Rafræn viðskipti

RÍKISENDURSKOÐUN

Október 2000

Efnisyfirlit

Inngangur

Á síðasta áratug hafa rafrænir viðskiptahættir í sívaxandi mæli rutt sér rúm hér á landi. Viðskipti sem eru að öllu leyti rafræn byggjast á því að upplýsingakerfi viðskiptaaðila skiptast á rafrænum gögnum sem unnið er úr á vélrænan hátt. Slík viðskipti eru í eðli sínu pappírslaus og því í veigamiklum atriðum, m.a. bæði lögfræðilega og endurskoðunarlega, frábrugðin hefðbundnum viðskiptum sem byggja á pappírsnotkun á öllum stigum.

Nauðsynlegt er að vanda vel undirbúning að upptöku rafrænna viðskipta og mikilvægt að stjórnendur axli ábyrgð á breyttu rekstrarumhverfi sem kallar á alveg nýja sýn vegna áhættuþátta, innra eftirlits, öryggismála, endurskoðunar o.fl.

Rafræn viðskipti eru áhugaverður kostur fyrir þá ríkisaðila sem stunda viðskipti með hefðbundnum aðferðum því hinn nýi kostur er einfaldari, fljótvirkari, öruggari og hagkvæmari. Rit þetta, sem er í röð upplýsingarita Ríkisendurskoðunar, geymir auk ýmissa upplýsinga um rafræn viðskipti, umfjöllun um þau öryggisatriði sem ríkisaðilar verða að huga að og þær meginreglur sem þeir verða að fylgja ætli þeir sér að taka upp og stunda rafræn viðskipti.

Ríkisendurskoðun vill sérstaklega þakka ICEPRO og embætti ríkistollstjóra fyrir góðar ábendingar og veitta aðstoð við gerð þessa rits.

Ríkisendurskoðun, 20. október 2000

1. Umfang úttektarinnar

Í október 1998 gaf Ríkisendurskoðun út ritið „Rekstrar-öryggi upplýsingakerfa - Innra eftirlit“. Þar er fjallað um þau atriði sem máli skipta vegna reksturs upplýsingakerfa, þar á meðal helstu áhættuþætti, gerð áhættumats, mótun öryggisstefnu, öryggisráðstafanir og þörfina fyrir stöðugt eftirlit og endurmat öryggismála.

Áðurnefnt rit stofnunarinnar er almennt rit varðandi rekstur rafrænna viðskiptakerfa ríkisaðila. Þetta rit er aðeins viðbótarrit sem ætlað er að fjalla um þau atriði sem sérstaklega þarf að huga að vegna rafrænna viðskipta ríkisaðila. Saman mynda ritin samstæða heild.

Umfjöllunin byggir á aðferðunum við viðskiptin

Umfjöllun um rafræn viðskipti byggir oft á því hvaða aðilar/markhópar stunda þau. Er þá talað um rafræn viðskipti milli rekstraraðila (B2B „Business to Business“), rekstraraðila og neytanda (B2C „Business to Consumer“) rekstraraðila og stjórnvalda (B2G „Business to Government“) o.s.frv. Umfjöllun byggð á þessari flokkun rafrænna viðskipta var ekki talin sú sem best hentaði upplýsingariti sem þessu.

Í riti þessu er fjallað um rafræn viðskipti út frá þeim aðferðum sem beitt er við þau. Umfjöllunin er ýmist um bein eða óbein rafræn viðskipti eða almennt um báðar tegundirnar. Bein rafræn viðskipti nefnast þau sem byggja á því að ferlið frá viðskiptakerfi kaupanda yfir í viðskiptakerfi seljanda sé sem sjálfvirkast og feli m.a. í sér skráningu í kerfi kaupanda. Sjálfvirkni sem þessari er ekki til að dreifa í óbeinum rafrænum viðskiptum en þau byggja á samblandi af hefðbundnum og rafrænum viðskiptaaðferðum. Stundum er muninum á þessum aðferðum í stuttu máli lýst með því að segja að bein rafræn viðskipti séu á milli tveggja tölva en óbein á milli tölvu og manns.

Umfjöllunin er tæknilega óháð

Nauðsynlegt var talið að í riti sem þessu væri umfjöllun með þeim hætti að hún stæðist sem best tímans tönn. Þar sem þróun á sviði rafrænna viðskipta er geysiör og engin teikn á lofti um breytingar í þeim efnum var ákveðið að tilgreina ekki einstakar tæknilegar útfærslur sem núna eru taldar bestar til þess að leysa einstök vandamál tengd rafrænum viðskiptum. Í staðinn er greint frá skilyrðum sem verða að vera uppfyllt til þess að leysa vandamálin. Þannig er ekki lokað fyrir þann möguleika að ýmsar aðferðir megi viðhafa til þess að uppfylla þau, m.a. aðferðir sem ekki eru til í dag. Með þessari nálgun er reynt að tryggja að umfjöllunin í riti þessu verði ekki of háð tækniþróuninni.

Efnisuppbygging ritsins

Vegna náinna tengsla rits þessa við rit stofnunarinnar um rekstraröryggi upplýsingakerfa, var talið nauðsynlegt að hafa uppbyggingu ritanna eins líka og kostur væri.

Í 2. kafla ritsins er að finna ýmsar skilgreiningar vegna rafrænna viðskipta auk umfjöllunar um ávinning af upptöku þeirra og lýsingu á því umhverfi sem rafrænum viðskiptum er nú búið hér á landi. Í 3. kafla er lýst þeim áhættuþáttum sem sérstaklega koma til skoðunar vegna rafrænna viðskipta og í 4. kafla hvernig meta skal þá með tilliti til þeirra hagsmuna sem í húfi eru. Einnig er í kaflanum fjallað um mótun öryggisstefnu en í henni skal skilgreina þau markmið sem viðkomandi aðili ætlar sér að ná með öryggisráðstöfunum sínum. Í 5. kafla er síðan ítarlega fjallað um ráðstafanirnar en í 6. kafla um þær miklu breytingar sem upptaka rafrænna viðskipta hefur á allt eftirlit og endurskoðun. Ritinu lýkur á 7. kafla þar sem fjallað er um þróun rafrænna viðskipta og er sjónum þar annars vegar beint að alþjóðlegum staðlamálum og hins vegar að rafrænum viðskiptum hjá ríkisaðilum hér á landi. Það síðast nefnda er gert í þeim tilgangi að sýna lesendum fram á að það sem á undan er komið er ekki eingöngu fræðileg umfjöllun heldur einnig umfjöllun um íslenskan veruleika.

2. Rafræn viðskipti, ávinningur og umhverfi

Þegar talað er um rafræn viðskipti, á ensku „electronic commerce“, er átt við viðskipti sem stofnað er til eða þau stunduð á rafrænan hátt.

Í tæknilegri handbók evrópska vinnuhópsins um opin kerfi, EWOS („European Workshop on Open Systems“) eru rafræn viðskipti skilgreind þannig[1]:

> *„Electronic exchange of data to support business transactions, i.e. the exchange of value through the delivery of a product from a seller to a buyer.“*
>
> þ.e.:
>
> *„Rafræn skipti á gögnum vegna viðskiptafærslna, þ.e. skipti á verðmætum með afhendingu varnings frá seljanda til kaupanda.“*

Skilgreiningin er mjög víð bæði varðandi verðmæti og þá sem skiptast á þeim. Með verðmætum er m.a. átt við vörur eða þjónustu verslana, tryggingarfyrirtækja, heilsugæslunnar og aðilar viðskiptanna eru ekki bara fyrirtæki og stofnanir heldur einnig einstaklingar. Skilgreiningin er í góðu samræmi við veruleika rafrænna viðskipta í dag.

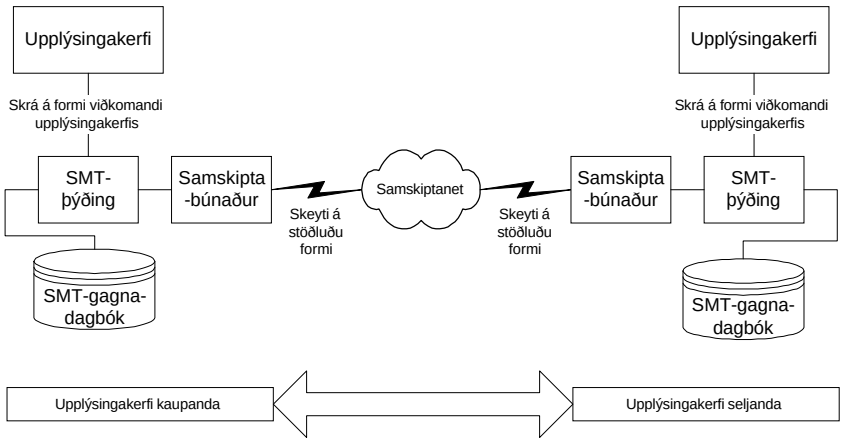
Hægt er að flokka rafræn viðskipti ýmist sem bein eða óbein. Þau beinu fara alfarið fram rafrænt en hin óbeinu með blöndu af hefðbundnum og rafrænum viðskiptaaðferðum. Þessi flokkun rafrænna viðskipta byggist á aðferðunum við viðskiptin.

[1] Sbr. EWOS ETC 066.

Einnig er hægt að flokka rafræn viðskipti ýmist sem milli tveggja rekstraraðila (B2B „Business to Business“), rekstraraðila og neytanda (B2C „Business to Consumer“), rekstraraðila og stjórnvalda (B2G „Business to Government“) o.s.frv. Þessi flokkun rafrænna viðskipta byggist á aðilum/markhópum viðskiptanna. Oftast heyrir fyrri flokkurinn undir beinu rafrænu viðskiptin en sá síðari undir hin óbeinu.

2.1 Bein rafræn viðskipti

Sumar tegundir rafrænna viðskipta eru alfarið vélrænar, þ.e. mannshöndin kemur ekki nálægt þeim. Einnig má lýsa þessum viðskiptum með því að segja að þau séu bein rafræn viðskipti á milli tölva. Slík viðskipti eru nú nær eingöngu stunduð af fyrirtækjum eða stofnunum í föstu viðskiptasambandi.



Mynd 1. Ferli beinna rafrænna viðskipta.

Bein rafræn viðskipti eru ekki bundin við notkun viðurkenndra staðla þó að þeir séu oftast notaðir. Stundum styðjast aðilar við eigin aðferðir og einnig eru dæmi um að hópur viðskiptaaðila komi sér saman um notkun samskiptaforms tiltekins upplýsingakerfis.

1. Hefðbundin SMT-viðskipti

Hugtakið hefðbundnar skjalasendingar milli tölva, oft nefnt hefðbundin SMT[2]-viðskipti, (á ensku, „Traditional/Standard Electronic Data Interchange“ eða EDI), er notað um viðskiptagögn á stöðluðu eða fyrirfram ákveðnu sniði, sem send eru í skeytaformi frá upplýsingakerfi kaupanda til upplýsingakerfis seljanda, þar sem unnið er úr viðskiptagögnunum vélrænt. Oftast fer þetta ferli fram án þess að mannshöndin komi þar nálægt og er í eðli sínu pappírslaust.

Hefðbundnum SMT-viðskiptum má einnig lýsa sem ferli sem felst í því að aðilar viðskiptasambands, sem nota mismunandi upplýsingakerfi, skiptast með aðstoð sérstaks þýðingarhugbúnaðar á rafrænum upplýsingum í formi skeyta sem annað hvort byggja á þekktum viðurkenndum staðli eða eigin sniði viðskiptaaðilanna. SMT-skeyti eru stundum nefnd rammaskeyti en með því er átt við að upplýsingarnar í þeim eru fylltar inn í fyrirfram ákveðna ramma sem líkja má við ramma á eyðublöðum. Árangursrík SMT-viðskipti byggja ekki síst á því að sem minnst sé breytt út frá eða bætt við viðurkennd, stöðluð rammaskeyti.

Í hefðbundnum SMT-viðskiptum eru alltaf til staðar þeir hlutar sem nefndir eru í liðum 1. - 3. hér á eftir og oft einnig sá í lið 4.

1) **Upplýsingakerfi með hefðbundinni SMT-tengingu**

   Upplýsingakerfi vinna með gögn á eigin gagnasniði. Í þeim er búin til skrá með viðskiptagögnum sem senda á. Skráin er á sniði kerfisins og er oftast nefnd innanhússskrá.

2) **SMT-þýðandi**

[2] Í 3. útg. Tölvuorðasafns er SMT nefnt skjalaskipti milli tölva en í desember 1999 lagði Orðanefnd Skýrslutæknifélagsins til að talað yrði um skjalalaus samskipti milli tölva. Í riti þessu verður notað hugtakið skjalasendingar milli tölva þar sem það hefur náð víðtækri útbreiðslu og er m.a. notað í ýmsum lögum og reglugerðum.

SMT-þýðandi þýðir gögnin í innanhússkránni yfir á það snið sem aðilar hafa samið um að nota í samskiptum sín á milli.

3) Samskiptabúnaður

Samskiptabúnað þarf á milli SMT-þýðanda og þess tækniumhverfis sem notað er til sendinga á gögnum milli viðskiptaaðilanna. Símakerfið er órjúfanlegur þáttur í hefðbundnum SMT-viðskiptum, sem fara oftast fram í lokuðum kerfum, ýmist á milli einkaneta aðilanna eða í gegnum sérstakar gagnaflutningsnet þjónustuaðila sem oft eru kölluð VAN („Value Added Network“).

4) Virðisaukandi netþjónusta (VAN)

Ef þriðji aðili sér um skeytasendingar milli viðskiptaaðila þarf búnað til tengingar við hann. Virðisaukandi netþjónusta er þjónusta sem bæði opinberir og einkaaðilar bjóða upp á víða um lönd og fara samskiptin þá fram á einkaneti þjónustuaðilans, sem oft er nefnt VAN.

Algengasta tegund beinna rafrænna viðskipta nú eru hefðbundin SMT-viðskipti sem styðjast við alþjóðlega staðalinn UN/EDIFACT[3] sem útgefinn er af Sameinuðu þjóðunum.

2. Einfaldari SMT-viðskipti

Vegna mikils fasts kostnaðar eru hefðbundin SMT-viðskipti hagkvæmust þegar skeytasendingar eru mjög tíðar. Þau henta því oft illa litlum og meðalstórum fyrirtækjum. Því hefur í nokkurn tíma verið hugað að einfaldari og ódýrari leiðum vegna SMT-viðskipta, þ.e. beinna viðskipta á milli tölva, án þess að mannshöndin kæmi þar mikið nálægt. Helstu tegundir sem skilgreindar hafa verið í þessu skyni eru:

[3] Nánar er fjallað um UN/EDIFACT-staðalinn og fleiri staðla vegna rafrænna viðskipta í kafla 7.1.1 aftar í riti þessu.

1) Einföld SMT-viðskipti („Simpler UN/EDIFACT“, oft nefnd „SimplEDI“)

   og

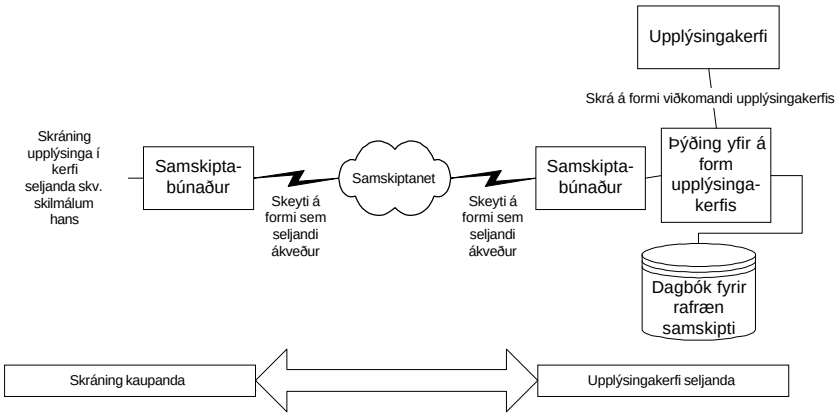
2) Hlutbundin SMT-viðskipti („Object Oriented EDI-FACT“, oft nefnd OO/EDI) en þau eru flokkuð sem opin SMT-viðskipti („Open EDI“).

Þessum nýju tegundum er lýst í kafla 7.1.1 sem fjallar um þróun staðla í beinum rafrænum viðskiptum.

2.2 Óbein rafræn viðskipti

Á síðustu árum hafa orðið miklar breytingar á þeim aðferðum sem menn nota við kaup og sölu verðmæta. Hefðbundin SMT-kerfi í lokuðum kerfum henta illa aðilum í tilfallandi viðskiptasambandi. Á síðustu árum hafa menn verið að þróa ný mynstur í rafrænum samskiptum í opnum kerfum, þar sem samskipti eru möguleg á milli hópa sem áður gátu ekki án mikils tilkostnaðar stundað viðskipti sín rafrænt.

Áður fólust rafrænu samskiptin aðallega í flutningi gagna frá einni tölvu til annarrar án mannlegra afskipta. Nú eru einnig algeng samskiptamynstur sem byggjast á því að maðurinn setji viðskiptin af stað. Mikil aukning hefur því orðið á þeim rafrænum viðskiptum sem í riti þessu eru nefnd óbein, þ.e. þeim sem fara fram með blöndu af hefðbundnum og rafrænum aðferðum.



Mynd 2. Óbein rafræn viðskipti

Landamærin milli þeirra tæknilegu aðferða sem notaðar eru við sendingar verða æ sveigjanlegri því nú getur skeyti sem sent er sem hefðbundið SMT-rammaskeyti hæglega endað sem tölvupóstur hjá móttakanda vegna þess að þýðingar-hugbúnaðurinn, sem e.t.v. er staðsettur hjá þriðja aðila, hefur breytt skeytinu yfir í það form. Búast má við því að í framtíðinni fjölgi mjög þeim SMT-aðferðum sem nota Netið sem samskiptaleið.

Þessum nýju tegundum er lýst í kafla 7.1.2 sem fjallar um þróun staðla í óbeinum rafrænum viðskiptum en helstar eru eftirfarandi:

1) Vef SMT, („Web-EDI“).
2) Létt SMT („EDI-Light/Lite“).
3) XML/SMT („XML/EDI“).

2.3 Ávinningur af rafrænum viðskiptum

Tilgangurinn með beinum rafrænum viðskiptum er að flýta viðskiptum með sjálfvirkri miðlun upplýsinga milli vinnslu-kerfa og notkun gagna í áframhaldandi vinnslu án endur-skráningar. Hvort tveggja leiðir til minni villuhættu og lægri kostnaðar.

Á sama hátt er tilgangurinn með óbeinum rafrænum viðskiptum að flýta viðskiptum með sjálfvirkari miðlun upplýsinga en tíðkast í hefðbundnum viðskiptum. Hér er þó að jafnaði ekki um sama hagræði að ræða og í beinum rafrænum viðskiptum vegna þess að gögn skrást ekki sjálfkrafa hjá móttakanda.

Ávinningur af rafrænum viðskiptum getur komið fram í hagkvæmara verklagi og í formi lægri kostnaðar.

1. Hagkvæmara verklag

Hefðbundin viðskipti geta verið mjög óskilvirk að því leyti að sömu gögnin kunna að vera margskráð hjá báðum aðilum viðskiptanna. Með því að taka upp rafræn viðskipti er mögulegt að minnka verulega tvíverknað af þessu tagi.

Áður en rafræn viðskipti eru tekin upp er mikilvægt að stofnanir og fyrirtæki skoði fyrst verklag innanhúss. Endurskoðun á því, samfara upptöku rafrænna viðskipta, gefur mikla möguleika á hagkvæmara verklagi.

Ein algengasta innri eftirlitsaðgerð hefðbundinna viðskipta er aðgreining starfa þó oft sé erfitt að koma henni við vegna smæðar stofnunar eða fyrirtækis. Þegar rafræn viðskipti eru tekin upp þarf að endurskoða eða leggja af aðgreiningu starfa á þeim sviðum þar sem hún þjónar ekki lengur tilgangi sínum. Þess í stað koma eftirlitsþættir sem byggðir eru inn í upplýsingakerfin sem notuð eru við viðskiptin og geta ef vel er að verki staðið verið áreiðanlegri og skilvirkari en það eftirlit sem hefðbundin verkaskipting skilar.

Til þess að bein rafræn viðskipti renni algjörlega inn í bókhald viðskiptaaðila er ekki nóg að þeir komi sér saman um sömu sniðstaðla heldur þarf einnig að samræma vörunúmer. Hér á landi hefur samræmt vörunúmerakerfi ekki hlotið almenna útbreiðslu. Í mörgum tilvikum býr hver verslun til sín eigin númer. Ef ekki er gætt að samræmingu númera er ómögulegt að ná fram öllu því hagræði sem bein rafræn viðskipti bjóða í raun uppá. Í þessu sambandi má minna á að

vörunúmer taka sífelldum breytingum og getur því umbreyting frá vörunúmerum seljanda yfir í vörunúmer kaupanda verið mjög kostnaðarsöm ef aðilarnir nota ekki samræmt númerakerfi. Í óbeinum rafrænum viðskiptum gengur það upp í flestum tilvikum að aðilar noti ólík vörunúmer þar sem tilteknum starfsmönnum er falið það verk að handvinna bókhaldssundurliðanir. Rétt er að geta þess að EAN[4] á Íslandi hefur unnið að útbreiðslu alþjóðlegs númerakerfis sem birtist gjarnan í formi strikamerkja til auðkenningar á vöru og þjónustu.

2. Minni kostnaður

Samsetning kostnaðar í hefðbundnum viðskiptum er frábrugðin þeirri sem er í rafrænum viðskiptum.

