

Krav på Fakturapresentatör

Dokumentbeskrivning:

Detta dokument innehåller krav som skall följas av aktör som presenterar fakturor samt anmälningssida, sk Fakturapresentatör (FP) i samverkan e-faktura privat. Dessa riktlinjer kan efter beslut av Arbetsutskottet ändras

Observera att Bankerna inte ansvarar för att nedan beskrivna åtgärder är tillräckliga för att förhindra angrepp, kapacitetsproblem eller andra problem.

Använda begrepp:

Presentation – Presentation via webben av faktura eller anmälningssida, inklusive funktionalitet hos dessa,

Förkortningar i dokumentet

FM	Fakturamottagare
FU	Fakturautställare
FUB	Fakturautställarbank
PB	Presentatörsbank
FP	Fakturapresentatör

Ändringshantering

<u>Datum</u>	<u>Version</u>	<u>Ansvarig</u>	<u>Beskrivning av förändring</u>
2009-10-23	1.9	Johan Schmalholz	2.11 Ny tvingande regel efter beslut i Arbetsutskott e-faktura privat. ”Visning av URL till faktura i webbläsarens adressfält (Location, directories) får inte ske på ett sådant sätt att det är möjligt att utläsa den faktiska sökvägen till en e-faktura. Location och directories får inte heller på något sätt möjliggöra obehörig åtkomst av e-faktura via manipulering av dessa.” 5.4 Ny tvingande regel efter beslut i Arbetsutskott e-faktura privat.” FP är skyldig att utan dröjsmål underrätta FUB i det fall obestånd eller väsentlig risk för obestånd föreligger.” 5.5 Ny tvingande regel efter beslut i Arbetsutskott e-faktura privat.” FP är skyldig att underrätta FUB om aktuell URL adress mot vilken presentation av fakturor sker” 5.6 Ny tvingande regel efter beslut i Arbetsutskott e-faktura privat.” FP är skyldig att underrätta FUB om aktuella kontaktuppgifter till FP avseende firma, styrelsens säte, organisationsnummer, telefonnummer och e-postadress. I det fall förändringar sker åligger det FP att utan dröjsmål underrätta FUB därom. 1.4 Beslut i verksamhetsråd för e-dokument <u>Ny text:</u> Storleken är minst 800* 600 (bredd * höjd) med följande satt till "true": toolbar, scrollbars, resizable och

			<i>status.</i>
2012-03-16	2.0	Johan Schmalholz	1.3 Beslut i verksamhetsråd för e-dokument En Fakturautställares genomsnittliga faktura får ej vara större än 1 megabyte, eventuella bilder inkluderade.
2013-04-22	2.1	Johan Schmalholz	2.12 Beslut vid extra möte i Arbetsutskotten för e-faktura 2013-04-22. Faktura som visas för en användare får inte cahas av användarens webbläsare.
2013-08-19 / 2013-09-25	2,2	Tomas Rimming/ Erik Engberg (Know IT) Johan Schmalholz	Uppdatering efter säkerhetsutredning av Know IT 2013 - Ändring av rubriker till ”Krav”, ”Skall/Bör” samt ”Beskrivning” 2.5 Nytt tvingande krav på att Nyckellängd 2013 ska vara minst 128 bitar 2.7 Nytt tvingande krav på att FP:s server skall vara säkerhetsoptimerad enligt en etablerad standard och att Samtliga portar och tjänster som ej är nödvändiga för applikationen eller driften av denna skall vara avstängda. 2.12 Integritetskontroll, exekveringskontroll eller annat bevisat effektivt skydd mot skadlig kod användas istället för klassiskt antivirus (gäller framför allt på Unix/Linux plattform). Status för samtliga krav nedan ändras efter beslut av samverkande banker från ”bör” till ”skall”. 1.1, 1,8, 2,7- 2,9, 2,11-2.12, 3,3-3,4, 4,1-4,4, 5,2-5,3

