



Polismyndigheten
Nationella operativa avdelningen
Utredningsenheten
Nationellt bedrägericentrum (NBC)

Frågor och svar

Här finner du en sammanställning på frågor och svar som bland annat berör den tekniska delen i anslutningsprocessen, säkerhet och juridik samt verksamhet och övriga frågor.

Hittar du inte svaret på din fråga, mejla till: bankinfo@polisen.se

Rör din fråga IT mejla till: forvaltning-it.finansiella-fragor@polisen.se

Observera att vi har möjlighet att svara på frågor gällande etapp ett och två. Vi kommer återkomma gällande etapp tre och fyra när det börjar närma sig.

Vi vill även understryka att Polismyndigheten inte har möjlighet till enskilda informationsmöten. Vi erbjuder ett möte i samband med onboarding som framgår av startpaketet. Har du inte fått ta del av startpaketet mejla till forvaltning-it.finansiellafragor@polisen.se.

Innehållsförteckning

IT 4

Hur förväntas kreditinstituten genomföra anslutningsprocessen gällande testning och verifikation av kommunikationslösningen?	4
Vilken teknologi kommer att användas?	4
Hur ska transaktionskoder (BankTransactionCode) hanteras?	5
Ska det vara Business Application Header (BAH) på alla meddelanden?	5
Vilka sökbegrepp kommer att användas?	5
Kommer ett anrop kunna innehålla flera sökbegrepp personer/konton/kort?	5
Vad gör vi när filerna blir stora?	5
I vilket format ska filerna skickas?	6
Hur aktuell måste datan vara?	6
Hur skickas kreditkortsnummer?	6
Enligt vilken tidszon ska tidsstämplar rapporteras i svaret?	6
I vilket format förväntar ni er svaren?	6
Kan en kortfråga göras som ett begränsat utdrag?	6
Hur hanteras saldon i en kortfråga i etapp 2?	6
För vilka transaktioner ska reserverade/avvisade/returnerade transaktioner i etapp 2 redovisas?	7
Ska reserverade/avvisade/returnerade transaktioner i etapp 2 redovisas historiskt när en fråga ställs bakåt i tiden?	7
Vad är en nekad returnerad transaktion?	7
Hur ska återköp hanteras?	7
Kan institut svara på samma fråga två gånger?	7
Hur svarar man när konto är avslutat innan efterfrågat start-datum? ...	7
Vad betyder felmail från polisen att ”svarsfilen kan ej processas av Polismyndigheten då den ej finns begärd eller redan tagits bort”?	7

Säkerhet och juridik 8

Är finansiella företag tvungna att lämna ut uppgifter till kund i enlighet med GDPR om att uppgifter om bl.a. korttransaktioner har överlämnats till Polismyndigheten?	8
Vad händer om banken inte On-boardar sig i tid?	8
Hur säkerställs Polismyndighetens behörigheter och att ingen obehörig skickar frågor?	8
Vilka säkerhetsmekanismer tänker ni använda i den initiala Epostlösningen?	9

Verksamhet och övrigt..... 9

Svara skyndsamt - vad innebär det?	9
--	---

Hur prioriteras frågorna – finns det någon prioritering, exempelvis vid frihetsberövande?	9
Kommer övriga brottsutredande myndigheter använda den standardiserade lösningen?	9
Vilka är övriga brottsutredande myndigheter?	9
Vilka konton och produkter kommer att omfrågas?	9
Vilka konton ska vara med? Skiljer det något mellan privat- och företagssidan vilka konton som är intressanta?	9
Hur ska historiska uppgifter hanteras?	9
Kommer manuella frågor kvarstå?	10
Kan vi få information om projektet på andra språk än svenska?	10
Hur hänger Skatteverkets Mekanismen och finansiella frågor ihop? ..	10

IT

Hur förväntas kreditinstituten genomföra anslutningsprocessen gällande testning och verifikation av kommunikationslösningen?

För att genomföra test och verifikation har polisen tagit fram en process för onboarding.

