Regeringens skrivelse 2011/12:91

Stärkt säkerhet i statens betalningar

Skr. 2011/12:91

Regeringen överlämnar denna skrivelse till riksdagen.

Stockholm den 22 mars 2012

Fredrik Reinfeldt

Anders Borg
(Finansdepartementet)

Skrivelsens huvudsakliga innehåll

I skrivelsen redovisar regeringen åtgärder som vidtagits de senaste åren för att förbättra säkerheten i statens betalningar.

Riksdagen tillkännagav i betänkandet 2010/11:FiU22, rskr. 2010/11:167 att regeringen bör återkomma till riksdagen under första kvartalet 2012 med en redovisning av vilka åtgärder som vidtagits för att förbättra säkerheten i statens betalningar.

Statens betalningsmodell är en samlad benämning på de regelverk, avtal, kontostrukturer och system som stöder myndigheternas betalningar. Huvudaktörer i modellen är Riksgäldskontoret, ramavtalsbankerna och myndigheterna. Statens betalningsmodell utvecklas löpande i fråga om funktionalitet och säkerhet. Bland de viktigare åtgärder som vidtagits de senaste åren för att öka säkerheten i statens betalningar kan nämnas följande.

- En årlig process i syfte att få en tydligare bild av de samlade riskerna i statens betalningsmodell har inrättats fr.o.m. 2012. Riksgäldskontoret har tilldelats ansvaret för att göra en sammanställning av riskerna. På begäran ska myndigheterna lämna uppgifter till Riksgäldskontoret. Senast den 1 november varje år ska Riksgäldskontoret lämna en redogörelse till regeringen avseende de samlade riskerna i den statliga betalningsmodellen.
- Myndigheternas ansvar för säkerheten i sina betalningar har förtydligats i förordningen (2006:1097) om statliga myndigheters betalningar och medelsförvaltning samt i anslutande föreskrifter och allmänna råd. En myndighet ska analysera de risker som är förknippade med myndighetens betalningar.
- Säkerhetskraven har höjts i ramavtalen för betaltjänster. De ramavtal som trädde i kraft den 1 april 2011 innehåller bl.a. funktionalitet för

beloppsgränser för utbetalningar från myndigheternas bankkonton hos samtliga ramavtalsbanker. Avtalen innehåller även utökade möjligheter för myndigheter med omfattande eller kritiska samhällsbetalningar att avropa reservrutiner.

- Regeringskansliet har gett en sakkunnig person i uppdrag att se över frågor och regelverk kring identifikation av behöriga företrädare för myndigheter. Uppdraget ska redovisas senast den 31 mars 2012.

Ansvarsförhållandena när det gäller säkerheten i betalningsmodellen är i grunden oförändrade. Det är således även fortsättningsvis myndighetens eget ansvar att kontrollera att samtliga utbetalningar görs till rätt mottagare, med rätt belopp och vid rätt tidpunkt.

Innehållsförteckning

Enligt riksdagens tillkännagivande bör regeringen under första kvartalet 2012 återkomma till riksdagen med en redovisning av vilka åtgärder som vidtagits för att förbättra säkerheten i statens betalningar (bet. 2010/11:FiU22). Frågan behandlades av riksdagen med anledning av Riksrevisionens styrelses framställning om statens betalningar (2010/11:RRS5). Till grund för framställningen låg Riksrevisionens granskning av säkerheten i statens betalningar. Granskningen publicerades den 10 juni 2010 i rapporten Säkerheten i statens betalningar (RiR 2010:13). Föremål för granskningen var regeringen, Kammarkollegiet, Ekonomistyrningsverket och 20 andra myndigheter.

Stärkt krisberedskap i det centrala betalningssystemet

Riksrevisionens fördjupade granskning av säkerheten i statens betalningar har sin bakgrund i rapporten Krisberedskap i betalningssystemet (RiR 2007:28) från december 2007. I rapporten gjordes en bred genomlysning av krisberedskapen i betalningssystemet där det statliga betalningssystemet utgör en delmängd. I rapporten riktades kritik mot regeringen för att den inte skaffat en samlad bild av hot, sårbarheter och konsekvenser av omfattande tekniska störningar i betalningssystemet och att den inte beslutat om vilken myndighet som ska ha det övergripande krisberedskapsansvaret. Riksrevisionen rekommenderade också regeringen att fastställa vilka grundläggande krav på uthållighet och säkerhet som betalningssystemet måste klara. I regleringsbrevet för 2008 gavs Finansinspektionen i uppdrag att redovisa vidtagna och planerade insatser med anledning av Riksrevisionens rapport, medan Riksgäldskontoret i sitt regleringsbrev för samma år fick i uppdrag att lämna en rapport avseende risker i den statliga betalningsmodellen. Under våren 2008 avlämnades myndigheternas rapporter innehållande analyser, förslag och planer på området (Fi2008/2943 och Fi2008/3727). I mars 2010 påbörjades inom Regeringskansliet ett arbete med att utreda hur statens förmåga att hantera allvarliga kriser i betalningssystemet kan stärkas. Arbetet slutfördes i december 2010 och rapporten En samlad reglering för stärkt krisberedskap mot allvarliga tekniska fel och störningar i det centrala betalningssystemet (Fi2010/1619) togs fram. Rapporten remissbehandlades (Fi2010/5860).

