NTAES

Nyere betalingstjenester

TRUSSELVURDERING

Nasjonalt tverretatlig analyse- og etterretningssenter

Publikasjonens tittel: Nyere betalingstjenester – Trusselvurdering
Utgitt: juni 2017
Utgitt av: Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES)
Kontakt: post@ntaes.no
Postadresse: c/o ØKOKRIM, Postboks 8193 Dep, N-0034 Oslo
Besøksadresse: C.J. Hambros plass 2, 0164 Oslo

Illustrasjoner: Shutterstock
Grafisk design: ØKOKRIM

Forord

Nasjonalt tverretatlig analyse- og etterretningssenter (NTAES) har utarbeidet trusselvurderingen på oppdrag fra Det sentrale samarbeidsforum (DSSF). Trusselvurderingen beskriver hvordan nye betalingstjenesters manglende sporbarhet utgjør en trussel for etatenes arbeid med bekjempelse av økonomisk kriminalitet.

Til grunn for trusselvurderingen ligger grunnlagsdokumentet. Her beskrives nyere betalingstjenester, deres sporbarhet, bruk av tjenestene innen økonomisk kriminalitet samt kontrolletatenes erfaringer med nyere betalingstjenester.

Det fremkommer av trusselvurderingen at nyere betalingstjenester benyttes når økonomisk kriminalitet begås. På grunn av rask teknologisk utvikling og et stadig økende antall tjenester å velge mellom er det sannsynlig at bruken av tjenestene vil øke i fremtiden.

Innholdsfortegnelse

Forord 3
Sammendrag 5
Innledning 7
Forhåndsbetalte kort 8
Utenlandsk trussel 8
Vouchers 10
Vouchers i fremtiden 10
E-wallets 11
E-wallets i fremtiden 11
Betalingsformidlere 12
Betalingsformidlere i fremtiden 12
Virtuell valuta 13
Utvikling 13
Bruk 14
Regulering 15
Virtuell valuta i fremtiden 15
Vedlegg 1 Metodebeskrivelse 16
Vedlegg 2 Sannsynlighetsgrader 18

Sammendrag

Flere nye betalingstjenester kjennetegnes av lite gjennomsiktighet og sporbarhet. Dette vanskeliggjør identifisering av avsender/mottaker i finansielle transaksjoner og utgjør en trussel mot etatenes bekjempelse av økonomisk kriminalitet og annen profittmotivert kriminalitet. Tjenestene tiltrekker seg kriminelle som ønsker å skjule spor.

Kryptovaluta, forhåndsbetalte kort (norske og utenlandske), vouchers, e-wallet og betalingsformidlere er tjenestene som utpeker seg.

Følgende momenter utfordrer etatenes mulighet for identifisering og innhenting:

- *Rapportering til norske myndigheter*. E-pengeforetak og vekslere av kryptovalutaer har ikke samme krav til rapportering til norske myndigheter som finansinstitusjoner har. Dette gir politi- og kontrolletatene utfordringer knyttet til identifisering av aktører.
- *Høy grad av hemmelighold*. Mange av tjenestetilbyderne er utenlandske, gjerne hjemmehørende i land tradisjonelt forbundet med høy grad av hemmelighold. Dette gir politi- og kontrolletatene utfordringer knyttet til innhenting.
- *Anonymitet*. En kunde kan velge å være anonym, eller oppgi personopplysninger som ikke verifiseres, og kan foreta innskudd og uttak av penger gjennom tjenester som tilbyr anonyme grensekryssende transaksjoner.
- Anonymitet er ofte knyttet opp mot beløpsstørrelse. Kravet til identifisering øker proporsjonalt med beløpsstørrelsen.

Foreslåtte endringer til det 4. hvitvaskingsdirektivet, skattemyndighetenes utveksling av finansielle kontoopplysninger etter Common Reporting Standard (CRS) og et pågående lovarbeid om hvem som er rapporteringspliktig til valutaregisteret, forventes å virke risikoreduserende.