1. Tekniska krav

Krav #	(S)kall (B)ör	Beskrivning	Motovering
1	B	FP ska se till att Presentation fungerar korrekt för varje kombination av operativsystem och browser som stöds av de samverkande bankerna.	Minimikrav på tjänstekvalitet.
2	S	Fakturor skall presenteras i PDF-format eller HTML-format. Fakturor avsedda för juridiska personer skall presenteras i PDF format	Båda formaten är spridda och allmänt accepterade.
3	B	Fakturor bör presenteras i HTML-format då det ger kortare svarstid för kund.	HTML ger kortare svarstid för kund. Vissa kunder kanske inte har PDF-läsare installerad.
4	S	Presentation i HTML-format skall följa standard enligt W3C//DTD HTML 4.0.1 Transitional//EN. Det är tillåtet att använda Cascading Style Sheets, version CSS1 and CSS2, och javascript, version 1.1, version 1.2, version 1.3. FP kan för Presentation även följa senare standards under förutsättning att kontroll vid presentationstillfället görs av fakturamottagarens webbläsares versionsnummer och presentation sker enligt de standards denna stödjer.	Detta säkerställer läsbarhet i alla standard webbläsare.
5	S	Om fakturor presenteras i PDF-format skall de skapas i sådan version att faktura är tillgänglig för kund med Acrobat Reader version 5 eller senare.	Säkerställer läsbarhet i alla standard PDF-läsare.
6	S	En Fakturautställares genomsnittliga faktura får ej vara större än 1 megabyte, eventuella bilder inkluderade.	För att få korta svarstider och begränsa kapacitetsutnyttjande för kund och FP.
7	S	Presentation skall vara anpassad för browser-fönster med följande parametrar: Storleken är minst 800 * 600 (bredd * höjd) med följande satt till "true": toolbar, scrollbars, resizable och status. Location, directories ska inte visas. Övriga parametrar kan variera. I de fall FP öppnar nytt fönster på kundens PC, t.ex. vid val av PDF-faktura skall fönstret följa dessa regler. Samma regler gäller för ev. fönster som öppnas av Fakturapresentatören för t.ex. visning av PDF-faktura.	Säkerställer läsbarhet i alla standardläsare.
8	S	Kunden skall kunna verifiera att sessionen är SSL-säkrad genom att symbolen (exempelvis	Kunden kan då själv enkelt säkerställa att webbplatsen är

		lås eller nyckel) för SSL-kryptering visas i browser-fönstret	den rätta och inte en förfalskad.
--	--	---	-----------------------------------

2. Allmänna säkerhetsregler

Krav #	(S)kall (B)ör	Beskrivning	Motivering
1	S	FP skall använda programvara som uppfyller specifikationen i Referens 1 - <i>Specifikation över tekniskt gränssnitt för biljettuppackaren</i> för att kontrollera biljett.	Säkerställer kompatibilitet med bl.a. anropande bank.
2	S	Webbservrar som används för presentation av faktura eller anmälningsärende skall ha klockan tekniskt synkroniserad enligt regler för Stratum 5 eller bättre.	Förhindrar att en angripare återanvänder gamla biljetter. Dessutom behövs korrekta tidsstämplar i log vid felhantering och incidentutredning.
3	S	Systemet skall ej godkänna biljett där tidstämpeln är äldre än 180 sekunder.	Gamla biljetter skall inte kunna återanvändas.
4	S	All kommunikation med Fakturamottagare som initierats av att Fakturamottagare länkats vidare av Presentatörsbank skall vara skyddad med Https://SSL v3/TLS. Undantag från denna regel är visning av informationssidan för vilken Https: inte behöver användas.	Trafiken skyddas mot avlyssning. Äldre protokoll är inte längre säkra och kan därför ej användas.
5	S	Endast starka chiffer och långa nycklar skall användas. Nyckellängd 2013 ska vara 128 bitar eller mer.	Se motivering till krav A4.
6	S	FP:s server skall endast vara dedikerad för syftet att lagra och presentera elektroniska fakturor. (Skall ej fungera som mailserver, news osv)	Övriga tjänster ger ökad riskexponering.
7	S	FP:s server skall vara säkerhetsoptimerad enligt en etablerad standard , t.ex. tillämpliga delar av: http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf Hårdningen ska bland annat säkerställa att erforderliga säkerhetspatchar appliceras, fördefinierade standardlösenord ändras och att komponenter och tjänster som inte används tas bort. Samtliga portar och tjänster som ej är nödvändiga för applikationen eller driften av denna skall vara avstängda.	Hårdningen minskar sårbarheten för angrepp.
8	S	FP:s system skall implementeras så att obehörig åtkomst förhindras, exempelvis genom:	Åtgärderna minskar risken för lyckade angrepp och medför att angreppsförsök kan upptäckas