Stärkt säkerhet i statens betalningar

Mot bakgrund av Riksrevisionens iakttagelser i rapporten RiR 2010:13 gav regeringen den 8 juli 2010 Riksgäldskontoret, Ekonomistyrningsverket och Kammarkollegiet i uppdrag att redogöra för vilka åtgärder respektive myndighet kommer att vidta utifrån de redovisade iakttagelserna i rapporten. Av uppdraget till de tre myndigheterna framgick att en delrapport respektive en slutrapport skulle lämnas under hösten 2010. För att uppmärksamma myndigheterna på Riksrevisionens iakttagelser skickades rapporten till samtliga myndighetschefer tillsammans med ett brev från dåvarande kommun- och finansmarknadsministern. I brevet förtydligades att varje myndighet själv

ansvarar för säkerheten i den egna verksamheten samt att detta även avser myndighetens betalningar.

I 2011 års regleringsbrev gav regeringen Riksgäldskontoret i uppdrag att lämna förslag på reglering av insamling av riskanalyser från de statliga myndigheterna. Förslaget skulle lämnas till regeringen senast den 15 juni 2011. I regleringsbrevet gavs Riksgäldskontoret även i uppdrag att analysera riskerna och sårbarheten i den statliga betalningsmodellen under 2011. I uppdraget ingick även att genomföra utbildnings- och informationsinsatser kring säkerheten i den statliga betalningsmodellen. Riksgäldskontorets rapport om risker och sårbarheter i den statliga betalningsmodellen 2011 inkom till regeringen i november 2011.

1 Den statliga betalningsmodellen

1.1 Definition och mål

Den statliga betalningsmodellen är en samlad benämning på de regelverk, avtal, kontostrukturer och system som stöder myndigheternas betalningar. Modellen omfattar också den centrala likviditetshanteringen som är konstruerad för att samla likviditeten från alla in- och utbetalningar till och från staten på ett ställe – statens centralkonto i Riksbanken. Huvudaktörer i modellen är Riksgäldskontoret, ramavtalsbankerna och myndigheterna.

De statliga betalningarna förmedlas via det svenska betalningssystemet, och därmed utgör betalningsmodellen en viktig del i det svenska betalningssystemet. Betalningssystemet ägs och förvaltas av banksektorn, inklusive Riksbanken. Enligt förordningen (2007:1447) med instruktion för Riksgäldskontoret är en av myndighetens huvuduppgifter att ansvara den statliga betalningsmodellen inklusive statens centralkonto.

Av Riksgäldskontorets regleringsbrev framgår att ett övergripande mål för Riksgäldskontoret – när det gäller den statliga betalningsmodellen – är att tillgodose statsmakternas uttalade krav på kostnadseffektivitet, säkerhet, information och valfrihet. Vidare ska staten ha en konkurrensneutral relation till bankerna.

1.2 Betalningsförordningen styr myndigheterna

Statliga betalningar regleras i förordningen (2006:1097) om statliga myndigheters betalningar och medelsförvaltning (betalningsförordningen). Förordningen innehåller regler om statens centralkonto samt om myndigheters bankkonton, betalningar, medelsförvaltning och valutasäkring. Riksgäldskontoret meddelar verkställighetsföreskrifter och allmänna råd till förordningen.

1.3 Ramavtalen styr bankerna

För att uppnå effektivitet och konkurrensneutralitet upphandlar Riksgäldskontoret ramavtal, med svenska och utländska banker och kortleverantörer, för kort- och betaltjänster på marknaden. Det möjliggör för staten och myndigheterna att använda befintlig struktur i det svenska betalningssystemet och skapar bra betalningsmöjligheter för myndigheterna.

I ramavtalen ingår infrastruktur och betaltjänster. Infrastrukturen omfattar koncernkontostruktur och bankkonton, kommunikation, återrapportering och internetbank. Exempel på betaltjänster är kontoinsättning, girering, utlandstjänster, internetbetalningar och kortbetalningar. Merparten av dessa tjänster är standardiserade och används av både företag och myndigheter. Myndigheterna utnyttjar bankernas betalningslösningar, inklusive tjänster från bankernas underleverantörer som t.ex. Bankgirocentralen (BGC). Myndigheterna är enligt betalningsförordningen skyldiga att avropa betalningstjänster enligt ramavtalen såvida Riksgäldskontoret inte medgivit annat. Myndigheterna är också skyldiga att följa Riksgäldskontorets rangordning av tjänsterna.