Utviklingen av ny teknologi og nye betalingstjenester øker i omfang – raskt. Tjenestene er bygd opp forskjellig og det kreves ulik fremgangsmåte for å identifisere avsender og/eller mottaker. Dette vil kreve mer av etatenes arbeid med å identifisere avsender og/eller mottaker i årene fremover.

En felles offensiv samhandling vil kunne bidra til at etatene gjør hverandre gode og demmer opp for trusselen.

Innledning

Rapporten utarbeidet av NTAES til DSSF vurderer truslene etatene står overfor med nyere betalingstjenester og manglende sporbarhet.

Det er tatt utgangspunkt i grunnlagsdokumentet for nyere betalingstjenester, som deler nyere betalingstjenester inn i følgende hovedkategorier:

Forhåndsbetalte kort
Internettbaserte betalingstjenester
Mobile betalingstjenester
Virtuell valuta

Tjenestene er vurdert med bakgrunn i politi- og kontrolletatenes erfaringer, fakta om tjenestene og informasjon fra åpne kilder. Tjenestene er vurdert på grunnlag av syv vurderingskriterier som er vektet likt. Kriteriene er anonymitet, tilgjengelighet, bruk og utbredelse, sporbarhet, beløpsstørrelse, kompetanse og kombinasjonspotensialet.[1]

Betalingstjenestene som beskrevet her er de som har blitt vurdert i å utgjøre størst trussel for etatenes arbeid med bekjempelse av økonomisk kriminalitet:

Forhåndsbetalte kort

- Norske anonyme kort
- Utenlandske personlige og anonyme kort

Internettbaserte betalingstjenester

- Vouchers
- E-wallets
- Betalingsformidlere

Virtuell valuta

Trusselvurderingen skal gi politi- og kontrolletatene et felles grunnlag for å vurdere hvilken trussel de nyere betalingstjenestene og deres manglende sporbarhet representerer.

[1] Vedlegg 1 Metodebeskrivelse

Forhåndsbetalte kort

Forhåndsbetalte kort blir benyttet ved utøvelse av økonomisk kriminalitet. Kriminelle benytter seg av mulighetene forhåndsbetalte kort representerer for å unngå politi- og kontrolletatenes søkelys.

Forhåndsbetalte personlige og anonyme kort kan brukes til å overføre penger til både nye betalingstjenester og tradisjonelle betalingsmetoder.

Norske anonyme forhåndsbetalte kort utgjør en moderat trussel innen økonomisk kriminalitet. De benyttes i stor grad til taktiske valg som et verktøy i den kriminelle handlingen for å skjule spor. Et utvalg straffesaker som er gjennomgått viser at kortene benyttes til å hvitvaske et mindre utbytte, for å skjule spor og overføre anonymt i innland og utland. Det er ingen antallsbegrensning ved kjøp av anonyme kort. Utsalgssteder for anonyme forhåndsbetalte kort er ikke underlagt rapporteringsplikt etter hvitvaskingsregelverket.

Utenlandsk trussel

Utenlandske anonyme og personlige forhåndsbetalte kort utgjør en betydelig større trussel enn norske forhåndsbetalte kort fordi beløpsgrensene ved bruk er alt fra 15 000 kroner i uken, til ubegrenset. Også bruk av tradisjonelle utenlandske bankkort utgjør en trussel for etatenes bekjempelse av økonomisk kriminalitet, fordi det er høye beløpsgrenser, og vanskelig å avdekke hvem som bruker kortene.

Trusselen bekreftes ved søk i valutaregisteret. Det gjøres eksempelvis kontantuttak fra samme minibank med beløp mellom 10 000 og 15 000 kroner, samme dag, fra forskjellige kort utstedt av samme bank.

