktyg.

6.1 Signeringsprocessen

6.1.1 Skapa signatur för elektroniskt dokument till Tullverket



Före signering skall det elektroniska dokumentet vara omvandlat till ett EDIFACT-meddelande.

EDIFACT-överföringen består av EDIFACT-meddelanden för de ingående elektroniska dokumenten samt ett AUTACK-meddelande för säkerhetsinformationen.

Först beräknas en checksumma på det elektroniska dokumentets representation i EDIFACT-format. Checksumman beräknas med algoritm enligt avsnitt 6.2 på hela meddelandet inkluderande all information, d v s även EDIFACT-orienterad styrinformation såsom avgränsningstecken och segmentnamn, se regelverk SCTS-SC.

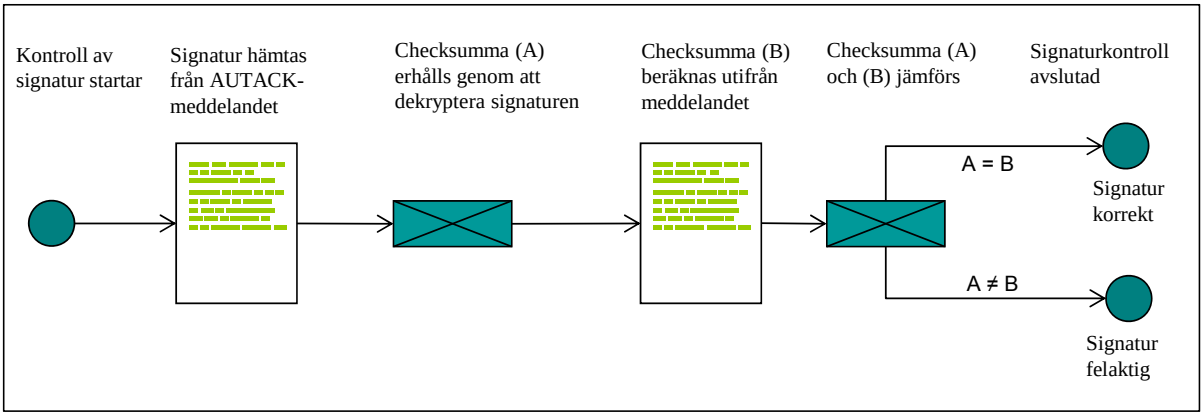
I nästa steg krypteras checksumman[11] via algoritm för elektronisk signatur enligt avsnitt 6.2. För denna kryptering används företagets aktuella signeringsnyckel (privata nyckel) kopplad till certifikatet. Den krypterade checksumman utgör det elektroniska dokumentets signatur.

[11] Före krypteringen kompletteras checksumman, se avsnitt 6.2

För att mottagaren unikt ska kunna identifiera det använda certifikatet skall referens lagras i AUTACK-meddelandet med certifikatserienumret (*serialNumber*) och hänvisning till certifikatutfärdaren (*authorityKeyIdentifier[keyIdentifier]*), se bilaga A.

Certifikatets *serialNumber* respektive *authorityKeyIdentifier[keyIdentifier]* skall lagras i Base64-format i AUTACK-meddelandets *certificate reference* respektive *key name*, se bilaga C.

6.1.2 Kontrollera signatur för elektroniskt dokument från Tullverket



EDIFACT-överföringen består av EDIFACT-meddelanden för de ingående elektroniska dokumenten samt ett AUTACK-meddelande för säkerhetsinformationen.

Avsändarens publika nyckel hämtas från avsändarens (Tullverkets) certifikat. Certifikatet publiceras av Tullverket men sänds inte med i EDIFACT-överföringen. Flera certifikat kan vara giltiga samtidigt, exempelvis i samband med att certifikat ersätts. För att avgöra vilket certifikat som har använts måste *key name* och *certificate reference* från AUTACK-meddelandet nyttjas, se regelverk SCTS-SC.