För att påbörja en onboarding måste följande krav uppfyllas:

- Ni måste tillhandahålla en testmiljö med relevant testdata
- Det ska finnas en funktionsbrevlåda för test dit myndigheter kan skicka frågor
- Förutsättningar för en säker kommunikation ska finnas på plats (TLS)
- Krypteringsnycklar för test ska ha skapats och utbytts
- Verifierade och godkända XML-meddelanden
- Systemet ska i övrigt vara klart för att användas och testa mot, inklusive krypteringshantering

När kreditinstitutet är redo för onboarding ska ett första möte bokas in genom att kontakta forvaltning-it.finansiella-fragor@polisen.se. I mötet säkerställer vi att allt är redo och godkänt, samt planerar inför testfasen där vi mellan våra testmiljöer ska:

- Skicka samtliga XML-meddelanden och se att rätt svar kommer från finansinstitutet
- Testa olika scenarion som ska hanteras på specifika sätt

Sist kommer en sista verifiering i produktion för samtliga meddelanden för etappen då den automatiserade lösningens svar ska jämföras mot ett manuellt svar av samma fråga.

Vilken teknologi kommer att användas?

Till en början, E-post (TLS)/XML

Till API-lösningen, REST/XML

Meddelandestrukturen baseras på ISO20022 och meddelandena auth.001.001.01 tillsammans med head.001.001.02 är frågan och auth.002.001.01 med head.001.001.02 tillsammans med antingen supl.027.001.01 eller camt.053.001.08 är svaret. Auth och head-meddelandena kapslas in i ett polis-definierat meddelande.

För kryptering under e-postlösningen används PGP.

Hur ska transaktionskoder (BankTransactionCode) hanteras?

Inledningsvis kan både ISO-koder och proprietärt (fritextfält) användas. Polisen ser gärna att bankerna sätter båda, men de går bra att använda den ena eller den andra. På sikt ska ISO-koderna användas men det är fortfarande okej att sätta proprietär samtidigt.

Ska det vara Business Application Header (BAH) på alla meddelanden?

BAH ska finnas tillsammans med auth001 från polisen och auth002 från banken.

Vilka sökbegrepp kommer att användas?

Följande sökbegrepp kommer att användas, varje fråga innehåller endast ett sökbegrepp:

- Kontonummer
- Kortnummer
- Personnummer
- Samordningsnummer
- Organisationsnummer
- Namn + Födelsedatum och -plats

Kommer ett anrop kunna innehålla flera sökbegrepp personer/konton/kort?

I varje anrop skickas bara en fråga som endast avser ett sökbegrepp.

Vilka uppgifter lämnas vid sökningen och vilka svar förväntas?

Kontonummer => omfattande kontoutdraget (camt.053.001.08).

Kontonummer, Limited => begränsade kontoutdraget, begränsat med personuppgifter (camt.053.001.08).

Kortnummer => korttransaktioner (camt.053.001.08).

Personnummer, samordningsnummer, organisationsnummer => Engagemang (supl.027.001.01).

Om vi inte får någon träff i våra system, förväntar sig systemet något svar?

Blir det ingen träff ska NFOU (NOT FOUND) skickas med i svaret (auth.002.001.01).

Vad gör vi när filerna blir stora?

Komprimering sker i samband med kryptering. Blir filen ändå för stor ska en delmängd av konto-/kortutdraget skickas och markeras i StatementPagination i camt.053.001.08. Delmängden ska vara kronologisk och ha samma startdatum som den ursprungliga frågan för att myndigheten lätt ska kunna skicka en ny förfrågan för nästa delmängd.

Max 20 000 transaktioner per fil är den gräns som är uppsatt av Polismyndigheten

I vilket format ska filerna skickas?

Vi kommer att skicka .xml och ta emot .xml eller .xml.zip.

Hur gör vi med svar som tar längre tid än skyndsamt?

Svaret ska inväntas och responseStatus ska vara COMP.

Hur aktuell måste datan vara?

När det gäller dataaktualitet kommer data som polisen efterfrågar vara minst 24 timmar gammal.

Hur skickas kreditkortsnummer?

Polismyndigheten kommer att under etapp 2 inte skicka kortnummer tokeniserat eller maskade, men hela förfrågan kommer att vara krypterad. Väljer kreditinstitutet att skicka tillbaka kortnumren maskade så är det okej.

Enligt vilken tidszon ska tidsstämplar rapporteras i svaret?