		☐ att ha en adekvat installerad Brandvägg ☐ att upprätthålla rutiner och verktyg för att detektera försök till angrepp	och skada förhindras.
9	S	Lösningen skall vara dokumenterad, varav säkerhetsdokumentationen skall beskriva vilka säkerhetsåtgärder som vidtagits samt varför man vidtagit dessa.	Säkerställer spårbarhet och ökar förvaltningsbarheten.
10	S	SSL-certifikat som installeras på server skall vara utfärdat av CA vars giltiga root-certifikat förutsätts vara förladdat i kundernas browser.	Kunderna kan därmed lita på att det är rätt server de kommunicerar med.
11	S	Verifikation av biljett/Identifikation av FM, skall ske i samma http-session som upprättas då FM:s faktura presenteras (Ticket Resolver bör vara tillgänglig för den server som presenterar fakturan). Eventuell vidare återidentifikation av FM (mot samma server eller om kunden genom "redirect" hamnar på annan server) skall utföras med skyddsmekanismer av motsvarande nivå som används då FM identifieras av biljetten. Det vill säga SSL-session och en kryptografiskt tillräckligt stark (i dagsläget 128 respektive 1024 bitar beroende på metod) cookie och/eller identifikationssträng.	Åtgärderna syftar till att hela kommunikationskedjan skall hålla samma säkerhetsnivå och minskar på så sätt angreppsmöjligheterna.
12	S	Systemet skall skyddas av ett för syftet väl anpassat virusskydd som skall hållas uppdaterat med de senaste virusdefinitionerna. Alternativt kan integritetskontroll, exekveringskontroll eller annat bevisat effektivt skydd mot skadlig kod användas istället för klassiskt antivirus (gäller framför allt på Unix/Linux plattform).	Minskar risken för att skadlig kod kommer in i systemet.
13	S	Visning av URL till faktura i webbläsarens adressfält (Location, directories) får inte ske på ett sådant sätt att det är möjligt att utläsa den faktiska sökvägen till en e-faktura. Location och directories får inte heller på något sätt möjliggöra obehörig åtkomst av e-faktura via manipulering av dessa.	En angripare skall ej kunna visa faktururor eller få åtkomst till annan information genom att gissa eller manipulera sökvägar.
14	B	Samtliga försök till ogiltiga URL som ej beror på fel eller gamla fakturor <i>bör</i> loggas och flaggas som angreppsförsök.	Uppmärksamhet på försök till obehörig åtkomst.
15	S	Faktura som visas för en användare får inte cachas av användarens webbläsare. För att hindra detta måste samtliga HTTP response anrop som innehåller en faktura inneha följande två HTTP headrar: Pragma: No-cache Cache-Control: no-cache, no-store	Informationen skall ej ligga kvar på kundens dator av säkerhetsskäl. Särskilt viktigt om det är en lånedator eller t.ex. internetcafé.

16	S	FP skall på begäran ge tillträde till Samverkan e-faktura Privat eller av Samverkan utsedd representant för att denne ska kunna genomföra säkerhetstester och granskning av uppfyllandet av detta regelverk.	Ger möjlighet att testa säkerhet och tillgänglighet.
----	---	--	--

3. Tillgänglighet

Krav #	(S)kall (B)ör	Beskrivning	Motivering
1	S	FP ska tillse att Presentation kan ske varje dygn mellan kl 00.00 och kl 24.00.	Garant för att FP lever upp till de krav som ställs på Presentatörsbanken i Det gemensamma regelverket.
2	S	FP ska tillse att systemet är dimensionerat och konstruerat så att driftavbrott förebyggs. Systemet ska klara höga belastningar som kan förekomma t ex i samband med månadsskiften. Fakturautställaren, eller fakturautställarens underleverantör, ska utforma sina system så att den planerade tillgängligheten under avtalade öppettider inte underskrider 96% per dygn och 99% per månad. Den faktiska tillgängligheten hos sådana system ska dock inte underskrida 96% per månad.	Garant för att FP lever upp till de krav som ställs på Presentatörsbanken i Det gemensamma regelverket.
3	S	FP skall skriftligen kunna redovisa uppnådd tillgänglighet för systemet.	Enligt avtal med FUB. Möjliggör uppföljning av T1-T2.
4	S	FP skall tillse att webservern som används för visning av fakturor övervakas utifrån, som minst övervakning utanför brandväggen.	Åtgärden gör att problem med t.ex. lastbalansering och brandväggar som kan blockera åtkomsten upptäcks.
5	S	Svarstiden vid Presentation hos FP skall inte överstiga 3 sekunder (svarstiden inkluderar inte transport av data till och från Fakturamottagaren).	Garant för att FUB ska kunna leva upp till krav enligt Det gemensamma Regelverket.
6	S	FP ska tillse att fakturor ska vara tillgängliga minst 19 månader efter det förfallodatum som är angivet för respektive faktura.	Garant för att FUB ska kunna leva upp till krav enligt Det gemensamma Regelverket.