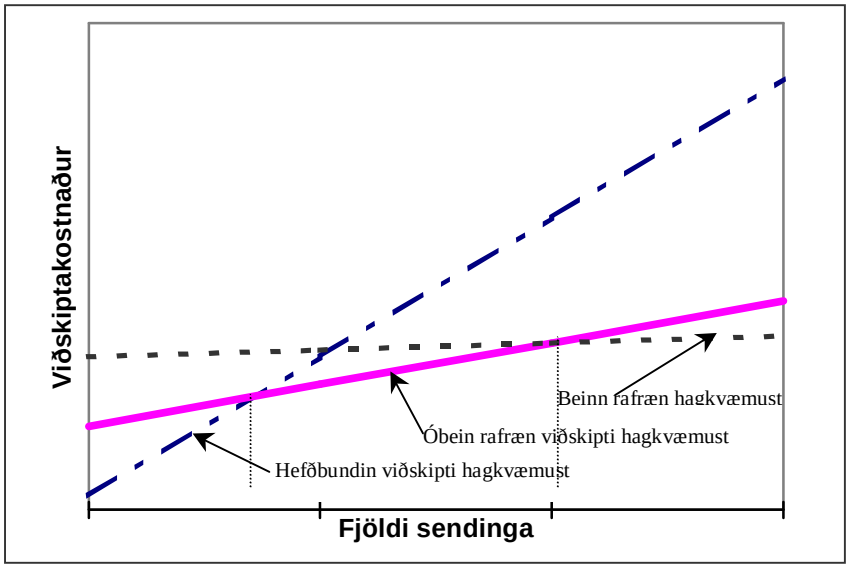
Í hefðbundnum viðskiptum eru stærstu kostnaðarliðirnir breytilegir, t.d. þarf að ráða fleiri starfsmenn til þess að sinna viðskiptunum ef þau aukast verulega.

Í beinum rafrænum viðskiptum eru stærstu kostnaðarliðirnir fólgnir í hugbúnaði, vélbúnaði, uppsetningu búnaðar og endurskipulagningu verkferla. Stærstur hluti þessa kostnaðar er fastur og tilltölulega óháður fjölda skeytasendinga. Viðskiptakostnaður við þúsund sendingar í beinum rafrænum viðskiptum er lítið meiri en við eina sendingu þar sem sama búnaðinn þarf til. Með viðskiptakostnaði er átt við heildarkostnað, þ.e. bæði fastan og breytilegan, af því að stunda viðskipti. Litið er á kostnað vegna starfsmanna sem breytilegan þar sem fjöldi þeirra er mjög háður fjölda þeirra viðskipta sem eiga sér stað.

Óbein rafræn viðskipti eru millistig milli hefðbundinna og beinna rafrænna viðskipta þar sem sjálfvirkni hefur verið beitt í hluta viðskiptaferlisins. Fastur kostnaður við óbein rafræn viðskipti er lægri en við bein vegna þess að búnaðurinn sem til þarf er ódýrari og í flestum tilvikum sá sami hvort sem viðskiptavinirnir eru fleiri eða færri. Breytilegi kostnaðurinn er hins vegar hærri en í beinum rafrænum

[4] Sjá http://www.ean.is

viðskiptum þar sem sjálfvirkni er ekki á jafn háu stigi.



Mynd 3. Tengsl fjölda sendinga og viðskiptakostnaðar við mismunandi aðferðir í viðskiptum tveggja aðila.

Á myndinni að ofan koma fram línur sem tákna einstakar viðskiptaaðferðir, þ.e. hefðbundin viðskipti, bein rafræn viðskipti og óbein rafræn viðskipti. Á henni má sjá að hefðbundinn viðskiptamáti er hagkvæmasti kosturinn þegar um lítil viðskipti er að ræða. Ástæðan er sú að slíkur viðskiptamáti hefur í för með sér mikinn fastan kostnað eins og bein og óbein rafræn viðskipti gera.

Eftir því sem fjöldi sendinga vex kemur að því að hagkvæmara verður að taka upp óbein rafræn viðskipti en að ráða starfsmenn til þess að anna auknum viðskiptum.

Þegar sendingar eru orðnar mjög margar verður hagkvæmara að stunda bein rafræn viðskipti í stað óbeinna vegna þess að breytilegur kostnaður beinna rafrænna viðskipta er lægri. Þetta er ástæða þess að bein rafræn viðskipti eru útbreiddust milli aðila sem eru í miklum föstum viðskiptum.

2.4 Umhverfi rafrænna viðskipta

1. Afskipti stjórnvalda

Íslensk stjórnvöld hafa lengi látið sig þróun rafrænna viðskipta varða og hafa fjármála- og viðskiptaráðuneyti gegnt þar lykilhlutverki.

Í mars 1999 samþykkti ríkisstjórnin tillögu þess efnis að Verkefnisstjórn forsætisráðuneytisins í málefnum upplýsingasamfélagsins, mótaði heildarstefnu ríkisstjórnarinnar um rafræn viðskipti. Í apríl 2000 sendi verkefnastjórnin síðan frá sér vinnuáætlun um þróun rafrænna viðskipta og rafrænnar stjórnsýslu.[5]

Til þess að auðvelda upptöku rafrænna viðskipta hefur fjármálaráðuneytið bæði beitt sér fyrir breytingu á lögum og reglugerðum. Á vegum ráðuneytisins hafa og starfað nefndir til að auka rafræn viðskipti bæði innan ríkiskerfisins sem utan þess. Hér skal t.d. nefndur stýrihópur um rafræn viðskipti í opinberum innkaupum.

Í samstarfi viðskiptaráðuneytisins og Verslunarráðs var á sínum tíma sett á fót sérstök nefnd, ICEPRO, sem þá nefndist „Nefnd um verklag í viðskiptum“. Henni var falið að fylgjast með starfi SÞ og öðru alþjóðlegu starfi á sviði rafrænna viðskipta. Nefndin hefur leitt þróun rafrænna viðskipta hér á landi. Hún gaf strax á árinu 1991 ítarlega handbók um SMT-viðskipti og það hefur komið í hennar hlut að sjá um staðfærslu þeirra alþjóðlegu rammaskeyta sem notuð eru í hefðbundnum SMT-viðskiptum. ICEPRO hefur haldið uppi öflugu nefndastarfi auk þess að gefa út fréttabréfið Viðskiptavakann sem fjallar um það helsta sem er að gerast á sviði rafrænna viðskipta hér á landi. Nefndin rekur einnig heimasíðu[6] með ítarlegum upplýsingum um rafræn viðskipti og tengingum við erlendar heimasíður um sama efni, ásamt

[5] Áætlunina er að finna á vefsíðu verkefnarstjórnarinnar, sjá: http://brunnur.stjr.is/interpro/for/for.nsf/pages/verk
[6] Sjá: http://www.chamber.is/icepro

því að standa reglulega fyrir ráðstefnum um það sem nýjast er á sviði rafrænna viðskipta hverju sinni.

Á sínum tíma var einnig stofnað sérstakt félag vegna SMT og nefndist það EDI-félagið og gaf það ásamt ICEPRO í október 1997 út bækling með fróðleik um rafræn viðskipti. Þann 1. júní 1998 sameinaðist EDI-félagið ICEPRO, sem nefnist nú „Nefnd um rafræn viðskipti". Hlutverk hennar er að stuðla að einföldun og samræmingu í rafrænum viðskiptum. Í starfsreglum ICEPRO eru nú m.a. ákvæði um að nefndin vinni að breytingum í þjóðfélaginu, þ.m.t. lagabreytingum sem styrkt geti hlutverk nefndarinnar.

Öflugt starf hefur farið fram á þessu og síðasta ári vegna rafrænna viðskipta á vegum viðskiptaráðuneytisins. Fyrst skal hér nefna útgáfu þess á ritinu „Rafræn viðskipti, umfjöllun um íslensk lög"[7]. Vorið 2000 voru síðan samþykkt þrjú lagafrumvörp sem unnin voru af nefndum á vegum ráðuneytisins, sem öll koma til með að hafa mikil áhrif á umhverfi og þróun rafrænna viðskipta. Nú síðast þann 17. maí s.l., kynnti ráðuneytið drög að frumvarpi um rafrænar undirskriftir sem ætlunin er að leggja fram á næsta þingi.

2. Þörf fyrir löggjöf

Í skýrslu Evrópubandalagsins frá 1991[8] vegna framkvæmdar svonefndrar TEDIS-áætlunar Evrópubandalagsins og EFTA um rafræn viðskipti, kemur fram að mestu erfiðleikarnir við framkvæmd hennar verði að sett lög geri ekki ráð fyrir rafrænum viðskiptaháttum. Í löggjöf aðildarlanda áætlunarinnar voru á þessum tíma og eru víðast enn ýmis ákvæði um að skjöl þyrftu hvort sem þau væru undirrituð eða ekki, að uppfylla ýmis skilyrði um ritun, útgáfu, sendingu, móttöku og varðveislu, til þess að tryggt væri að þau hefðu lagalegt gildi, hægt væri að framselja réttindi samkvæmt þeim, hlýtt væri ákvæðum laga og reglna um bókhald og skatta og hægt væri að nota þau sem sönnunargögn.

[7] Rafræn viðskipti, umfjöllun um íslensk lög eftir Gunnar Thoroddsen og Skúla Magnússon, rit 99-2, útgefið af iðnaðar- og viðskiptaráðuneytinu í febrúar 1999.
[8] Skýrsla nr. XIII/252/91-EN.

Í áðurnefndri handbók ICEPRO er sérstakur kafli um áhættuþætti í rafrænum viðskiptum og eru lagareglur og undirskrift í tölvu á meðal þeirra. Þar er talið afar mikilvægt að SMT-viðskipti verði að öllu leyti viðurkennd að lögum og endurskoðun lagaákvæða taki mið af þeim tækninýjungum sem séu að ryðja sér til rúms. Í bókinni kom jafnframt fram sú skoðun að nauðsynlegar breytingar á löggjöf vegna tilkomu rafrænna viðskipta myndu taka langan tíma.

Allsherjarþing Sameinuðu þjóðanna samþykkti á sínum tíma tilmæli til ríkisstjórna aðildarlanda samtakanna um að þær tryggðu fullnægjandi öryggi að lögum til þess að hægt yrði að taka upp sjálfvirkar gagnasendingar í alþjóðlegum viðskiptum. Vegna þessa gaf Efnahagsstofnun SÞ árið 1996 út fyrirmynd að lögum um rafræn viðskipti sem hægt væri að nota sem fyrirmynd að almennri löggjöf um þau.

Óhætt að segja að sú spá að breytingar á lagalegu umhverfi vegna breyttra viðskiptahátta myndu taka langa tíma hafi ræst. Hér á landi hefur laga- og reglugerðarumhverfi þó tekið miklum breytingum á undanförnum árum þannig að lagalegt umhverfi rafrænna viðskipta er nú allt annað en var í upphafi þeirra.

3. Sett lög

Hér og í næsta kafla verður getið helstu laga og reglna sem áhrif hafa á rafræn viðskipti almennt. Í kafla 7.2 er hins vegar fjallað um lög og reglur sem settar hafa verið vegna rafrænna viðskipta einstakra ríkisaðila.

Hér á landi hefur ekki verið gert markvisst átak til þess að breyta öllum þeim lögum og reglugerðum sem hugsanlega þarf að breyta vegna rafrænna viðskipta né hefur verið sett heildarlöggjöf vegna þeirra.

Norrænir fræðimenn í lögfræði eru almennt sammála um að rafræn skjöl rúmist ekki innan hefðbundinnar skilgreiningar

á hugtakinu skjal. Í íslenskum lögum og reglum hefur skjal því ekki verið talið ná til þeirra upplýsinga sem geymdar eru á tölvutæku formi, hvort sem þær nefnast rafræn skjöl, gögn eða upplýsingar, nema slíks sé sérstaklega getið.

Í bókhaldi fyrirfinnast ýmis konar fylgiskjöl. Þau eru ekki öll háð kröfum um form og efni því almennt gildir sú regla í viðskiptum að kaupandi og seljandi geta komið sér saman um hvaðeina, t.d. hvort fylgiskjal er rafrænt eða á pappír. Veigamesta undantekningin frá þessu samningsfrelsi tekur til reikninga því um þá gilda sérstakar reglur. Þau lög sem mestu máli skipta hér eru bókhaldslögin nr. 145/1994 og lög um virðisaukaskatt, nr. 50/1988. Ákvæði um form fylgiskjala er og að finna í fleiri sérlögum, t.d. tollalögum nr. 55/1987 með síðari breytingum.

1. Bókhaldslög nr. 145/1994

Þróun hófst fyrir nokkrum árum í þá átt að laga íslenska löggjöf að breyttum veruleika tölvualdar, sbr. inngang að athugasemdum með frumvarpi að lögum um bókhald, nr. 145/1994, þar sem segir m.a.:

> *„Þróun viðskipta á undanförnum árum er æ meir í þá átt að þau fari um tölvur og jafnvel án þess að pappír eða skjöl í almennum skilningi liggi til grundvallar. Að þessu leyti má halda því fram að núgildandi bókhaldslög standi íslensku viðskiptalífi og þróun þess fyrir þrifum og hamli gegn því að viðskiptalífið geti tileinkað sér þá kosti sem erlendir viðskipta- og samkeppnisaðilar geta nýtt sér.“*

Í bókhaldslögunum eru sérstök ákvæði um SMT-viðskipti. Í athugasemdum með frumvarpinu kemur fram að þörfin fyrir sérákvæðin um þau eigi rætur sínar í hinni viðteknu þröngu skilgreiningu skjalahugtaksins því þar segir m.a.:

> *„Í þessu kemur fram ný skilgreining á hugtakinu skjal. Fjallað er um pappírslaus viðskipti og skjalasendingar á milli tölva þótt engin skjöl í eiginlegri merkingu þess*

orðs fari á milli þeirra. Að vísu er hægt að prenta skjalið bæði hjá sendanda og viðtakanda. Skjalið er í tölvunni, óáþreifanlegt en sjáanlegt. Útprentunin er þá aðeins afrit af frumskjalinu.“

Bókhaldslögin gera ráð fyrir því að bókhaldsfærslur sem byggja á skjalasendingum milli tölva, SMT (EDI) séu jafnréttháar öðrum færslum ef þær uppfylla sömu kröfur um öryggi og áreiðanleika og gerðar eru til pappírsskjala, þar með talda samfellda númeraröð skjala og færslna. Krafa er hins vegar um að ávallt skuli vera unnt að kalla fram og prenta þau skjöl sem liggja til grundvallar SMT-færslum í bókhaldi.

II. kafli bókhaldslaganna fjallar um almenn ákvæði um bókhald. Í honum segir í 2. mgr. 9. gr.:

„Færslur, sem eingöngu byggjast á skjölum sem flutt eru milli tölvukerfa, skulu skráðar í bókhaldið jafntryggilega og aðrar færslur.“

Í greinargerð með frumvarpi að bókhaldslögunum segir m.a. eftirfarandi um II. kafla laganna:

„Í 2. mgr. 9. gr. er nýmæli er varðar skjalasendingar milli tölva, sem nefnt er pappírslaus viðskipti og er nýjasta þróunin í viðskiptum. Átt er við skjalasendingar milli tölva, SMT, sem er þýðing á enska heitinu Electronic Data Interchange, EDI. Hugtakið er notað um sendingar á stöðluðum og forsniðnum upplýsingum milli tölvukerfa tveggja aðila sem eiga í viðskiptum án þess að mannshöndin þurfi að koma þar nálægt, eða a.m.k. mjög lítið, eins og fram kemur í handbók ICEPRO, nefndar um verklag í viðskiptum, en upplýsingar úr þeirri handbók eru notaðar hér í þessari greinargerð.

Skjalasendingar milli tölva felast í því að sameina tölvu- og símatækni. Þær leysa af hólmi hefðbundin viðskiptaskjöl af ýmsu tagi sem venjulega eru á pappír og geyma alls kyns upplýsingar um viðskiptin sem þeim tengjast. Byggt er á fyrirfram ákveðnum og stöðluðum rammaskeytum í sam-

skiptum milli þeirra sem eiga í viðskiptum. Um er að ræða skipulögð upplýsingaskipti milli tölva sem gera þeim kleift að vinna og nýta upplýsingar sem þeim berast. Þessi skjalaskipti fara því aðeins fram að báðir aðilar samþykki þau fyrir fram. Jafnframt því sem viðskipti eiga sér stað á þennan hátt getur farið fram bókun þeirra beint á viðeigandi reikninga í bókhaldi beggja án frekari aðgerða og engin önnur skjöl liggja fyrir en þau sem tölvurnar geyma. "

Aðeins síðar segir og í athugasemdum við II. kaflann:

„Lagt er til að bókhaldsfærslur, sem byggjast á skjalasendingum milli tölva, verði jafnréttháar öðrum færslum enda uppfylli þær allar kröfur um öryggi og áreiðanleika sem gerðar eru til pappírsskjala. Gert er ráð fyrir að ráðherra setji með reglugerð nánari ákvæði um pappírslaus viðskipti og geymslu gagna á rafrænu formi."

Árið 1994 var hugtakið rafræn viðskipti lítið notað og það er hvorki að finna í bókhaldslögunum né í greinargerð með frumvarpi að lögunum. Þar er hins vegar talað um „skjalasendingar milli tölva sem nefnt er pappírslaus viðskipti". Af þeim tilvitnunum sem fram koma hér á undan er ljóst að bókhaldslögin fjalla beinlínis eingöngu um þá tegund rafrænna viðskipta sem allsráðandi voru á þeim tíma sem þau voru sett og nefnd eru bein og hefðbundin SMT-viðskipti í riti þessu. Talað er um samskipti með stöðluðum skeytum skv. UN/EDIFACT-staðli á milli tveggja tölvukerfa sem vinna bæði að mestu sjálfvirkt úr gögnunum og viðskiptin eru á milli aðila sem fyrirfram hafa samið um viðskipti sín vegna þess að þeir eru í föstu viðskiptasambandi. Lögin og greinagerðin fjalla því ekki beinum orðum um rafræn viðskipti í þeim víða skilningi sem einkennir notkun þessa hugtaks í dag, því það nær til rafrænna viðskipta sem gerð eru með afar fjölbreyttum tæknilegum aðferðum og ólíkum sniðum, þar sem stofnanir, fyrirtæki eða einstaklingar geta átt hlut að máli.

2. Lög nr. 50/2000 um lausafjárkaup

Í maí s.l. voru samþykkt á Alþingi ný lög um lausafjárkaup. Lögin sem ætlað er að leysa af hólmi eldri lög frá árinu

1922, öðlast ekki gildi fyrr en 1. júní 2001 og gilda eingöngu um samninga sem gerðir eru eftir þann tíma.

Lögin eiga við um svokölluð neytendakaup en það eru kaup þar sem seljandinn hefur atvinnu sína af sölu og söluhlutur er aðallega ætlaður til persónulegra nota fyrir kaupandann, fjölskyldu hans og þá sem hann umgengst nema seljandi hafi við samningsgerð hvorki vitað né mátt vita að hluturinn var keyptur í þessu skyni.

Við setningu hinna nýju kaupalaga voru fjögur meginmarkmið höfð að leiðarljósi. Í fyrsta lagi að laga íslenska viðskiptalöggjöf að breyttum viðskiptaháttum, m.a. rafrænum, og breyttri þjóðfélagsumgjörð enda bráðum 80 ár frá lögfestingu gildandi kaupalaga. Í öðru lagi að efla réttarstöðu neytenda. Í þriðja lagi að tryggja norræna réttareiningu á sviði kauparéttar og í fjórða lagi að leiða í lög hér á landi efnisákvæði samnings Sameinuðu þjóðanna um sölu á vöru milli ríkja, „The 1980 United Nations Convention of the International Sale of Goods“ (CISG). Hinum nýju lögum er ætlað að tryggja að þeir sem viðskipti stunda geti fremur reitt sig á að svipaðar reglur gildi í megindráttum um sömu réttaratriðin, hvort sem kaup gerast á innlendum eða erlendum vettvangi.

3. Lög nr. 46/2000 um húsgöngu- og fjarsölusamninga

Í maí s.l. voru samþykkt ný lög um húsgöngu- og fjarsölusamninga. Frumvarp að lögum þessum var samið í viðskiptaráðuneytinu í þeim tilgangi að lögleiða ákvæði tilskipunar Evrópubandalagsins nr. 97/7 um neytendavernd að því er varðar fjarsölusamninga. Við undirbúning frumvarpsins var ákveðið að jafnframt skyldi í frumvarpinu vera ákvæði sem lögleiða tilskipun 85/577 um að vernda neytendur þegar samningar eru gerðir utan fastra starfsstöðva en áðurnefnd tilskipun var lögleidd með setningu laga nr. 96/1992 um húsgöngu- og fjarsölu.

Ástæða áðurnefndrar sameiningar er sú að hagræði er talið felast í því fyrir neytendur og seljendur að hafa reglur um

neytendavernd innan sömu laganna, sérstaklega þar sem ör þróun hafi verið í þá átt að skil milli ólíkra söluaðferða hafi verið að eyðast. Þannig sé nú algengt að samhliða því að stunda verslun á fastri starfsstöð skipuleggi seljandi auk þess netverslun eða aðrar tegundir fjarsölu. Við gildistöku laganna þann 1. júní 2000 féllu úr gildi áðurnefnd lög nr. 96/1992 um húsgöngu og fjarsölu.

4. Lög nr. 43/2000 um lagaskil á sviði samningaréttar

Lagaskilaréttur, þ.e. alþjóðlegur einkamálaréttur, er sú grein lögfræðinnar sem segir til um hvaða landslögum beri að beita við úrlausn ágreiningsefnis sem tengist fleiri en einu réttarkerfi.

