2021

Temaundersøgelse om brugen af stærk kundeautentifikation i e-handlen

Indholdsfortegnelse

1. Indledning

1.1 Baggrund for undersøgelsen

Stærk kundeautentifikation (SCA) – også kaldet tofaktor-autentifikation – indebærer, at en betaler skal bruge mindst to faktorer til at godkende en betaling. De to faktorer indbefatter noget, betaleren *ved* (f.eks. et password); noget, betaleren *har* (f.eks. en mobiltelefon, der kan modtage en engangskode); eller noget, betaleren *er* (f.eks. et fingeraftryk). Fysisk handel i Danmark har i længere tid benyttet SCA i form af chipkort (noget, betaleren *har*) og pinkode (noget, betaleren *ved*).

Ikke-fysisk handel, primært netbutikker, har derimod traditionelt set ikke benyttet SCA i vidt omfang i Danmark. Det ændrede sig med det reviderede betalingstjenestedirektiv (PSD2[1]), som indførte krav om SCA i forbindelse med alle elektroniske betalinger iværksat af brugeren, både i fysisk handel og i netbutikker[2].

Reglerne om brug af SCA indeholder også et krav om brug af såkaldt dynamisk tilknytning (dynamic linking) ved fjernbetalinger, herunder betalinger i netbutikker. Kravet indebærer blandt andet, at betaleren gøres opmærksom på transaktionsbeløbet og på betalingsmodtageren, i forbindelse med at betaleren gennemfører SCA[3].

Kravet om SCA trådte i kraft den 14. september 2019 for såvel fysisk som ikke-fysisk handel. Sektoren havde dog betydelige udfordringer med at efterleve to-faktor kravet for kortbetalinger i e-handlen. Den Europæiske Banktilsynsmyndighed (EBA) fastsatte derfor en forlænget implementeringsperiode med én fælleseuropæisk deadline for håndhævelsen af de nye regler den 1. januar 2021 for den ikke-fysiske handel. Målet med forlængelsen af implementeringsperioden var at undgå store forstyrrelser i e-handlen, der kunne opstå ved afviste betalinger. Udskydelsen ændrede dog ikke på, at reglerne om SCA trådte i kraft den 14. september 2019. Derfor har hæftelses- og ansvarsreglerne i lov om betalinger været gældende fra denne dato. Det betyder blandt andet, at betalingstjenesteudbydere i hele perioden har hæftet for alt misbrug af betalingskort, hvor der ikke har været benyttet SCA.

På baggrund af det lange og vanskelige implementeringsforløb har Finanstilsynet gennemført en temaundersøgelse om danske betalingstjenesteudbyderes brug af SCA ved kortbetalinger i e-handlen.

1.2 Afgrænsning af undersøgelsen

Finanstilsynet udvalgte ti kortudstedere og to kortindløsere[4], til undersøgelsen, som dermed dækker:

---

[1] Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF

[2] Kravene er implementeret i dansk ret i § 128, stk. 1, nr. 2, i lov om betalinger (betalingsloven).

[3] Når betaleren gennemfører SCA, skal det være tydeligt, hvilken betaling der godkendes. Det vil sige, at eksempelvis en SMS-besked med en engangskode også skal indeholde oplysninger om transaktionsbeløbet og betalingsmodtageren.

[4] En kortindløser sørger for, at der sendes besked fra butikken til kortudstederen om, at brugeren vil foretage en betaling. Kortindløseren sørger også sammen med kortudstederen for at pengene i sidste ende overføres til butikken.

- størstedelen af danske kortholdere
- størstedelen af danske betalingsmodtagere
- kortudstedere hos alle de tre fælles datacentraler (Bankdata, BEC og SDC)
- forskellige størrelser af pengeinstitutter.

Undersøgelsen omfatter brugen af SCA i perioden fra den 11. januar til den 30. april 2021 i netbutikker og forholder sig altså ikke til kortbetalinger i fysisk handel.[5] Undersøgelsen forholder sig heller ikke til betalinger i netbutikker gennemført som kontooverførsler, herunder kontooverførsler igangsat via en udbyder af betalingsinitieringstjenester.

Finanstilsynet har som led i undersøgelsen bedt virksomhederne om data for indrullering[6] af kortholdere og betalingsmodtagere i de relevante autentifikationsløsninger samt transaktionsdata for brugen af SCA, herunder data for misbrug af betalingskort. Institutterne blev desuden bedt om at besvare et kvalitativt spørgeskema om deres implementering af kravet om SCA.