Tidsstämplar kan rapporteras enligt önskad tidszon, men om zonangivelse saknas antas tiden vara enligt svensk tidszon.

I vilket format förväntar ni er svaren?

XML med UTF-8 encoding (ej BOM)

Kan en kortfråga göras som ett begränsat utdrag?

Nej, endast kontofråga kan göras som ett begränsat utdrag.

Kommer Polismyndigheten ställa fråga på ett Swish-nummer?

Nej. Däremot vill Polismyndigheten ha information om Swish-transaktioner i svarsfiler för kontofråga enligt specifikationer.

Hur hanteras saldon i en kortfråga i etapp 2?

Slut-saldo kommer inte vara start-saldo + summan av transaktionerna i en kortfråga eftersom endast korttransaktioner redovisas i svaret på en kortfråga.

Hur hanteras antalet transaktioner och summering av transaktionerna gällande reserverade/avvisade/returnerade transaktioner i etapp 2?

Summan är summan av bokförda transaktioner d v s avvisade och reserverade är inte medräknade. Antalet är antalet transaktioner oavsett status.

För vilka transaktioner ska reserverade/avvisade/returnerade transaktioner i etapp 2 redovisas?

Reserverade transaktioner ska redovisas för alla typer av transaktioner. De ska redovisas i svar för både kontofråga och kortfråga.

Nekade transaktioner (avvisade och returnerade) ska endast rapporteras för nekade kortköp, bankomatuttag samt Swish-transaktioner. De ska redovisas i svar för både kontofråga och kortfråga.

Ska reserverade/avvisade/returnerade transaktioner i etapp 2 redovisas historiskt när en fråga ställs bakåt i tiden?

Nekade avvisade och nekade returnerade transaktioner ska redovisas historiskt.

Det har framkommit att samtliga institut inte har information om historiska reservationer. De institut som har information om historiska reservationer skickar dessa. De institut som inte har den informationen skickar nuvarande status på transaktionen.

Vad är en nekad returnerad transaktion?

En nekad returnerad transaktion är en transaktion som nekats hos mottagaren när transaktionen ska processas i mottagarens system. Exempel vid en Swish-transaktion där mottagande konto är under likvidation och mottagande institut returnerar transaktionen med en lämplig returkod.

Hur ska återköp hanteras?

Som en vanlig transaktion men tydliggör att transaktionen är ett återköp och det är viktigt att ha med vem återköpet kommer från.

Kan institut svara på samma fråga två gånger?

Nej, när institutet skickat ett svar på en fråga är frågan förbrukad.

Hur svarar man när konto är avslutat innan efterfrågat start-datum?

Exempelvis med ett NFOU-svar där man skriver att kontot är avslutat innan efterfrågat start-datum i elementet "AddtlInf".

Vad betyder felmail från polisen att "svarsfilen kan ej processas av Polismyndigheten då den ej finns begärd eller redan tagits bort"?

Användaren i Bankinfo har möjlighet att radera sin förfrågan om denne har gjort något fel. Om institutet skickar ett svar efter att användaren raderat

frågan så skickas ett felmail tillbaka till institutet med denna text. Institutet kan bortse från detta mail.

Säkerhet och juridik

Är finansiella företag tvungna att lämna ut uppgifter till kund i enlighet med GDPR om att uppgifter om bl.a. korttransaktioner har överlämnats till Polismyndigheten?

Nej, finansiella företagen är inte skyldig att till kunden lämna ut information om att uppgifter om personen lämnats till polismyndigheten. Lagstödet för detta är 5 kap 1§ dataskyddslagen.

Av 5 kap. 1 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) framgår att skyldigheten att informera den registrerade (artikel 13–15 i GDPR) inte gäller sådana uppgifter som hade omfattats av sekretess mot den enskilde själv hos en myndighet. Hos polismyndigheten föreligger s.k. förundersökningssekretess enligt 18 kap. 1 § offentlighets och sekretesslagen (2009:400). Anledningen är att om misstänkta skulle få information om alla åtgärder polisen vidtagit, eller kan komma att vidta, finns också risk att viktiga bevis förstörs.

Vad händer om banken inte On-boardar sig i tid?