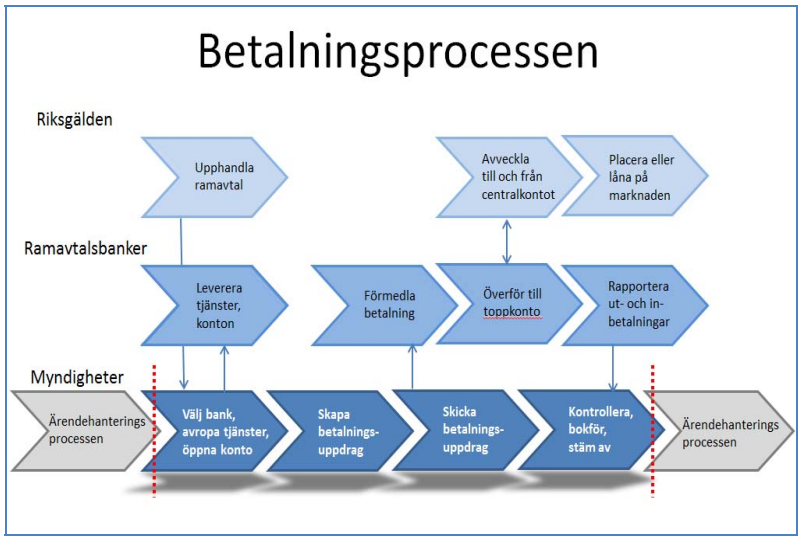
1.4 Likviditetsstyrningen är centraliserad

För att reducera statens räntekostnader och risk är den statliga betalningsmodellen konstruerad för att samla likviditeten från alla in- och utbetalningar till och från staten på ett ställe, statens centralkonto i Riksbanken. Statens centralkonto i Riksbanken förs i svenska kronor. Det innebär att myndigheterna måste växla alla in- och utflöden i annan valuta än svenska kronor. Växlingen görs till spotkurs i den ramavtalsbank som förmedlar betalningen. För att myndigheterna ska kunna säkra sina valutaflöden erbjuder Riksgäldskontoret valutaterminer. Myndigheterna kan enligt regeringsbeslut förvalta likviditet i svenska kronor eller annan valuta utanför centralkontot. Exempel på betalningar som går utanför statens centralkonto är fondmedel, deponerade medel, donationer, EU-medel som ligger utanför statsbudgeten och andra bidrag i svenska kronor och annan valuta. Merparten av de statliga betalningarna omfattas av ramavtalen, men det finns ett fåtal separatavtal och en mindre andel bankkonton som inte omfattas.

1.5 Myndigheternas betalningsprocesser

Myndigheterna ansvarar för att avropa betaltjänster från ramavtal, öppna, ändra och avsluta bankkonton, samt för att hantera eventuella kvarstående saldon som inte töms till centralkontot. Myndigheterna ansvarar också för att betalningar från deras bankkonton görs i rätt tid, till rätt mottagare och med rätt belopp. Vidare ska myndigheterna tillämpa betalningsförordningen och verkställighetsföreskrifterna till den förordningen samt ansvara för en god intern styrning och kontroll av sin betalningsverksamhet.

Myndigheternas betalningar är av olika slag, exempelvis samhällsbetalningar, löneutbetalningar och fakturabetalningar. En övergripande beskrivning av statens betalningsprocess, med huvudaktörerna Riksgäldskontoret (Riksgälden), ramavtalsbankerna och myndigheterna finns illustrerad nedan. Fokus i bilden ligger på myndigheternas del i processen.



Bilden visar att Riksgäldskontoret upphandlar ramavtal, hanterar betalningar över centralkontot och placerar och lånar likviditet på marknaden. Ramavtalsbankerna levererar betaltjänster och förmedlar betalningar. Myndigheternas betalningsprocess börjar med avrop av tjänster och öppnande av bankkonton. Myndigheterna har interna system som skapar betalningsuppdrag.

Betalningsprocessen innebär att när betalningsunderlaget har godkänts och attesterats, skapas ett betalningsuppdrag som godkänns (bemyndigas) och skickas till banken. Betalningsuppdraget bemyndigas av behörig person på myndigheten, så att banken kan förmedla betalningen till mottagaren. Betalning utförs och myndigheternas bankkonton belastas. Banken återrapporterar information om utförda utbetalningar till myndigheten. Myndigheterna gör avstämning utifrån återrapporteringen från ramavtalsbankerna. Informationen används vidare i ärendehanteringsprocessen.

Betalningsprocessen innefattar också att myndigheten tar emot inbetalning av till exempel skatt, avgift eller återbetalning. Myndigheten tar också emot information om inbetalningen. För de allra flesta inbetalningar ska informationen användas i ärendehanteringsprocessen. Viktigt att notera är att det finns en skillnad mellan myndighetens ärendehanteringsprocess och betalningsprocess. Exempel på ärendehanteringsprocess kan vara hantering och godkännande av faktura, hantering av löneärende, registrering och godkännande av pensionsärende, hantering och godkännande av låne-, ersättnings- eller bidragsärende. Först när ärendehanteringen är avslutad, genom att en

handläggare på myndigheten godkänt att en utbetalning ska utföras, vidtar betalningsprocessen.

2 Riksrevisionens iakttagelser

I Riksrevisionens styrelses framställning om statens betalningar (2010/11:RRS5) görs bedömningen att den särskilt allvarliga risk och sårbarhet i den statliga betalningsprocessen som påvisades i Riksrevisionens rapport RiR 2007:28 kvarstår.

