Datum 2023-11-14

Informationsklass Öppen

Diarienr (åberopas)

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 anslutning som framgår av startpaketet. Har du inte fått ta del av startpaketet mejla till forvaltning-it.finansiellafragor@polisen.se.

Innehållsförteckning

IT 3
Hur förväntas kreditinstituten genomföra anslutningsprocessen gällande testning och verifikation av kommunikationslösningen? 3
Vilken teknologi kommer att användas? 3
Hur ska transaktionskoder (BankTransactionCode) hanteras? 4
Ska det vara Business Application Header (BAH) på alla meddelanden? 4
Vilka sökbegrepp kommer att användas? 4
Kommer ett anrop kunna innehålla flera sökbegrepp personer/konton/kort? 4
Om vi inte får någon träff i våra system, förväntar sig systemet något svar? 4
Vad gör vi när filerna blir stora? 4
I vilket format ska filerna skickas? 5
Hur gör vi med svar som tar längre tid än skyndsamt? 5
Hur aktuell måste datan vara? 5
Hur skickas kreditkortsnummer? 5
Enligt vilken tidszon ska tidsstämplar rapporteras i svaret? 5
I vilket format förväntar ni er svaren? 5

Säkerhet och juridik 5
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? 5
Vad händer om kreditinstitutet inte ansluter sig i tid? 6
Hur säkerställs Polismyndighetens behörigheter och att ingen obehörig skickar frågor? 6
Vilka säkerhetsmekanismer tänker ni använda i den initiala Epostlösningen? 6

Verksamhet och övrigt 6
Svara skyndsamt - vad innebär det? 6
Hur prioriteras frågorna – finns det någon prioritering, exempelvis vid frihetsberövande? 6
Kommer övriga brottsutredande myndigheter använda den standariserade lösningen? 6
Vilka är övriga brottsutredande myndigheter? 7
Vilka konton kommer att omfrågas? 7
Hur ska historiska uppgifter hanteras? 7
Kommer manuella frågor kvarstå? 7
Kan vi få information om projektet på andra språk än svenska? 7
Hur hänger Skatteverkets Mekanismen och finansiella frågor ihop? 8

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 anslutning.

För att påbörja en anslutning 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 anslutning 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-meddelanden 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, namn+födelsedatum+plats => 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. Gränsen för antalet transaktioner är 20 000. Vid flera transaktioner 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.

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. Polismyndigheten utreder fortsatt frågan hur kortnumret ska vara utformat i svaret till Polismyndigheten. Mer information kommer när beslut är fattat.

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)

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 kreditinstitutet inte ansluter sig i tid?

Det finns en övergångsbestämmelse i föreskriften som innefattar en övergångsperiod. Övergångsperioden tar slut 31 december 2023. Polismyndigheten kommer att fortsätta skicka begäran som vi gör idag till de kreditinstitut som inte har anslutit sig. När övergångsperioden är slut kommer Polismyndigheten börja skicka anmälningar till Finansinspektionen gällande att kreditinstitutet 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 standariserade lösningen?

Föreskriften täcker samtliga brottsutredande myndigheter och polisens framtagna standard kommer att kunna användas av dessa myndigheter. Föreskriften kan du läsa på polisen.se.

Vilka är övriga brottsutredande myndigheter?

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

Vilka konton kommer att omfrågas?

Lagstiftningen och tillhörande föreskrifter reglerar endast begäran om information som omfattas av 1 kap. 11 § lagen (2004:297) om bank- och finansieringsrörelse. Konton som efterfrågas kan se olika ut och ha olika funktioner hos olika institut. Det går därför inte att bedöma varje specifikt konto utan närmare kännedom om omständigheterna i det enskilda fallet. Detta innebär att i slutändan är det upp till varje enskilt institut att göra bedömningen om just deras konton omfattas av lagstiftningen.

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 tidsspann 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. Manuella frågor kommer att kvarstå då ISO-standarden har vissa begränsningar gällande vilken information som kan hanteras. Tex kan utredare behöver inhämta underskrivna avtal. Även vissa kompletterande frågor kan behöva ställas via ett manuellt flöde (e-postadress).

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

Information och dokumentation från polisen finns endast på svenska. Gällande ISO-standarden 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 hos vilka kreditinstitutet. Läs mer om Konto- och värdefackssystem, Mekanismen, på Skatteverkets hemsida.