Eftir því sem viðskipti einstaklinga og fyrirtækja verða algengari yfir landmæri eykst nauðsyn þess að í lögum sé að finna skýrar reglur um hvaða lög eigi að leggja til grundvallar í viðskiptum tveggja aðila sem ekki eru búsettir innan sama ríkis. Vegna örrar þróunar rafrænna viðskipta hefur þörf fyrir löggjöf um meginreglur lagaskila á sviði samningaréttar vaxið mjög á undanförnum árum.

Sett hafa verið sérstök lög nr. 43/2000 um lagaskil á sviði samningaréttar. Í þeim eru skrásettar ýmsar meginreglur lagaskilaréttar og skýrt kveðið á um eftir lögum hvaða ríkis skuli fara ef upp kemur ágreiningur í viðskiptum yfir landamæri. Lögin, sem grundvölluð eru á svonefndum Rómarsamningi („The Rome Convention“) frá 19. júní 1980, leiða til þess að íslenskar lagaskilareglur hafa nú verið samræmdar þeim reglum sem um lagaskil gilda í aðildarríkjum Evrópubandalagsins og ættu að stuðla að aukinni réttarvernd aðila í viðskiptum.

4. Útgefnar reglugerðir

Hér á eftir verður fjallað um tvær nýlegar reglugerðir sem skipta verulegu máli varðandi notkun rafrænna viðskipta almennt.

1. Reglugerð nr. 598/1999 um rafrænt bókhald o.fl.

Þann 6. september 1999 gaf fjármálaráðuneytið með vísan til heimildar í bókhaldslögum, út reglugerð nr. 598/1999. Í fréttatilkynningu ráðuneytisins nr. 13/1999, frá 1. október 1999 segir svo m.a.:

„Með útgáfu reglugerðar um rafrænt bókhald, geymslu rafrænna gagna og lágmarkskröfur til rafrænna bókhaldskerfa er stigið stórt skref í átt til framfara sem eflaust mun auðvelda frekari þróun rafrænna viðskipta. Bókhald, sem hingað til hefur verið fært með hjálp tölvu, hefur annað hvort orðið að liggja fyrir í prentuðu formi eða verið myndað á örfilmu og öll bókhaldsskjöl hafa verið á pappír. Við samningu reglugerðarinnar hefur verið gengið út frá því að allar upplýsingar sem eiga uppruna sinn í tölvu og sendar eru á milli gagnavinnslukerfa fyrirtækja megi varðveita áfram á rafrænu formi bæði hjá sendanda og móttakanda í þeim miðli án þess að þær verði færðar yfir á pappír og á það bæði við um sölureikninga og kostnaðarreikninga."

Heiti I. kafla reglugerðarinnar er „Bókun rafrænna viðskipta." Í 1. gr. rgl. eru þau skilgreind þannig:

> ***Rafræn viðskipti:*** *„Viðskipti þar sem pöntun, reikningsútgáfa eða greiðslur fara fram með rafrænum hætti."*

Skilgreining þessi er mjög víð, þ.e. nær til margra mismunandi tegunda af rafrænum viðskiptum, og er það í góðu samræmi við það sem nú tíðkast.

Í 1. greininni er og að finna eftirfarandi skilgreiningar:

> ***Rafrænt bókhald****: „Bókhald, eða sá hluti bókhalds, sem byggist á gögnum og færslum sem eiga uppruna sinn í gagnavinnslukerfum og send eru á milli þeirra með skeytum."*

Gagnavinnslukerfi: *„Ein eða fleiri tölvur, fylgitæki og hugbúnaður sem notuð eru til skipulagðra aðgerða á bókhaldsfærslum.“*

Skeyti: *„Safn samstæðra gagna sem raðað er samkvæmt ákveðnum stöðlum til gagnaflutnings og mynda fylgiskjöl í rafrænu bókhaldi. “*

Gagnaflutningur: *„Sending skeyta með rafeindaboðum þar sem skeytið er þannig forsniðið að unnt sé að lesa það í slíku kerfi og vinna sjálfvirkt á rafrænan og ótvíræðan hátt.“*

I. kafli reglugerðarinnar geymir auk skilgreininga ákvæði um skilyrði, áreiðanleika skeyta, gagnadagbók, skráningu sendra og móttekinna skeyta, hvenær skeyti telst skráð, leiðréttingar og aðgang að gögnum. Skoðun á ákvæðum kaflans vekur spurningar um það hvort heiti hans „Bókun rafrænna viðskipta“ sé ekki mun víðara en efni hans því ekki er annað að sjá en að ákvæði kaflans nái aðeins til tiltekinna tegunda af rafrænum viðskiptum, þ.e. þeirra sem nefnd eru bein í riti þessu og fara fram á milli tveggja tölva. Óljóst er hvort ákvæði kaflans ná til óbeinna rafrænna viðskipta. Sama gildir um önnur ákvæði reglugerðarinnar.

2. Breytingar á reglugerð nr. 50/1993 um bókhald og tekjuskráningu vsk-skyldra aðila

Hér á landi gildir sú meginregla að við hverja sölu eða afhendingu á vöru eða skattskyldri þjónustu, skuli seljandi gefa út reikning, sbr. 1. mgr. 20. gr. laga nr. 50/1988 um virðisaukaskatt. Heimild til undanþágu frá meginreglunni er í 2. mgr. 21. gr. sömu laga því þar segir að fjármálaráðherra sé heimilt að mæla fyrir um í reglugerð, að þegar sérstakar aðstæður séu fyrir hendi megi taka upp aðrar aðferðir við tekjuskráningu enda sé í stað reiknings notað annað öruggt skráningar- og eftirlitskerfi. Slík reglugerðarákvæði hafa nú verið sett.

Samhliða útgáfu áðurnefndrar reglugerðar um rafrænt bókhald o.fl., gaf fjármálaráðuneytið einnig út reglugerð nr. 599/1999 um breytingu á reglugerð nr. 50/1993 um bókhald og tekjuskráningu virðisaukaskattskyldra aðila. Í fyrrnefndri fréttatilkynningu ráðuneytisins segir m.a. að breytingarnar séu „.... í þá veru að þeim aðilum verði gert mögulegt að nýta sér rafrænt bókhald og rafræn gögn, þ.m.t. rafræna sölureikninga.“ Með öðrum orðum má segja að breytinga-reglugerðin mæli fyrir um að rafrænn sölureikningur jafngildi sölureikningi á pappír ef sá fyrrnefndi uppfyllir sérstaklega tilgreind ákvæði reglugerðar um rafrænt bókhald, m.a. í I. kafla hennar, sem áður var vikið að.

3. Helstu áhættuþættir í rafrænum viðskiptum

Í 2. kafla rits Ríkisendurskoðunar um rekstraröryggi upplýsingakerfa er fjallað um helstu áhættuþætti í rekstri þeirra. Þar er bent á að tegundir tölvuumhverfis, hegðun starfsmanna, Netið, tölvuveirur, rafræn viðskipti, eldsvoðar og vatnsskemmdir, náttúruhamfarir, opnun upplýsingakerfa ríkisins, gjaldþrot hugbúnaðarfyrirtækja, brotthvarf lykilstarfsmanna og tölvuinnbrot séu helstu áhættuþættirnir.

Rafræn viðskipti eru talin til áhættuþátta í rekstri upplýsingakerfa og er áhættan í beinu hlutfalli við mikilvægi viðskiptanna fyrir viðkomandi rekstur. Í þessu riti verður sjónum eingöngu beint að þeim áhættuþáttum sem tengjast rafrænum viðskiptum sérstaklega. Um aðra áhættuþætti vísast í áðurnefnt rit um rekstraröryggi upplýsingakerfa.

Nú eru rafræn viðskipti ekki eingöngu bein og hefðbundin SMT-viðskipti sem fylgja staðlinum UN/EDIFACT. Nýjar einfaldari og ódýrari leiðir til þess að stunda rafræn viðskipti eru nú ýmist til staðar eða í þróun. Því mun á næstunni ört fjölga þeim aðilum sem telja hagkvæmt að taka rafræn viðskipti upp í stað hefðbundinna. Ríkisaðilar hljóta að verða þar á meðal. Nauðsynlegt er að gera sér grein fyrir því hvaða áhætta getur fylgt því fyrir þá að stunda viðskipti með þessum hætti og hvernig á að bregðast við henni.

Í þessum kafla verður fjallað um það hverjir eru helstu áhættuþættir rafrænna viðskipta. Mikilvægt er að gera sér grein fyrir því að áhætta nær bæði til þess sem gerst getur innanhúss og þess sem gerst getur í samskiptum við gagnaðilann.

3.1 Allt stendur og fellur með kerfinu

Rekstraröryggi upplýsingakerfa byggir á því að kerfi sé bæði aðgengilegt og nothæft.

Miklu máli skiptir að vel sé vandað til verka við undirbúning þess að rafrænir viðskiptahættir leysi þá hefðbundnu af hólmi. Áhætta getur falist í því að flýta sér um of við slíkt verkefni. Mikilvægt er að vel sé staðið að vali og prófun tæknilegra útfærslna, m.a. er viss áhætta falin í því að styðjast ekki við viðurkennda staðla því það getur falið í sér ógnun við framtíðar samskiptamöguleika við aðra viðskiptaaðila. Rangt hannað eða uppsett rafrænt viðskiptakerfi getur valdið truflunum á viðskiptum eða jafnvel stöðvun þeirra um lengri eða skemmri tíma.

Eftir að rafrænt viðskiptakerfi er orðið að föstum lið í viðkomandi rekstri og það hefur unnið vandræðalaust um lengri tíma blasir við nýr áhættuþáttur. Hann er sá að menn fari algjörlega að treysta á hina rafrænu viðskiptahætti þannig að með tímanum dragi úr möguleikunum á því að hverfa aftur til eldri viðskiptaaðferða ef rafræna viðskiptakerfið verður óstarfhæft um lengri eða skemmri tíma vegna t.d. bilana, óhappa, bruna eða náttúruhamfara.

3.2 Áreiðanleiki og uppruni gagna

Áreiðanleiki gagna byggir á því að þau séu rétt skráð, heildstæð, þ.e. öll gögn skráð, og gild. Uppruni gagna tengist sönnun á því að höfundur þeirra sé sá sem hann segist vera en ekki einhver annar.

Rafræn viðskipti fela í sér lagalega bindandi gerning á milli viðskiptaaðila. Mikilvægt er því að ekki sé hægt að breyta skeyti án þess að það sjáist, að hægt sé að staðfesta að skeyti sé rétt og hægt sé að tengja efni þess við sendanda. Því þarf að huga vel að þeim áhættuþáttum sem tengjast áreiðanleika og uppruna skeyta.

Kröfur um áreiðanleika gagna er m.a. að finna í 8. gr. laga nr. 145/1994 um bókhald en þar segir að sérhver færsla í bókhaldi skuli byggð á áreiðanlegum og fullnægjandi gögnum sem rekja megi til viðskiptanna. Í 2. mgr. 9. gr. sömu laga segir svo að færslur sem eingöngu byggjast á skjölum sem flutt eru milli tölvukerfa skulu skráðar í bókhaldið jafntryggilega og aðrar færslur. Í greinargerð með frumvarpinu segir að um sé að ræða nýmæli því lagt sé til að bókhaldsfærslur sem byggjast á slíku kerfi pappírslausra viðskipta verði jafnréttháar öðrum færslum enda uppfylli viðkomandi færslur allar kröfur um öryggi og áreiðanleika.

Þegar samskipti fara fram með pappírsskjölum getur móttakandi bréfs séð hvort umslag hefur verið opnað og texta bréfsins breytt. Bréfsefni og undirskrift þjóna síðan þeim tilgangi að sanna fyrir móttakanda bréfs hver sendandi þess er. Í reynd eru bréfleg samskipti venjulega með þeim hætti að menn gefa framangreindum atriðum ekki gaum nema eitthvað sérstakt komi til.

Þegar samskipti eru rafræn eru ekki í þeim nein sýnileg ummerki sem leiða til þess að móttakandi uppgötvi að innihaldi skeytis hafi verið breytt eða að sendandi þess sé í raun annar en skeytið ber með sér. Sérstakar aðgerðir þurfa því að koma til svo að móttakandi rafræns skeytis uppgötvi svik eða heimildarlausar færslur.

Meðal áhættuþátta vegna áreiðanleika og uppruna gagna í rafrænum viðskiptum eru lélegt aðgangskerfi, kæruleysilegur umgangur við lykilorð, ónógar varnir gegn tölvuinnbrotum og ónógt öryggi við skeytasendingarnar sjálfar.

Ef ekki er brugðist við framangreindum áhættuþáttum geta þeir leitt til heimildarlausra breytinga, t.d. á magni, fjárhæð og móttakanda eða sendanda skeytis, frá því að starfsmaður sem til þess hefur heimild skráði gögnin þar til þau eru send. Slíkar breytingar geta bæði aðrir starfsmenn og óviðkomandi aðilar gert.

Sérstaklega skal bent á það að ónógt öryggi felur ekki bara í sér hættu á því að verið sé að hrófla við þegar gerðum

færslum áður en þær er sendar. Hætta getur og verið á því að færslur séu búnar til í heimildarleysi eða á sviksamlegan hátt af starfsmanni sem hefur heimild til þess að búa til viðskiptaskeyti. Viðskiptaaðilar þurfa því að huga að því hvernig þeir vilja bregðast við heimildarlausum færslum starfsmanna sinna. Mesta hættan felst þó líklega í því að óviðkomandi aðilar brjótist inn í kerfi og búi þar til færslur til sendingar til aðila sem sá sem brotist er inn hjá í reglulegu viðskiptasambandi við því í slíkum tilvikum má búast við því að móttakandinn bregðist eðlilega við og afgreiði málið.

Í rafrænum viðskiptum verður að tryggja að skeytum sé ekki breytt eða þau búin til af starfsmanni í heimildarleysi eða af utanaðkomandi aðila áður en þau eru send móttakanda.

Vegna innra eftirlits er í hefðbundnum pappírsviðskiptum oft gerðar kröfur um að heimild til afgreiðslu, pöntunar, greiðslu o.fl., sé staðfest með áritun tiltekins aðila, eins eða fleiri. Í rafrænum viðskiptum þurfa aðrar aðferðir að leysa af hólmi slíkar staðfestingar til þess að tryggja að færslur séu ekki gerðar í heimildarleysi.

3.3 Villur í gagnavinnslu, hugbúnaði eða skeytasendingum

Meðal áhættuþátta í rafrænum viðskiptum eru villur sem geta komið upp í vinnslu gagna eða í þeim hugbúnaði sem notaður er hjá viðskiptaaðilunum. Einnig geta villur komið upp við gagnasendingarnar sjálfar og geta þær átt uppruna sinn hjá sendanda eða virðisaukandi netþjónustu, í símakerfinu eða hjá móttakanda.

Veruleg áhætta felst og í ónógum eða röngum leiðbeiningum til starfsmanna sem koma að vinnslu rafrænna viðskiptagagna og skorti á verklagsreglum því það getur bæði leitt til rangra viðbragða þegar eitthvað fer úrskeiðis og rangra eða ónógra leiðréttinga á villum. Miklu máli skiptir og að öguð vinnubrögð séu viðhöfð við allar breytingar sem

gerðar eru á hugbúnaði.

Hugsanlegt er að villur af ofangreindum ástæðum séu þess eðlis að þær fari óhindrað alla leið í gegnum vinnslu og afgreiðslu hjá móttakanda og uppgötvist ekki fyrr en síðar ef ekki eru viðhafðar öryggisráðstafanir sem tryggja að efni skeytis sé rétt. Dæmi um þetta gæti t.d. verið ef pöntun á 1,00 tölvu yrði að pöntun á 100 tölvum vegna villu við þýðingu innanhússskrár yfir á staðlað eða annað snið sem aðilar hafa samþykkt að nota í viðskiptum sínum. Ef svona villa kemur upp í framhaldi af breytingum á þýðingarhugbúnaði getur hún valdið því að allar færslur verði rangar.

Villur af þeim ástæðum sem að ofan greinir geta þó uppgötvast hjá móttakanda þar sem þær eru þess eðlis að hugbúnaðarkerfi hans getur ekki vélrænt og viðstöðulaust unnið úr skeytinu. Svo væri m.a. ef skeyti fylgir ekki umsömdum staðli eða er skemmt að hluta til eða alveg.

Villur geta einnig leitt til þess að skeyti eru send oftar en einu sinni, skila sér ekki fyrr en seint og um síðir eða þau týnast jafnvel alveg.

Öryggisráðstafanir þurfa að vera til staðar til þess að taka á öllum ofangreindum tilvikum. Um þær er fjallað í 5. kafla.

3.4 Leynd gagna ekki tryggð

Skeyti í rafrænum viðskiptum geyma oft viðkvæmar upplýsingar, t.d. um verð, sem leynt eiga að fara. Leynd viðskiptagagna er sjaldnast lögbundin. Oftast byggist hún á samkomulagi aðila. Oft skiptir leynd svo miklu máli að viðskiptin myndu ekki fara fram með rafrænum hætti ef menn teldu hættu á því að óviðkomandi aðilar gætu komist að efni þeirra.

Algengt er í rafrænum viðskiptum að skeytasendingar fari fram í gegnum virðisaukandi netþjónustuaðila sem reka sérstakar gagnaflutningslínur. Skeyti í rafrænum viðskiptum

getur þurft að fara í gegnum mörg net áður en það nær endanlegum áfangastað. Ef skeyti er ekki dulkóðað geta þjónustuaðilar og aðrir hugsanlega lesið, eytt eða breytt innihaldi skeytisins eða tafið móttöku þess, ýmist af ásetningi eða gáleysi, á þeim tíma sem líður frá því að það er sent þar til það er komið á áfangastað.

3.5 Vélrænt eftirlit án hefðbundinnar endurskoðunarslóðar

Ein af meginreglum innra eftirlits í hefðbundnum pappírsviðskiptum er sú að dreifa einstökum liðum verkferlis á milli starfsmanna til þess að draga úr hættu á villum og svikum. Dæmi um þetta er þegar einn starfsmaður samþykkir pöntun en annar ber saman reikning, pöntun og afhendingarseðil áður en greiðsla er innt af hendi.

Vegna vélræns flæðis gagna í rafrænum viðskiptum kemur færra fólk að þeim en hinum hefðbundnu. Slíkt hefur í för með sér skort á viðteknum eftirlitsaðgerðum sem fylgja aðgreiningu starfa. Að auki fylgir rafrænum viðskiptum yfirleitt lítið sem ekkert af þeim pappírsgögnum sem skipta höfuðmáli við eftirlit í hefðbundnu pappírsumhverfi.

Þar sem hefðbundnir eftirlitsþættir eru af skornum skammti skiptir höfuðmáli að þær eftirlitsaðgerðir sem byggðar eru inn í rafræna viðskiptakerfið vegi upp á móti því að eftirlit er á fárra höndum og hefðbundin endurskoðunarslóð að litlu leyti til staðar.

3.6 Treysta þarf á gagnaðila/þriðja aðila

Einn af áhættuþáttum í rafrænum viðskiptum er að aðilar viðskiptanna hafa ekki lögsögu yfir öllum þeim öryggisráðstöfunum sem máli geta skipt til þess að viðskiptin gangi snurðulaust fyrir sig. Samskiptin eru með þeim hætti að viðskiptaaðilar eru í raun með sameiginlega lausn því skeyti sem send eru á milli þeirra fá vélræna úrvinnslu án þess að

mannshöndin þurfi að koma þar nærri, a.m.k. í beinum rafrænum viðskiptum. Aukin áhætta er því til staðar vegna tengsla viðskiptaaðilanna og þeirrar opnunar og sjálfvirkni sem fylgir þeirri hagkvæmni sem rafrænum viðskiptum er ætlað að stuðla að. Þetta hefur það í för með sér að brestir í öryggi gagnaðila geta haft alvarlegar afleiðingar fyrir hinn aðilann.

Þegar aðilar í rafrænu viðskiptasambandi eru háðir hvor öðrum með þeim hætti sem áður er lýst þurfa þeir ekki eingöngu að vera vissir um að öryggismál séu í besta lagi hjá þeim sjálfum, heldur verða þeir og að vera vissir um að svo sé einnig hjá gagnaðilanum. Óhjákvæmlegt er því að aðilar í föstu viðskiptasambandi semji um öryggismál sín.

Þegar viðskiptaaðilar hafa falið þriðja aðila, þ.e. virðisaukandi netþjónustu, að sjá um samskipti sín þurfa aðilar viðskiptasambandsins að geta treyst því að þau séu og verði í lagi. Meðal áhættuþátta hér eru þeir að virðisaukandi netþjónustuaðilinn sendi viðskiptaaðilum gögnin ekki á réttum tíma eða að neyðaráætlanir séu ekki til staðar ef rekstur netþjónustunnar stöðvast af einhverjum ástæðum. Viðskiptaaðilar skulu ekki treysta í blindni á öryggi þjónustuaðila. Semja þarf um öryggismál í tilvikum sem þessum.

3.7 Lagaleg óvissuatriði

1. Skortur á lagareglum

Skortur á lagareglum er nú mun minni áhættuþáttur í rafrænum viðskiptum en á fyrstu árum þeirra, sbr. kafla 2.4 þar sem farið er yfir helstu breytingar sem gerðar hafa verið á lagalegu umhverfi í rafrænum viðskiptum á undanförnum árum.

Athyglisvert er að þrátt fyrir áhyggjur manna á árum áður vegna skorts á lagareglum um rafræn viðskipti virðist sem enn hafi hvergi komið til umtalsverðra málaferla vegna þeirra.

