# RAFRÆNN REIKNINGUR – STOÐUPPLÝSINGAR

## BURÐARLAG OG ÖRYGGI

14. október 2009

Ritnefnd um burðarlag og öryggi

### Inngangur

Þetta skjal er hluti af stoðupplýsingum sem styðja tækniforskrift fyrir rafræna reikninga. Umfjöllunin miðast við lesendur sem hafa ekki tæknilega þekkingu en eru ábyrgir fyrir innleiðingu rafrænna reikninga og útfærslu á samskiptum milli viðskiptaaðila. Í sumum tilvikum er vísað á ítarefni sem getur verið af tæknilegum toga.

### Almenn umfjöllun

Öryggi í rafrænum viðskiptum byggir á því að hægt sé að koma rafrænum skjölum á milli útgefanda og viðtakanda án þess að innihald þeirra spillist eða komist í hendur óviðkomandi meðan á flutningi stendur.

Í nútíma viðskiptum verður að gera ráð fyrir því að útgefandi og viðtakandi hafi ekki stjórn á því hvernig og hvaða leið skjölin fara í fjarskiptanetum. Því ganga flestar aðferðir út frá því að tryggja öryggi milli útgefanda og viðtakanda óháð flutningsaðferð (transport protocol t.d. HTTP, SMTP, X.400) og undirliggjandi flutningsleið (transport, Internet og network interface layer).

Öryggi skeytasendinga frá útgefanda og viðtakanda er tryggt í burðarlaginu þar sem útgefandi og viðtakandi hafa sjaldnast fulla stjórn á flutningslaginu. Hér verður gengið út frá því að burðarlag í rafrænum viðskiptum sé sá hugbúnaður sem viðskiptakerfi nota til að senda og taka við rafrænum skjölum á öruggan hátt. Aðferðir til að tryggja öryggi í burðarlaginu byggja á tæknilegri útfærslu á því hvernig tekið er við skeytum, þau send og varðveitt ásamt samkomulagi milli aðila um hvernig útfærslunni skuli háttað. Burðarlag er mjög almennt og opið hugtak. Í meginatriðum er afmörkun hugtaksins allt það sem þarf til að koma viðskiptaskjali á milli viðskiptaaðila. Lykilþáttur í slíkum samskiptum er það traust sem þarf að ríkja um viðskiptaupplýsingarnar og á milli viðskiptaaðilanna, traust sem felst í þeim öryggisþáttum sem útfærðir eru.

Burðarlag þarf að hafa eftirfarandi eiginleika:

- Styðst við almenna viðurkennda staðla.
- Stofnkostnaður notenda þekktur.
- Styður almenna samskiptahætti.
- Öryggi.
- Áreiðanleiki.
- Rekjanleiki.

Auk þess er æskilegt að burðarlagið hafi eftirfarandi eiginleika:

- Staðfest samskipti (handshaking).
- Staðfest og einkvæmt (1:1).
- Kom ekki (1:0).
- Kom margfalt (1:n).

Til að hægt sé að útfæra samskiptin um burðarlagið þarf að svara því hvenær þessir eiginleikar eiga við, af hverju þeir skipta máli og hvernig þeir eru tryggðir.

Í þessari umfjöllun er miðað við miðlun rafræns reiknings á formi samkvæmt NES-UBL. Tekið er tillit til annarra forma á rafrænum reikningum, t.d. EDIFACT INVOIC skeytisins, en ekki miðað sérstaklega við það né önnur einstök form.