Den elektroniska signaturen hämtas från AUTACK-meddelandet. Via avsändarens publika nyckel och algoritm för elektronisk signatur enligt avsnitt 6.2, dekrypteras den mottagna signaturen varvid checksumman[12] erhålls (checksumma A i bilden). En ny checksumma[13] beräknas på respektive mottaget EDIFACT-meddelande (checksumma B i bilden). Beräkningen sker på samma sätt som när meddelanden ska signeras. Checksumma A och B jämförs sedan och ska vara lika för att signaturen ska vara korrekt. I signaturkontrollen ingår även att på vedertaget sätt kontrollera att certifikatet är korrekt, d v s utföra kontroll mot spärrlista, kontroll av giltighetstid, kontroll av rotcertifikat inklusive certifikatkedjor etc.

Vid felaktig signatur skall ett felmeddelande sändas till Tullverket enligt gällande regelverk.

[12] Den kompletterade checksumman enligt avsnitt 6.2
[13] Checksumman kompletteras enligt avsnitt 6.2 före jämförelse

6.2 Algoritmer för checksumma och elektronisk signatur

Checksumma	SHA-256 skall användas som checksummealgoritm.
Elektronisk signatur	RSA skall användas som krypteringsalgoritm för elektronisk signatur, se RFC 3447, RSASSA-PKCS1-v1_5. Nyckellängd för RSA-nycklar skall vara enligt bilaga A.

Innan checksumman krypteras kompletteras den med uppgift om checksummealgoritm och utfylls till samma längd som krypteringsnyckeln. *Observera att detta normalt sker automatiskt i standardfunktioner för signering.*

6.3 Att tänka på vid hantering av binära tal

Lagring i dataelementet ”Key name” i AUTACK

Certifikatfältet *authorityKeyIdentifier[keyIdentifier],* som innehåller information för utpekande av certifikatutgivarens (Tullverkets) utställarcertifikat, lagras i dataelement *key name* i AUTACK, se bilaga A och regelverk SCTS-SC. Före lagringen skall informationen Base64-kodas, se bilaga C.

Lagring i dataelementet “Certificate reference” i AUTACK

Certifikatfältet *serialNumber,* som innehåller certifikatserienummer, lagras i dataelementet *certificate reference* i AUTACK, se bilaga A och regelverk SCTS-SC. Före lagringen skall informationen Base64-kodas, se bilaga C.

Lagring i dataelementet “Validation value” i AUTACK

Framräknad checksumma respektive elektronisk signatur lagras i dataelementet *validation value* i AUTACK, se bilaga A och regelverk SCTS-SC. Före lagringen skall värdena hexadecimalkodas, se bilaga C.

Byteordning vid anrop av säkerhetsfunktioner för signering

Den som gör teknisk implementering av säkerhetskonceptet bör vara uppmärksam på att olika datormiljöer (Windows, Java etc.) kan förutsätta olika byteordningen för binära tal i API-anrop av säkerhetsfunktioner (big endian respektive little endian).

7 Bilaga A: Certifikat - teknisk beskrivning

7.1 Certifikathierarki

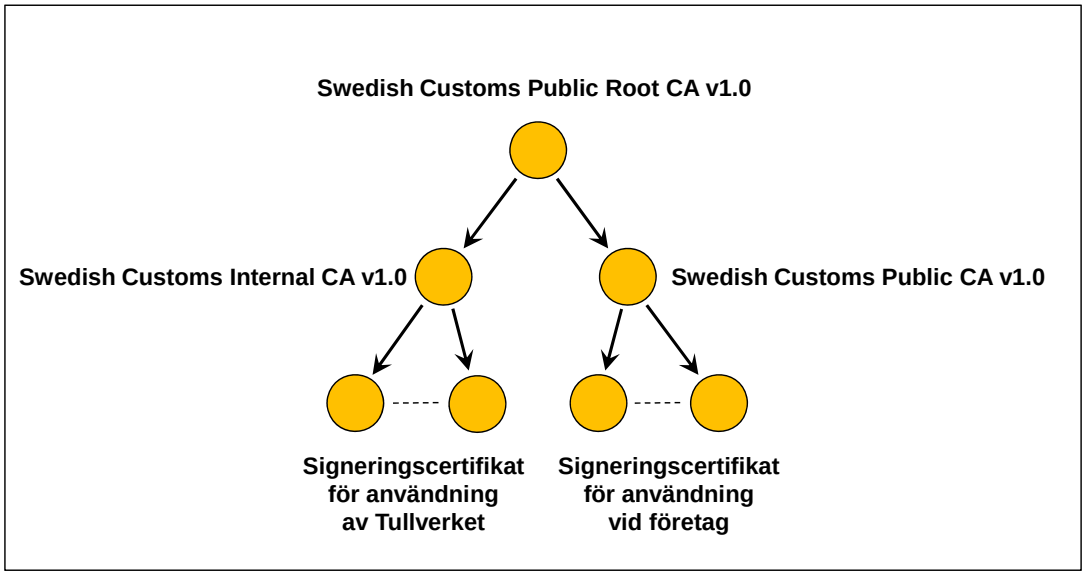
Certifikat för Tullverkets PKI-baserade säkerhetskoncept för EDI ingår i en certifikathierarki i tre nivåer.