Þó að löggjöf hérlendis hafi að nokkru verið sniðin að rafrænum viðskiptum og gera megi ráð fyrir því að fljótlega komi til löggjöf um rafrænar undirskriftir, er langt frá því að allri óvissu vegna rafrænna viðskipta hafi verið eytt. Nauðsynlegt er því fyrir viðskiptaaðila að eyða henni eftir því sem kostur er.

2. Gildi rafrænna skjala og undirskrifta

Í lögum og reglugerðum er víða að finna skilyrði um að undirskriftir eigi að vera skriflegar. Eins og áður er komið fram er í norrænum rétti gert ráð fyrir því að skjal eigi aðeins við um pappírsskjal og undirskrift eigi aðeins við um skriflega undirskrift nema annað sé beinlínis tekið fram. Vegna þessa var strax við upptöku rafrænna viðskipta talið ljóst að einn af áhættuþáttum þeirra væri lagalegt gildi rafrænna skjala og undirskrifta.

Engar kröfur eru um form við samningagerð í norrænum rétti. Samningur er gildur og bindandi hvort sem hann er gerður munnlega, skriflega eða með milligöngu tölva. Formið getur hins vegar skipt máli þegar upp kemur ágreiningur um gildi, efni eða efndir samningsins þar sem sönnun er að jafnaði erfiðari ef ekki er gengið frá samningi með formlegum hætti.

Með auknum rafrænum samskiptum á Netinu hefur æ betur komið í ljós hversu hinar hefðbundnu kröfur löggjafarinnar um að skjöl séu á pappír og undirrituð duga skammt í tæknivæddum heimi. Þjóðhagslega er hagkvæmt að auka rafræn samskipti. Þess vegna væri æskilegt að ákveðið væri með lögum hvenær og á hvaða sviðum rafræn samskipti með rafrænni undirskrift eru talin jafngild hefðbundnu pappírsskjali með undirskrift og hvenær ekki.

Mikil vinna hefur á síðustu árum farið fram bæði í einstökum löndum og á alþjóðavettvangi við að kanna hvernig hægt er með formlegum hætti að fullgilda efni löggernings og þeirra skuldbindinga sem honum fylgja, þegar

tölvur eru notaðar sem tæki í viðskiptum í stað hefðbundinna pappírsskjala með skriflegri undirritun. Virðist sem hilli undir raunverulegur árangur af því starfi.

Árið 1996 gaf Alþjóða viðskiptalaganefnd Sameinuðu þjóðanna UNCITRAL („United Nation Commission of International Trade Law"), út drög að lögum um rafræn viðskipti[9] sem síðan voru samþykkt með sérstakri ályktun á Allsherjarþingi SÞ. Drögunum er ætlað að auðvelda aðildarríkjum samtakanna að setja almenna löggjöf um rafræn viðskipti sem byggi á því að rafræn skjöl séu lögð að jöfnu við pappírsskjöl, ef þau réttindi sem pappírsskjalið tryggir eru eins vel tryggð með rafrænu skjali. Með drögunum fylgir leiðbeiningabæklingur með ýmsum bakgrunnsupplýsingum og skýringum til að auðvelda vinnu þeirra sem vilja nýta sér drögin til þess að undirbúa almenna löggjöf um rafræn viðskipti í ríkjum sínum.[10]

Einhverjar þjóðir munu væntanlega nýta sér áðurnefnt starf og setja löggjöf með svipuðu sniði og að framan greinir en ljóst er að ekki geta rafræn skjöl í öllum tilvikum verið jafngild skriflegum. Mikil vinna við undirbúning slíkrar löggjafar felst því í að kanna hver þau tilvik eru og undanskilja þau. Sama vinna er nauðsynleg fyrir þær þjóðir sem ekki ætla sér að setja almenn lög um jafngildi heldur fara þá leið að breyta einstökum lögum sem áskilja pappírsskjöl og skriflega undirskrift ef rafræn skjöl og undirskriftir eru taldar koma að sama gagni.

Ekki er nægilegt að ákveða í löggjöf að rafræn undirskrift jafngildi skriflegri. Með verður að fylgja hvaða tegundir rafrænna undirskrifta teljast jafngildar. Það eru yfirleitt eingöngu þær tegundir sem taldar eru tryggja að efni rafræna skjalsins sé óbreytt frá því að skrifað var undir það rafrænt og að öruggt sé að undirskriftin sé gild. Jafnframt að móttakandi geti ekki neitað að hafa tekið við skjali sem hann hefur móttekið.

[9] „UNCITRAL Model Law on Electronic Commerce". Ályktun Allsherjarþings Sameinuðu þjóðanna nr. 51/162 frá 16. desember 1996.

[10] „Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce ", 1996.

Iðnaðar- og viðskiptaráðuneytið kynnti á fundi þann 17. maí s.l. drög að frumvarpi til laga um rafrænar undirskriftir og hefur viðskiptaráðherra lýst því yfir að frumvarpið verði lagt fyrir Alþingi á haustþingi 2000.

Drögin gera ráð fyrir því að þróuð rafræn undirskrift sem studd er gæðavottorði, (hvort tveggja nákvæmlega skilgreind hugtök), og gerð með öruggum undirskriftarbúnaði séu jafngild handritaðri undirskrift. Ekki er gert ráð fyrir því að lögin veiti sjálfstæðan rétt til að eiga samskipti með rafrænum hætti og þeim er ekki ætlað að grípa inn í samningarétt eða formkröfur í lögum. Ætlunin er að semja um tiltekið kerfi vegna rafrænna undirskrifta. Ef það væri notað tryggði það tiltekin réttaráhrif sem víðtæk samstaða hefur náðst um meðal aðildarlanda EB, Íslands og Noregs.

Þess er að vænta að rafræn undirskrift í samræmi við kröfur laga muni hafa mikið sönnunargildi í málaferlum en lokaorðið um það hvort hún er sönnun fyrir því að tiltekinn aðili hafi skrifað undir tiltekna tilkynningu verður dómstólanna. Þeir verða, alveg eins og vegna hefðbundinna undirskrifta, að leysa úr því í hverju máli, hvort sá sem skrifaði undir er sá sem undirskrift segir að hann sé, og í hve ríkum mæli skjalinu hefur verið breytt eftir útgáfu þess.

4. Áhættumat og öryggisstefna

Í kaflanum hér á undan var fjallað um þá sérstöku áhættuþætti sem fylgt geta rafrænum viðskiptum en jafnframt var þar vísað til rits Ríkisendurskoðunar um rekstraröryggi upplýsingakerfa en þar er að finna ítarlega umfjöllun um almenna áhættuþætti vegna reksturs þeirra.

Grundvöllur að allri öryggisvinnu vegna upplýsingakerfa er gerð áhættumats og mótun öryggisstefnu. Því þarf hver sá ríkisaðili sem fyrirhugar að taka upp rafræn viðskipti að meta hvaða áhættu það getur haft í för með sér fyrir rekstur hans og í framhaldi af því að taka á því í öryggisstefnu sinni.

4.1 Gerð áhættumats

Í margnefndu riti stofnunarinnar um rekstraröryggi upplýsingakerfa er mjög ítarlegur kafli um gerð áhættumats. Þar er fjallað um mikilvægi upplýsingakerfa og gagna og flokkun og forgangsröðun kerfa og gagna út frá mikilvægi þeirra. Fjallað er um stofnun öryggishóps, nauðsyn þess að meta þá sérstöku áhættuþætti sem steðjað geta að öryggi kerfanna í þeim tiltekna rekstri sem um er að ræða, hvaða líkur eru á því að áhætta verði að raunveruleika og hverjar eru hugsanlegar afleiðingar rekstrartruflana. Einnig er rætt um þau svör sem liggja eiga fyrir að áhættumati loknu og þá þörf sem er fyrir stöðugt endurmat áhættunnar. Til viðbótar við þessi atriði þarf við áhættumatið að skoða og meta þá þætti sem fjallað er um hér á eftir. Einnig er gagnlegt í þessu sambandi að lesa kaflann um áhættumat í riti Ríkisendurskoðunar um innra eftirlit[11].

[11] Innra eftirlit, Ríkisendurskoðun, útgefið í desember 1998.

Það á að vera hlutverk öryggishóps vegna reksturs upplýsingakerfa að meta þá áhættu sem fylgt getur rafrænum viðskiptum fyrir viðkomandi stofnun eða fyrirtæki.

1. Eðli viðskiptasambands

Ekki er í ritinu um rekstraröryggi upplýsingakerfa fjallað um eðli viðskiptasambanda en skoðun á þeim þætti skiptir höfuðmáli við áhættumat vegna rafrænna viðskipta.

Ljóst er að áhætta í rafrænum viðskiptum er mismunandi mikil eftir því hvort þau eru á milli aðila í föstu eða tilfallandi viðskiptasambandi.

Minni áhætta ætti að jafnaði að fylgja rafrænum viðskiptum aðila í föstu viðskiptasambandi en tilfallandi. Ástæðan er sú að þeir fyrrnefndu geta dregið úr áhættunni með því að ákveða tilhögun samskiptanna í samningi, þar sem m.a. er fjallað um það hvernig leysa á úr hugsanlegum álitaefnum. Þetta þarf öryggishópurinn þó að vega og meta.

2. Tæknilegar útfærslur

Ljóst er að meðal þeirra þátta sem þarfnast alveg sérstakrar skoðunar við áhættumat vegna rafrænna viðskipta er sú hlið þeirra sem snýr að því hvernig þau eigi að fara fram. Hér er í raun átt við skoðun og mat á upplýsingatæknilegum atriðum sem skipta máli við val á rafrænum viðskiptaaðferðum.

Hér skiptir m.a. meginmáli hvort um er að ræða bein samskipti á milli tölva, þ.e. það sem oft eru nefnd bein rafræn viðskipti eða hvort um er að ræða samskipti á milli manns og tölvu, oft nefnd óbein rafræn viðskipti. Í síðara tilvikinu er oft um það að ræða að kaupanda er veittur aðgangur að tölvukerfi seljanda og í það skráir kaupandi pöntun sína, greiðslufyrirkomulag o.fl.

3. Flokkun upplýsingakerfa og gagna

Vegna flokkunar upplýsingakerfa út frá mikilvægi við áhættumat skal aðeins drepið á það hér að rafræn viðskiptakerfi eru oft á tíðum ákaflega mikilvæg í rekstri og því mikil þörf á því að tryggja rekstraröryggi þeirra. Þetta verður að hafa í huga við áhættumat. Hér kemur m.a. til skoðunar hversu langur sá tími er sem ásættanlegt telst að kerfi sé ekki aðgengilegt eða nothæft.

Við mat á áhættu við það að fara úr hefðbundu viðskiptaumhverfi yfir í rafrænt þarf að meta og flokka rafrænu viðskiptagögnin út frá fleiri þáttum en hefðbundið er vegna almenns rekstraröryggis upplýsingakerfa.

Við áhættumat ætti að flokka rafræn viðskiptagögn út frá:

1) Mikilvægi gagnanna fyrir viðkomandi rekstur.
2) Kröfum um aðgengileika.
3) Mikilvægi þess að gögnin séu áreiðanleg, þ.e. rétt skráð, heildstæð og gild.
4) Kröfum um að leynd hvíli yfir efni þeirra.
5) Kröfum sem gerðar eru um staðfestingar vegna innra eftirlits.
6) Mikilvægi rekjanleika, þ.e. þess að hægt sé að staðfesta móttöku og sendingu gagna til þess að koma í veg fyrir að móttakandi haldi því ranglega fram að hann hafi ekki fengið tiltekin gögn eða sendandi að hann hafi sent tiltekin gögn.
7) Mikilvægi þess að vita hver sendandi gagna er og þörfinni fyrir staðfestingu á því að hann sé sá sem hann segist vera en ekki einhver annar.

4.2 Mótun öryggisstefnu

Ríkisaðilar þurfa auk þess að framkvæma áhættumat vegna hugsanlegrar upptöku á rafrænum viðskiptum að móta sér öryggisstefnu vegna þeirra ef ákveðið er að taka þau upp.

Það er hlutverk forstöðumanna stofnana og fyrirtækja ríkisins að móta öryggisstefnu vegna rafrænna viðskipta því það eru þeir sem bera ábyrgð á öryggi upplýsingakerfa stofnana eða fyrirtækja sinna. Öryggisstefnan skal byggð á áhættumati öryggishópsins og á að fella hana á eðlilegan hátt inn í heildaröryggisstefnu vegna upplýsingakerfa viðkomandi.

Mótun öryggisstefnu er lýst í 4. kafla ritsins um rekstraröryggi upplýsingakerfa og vísast þangað varðandi þetta verkefni.

5. Öryggisráðstafanir

Í þessum kafla verður fjallað um þær öryggisráðstafanir sem beita má til þess að mæta þeim áhættuþáttum sem fjallað hefur verið um hér að framn.

Sumum öryggisráðstöfunum er ætlað að mæta fleiri en einum áhættuþætti. Til þess að koma í veg fyrir tvítekningar er fjallað heildstætt um hverja ráðstöfun fyrir sig og þær flokkaðar í þrjá kafla eftir eðli. Er þetta sama fyrirkomulag og í riti stofnunarinnar um rekstraröryggi upplýsingakerfa[12]. Ráðstafanirnar skiptast í eftirfarandi þrjá flokka:

1) Stjórnunar- og skipulagsráðstafanir.
2) Umhverfis- og aðbúnaðarráðstafanir.
3) Tæknilegar ráðstafanir.

Aftast í kaflanum er að finna yfirlit þar sem í fljótu bragði má sjá hvaða ráðstöfunum er hægt að beita vegna hvers áhættuþáttar fyrir sig.

5.1 Val á öryggisráðstöfunum

Þegar áhættumat og öryggisstefna liggur fyrir eru forsendur fyrir því að kanna þær öryggisráðstafanir sem til greina koma til þess að ná fram markmiðum öryggisstefnu viðkomandi stofnunar eða fyrirtækis. Þar sem forstöðumenn sem bera ábyrgð á rekstri ríkisaðila, ber þeim að ákveða til hvaða öryggisráðstafana skuli grípa.

Við val á öryggisráðstöfunum þarf forstöðumaður alltaf að huga að þeim kostnaði sem þær hafa í för með sér og bera

[12] Rekstraröryggi upplýsingakerfa, Ríkisendurskoðun, október 1998.

hann saman við mögulegt tjón sem hlotist getur séu ráðstafanir ekki viðhafðar. Fleira þarf að meta hér en beint fjárhagslegt tjón. Álitshnekkir og missir trausts getur t.d. einnig haft alvarlegar afleiðingar.

Lýsing á þeim öryggisráðstöfunum sem fyrir valinu verða á að vera skrifleg til þess að öllum notendum séu þær ljósar, hægt sé að meta fylgni starfsfólks við þær og virkni þeirra til verndar þeim hagsmunum sem þær eiga að gæta.

Öryggisráðstöfunum í rafrænum viðskiptum er ætlað að:

1) koma í veg fyrir að brotist sé inn í kerfið.
2) koma í veg fyrir breytingar á gögnum.
3) tryggja að sendandi sé sá sem hann segist vera.
4) tryggja að gögn séu send til rétts móttakanda.
5) tryggja að móttekin og send gögn séu skráð.
6) koma í veg fyrir óheimilan lestur gagna.
7) tryggja að aðilar geti ekki ranglega neitað því að hafa sent eða tekið á móti gögnum.
8) tryggja að rétt sé unnið úr mótteknum gögnum í rafræna viðskiptakerfinu.
9) sjá til þess að ljóst sé á hverjum tíma hver ber ábyrgð á gögnum.
10) tryggja að rafræna viðskiptakerfið sé aðgengilegt eftir þörfum.
11) tryggja að skeyti séu hvorki tvítekin né að þau falli niður án þess að það sé skynjað.

Hér á eftir verður ítarlega fjallað um þær sérstöku öryggis- og eftirlitsaðgerðir sem til skoðunar hljóta að koma vegna áhættuþátta sem tengjast rafrænum viðskiptum sérstaklega og fjallað er um í köflum 3.1 - 3.7 hér framar í ritinu. Aðallega eru þessi umfjöllun til viðbótar við þá sem til staðar er í ritinu um rekstraröryggi upplýsingakerfa. Í einhverjum mæli er þó ekki hægt að komast hjá því að fjalla hér um sömu hluti og þar.

5.2 Kröfur til rekstraröryggis

Öryggisráðstafanir sem tryggja eiga rekstraröryggi hins rafræna viðskiptakerfis skipta mjög miklu máli til þess að mæta hættu á truflunum eða stöðvun á rekstri þess. Ráðstafanirnar þurfa því að tryggja áreiðanleika kerfisins í þeim mæli sem ákveðið hefur verið í öryggisstefnu.

Rekstraröryggi kerfis sem notað er í rafrænum viðskiptum byggir á því að kerfið sé bæði aðgengilegt og nothæft til þess að það geti þjónað því viðskiptalega hlutverki sem því er ætlað, þar með að skrá upplýsingar um viðskipti milli aðila eins og lög gera ráð fyrir.

Í riti Ríkisendurskoðunar um rekstraröryggi upplýsingakerfa er að finna ítarlegar lýsingar á almennum öryggisráðstöfunum vegna þeirra. Þær almennu aðgerðir sem hér skipta höfuðmáli tengjast afmörkun netumhverfis, afritatöku, aðgangi að kerfinu og gerð og prófun neyðaráætlunar. Einnig skiptir hér miklu máli tvöföldun vélbúnaðar, veiruvarnir, ýmsar aðgerðir í tengslum við aðgang og aðbúnað í tölvuherbergi o.fl. Stöðugt endurmat þarf og að fara fram á þeim öryggisráðstöfunum sem tryggja eiga rekstraröryggi upplýsingakerfa. Vísað er til áðurnefnds rits varðandi þessar almennu öryggisráðstafanir.

5.3 Stjórnunar- og skipulagsráðstafanir

Undir stjórnunar- og skipulagsráðstafanir falla ýmsar aðgerðir sem segja má að falli beint undir stjórnunarþátt rekstursins. Þessar aðgerðir tengjast rafræna viðskiptakerfinu sjálfu, starfsmönnum viðkomandi og samskiptunum við viðskiptaaðila og eru allar liður í því að tryggja öryggi rafrænu viðskiptanna sem best.

1. Skjölun rafræna viðskiptakerfisins

Kerfi sem notuð eru í rafrænum viðskiptum eru oft flókin og vinna í mörgum þrepum. Til þess að hægt sé m.a. að rekja færslur og átta sig á uppbyggingu þeirra vélrænu eftirlitsþátta sem einkenna slík kerfi ætti það að vera ófrávíkjanleg regla við upptöku rafrænna viðskipta að fyrir liggi ítarleg skrifleg lýsing á rafræna viðskiptakerfinu. Sama regla ætti og að gilda um allar breytingar sem gerðar eru á kerfinu.

2. Verklýsingar, ábyrgð og þjálfun starfsmanna

Einn mikilvægasti þátturinn sem stjórnendur þurfa að sinna við upptöku rafrænna viðskipta er að undirbúa starfsmenn vel undir breytt vinnuumhverfi.

Nauðsynlegt er að byrja á því að útbúa verklýsingar vegna þeirra starfa sem tengjast rafræna viðskiptaferlinu og gera í þeim jafnframt grein fyrir þeirri ábyrgð sem fylgir hverju starfi fyrir sig. Síðan þarf að þjálfa starfsmenn í nýjum vinnubrögðum til þess að tryggt sé að þeir geti af þekkingu og öryggi sinnt þeim verkefnum sem þeim eru falin og jafnframt tekist á við þau vandamál sem upp kunna að koma.

3. Verklagsreglur vegna eftirlits

Við upptöku rafrænna viðskipta þurfa einnig að liggja fyrir skriflegar og ítarlegar verklagsreglur því þar sem verklýsingu vegna tiltekins starfs sleppir taka þær við.

Í verklagsreglum skal m.a. lýsa því í smáatriðum hvernig og hversu oft eigi að fylgjast með tilteknum boðum sem rafræna viðskiptakerfið sendir frá sér og hvernig bregðast eigi við hverjum þeirra til þess að rafrænu viðskiptin gangi eins snurðulaust fyrir sig og kostur er.

Í verklagsreglum á t.d. að koma fram hve oft skuli skoða

dagbækur rafræna viðskiptakerfisins og hvernig eigi að bregðast við tilkynningum frá kerfinu um villur í gögnum, hugbúnaði eða sendingum. Nákvæmar lýsingar skulu t.d. vera í verklagsreglur um leiðréttingu villna í færslum. Segja má að í verklagsreglum skuli koma fram lýsingar á öðrum eftirlitsaðgerðum en þeim sem eru vélvæddar og oft eru þær í raun viðbót þær.

4. Samningar í föstum viðskiptum

Ljóst er að sett lög og reglugerðir munu aldrei taka á öllum vandamálum sem upp geta komið í rafrænum viðskiptum. Aðilar í föstu viðskiptasambandi ættu því undantekningarlaust að draga úr hættu á þrætuefnum sín á milli með því að skipa málum með samningum. Hér er ekki aðeins átt við samninga á milli viðskiptaaðilanna sjálfra heldur og samninga á milli viðskiptaaðila og virðisaukandi netþjónustu ef þriðji aðili sér um samskiptin.

Í rafrænum viðskiptum er innsýn ekki möguleg í kerfi og eftirlitsaðgerðir gagnaðilans. Ef hann er með illa prófuð forrit og eða illa uppbyggt eftirlit bitnar það á þeim gögnum sem hann sendir og gagnaðilinn tekur við. Þar sem skýrar og almennt viðurkenndar reglur um ábyrgð í rafrænum gagnaflutningum eru ekki til geta aðilar haft ólíkar skoðanir á því t.d. hvenær ábyrgð flyst frá sendanda til móttakanda. Margt fleira getur komið til.