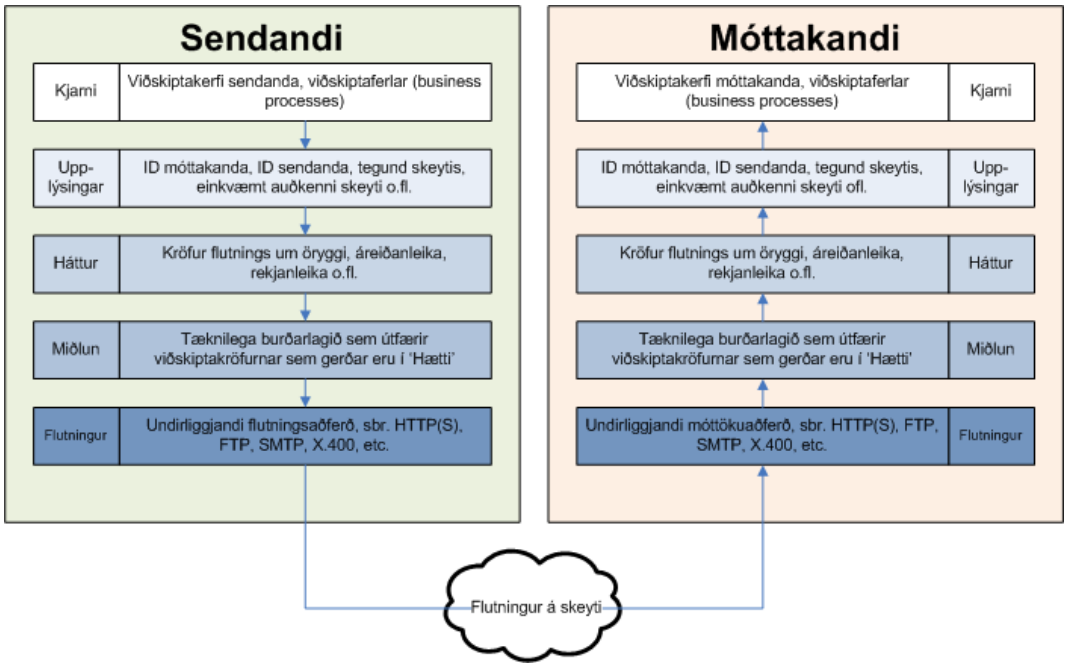
## Upplýsingar um sendingu

Í miðlun viðskiptaupplýsinga á milli viðskiptaaðila þarf að tryggja að skeytið berist réttum aðila og sé meðtekið af móttakanda á réttum forsendum. Upplýsingar sem þarf að tilgreina í haus skeytisins eru frá hverjum það er, til hvers það á að fara og tegund skeytisins sem er verið að senda.

Til að einkenna sendanda og móttakanda verður að nota einkvæm auðkenni, t.d. kennitölu eða skráða GLN kennitölu (einnig þekkt sem EAN kennitala) til að auðkenna viðskiptaeiningarnar sem eru að skiptast á skeytum. Mikilvægt er að nota alþjóðlega þekkt og einkvæmt auðkenni í alþjóðlegum viðskiptum.

Tegund skeytisins vísar í samkomulag þeirra sem eru að skiptast á skeytum um hvernig þau eiga að vera uppbyggð og hvernig eigi að vinna úr þeim. Dæmi um slíkt samkomulag væri ef tegund skeytisins væri BasicInvoice úr NES2.0. Þá lægi fyrir sameiginlegur skilningur um hvernig eigi að búa til skeytið sem og að bregðast við þegar það er móttekið.

Sé nauðsynlegt að gera aðgengilegar ítarlegri upplýsingar um slíkt samkomulag er t.d. hægt að nota kennimark viðfangs (e. Object Identifier), sjá nánar á (http://www.pta.is/Default.aspx?cat_id=238 og www.oid-info.com).




## Háttur samskipta

Eftirfarandi þættir varða trygga afhendingu, túlkun og úrvinnslu rafrænna reikninga sem miðlað er á milli viðskiptaaðila:

- Forgangur (e. priority).
- Þjónustustig (e. service level).
- Staðfesting/svörun (e. confirmation – handshaking).
- Rekjanleiki (e. traceability).
- Leiðstýring (e. routing).
- Röðun og samsöfnun/sundurliðun innihalds (e. ordering, collecting and segmentation of payload).
- Reglur/kröfur til 3ja aðila (e. service policies).
- Eftirlit – úttektir (e. observation and reporting).

Ofangreind atriði eru meðal þeirra þátta sem aðilar verða að vera sammála um til að geta skiptist á rafrænum skjölum. Einfaldast er að gera slíkt samkomulag fyrirfram, t.d. í þjónustusamningum. Það fer síðan eftir tæknihöguninni hvort mögulegt sé að breyta einhverjum þætti í rauntíma meðan samskipti eiga sér stað. Vefþjónustuskilgreiningar sem ná yfir þessi atriði eru m.a. WS-Reliability, WS-ReliableMessaging og ebXML Message Service.

## Öryggisþættir

Markmið fyrirtækja með notkun rafrænna reikninga er lækkun kostnaðar og stytting tíma við gerð, dreifingu, innheimtu og greiðslu reikninga. Rafræn viðskipti verða aðeins valkostur ef þau eru álitin jafn örugg eða öruggari en hefðbundari aðferðir.

Með því að útfæra öryggisþætti getum við tryggt að traust sé ríkjandi um uppruna, miðlun og innihald skeytis, og þeirra skuldbindinga sem skeytið felur í sér.

Þeir öryggisþættir sem skipta mestu máli eru **áreiðanleiki í flutningi, staðfesting á uppruna og öryggi innihalds**, bæði leynd og heilleiki.