Medmindre andet står skrevet, stammer de angivne data fra danske kortudstedere. Det vil sige, at data omhandler betalinger foretaget af danske kortholdere.

[5] For at sikre en stabil betalingsafvikling henover årsskiftet og for at undgå driftsmæssige forstyrrelser i julehandlen accepterede Finanstilsynet undtagelsesvist, at kravet i praksis skulle gælde for alle betalinger senest den 11. januar 2021.
[6] Ved "indrullering" forstås den proces, hvor en bruger tilmeldes en konkret autentifikationsløsning, og kortudstederen knytter brugerens identitet til autentifikationsløsningen. Her sikres det f.eks., at det er den rigtige bruger, der har telefonen, som modtager de SMS-engangskoder, som brugeren godkender en kortbetaling med.

2. Udviklingen i misbrug med betalingskort

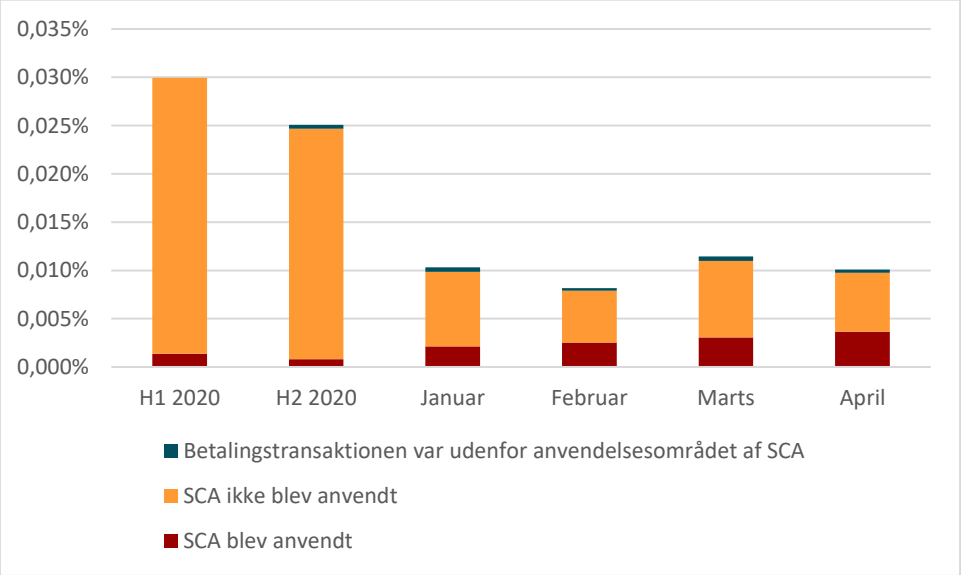
Formålet med at indføre kravet om SCA var at sænke misbruget med betalingskort og andre elektroniske betalingsformer.

Nedenfor gennemgås udviklingen i misbruget med betalingskort udstedt af de undersøgte kortudstedere.

Tallene viser, at andelen af svigagtige transaktioner er faldet markant, efter at SCA er blevet rullet bredt ud i januar 2021. Andelen af svigagtige kortbetalinger på internettet er faldet fra 0,03 pct. af alle transaktioner i første halvår af 2020 og 0,025 pct. i andet halvår 2020 til omkring 0,01 pct. i perioden fra januar til april 2021. Det fremgår af figur 1.

Der er dermed tale om et fald i misbruget på to tredjedele siden første halvår af 2020 i den udvalgte stikprøve.

Figur 1: Andel misbrugstilfælde ud af alle kortbetalinger



Note: At SCA ikke blev brugt kan både dække over, at betalingen ikke levede op til lovkravene, eller at der blev anvendt en lovlig undtagelse.

Finanstilsynet finder det tilfredsstillende, at kravet om anvendelse af SCA virker til at have haft en markant effekt på misbruget af betalingskort.

