

Finansdepartementet

103 33 STOCKHOLM

En samlad reglering för stärkt krisberedskap mot allvarliga tekniska fel och störningar i det centrala betalningssystemet

Sammanfattning

Riksgälden stöder utredningens förslag att grundläggande säkerhetskrav ska ställas. Vi anser dock att formuleringen av kraven bör utformas så att de blir mer kvantitativa till sin karaktär även för samhällsviktiga betalningar. Vi stöder utredningens förslag att de grundläggande säkerhetskraven tas in i en ny lag tillsammans med det nationella samordningsansvaret.

Riksgälden stöder också förslaget att Riksbanken ska ha det nationella samordningsansvaret för krisberedskapsfrågor som rör de centrala delarna av betalningssystemet. Riksgäldens betalningar över centralkontot och bankernas tjänster för förmedling av samhällsviktiga betalningar kommer att omfattas av det nationella samordningsansvaret.

Riksgälden välkomnar utredningens förslag att Riksgälden ska ha det nationella samordningsansvaret för säkerheten i den statliga betalningsmodellen, vilket innebär att upprätta en samlad risk- och sårbarhetsanalys över riskerna i den statliga betalningsmodellen och i statens betalningsprocesser. Riksgälden anser i likhet med utredaren att ansvaret för säkerheten i myndighetens egen betalningsverksamhet och riskanalys av denna ska ligga kvar på den enskilda myndigheten.

Ansvaret för informations- och utbildningsinsatser i säkerhetsfrågor och stöd till myndigheterna i säkerhetsarbetet anser vi dock inte ska ses som några egna ansvarsområden som utpekas särskilt. Prioriteringen av vilka insatser som ska betonas måste vara en uppgift för Riksgälden att ta ställning till.

Riksgälden anser att outsourcing inte ska utpekas som en särskild risk som skulle vara mera betydelsefullt att uppmärksamma än andra risker. Vi anser inte heller att det är motiverat att införa ett särskilt säkerhetssamråd vid outsourcing. Om det i Riksgäldens samlade risk- och sårbarhetsanalys över riskerna i den statliga betalningsmodellen framkommer att det finns förhöjda risker på grund av outsourcing ska relevanta åtgärder tas därefter.

Riksgälden som aktör i betalningssystemet

Riksgälden ansvarar för statens finansförvaltning. I den verksamheten är Riksgälden en central aktör i betalningssystemet. Riksgälden innehar och ansvarar för statens centralkonto i Riksbanken. Centralkontot nås via RIX-systemet som används för att genomföra betalningar mellan oss och bankerna.

Enligt statsmakternas krav ska statliga betalningar utföras på ett kostnadseffektivt och säkert sätt. Att ställa krav på god säkerhet i bankernas betalningar och att delta i säkerhetsarbetet för att undvika allvarliga tekniska fel och störningar i betalningssystemet är därför en prioriterad uppgift för Riksgälden.

Riksgäldens och de statliga myndigheternas betalningsverksamhet är omfattande. Vi kommer därför alltid att på något sätt bli berörda om en av de av utredningen definierade typkriserna – infrastrukturkris, kärnkris eller utbetalningskris – inträffar.

I Riksgäldens roll som ansvarig för den statliga betalningsmodellen är arbetet med s.k. utbetalningskriser central. Utbetalningskriser innebär i det sammanhanget att betalningar som är nödvändiga för allmänheten, t.ex. utbetalningar från socialförsäkringssystemet, arbetslöshetsförsäkringen, studiemedelssystemet eller liknande inte kan betalas ut.

Avsnitt 3 De utbetalande myndigheternas beredskap att hantera en kris i betalningsverksamheten

Vi har under flera år arbetat aktivt med att definiera och förbättra de utbetalande myndigheternas beredskap att hantera en kris i betalningsverksamheten. Även andra myndigheter som Myndigheten för samhällsskydd och beredskap (MSB/SOES) och speciellt de större betalningsmyndigheterna som Försäkringskassan, Skatteverket, Centrala studiestödsnämnden, Arbetsförmedlingen, Pensionsmyndigheten, Tullen och Statens pensionsverk har lagt ner resurser på att både i samverkan och enskilt identifiera åtgärder för att förbättra beredskapen.