Afgreiðslutími skiptir einnig miklu máli. Afgreiðslutími er sá tími sem það tekur að koma reikningum frá sendanda til viðtakanda og hjá viðtakanda sá tími sem það tekur að koma reikningi inn til samþykktar og í greiðsluferli. Hér verður nánar lýst hvað hver þáttur felur í sér.

Eftirfarandi er umfjöllun um þá öryggisþætti sem þarf að uppfylla í rafrænum viðskiptum. Tekið er sérstakt mið af því hvernig slíkt er gert í almennu netumhverfi. Það má ná sambærilegu öryggistigi í lausnum sem útfærðar eru á annan máta en þá er yfirleitt fyrir hendi samningur milli aðila um útfærslu.

### Áreiðanleiki í flutningi (reliable messaging)

Sendandi á að geta treyst því að reikningar sem hann sendir á rafrænan máta berist til viðtakenda, en glatist ekki eða fari til rangra aðila. Það getur einnig skipt máli að reikningar berist viðtakanda í réttri röð.

Skilgreining á „Reliable messaging“ er að skeyti berast örugglega einu sinni og aðeins einu sinni, og í réttri röð þar sem röðin skiptir máli. Þetta eru mikilvægustu eiginleikar öruggs burðarlags.

Þar sem viðskiptaferlar innan og á milli fyrirtækja eru drifnir áfram af rafrænum samskiptum verður þessi skilgreining ítarlegri og nær yfir þá högun sem notuð er til að flytja boð eða skeyti milli viðskiptaferla, þar sem ferlið sjálft truflast ekki þó undirliggjandi kerfi verði fyrir truflunum meðan ferlið vinnur.

Til eru staðlar og skilgreiningar sem lýsa því hvernig koma skal slíkri högun á. Þó útfærslan sé mismunandi þá byggja allir staðlarnir á því að rafræn skjöl, reikningar eða annað séu send á áreiðanlegan máta yfir almenn fjarskiptanet eins og Internetið.

Ein leið til að koma á slíkri högun er að nota tækni sem byggir á ebMS eða ISO 15000 stöðlum. Hin leiðin er að byggja slíka högun á vefþjónustum (web services) og styðjast við skilgreiningar eins og WS-Reliability og WS-ReliableMessaging (sem byggja á ebMS[1]).

Það er okkar mat að högun sem byggir á WS-* skilgreiningum sé vænlegri kostur þar sem útbreiddur stuðningur er við þau viðmið í forritunartólum og öðrum stöðluðum hugbúnaði og því meira frelsi í vali á birgjum og samstarfsaðilum. Áreiðanlegur flutningur (reliable messaging) sem byggir á WS-Reliabilty og WS-ReliableMessaging[2] notar SOAP skeyti, með og án viðhengis, til að senda upplýsingar yfir almenn fjarskiptanet (Internetið) eftir stöðluðum óöruggum samskiptaleiðum (Transport Protocols: HTTP, SMTP, FTP).

Áreiðanlegt burðarlag (Reliable Messaging Processing layer) skal tryggja eftirfarandi:

1) Skeyti sem send eru berist milli þátttakenda (sendendur og viðtakendur) þótt þátttakendur séu ekki alltaf tengdir eða truflanir verði á undirliggjandi kerfum eða neti á meðan sending stendur yfir.

2) Gæði þjónustunnar skulu tryggja að:

   a) Hvert skeyti berist örugglega til viðtakanda og aðeins einu sinni.

   b) Skeyti berist í sömu röð og þau voru send.

   c) Sendandi og viðtakandi fá boð ef mistekst að senda eða taka við skeyti.

Það er mikilvægt að sendandi geti séð hvort skeyti hafi borist til viðtakanda og hann tekið við því. Það væri eðlilegt að burðarlag byði uppá slíka þjónustu þótt þetta sé ekki hluti af stöðlum.

### Staðfesting á uppruna og óhrekjanleiki

WSS (Web Services Security: SOAP Message Security, eða WS-Security) lýsir staðlaðri leið til að tryggja uppruna og innihald SOAP skeytis þó það fari yfir opin net. Innihald og uppruni SOAP skeytis sem varið er samkvæmt WS-Security, og viðeigandi stuðningsskilgreiningum er tryggt óháð þeirri aðferð og leið sem notuð er til að koma skeytinu frá útgefanda reiknings til viðtakanda hans.