På lägsta nivån finns de signeringscertifikat som används av företagen respektive av Tullverket för säkert informationsutbyte via EDI. Dessa är signerade av mellanliggande CA-certifikat.

På en mellannivå finns CA-certifikat med en maximal giltighetstid på 10 år. Dessa har signerats med rotcertifikatet. En uppdelning görs i CA-certifikat för signering av företagens signeringscertifikat respektive Tullverkets egna signeringscertifikat.

Högst upp i certifikathierarkin finns Tullverkets rotcertifikat med en giltighetstid på 20 år. Detta används endast för utfärdandet av mellanliggande CA-certifikat.

Rot- och mellanliggande certifikat publiceras på www.tullverket.se.



7.2 Rotcertifikat

Nyckellängd och giltighetstid
RSA-nyckel med längden 2048-bitar.
Giltighetstid: 20 år

Certifikatfält

Fältnamn	Kommentar
version	X.509 version 3 (värde = 2)
serialNumber	Unikt nummer för varje certifikat utgivet av en viss CA (Issuer)
signatureAlgorithm	sha1WithRSAEncryption
issuer	Utfärdare, för rotcertifikatet är issuer samma som subject
validity	Se RFC 5280
subject	Organisation för vilket certifikatet är utställt. C = SE, O = Tullverket, OU = Swedish Customs, OU = Root Certificate Authority, SERIALNUMBER = SE2021000969, CN = Swedish Customs Public Root CA 1.0
subjectPublicKeyInfo	Signaturalgoritm samt publik nyckel kodad enligt RFC 5280
authorityKeyIdentifier	non-critical, se avsnitt 7.5 samt RFC 5280
subjectKeyIdentifier	non-critical, se RFC 5280
keyUsage	critical. Följande bitar ska vara satta: *keyCertSign, cRLSign*
basicConstraints	critical. Är uppdelat i två delfält: `cA`= TRUE; pathLenConstraint ej angivet

7.3 CA-certifikat

Nyckellängd och giltighetstid
RSA-nyckel med längden 2048-bitar.
Giltighetstid: 10 år

Certifikatfält

Fältnamn	Kommentar
version	X.509 version 3 (värde = 2)
serialNumber	Unikt nummer för varje certifikat utgivet av en viss CA (issuer)
signatureAlgorithm	sha1WithRSAEncryption
issuer	Utfärdare är samma som rotcertifikatets subject
validity	Se RFC 5280
subject	Organisation för vilket certifikatet är utställt. För signering av företagens signeringscertifikat: C = SE, O = Tullverket, OU = Swedish Customs, OU = Public Intermediate Certificate Authority, OU = Only for authorized use, SERIALNUMBER = SE2021000969, CN = Swedish Customs Public CA 1.0 För signering av Tullverkets signeringscertifikat: C = SE, O = Tullverket, OU = Swedish Customs, OU = Internal Intermediate Certificate Authority, OU = Only for authorized use, SERIALNUMBER = SE2021000969, CN = Swedish Customs Internal CA 1.0
subjectPublicKeyInfo	Signaturalgoritm samt publik nyckel kodad enligt RFC 5280
authorityKeyIdentifier	non-critical, se avsnitt 7.5 samt RFC 5280
subjectKeyIdentifier	non-critical, se RFC 5280
keyUsage	critical. Följande bitar ska vara satta: *keyCertSign, cRLSign*
certificatePolicies	non-critical. Pekar ut aktuell certifikatpolicy via OID.
basicConstraints	critical. Är uppdelat i två delfält: `cA`= TRUE; pathLenConstraint = 0