Tillgänglighet, reservsystem och -rutiner

I Riksgäldens upphandling av betalningstjänster under år 2010 togs initiativ på följande områden inom betalningsberedskapen

1. Vi ställde krav på att bankernas system ska vara tillgängliga, dvs. att banken ska ha en dokumenterad kontinuitetsplan och reservsystem för centrala betalningssystem och redundanta kommunikationslösningar till och från banken. Vi begärde också att få ta del av dokumentationen över bankens kontinuitetsplaner och rutiner.
2. När det gäller enskilda betalningstjänster ställdes krav på att banken i anbudet skulle dokumentera vilka reservrutiner, t.ex. annan likvärdig betalningstjänst, som banken ansåg att myndigheten kunde använda vid bortfall. För att motverka kommunikationsbortfall ställdes också krav på att banken kunde ta emot information på annan media, t.ex. CD/DVD eller USB-minne. För att kunna skicka utbetalningar även vid ett totalt kommunikationsbortfall upphandlades möjligheten att banken skulle spara föregående relevanta fil med betalningsuppdrag

för att samma fil med betalningsuppdrag även skulle kunna användas nästa månad eller vecka beroende på myndighetens betalningsfrekvens.

3. Kraven på bankernas upplysningsplikt vid bristande tillgänglighet skärptes. Myndigheterna har större möjligheter att ställa krav på bankerna vad som skall rapporteras och hur rutinerna för incidentrapportering till myndigheten ska utformas. Bankerna har också en skyldighet att medverka i myndigheternas risk- och sårbarhetsanalyser av betalningsverksamheten, att koordinera krisplaner och att öva krishantering.

Vi har vid sidan av upphandlingen tagit initiativ till att ändra i Betalningsförordningen och i föreskrifterna för att reglera myndigheternas verksamhet med att öka säkerheten inom dessa och inom andra områden.

Utredningen tar kortfattat upp Riksgäldens och myndigheternas löpande verksamhet med att identifiera, beskriva och införa reservsystem och rutiner. Beroende på scenario kan myndigheterna behöva reservsystem och rutiner för bortfall i

1. bankens betalningsförmedling, t.ex. förmedling via annan bank
2. enstaka betalningstjänster hos banken, t.ex. förmedling via annan betalningstjänst
3. kommunikationen med banken, t.ex. annan kommunikationsväg/tjänst
4. framställning av betalningsuppdrag hos myndigheten, t.ex. reservsystem hos myndigheten.

Ambitionen hos Riksgälden och hos myndigheterna har varit att identifiera och dokumentera existerande reservsystem och rutiner att användas vid olika scenarier. Vi har också övervägt huruvida vi ska införa nya. Införandet av nya reservsystem och rutiner kostar pengar. Ibland kan redan befintliga, och i andra sammanhang använda betalningstjänster, som t.ex. utbetalningskort, användas utan alltför stora extra kostnader. I vissa fall måste dubblerade system eller rutiner införas, vilket kan bli kostsamt.

Ett svårt övervägande att ta ställning till är att balansera tillgången till reservsystem och rutiner mot behovet. Ju säkrare bankernas betalningssystem är, både när det gäller kundbetalningar mellan avsändare och mottagare och betalningar mellan bankerna, desto mindre är behovet av reservrutiner hos myndigheterna för att motverka bortfall av en eller flera bankers betalningsförmedling.

Bankernas och centralbankens beredskap blir på det sättet en variabel i bedömningen av myndigheternas behov av att stärka beredskapen för att kompensera bortfall av betalningsfunktionalitet. Myndigheterna måste känna till bankens krisberedskap och kontinuitetsplaner för att kunna ta ställning till vilka svagheter i beredskapen som myndigheten ska förbereda för.

Ett annat alternativ kan vara att det finns klara och tydliga grundläggande säkerhetskrav som bankerna ska uppfylla. Bankerna måste förbinda sig till och ansvara för att uppnå säkerhetskraven. Det har ibland framförts från bankernas sida att de ansvarar i sin helhet för att betalningsförmedlingen fungerar från det att banken mottagit myndighetens betalningsuppdrag till dess att betalningen är insatt på mottagarens bankkonto. Det gäller vid löpande drift, men inte vid kris. Det har framkommit, både i myndigheternas enskilda arbete och i samverkan med MSB, att en myndighet i sitt beredskapsarbete måste beakta att betalningsförmedlingen inte fungerar i vissa lägen. Myndigheterna räknar då med att de måste kompensera med reservrutiner för bortfall, eller delvis bortfall, av betalningstjänster eller kommunikation i krislägen.

Det är dock inte rimligt att myndigheterna ska åta sig att klara sina betalningar oavsett läget i det allmänna betalningssystemet. Det kräver att parallella betalningssystem och parallella betalningstjänster finns, vilket vore orimligt kostsamt. För staten, liksom för andra användare av betalningstjänster, är det viktiga att insatser läggs på att säkerställa att det allmänna betalningssystemet är robust.

