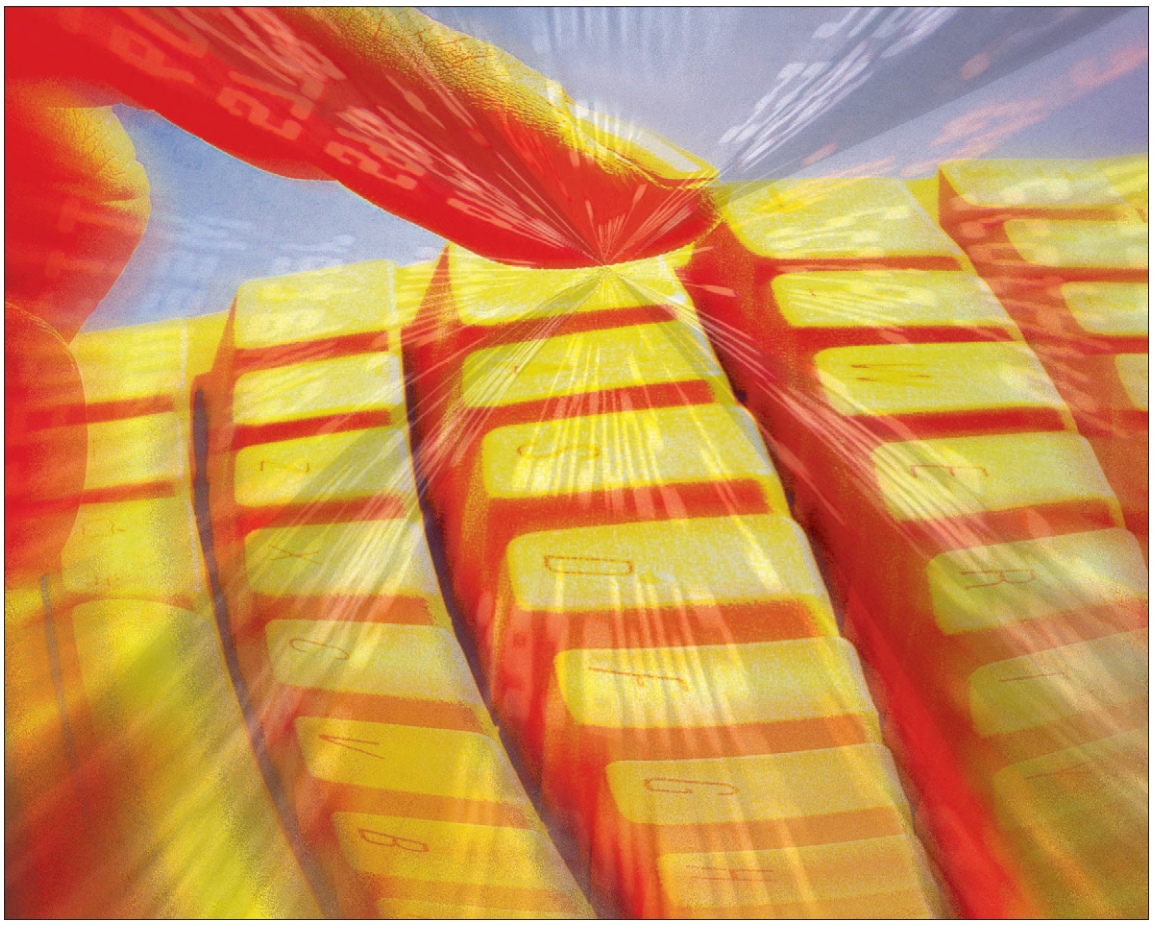
Skattelagstiftning blir IT-chefens huvudbry - IT-säkerhetskrav vid elektronisk fakturering i EU

Ett EU-direktiv har givit nya regler som gör elektronisk fakturering tillåtet i hela EU. En förutsättning är att den elektroniska fakturans äkthet och innehållets integritet kan garanteras, både i transporten och lagringen av fakturan. Trots att reglerna finns i ett skattedirektiv är säkerhetskraven något som landar på IT-chefens bord.