Bruken av utenlandske kort i Norge øker gradvis og det finnes ingen indikatorer på at trenden vil snu i fremtiden.[2]

ØKOKRIM har uttalt følgende om utenlandske kort:

> «Utbytte fra kriminalitet i Norge plasseres gjerne i utlandet. Skal midlene benyttes til forbruk, gjøres det ofte med utenlandske bankkort i Norge. Da unngår aktørene risikoen med å overføre pengene til en norsk bankkonto de kan knyttes til.»[3]

Politi- og kontrolletatene har sett at forhåndsbetalte kort i økende grad benyttes ved utøvelse av økonomisk kriminalitet.[4]

I forslag til endringer i 4. hvitvaskingsdirektiv foreslås å redusere grensen for krav til identifikasjon ved utstedelse av e-penger fra 250 til 150 Euro. Det foreslås videre at forhåndsbetalte kort utstedt utenfor EU bare skal kunne brukes i EU når disse oppfyller krav som svarer til 4. hvitvaskingsdirektiv.[5]

---

[2] Valutaregisteret
[3] ØKOKRIM trusselvurdering, 2015-2016, side. 17
[4] Fremgår av svar på spørreskjema til ulike politidistrikt
[5] Økonominytt fra EU-delegasjonen, Nr. 2 – Februar 2017

Det er allerede lave beløp som utløser krav til kundekontroll, og gjennomgang av et utvalg straffesaker viser at det er lettvint å omgå krav til legitimasjon hos enkelte utenlandske aktører.[6] Det er derfor lite sannsynlig at endrede krav til identifikasjon i nevneverdig grad vil påvirke den trusselen forhåndsbetalte kort representerer.

Om et forbud mot kort utstedt utenfor EU som ikke oppfyller krav som svarer til 4. hvitvaskingsdirektiv vil påvirke trusselen, avhenger av om implementeringen av forbudet er vellykket. På grunn av usikkerhet knyttet til hvorvidt forbudet kan gjennomføres, er det like sannsynlig som usannsynlig at de foreslåtte endringene vil påvirke trusselen som forhåndsbetalte kort utstedt utenfor EU, representerer.

Det er meget sannsynlig at bruk av forhåndsbetalte kort utgjør en høy trussel mot etatenes bekjempelse av økonomisk kriminalitet fremover.

[7]

[6] Vilkårene for forenklet kundekontroll følger av hvitvaskingsforskriften § 10, jf. hvvl. § 13
[7] Vedlegg 2 Sannsynlighetsgrader

Vouchers

Kjøp av og bruk av vouchers med lave beløp er anonymt og kan blant annet kjøpes kontant.[8] Kjøp av vouchers med høye beløp krever legitimering, men det er varierende krav til legitimasjonsdokument. Ved kjøp av vouchers på utenlandsk nettsted ved bruk av kort vil beløpet fremkomme i valutaregisteret. Dersom etatene ønsker å få kunnskap om hva pengene er brukt til, må henvendelse rettes til utenlandsk tjenestetilbyder, noe som ofte er tidkrevende. Ikke alle etater har hjemmel til innhenting fra utenlandsk tjenestetilbyder.

Voucherne eller kodene tar liten plass og kan enkelt fraktes eller sendes til personer over hele verden for eksempel ved bruk av SMS eller e-post. Dette gjør tjenesten egnet til å sende kriminelt utbytte ut av landet.

I norske butikker selges vouchers med begrensning på inntil 1 000 kroner. For å kunne unndra større beløp må man kjøpe flere vouchers. Utenlandske tilbydere selger vouchers med vesentlig høyere beløp. Én tjeneste selger enkeltvouchers til 50 000 kroner, uten antallsbegrensning. Høye beløpsgrenser uten begrensninger i antall kjøp, kombinert med potensialet for å være anonym medfører at tjenesten utgjør en høy trussel for etatenes bekjempelse av økonomisk kriminalitet.

Straffesaksdokumenter viser at vouchers hovedsakelig benyttes til å gjøre innskudd på brukerkonto hos utenlandske spillselskap. Man kan benytte seg av betalingskort for uttak.

Vouchers i fremtiden

Det er i hvitvaskingsregelverket foreslått en reduksjon i beløpsgrenser for krav om legitimering. Det er allerede lave beløp som utløser krav til kundekontroll. Forestående risikoreduserende tiltak forventes derfor ikke å utgjøre en vesentlig forskjell for potensialet for bruk av vouchers ved utøvelse av økonomisk kriminalitet.

Bruk av vouchers i forbindelse med økonomisk kriminalitet forventes å være stabil.

Det er sannsynlig at bruk av vouchers utgjør en høy trussel mot etatenes bekjempelse av økonomisk kriminalitet fremover.