Alternativa betalningsvägar

Myndigheterna som hanterar samhällsbetalningar som socialförsäkring, arbetslöshetsförsäkring, studiestöd, skatter eller liknande betalningar har ett ansvar för att betalningarna utförs, även i ett krisläge. Myndigheterna har ett ansvar från ansökan om ersättning ända tills betalningen är mottagaren tillhanda. För några myndigheter, t.ex. Försäkringskassan, finns reglerat när betalningen ska vara mottagaren tillhanda, pensioner den 18 och 19 i månaden, barnbidrag den 20 i månaden.

Det finns ingenstans angivet att myndigheten kan överväga att bidragsmottagaren i krislägen (brist på elförsörjning, bortfall av enstaka betalningstjänst eller om någon bank inte är tillgänglig) ska nöja sig med att få ersättningen tillhanda senare. Och i så fall hur långt senare. För närvarande gäller att ersättningen ska vara mottagaren tillhanda på den bestämda utbetalningsdagen.

Det ställer stora krav på betalningssystemets tillgänglighet för att samhällskritiska utbetalningar ska kunna genomföras på angivet datum. Det finns ingen ramavtalsbank som kan garantera en sådan tillgänglighet. I ramavtalen om förmedling av statliga betalningar står att banken i vissa fall är ersättningskyldig om det inträffar och att Riksgälden i vissa fall har rätt att säga upp avtalet om banken inte fullgör sina avtalsförpliktelser.

Det är inte rimligt att kräva att betalningen ska vara mottagaren tillhanda på den bestämda utbetalningsdagen i ett krisläge. Det har därför diskuterats om det går att fastställa kvantitativa mål för när betalningen ska vara mottagaren tillhanda i ett krisläge. Så vitt vi känner till finns ett exempel på en sådan reglering. Det är enligt EU-direktivet att medel på spar- och transaktionskonton som ersätts från den statliga insättningsgarantin ska vara

mottagaren tillhanda senast 20 dagar efter att banken ställt in betalningarna¹. Den tiden är till för handläggning av ärendet, dvs. att reda ut vem som skall ha hur mycket pengar och för att skapa ett utbetalningsuppdrag till ett annat bankkonto eller till mottagarens namn och adress.

Kan motsvarande kvantitativa mål fastställas i andra krislägen när banken inte kan betala ut samhällskritiska betalningar? Det skulle kunna ge myndigheterna tillgång till en kort omställningsperiod för att kunna använda alternativa betalningsvägar.

Arbetet med alternativa betalningsvägar har delvis skett i MSB/SOES regi. Det arbetet har kommit fram till att följande huvudtyper av lösningar finns

1. Utbetalningskort, där inlösen av beloppet kan ske med saldokontroll mot bankkontot och utan saldokontroll (olika säkerhetsnivåer tillämpas alltså vid inlösen av avin)
2. Kontantkort (prepaid card), alltså en lösning som bygger på att mottagaren får ett platskort laddat med ett belopp i kronor, kortet är återladdningsbart.
3. Konton utanför banksystemet, t.ex. hos kortbolag, konton med kort och utan kort (virtuella)

I dagsläget har Riksgälden upphandlat huvudtyperna 1 och 2, dvs. utbetalningskort och kontantkort.

Enligt ramavtalen har statliga myndigheter tillgång till en tjänst hos alla ramavtalsbankerna där Bangirocentralen (BGC) via underleverantör kan trycka upp 300 000 utbetalningskort om dagen. Till tjänsten har bankerna kopplat avtal med inlösenställen, bl.a. Nordea, Swedbank och Kuponginlösen.

Tjänsten används som ordinarie rutin av Skatteverket varje år i augusti vid återbetalning av skatt till mottagare som inte deklarerat elektroniskt och inte anmält mottagande bankkonto för återbetalningen. Tjänsten kan användas av alla myndigheter, både som ordinarie rutin och som reservrutin. Tjänsten är mycket dyrare (ca 7,00 kronor) än kontoinsättning på bankkonto (ca 0,34 – 0,59 kronor). Det krävs också en viss framförhållning för tryckeriet att planera och få i gång så stor tryckkapacitet. För att tjänsten ska kunna användas som reservrutin krävs därför att utbetalningen kan ske något senare än på ordinarie utbetalningsdag så att myndigheten hinner omforma och ställa om betalningsuppdraget.