Tallene viser også, at andelen af tilfælde, hvor et betalingskort misbruges på trods af brugen af SCA, var stigende fra januar til april 2021. Det skyldes formentlig, at antallet af betalinger med SCA generelt er stigende og dermed alt andet lige vil udgøre en større andel af misbrugstilfælde. Udviklingen skyldes dog formentlig også, at svindlere gradvist bliver bedre til at misbruge betalingskort på trods af SCA. I takt med at kortudstederne implementerer nye løsninger til at nedbringe misbruget, arbejder svindlere på at udvikle nye metoder til at omgå sikkerhedsforanstaltningerne og fortsætte misbruget på trods af det øgede sikkerhedsniveau.

Samtidig med at antallet af svindeltilfælde er faldet markant, bliver der i gennemsnit svindlet for højere beløb pr. tilfælde. Dette kan blandt andet skyldes, at de nye sikkerhedskrav gør det mere besværligt for svindlerne, så de i stedet går efter større beløb.

Finanstilsynet mener, at tallene understreger behovet for, at betalingstjenesteudbydere løbende vurderer effekten af de implementerede løsninger, justerer de tekniske systemer, uddanner kortholderne i SCA og gør andre relevante tiltag, der kan sikre kortholderne mod nye typer misbrug.

Svindel med abonnementer
I den nærmere gennemgang af data har det vist sig, at der særligt er sket en stigning i andelen af svig ved grænseoverskridende tilbagevendende betalinger – f.eks. abonnementer - hos danske kortindløsere. Det gælder hovedsageligt i forhold til transaktioner, der omfatter *udenlandske kortholdere*.

Svindlen sker særligt via abonnementer. SCA bliver brugt ved oprettelsen af et abonnement, hvorefter de løbende betalinger sker automatisk. Der er i denne særlige kategori af betalinger sket mere end en tidobling i andelen af svigagtige transaktioner. Grænseoverskridende tilbagevendende betalinger udgør en væsentlig del af den totale stigning. Finanstilsynet vil derfor følge særligt op på udviklingen på dette område og på, hvordan svindel kan reduceres.

Det er Finanstilsynets indtryk, at det stigende misbrug ved grænseoverskridende tilbagevendende betalinger er udtryk for, at svindlere søger derhen, hvor de kan opnå størst udbytte med én enkelt brug af SCA. Ved opsætning af et abonnement, er det muligt med ét enkelt SCA at igangsætte en fortløbende betalingsstrøm. Med dette ene SCA kan en svindler få en betaler til at gennemføre SCA ved hjælp af manipulation eller ved at gøre en købsproces meget uoverskuelig. Hvis det lykkedes for svindleren, har denne opnået potentielt mange overførsler med et enkelt SCA.

Finanstilsynet har indledt en dialog med kortindløserne om, hvad årsagen til misbruget er, og hvordan det nedbringes. Situationen understreger også behovet for, at kortudstederne løbende informerer kortholderne om nye typer misbrug og uddanner kortholderne i, hvordan de beskytter sig mod misbruget.

Hovedkonklusioner

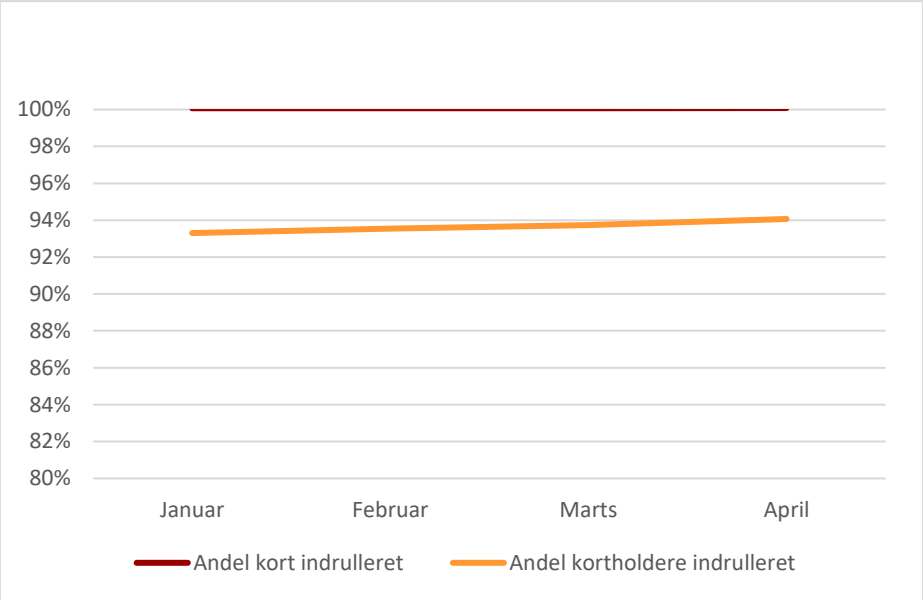
- Andelen af misbrugstilfælde er faldet med to tredjedele fra første halvår af 2020 til april 2021 i den udvalgte stikprøve. Samtidig med at antallet af svindeltilfælde er faldet markant, bliver der i gennemsnit svindlet for højere beløb pr. tilfælde.
- Betalingstjenesteudbydere bør løbende vurdere effekten af de implementerede løsninger, justere de tekniske systemer, uddanne kortholderne i SCA og gøre andre relevante tiltag, der kan sikre kortholderne mod nye typer misbrug.
- Svindlen med abonnementer er stigende, og Finanstilsynet vil derfor følge særligt op på udviklingen på dette område med kortindløserne, og på hvordan svindel kan reduceres.