[8] Under 250 Euro

E-wallets

E-wallet-tjenestene er ved flere tilfeller benyttet i forbindelse med økonomisk kriminalitet. E-wallets er enkelt tilgjengelig på nett, lette å bruke og kan benyttes i et stort utvalg av norske og utenlandske nettbutikker. Tjenestene tilbys over hele verden. Dette gjør tjenesten egnet til å flytte utbytte av økonomisk kriminalitet ut av landet med begrenset sporbarhet.

Tilbydere av e-wallet er utenlandske, men de fleste av dem har bankkonto i Norge. Dette innebærer at når norske kunder gjør innskudd på e-wallet, fremkommer ikke dette av valutaregisteret.

At tilbyderne er utenlandske og ofte hjemmehørende i land med høy grad av hemmelighold, gjør opplysningene mindre tilgjengelige for politi- og kontrolletatene. Enkelte etater har variert erfaring med innhenting fra utenlandske tilbydere og andre har ikke mulighet for å innhente opplysninger fra utenlandske tilbydere. Der innskudd gjøres ved bruk av andre anonyme betalingstjenester vil det være vanskelig å få kunnskap om at pengene er satt inn på e-walleten. Dette gjør tjenesten egnet til å skjule utbytte fra kriminell aktivitet.

E-wallet er i tillegg mulig å kombinere med flere av de anonyme nyere betalingstjenestene, blant annet forhåndsbetalte kort og vouchers, for å sette inn og for å ta ut midler fra e-walleten.

Når pengene er satt inn kan de overføres til andre brukere av e-wallet-tjenesten eller til nettbutikker over hele verden. Transaksjonene vil da være knyttet til e-wallet-tilbyderen. Dette vanskeliggjør arbeidet med å avdekke mottaker av transaksjonen. Det vil også være vanskelig å avdekke at en person har mottatt penger i e-walleten. Beløpet kan da benyttes til handel og overføring uten at det vil fremkomme av valutaregisteret eller skattemeldingen.

Det er også avdekket at e-wallet har blitt benyttet til kjøp av ulovlige varer i utlandet.

E-wallets i fremtiden

I likhet med vouchers vil e-wallets bli berørt av forslaget til reduksjon i beløpsgrensene knyttet til legitimasjonskravet i hvitvaskingsregelverket.

Det er ingen holdepunkter for å si at bruk av e-wallets i forbindelse med økonomisk kriminalitet er forventet å avta. De forestående risikoreduserende tiltak forventes ikke å utgjøre en vesentlig forskjell for bruk av e-wallets innen økonomisk kriminalitet.

Det er sannsynlig at bruk av e-wallets utgjør en høy trussel mot etatenes bekjempelse av økonomisk kriminalitet fremover.

Betalingsformidlere

Betalingsformidlere benyttes for å flytte penger på tvers av landegrenser gjennom formidlerens betalingsnettverk. Alle tilbyderne av slike tjenester i Norge i dag er utenlandske selskaper. Betaling til betalingsformidler kan skje fra ordinær bankkonto. Transaksjonen vil da fremgå av brukers kontoutskrift, men det vil ikke fremgå av kontoutskriften hvem den endelige mottakeren er. Det vil være krevende for politi- og kontrolletatene å finne ut hvor pengene overføres, noe som gjør tjenesten egnet til bruk i forbindelse med økonomisk kriminalitet.

Betalingsformidlere disponerer ofte en norsk bankkonto, som pengene rutes til i første omgang. Transaksjonen til mottaker vil vises i valutaregisteret med betalingsformidleren som avsender, gjerne i en større forsendelse sammen med flere andre transaksjoner. Politi- og kontrolletatene vil i slike tilfeller ikke finne transaksjonen på vedkommende i valutaregisteret. Betalingsformidlerne har informasjonen om hvem som er både mottaker og avsender.

Betalingsformidlere har blitt benyttet ved utøvelse av økonomisk kriminalitet. I ett eksempel ble inntekter unndratt fra beskatning ved å sende penger til utlandet gjennom betalingsformidler.[9] Pengene settes inn på utenlandsk bankkonto i land tradisjonelt forbundet med høy grad av hemmelighold, og tas ut i Norge ved bruk av debetkort utstedt i utlandet.