Syftet med granskningen i rapporten RiR 2010:13 var att komplettera den tidigare granskningen samt att följa upp vilka åtgärder som regeringen och myndigheterna har vidtagit och bedöma om de är tillräckliga. Följande revisionsfråga ställdes:
Är de åtgärder regeringen och myndigheterna hitintills vidtagit tillräckliga för att allvarliga felaktigheter i och ett brottsligt utnyttjande av statliga betalningar ska kunna förhindras eller hanteras om de inträffar?

De iakttagelser som Riksrevisionen har gjort avser bl.a. oklarheter kring fördelningen av ansvar för säkerheten i statens betalningar. Avsaknaden av samlade riskanalyser samt oklarheter kring vilka som ska göra sådana riskanalyser lyfts också fram. Riksrevisionen har även iakttagit ett antal grundläggande brister i rutiner och regler för den interna kontrollen och säkerheten inom myndigheterna.

3 Regeringens åtgärder

Det pågår ett löpande utvecklingsarbete när det gäller såväl säkerhet som funktionalitet i den statliga betalningsmodellen. I detta avsnitt redovisas de åtgärder som regeringen de senaste åren vidtagit för att öka säkerheten i statens betalningar. Redovisningen utgår från Riksrevisionens rapport RiR 2010:13. Som framgår av redovisningen är åtgärder vidtagna eller påbörjade i samtliga fall.

3.1 Sammanställd bild av risken i statens betalningar samt utpekat ansvar för sammanställningen[1]

Regeringen har fr.o.m. 2012 infört en årlig process med syftet att få en tydligare bild av de samlade riskerna i den statliga betalningsmodellen. Riksgäldskontoret har tilldelats ansvaret för att göra en sammanställning av riskerna. Enligt förordningen med instruktion för Riksgäldskontoret ska myndigheten senast den 1 november varje år lämna en redogörelse

[1] Riksrevisionens rekommendation var att regeringen skyndsamt och tydligt bör uttala huruvida Riksgäldskontoret eller någon annan myndighet ska ha ansvar för det statliga betalningssystemet, och att detta ansvar inkludera att ställa samman den samlade riskbilden på området samt utbildnings-, informations- och uppföljningsinsatser.

för de samlade riskerna i den statliga betalningsmodellen till regeringen. Av instruktionen framgår att Riksgäldskontoret ansvarar för den statliga betalningsmodellen inklusive statens centralkonto. Enligt en ändring av betalningsförordningen som träder i kraft den 1 april 2012 ska vidare samtliga myndigheter analysera de risker som är förknippade med myndighetens betalningar samt på begäran lämna uppgifter till Riksgäldskontoret om myndighetens betalningsverksamhet. Riksgäldskontoret har arbetat fram ett metodstöd till myndigheterna innehållande ett frågeformulär om myndigheternas betalningsverksamhet (se även avsnitt 3.3). Med hjälp av frågeformuläret ska Riksgäldskontoret kunna identifiera risker inom områdena teknik, personal, verksamhet, externa risker och kontinuitet. För att kunna samla in uppgifterna på ett säkert och effektivt sätt har samarbete inletts med Myndigheten för samhällsskydd och beredskap.

När riskerna och hoten är identifierade kommer Riksgäldskontoret att ta fram en sammanställning av åtgärder. Både åtgärder som har vidtagits och åtgärder som ska vidtas kommer att redovisas i den rapport som Riksgäldskontoret ska lämna till regeringen senast den 1 november varje år. De åtgärder som Riksgäldskontoret kan vidta för att förbättra säkerheten i betalningsmodellen är i första hand:

- ge förslag på ändringar i betalningsförordningen och meddela verkställighetsföreskrifter och allmänna råd,
- utreda och lämna förslag till regeringen på områden som behöver utredas,
- ändra och utveckla ramavtalen och
- informera, utbilda samt ge råd och stöd till myndigheterna.

För att redan under 2011 inhämta en samlad bild av riskerna på området gavs Riksgäldskontoret i regleringsbrevet för 2011 i uppdrag att analysera riskerna och sårbarheterna i den statliga betalningsmodellen samt att rapportera detta till regeringen senast den 15 november 2011. Riksgäldskontorets rapport utgör underlagsmaterial till denna skrivelse. I regleringsbrevsuppdraget ingick även att Riksgäldskontoret skulle genomföra utbildnings- och informationsinsatser kring säkerheten i den statliga betalningsmodellen. Riksgäldskontorets informationsinsatser redovisas i avsnitt 3.2 och 4.4.

3.2 Beloppsgränser för myndigheternas betalningar[2]

De ramavtal som började gälla den 1 april 2011 innehåller funktionalitet för beloppsgränser (limiter) på myndigheternas bankkonton hos samtliga ramavtalsbanker. I Riksgäldskontorets allmänna råd till betalningsförordningen anges att myndigheterna bör använda sig av beloppsgräns för sina utbetalningar. Riksgäldskontoret har även utformat riktlinjer för hur myndigheterna ska tillämpa beloppsgränserna, som ett stöd för myndigheterna i deras arbete med att införa sådana gränser på sina bank-

[2] Riksrevisionens rekommendation var att regeringen skyndsamt bör se till att en övre beloppsgräns sätts för myndigheternas betalningar, och att säkerställa att beloppsgränserna används av myndigheterna.

konton. Riktlinjerna har publicerats på Riksgäldskontorets webbplats. Vidare har Riksgäldskontoret vid utbildningar och andra möten med myndigheterna behandlat frågan om beloppsgränser. I november 2011 hade närmare 80 av myndigheterna börjat använda beloppsgränser och fler är på gång. Riksgäldskontoret kommer att följa upp myndigheternas arbete med beloppsgränser i de riskanalyser som ska samlas in från myndigheterna under 2012.