7.4 Signeringscertifikat

Nyckellängd och giltighetstid
RSA-nyckel med längden 2048-bitar.
Giltighetstid: 14 månader

Certifikatfält

Fältnamn	Kommentar
version	X.509 version 3 (värde = 2)
serialNumber	Unikt nummer för varje certifikat utgivet av en viss CA (issuer)
signatureAlgorithm	sha1WithRSAEncryption
issuer	Utfärdare är samma som överordnat mellanliggande CA-certifikats subject
validity	Se RFC 5280
subject	Organisation för vilket certifikatet är utställt (ett företag eller Tullverket) Exempel för signeringscertifikat för företag: C = SE, O = Example import and export, OU = IT department, SERIALNUMBER = SE1122334455, CN = Eximpexp Exempel för signeringscertifikat för Tullverket: SERIALNUMBER=SE2021000969, O=Tullverket, C=SE, OU=Swedish Customs, CN=Tullverket EDI
subjectPublicKeyInfo	Signaturalgoritm samt publik nyckel kodad enligt RFC 5280
authorityKeyIdentifier	non-critical, se avsnitt 7.5 samt RFC 5280
subjectKeyIdentifier	non-critical, se RFC 5280
keyUsage	critical. Följande bit ska vara satt: *nonRepudiation*
certificatePolicies	non-critical. Pekar ut aktuell certifikatpolicy via OID.
basicConstraints	critical. Är uppdelat i två delfält: cA= FALSE; pathLenConstraint ej angivet
cRLDistributionPoints	non-critical. Detta fält innehåller uppgift om var CRL finns att hämta.

7.5 authorityKeyIdentifier

Ett steg i kontrollen av ett dokuments signatur är att verifiera att det certifikat som använts för att skapa signaturen är korrekt. I detta ingår att kontrollera att alla överordnade certifikat (mellanliggande CA-certifikat och rotcertifikat) är korrekta.

För att unikt identifiera vilket överordnat certifikat som använts vid utfärdandet av ett visst certifikat används *authorityKeyIdentifier*, som är uppdelad i följande delfält (se RFC 5280):

Delfält	**Kommentar**
keyIdentifier	Checksumma av överordnat certifikats publika nyckel.
authorityCertIssuer	Utfärdare (issuer) av överordnat certifikat.
authorityCertSerialNumber	Certifikatserienummer för överordnat certifikat.

För signeringscertifikat utgivna av Tullverket anges delfältet *keyIdentifier*.

För att kontrollera signaturer måste mottagaren ha tillgång till avsändarens signerings-certifikat. I Tullverkets implementering av EDIFACT-formatet sänds inte signerings-certifikatet med i AUTACK-meddelandet (se avsnitt 6) utan det måste hämtas separat. I AUTACK-meddelandet ingår däremot certifikatserienumret, *serialNumber*, och hänvisning till certifikatutfärdaren, *authorityKeyIdentifier[keyIdentifier]*. Fälten *serialNumber* och *authorityKeyIdentifier[keyIdentifier]* identifierar unikt det använda signeringscertifikatet, vilket är nödvändigt för att välja rätt certifikat.

Rotcertifikat, mellanliggande CA-certifikat och Tullverkets signeringscertifikat kan hämtas från Tullverkets webbplats, www.tullverket.se.

8 Bilaga B: CSR-fil – Beskrivning och exempel

Syftet med nedanstående exempel är att visa några olika sätt att skapa en CSR. Avsnittet ligger på en relativt djup teknisk nivå och är därför främst riktad till tekniska specialister som skall implementera hantering av CSR-filer i företagets system. *Informationen ska ses som en vägledning och inte som exakta instruktioner för implementeringen.*

I exemplen har följande företagsuppgifter använts:

countryName	SE
organizationName	Example import and export
organizationalUnitName	IT-department
serialNumber	SE1122334455
commonName	Eximpexp