Betalingsformidlere i fremtiden

Det er ingen holdepunkter for å si at bruk av betalingsformidlere ved utøvelse av økonomisk kriminalitet vil avta.

Det er sannsynlig at bruk av betalingsformidlere utgjør en høy trussel mot etatenes bekjempelse av økonomisk kriminalitet fremover.

[9] Frostating lagmannsretts dom 29. oktober 2010 (LF-2010-55733).

Virtuell valuta

Utvikling

Økningen i bruk og verdi av virtuell valuta utgjør en tydelig trussel i bekjempelsen av økonomisk kriminalitet. Kryptovaluta har høyest markedsandel blant virtuell valuta, men tendenser viser også en økning i virtuell valuta som benyttes til pyramidespill.[10] Potensialet for å overføre store beløp i kombinasjon med anonymitet er attraktivt for kriminelle. Markedet for kryptovaluta og aksept for kryptovaluta som betaling er i kontinuerlig vekst og i bruk både i det legale markedet og på det mørke nettet.

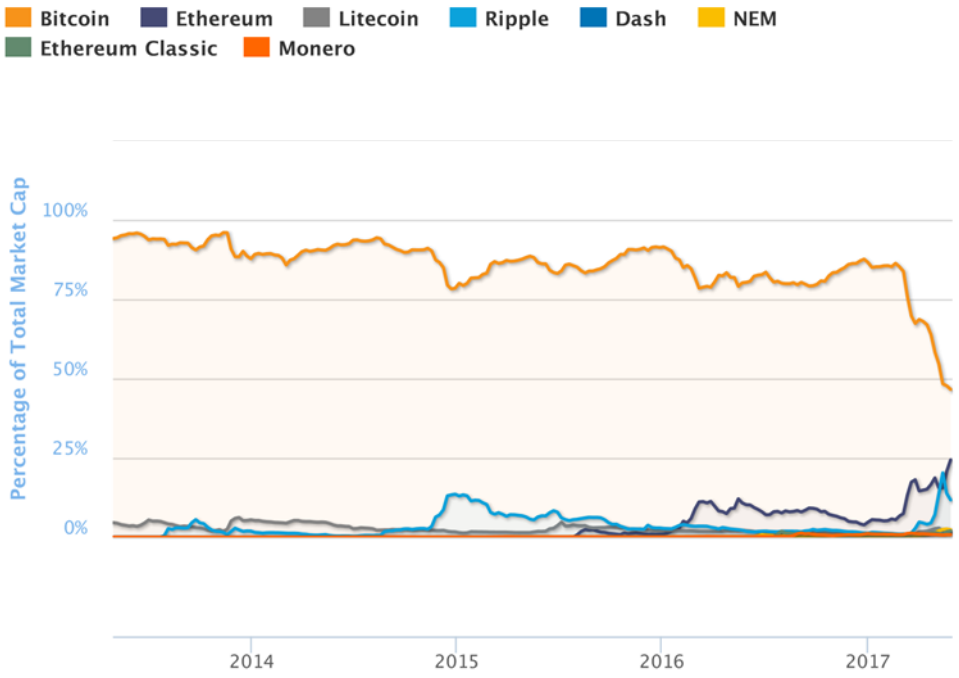
Bruken av kryptovaluta – og verdien av denne – har økt kraftig. Én Bitcoin har i løpet av det siste året økt i verdi med 2 210 US dollars, fra 579 US dollars til 2 789 US dollars per 8.6.2017.[11] Ordinære finansinstitusjoner utreder muligheten for, eller realiserer allerede kryptovalutatransaksjoner. Det eksisterer en rekke valutavekslere som veksler fra kryptovaluta til reell valuta, og antall transaksjoner mellom norske parter og utenlandske vekslere har økt hver termin de siste årene.[12]

[10] http://e24.no Lotteritilsynet sjekker pyramide tips
[11] www.coindesk.com Bitcoin prisindex
[12] Søk i valutaregisteret på vekslerne Kraken og Bitstamp

Bruk

Brukere av kryptovaluta er i utgangspunktet anonyme, men likevel i ulik grad anonyme, ved at forskjellig informasjon vises i de ulike blockchainene.[13] Det finnes 863 kryptovalutaer per 8.6.2017.[14] Dette tilsvarer 863 unike blockchainteknologier.