Skälet till att införandet av beloppsgränser görs successivt är att begränsa risken för att samhällsbetalningar eller löneutbetalningar stoppas på grund av att beloppsgränsen sätts för lågt. Genom att informera, ge myndigheterna stöd och sedan följa upp ges förutsättningar för att införandet och användningen av beloppsgränser sker på ett ändamålsenligt sätt.

3.3 Myndigheterna ska analysera väsentliga risker[3]

Regeringen har beslutat om en ändring i betalningsförordningen som innebär att myndigheterna ska analysera de risker som är förknippade med myndighetens betalningar. Analysen ska utföras i syfte att öka säkerheten i statens betalningsmodell. Ändringen träder i kraft den 1 april 2012. Den 6 mars 2012 skickade Riksgäldskontoret ut en första enkätundersökning till myndigheterna om deras betalningsverksamhet. Myndigheterna ska lämna svaren till Riksgäldskontoret senast den 2 maj 2012. Riksgäldskontorets redogörelse för de samlade riskerna i den statliga betalningsmodellen ska lämnas till regeringen senast den 1 november varje år. För närvarande arbetar Riksgäldskontoret även med att se över om ändringen i betalningsförordningen medför några tillägg i anslutande verkställighetsföreskrifter och allmänna råd.

3.4 Rutiner och regelverk för behöriga företrädare för myndigheterna[4]

Regeringskansliet har gett en sakkunnig person i uppdrag att se över frågor och regelverk kring identifikation av behöriga företrädare för myndigheter. Uppdraget ska redovisas senast den 31 mars 2012. I utredningen övervägs möjligheten att skapa ett register över behöriga myndighetsföreträdare. Regeringskansliet kommer skyndsamt att arbeta vidare med frågeställningen efter det att utredaren lämnat sitt förslag.

I avvaktan på utredarens förslag och regeringens beslut i frågan har Riksgäldskontoret i verkställighetsföreskrifterna till betalningsförordningen angett att myndigheten ska lämna uppgift till banken om vem

[3] Riksrevisionens rekommendation var att regeringen skyndsamt bör föreskriva att myndigheterna analyserar väsentliga risker och sårbarheter i de egna betalningsprocesserna samt vidtar åtgärder för att hantera identifierade risker.

[4] Riksrevisionens rekommendation var att regeringen skyndsamt bör ta ställning till den skrivelse med förslag om regelverk och rutiner för firmateckning och fullmaktshantering hos myndigheterna som Riksgäldskontoret inom kort avser att skicka till regeringen.

eller vilka som har behörighet att företräda myndigheten gentemot banken att öppna och avsluta bankkonto, betala från bankkonto m.m.

4 Riksgäldskontorets åtgärder

I detta avsnitt redovisas Riksgäldskontorets åtgärder för att öka säkerheten i statens betalningar utifrån Riksrevisionens iakttagelser i rapporten RiR 2010:13. Som framgår av redovisningen är åtgärder vidtagna eller övervägda i samtliga avseenden.

4.1 Skilda säkerhetskrav för olika kategorier av betalningar[5]

Riksgäldskontoret har övervägt behovet av att differentiera säkerhetskraven för olika betalningskategorier. Bedömningen är att säkerheten ska vara den högsta möjliga oavsett betalningskategori (små eller stora betalningar).

I de senaste ramavtalen för betaltjänster har kraven höjts på säkerhet för teknik, kommunikation och tjänster. Förbättringar avser bl.a. säkerhets- och tillgänglighetskrav, bättre skydd för känslig kommunikation och strängare regler för kontokopplingar till statens centralkonto. På utbetalningsområdet har även säkerheten höjts bl.a. genom att Riksgäldskontoret tagit bort kuverttjänster ur ramavtalen. Därmed har risken upphört för att utbetalningsuppdrag, som tidigare försändes i vanlig post, kommer obehöriga tillhanda.

4.2 Återredovisade filer av genomförda betalningar[6]

Tjänsten avseende skyddade (sigillerade och krypterade) återredovisade filer av genomförda betalningar finns med i de ramavtal som trädde i kraft den 1 april 2011. Riksgäldskontoret ställer krav på myndigheterna och ramavtalsbankerna att förändringsskydda filer för att undvika manipulation av betalningsuppdrag. För att undvika att angripare kommer över och utnyttjar dubblerade myndighets- eller bank-inloggningsuppgifter via Internet, ställs också krav på stängd sessionshantering.

I Riksgäldskontorets allmänna råd till betalningsförordningen framgår att e-post innehållande känslig information mellan myndighet och bank bör vara krypterad.