Með samningi má skipa því hvernig aðilar ætla að haga samskiptum sínum tæknilega, hvernig bregðast skal við og hver ber ábyrgðina ef eitthvað fer úrskeiðis. Einnig er sjálfsagt að samið sé um hvaða kröfur aðilar gera til öryggismála hvor hjá öðrum og hvernig ganga má úr skugga um að þeim sé mætt, t.d. með úttekt þriðja aðila. Samninga sem þessa ætti að gera með formlegum hætti.

Aðilar viðskiptasambands sem nota virðisaukandi netþjónustu til samskipta sín á milli þurfa því að geta gengið úr skugga um að hægt sé að treysta á að samskiptin séu í lagi. Hér er m.a. átt við það að netþjónustuaðilinn sendi frá sér

þær upplýsingar sem hann hefur tekið á móti með því fyrirkomulagi sem samið hefur verið um, að þær öryggisráðstafanir sem hann gerir séu viðunandi og að hann sé vel búinn undir óhöpp eða hamfarir með vel æfðum og áreiðanlegum neyðaráætlunum sem tryggt geti viðvarandi þjónustu.

Árið 1988 gaf Alþjóða verslunarráðið (ICC - „International Chamber of Commerce“) út svokölluð samræmd tilmæli varðandi samskipti á viðskiptagögnum með fjarskiptum UNCID („Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission“).

Í formála að íslensku þýðingunni að UNCID-tilmælunum segir m.a. að þó svo að þau séu ekki skuldbindandi frekar en aðrir staðlar, reglur eða leiðbeiningar frá Alþjóða verslunarráðinu, geti þau verið grundvöllur að samskiptasamningi svo bindandi sé að lögum.

Ríkisendurskoðun mælir með því að þeir sem ætla að gera sérstaka samninga við viðskiptaaðila sína vegna rafrænna viðskipta, kynni sér UNCID-tilmælin. Þau er að finna á slóð tækninefndar á heimasíðu ICEPRO [13].

5. Siðareglur í Netviðskiptum

Í rafrænum viðskiptum á Netinu eru viðskiptaskilmálar oft ákveðnir einhliða af seljanda og kaupandi verður að ganga að þeim skilyrðislaust ætli hann að eiga viðskipti við viðkomandi. Vegna þessa er afar mikilvægt að seljendur taki upp þær evrópsku siðareglur í Netviðskiptum sem Samtök verslunar og þjónustu hafa kynnt og hvatt til að notaðar verði upp hér á landi en þær er að finna á heimasíðu samtakanna[14].

5.4 Umhverfis- og aðbúnaðarráðstafanir

Sérstaklega þarf að huga að umhverfi og aðbúnaði tölvu-

[13] Sjá: http://www.chamber.is/icepro/t-nefnd1.htm
[14] Sjá: www.svth.is/evropa/eurocode_eng.html

búnaðar m.a. vegna eldvarna og þess að óviðkomandi aðilar geti ekki átt aðgang að þeim stöðum þar sem viðkvæmur tölvubúnaður er staðsettur.

Hér á eftir eru talin upp nokkur dæmi um það sem átt er við með öryggisráðstöfunum vegna umhverfis og aðbúnaðar tölvukerfis.

- Afrit skulu geymd í eldtraustri geymslu innanhúss. Afrit skulu einnig geymd á öruggum stað utan stofnunar eða fyrirtækis.
- Tölvuherbergi skal alltaf vera læst eða á svæði þar sem aðgangur er takmarkaður við tiltekna starfsmenn.
- Tölvubúnaður í tölvuherbergi skal vera á sérstökum rafmagnsöryggjum.
- Hvorki eiga að vera vatnsrör né miðstöðvarofnar í tölvuherbergi.
- Lágmarka ætti umgengni og rykmyndun í tölvuherbergi, liður í því er að þar séu hvorki staðsettir prentarar né pappír geymdur.
- Tölvuherbergi skal ekki notað sem pappírsgeymsla.
- Netþjónar og gáttir skulu tengdar við rafbakhjarl (UPS) til þess að koma í veg fyrir stöðvun af völdum rafmagnstruflana.
- Allar tölvulagnir í stofnuninni/fyrirtækinu skulu vera í lokuðum stokkum.
- Reykskynjari skal vera í tölvuherbergi.
- Til þess að slökkva elda í rafmagnstækjum er nauðsynlegt að hafa Halon-slökkvitæki fyrir utan dyr tölvuherbergis.
- Allur tölvubúnaður skal vera í að a.m.k. 10 cm. hæð frá gólfi til þess að minnka líkur á vatnstjóni.

Til viðbótar þessum almennu atriðum sem gilda um flest tölvukerfi koma nokkur atriði sem eru sérstaklega mikilvæg fyrir kerfi sem notuð eru í rafrænum viðskiptum.

- Sérstaklega þarf að gæta þess að samskiptalínur og innanhússímstöðvar sem þær fara um, séu háðar sömu

öryggiskröfunum og annar tölvubúnaður sem notaður er í rafrænum viðskiptum.

- Vera má að kanna þurfi umhverfis- og aðbúnaðarráðstafanir hjá aðilum sem átt eru rafræn viðskipti við. Til þess að þetta sé mögulegt þarf að vera til staðar samningur sem kveður á um að ákveðnum umhverfis- og aðbúnaðarráðstöfunum sé beitt. Um samninga milli aðila er fjallað í kafla 5.3.4 hér að framan.
- Í beinum rafrænum viðskiptum þarf sérstaklega að huga að aðgangi að þeim herbergjum þar sem sá búnaður er geymdur sem umbreytir SMT-skeytum yfir á og af stöðluðu samskiptaformi yfir á innanhúss-form og öfugt. Allur slíkur búnaður þarf að vera háður sömu eða jafnvel strangari umhverfis- og aðbúnaðarkröfum en annar búnaður sem notaður er í slíkum viðskiptum.

5.5 Tæknilegar ráðstafanir

1. Aðgangstakmarkanir

Í rafrænum viðskiptum er aðgangsheimildum beitt sem innri eftirlitsaðgerð til þess að tryggja verkaskiptingu milli starfsmanna eftir því sem kostur er. Þeir hafa því ólíkar heimildir til aðgangs að einstökum kerfum og aðgerðum innan þeirra og kann aðgangur og notkun hvers starfsmanns á rafrænu viðskiptakerfunum því að vera mismunandi.

Notendur tölvukerfis fá tiltekið auðkenni sem er í raun lykill að þeim kerfum og aðgerðum sem þeir eru taldir þurfa að nota í starfi sínu. Hér skal sérstaklega bent á að í rafrænum viðskiptum koma heimildir til þess að framkvæma tilteknar aðgerðir í stað hefðbundinnar heimildaráritunar í pappírsviðskiptum. Það mál er því leyst með því að gefa aðeins þeim sem geta samþykkt færslu heimild til þess að skrá hana.

Auðkennum má skipta í þrjá flokka sem tryggja misvel sönnun þess að notandi sé sá sem auðkennið ber með sér.

1. Hvað veit notandinn?

Þessi tegund aðgangstakmarkana byggir á vitneskju notenda og er algengasta aðferðin í notkun sérstakra leyniorða. Leyniorð tryggir í raun ekki að notandi sé eigandi lykilorðsins þar sem hann getur auðveldlega hagað sér þannig að auðvelt sé fyrir aðra að komast að því eða jafnvel sagt öðrum frá leyniorði sínu. Dæmi um það síðarnefnda er þegar yfirmaður segir ritara sínum leyniorð sitt til þess að ritarinn geti notað þær aðgangsheimildir sem yfirmaðurinn einn á að hafa.

2. Hvað hefur notandinn?

Þessi tegund aðgangstakmarkana byggir á því að aðgangur er veittur handhafa tiltekins hlutar, t.d. greiðslukorts. Til þess að auka aðgangsöryggi er ofangreindum tveimur tegundum aðferða oft beitt saman, meðal annars þegar tekið er út úr hraðbanka. Þá þarf viðkomandi bæði að hafa kortið og þekkja PIN-númer þess. Þessi tegund aðgangstakmarkana tryggir ekki að sá sem notar kortið sé eigandi þess.

3. Hver er notandinn?

Þessi tegund aðgangstakmarkana er sú sem öruggust er talin af þeim þremur sem hér er fjallað um. Í tölvukerfum er hægt að útfæra þessa aðferð með ýmsum hætti svo sem fingrafaralesara, raddgreiningu, lithimnulesara o.fl. Slíkum aðgangstakmörkunum hefur lítt verið beitt hingað til en breyting er nú að verða á þessu, aðallega vegna mikillar þróunar á fingrafaralesurum.

2. Vélrænt innra eftirlit

Í þessum kafla um vélrænt innra eftirlit er umfjöllun aðallega beint að beinum rafrænum viðskiptum. Mörg þeirra atriða sem um er fjallað geta þó einnig átt við um óbein rafræn viðskipti.

1. Prófun viðskiptakerfa

Þegar um er að ræða bein rafræn viðskipti samanstanda innri eftirlitsaðgerðir að stærstum hluta af vélrænum eftirlitsþáttum. Til þess að tryggja að þeir virki rétt þarf að prófa þá rækilega áður en nýtt kerfi eða ný útgáfa kerfis eru tekin í notkun. Mikilvægt er að við prófunina sé beitt almennt viðurkenndum reglum því prófun sem þessi er flókin m.a. vegna þess að mörg þrep eru í vinnsluferlinu og innsýn skortir í kerfi gagnaðilans. Afleiðingin er sú að erfitt getur verið að greina og staðsetja villur. Mikið öryggi felst í því fyrir aðila í föstu rafrænu viðskiptasambandi að beita sömu reglum við prófun kerfa sinna.

2. Samfelld röð skeyta tryggð

Mikilvægt er að tryggja að engin skeyti misfarist og það uppgötvist ef skeyti hefur verið sent oftar en einu sinni. Þess vegna eiga innri eftirlitsaðgerðir að tryggja að skeyti séu send og móttekin í réttri röð.

3. Úrvinnsla skeyta og afstemmingar í ferlinu innanhúss

Mikilvægt er að skeyti séu send og unnið sé úr mótteknum skeytum á réttum tíma. Ef það er ekki gert safnast skeyti upp í biðskrám. Vélrænar eftirlitsaðgerðir þurfa því að fylgjast með þeim og gera viðvart hafi gögn verið þar óeðlilega lengi.

Í beinum rafrænum viðskiptum á sér oftast stað vélræn úrvinnsla á skeyti eftir að tekið er á móti því en áður en það er skráð í viðskiptakerfi móttakanda. Vinnsla þessi felst m.a. í því að skeytið er þýtt af t.d. UN/EDIFACT-sniði yfir á snið viðskiptakerfisins og bókunarlyklum bætt við það. Að auki er hugsanlegt að skeytið hafi um tíma verið geymt í biðskrá. Útfærsla þessara atriða er mismunandi eftir kerfum.

Mikilvægt er að til staðar séu virkar vélrænar eftirlitsað-

gerðir sem gera afstemmingar mögulegar í ferlinu frá móttöku skeytis til endanlegrar skráningar þess í viðskiptakerfi móttakanda og gera jafnframt viðvart ef afstemmingar eru ekki í lagi.

4. Rekjanleiki færslna

Í venjulegu viðskiptakerfi er m.a. hægt að þekkja skjal á fylgiskjalsnúmerinu sem það fær við skráningu þar. Númerið gerir kleift að rekja feril færslunnar frá upphafi til enda. Endurskoðunarslóð er því mjög auðrakin.

Í hefðbundnu SMT-kerfi hefur skjal farið í gegnum ýmsar vinnslur áður en það er skráð í viðskiptakerfið sjálft þar sem það fær fylgiskjalsnúmer. Undanfarandi vinnslur eru m.a. til að rjúfa rafrænt innsigli skjals og þýða það yfir á innanhússform. Innbyggðar vélrænar eftirlitsaðferðir eiga að tryggja að SMT-færsla fari í gegnum allt vinnsluferlið villulaust. Ekki skal treysta því að svo sé. Mögulegt þarf að vera að bera kennsl á færslu hvar sem er í vinnsluferli hennar bæði til þess að ganga úr skugga um að ferlið sé eðlilegt og eins til þess að finna villur eða skjöl sem hafa horfið. Það vinnsluferli sem oftast er notað býður ekki upp á auðvelda leið í þessu efni því upplýsingar um endurskoðunarslóð færslu er oft að finna í ólíkum dagbókum og auðkenni hennar mismunandi eftir því hvar hún er stödd í ferlinu.

Mikilvægt er að rekjanleiki rafrænna færslna sé tryggður með eins einfaldri og virkri aðferð og nokkur kostur er.

5. Afneitun ómöguleg

Tryggt verður að vera að hvorki sendandi né móttakandi geti ranglega neitað því að hafa sent eða tekið á móti skeyti („non repudiation“).

Þær aðferðir sem nota má til þess að koma í veg fyrir ranga neitun um sendingu eða móttöku eru m.a. sending kvittunar, notkun rafrænnar undirskriftar eða vottun hlutlauss þriðja aðila.

6. Villur og leiðréttingar

Þegar sent hefur verið skeyti í beinum rafrænum viðskiptum og mótttakandi hefur tekið á móti því og sent kvittunar-skeyti því til staðfestingar eru aðilar skuldbundnir. Eftir það er ekki heimilt að hafna vinnslu skeytisins jafnvel þó að vélræn eftirlitsaðgerð telji efni skeytisins augljóslega rangt. Leiðréttingu á slíku efnislega röngu skeyti verður sendandi að gera með öðru skeyti. Hér gildir því sama regla og um skjalfestan reikning, rangan reikning skal leiðrétta með útgáfu leiðréttingarreiknings.

Fyrir getur komið vegna galla í hugbúnaði, t.d. villu í skilgreiningu í þýðingarhugbúnaði sem umbreytir sniði skeyta, vegna skemmda á biðskrá o.fl., að kerfisstjóri þurfi að gera leiðréttingar á rafrænum viðskiptagögnum. Heimild viðkomandi yfirmanns ætti að þurfa til þess að gera slíkar leiðréttingar auk þess sem skrá þarf sérstaka athugasemd um þessi tilvik.

3. Staðfestingar á áreiðanleika og uppruna gagna

Í rafrænum viðskiptakerfum getur verið tiltölulega auðvelt að breyta færslum.

Vélrænar innri eftirlitsþættir verða að tryggja að efni skeytis hafi ekki verið breytt á leiðinni frá sendanda til móttakanda án þess að vélrænt sé vakin athygli á því með afgerandi hætti.

Það á að vera hægt að sannreyna uppruna rafrænna skjala eins og pappírsskjala en slíkt getur verið erfitt sérstaklega ef viðskipti fara yfir Netið því þá er oft ekki yfirsýn yfir allar þær breytingar á sniði skeytis sem verða á leið þess frá sendanda til móttakanda.

Vélrænar innri eftirlitsaðgerðir verða því að vera til staðar sem geta sannað að skeyti komi frá þeim sem sagður er sendandi þess. Tæknin býður upp á nokkrar lausnir til þess að ná þessu marki og er rafræn undirskrift á meðal þeirra.

4. Dulkóðun

Hefðbundinn tilgangur með dulkóðun hefur jafnan verið sá að tryggja leynd. Á síðari árum hefur notkun dulkóðunar vaxið jafnt og þétt og nú er svo komið að hún er að verða ein mikilvægasta aðferðin til þess að tryggja öryggi og áreiðanleika í rafrænum viðskiptum.

1. Hlutverk dulkóðunar

Hlutverk dulkóðunar getur verið margþætt í rafrænum viðskiptum því með henni er hægt að:

1) **Tryggja gæði gagna**

   Ef skeyti er dulkóðað með öruggum hætti getur móttakandi þess gengið úr skugga um að það hafi skilað sér í heild sinni og að efni þess hafi ekki verið breytt á leiðinni til hans.

2) **Staðfesta uppruna**

Ef skeyti er dulkóðað með öruggum hætti getur móttakandi þess fengið staðfestingu á uppruna þess því slík dulkóðun á að tryggja að óviðkomandi aðili geti ekki sent skeyti í annars nafni.

3) Staðfesta móttöku/sendingu skeytis

Ef skeyti er dulkóðað með öruggum hætti er tryggt að sendandi geti ekki ranglega neitað því að hafa sent skeyti eða móttakandi neitað að hafa tekið við því vegna þess að opinberi lykillinn sem nánar er fjallað um hér á eftir, sendir kvittun.

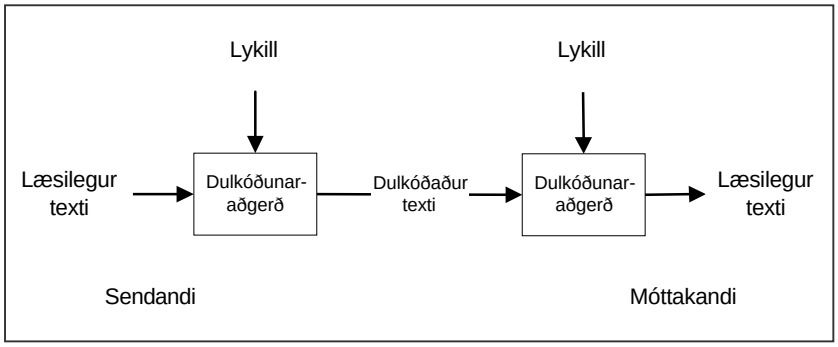
4) Tryggja leynd

Ef skeyti er dulkóðað með öruggum hætti er tryggt að óviðkomandi aðilar geta ekki komist að efni þess.

2. Ferli dulkóðunar

Dulkóðun fer fram með þeim hætti að sendandi dulkóðar skeyti með sérstökum dulkóðunarlykli sem er hluti af dulkóðunarbúnaði hans. Þegar móttakandi hefur fengið skeytið í hendur verður hann að senda það í gegnum dulkóðunarbúnað sinn til þess að koma því yfir á læsilegt form. Til þess er notaður lykill til þess að afkóða skeytið.

Ef sami lykill er notaður bæði við dulkóðun og afkóðun er dulkóðunin samhverf. Ef sinn hvor lykillinn er notaður telst dulkóðunin ósamhverf.



Mynd 4. Ferli dulkóðunar

3. Tegundir dulkóðunar

Í rafrænum viðskiptum er m.a. hægt að beita bæði samhverfri og ósamhverfri dulkóðun.

1) Samhverf dulkóðun

Þegar dulkóðun er samhverf er hún eins hjá báðum viðskiptaðilum því sami dulmálslykill er notaður bæði til þess að dulkóða skeyti og til þess að koma skeyti aftur yfir á læsilegt form með með afkóðun. Sú aðferð við dulkóðun sem menn notuðu fyrr á tímum er þessarar tegundar.

2) Ósamhverf dulkóðun

Þegar dulkóðun er ósamhverf er hún mismunandi hjá hvorum viðskiptaaðila fyrir sig því notaður er sinnhvor lykillinn við dulkóðun og afkóðun. Talað er um lyklana tvo sem par.

Í ósamhverfri dulkóðun er öðrum lyklinum alltaf haldið leyndum og nefnist hann einkalykill. Ef eigandi hans vill opna fyrir samskipti við marga aðila sem vilja senda honum skeyti á dulkóðuðu formi, gerir hann annan lykil sinn að opinberum lykli. Þeir sem þurfa að senda honum skeyti nota þá opinbera lykil móttakandans til þess að dulkóða skeytið en móttakandinn notar einkalykil sinn til þess að afkóða þau.

Opinber lykill

Opinberir lyklar eru oft geymdir í gagnasöfnum og eru þar aðgengilegir öllum þeim sem vilja senda dulkóðaðar upplýsingar til eiganda lykilsins.

Einkalykill

Einkalykill er varðveittur sem einkamál hjá þeim aðila sem móttekur dulkóðað skeyti og notar hann einkalykilinn til þess að afkóða skeytið.

4. Styrkleiki dulkóðunar

Styrkleiki dulkóðunar er yfirleitt metin út frá eftirfarandi þremur þáttum:

1) Dulkóðunaraðferðinni.
2) Lengd dulkóðunarlykilsins.
3) Útfærslu dulkóðunarinnar í hug- eða vélbúnaði.

Engin dulkóðunaraðferð er alveg örugg, aðferðirnar eru aðeins misöruggar.

Sú aðferð sem algengast er að beitt sé í almennum hugbúnaði nefnist DES („Data Encryption Standard“) en hún byggir á 56 stafa löngum dulkóðunarlykli. Útfærslu þessarar aðferðar er oft verulega áfátt, t.d. ef sami bókstafurinn er endurtekinn aftur og aftur í lyklinum. Þó að DES-dulkóðunaraðferðin sé vel útfærð er hægt að ráða dulmálið ef vilji og fjármagn er fyrir hendi[15].

Önnur algeng dulkóðunaraðferð er IDEA („International Data Encryption Algorithm“) og byggir hún á 128 bita löngum dulkóðunarlykli. Þessi aðferð er því mun öflugri en DES.

[15] Sjá: Cracking DES, Electronic Frontier Foundation 1998

5. Útgefendur dulkóðunarlykla og þátttaka í dulkóðuðum samskiptum

Útgefendur dulkóðunarlykla geta verið viðskiptaaðilar sjálfir, lyklamiðstöðvar eða sérstakir milliliðir í viðskiptum. Mismunandi er í hve ríkum mæli þeir koma að dulkóðuðum rafrænum samskiptum viðskiptaaðila.