Grafen under viser at andre kryptovalutaer enn Bitcoin øker i markedsandel og i verdi. Dette er kryptovalutaer som aksepteres som betaling på det mørke nettet og som enkelt kan veksles til reell valuta gjennom utenlandske valutavekslere.



[15]

Figur: Klippet ut fra nettsiden coinmarketcap.com

Brukere av ulike kryptovalutaer kan tilsløre spor ved forsiktig og riktig bruk av tjenesten. Brukerfeil og ekstern informasjon har inntil nå gjort det mulig å identifisere brukere bak transaksjoner av kryptovaluta.[16]

Kryptovaluta benyttes også til spekulasjon. Det er stor sannsynlighet for at personer i Norge har store verdier i kryptovaluta som ikke er oppgitt til myndighetene.[17] Kriminelle som godtar Bitcoin som betaling har fått en økonomisk fordel som følge av verdistigningen til kryptovaluta.

[13] Blockchainene har forskjellige nøkler, transaksjonsvisning og grad av anonymitet.
[14] https://coinmarketcap.com Liste over kryptovalutaer
[15] https://coinmarketcap.com Markedsverdi av ulike kryptovalutaer
[16] Ved tvangsmidler, visitasjon, avhør og opplysninger fra internasjonale samarbeidspartnere.
[17] https://localbitcoins.com Norske selgere som har over 500+ BTC (per 8.6.2017 vil det si drøyt tolv millioner NOK)

Regulering

Virtuell valuta er ikke særskilt regulert i noe lovverk. Dette skaper store utfordringer for politi- og kontrolletatene. Uten nødvendig regulering har etatene få verktøy å benytte seg av i bekjempelse av kriminalitet med bruk av kryptovaluta. Lokale vekslere har informasjon om kjøpere/brukere av kryptovaluta, men de er ikke underlagt rapporteringsplikt etter hvitvaskingsregelverket. Dette gjelder også utenlandske vekslere.

En tjeneste i Sveits har allerede fått konsesjon til å utstede Bitcoin debetkort til kunder over hele verden.[18] Kunder gis muligheten til å benytte debetkort til å betale med Bitcoins. Det er meget sannsynlig at flere tilbydere vil tilby lignende tjenester, noe som kan utgjøre en potensielt høy trussel i fremtiden.

Virtuell valuta i fremtiden

Det er meget sannsynlig at virtuell valuta og kryptovaluta vil eksistere i årene fremover. Teknologien og utviklingen innenfor de ulike valutaene endrer seg i tråd med behovet i markedet, øvrig teknologisk utvikling og brukernes behov.[19]

Det vil være krevende for politi- og kontrolletatene i tiden fremover å opparbeide seg nødvendig kompetanse om de ulike blockchainteknologiene. Selv om etatene opparbeider kunnskap om de ulike kryptovalutaene, vil utfordringen være å samle informasjon om brukere bak transaksjonene.

Det er stor sannsynlighet for at nettsteder som befinner seg på det mørke nettet vil akseptere flere ulike kryptovalutaer som betaling for salg av ulovlige varer.[20] Monero er et eksempel på en kryptovaluta med store begrensninger i sporbarhet, som har blitt akseptert som betaling på nettsteder med salg av ulovlige varer. Monero er kjent for å være totalt anonym og umulig å spore. Ethereum er en annen kryptovaluta som er i sterk vekst, både verdimessig og i markedsandel. Ethereum har også blitt akseptert som betaling på det mørke nettet.

I forslag til endringer i 4. hvitvaskingsdirektiv foreslås at tilbydere av vekslingstjenester mellom virtuelle penger og fysiske penger, såkalte wallet-providers, skal omfattes av direktivet, og dermed gjøres rapporteringspliktige etter hvitvaskingsregelverket.[21] På grunn av usikkerhet om hvordan dette kan gjennomføres i praksis, er det lite sannsynlig at dette vil påvirke trusselen ved bruk av virtuell valuta.