[5] Riksrevisionens rekommendation var att Riksgäldskontoret i kommande ramavtal bör överväga att skilja på olika kategorier betalningar vid formulering av kraven på säkerhet, så att bankerna kan erbjuda säkerhetslösningar anpassade för respektive betalningskategori.
[6] Riksrevisionens rekommendation var att Riksgäldskontoret i samråd med myndigheterna, bankerna och leverantörerna av ekonomi- och affärssystem bör skapa möjligheter att skydda återredovisade filer med genomförda betalningar.

4.3 Meddela föreskrifter om tydliga krav för säkra betalningar[7]

Den 1 maj 2011 trädde en rad ändringar i betalningsförordningen i kraft. Samtidigt trädde även ändringar i Riksgäldskontorets verkställighetsföreskrifter och allmänna råd till betalningsförordningen i kraft. Ändringarna i förordningen utgjordes till största del av förtydliganden, medan ändringarna i verkställighetsföreskrifterna och de allmänna råden syftade till att öka medvetenheten kring säkerheten i de statliga betalningarna. Ändringarna i verkställighetsföreskrifterna och de allmänna råden sammanfattas nedan.

- En myndighet ska lämna uppgift till banken om vem eller vilka som har behörighet att företräda myndigheten gentemot banken, t.ex. i ärenden som att öppna eller avsluta bankkonto och betala från bankkonto.
- En myndighet med omfattande eller kritiska samhällsbetalningar ska identifiera, avropa och dokumentera reservrutiner för sina affärssystem eller interna system som genererar betalningsuppdrag, kommunikationstjänster till och från banker och betaltjänster i ramavtalsbanker.
- En myndighets kommunikation av betalningsinformation ska ske på ett säkert sätt. Informationen ska vara förändringsskyddad (skyddad mot förvanskning). Av de allmänna råden framgår att informationen bör vara insynsskyddad (krypterad) och att mejlkommunikationen med banken bör krypteras. Det är av största vikt att betalningsinformationen inte kan förvanskas medan det endast finns behov av att kryptera hemlig information.
- En myndighet ska hantera lösenord och utrustning som används för signering av betalningar på ett säkert sätt.
- En myndighet bör använda sig av beloppsgränser (limiter) för utbetalningar.
- En myndighet som har behov av separatavtal om banktjänster ska ansöka om tillstånd för detta hos Riksgäldskontoret.
- För att understryka att valutakonton ska ligga i ramavtalsbankerna har Riksgäldskontoret även meddelat verkställighetsföreskrifter om detta.

4.4 Ökad information om risker för brott i de statliga betalningarna[8]

Riksgäldskontoret arbetar aktivt för att ge myndigheterna relevant information och för att hålla behovsanpassade utbildningar. För att minska risken för att det blir fel på grund av betalningsmodellens

[7] Riksrevisionens rekommendation var att Riksgäldskontoret bör utnyttja sin rätt att meddela föreskrifter och tydliggöra kraven på myndigheterna för att få till stånd säkra statliga betalningar.

[8] Riksrevisionens rekommendation var att Riksgäldskontoret i samarbete med andra expertmyndigheter och i ökad grad bör informera övriga myndigheter om de risker för brott m.m. som finns i de statliga betalningarna.

komplexitet, har Riksgäldskontoret tagit fram ett utbildningsmaterial och genomfört ett antal utbildningstillfällen för myndigheterna. Materialet har tagits fram efter dialog med myndigheterna samt med beaktande av synpunkter som lämnats vid årliga kundundersökningar. Vid de informationstillfällen som hölls för myndigheterna inför ramavtalen som trädde i kraft den 1 april 2011 beskrevs vad myndigheten kan göra för att öka säkerheten i betalningsprocesserna. Sammantaget deltog 140 personer från 80 myndigheter vid nämnda informationstillfällen. Riksrevisionens iakttagelser och rekommendationer har också diskuterats vid de möten med referensgruppen för betalningsfrågor som Riksgäldskontoret sammankallar två till tre gånger per år. I referensgruppen ingår representanter från ett tjugotal myndigheter. De myndigheter som har den mest omfattande betalningsverksamheten har samtliga representanter i gruppen.

Syftet med informationen har varit att öka förståelsen för hur betalningsmodellen fungerar samt hur myndigheterna i sin betalningsverksamhet kan påverka säkerheten i modellen. Det har också varit ett sätt att informera och förankra det nya uppdraget, att säkerställa att riskerna i myndigheternas betalningsprocesser kommer med i den samlade analys som Riksgäldskontoret ska göra av betalningsmodellen.

Riksgäldskontoret har även vid ett flertal andra tillfällen utbildat och informerat myndigheterna om betalningsmodellen, säkerhet och riskanalys. Det har bl.a. skett på Riksgäldens Finansdag, Ekonomistyrningsverkets (ESV) grundkurs i statlig redovisning, finansiering och styrning för nya ekonomer i staten samt på Riksrevisionens utbildning i grundläggande statlig redovisning och ekonomistyrning för nya revisorer i staten. Riksgäldskontorets förhoppning är att det metodstöd som ska skickas till myndigheterna under våren 2012 (inför sammanställningen av de samlade riskerna i den statliga betalningsmodellen) kommer att leda till en ökad säkerhetsmedvetenhet inom betalningsmodellen. Eftersom myndigheterna kommer att få återkoppling på de riskanalyser som de lämnat till Riksgäldskontoret skapas även en för ändamålet effektiv informationskanal. Utöver nämnda informationsarbete medverkar Riksgäldskontoret även i FSPOS (Finansiella Sektorns Privat–Offentliga Samverkansgrupp) som är ett samverkansforum mellan banker, försäkringsbolag och myndigheter med syfte att stärka stabiliteten i finanssektorn lokalt, regionalt och nationellt.