Kontantkort upphandlades den 1 januari 2010 från ICA Banken AB, men används än så länge i mindre volymer. Tjänsten har alltså ännu inte använts i så stor skala att man kan säga att den går att använda som reservrutin vid stora volymer dagskritiska samhällsbetalningar. Om användningen av tjänsten ökar och därmed även kapaciteten att trycka

¹ DIRECTIVE 2009/14/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 2009 amending Directive 94/19/EC on deposit-guarantee schemes as regards the coverage level and the payout delay (10)

och distribuera kort ökar kan tjänsten bli en alternativ betalningsväg. Det förutsätter dock att utbetalningen är på ett mindre belopp, exempelvis kring 10 000 kronor eller mindre, eftersom beloppet måste tas ut kontant eller användas vid köp. Det går inte att föra över beloppet på kortet till ett annat bankkonto.

Ytterligare en aspekt på dessa alternativa betalningsvägar är hur länge de kan fungera i ett läge när bankerna inte fungerar. Hur länge kan t.ex. mataffärer fortsätta att bedriva verksamhet utan att själva ha tillgång till betalningsförmedling i bankerna?

För myndigheter som önskar införa reservrutiner och alternativa betalningsvägar finns lämpliga tjänster upphandlade. Beslut om införande måste tas av myndigheterna. Användningen av reservrutinerna innebär också att myndigheten måste göra en ändring/omställning i myndighetens interna system och rutiner för att producera betalningsuppdrag som är utställda på mottagarens namn och adress i stället för mottagarens bankkontonummer.

Myndigheten måste vid beslutet avväga om de ytterligare kostnaderna för att införa reservrutiner i form av alternativa betalningsvägar motiveras av samhällsbehovet att betalningen ska vara mottagaren tillhanda på den bestämda utbetalningsdagen.

Avsnitt 6 Grundläggande säkerhetskrav (mål), kvalitativa eller kvantitativa krav

Det är viktigt att grundläggande säkerhetskrav för betalningssystemet fastställs, inte bara kvalitativt utan också kvantitativt. Vi stöder utredningens förslag att grundläggande säkerhetskrav ska ställas. Vi anser dock att formuleringen av kraven bör utformas så att de blir mer kvantitativa till sin karaktär.

Utredningen föreslår kvantitativa mål för centrala betalningar i RIX-systemet

”Även vid allvarliga störningar eller avbrott ska merparten av alla betalningar i RIX-systemet avvecklas inom ett dygn.”

För samhällsviktiga betalningar har utredningen inte samma ambitionsnivå att formulera kvantitativa mål

”... Det ska så långt som möjligt säkerställas att samhällsviktiga betalningar kan genomföras inom rimlig tid även vid allvarliga tekniska störningar och avbrott.”

Bankernas och centralbankens beredskap är en variabel i bedömningen av myndigheternas behov av att stärka sin beredskap för att kompensera bortfall av betalningsfunktionalitet. För att myndigheterna ska veta vilken beredskap som bankerna och centralbanken planerar för måste det finnas klara och tydliga grundläggande säkerhetskrav som bankerna ska uppfylla. De grundläggande kraven bör formuleras kvantitativt i så stor utsträckning som möjligt, även för samhällsviktiga betalningar.

Exempel:

”Även vid allvarliga tekniska störningar eller avbrott ska merparten av samhällsviktiga betalningar genomföras inom rimlig tid, vilket avser inom x dagar .”

Myndigheterna får då klara besked om vad banken förbinder sig till och kan därmed också bättre ta ställning till vilka scenarios man behöver utveckla reservsystem och rutiner för eller om myndigheten måste planera för övergång till alternativa betalningsvägar.

Vi stöder utredningens förslag att de grundläggande säkerhetskraven tas in i en ny lag tillsammans med det nationella samordningsansvaret.

Avsnitt 7 Nationellt samordningsansvar

Riksgälden stöder förslaget att Riksbanken ska ha det nationella samordningsansvaret för krisberedskapsfrågor som rör de centrala delarna av betalningssystemet.

Riksgälden deltar i FSPOS samverkan och anser att samarbetet fungerar bra och har bidragit till bättre beredskap i det centrala betalningssystemet och bättre förståelse för olika typer av betalningsflöden, både mellan de centrala aktörerna och när det gäller samhällsbetalningar mellan mottagare och avsändare.