Det er meget sannsynlig at bruk av virtuell valuta utgjør en høy trussel mot etatenes bekjempelse av økonomisk kriminalitet fremover.

[18] Se tilbyderens hjemmeside https://xapo.com
[19] www.huffingtonpost.com What is the future of cryptocurrency
[20] I 2016–2017 har flere nettsteder på det mørke nettet åpnet muligheten for bruk av en ny kryptovaluta som betaling: https://alphabaymarket.com Alphabay market announced will accept ethereum
[21] Wallet-providers er leverandører av digitale lommebøker som gir tilgang til virtuelle penger

Vedlegg 1 Metodebeskrivelse

De fire hovedkategoriene av tjenester er brutt videre ned for å muliggjøre en vurdering av hvilken trussel den enkelte tjeneste representerer. Inndelingen er som følger:

- Forhåndsbetalte kort
  - Norske
    - Anonyme
    - Personlige
  - Utenlandske kort
    - Anonyme
    - Personlige
- Internettbaserte betalingstjenester
  - E-wallets
  - Vouchers (open loop)
  - Betalingsformidlere
  - Tredjepartstilbyder
  - Faktureringstjeneste
- Mobile betalingstjenester[22]
- Virtuell valuta
  - Kryptovaluta

Tjenestene er vurdert på grunnlag av syv vurderingskriterier som er vektet likt:

Anonymitet – Hvilke krav som stilles til identifisering av vedkommende som bruker tjenesten og hvor lett tjenesten kan misbrukes (eksempelvis ved bruk av stjålet kort, bruk av falsk identitet og så videre)

Tilgjengelighet – Hvor enkelt det er å skaffe/ta i bruk tjenesten. Videre om det er mange brukersteder, og om pengene kan overføres til utlandet ved bruk av tjenesten.

Bruk /utbredelse – I samfunnet generelt og innen økonomisk kriminalitet.

Sporbarhet – Hvor enkelt det er for etatene å kartlegge forhold som kan identifisere bruker av tjenesten, og hvor enkelt det er å finne transaksjonen.

Beløpsstørrelse – Hvor store beløp som kan overføres ved bruk av tjenesten.

[22] Ved vurdering av mobile betalingstjenester er kun tjenestene som i grunnlagsdokumentet benevnes som "Betalingsformidler", eksempelvis MobilePay og VIPPS, tatt med. Dette fordi de øvrige kategoriene enten ikke tilbys i Norge, eller også tilbys på internett, og derfor er vurdert under internettbaserte betalingstjenester

Kompetanse – Hvilken kunnskap etatene har om tjenestene.

Kombinasjon – I hvilken grad tjenesten lar seg kombinere med andre betalingstjenester.

Med utgangspunkt i vurderingskriteriene er det gjort en skjønnsmessig vurdering av tjenestene, basert på politi- og kontrolletatenes erfaringer, fakta om tjenestene og informasjon fra åpne kilder.

Tjenestene er vurdert mot kriteriene på en skala bestående av fem ulike nivåer, representert ved fargene Rød / Oransje / Gul / Lysegrønn / Grønn / Blå, der fargen rød tilsier at tjenesten utgjør høy trussel og fargen grønn tilsier at tjenesten utgjør lav trussel. Fargen blå innebærer at informasjonsgrunnlaget er for svakt til å vurdere trusselnivået. Hvordan hver enkelt tjeneste er vurdert mot de syv vurderingskriteriene fremkommer av matrisen under.

Det er endelig gjort en vurdering av hvorvidt risikoreduserende eller risikoøkende elementer kan forventes å påvirke hvilken trussel tjenesten vil utgjøre fremover.