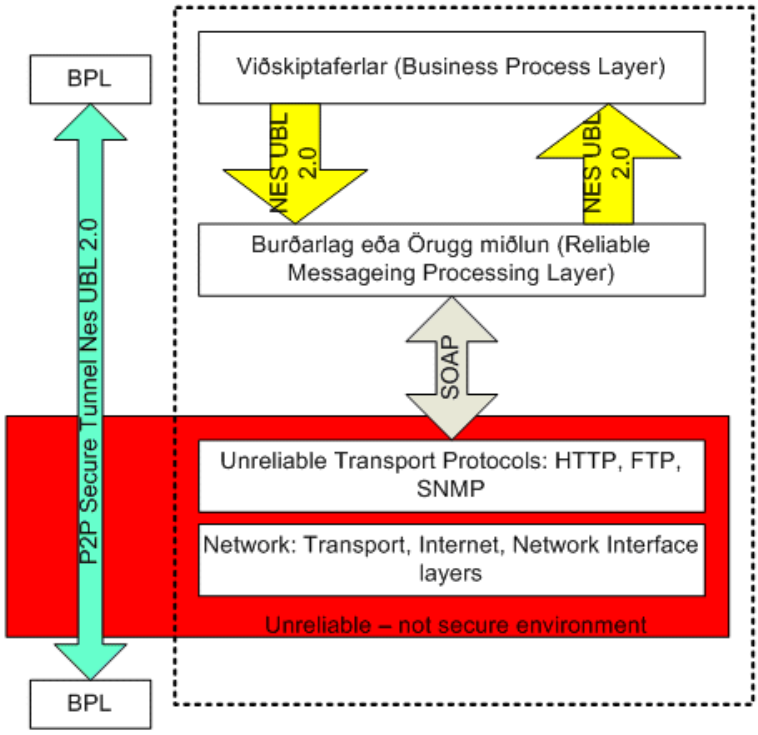
[1] WS-Reliabilty er einfaldari í innleiðingu. Það ætti að vera hægt að byrja með WS-Reliability og fara svo í WS-ReliableMessaging, þegar þörf krefur.
[2] WS-ReliableMessaging er flóknari í innleiðingu en WS-Reliability, bíður uppá meiri möguleika á sjálfvirki og dynamic breytingum og þá meiri stöðuleika og hugsað fyrir því að geta aukið afköst „on-the–fly“.

Viðtakandi verður að geta fullvissað sig um að uppruni reikninga sem honum berast sé réttur þ.e. að höfundur reiknings sé sá sem hann segist vera (Message Authentication). Þetta er gert með rafrænni undirritun skeytis (SOAP-DSIG). Til að tryggja óhrekjanleika (non-repudiation) verður að nota saman SSL og SOPA-DSIG. Mikilvægi þess að tryggja óhrekjanleika verður meira eftir því sem sjálfvirk meðhöndlun og samþykkt reikninga verður meiri.

### Öryggi innihalds

Bæði sendandi og viðtakandi hafa sameiginlega hagsmuni af að geta sannreynt að reikningur hafi borist óbrenglaður og óviðkomandi hafi ekki getað séð eða breytt honum meðan á flutningi stóð, hvort sem flutningurinn átti sér stað með milligöngu 3ja aðila eða ekki. WSS lýsir hvernig þetta er gert með dulritun og undirskrift.

Öðrum leiðum má beita til að tryggja uppruna, innihald og óhrekjanleika en lýst var hér að ofan. Það á sérstaklega við




þar sem aðilar skiptast á rafrænum reikingum í lokuðu umhverfi.

Þeir sem vilja stunda rafræn viðskipti verða að vera meðvitaðir um hvaða öryggisþættir skipta þá mestu máli og hvaða afleiðingar það getur haft ef slakað er á kröfunum.

## Flutningur viðskiptaskjala

### Miðlunaraðferð

Rafrænum skjölum er miðlað milli viðskiptaaðila samkvæmt aðferðum sem: a) eru ákveðnar af móttakanda einhliða; eða b) sendandi og móttakandi koma sér saman um að nota.

### Flutningsaðferðir

Flutningsaðferðir ráðast í mörgu af skilgreindri miðlunaraðferð milli viðskiptaaðila. Við val á flutningsaðferð ber að hafa í huga eðli viðskipta, kröfur um öryggi, gagnamagn sem senda á og einnig tengsl við aðra viðskiptaferla

Í grófum dráttum eru tvær tegundir gátta notaðar við flutning gagna, opin gátt[3] og lokuð gátt[4]. Þá er og miðað við að skjöl sem flytja á séu annaðhvort opin eða undirrituð rafrænt samkvæmt lagaákvæðum þess efnis.

[3] T.d. http, FTP, SMTP.
[4] T.d. P2P (point-to-point), X.25, X.400, https, sftp, virðisaukandi þjónusta.