HUR UPPFYLLS SÄKERHETSKRAVEN?

Enligt direktivet kan säkerhetskraven huvudsakligen uppfyllas på två sätt; genom att använda en s.k. avancerad elektronisk signatur (en digital signatur baserad på PKI-teknologi) eller genom EDI (Electronic Data Interchange (EDI) med säkerhetsförfarande fastställt i avtal. EDI-begreppet i direktivet är vidare än den traditionella EDI-FACT-standarden och innefattar all strukturerad kommunikation som möjliggör automatisk hantering. Detta innebär att exempelvis en faktura som skickas i XML-format anses vara EDI enligt direktivet. Uppmärksammas bör dock att enbart det faktum att kommunikationen klassas som EDI inte uppfyller direktivets krav – äktheten och integriteten måste fortfarande säkerställas.

Förutom huvudalternativen ges EU-länderna möjlighet att höja säkerheten och kräva s.k. kvalificerade elektroniska signaturer samt möjlighet att sänka kraven och godkänna fakturor skickade på elektronisk väg enligt ”andra metoder”. En faktura som enligt den sistnämnda undantagsregeln accepteras i ett land blir inte automatiskt accepterad i övriga EU-länder.

VARIERANDE KRAV INOM EU

Eftersom direktivet ger medlemsstaterna viss valfrihet när det gäller säkerhetskraven har resultatet blivit att kraven skiljer sig åt länder emellan. Även om elektroniska fakturor nu accepteras i hela EU så varierar säkerhetskraven från kvalificerade elektroniska signaturer (i t.ex. Tyskland, Slovakien, Spanien) till enbart krav på oföränderlighet av fakturan (i Sverige och Finland).

SVENSKA FÖRETAG MED INTERNATIONELL HANDEL

Enligt svensk rätt ska en elektronisk faktura bibehållas oförändrad, men det ställs inga krav på tekniken för att garantera detta. Kraven är desamma som ställs på en pappersfaktura, skillnaden är givetvis att man i den elektroniska miljön måste se till att fakturan får motsvarande skydd mot förändring som pappret ger. Ofta används elektroniska signaturer för att replikera papprets integritetsfunktion i den elektroniska miljön.

Vid fakturering till andra länder räcker det dock inte att följa svensk lag. Eftersom Sverige valt en lägre säkerhetsnivå än direktivets huvudregel kommer inte svenska fakturor att per automatik godkännas i övriga EU-länder, utan man tvingas höja nivån till för att möta övriga länders krav.

RÅD TILL IT-CHEFEN

Använd en avancerad elektronisk signatur som grund. Använder man en avancerad elektronisk signatur så uppfyller man direktivets huvudregel och uppnår god interoperabilitet med övriga EU. En avancerad elektronisk signatur är lämpligt för både EDI och ad-hoc fakturor i ej strukturerade format.

Tänk på ” treenigheten”: För att uppnå en säker och väl fungerande affärsprocess måste tre delar samspela: säkerhetstekniken, juridiken och applikationen. En rent teknisk implementation är sällan tillräcklig eftersom de legala aspekterna också måste beaktas för att skapa en pålitlig elektronisk signatur.

Se vad applikationen kan erbjuda: Om applikationen tillhandahåller funktioner för elektronisk signering kan man få en både tekniskt och legalt säker lösning, som även är användarvänlig. Trenden går mot att allt fler applikationsleverantörer bygger in signeringsfunktionalitet. Kontrollera dock med leverantören att applikationen uppfyller lagkraven både i Sverige och övriga EU.

Var inte rädd för att själv hantera certifiktutgivning om företaget är en naturlig hub i t.ex. ett leverantörsnät: I ett större internationellt nätverk av affärspartners är det ofta svårt att hitta lämpliga leverantörer av certifikat. Leverantörer är ofta lokala och deras policy hanterar ofta inte de legala krav som en gränsöverskridande lösning kräver. I situationer som denna är det ofta lämpligt att ett naturligt nav i nätverket tar ansvaret för certifikatutgivningen.

Anna Nordén
IT-säkerhetsjurist
TrustWeaver