1) Viðskiptaaðili útbýr lykla

Einfaldasta fyrirkomulag á útgáfu dulkóðunarlykla er að viðskiptaaðili gefi sjálfur út lykla sína. Þetta er algengt þegar aðilar sem þekkjast eiga í milliliðalausum samskiptum. Nauðsynlegt er í tilvikum sem þessum að viðskiptaaðilarnir hittist vegna afhendingar lykils eða lykla. Nánar er fjallað um eigin útgáfu lykla í kafla 5.5.5 um rafræna undirskrift hér á eftir.

2) Lyklamiðstöð útbýr lykla

Ef ekki er raunhæft að viðskiptaaðili hitti þá sem hann vill eiga dulkóðuð rafræn viðskipti við til þess að afhenda þeim dulkóðunarlykla þarf hann að fá sérstakan aðila til þess að sjá um útgáfu þeirra, t.d. miðstöð sem sérhæft hefur sig í slíku. Færslur sem dulkóðaðar eru með lyklum lyklamiðstöðvar fara ekki í gegnum hana og kemur hún því ekki að dulkóðuðum samskiptum aðilanna. Nánar er fjallað um lyklamiðstöðvar í kafla 5.5.5 um rafræna undirskrift hér á eftir.

3) Milliliður útbýr lykla

Í ýmsum tilvikum fara öll dulkóðuð samskipti um sérstakan millilið sem einnig sér um útgáfu dulkóðunarlykla. Hann ber jafnframt ábyrgð á öllum dulkóðuðum samskiptum milli aðila. Dulkóðunaraðferðirnar eða lyklarnir sem notaðar eru þegar svona háttar til þurfa ekki að vera þeir sömu vegna sendinga frá sendanda til milliliðs og vegna sendinga frá millilið til móttakanda.

5. Rafrænar undirskriftir

1. Hlutverk rafrænna undirskrifta

Ef kafli 5.5.4.1 um hlutverk dulkóðunar er borinn saman við efni þessa kafla kemur í ljós að rafræn undirskrift getur gegnt þremur hlutverkum af fjórum hlutverkum dulkóðunar. Ástæðan er sú að dulkóðun gegnir lykilhlutverki við gerð rafrænnar undirskriftar.

Hlutverk rafrænnar undirskriftar er að:

1) **Tryggja gæði gagna**

   Ef skeyti er rafrænt undirritað getur móttakandi þess gengið úr skugga um að það hafi skilað sér í heild sinni og að innihaldi þess hafi ekki verið breytt á leiðinni til hans.

2) **Staðfesta uppruna**

   Ef skeyti er rafrænt undirritað getur móttakandi þess fengið staðfestingu á uppruna þess því undirritunin tryggir að óviðkomandi aðili geti ekki sent skeyti í annars nafni án heimildar.

3) **Staðfesta sendingu skeytis**

   Ef skeyti er rafrænt undirritað er tryggt að sendandi þess getur ekki ranglega neitað því við móttakandann að hafa sent það.

Rafræn undirskrift tryggir ekki leynd þess skeytis sem hún tengist. Dulkóða þarf efni skeytis sérstaklega ef leynd á að hvíla yfir því.

2. Tegundir dulkóðunarlykla

Rafrænar undirskriftir eru byggðar á notkun einkalykils og opinbers lykils. Saman mynda einkalykill og opinber lykill tiltekins eiganda par sem verður að nota saman.

Einkalykill

Einkalyklar eru varðveittir sem einkamál hjá þeim sem ætlar að undirrita skeyti og eru notaðir til þess að útbúa rafræna undirskrift.

Ef einkalykill er búinn til hjá þeim sem ætlar að skrifa undir notar hann venjulega til þess hugbúnað á einkatölvu sinni og þar geymir hann einnig oftast lykilinn.

Ýmsir þjónustuaðilar, t.d. bankar, bjóða viðskiptavinum sínum upp á rafræn samskipti sem krefjast þess að þeir síðarnefndu hafi einkalykil. Þjónustuaðilarnir útbúa þá slíkan lykil og afhenda hann á disklingi eða öðrum handhægum geymslumiðli.

Þörf er á sérstöku lykilorði með einkalykli því þeir eru yfirleitt of langir til þess að leggja á minnið. Það verður eigandi lykilsins að skrá áður en hann getur notað lykilinn og er þannig komið í veg fyrir að óviðkomandi geti notað lykilinn nema hann hafi með einhverjum hætti komist að lykilorði eigandans. Meðferð þess skiptir því höfuðmáli varðandi öryggi lykilsins.

Opinber lykill

Opinberir lyklar eru oft geymdir í gagnasöfnum og eru þar aðgengilegir öllum þeim sem þurfa að nota þá til þess að sannreyna að rafræn undirskrift skeytis sem þeir hafa tekið á móti sé frá réttum aðila og að gögnin í skeytinu séu óbreytt frá því að þau voru send til hans.

3. Lyklamiðstöðvar eða eigin útgáfa

Lyklamiðstöðvar gefa út skrár á rafrænu formi sem nefndar eru lyklaskírteini. Í slíkum skrám er alltaf að finna annars vegar nafn/heiti lykileiganda eða annað sem auðkennir hann og hins vegar opinberan lykil viðkomandi aðila. Auk þessara tveggja atriða er þar stundum að finna upplýsingar um gildistíma skírteinisins og takmarkanir sem gilda um notkun þess. Til einföldunar og samræmis við aðra umfjöllun í riti þessu verður hér á eftir talað um lyklaskírteinið í heild sinni sem opinberan lykil þó að það sé ekki að öllu leyti nákvæmt.

Lyklamiðstöð getur lokað tilteknum opinberum lykli vegna þess að eigandinn hefur týnt honum eða hann hefur verið misnotaður. Ef lykillinn er lokaður er ekki hægt að byggja rétt á rafrænu undirskriftinni nema hún hafi verið gerð áður en lyklamiðstöðin tilkynnir um lokunina. Upplýsingar um lokaða lykla þurfa að vera aðgengilegar almenningi hjá lyklamiðstöðvum.

Útgáfa dulkóðunarlykla er ekki bundin við lyklamiðstöðvar því hver sem til þess hefur hugbúnað getur gefið út sinn opinbera lykil. Notkun þeirra er þó yfirleitt takmörkuð við notkun innan stofnunar eða og fyrirtækis.

4. Undirskrift útbúin

Sendandi útbýr rafræna undirskrift skeytis með því að reikna út frá efni skeytisins sérstaka afstemmingartölu sem nefnd er tætigildi („hash value“). Þetta er gert annað hvort með sérstakri aðgerð í póstkerfi eða í öðrum hugbúnaði. Síðan er tætigildið dulkóðað með einkalykli þess sem skrifar undir skeyti, þ.e. sendanda. Þá er orðin til rafræn undirskrift sem gengt getur mikilvægu öryggishlutverki í rafrænum viðskiptum. Rafræna undirskriftin er síðan send með skeytinu.

5. Sannreynd efnis og uppruna og könnun heimildar

Til þess að sannreyna óbreytt efni og uppruna skeytis byrjar móttakandi þess á því að afkóða rafrænu undirskriftina með opinberum lykli sendandans og fær þá út tætigildi (afstemmingartölu) á efni skeytisins. Síðan reiknar móttakandinn sjálfur út tætigildi efnis skeytisins með sérstakri aðgerð í póstkerfi eða í öðrum hugbúnaði og ber það saman við tætigildið sem hann var áður búinn að afkóða. Ef tætigildin eru þau sömu er það sönnun þess að efni skeytis sé óbreytt og sendandi sá sem skeyti ber með sér. Móttakandi verður auk þessara aðgerða einnig að fá staðfest hvort sendandi hafði heimild til rafrænu undirskriftarinnar vilji hann tryggja rétt sinn samkvæmt skeytinu.

Til þess að kanna heimild sendanda til rafrænnar undirskriftar þarf móttakandi hennar að kanna:

1) **Hvort opinbera lyklinu hefur verið lokað?**

   Ef opinbera lyklinum hefur verið lokað fær móttakandinn vitneskju um það í gegnum tölvubúnað sinn sem sækir vélrænt upplýsingar um í gagnagrunn viðkomandi lyklamiðstöðvar.

2) **Hvort opinberi lykillinn er útrunninn?**

   Ef undirskrift hefur takmarkaðan gildistíma fær móttakandi hennar vélrænt vitneskju um það í gegnum tölvubúnað sinn.

3) **Hvort takmarkanir eru á notkun rafrænu undirskriftarinnar og ef svo er, hvort skrifað hefur verið undir annað en heimild var til?**

   Ef takmarkanir eru á notkun lykils, t.d. þannig að aðeins má nota hann til þess að versla við tiltekna aðila, kemur slíkt í ljós ef móttakandi kannar heimildir í gegnum tölvubúnað sinn, annars ekki.

Það er á ábyrgð móttakanda að treysta rafrænni undirskrift án þess að kanna þau atriði sem nefnd eru hér að framan. Hafi hann sleppt því og það kemur í ljós að lykill var lokaður, runninn út eða undirskrift var notuð í tilvikum þar

sem hún er ekki heimil verður móttakandi að bera hugsanlegt tjón vegna þessa.

6. Dagbækur

Dagbækur gegna lykilhlutverki í rafrænum viðskiptum því þær eiga að geyma allar nauðsynlegar upplýsingar um hið rafræna viðskiptaferli. Dagbók sinnir í raun tvíþættu hlutverki, annars vegar þarf hún að geta verið sönnunargagn sem sýnir feril færslu frá upphafi til enda og hins vegar er hún nauðsynleg til þess að uppfylla ýmsar kröfur laga um bókhald nr. 145/1994 og reglugerðar nr. 598/1999 um rafrænt bókhald o.fl.

Í tölvukerfum geta verið haldnar nokkrar mismunandi tegundir dagbóka. Þær algengustu eru:

- Sérhæfðar dagbækur vegna tiltekinna upplýsingakerfa, t.d. kerfa sem notuð eru í rafrænum viðskiptum. Þar er mikilvægasta dagbókin svonefnd gagnadagbók. Lýsing á gagnadagbókum eru í áðurnefndri reglugerð um rafrænt bókhald en tilvist þeirra er meðal skilyrðanna fyrir því að ekki þurfi að gefa reikning út á pappír í rafrænum viðskiptum.

- Dagbækur sem skrá kerfisatburði á innra neti.

- Samskiptadagbækur sem skrá kerfisviðburði á ytra neti, þ.e. samskipti við önnur net.

Allar þessar dagbækur geta skipt máli þar sem sami atburður, t.d. innbrot í tölvukerfi, kann að vera skráður í þær hverja og eina út frá mismunandi sjónarhorni. Tryggt þarf að vera að færslum í dagbókum sé ekki breytt því annars er sönnunargildi þeirra lítið sem ekkert. Minnt skal og á nauðsyn þess að reglulega sé fylgst með dagbókum tölvukerfis og í verklagsreglum fjallað um þau mál.

7. Afmörkun netumhverfis

Í rafrænum viðskiptum er aðallega um þrjá kosti að ræða þegar kemur að vali á netumhverfi fyrir þau, leigulínu milli tveggja staða, virðisaukandi netþjónustu þriðja aðila (VAN) eða að nota Netið annað hvort beint eða á lokuðum rásum sem þá eru nefndar sýndareinkanet (VPN „Virtual Private Network“).

Leigulínur

Oft eru sérstakar símalínur leigðar af símafyrirtækjum beinlínis til rafrænna viðskipta milli aðila og er þá talað um viðskipti á lokuðu neti.

Leigusali línu ábyrgist yfirleitt aðeins að hún sé nothæf til gagnaflutnings. Auðvelt er að tryggja öryggi í lokuðum netum þar sem engir utanaðkomandi eiga aðgang að þeim.

Virðisaukandi netþjónusta

Virðisaukandi netþjónusta (VAN) fer venjulega fram í lokuðu netkerfi sem notað er til þess að flytja rafræn viðskiptagögn milli ýmissa aðila.

Eigandi virðisaukandi netþjónustu er undir eðlilegum kringumstæðum ábyrgur fyrir því að flutningur viðskiptagagna um net hans gangi áfallalaust.

Í innkaupahandbók RUT-nefndarinnar um upplýsingatækni, 1998[16] kemur eftirfarandi fram í kafla 12.9.3 Skjalasendingar milli tölva:

„Það er augljós kostur ef allir nota sömu staðla við SMT-samskipti. Þær samskiptaaðferðir sem tryggja viðunandi öryggi í samskiptum (sjá kafla 10.5.5.2. mgr.) byggjast á X.400 stöðlum alþjóðafjarskiptasambandsins og Evrópuforstöðlum um skráaflutning. ..... Mælt er með því að við

[16] Innkaupahandbókina er að finna á heimasíðu RUT-nefndarinnar: http://brunnur.stjr.is/interpro/fjr/fjr.nsf/pages/ih99index.html

sendingu SMT-skjala séu notaðir staðlarnir X.435 og FS ENV 41204 og 41206.“

Virðisaukandi netþjónusta er oft byggð á notkun áðurnefndra X.400-staðla og við flutning á SMT-skeytum við X.435-staðalinn. Í báðum þessum stöðlum eru skilgreindir ýmsir þættir sem tryggja eiga öryggi í gagnaflutningum og í þeim síðarnefnda fjölmargir sem eingöngu eiga við í hefðbundinum SMT-viðskiptum. Öryggi gagnaflutninga í virðisaukandi netþjónustu er mikið.

Netið

Netið er eins og kunnugt er það sem kallað er opið net þar sem hver sem er með tiltekinn vélbúnað og hugbúnað getur m.a. keypt vöru eða þjónustu í rafrænum viðskiptum af þeim sem eru með sölusetur á Netinu.

Þegar Netið er notað beint við rafræn viðskipti er enginn sérstakur aðili ábyrgur fyrir því sem aflaga fer í flutningi viðskiptagagna um það, t.d. því að skeyti komist óbrenglað eða alls ekki til rétts aðila.

Öryggi á Netinu er enn sem komið er lítið því það sem sent er um það án dulkóðunar er hægt að hlera og ekki er hægt að segja fyrir um hvort eða hvenær skeyti berst. Netið er hins vegar í mjög örri þróun þannig að vera má að lausnir sem tryggja betur öryggi gagnaflutninga á því komi fram innan tíðar. Liður í þessu er t.d. þróun staðla fyrir uppsetningu lokaðra rása á Netinu (VPN), sem nefndar voru í inngangi kaflans.

5.6 Ráðstafanir vegna einstakra áhættuþátta

Í 3. kafla rits þessa er fjallað um þá áhættuþætti sem einkenna rafræn viðskipti sérstaklega en varðandi almenna áhættuþætti í rekstri upplýsingakerfa er vísað í rit Ríkisendurskoðunar um það efni. Hér á eftir má sjá yfirlit úr efni kafla 5.1 - 5.5 sem sýnir hvaða öryggisráðstöfunum þarf að beita til þess að mæta einstökum áhættuþáttum í köflum 3.1 - 3. 7. Þar sem sumar ráðstafanir mæta fleiri en einum áhættuþætti eru tvítekningar í yfirlitinu.

Áhættuþættir:	**Öryggisráðstafanir:**
1. Kerfi ekki aðgengilegt:	5.2 Rekstraröryggi
	5.4 Umhv.- og aðbún.ráðst.
2. Kerfi ekki nothæft:	5.2 Rekstraröryggi
	5.4 Umhv.- og aðbún.ráðst.
3. Áreiðanleiki gagna:	5.5.3 Staðfesting áreiðanleika
	5.5.4 Dulkóðun
	5.5.5 Rafræn undirskrift
4. Uppruni gagna:	5.5.3 Staðfesting á uppruna
	5.5.4 Dulkóðun
	5.5.5 Rafræn undirskrift
5. Villur í gagnavinnslu:	5.5.2 Vélrænt innra eftirlit
	5.3.3 Verklagsreglur
6. Villur í hugbúnaði:	5.3.3 Fylgst með dagbókum
	5.3.1 Góð skjölun kerfis
	5.3.3 Verklagsreglur

Áhættuþættir:	**Öryggisráðstafanir:**
7. Villur í skeytasend.:	5.5.2 Vélrænt innra eftirlit 5.5.4 Dulkóðun 5.5.5 Rafræn undirskrift
8. Leynd gagna:	5.5.4 Dulkóðun
9. Vélrænt eftirlit:	5.3.3 Fylgst með dagbókum 5.3.3 Góð skjölun kerfis 5.5.2 Verklagsreglur
10. Óhefðbundin endurskoðunarslóð:	5.5.2 Rekjanleiki 5.5.6 Dagbækur 5.3.1 Góð skjölun kerfis
11. Treysta þarf á gagnaaðila:	5.5.7 Afmörkun netumhverfis 5.3.4 Öflun vitneskju um öryggismál gagnaðila 5.3.4 Gerð samskiptasamn. 5.3.5 Siðareglur virtar
12. Treysta þarf á þriðja aðila:	5.5.7 Afmörkun netumhverfis 5.3.4 Öflun vitneskju um öryggismál þriðja aðila

6. Endurskoðun

Helstu vandamálin við endurskoðun í rafrænu viðskiptaumhverfi eru að hún fer fram í umhverfi þar sem eiginleg skjöl er ekki að finna og að jafnaði er skortur á vitneskju um öryggi hjá gagnaðila viðskiptanna eða virðisaukandi netþjónustuaðila. Vegna þessa m.a. krefst endurskoðun rafrænna viðskipta nýrra vinnubragða sem að hluta til eru gjörólík þeim sem notuð eru í hefðbundnu viðskiptaumhverfi. Endurskoðun á rafrænum viðskiptum lýtur hins vegar hefðbundnum lögmálum varðandi áherslur og umfang.

6.1 Hlutverk endurskoðenda

Hefðbundið hlutverk endurskoðenda er að sannreyna þær upplýsingar sem settar eru fram í reikningsskilum og votta að þau gefi glögga mynd af viðkomandi rekstri og efnahag. Þær spurningar sem vakna við endurskoðun í rafrænu viðskiptaumhverfi lúta að því hvernig eigi að sannreyna upplýsingar eða með öðrum orðum á hverju á að byggja vottunina í slíku umhverfi.

Áhrifin sem rafræn viðskipti hafa á endurskoðunina fara eftir umfangi og fyrirkomulagi þeirra. Ef um er að ræða meiri háttar endurskipulagningu viðskiptaferla eru áhrifin mikil.

Við upptöku rafrænna viðskipta og einkum þegar þau verða fyrirferðarmikil í rekstrinum, dregur úr mikilvægi tiltekinna þátta í efnahagsreikningnum. Hin hefðbundna endurskoðun á útistandandi viðskiptakröfum og gjaldföllnum skuldum með ytri afstemmingum skiptir þá minna máli en áður þar sem umfang þessara þátta er ekki jafn mikið og ella væri.

Æskilegast er að þeir sem endurskoða fylgist með áætlunum um upptöku rafrænna viðskipta og fái tækifæri til þess á hönnunarstigi að gera kröfur um gott innra eftirlit og rekjanleika.

6.2 Krafa um þekkingu á upplýsingatækni

Ekki er hægt að endurskoða rafræn viðskipti án þess að kynna sér hönnun og vinnsluaðferðir viðkomandi upplýsingakerfis vegna þess að í því hefur pappírsgögnum að mestu verið skipt út fyrir rafrænar færslur.

Þeir sem endurskoða þurfa bæði að þekkja vel til áhættuþátta í rekstri upplýsingakerfa, einnig þeirra sem sérstaklega tengjast rafrænum viðskiptum, og átta sig á meginþáttum rafrænna viðskipta. Þar sem verið er að vinna með gögn sem koma frá öðrum er mikilvægt að þau séu örugg og að öll þau gögn sem von var á skili sér og aðeins einu sinni.

6.3 Endurskoðunarslóð pappírslaus

Krafa um að til staðar sé endurskoðunarslóð til sönnunar og rekjanleika er fyrir hendi hvort sem viðskipti eru hefðbundin eða rafræn.

Hefðbundin endurskoðunarslóð er sjaldnast til staðar í rafrænum viðskiptum. Séu þau í sinni hreinustu mynd er fræðilegur möguleiki á því að eina skjalið á pappír sem tengist þeim sé samskiptasamningur viðskiptaaðila. Slíkur samningur myndi þó eingöngu vera til ef aðilar í föstum viðskiptum hefðu ákveðið að skjalfesta leikreglur er gilda um samskipti þeirra.

Í raun er sjaldnast gengið svo langt að pappírsleysi sé algjört. Alltaf á samkvæmt núgildandi reglum hér á landi að vera mögulegt að prenta út ýmis gögn sem viðskiptunum tengjast, þ.á.m. reikninga, ef þörf krefur.

6.4 Innra eftirlit vélvætt

Eftirlitsþættir við hefðbundna endurskoðun tengjast oftar en ekki pappírsgögnum, sbr. könnun á því að frumrit reiknings sé til staðar, færsla samþykkt af réttum aðila o.s.frv. Meginreglan í rafrænum viðskiptum er hins vegar sú að innra eftirlit er vélvætt og hefðbundnum eftirlitsaðferðum að jafnaði lítið beitt. Hér er því yfirleitt ekki til staðar sú tegund eftirlits sem felst í eftirtekt og beitingu dómgreindar. Endurskoðun krefst af þessum sökum alveg nýrrar nálgunar og vinnubragða.

Hafa verður í huga að innri eftirlitsaðgerðir sem taldar eru góðar og gildar í verkferli sem byggir á pappírsskjölum, geta verið til mikillar óþurftar í rafrænu verkferli og komið í veg fyrir ávinning sem að var stefnt með upptöku þess.