CSR:en som skapas är en textfil. Nedan visas ett exempel på innehåll:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuDCCAaACAQAwczELMAkGA1UEBhMCU0UxIjAgBgNVBAoTGUV4YW1wbGUgaW1w
b3J0IGFuZCBleHBvcnQxFjAUBgNVBAsTDUlUIGRlcGFydG1lbnQxFTATBgNVBAUT
DFNFMTEyMjMzNDQ1NTERMA8GA1UEAxMIRXhpbXBleHAwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQD5iVkD/dcGo3Vy9L9hT4FH4e400+2wma8CJ+0dmT2k
FsHzuwfWnUD8R433BemmxIs+3aglkgbMr8yV74xtBMldW63NUADYOPwJ87o07UGw
JSq6Ql9iIK//srPDbIpvJCv/Ns9GKM54HuI3zLGN8FGPKDpN9rxoD5gAx7rhK7oj
ANZPemGydaRtIlDSFfiGnZcjvK9tz/XzvOKTgGaqBydSnWaUhul+2noy9fkjcn7d
bxHbwqMZfyEPEO+Hxxu8bSrxtodSJDzLRBrhYM/bF0oTwF7AnrXafl3vYzvClWT5
B8ylKmZl/MP4csQ+nn1eUQe9lILR9tt+EA+xdxMqCStzAgMBAAGgADANBgkqhkiG
9w0BAQUFAAOCAQEAavdGqU8ToG+/NwrA0DyoR30zg9YQTfYcKgc5KztjelDdbovG
RbSyfKis05u7V2Re3VDe3Oy3fArnab+/1mavLkVuVTmhjEGAlaCbC5abI7tZewaU
NquTAKKVhYTBf3/XvHpNZJEzKEQ/yrytiyu6kdzZyvORLejhWoATzAOjudPlzy3/
kBqf3B/YafeJMJ6JMyHHjMFr5AF8vLFFe7PqjjALrSno1fr/TKNE80IGHxvEKvqh
8tgIvLF0CJSaOjKWiH7EdxLECksBN09k/3oDUQtExnUmtUQOqVhnpg4zj9EKcP6m
FJ2qb9gJtvTU+7MsF6mF0dEjTlr0/q8kV/RWaw==
-----END CERTIFICATE REQUEST-----
```

Kontaktperson för signeringscertifikat ska kopiera in hela texten från CSR-filen in i ett e-postmeddelande (avsnitt 4.1, steg 2) och sända det till edi.certifikat@tullverket.se. Företagets namn och EORI-nummer ska anges i e-postmeddelandets ämnesrad.

Hela texten från CSR-filen ska även kopieras in i ett dokument med rubriken "Beställning av signeringscertifikat". Företagets namn och EORI-nummer ska även anges i dokumentet. Dokumentet ska undertecknas av kontaktperson för signeringscertifikat (inklusive namnförtydligande) och skickas per brev till:

Tullverkets IT-avdelning
EDI-certifikat
Aurorum 3
977 75 LULEÅ

Det undertecknade brevet är nödvändigt för att juridiskt kunna koppla kontaktpersonen till det utfärdade signeringscertifikatet.

8.1 OpenSSL

OpenSSL finns för många olika datormiljöer och är öppen källkod. Dokumentation av OpenSSL kan hämtas från www.openssl.org.

Kommandorad för att skapa CSR:

```
openssl req -newkey rsa:2048 -keyout example.key -out example.csr
-subj "/countryName=SE/organizationName=Example import and export
/organizationalUnitName=IT department/serialNumber=SE1122334455/
commonName=Eximpexp"
```

När kommandot körs ombeds man ange ett lösenord för att skydda den privata nyckeln. I kommandoexemplet ovan lagras CSR:en i filen *example.csr* och den privata nyckeln i *example.key*.

OpenSSL kan även användas för att visa innehållet i en CSR:

```
openssl req -text -noout -in example.csr
```

Observera dock att presentationen har begränsningar som gör att den inte klarar av att påvisa vissa inmatningsfel i *subject*.

Ett annat program i openssl-paketet är *asn1parse* som kan användas för att på detaljnivå visa innehållet i en CSR. Via detta kan fel upptäckas som inte upptäcks via *req*.