4. Loggning och säkerhetskopiering

Krav #	(S)kall (B)ör	Beskrivning	Motivering
1	S	FP ansvarar för att tillräckliga loggar finns så att händelseförlopp kan följas vid exempelvis felutredningar. Det innebär att klockslag och all information som mottagits från kundens biljett skall lagras på ett sådant sätt att det kan återfinnas minst tre månader bakåt i tiden.	Loggarna behövs för att förenkla/möjliggöra incidentutredning.
2	S	FP:s system skall vara robust konstruerat så	Systemet innehåller värdefull

Samverkan e-faktura privat

Utarbetat av/direkt telefon

”Förvaltningsansvarig”

Upphovsman

Område

6. Kvalitetshöjande åtgärder

Dokumenttyp

Driftshandbok

Avsnitt

Externt dokument

		att information inte tappas bort.	information som inte får gå förlorad.
3	S	FP ansvarar för att all information i Systemet säkerhetskopieras kontinuerligt så att förlust av information förhindras.	Se L2
4	S	FP skall också ha dokumenterade rutiner för att återskapa Systemet från säkerhetskopia.	Se L2

Godkännes av/signatur

Dokument-id

Version

2.2

Datum

2013-09-25

Flik

5

Sida

7 (8)

5. Övriga krav

Krav #	(S)kall (B)ör	Beskrivning	Motivering
1	S	I de fall även annan information än fakturan eller anmälningssida presenteras för Fakturamottagare, skall fakturan eller anmälningssida vara det första som presenteras.	Krav på Fakturautställarbank enligt Det gemensamma Regelverket.
2	S	FP skall utöver vad som tidigare beskrivits upprätthålla skriftligt dokumenterade beskrivningar av: • Implementerad systemdesign • Arbetsrutiner för kundtjänst och upprätthållande av kompetens hos kundtjänst • Rutin för löpande drift och systemförvaltning • Dokumenterade rutiner för regelbunden hantering av/genomgång av säkerhetsoptimering , patchar FW-konfiguration	Säkerställer kvalitet, spårbarhet och ökar förvaltningsbarheten.
3	S	Innan produktionssättning av nytt eller förändrat system skall FP genomföra erforderliga tester av hela systemet. Dessa tester skall säkerställa att funktionalitet och säkerhet följer de krav som deltagarna i samverkan ställer. Speciellt skall FP testa att simultana anrop från FM aldrig resulterar i att fakturor visas för fel FM. Testerna skall dokumenteras i testrapport omfattandes minst kortfattad beskrivning av genomförda testfall, upptäckta fel och kvarvarande fel.	Säkerställer kvalitet, spårbarhet och ökar förvaltningsbarheten.
4	S	FP är skyldig att utan dröjsmål underrätta FUB i det fall obestånd eller väsentlig risk för obestånd föreligger.	e-faktura -samarbetet involverar många olika parter där alla är beroende av varandra för att tjänsterna ska fungera väl..
5	S	FP är skyldig att underrätta FUB om aktuell URL adress mot vilken presentation av fakturor sker	I annat fall kan ingen fakturavisning ske.
6	S	FP är skyldig att underrätta FUB om aktuella kontaktuppgifter till FP avseende firma, styrelsens säte, organisationsnummer, telefonnummer och e-postadress. I det fall förändringar sker åligger det FP att utan dröjsmål underrätta FUB därom.	Möjliggör snabba kontaktvägar vid driftstörningar samt uppmärksammar FUB om organisatoriska förändringar.