6.5 Krafa um nýja nálgun og vinnubrögð

Svör við eftirfarandi spurningum skipta höfuðmáli við endurskoðun á rafrænu viðskiptaumhverfi:

a) Hvert er mikilvægi kerfisins í rekstrinum?
b) Hverjir eru áhættuþættirnir?
c) Er skjölun kerfisins í lagi?
d) Tryggja eftirlits- og staðfestingaraðgerðir öryggi og áreiðanleika gagna?
e) Er umsjón með rekstri kerfisins í lagi?
f) Er gerður samningur við aðila í föstu viðskiptasambandi?
g) Eru öryggismál viðkomandi almennt í lagi?

Þar sem rafrænar viðskiptafærslur eru eingöngu geymdar á gagnamiðlum þarf sá sem endurskoðar að geta valið þær og greint með aðferðum tölvutækninnar. Mikilvægt atriði þessu tengt er að mikla áherslu þarf að leggja á þjálfun í aðferðum tölfræðinnar við val á úrtökum til endurskoðunar.

Í stað verkaskiptingar verður sá sem endurskoðar að horfa til annarra innri eftirlitsþátta sem koma verða í staðinn fyrir þennan þátt. Hann þarf því að geta prófað og sannreynt að staðfestingarferlar og forritaðar eftirlitsaðgerðir virki eins og til er ætlast. Hann þarf og að geta gengið úr skugga um að þær síðast nefndu hafi farið í gang þegar skipst er á viðskiptagögnum og virkað eins og til var ætlast á því tímabili sem til endurskoðunar er. Einnig þurfa þeir sem endurskoða að geta lagt sjálfstætt mat á það hvort þessir þættir tryggi fullnægjandi öryggi og áreiðanleika.

Ljóst er að tölvur geta auðveldlega séð um kerfisbundnar eftirlitsaðgerðir af ýmsu tagi. Jafnljóst er að flóknustu þættir eftirlits, þ.e. þeir sem m.a. krefjast mannlegrar dómgreindar, verða aldrei vélvæddir. Af því leiðir að þeir sem endurskoða eiga m.a. að einbeita sér að þeim verkefnum sem maðurinn einn ræður við.

6.6 Kerfi óendurskoðunarhæft

Sú staða að upplýsingakerfi rafrænna viðskipta sé óendurskoðunarhæft getur komið upp ef þeir vélrænu eftirlitsþættir sem til staðar eru í tilteknu kerfi eru alls ófullnægjandi. Svo myndi t.d. vera ef:

a) Ekki er hægt að treysta því að færslum hafi ekki á einhverju stigi verið breytt.
b) Uppruni færslna er talinn vafasamur.
c) Ekki eru til staðar aðgerðir sem koma í veg fyrir að sama færslan fari tvívegis eða oftar í gegnum kerfið.

7. Þróun rafrænna viðskipta

Óhætt er að fullyrða að aldrei hafi þróun rafrænna viðskipta fleygt jafnört fram og um þessar mundir og það á bæði við tæknilega hlið þeirra og lagaumhverfi. Áhrifin hafa ekki látið á sér standa, stöðugt fjölgar þeim sem stunda rafræn viðskipti hvort sem litið er til fyrirtækja, opinberra stofnana eða einstaklinga.

Þar sem rafræn viðskipti eru alþjóðleg í eðli sínu hafa bæði alþjóðlegar stofnanir og ríkjasamtök beitt sér í því skyni að auðvelda viðskipti milli landa og samræma reglur, bæði staðla og löggjöf. Meðal þeirra eru Evrópusambandið, EFTA, Sameinuðu þjóðirnar, Alþjóða viðskiptastofnunin (WTO), Efnahags og framfarastofnunin í París (OECD) og sjö helstu iðnríki heims (G7).

Þar til á allra síðustu árum voru rafræn viðskipti aðallega bein og oftast svonefnd hefðbundin SMT-viðskipti sem fram fóru ýmist fram millliliðalaust eða í gegnum virðisaukandi netþjónustu, á milli tveggja aðila í föstu viðskiptasambandi. Síaukin tölvueign almennings og útbreiðsla Netsins hafa kallað á staðlavinnu vegna ódýrari aðferða til þess að stunda rafræn viðskipti. Hún hefur svo aftur leitt til aukinnar notkunar á ýmsum þeim tegundum rafrænna viðskipta sem í riti þessu eru flokkuð sem óbein.

Vegna mikilla öryggiskrafna í viðskiptum milli stofnana og/eða fyrirtækja hafa þessir aðilar hingað til aðallega stundað bein rafræn viðskipti með beinlínutengingu eða í gegnum virðisaukandi netþjónustu. Þeir sem hafa getað sætt sig við minna öryggi, oftast einstaklingar og fyrirtæki, hafa hins vegar stundað rafræn viðskipti á Netinu, oftast óbein.

7.1 Þróun staðla

Unnið er að gerð staðla beggja vegna Atlantshafsins á vegum stofnana Sameinuðu þjóðanna og Evrópusambandsins. Miklu máli skiptir að þeir ríkisaðilar sem hyggja á upptöku annarra tegunda rafrænna viðskipta en hefðbundinna SMT-viðskipta skv. UN/EDIFACT staðli, fylgist vel með framvindu mála og noti af hagkvæmnis- og öryggisástæðum eingöngu alþjóðlega viðurkennda staðla.

Í þessum kafla verður rakin nokkuð þróun staðla í rafrænum viðskiptum frá því að samvinna um þá hófst á alþjóðlegum vettvangi.

1. Staðlar í beinum rafrænum viðskiptum

1. Eldri staðlar

Hér á eftir verður fjallað um helstu staðla sem notaðir eru í beinum rafrænum viðskiptum í dag, þ.e. þeim sem oft eru einnig nefnd hefðbundin SMT-viðskipti. Hefðbundnir SMT-staðlar fjalla eingöngu um þær reglur sem gilda þegar forsníða á gagnastök („data element“) innan tiltekinnar tegundar af rammaskeyti. Þeir fjalla ekki um hvernig koma eigi skeytum milli viðskiptaaðila.

1. SMT skv. UN/EDIFACT-staðli

Algengast er að skjalalaus samskipti milli tölva séu í samræmi við staðal sem gerður var í samvinnu Efnahagsstofnunar Sameinuðu þjóðanna og alþjóðlegu staðlastofnunarinnar ISO undir samheitinu UN/EDIFACT.[17]

[17] Uppbygging og málfræði þeirra SMT-skjala sem fylgja UN/EDIFACT-staðli, er skilgreind í staðlinum ÍST EN 29735 „Electronic data interchange for administration, commerce and trade (EDIFACT) - Application level syntax rules“. Táknun helstu tegunda viðskiptagagna er hins vegar skilgreind í staðlinum ÍST EN 27372 „Trade data interchange - Trade Data Element Directory“.

Evrópubandalagið samþykkti árið 1987 svokallaða TEDIS-áætlun um SMT og kerfisbindingu slíkra samskipta og hófst fyrsti áfangi áætlunarinnar árið 1988 og lauk 1990 þegar annar áfangi hófst. Frá því ári hafa EFTA-löndin, þ.á.m. Ísland, tekið þátt í henni.

TEDIS-áætlunin leiddi til þess að aðildarríki hennar samþykktu sérstakan samning sem ætlað var að vera vegvísir við gerð samninga um SMT á milli viðskiptaaðila í Evrópu („Terms of European EDI Agreement“). TEDIS-áætlunin miðaði strax að notkun UN/EDIFACT staðalsins og hefur því stuðlað mjög að útbreiðslu hans. Af áðurnefndum samningi er þó ljóst að gert var ráð fyrir því að viðskiptaaðilar þurfa ekki að fylgja þessum staðli heldur geta þeir samið um að nota einhvern annan staðal, því í 1. grein samningsins og skýringum við hana er m.a. að finna eftirfarandi skilgreiningu:

> *„EDI: Electronic Data Interchange is the transmission of data structured according to agreed message standards, between information systems, by electronic means.“ .... „Agreed message standards“ has a broad meaning which includes but is not limited to the use of UN/EDIFACT standards and may be applied to such other standards as are agreed between the parties.“*

UN/EDIFACT hefur hingað til aðallega verið notaður í Evrópu og í alþjóðlegum viðskiptum.

Alþjóðleg staðlavinna vegna hefðbundinna SMT-viðskipta felst fyrst og fremst í gerð rammaskeyta fyrir hin ýmsu svið viðskipta. Þróun UN/EDIFACT staðals á tilteknu viðskiptasviði á sér oft þá forsögu að fyrirtæki hafa komið sér upp einkastaðli í samskiptum sínum en hann hefur síðan smám saman orðið sérstakur fyrir iðngreinina í heild og síðar að alþjóðlegum staðli.

Bein rafræn viðskipti á milli stofnana og/eða fyrirtækja hafa ekki náð þeirri útbreiðslu sem stefnt var að í upphafi og er

ein aðalástæða þess sú að UN/EDIFACT staðallinn þykir flókinn og kostnaður við hefðbundin SMT of mikill fyrir lítil og meðalstór fyrirtæki. Mikil vinna hefur því verið lögð í það í Evrópu og á alþjóðavettvangi að finna einfaldari og ódýrari leiðir til þess að örva rafræn viðskipti, bæði bein og óbein. Síðar í kaflanum verður drepið á það helsta sem þar er í nú deiglunni.

2. SMT skv. X-12 staðli

Í Bandaríkjunum hefur til þessa aðallega verið stuðst við X-12-staðalinn í SMT-viðskiptum en hann var gerður af bandarísku staðlanefndinni ANSI. Þróun hans var hætt árið 1995. Þegar sú ákvörðun var tekin nokkru áður var það í þeim tilgangi að Bandaríkjamenn færðu sig smám saman yfir í UN/EDIFACT þar sem hann var þá orðinn alls ráðandi í alþjóðlegum beinum rafrænum viðskiptum.

Nú hafa þeir aðilar sem eru í forsvari fyrir stefnumótun í þessum efnum í Bandaríkjunum ákveðið að horfa frekar til þess að ráðandi staðall í framtíðinni verði einfaldari en UN-/EDIFACT. Þessa dagana beinist skoðun þessara aðila aðallega að XML/SMT. Hver lokaniðurstaða málsins verður er óljóst á þessu stigi.

2. Þróun gamalla og nýrra staðla

1. Staðlastarf á vegum SÞ

Öflugt starf og mikilvægt vegna beinna rafrænna viðskipta fer fram í TMWG[18] en það er vinnuhópur tæknilegra sérfræðinga sem tilnefndir hafa verið á vegum UN/CEFACT[19], miðstöðvar á vegum Sameinuðu þjóðanna, en hún hefur það hlutverk að stuðla bæði að framgangi rafrænna viðskipta almennt og SMT. Á vegum UN/CEFACT og TMWG fer því enn fram hið alþjóðlega viðurkennda starf að þróun í

[18] „The Techniques and Methodologies Work Group".
[19] „United Nations Center for the Facilitation of Procedures and Practices for Administration, Commerce and Transport".

þessum málum.

TMWG-hópurinn hefur gefið út stefnumörkun fyrir næsta áfanga í þróun UN/EDIFACT-staðalsins[20] en þar er gert ráð fyrir að hópurinn vinni samhliða að eftirfarandi þremur verkefnum:

1) Viðhaldi og áframhaldandi þróun hins hefðbundna UN/EDIFACT-staðals, „Track 1: Mainstream UN/-EDIFACT“.

2) Að ýta undir þróun á einföldu SMT, „SimplEDI“ þ.e. einfaldari UN/EDIFACT-skeytum, „Track 2: Simpler UN/EDIFACT“.

   Nú þegar fylgist TMWG-hópurinn grannt með starfi ýmissa annarra hópa og framgangi tilrauna-verkefna og telur margt þar mjög áhugavert

3) Fullri þróun hlutbundinna SMT-viðskipta til þess að hanna viðskiptaskeyti framtíðarinnar, „Track 3: Object Oriented - OO/EDIFACT“.

Lögð er áhersla á að allar séu leiðirnar þrjár sem verkefnin fela í sér jafnmikilvægar og þær þurfi m.a. að þróa með það í huga að notendur geti áreynslulítið flutt sig á milli þeirra.

2. Um einföld SMT-viðskipti

Einföld SMT-viðskipti felast í gagnaflutningi í algjörlega sjálfvirku umhverfi þar sem gögn styðjast við einfaldað undirmengi af UN/EDIFACT. Þetta er leið til beinna raf-rænna viðskipta sem talin eru geta hentað þörfum bæði lítilla og meðalstórra fyrirtækja. Einföld SMT-viðskipti eru eins og að framan greinir ein af þeim þremur leiðum sem TMWG telur að þróa þurfi vegna rafrænna viðskipta í fram-tíðarinni.

[20] „UN/EDIFACT, A strategy for the next phase“, Trade/WP.4/-CRP.123/Appendix 2.

3. Um opin SMT-viðskipti

TMWG skilgreinir opin SMT-viðskipti á eftirfarandi hátt sem augljóslega ber með sér megineinkenni þeirra rafrænu viðskipta sem í riti þessu hafa verið flokkuð sem bein:

> *„The application to application exchange of any pre-defined and structured data for business purposes without human intervention and without prior agreement*"
>
> þ.e.:
>
> *„Sendingar frá notendahugbúnaði til notendahugbúnaðar á fyrirfram skilgreindum og sniðnum gögnum í viðskiptalegum tilgangi án þess að mannshöndin komi þar nærri og án fyrirfram gerðs samkomulags á milli aðilanna.“*

Áðurnefnd skilgreining TMWG á opnu-SMT byggir á nokkrum lykilatriðum:

1) Gögn verða að vera mótuð og fyrirfram skilgreind.
2) Ekki hefur fyrirfram verið gert samkomulag um viðskiptin.
3) Mannshöndin kemur ekki nálægt gagnasendingunum.
4) Gagnasendingarnar eru óháðar grunnupplýsingakerfum viðskiptaaðilanna.
5) Gagnasendingar geta farið fram á milli ólíkra atvinnugreina.

Ofangreind skilgreining á opnu-SMT felur í sér lýsingu á sendingum viðskiptagagna sem óháð er sérstakri tækni og nálgun einstakra atvinnugreina. Það sem einnig vekur athygli er að ekki þarf fyrirfram að liggja fyrir samkomulag á milli aðilanna um viðskiptin andstætt því sem nú er á milli þeirra sem nota hefðbundið SMT skv. UN/EDIFACT staðli. Af þessari ástæðu og fleirum sem þarna eru taldar er ljóst að hér er um að ræða möguleika til beinna rafrænna viðskipta sem hentað geta mun stærra hópi en þeim sem notar þennan möguleika í dag.

Hugmyndin um opið-SMT felur í sér að staðlar eru skoðaðir annars vegar með tilliti til viðskiptalegrar hliðar samskiptanna „BOV“, („Business Operational View“) og hins vegar með tilliti til upplýsingatæknilegrar hliðar þeirra, „FSV“, („Functional Service View“). Hugsanlega þarf að uppfylla marga staðla vegna beggja hliðanna svo að líkanið gangi upp. Viðskiptalega hliðin snýst um hvaða aðilar eiga í hlut, hlutverk þeirra, atriði sem snerta viðskiptaferlið sjálft, samþykki, gögnin o.fl., en upplýsingatæknilega hliðin lýtur að því hvernig hægt er að koma viðskiptunum á, hvaða SMT-staðal, samskiptastaðla og tengingar við notendahugbúnað á að nota o.fl. Gert er ráð fyrir því að notað verði „UML“, („Universal Model Language“).

Opið-SMT er auk þess að vera hluti af framtíðarsýn Sameinuðu þjóðanna sú framtíðarleið sem ISO/IEC horfir nú til. Ljóst er því að þessi leið nýtur mikils stuðnings þeirra sem vinna að samræmingarmálum í rafrænum viðskiptum.

Hlutbundin SMT-viðskipti

Hlutbundin SMT-viðskipti „Object Oriented-EDI“ eða „OO-EDI“, teljast til opinna SMT-viðskipta og flokkast því sem bein rafræn viðskipti.

Hlutbundin SMT-viðskipti byggja á viðskiptaferlum og aðferðafræði gagnalíkana. Í gagnalíkani hlutbundins SMT koma fram þarfir viðskiptaferlisins og þættir tengdir því í þeim mæli að fjöldaframleiðsla notendahugbúnaðar sem styður SMT-gagnaflutninga er talin verða fýsilegur kostur fyrir hugbúnaðarframleiðendur .

Gert er ráð fyrir því að þróunarkostnaður kerfa sem byggja á hlutbundinni tækni verði mun minni en hefðbundinna SMT-kerfa vegna endurnýtingarmöguleika gagna. Einnig er gert ráð fyrir að auðveldara og ódýrara verði að viðhalda þeim og að samskipti við annan hugbúnað verði mun auðveldari en þau eru nú í hefðbundnum SMT-viðskiptum.

2. Staðlar í óbeinum rafrænum viðskiptum

Óbein rafræn viðskipti á Netinu fara nú oftast þannig fram að seljendur hleypa kaupendum beint inn í tölvukerfi sitt að skrá gögn. Í þessum tilvikum er ekki er um skjalasendingar milli tveggja tölvukerfa og sjálfvirka vinnslu gagnanna í þeim báðum að ræða eins og í beinum rafrænum viðskiptum, enda eru aðilar viðskiptanna hér oftast fyrirtæki eða stofnun og einstaklingur. Mikil vinna hefur að undanförnu verið lögð í þróun nýrra aðferða vegna óbeinna rafrænna viðskipta og verður hér á eftir fjallað um þær helstu.

1. Óbein SMT-viðskipti á Netinu

Fram eru komnar nýjar tegundir af óbeinum SMT-viðskiptum sem horfa fyrst og fremst til rafrænna viðskipta í gegnum Netið. Létt SMT, Vef SMT, og XML/SMT eru þær tegundir sem hæst ber nú um stundir. Meðal þeirra sem að þessu verki hafa komið er UN/CEFACT. Hér á landi hefur ICEPRO, nefnd um rafræn viðskipti, unnið ötullega að þróun þessara nýju tegunda. Tæknihópur ICEPRO hefur fylgst náið með þróunarstarfi vegna XML/SMT og er ýmsar upplýsingar um þetta að finna á heimasíðu[21] hópsins.

Líklegt má telja að XML/SMT staðallinn sem nú er unnið að m.a. á vegum Sameinuðu þjóðanna muni verða ráðandi á næstu árum og önnur afbrigði eins og létt SMT og Vef SMT muni því ekki ná fótfestu og hverfa.

1. Vef SMT

Vef SMT fer fram með þeim hætti að kaupandi fer beint inn á vefsíðu viðtakanda sem annað hvort er staðsett í tölvukerfi hans eða þjónustuaðila, þ.e. kaupandinn fær beinan aðgang að viðkomandi tölvukerfi og skráir þar upplýsingar inn í staðlað skjal svipað og hann væri að fylla út eyðublað. Hug-

[21] Sjá: http://www.chamber.is/icepro/xmlnefnd.htm

búnaður þar þýðir síðan gögnin og sendir þau sem SMT-skeyti til áframhaldandi vinnslu. Þessi rafrænu viðskipti eru óbein því þó að algengast sé að seljandi sendi kaupanda tölvupóst til baka þar sem hann greinir frá móttöku pöntunar o.fl. er ekki um að ræða sjálfvirka vinnsla þeirra upplýsinga í kerfi kaupandans. Hefðbundin viðskiptaskjöl eru svo að jafnaði send með vörunni nema hún sé afgreidd yfir Netið eins og t.d. hugbúnaður.

2. Létt SMT

„EDI-Lite/Light“ er tilraunaverkefni á vegum nefndar sem kom í stað Vestur-Evrópsku EDIFACT-nefndarinnar, og felst það í þróun þægilegrar allsherjar lausnar á skjalalausum samskiptum milli tölva, og byggir á einfaldaðri útfærslu UN/EDIFACT fyrir vefsíður.

3. XML/SMT

Eitt af því sem nú er mikið rætt um er hvort stefna eigi að upptöku á „XML-málskipan“ „eXtensible Markup Language“ í rafrænum viðskiptum.

XML-málskipan er náskyld HTML-málskipan „Hypertext Markup Language“ sem er grundvöllur Veraldarvefsins í dag. Í HTML-skjölum er oftast að finna eftirfarandi þætti í einu og sama skjalinu:

1) Efni, þ.e. texta.
2) Virkni, t.d. JavaScript.
3) Framsetningu, þ.e. leturgerðir, leturstærðir o.s.frv.

Í XML eru framangreindir þrír þættir aðskyldir enda sjá mismunandi aðilar oftast um þá, þ.e. almennir starfsmenn sjá um efni, forritarar um virkni og grafískir hönnuðir um framsetningu. Ávinningur af aðgreiningu þáttanna þriggja er margþættur, m.a. vinnusparnaður og auðveldari tölvuvinnsla gagna. Annar mikilvægur ávinningur felst í því að í XML eru gagnaskilgreiningar sem leyfa túlkun gagnastaka bæði af mönnum (með framsetningu) og af kerfum á sjálfvirkan hátt. HTML geymir ekki skilgreiningar

gagnastaka.

Þegar XML-málskipan er tengd við UN/EDIFACT-staðalinn verður til staðall sem hlotið hefur heitið XML/SMT (XML/EDI). Í þessum nýja staðli sameinast öflug blanda nýrrar tækni og margra ára reynsla af notkun hefðbundinna SMT-viðskipta.

„The International XML/EDI-Group“ hefur sett fram drög að leiðbeiningum[22] um notkun XML í SMT-viðskiptum. Talin var þörf á því að prófa leiðbeiningarnar í Evrópu vegna fjölda tungumála og ólíkra hefða í viðskiptum innan álfunnar. Þetta verkefni er nefnt: „The ISIS European XML/EDI Pilot Project“[23] og er það fjármagnað sameiginlega af Evrópusambandinu og ýmsum fyrirtækjum og opinberum aðilum innan þess. Verkefnið sem hófst í janúar 1999 er unnið í opnum hópi innan CEN/ISSS Electronic Commerce Workshop[24] og á því að ljúka á árinu 2000. Rétt er að geta þess að sami aðili, þ.e. Staðlastofnun Evrópu (CEN), sér jafnframt um UN/EDIFACT staðalinn í Evrópu þannig að miklar líkur eru á því að verkefnið skili árangri.