Riksgäldens betalningar över centralkontot kommer att omfattas av det nationella samordningsansvaret. Även bankernas tjänster för förmedling av samhällsviktiga betalningar omfattas. Myndigheters betalningar, även de samhällsviktiga betalningarna, hanteras inom statens betalningsmodell och omfattas därför av Riksgäldens föreslagna risk- och sårbarhetsanalys.

Avsnitt 8 Säkerheten i den statliga betalningsmodellen

Nationellt samordningsansvar för säkerheten i den statliga betalningsmodellen

Vi välkomnar förslaget att Riksgälden ska ha det nationella samordningsansvaret för säkerheten i den statliga betalningsmodellen.

I uppdraget ingår att upprätta en samlad risk- och sårbarhetsanalys över riskerna i den statliga betalningsmodellen och i statens betalningsprocesser. För att genomföra detta avser vi att samla in information från myndigheterna. Myndigheterna får svara på ett antal frågor, vi sammanställer svaren och sätter de risker som framkommer i relation till rådande hotbild. Det pågår för närvarande diskussioner med Finansdepartementet om hur uppdraget närmare ska utformas.

Frågorna som myndigheterna får från oss kan myndigheten använda som hjälp i sina egna risk- och sårbarhetsanalyser. Riksgälden anser i likhet med utredaren att ansvaret för säkerheten i myndighetens betalningsverksamhet och riskanalys av denna ska ligga kvar på den enskilda myndigheten. Myndigheten ansvarar för att åtgärda risker som framkommit i den egna risk- och sårbarhetsanalysen.

Utifrån de svar som myndigheten lämnat på våra frågor kan sedan beredskapen stärkas genom exempelvis nya föreskrifter, utbildningar och ändrade ramavtal.

Riksgälden kan också påtala brister till regeringen med önskan om åtgärder.

Särskilt ansvar för information och utbildning i säkerhetsfrågor

Ansvar för informations- och utbildningsinsatser i säkerhetsfrågor och stöd till myndigheterna i säkerhetsarbetet anser vi dock inte ska ses som några egna ansvarsområden som utpekas särskilt. Dessa ska i stället utföras på samma sätt som andra informations-, utbildnings- och stödinsatser av t.ex. själva betalningsmodellen, kontostrukturen, fullmakter, betalningsflöden, kommunikation med bankerna, upphandlade betalningstjänster inklusive kortbetalningar, återredovisning från bankerna eller avstämningar av gjorda betalningar. Prioriteringen av vilka insatser som ska betonas särskilt vid vilka tillfällen måste göras efter behov och vara en uppgift för Riksgälden att ta ställning till.

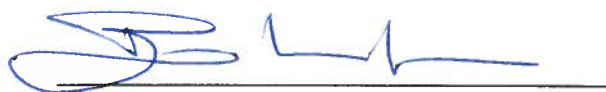
Outsourcing

Riksgälden anser att outsourcing inte ska utpekas som ett särskilt område eller en särskild risk som skulle vara mera betydelsefullt att uppmärksamma än andra risker. Att det skulle behövas ett särskilt säkerhetssamråd vid outsourcing anser vi inte heller är motiverat. Outsourcing inom myndigheterna kan avse ett antal olika verksamhetsområden som inte nödvändigtvis behöver ha någon relevans för myndighetens betalningsverksamhet. Outsourcing kan också ibland stärka säkerheten då man överläter verksamhet åt någon som är specialist på området med bättre tillgång till rutiner, inklusive reservrutiner.

I den löpande uppföljningen av ramavtalen uppmärksammar vi tillsammans med ramavtalsbankerna riskerna för myndigheternas betalningar när ramavtalsbankerna outsourcar verksamhet som till exempel administrationen kring löneutbetalningar eller hela IT-driften för bankens betalningssystem.

Riksgälden kan i sin roll som ansvarig för betalningsmodellen och de samlade riskerna i modellen dokumentera och behandla också de risker som avser betalningsverksamheten som är aktuella i samband med outsourcing, både hos myndigheterna och hos ramavtalsbankerna. Om det i Riksgäldens analys av riskerna i betalningsprocesserna framkommer att det finns förhöjda risker på grund av outsourcing ska relevanta åtgärder tas därefter.

I ärendet har riksgäldsdirektör Bo Lundgren beslutat efter föredragning av Anita Nyqvist i närvaro av biträdande riksgäldsdirektör Pär Nygren och avdelningschef Jenny Rolling. I ärendets handläggning har säkerhetschef Lotta Oscarsson och chefsekonom Lars Hörngren också deltagit.



Bo Lundgren, beslutande



Anita Nyqvist, föredragande