3. Brug af SCA

3.1 Indrullering af kortholdere og brug af autentifikationsløsninger

Alle udstedte kort var klar til at gennemføre SCA i januar 2021, og omkring 94 procent af alle kortholdere var indrulleret i en SCA-løsning i april 2021. Det fremgår af figur 2.

Figur 2: Andel af kortholdere og betalingskort, der kan gennemføre SCA



Note: Data for indrullering af kortholdere er baseret på estimater, da kortudstedere ikke er i besiddelse af alle oplysninger om kortholders indrullering i NemID, herunder om kortholder bruger NemID-app'en, nøgleviser eller nøglekort.

Finanstilsynet finder overordnet, at indrullering af kortholdere i løsninger, der lever op til kravene om SCA, er foregået tilfredsstillende.

I april 2021 var ca. 6 pct. af kortholderne fortsat ikke indrulleret i en SCA-løsning. Det kan dog skyldes, at nogle kortholdere ikke ønsker at handle online og derfor ikke opretter et kodeord. Derudover tilbyder nogle kortudstedere ikke kortholdere under 13 år at indrullere sig i en SCA-løsning. Er man ikke indrulleret i en SCA-løsning, kan man som udgangspunkt ikke handle på internettet.

Der var en overgang problemer med indrullering af kortholdere, der ikke benyttede NemID-app eller NemID-nøgleviser[7]. De fleste kortudstedere har angivet, at de har implementeret en løsning, der gør det muligt at oprette et kodeord uden brug af NemID.

[7] Det kræver brug af en anden SCA-løsning at indrullere en bruger i en SCA-løsning via en fjernkanal (f.eks. gennem mobilbank, netbank eller en anden hjemmeside). Da NemID-nøglekortet og andre papirbaserede kodelister kan fotokopieres, anses de ikke for at overholde reglerne om, at besiddelseselementer skal være tilstrækkeligt beskyttet mod kopiering. NemID-nøglekortet kan derfor ikke bruges til indrullere kortholder i en anden autentifikationsløsning, da autentifikation med nøglekortet ikke anses som stærk kundeautentifikation.

Finanstilsynet har indtryk af, at dette har løst en meget stor del af de problemer, der har været for restgruppen af kortholdere uden NemID-app eller nøgleviser. Det er dog vigtigt, at kortudstederne fortsat arbejder på at sikre, at alle, der ønsker at handle på internettet, kan indrullere sig i en løsning, der gør det muligt.