Hópurinn sem vinnur að þessu sameiginlega evrópska verkefni er að kanna leiðir sem eiga að gera það kleift að varpa hefðbundnum SMT-skeytum yfir á XML-snið. Það er gert í því skyni að hægt sé að birta skeytin á hefðbundnum skjalavöfrum á Netinu og að snúa XML-skeytum, sem byggja á SMT-samhæfðum gagnaþáttum, yfir í viðeigandi SMT-skeyti. Einnig er hópurinn að skoða hvernig hægt er að samþætta gögn úr XML-skeytum í gagnagrunnum og innri viðskiptaferlum hjá viðskiptaaðila en þetta er eitt að því sem er vandamál í dag fyrir SMT-notendur. Í nálgun hópsins er aðaláhersla lögð á að vörpunarferlið verði eins sjálfvirkt og mögulegt er og að þeir ferlar sem þróaðir verða séu nægilega einfaldir til þess að hægt sé að koma þeim í gagnið hjá litlum og meðalstórum fyrirtækjum ef þar er ekki til staðar sérstök tölvuþekking.

[22] Sjá: http://www.xmledi-group.org/xmledigroup/guide.htm
[23] Sjá: http://www.cenorm.be/isss/workshop/ec/xmledi/isss-xml.html
[24] CEN/ISSS stendur fyrir „European Center for Standardization/Information Society Standardization System“ og eru stofnun og kerfi innan Evrópusambandsins.

TMWG vinnuhópur UN/CEFACT hefur eins og áður er komið fram sett fram áætlun vegna þróunar á hlutbundnum rafrænum viðskiptum sem teljast til opinna SMT-viðskipta. Hópurinn hefur m.a. kannað samhæfni þeirra og XML/SMT og gefið út skýrsludrög um það efni. Í þeim telur TMWG að þessar tegundir séu fullkomlega samhæfðar og bæti hvor aðra upp.

Annað verkefni sem tengt er UN/CEFACT og vert er að vekja athygli á, er ebXML „Electronic Business XML“[25]. Verkefninu er ætlað að staðla notkun á XML í rafrænum viðskiptum. Meginviðfangsefni þess er að gera rafræn viðskipti að hagkvæmari kosti fyrir lítil og meðalstór fyrirtæki ásamt því að vera álitlegur kostur fyrir þróunarríkin.

Miklar líkur eru á því að XML muni hafa veruleg áhrif á þróun rafrænna viðskipta á komandi árum. Ríkisendurskoðun hvetur alla þá sem áhuga hafa á þessum málum að fylgjast með starfi XML/EDI-nefndar ICEPRO[26] auk starfs þeirra sem nefndir hafa verið hér að ofan.

7.2 Þróun hjá ríkisaðilum

Rafræn viðskipti voru fyrst tekin upp hjá ríkinu árið 1991. Ríkistollstjóraembættið hóf undirbúning og prófanir á rafrænni tollafgreiðslu samkvæmt sérstakri heimild fjármálaráðuneytisins og fóru fyrstu skeytasendingar vegna farmskráruppl ýsinga fram það ár. Fyrstu tollafgreiðslurnar fóru fram hjá tollstjóranum í Reykjavík 1992 en fljótlega þar á eftir í öllum tollumdæmum. Frá þeim tíma hafa ýmsir aðilar smám saman verið að bætast við, t.d. Tryggingastofnun vegna rafrænna lyfseðla frá apótekum árið 1997.

Framundan eru líklega aukin rafræn viðskipti ríkisaðila og kemur þar tvennt til. Annars vegar ör þróun í þessa átt almennt og hins vegar stefna ríkisstjórnarinnar. Hún sam-

[25] Sjá: http://www.ebxml.org
[26] Sjá http://www.chamber.is/icepro/xmlnefnd.htm

þykkti í mars 1999 að verkefnisstjórn forsætisráðuneytisins í málefnum upplýsingasamfélagsins mótaði heildarstefnu ríkisstjórnarinnar um rafræn viðskipti. Í apríl 2000 sendi verkefnastjórnin síðan frá sér vinnuáætlun bæði um þróun rafrænna viðskipta og stjórnsýslu á árunum 2000-2002.[27] Ef áætlunin gengur eftir má búast við örri þróun rafrænna viðskipta hjá ríkisaðilum því gert er ráð fyrir því að þau verði í hópi forgangsverkefna stjórnvalda á fyrrgreindu tímabili.

Næsta stóra verkefnið á þessu sviði er líklega rafræn skil á virðisaukaskatti en einnig er gert ráð fyrir frekari útfærslu á viðskiptum með innkaupakortum ríkisins.

1. Rafræn tollafgreiðsla

Með stoð í tollalögum og virðisaukaskattslögum var sett reglugerð nr. 309/1992 um tollafgreiðslu og greiðslufrest á aðflutningsgjöldum þegar tollskjöl eru send milli tölva. Hún var forsenda upptöku á rafrænni afgreiðslu tollskýrslna í tölvukerfi ríkistollstjóra (Tollakerfið) og aðalheimildin varðandi útfærslu hennar allt þar til ákvæði hér að lútandi voru lögfest með lögum nr. 69/1996 um breytingu á tollalögum.

Setning áðurnefndrar reglugerðar var tímamótaverk og geymir fyrstu reglurnar um framkvæmd beinna rafrænna viðskipta hér á landi. Í reglugerðinni er mikið um hugtakaskýringar svo sem eðlilegt er og hafa flestar þeirra nú skilað sér inn í tollalögin. M.a. er SMT skilgreint sem „Skjalasending milli tölva“ og lýst þannig: „Sendingar á gögnum milli gagnavinnslukerfa sem fylgja ákveðnum stöðlum.“ Ljóst er hvaða staðla er átt við hér því að lokinni skilgreiningu á hugtakinu rammaskeyti segir að þau skulu gerð samkvæmt staðlinum UN/EDIFACT fyrir SÞ-rammaskeyti vegna tollafgreiðslu vara.

[27] Áætlunina er að finna á vefsíðu verkefnastjórnarinnar, sjá: http://brunnur.stjr.is/interpro/for/for.nsf/pages/vinnuaaetlun_april00.html

Þeir sem fá leyfi til skjalalausra samskipta milli tölva við Tollakerfið nefnast leyfishafar. Eitt af þeim skilyrðum sem þeir verða að uppfylla er að ríkistollstjóri hafi samþykkt þann hugbúnað sem umsækjandi hyggst nota til samskipta við tollyfirvöld.

Hefja má rafræna tollmeðferð vara og sendinga þegar ríkistollstjóri hefur veitt heimild til að tengja tölvukerfi leyfishafa við tölvukerfi ríkistollstjóra og leyfishafi hefur fengið lykilorð að gagnahólfi sem skráð er á hans nafn. Innflytjandi sendir síðan rafræna aðflutningsskýrslu með skeyti um gagnaflutningsnet Skýrr h.f. til Tollakerfis ríkistollstjóra sem beinir því til þess tollstjóra sem afgreiða á vöruna. Vara eða sending telst tekin til tollmeðferðar um leið og skeyti sem geymir aðflutningsskýrsluna er skráð í Tollakerfið. Það sendir síðan í gagnahólf viðkomandi leyfishafa skeyti sem geymir bæði heimild til að veita vörunni eða sendingunni viðtöku frá vörsluhafa og tilkynningu um skuldfærslu aðflutningsgjalda. Enn fremur sendir Tollakerfið farmflytjanda eða öðrum vörsluaðila vöru eða sendingar skeyti með heimild til afhendingar hennar.

Þegar um SMT-tollafgreiðslu er að ræða er innflytjanda veittur greiðslufrestur á aðflutningsgjöldum og er hann skuldfærður fyrir þeim nema greiðsla í ríkissjóð fari þegar fram með millifærslu af bankareikningi innflytjanda. Vegna þessa hefur SMT-tollafgreiðslan fengið heitið „Tollkrít“ manna á meðal.

Í ársbyrjun 1998 var einnig tekin upp rafræn tollafgreiðsla útflutnings.

Með áður nefndum lögum nr. 69/1996 um breytingu á tollalögunum nr. 55/1987 var gert ráð fyrir því að tollafgreiðsla á vegum fyrirtækja yrði eingöngu rafræn frá og með ársbyrjun 2000. Með lögum nr. 109/1999 var því frestað þar til í ársbyrjun 2001 bæði vegna óljósrar stöðu mála vegna 2000-vandans og þó aðallega vegna örra tæknibreytinga. Um þetta segir í athugasemdum með frumvarpinu:

> *„Meginástæða þess að þessi breyting er lögð til er sú að örar breytingar í tölvutækni á undanförnum árum, einkum vegna aukinnar notkunar internetsins, hafa skapað nýja möguleika við tölvuvædda tollafgreiðslu, sem nauðsynlegt þykir að kanna betur. Er þar einkum um að ræða möguleika fyrir lítil fyrirtæki til að taka upp SMT-tollafgreiðslu með aðstoð internetsins með minni tilkostnaði en ella hefði orðið. " ..... „ ... er lagt til að frestur til að taka upp SMT-tollafgreiðslu verði framlengdur um eitt ár. Er talið að sá tími verði nægilegur fyrir tollyfirvöld til að kanna möguleika á breyttum tollafgreiðsluháttum."*

Enn liggur ekki fyrir með hvaða hætti breytingar verða gerðar á tollafgreiðsluháttum. Hitt er ljóst að enn er gerð sú krafa að tollskjöl berist um X.400 virðisaukandi netþjónustu og er ekki gert ráð fyrir breytingu á því fyrr en menn sannfærast um öryggi annarra gagnaflutningsleiða.

2. Rafræn viðskipti lyfjaverslana og TR

Á árinu 1997 var tekið í notkun hjá Tryggingastofnun ríkisins nýtt hugbúnaðarkerfi sem nefnt er Lyfjaeftirlitskerfi. Kerfi þetta gegnir tvíþættu hlutverki. Annars vegar lyfjaeftirliti og hins vegar pappírslausum viðskiptum við lyfjaverslanir vegna kostnaðarhlutdeildar ríkisins í lyfjaverði.

Þau gögn sem unnið er með í Lyfjaeftirlitskerfinu eru lyfseðlar sem sendir eru frá tölvukerfum lyfjaverslana í formi skeyta skv. UN/EDIFACT-staðli. Þau rafrænu viðskipti sem hér um ræðir eru því bein og hefðbundin SMT-viðskipti. Nánari umfjöllun um lyfjaeftirlitskerfið er að finna í skýrslu Ríkisendurskoðunar um kerfið sem gefin var út í júlí 1997.

3. Rafræn skil á virðisaukaskatti

Einn af starfshópum nefndar um framkvæmd virðisauka-

skatts[28] kannaði möguleika og kosti rafrænna skila á skýrslum og greiðslum vegna virðisaukaskatts og lagði til að könnun lokinni að upp yrðu tekin slík rafræn skil.

Í skýrslu sinni telur nefndin að ekki sé um einfalt mál að ræða enda hafi það víðast hvar erlendis reynst vandleyst. Nefndin telur og að forsendur fyrir rafrænum skilum séu að rafræn undirritun skýrslu sé lögformlega örugg og óvéfengjanleg. Jafnframt sé nauðsynlegt að við hönnun kerfis til að taka á móti rafrænni virðisaukaskattsskýrslu sé gætt öryggis með tilliti til meðferðar á fjármunum og aðgengis að upplýsingum.

Nefndin mælti með því meðan hún var að störfum að fjármálaráðuneytið beindi því til embættis ríkisskattstjóra að hafist yrði handa um að undirbúa rafræn skil virðisaukaskatts. Á vegum þess hefur því farið fram undirbúningsvinna vegna rafrænna skila virðisaukaskatts í starfshópi sem í eiga sæti fulltrúar frá ríkisskattstjóra, skattstjóranum í Reykjavík, ríkisbókhaldi og tollstjóranum í Reykjavík. Hópurinn hefur í starfi sínu m.a. horft til lagalegra atriða og tæknilegrar uppbyggingar slíks kerfis og vegna þessa kynnt sér rafræn skil á virðisaukaskatti á hinum Norðurlöndunum. Hvað tæknilegar útfærslur varðar hefur starfshópurinn velt fyrir sér nokkrum leiðum sem allar eiga það sameiginlegt að byggja á notkun Netsins.

Ef frumvarp það að rafrænum undirskriftum sem nú liggur fyrir í drögum verður óbreytt að lögum er komin fram lausn á vandamálinu varðandi lagalega bindandi undirskrift virðisaukaskattsskýrslu því í drögunum, sem ná aðeins til opinna kerfa eins og Netsins, er gert ráð fyrir því að tiltekin útfærsla af rafrænni undirskrift jafngildi „handritaðri“.

Til að fylgja eftir tillögum nefndarinnar um upptöku rafrænna skila á skýrslu og greiðslu var frumvarp lagt fram á Alþingi í vor til breytinga á lögum nr. 50/1988 um virðisaukaskatt. Eftir samþykkt þess með lögum nr. 105/2000 hljóðar 3. málsl. 1. mgr. 24. gr. laganna um virðisaukaskatt

[28] Framkvæmd virðisaukaskatts, nefndarálit, útg. af fjármálaráðuneytinu, rit 2000-1, mars 2000.

SVO:

> *Fjármálaráðherra ákveður í reglugerð um greiðslustaði, greiðslufyrirkomulag og efni skýrslu, þar á meðal um rafræn skil á skýrslu og greiðslu.*

Þó að það sé ótengt áðurnefndum fyrirætlunum um rafræn skil er rétt að geta þess hér að fyrirsjáanlegt er að auknum rafrænum viðskiptum fylgi ný tegund skattalegra vandamála, einkum við innheimtu og eftirlit með virðisaukaskatti. Sérstaklega á þetta við vegna vöru eða þjónustu sem keypt er og afhent yfir Netið þar sem eðli þess er með þeim hætti að þar eru engin landamæri sem skattayfirvöld eiga auðvelt með að skilgreina.

4. Innkaupakort ríkisins

Á árinu 1998 skipaði fjármálaráðherra nefnd til þess að kanna kosti og galla þess að taka í notkun greiðslukort hjá ríkisstofnunum og skilaði hún áliti snemma árs 1999. Niðurstaðan var í meginatriðum sú að umtalsverðum sparnaði mætti ná með upptöku greiðslukorta, einkum í viðskiptum sem ekki ná 50 þúsund krónum. Til stuðnings þessari niðurstöðu voru lagðar fram eftirfarandi upplýsingar úr bókhaldi 93 stofnana sem voru í bókhaldsþjónustu Ríkisbókhalds:

Fjárhæðir reikninga	Hlutfall af heildarfjölda reikninga	Hlutfall af heildarfjárhæð reikninga
Undir kr. 10.000	63%	10%
Kr. 10.000 – 49.999	28%	26%
Kr. 50.000 – 99.999	5%	16%
Yfir kr. 100.000	4%	48%
Alls:	100%	100%

Tafla 1. Flokkun reikninga í bókhaldsþjónustu Ríkisbókhalds eftir fjárhæðum.

Eins og sjá má var voru 63% reikninganna undir 10.000 kr. en heildarverðmæti þessara smáreikninga aðeins um 10% af heildarviðskipunum.

Eftir að útboð hafði farið fram var fyrr á þessu ári gerður samningur við Europay Ísland um sérstök innkaupakort ríkisins. Markmið hans eru að einfalda greiðsluferli reikninga og draga úr umsýslukostnaði við smáinnkaup ríkisstofnana og auka um leið yfirsýn stjórnenda vegna innkaupa og styrkja rammasamningskerfi Ríkiskaupa. Af framangreindum markmiðum má sjá að innkaupakortunum er ætlað stærra hlutverk en almennum greiðslukortum en þau eru fyrst og fremst til hagræðis við greiðslu.

Fyrst í stað verða innkaupakortin væntanlega eingöngu notuð við kaup sem ekki ná 50 þúsund krónum og til innkaupa fyrir hærri fjárhæð í sérstökum tilfellum. Jafnframt er ætlunin að safna rafrænum upplýsingum í gagnagrunn vegna hverrar færslu til vinnslu á upplýsingum um innkaup ríkisins sem gagnlegar geti verið fyrir stjórnendur ríkisaðila.

Síðar er ætlunin að taka gögn úr gagnagrunninum beint inn í bókhald ríkisaðila og hætta að gefa út pappírsreikninga vegna þeirra viðskipta sem gerð eru með innkaupakortunum. Í framkvæmd er þetta hins vegar nokkrum erfiðleikum háð bæði vegna þess að ekki er í notkun samræmt vörunúmerakerfi hér á landi og að ekki er með einföldum hætti hægt að tengja saman samræmdan bókhaldslykil ríkisins við

bókunarlykla fjölmargra seljenda.

Ef þessar fyrirætlanir ná fram að ganga mun það hafa veruleg áhrif á innra eftirlit og innkaupaferli stofnana. Af þessum sökum er gert ráð fyrir því að innkaupaferli ríkisaðila verði endurskoðað jafnhliða upptöku kortanna.

Hafin er tilraunanotkun á innkaupakortunum hjá þremur stofnunum ríkisins. Þegar þetta er skrifað er ekki búið að fullmóta reglur um notkun kortanna þannig að ekki eru forsendur fyrir því að fjalla nánar um þau hér.

5. Rafræn opinber innkaup

Á árinu 1999 skipaði fjármálaráðherra nefnd til þess að vinna að tillögum um rafrænt innkaupakerfi fyrir ríkisstofnanir í tengslum við rammasamningakerfi Ríkiskaupa. Verkefni nefndarinnar skiptist í eftirfarandi verkþætti:

- Að kanna útbreiðslu rafrænna viðskipta á Íslandi.
- Skoða möguleikana á því að sameina rafrænt útboðs- og pöntunarkerfi.
- Leggja mat á kostnað við undirbúning og uppbyggingu slíks sameiginlegs kerfis.
- Að móta sameiginlega stefnu ríkisins og viðskiptalífsins vegna rafrænna viðskipta í opinberum innkaupum.

Nefndin skilaði í júlí 2000 skýrslu um rafræn viðskipti í opinberum innkaupum og mun þegar er skrifað vera að vinna að öðrum verkþáttum. Vænta má þess að niðurstaða nefndarinnar muni hafa veruleg áhrif á það með hvaða hætti rafræn viðskipti þróast hjá ríkisaðilum á næstu árum.

Helstu heimildir

Applied Cryptography
Bruce Scheneier
John Wiley & Sons Inc., 1996

Cracking DES
Electronic Frontier Foundation, 1998

Drög að frumvarpi til laga um rafrænar undirskriftir
Iðnaðar- og viðskiptaráðuneyti, 14. maí 2000.

EDI Control Guide
EDI Council of Australia, 1990

EDI - kontroller och revision
Riksrevisionsverket, 1993

EFTA Trader's ABC
A Trade Facilitation Manual
EFTA, 1999

Electronic Commerce
Control Issues for Securing Virtual Enterprises
Marcella, Stone & Sampias
Institue of Internal Auditors, 1998

Electronic Commerce legislation, frequently asked questions
Benjamin Wright, mars 1997

Evrópskar siðareglur um Netviðskipti
Proposal for a European Code of Conduct for On-line Commercial Relations
Sjá heimasíðu Samtaka verslunar og þjónustu:
http://www.svth.is/

Framkvæmd virðisaukaskatts, nefndarálit, rit 2000-1
Fjármálaráðuneyti, 2000

Innra eftirlit
Ríkisendurskoðun, 1998

Lyfjaeftirlitskerfi Tryggingastofnunar
Ríkisendurskoðun, 1997

Innkaupahandbók um upplýsingatækni 1998
Fjármálaráðuneytið/RUT-nefndin, 1998

Internet and EDI in Effective Accounting
Heli Salmi & Pauli Vahtera, 1997

Performance Auditing of the use of EDP Future Challenges
Riksrevisionsverket, 1995

Rafræn viðskipti, umfjöllun um íslensk lög
Gunnar Thoroddsen og Skúli Magnússon
Iðnaðar- og viðskiptaráðuneyti, 1999

Rekstraröryggi upplýsingakerfa
Ríkisendurskoðun, 1998

Risk and Controls in an EDI Environment
Raju Navin Metha
IS Audit & Control Journal, Volume V, 1998

Samræmd tilmæli varðandi samskipti á viðskiptagögnum með fjarskiptum - UNCID

(„Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission“) Sjá heimasíðu tækninefndar ICEPRO: http://www.chamber.is/icepro/t-nefnd1.htm

Skjalasendingar milli tölva, SMT Handbók

ICEPRO, nefnd um rafræn viðskipti, 1991

Starfsskýrsla stýrihóps um rafræn viðskipti í opinberum innkaupum

Fjármálaráðuneytið, 2000

Tölvuorðasafn

Orðanefnd Skýrslutæknifélags Íslands

Íslensk málnefnd, 1998

UNCITRAL Model Law on Electronic Commerce

Ályktun Sameinuðu þjóðanna nr. 51/162 frá 16. des. 1996

Vinnuáætlun um þróun rafrænna viðskipta og rafrænnar stjórnsýslu 2000 - 2002

Verkefnisstjórn um upplýsingasamfélagið, apríl 2000

Web Security & Commerce

Garfinkel & Spafford

O'Reilly & Associates Inc., 1997

XML/EDI, Cyber Assisted Business in practice

Dick Raman

TIE Holding NV, 1999