Det kommer att formuleras en övergångsbestämmelse i föreskriften om innefattar en övergångsperiod. Myndigheten har förståelse för att anslutningen kan ta tid. Vi kommer att fortsätta skicka begäran som vi gör idag till de företag som inte har anslutit sig. När övergångsperioden är slut kommer vi börja meddela Finansinspektionen att företaget inte uppfyller sina förpliktelser mot Polismyndigheten.

Hur säkerställs Polismyndighetens behörigheter och att ingen obehörig skickar frågor?

Kommunikationen mellan kreditinstitut och myndigheter sker via TLS. Dessutom är alla filer som skickas krypterade och signerade. Detta gör det möjligt att säkerhetsställa vem motparten är i kommunikationen. Frågor från Polismyndigheten kommer att ha behörighetskontroll och spårbarhetsloggning. E-post som kommer från polisens automatiserade system kommer alltid ha samma avsändare.

Vilka säkerhetsmekanismer tänker ni använda i den initiala Epostlösningen?

I den initiala E-postlösningen kommer Transport Layer Security (TLS) samt kryptering och signering med PGP att användas.

Verksamhet och övrigt**Svara skyndsamt - vad innebär det?**

Kreditinstituten ska svara på förfrågan skyndsamt, inom 18 timmar under kontorstid, vardagar 8–17.

Hur prioriteras frågorna – finns det någon prioritering, exempelvis vid frihetsberövande?

Ingen prioritering finns, alla finansiella frågor ska ses som lika viktigt.

Kommer övriga brottsutredande myndigheter använda den standardiserade lösningen?

Föreskriften täcker samtliga brottsutredande myndigheter och polisens framtagna standard kommer att kunna användas av dessa myndigheter. Arbetet med föreskriften pågår inom Polismyndigheten.

Vilka är övriga brottsutredande myndigheter?

Ekobrottsmyndigheten, Kustbevakningen, Skatteverket, Säkerhetspolisen, Tullverket och Åklagarmyndigheten.

Vilka konton och produkter kommer att omfrågas?

För kontoutdraget ingår de konton som Skatteverkets plattform Mekanismen levererar. Övriga konton hanteras via ett manuellt förfarande. I engagemangsbekedet ska alla typer av konton, produkter och engagemang vara inkluderade.

Vilka konton ska vara med? Skiljer det något mellan privat- och företagssidan vilka konton som är intressanta?

Samtliga konton ska redovisas i svaret till Polismyndigheten. Det är polisen själva som bedömer vad som är av intresse efter att ha tagit del av helheten. Samtliga konton är därför av intresse för Polismyndigheten.

Hur ska historiska uppgifter hanteras?

- Tidsspannet bakåt i tiden är initialt 24 månader i etapp 1 och 2.
- När transport av information i framtiden sker via en api-lösning, skall de automatiserade frågorna successivt utökas bakåt i tid.

- När api-lösningen har varit i drift i 12 månader kommer frågor bakåt i tiden att utökas med 12 månader. Tidsspannet kommer vid denna tidpunkt omfatta 24 + 12 månader.
- Vid samma tidpunkt ett år senare utökas omfånget med ytterligare 12 månader, och begäran om information kommer således kunna omfatta 36 + 12 månader bakåt i tiden.
- Denna successiva ökning fortsätter med 12 månader varje år, och kommer avslutas vid 60 månader, dvs 5 år bakåt i tiden är det längsta tids-
spann som den automatiserade lösningen kommer att efterfråga.
- Manuella frågor kan fortsatt komma att ställas för att efterfråga perioder ännu längre bakåt i tiden. Mängden manuella följdfrågor kommer successivt att minska i takt med att de automatiserade tidsspannet utökas.

Kommer manuella frågor kvarstå?

Ja.

Kan vi få information om projektet på andra språk än svenska?

Information och dokumentation från polisen finns endast på svenska. Gällande ISOstandarden och dess värden kan engelska termer förekomma.

Hur hänger Skatteverkets Mekanismen och finansiella frågor ihop?

Myndigheter får information från Mekanismen om vilka konton en person/organisation har i vilka kreditinstitutet. Kontonumret används i kontofrågan inom ramen för lagstiftningen. [Läs mer om Konto- och värdefackssystem, Mekanismen, på Skatteverkets hemsida.](#)