Eftirfarandi tafla sýnir samspil öryggis og kostnaðar við mismunandi notkun skjala og gátta, þar sem hærri talan þýðir meira öryggi, en það gæti einnig leitt til meiri kostnaðar.

| Flutningur / skjalategund | Opin gátt | Lokuð gátt |
|---|---|---|
| **Opið skjal** | 1 | 3 |
| **Rafrænt undirritað skjal** | 2 | 4 |

## Samtenging við jaðarferla og ytri ferla

Þegar rafrænum reikningum er miðlað á milli viðskiptaaðila þarf að gera ráð fyrir tengingum við viðskiptaferla (e. business process) hjá báðum viðskiptaaðilum, og hugsanlega hjá ytri aðilum, til að nýta sjálfvirkni og tryggja skilvirkni í viðskiptunum.

### Innri skeytamiðlun

Í vissum tilfellum er þörf á að miðla skeytinu sem móttakandi hefur fengið, áfram á milli ólíkra hugbúnaðakerfa innan fyrirtækis eða á milli stofnana eða birgja. Við slíka miðlun er lagt til að notast verði við sömu grunnþætti og almennt er lagt til í þessu skjali í samskiptum viðskiptaaðila.

### Samtenging ferla og samhæfing við önnur skjöl.

Gera þarf ráð fyrir að gögnin séu endurnýtanleg. Túlkun og meðhöndlun upplýsinga er mismunandi eftir móttakendum og sendendum þar sem viðskiptahættir eru mismunandi. Því þarf að vera tryggt að engin gögn tapist í ferlinu, þ.e. burðalag má ekki raska gögnunum.

Eitt helsta markmið rafrænna lausna er að auðvelda samskipti milli aðila í viðskiptum og auðvelda þeim að deila með sér gögnum á rafrænan máta. Viðskiptaferlarnir krefjast samræmingar og staðlarnir eru mikilvægur þáttur í árangri. Viðskiptaferlin einblína á alla virðiskeðjuna, allt frá rafrænni úrvinnslu pöntunar og þjónustu við viðskiptavini, til rafræns reiknings. Staðlar stuðla að betri skilvirkni viðskiptaaðgerða (ásamt auknu öryggi gagna), t.d. fyrir rafræna vörulista, pantanir og rafræna reikninga. Aðferðir rafrænna viðskipta gera aðilum kleift að tengja innri og ytri ferli þeirra með meiri skilvirkni, að starfa nánar með birgjum og fullnægja betur þörfum og væntingum viðskiptavina sinna. Hugbúnaðarlausnir í rafrænum viðskiptum gera mögulegt að samhæfa viðskiptaferla innan fyrirtækis og milli fyrirtækja.

Umgjarðirnar í NES snúast um að staðla og tengja viðskiptaferlana. Hver umgjörð er viðskiptaferill þar sem viðskiptareglur milli aðila eru skilgreindar. Í hverjum viðskiptaferli eru stök og klasar skilgreindir í hverju skeyti. NES umgjarðirnar eru:

- Umgjörð 1: Vörulisti (catalogue only).
- Umgjörð 2: Uppfærsla vörulista (catalogue update).
- Umgjörð 3: Grunnpöntun (Basic Order).
- Umgjörð 4: Grunnreikningur (Basic Invoice).
- Umgjörð 5: Grunnreikningur með kreditnótu (Basic Billing).
- Umgjörð 6: Grunninnkaup (Basic Procurement).
- Umgjörð 7: Einföld innkaup (Simple Procurement).
- Umgjörð 8: Grunnreikningur með kreditnótu og svari.

### Virðisaukandi þjónusta

Ýmsar virðisaukandi þjónustur eru í boði:

- Þjónusta sem umvarpar innsendum reikningum á réttan staðal en það þarf að vera möguleiki að senda reikning á mismundandi formi. T.d. að senda reikninga á pappírsformi, EDI skeyti, xml, o.fl. Fyrir þau fyrirtæki sem vilja senda reikninga á EDIFACT eða á öðru formi þá er hægt að varpa þeim reikningum yfir á NES form. Einnig býðst sá möguleika að ganga frá NES reikningi á pdf formi fyrir þá sem það vilja.
- Þjónusta sem útbýr reikninga fyrir viðskiptavini og sér um að senda reikninga á NES formi.

### Önnur rafræn skjöl

Auk miðlunar rafrænna reikninga er æskilegt að boðið verði uppá miðlun ýmissa rafrænna skjala eins og úttektarbeiðnir, verðlista, tilboð, afhendingarseðla og skilagreinar.