```
openssl asn1parse -in example.csr.
```

Med *asn1parse* går det t ex att kontrollera att *serialNumber* är ett separat objekt, se *OBJECT* i nedanstående exempel.

För CSR-filerna *exemple.csr* och *fel.csr*, där *exemple.csr* är korrekt och och *fel.csr* felaktig, kommer programmet *req* att presentera samma innehåll för *subject*. Används istället kommandot *asn1parse* syns felaktigheterna i *fel.csr*, se nedan.

Resultat av *asn1parse* för korrekt CSR:

```
openssl asn1parse -in example.csr
    0:d=0  hl=4 l= 696 cons: SEQUENCE
    4:d=1  hl=4 l= 416 cons: SEQUENCE
    8:d=2  hl=2 l=   1 prim: INTEGER           :00
   11:d=2  hl=2 l= 115 cons: SEQUENCE
   13:d=3  hl=2 l=  11 cons: SET
   15:d=4  hl=2 l=   9 cons: SEQUENCE
   17:d=5  hl=2 l=   3 prim: OBJECT            :countryName
   22:d=5  hl=2 l=   2 prim: PRINTABLESTRING   :SE
   26:d=3  hl=2 l=  34 cons: SET
```

```
  28:d=4  hl=2 l=  32 cons: SEQUENCE
  30:d=5  hl=2 l=   3 prim: OBJECT            :organizationName
  35:d=5  hl=2 l=  25 prim: PRINTABLESTRING   :Example import and export
  62:d=3  hl=2 l=  22 cons: SET
  64:d=4  hl=2 l=  20 cons: SEQUENCE
  66:d=5  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
  71:d=5  hl=2 l=  13 prim: PRINTABLESTRING   :IT department
  86:d=3  hl=2 l=  21 cons: SET
  88:d=4  hl=2 l=  19 cons: SEQUENCE
  90:d=5  hl=2 l=   3 prim: OBJECT            :serialNumber
  95:d=5  hl=2 l=  12 prim: PRINTABLESTRING   :SE1122334455
 109:d=3  hl=2 l=  17 cons: SET
 111:d=4  hl=2 l=  15 cons: SEQUENCE
 113:d=5  hl=2 l=   3 prim: OBJECT            :commonName
 118:d=5  hl=2 l=   8 prim: PRINTABLESTRING   :Eximpexp
 128:d=2  hl=4 l= 290 cons: SEQUENCE
 132:d=3  hl=2 l=  13 cons: SEQUENCE
 134:d=4  hl=2 l=   9 prim: OBJECT            :rsaEncryption
 145:d=4  hl=2 l=   0 prim: NULL
 147:d=3  hl=4 l= 271 prim: BIT STRING
 422:d=2  hl=2 l=   0 cons: cont [ 0 ]
 424:d=1  hl=2 l=  13 cons: SEQUENCE
 426:d=2  hl=2 l=   9 prim: OBJECT            :sha1WithRSAEncryption
 437:d=2  hl=2 l=   0 prim: NULL
 439:d=1  hl=4 l= 257 prim: BIT STRING
```

Resultat av *asn1parse* för felaktig CSR:

```
openssl asn1parse -in fel.csr
    0:d=0  hl=4 l= 699 cons: SEQUENCE
    4:d=1  hl=4 l= 419 cons: SEQUENCE
    8:d=2  hl=2 l=   1 prim: INTEGER           :00
   11:d=2  hl=2 l= 118 cons: SEQUENCE
   13:d=3  hl=2 l=  11 cons: SET
   15:d=4  hl=2 l=   9 cons: SEQUENCE
   17:d=5  hl=2 l=   3 prim: OBJECT            :countryName
   22:d=5  hl=2 l=   2 prim: PRINTABLESTRING   :SE
   26:d=3  hl=2 l=  34 cons: SET
   28:d=4  hl=2 l=  32 cons: SEQUENCE
   30:d=5  hl=2 l=   3 prim: OBJECT            :organizationName
   35:d=5  hl=2 l=  25 prim: PRINTABLESTRING   :Example import and export
   62:d=3  hl=2 l=  48 cons: SET
   64:d=4  hl=2 l=  46 cons: SEQUENCE
   66:d=5  hl=2 l=   3 prim: OBJECT            :organizationalUnitName
   71:d=5  hl=2 l=  39 prim: PRINTABLESTRING   :IT department/serialNumber=SE1122334455
  112:d=3  hl=2 l=  17 cons: SET
  114:d=4  hl=2 l=  15 cons: SEQUENCE
  116:d=5  hl=2 l=   3 prim: OBJECT            :commonName
  121:d=5  hl=2 l=   8 prim: PRINTABLESTRING   :Eximpexp
  131:d=2  hl=4 l= 290 cons: SEQUENCE
  135:d=3  hl=2 l=  13 cons: SEQUENCE
  137:d=4  hl=2 l=   9 prim: OBJECT            :rsaEncryption
  148:d=4  hl=2 l=   0 prim: NULL
  150:d=3  hl=4 l= 271 prim: BIT STRING
  425:d=2  hl=2 l=   0 cons: cont [ 0 ]
  427:d=1  hl=2 l=  13 cons: SEQUENCE
  429:d=2  hl=2 l=   9 prim: OBJECT            :sha1WithRSAEncryption
  440:d=2  hl=2 l=   0 prim: NULL
  442:d=1  hl=4 l= 257 prim: BIT STRING
```

Av den rödmarkerade texten ovan från resultatet från *openssl asn1parse* framgår att *serialNumber* inte är ett eget objekt utan felaktigt ingår i strängen *organizationalUnitName*. Detta framgår däremot inte av *openssl req*, där *subject* presenteras på samma sätt i båda fallen:

Det framgår av den rödmarkerade texten ovan att att *serialNumber* inte är ett eget objekt utan felaktigt ingår i strängen *organizationalUnitName*. Denna skillnad framgår däremot inte med *openssl req*, där *subject* presenteras på samma sätt i båda fallen:

```
Subject: C=SE, O=Example import and export, OU=IT  department/serialNumber=SE1122334455,
CN=Eximpexp
```

8.2 Windows certreq

I Windows-miljö kan programmet *certreq* användas för att skapa CSR:er. Dokumentation finns bland annat på http://technet.microsoft.com/en-us/library/cc725793(WS.10).aspx för Windows Server 2008 och http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx för Windows Server 2003.

Skapa konfigurationsfilen (policyfilen) *example.inf* med innehåll enligt följande exempel:

```
[NewRequest]
KeyLength=2048
RequestType=PKCS10
Subject="C=SE, O=Example import and export, OU=IT department,
serialNumber=SE1122334455, CN=Eximpexp"
Exportable = TRUE ; TRUE = Private key is exportable
SMIME = FALSE
```

Kör sedan följande kommando för att skapa nyckelpar och CSR:

```
certreq -New example.inf example.csr
```

Se även http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx för beskrivning av *certreq* och konfigurationsfil.

För att kontrollera CSR:en kan man använda kommandot *certutil*:

```
certutil -dump example.csr
```

Exempel på resultat från certutil:

```
PKCS10 Certificate Request:
Version: 1
Subject:
    C=SE
    O=Example import and export
    OU=IT department
    SERIALNUMBER=SE1122334455
    CN=Eximpexp
Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
    05 00
Public Key Length: 2048 bits
Public Key: UnusedBits = 0
    0000  30 82 01 0a 02 82 01 01  00 f5 36 cf c3 e4 a9 27
    0010  91 5b 4c 72 a4 45 81 39  ac 9c da f8 b4 93 af 6c
…
```

8.3 Java

Java *keytool* finns för många olika datormiljöer. Dokumentation av Java *keytool* kan hämtas från http://download.oracle.com/javase/6/docs/technotes/tools/index.html#security

Kör följande kommando för att skapa nyckelpar:

```
keytool -genkeypair -alias SE1122334455 -keyalg RSA -keystore
keystore.jks -keysize 2048 -dname "C=SE, O=Example import and export,
OU=IT department, serialNumber=SE1122334455, CN=Eximpexp"
```

Kör följande kommando för att skapa CSR:

```
keytool -certreq -alias SE1122334455 -keystore keystore.jks
-file example.csr
```

Kontroll av CSR:en kan göras med t ex *openssl req*, *openssl asn1parse* eller Windows *cerutil –dump* (se 8.1 och 8.2).

9 Bilaga C: Hexadecimal- och Base64-kodning

9.1 Hexadecimal kodning

Hexadecimal kodning (benämns även Base16-kodning) används för att lagra binär information som alfanumeriska tecken.

En uppdelning görs i grupper om 4 bitar. Varje grupp om 4 bitar omvandlas till ett alfanumeriskt tecken (0-9, A, B, C, D, E eller F) som representerar det hexadecimala värdet. En oktett representeras på så sätt av två alfanumeriska tecken.

I kodningsformatet för EDIFACT sätts ”Filterfunction 0505” till 2 för att ange att hexadecimalt filter används för kodning.

Hexadecimal kodning beskrivs i avsnitt 8 i RFC 4648,”The Base16, Base32, and Base64 Data Encodings”.

Exempel

Det decimala talet 31420 motsvaras av det binära 16-bitarstalet 0111 1010 1011 1100. Detta representeras via hexadecimal kodning av de fyra alfanumeriska tecknen 7 A B C.

9.2 Base64-kodning

Base64-kodning används för att lagra binär information som alfanumeriska tecken. Base64-kodning ger mindre antal alfanumeriska tecken än hexadecimal kodning och används istället för hexadecimal kodning då behov finns att komprimera informationen för att få plats.

I kodningsformatet för EDIFACT sätts ”Filterfunction 0505” till 7 för att ange att Base64-kodning har använts.

Base64-kodning beskrivs i avsnitt 4 i RFC 4648,”The Base16, Base32, and Base64 Data Encodings”.

Exempel

Som ett första steg görs gruppering i 24-bitars grupper (3 oktetter). Om det binära talet inte motsvarar ett jämt antal grupper om 24 bitar måste utfyllnadstecken (padding-byte) läggas till på slutet.

En uppdelning görs sedan av 24-bitars grupperna 4 x 6 bitar. De 6 bitarna tilldelas ett tecken utifrån nedanstående tabell.

Hex	Tecken	Hex	Tecken	Hex	Tecken	Hex	Tecken
0	A	10	Q	20	g	30	w
1	B	11	R	21	h	31	x
2	C	12	S	22	i	32	y
3	D	13	T	23	j	33	z
4	E	14	U	24	k	34	0
5	F	15	V	25	l	35	1
6	G	16	W	26	m	36	2
7	H	17	X	27	n	37	3
8	I	18	Y	28	o	38	4
9	J	19	Z	29	p	39	5
A	K	1A	a	2A	q	3A	6
B	L	1B	b	2B	r	3B	7
C	M	1C	c	2C	s	3C	8
D	N	1D	d	2D	t	3D	9
E	O	1E	e	2E	u	3E	+
F	P	1F	f	2F	v	3F	/

Nedan används följande binära tal om 160 bitar som exempel:
00:12:87:EC:A7:BD:25:20:2D:6D:2B:F5:5B:3D:1E:D7:86:07:BB:67
Användning av kolon (:) i exemplet är endast till för att öka läsbarheten.

Gruppering i grupper om 3*8 = 24 bitar:

```
00:12:87 =    0000 0000   0001 0010   1000 0111
EC:A7:BD =    1110 1100   1010 0111   1011 1101
25:20:2D =    0010 0101   0010 0000   0010 1101
6D:2B:F5 =    0110 1101   0010 1011   1111 0101
5B:3D:1E =    0101 1011   0011 1101   0001 1110
D7:86:07 =    1101 0111   1000 0110   0000 0111
BB:67:00 =    1011 1011   0110 0111   0000 0000
```

där avslutande 8 bitar (00) i sista gruppen är utfyllnad (padding-byte)

Omgruppering med 4*6 = 24 bitar uttryckta som hexadecimala tal:

```
000000  000001  001010  000111 = 00:01:0A:07
111011  001010  011110  111101 = 3B:0A:1E:3D
001001  010010  000000  101101 = 09:12:00:2D
011011  010010  101111  110101 = 1B:12:2F:35
010110  110011  110100  011110 = 16:33:34:1E
110101  111000  011000  000111 = 35:38:18:07
101110  110110  011100  000000 = 2E:36:1C:00
```

Omvandling av 6-bitars hexadecimala tal till alfanumeriska tecken enligt tabellen:

```
00:01:0A:07 = ABKH
3B:0A:1E:3D = 7Ke9
09:12:00:2D = JSAt
1B:12:2F:35 = bSv1
16:33:34:1E = Wz0e
35:38:18:07 = 14YH
2E:36:1C:00 = u2c=
```

För exemplet fås då följande alfanumeriska tal om 28 tecken:
ABKH7Ke9JSAtbSv1Wz0e14YHu2c=
(“=” på slutet visar att det finns en avslutande padding byte).

Box 12854, 112 98 Stockholm
Telefon: 0771-520 520
tullverket.se