4.5 Möjligheten till faxbetalningar har tagits bort[9]

Riksgäldskontoret har tagit bort möjligheten att skicka direktbetalningar över statens centralkonto via faxuppdrag. I stället registrerar myndigheterna dessa betalningsuppdrag med e-legitimation.

[9] Riksrevisionens rekommendation var att Riksgäldskontoret bör ta bort möjligheterna till faxbetalningar, alternativt komplettera denna rutin med andra kontrollåtgärder.

5 Kammarkollegiets åtgärder

5.1 Riskanalyser och införande av säkrare lösningar för bemyndigande[10]

Kammarkollegiet har bedrivit ett särskilt riskanalysarbete kring betalningsrutinerna. Inför verksamhetsplaneringen för 2011 och de nya ramavtalen för betaltjänster har Kammarkollegiet arbetat med Riksgäldskontoret, ramavtalsbanker och Agresso AB för att uppnå de högre säkerhetskraven som de nya ramavtalen ställer. I övrigt har åtgärder vidtagits för att svara upp mot rekommendationer som Riksrevisionen lyft fram i sin rapport. Kammarkollegiet har bl.a. ändrat rutinerna gällande bemyndigande av betalningar. Sedan i december 2010 används ett program avseende bemyndigande för två i förening.

6 Ekonomistyrningsverkets åtgärder

6.1 Möjligheten att granska ekonomisystem [11]

I det avtal om drift av ekonomisystem som slutits mellan svenska myndigheter och affärssystemsleverantören Agresso AB saknas en klausul som tillåter Riksrevisionen att granska de system som används av myndigheterna, men som underhålls, förvaltas och körs av Agresso AB. Det är Ekonomistyrningsverket (ESV) som för statens räkning tecknar avtal med Agresso. Alla myndigheter använder dock inte Agresso.

ESV bedömer att det inte finns möjlighet att ändra villkoren i ESV:s redan ingångna och avslutade uppdragsavtal med Agresso AB. I den upphandling av ekonomisystem som nu pågår har ESV ställt krav som säkerställer att de behov gällande revision som Riksrevisionen framfört, kan uppfyllas. De nya ramavtalen är tänkta att träda i kraft vid årsskiftet 2012/13.

[10] Riksrevisionens rekommendation var att Kammarkollegiet bör göra en omfattande riskanalys av betalningsrutinerna och rutinerna för bemyndiganden och vidta nödvändiga förbättringar av säkerheten och den interna kontrollen inom myndigheten. I samband med detta bör Kammarkollegiet tillsammans med bankerna överväga att införa de nya säkrare lösningarna för bemyndigande av flera av myndigheternas betalningar som Riksgäldskontoret ställt krav på att bankerna ska kunna leverera från och med april 2011.

[11] Riksrevisionens rekommendation var att Ekonomistyrningsverket bör se till att en bestämmelse ingår i avtalet med Agresso AB som tillåter revision av system hos driftsleverantören.

7 Övriga myndigheters åtgärder

7.1 Myndigheterna bör utnyttja beloppsbegränsningar[12]

Samtliga ramavtalsbanker erbjuder myndigheterna sedan den 1 april 2011 funktionalitet för beloppsgränser för utbetalningar från deras bankkonton. På sikt ska samtliga konton i betalningsmodellen omfattas av beloppsgränser. Införandet görs dock gradvis genom ett noggrant och kontrollerat förfarande hos myndigheterna. Anledningen till att införandet görs gradvis och efter mycket noggranna kontroller är att minska risken för att viktiga samhällsbetalningar eller löneutbetalningar stoppas på grund av felaktigt satta beloppsgränser. Riksgäldskontoret kommer under våren 2012, i samband med insamlingen av myndigheternas risker i betalningsverksamheten, att fortsätta stämma av myndigheternas arbete med införandet av beloppsgränser på sina bankkonton (se även avsnitt 4.2).

7.2 Utpekat ansvar för säkerheten i myndighetens betalningar[13]

Enligt Riksgäldskontorets verkställighetsföreskrifter till betalningsförordningen gäller följande:

– Myndigheten ska kontrollera att samtliga utbetalningar sker till rätt mottagare, med rätt belopp och vid rätt tidpunkt.
– Myndigheten ska dokumentera hur denna kontroll ska utföras hos myndigheten.

I samband med riskanalysen 2012 kommer Riksgäldskontoret att följa upp om myndigheterna har pekat ut ett tydligt ansvar för säkerheten i de sammantagna processerna för betalningar från myndigheten.