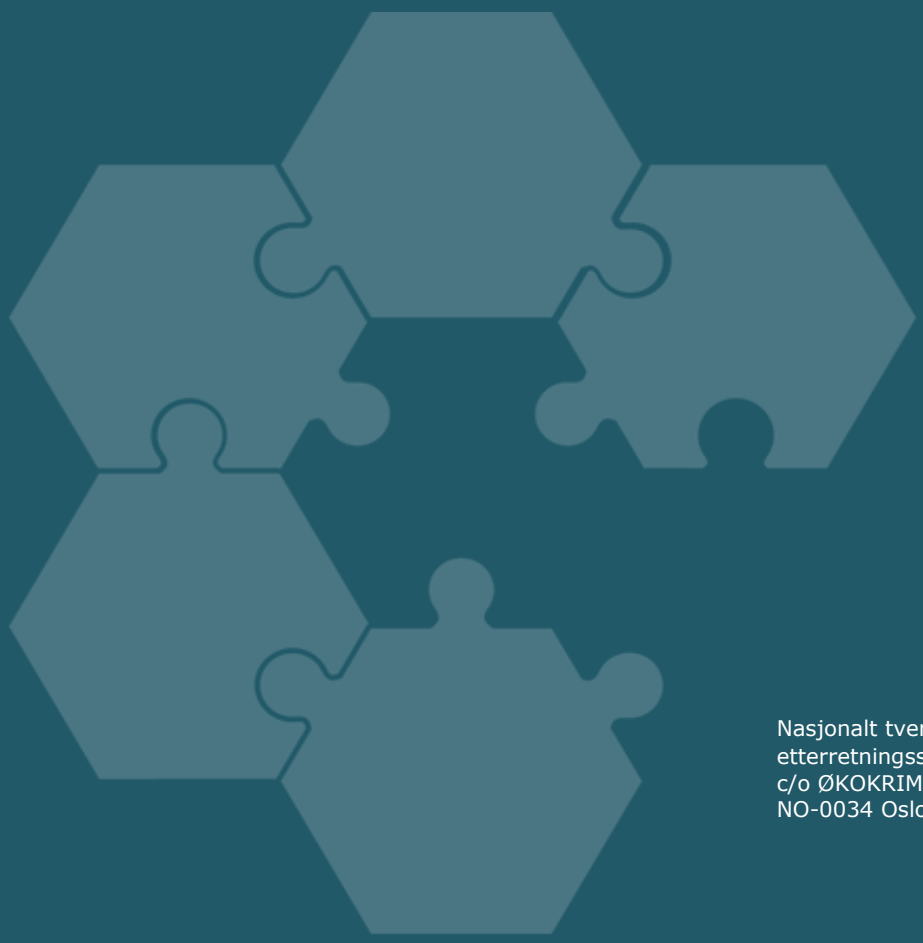
	Forhåndsbetalte kort (open loop)				**Internett**					**Mobil**	**Virtuell valuta**
	Norske		**Utenlandske**								
	Anonyme	Personlige	Anonyme	Personlige	E-Wallet	Vouchers (open loop)	Betalingsformidler	Tredjepartstilbyder	Fakturering stjeneste	Mobile betalingstjenester	Kryptovaluta
Anonymitet											
Tilgjengelighet											
Bruk/utbredelse											
Sporbarhet											
Beløpsstørrelse											
Kompetanse											
Kombinasjon											

	Høy trussel
	Moderat høy trussel
	Moderat trussel
	Moderat lav trussel
	Lav trussel
	Ukjent

Vedlegg 2 Sannsynlighetsgrader

For å beskrive hvor stor sannsynlighet det er for at de nyere betalingstjenestene og deres manglende sporbarhet representerer en trussel fremover er det benyttet sannsynlighetsgrader. Disse er hentet fra Etterretningsdoktrinen for politiet:

Sannsynlighetsgrader	Prosent sannsynlighet	Synonymer
Meget sannsynlig	>90	Vi er overbevist om…
Sannsynlig	60-90	Vi fester stor tillit til... Vi tror at…
Like sannsynlig som usannsynlig	40-60	Det er mulig at... 50/50-sjanse... Det er indikatorer…
Lite sannsynlig	10-40	Det er tvilsomt at..
Usannsynlig	<10	Det er nesten umulig… Det er svært tvilsomt…



Nasjonalt tverretatlig analyse- og etterretningssenter
c/o ØKOKRIM, Postboks 8193, dep.,
NO-0034 Oslo