7.3 Tillförlitlig behörighetshantering[14]

Enligt Riksgäldskontorets verkställighetsföreskrifter till betalningsförordningen gäller sedan den 1 maj 2011 följande:

– Myndigheten ska lämna uppgift till banken om vem eller vilka som har behörighet att företräda myndigheten gentemot banken att öppna/avsluta bankkonto, betala från bankkonto m.m.

Föreskrifterna reglerar området i avvaktan på att frågan kring identifikation av behöriga företrädare utreds (se avsnitt 4.4). I samband

[12] Riksrevisionens rekommendation var att övriga myndigheter bör utnyttja möjligheterna att begränsa de utbetalningar som kan göras från myndigheten.
[13] Riksrevisionens rekommendation var att övriga myndigheter bör säkerställa att någon vid myndigheten har ett tydligt utpekat ansvar för säkerheten i de sammantagna processerna för betalningar från myndigheten och för att säkerheten i betalningsprocesserna löpande följs upp.
[14] Riksrevisionens rekommendation var att övriga myndigheter bör leva upp till kravet på en tillförlitlig behörighetshantering.

med riskanalysen 2012 kommer Riksgäldskontoret att följa upp behörighetshanteringen.

7.4 Analys av säkerheten i koppling mellan handläggarsystem och betalningsbemyndigande[15]

Enligt en ändring av betalningsförordningen som träder i kraft den 1 april 2012 ska samtliga myndigheter analysera de risker som är förknippade med myndighetens betalningar. Kravet på analysen omfattar således även kopplingen mellan handläggarsystem och betalningsbemyndigande.

Riksgäldskontoret kommer i samband med riskanalysen 2012 att följa upp att samtliga betalningsfiler från myndigheternas affärssystem är förändrings- och insynsskyddade från skapandet av filerna och att samtliga återrapporteringsfiler från ramavtalsbank till myndigheternas affärssystem likaså är förändrings- och insynsskyddade.

För att förhindra manipulation av betalningsuppdrag har Riksgäldskontoret ställt krav på myndigheterna att förändrings- och insynsskydda betalningsuppdragen till banken och återrapporteringen av genomförda betalningsuppdrag från banken. Motsvarande krav ställs också på återrapporteringen av genomförda inbetalningar till myndigheten.

7.5 Användning av och rutiner för bankdosor och pin-koder[16]

I Riksgäldskontorets verkställighetsföreskrifter till betalningsförordningen anges sedan den 1 maj 2011 följande:

– Myndigheten ska hantera lösenord och utrustning (pin-koder, dosor, kort) som används vid signering, debiteringsbemyndigande, avstämningsuppgift eller liknande på ett säkert sätt.

I samband med riskanalysen 2012 kommer Riksgäldskontoret att följa upp säkerheten i myndigheternas hantering av lösenord och utrustning.

8 Fortsatt arbete och kommande rapportering

I juli 2011 beslutade regeringen om direktiv till utredningen om Stärkt krisberedskap i det centrala betalningssystemet. Uppdraget till utredaren var att vidareutveckla och ytterligare konkretisera de förslag avseende de grundläggande säkerhetsnivåerna och det nationella samordningsansvaret

[15] Riksrevisionens rekommendation var att övriga myndigheter bör analysera hur säker kopplingen mellan handläggningssystem och betalningsbemyndiganden är i de systemlösningar som utnyttjas.

[16] Riksrevisionens rekommendation var att övriga myndigheter uteslutande bör använda bankdosor eller andra lösningar som har egen knappsats, så att pin-koden inte kan registreras av programvara i datorn, eller på annat sätt. Ytterligare en rekommendation till övriga myndigheter var att de bör se över rutiner för hantering av bankdosor och lösenord, och informera personalen om riskerna och om lämpliga åtgärder.

som lämnades i rapporten En samlad reglering för stärkt krisberedskap mot allvarliga tekniska fel och störningar i det centrala betalningssystemet (Fi2010/1619). I december 2011 avlämnades betänkande Stärkt krisberedskap i det centrala betalningssystemet (SOU2011:78). Betänkandet har remissbehandlats. En proposition om stärkt krisberedskap i det centrala betalningssystemet planeras att överlämnas till riksdagen under 2012.

Som tidigare nämnts ska Riksgäldskontoret senast den 1 november varje år lämna en redogörelse till regeringen avseende de samlade riskerna i den statliga betalningsmodellen. I de fall rapporten innehåller förslag om tillägg eller ändringar på området kommer regeringen att ta ställning till dessa. Regeringen avser att i kommande budgetpropositioner lämna en övergripande redovisning av ytterligare åtgärder som vidtagits för att förbättra säkerheten i statens betalningar.

Finansdepartementet

Utdrag ur protokoll vid regeringssammanträde den 22 mars 2012

Närvarande: Statsministern Reinfeldt, ordförande, och statsråden Björklund, Bildt, Ask, Larsson, Hägglund, Borg, Sabuni, Billström, Adelsohn Liljeroth, Björling, Ohlsson, Attefall, Kristersson, Elmsäter-Svärd, Hatt, Ek, Lööf

Föredragande: statsrådet Borg

Regeringen beslutar skrivelse 2011/12:91 Stärkt säkerhet i statens betalningar