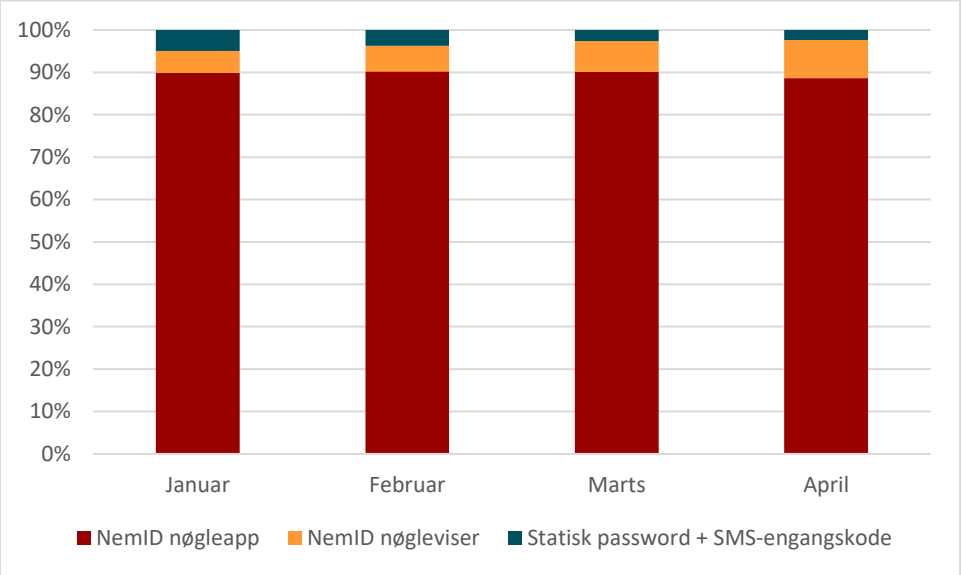
Autentifikationsløsninger
Danske kortudstedere har valgt at tilbyde deres kunder to forskellige løsninger til SCA, nemlig henholdsvis NemID-løsningen og SMS-engangskoder kombineret med et statisk kodeord.

NemID-løsningen bygger på viden om et NemID-kodeord (noget, kun brugeren *ved*) og besiddelse af NemID-appen eller NemID-kodeviseren (noget, kun brugeren *har*).

Den anden løsning bygger på viden om et fast kodeord (noget, kun brugeren *ved*) og besiddelse af et SIM-kort, der kan modtage engangskoder via SMS (noget, kun brugeren *har*).

Den mest brugte løsning er NemID-appen. Det fremgår af figur 3, der viser fordelingen i brugen af de forskellige autentifikationsmetoder. Løsningen med et statisk kodeord og en SMS-engangskode synes primært at blive brugt af kortholdere, der ikke bruger NemID-appen eller NemID-nøgleviseren.

Figur 3: Brug af autentifikationsløsninger



Brug af dynamisk tilknytning
Undersøgelsen viste, at kortholdere pr. 14. april 2021 blev oplyst om beløb og betalingsmodtager for betalinger i NemID-appen, før kortholderen gennemførte autentifikationen. Finanstilsynet finder det tilfredsstillende, at NemID-app'en dermed lever op til kravet om dynamisk tilknytning i henhold til artikel 5, stk. 1, litra b, i den delegerede forordning.[8]

[8] Ved anvendelse af SMS-engangskode sammen et fast kodeord oplyses brugeren om beløb og betalingsmodtager i den SMS, hvor engangskoden modtages. Dermed leve denne løsning op til kravet i artikel 5, stk. 1, litra b, i den delegerede forordning.

Hovedkonklusioner

- Indrullering af kortholdere i løsninger, der lever op til kravene om SCA, er overordnet foregået tilfredsstillende.
- Kortudstederne bør fortsat arbejde på at sikre, at alle, der ønsker at handle på internettet, kan indrullere sig i en løsning, der gør det muligt.
- Den mest brugte løsning er NemID-appen. Løsningen med et statisk kodeord og en SMS-engangskode synes primært at blive brugt af kortholdere, der ikke bruger NemID-appen eller NemID-nøgleviseren.
- Finanstilsynet finder det tilfredsstillende, at NemID-app'en nu lever op til kravene om dynamisk tilknytning.

3.2 Indrullering af betalingsmodtagere

For at bruge SCA skal kortindløsere og betalingsmodtagers leverandør af online betalingsløsninger, såkaldte betalingsgateways, have et set-up, der understøtter brugen af SCA. Det vil konkret sige, at en netbutik skal have opdateret sin betalingsplatform for at kunne føre betalere igennem et SCA-forløb. I praksis har det vist sig, at næsten alle netbutikker havde foretaget den nødvendige migration, inden reglerne trådte i kraft.

I tillæg til at understøtte brugen af SCA er det også muligt for netbutikker at understøtte brugen af undtagelserne fra kravet. Udgangspunktet er som nævnt, at alle transaktioner skal autentificeres med SCA. Brugen af en undtagelse skal derfor ses som en mulighed, der i særlige tilfælde kan gøre en betaling nemmere ved lavrisikotransaktioner. Det kræver dog, at netbutikkernes betalingsgateways har foretaget yderligere migration til et mere avanceret system. Det er Finanstilsynets indtryk, at denne migration er i gang, og at brugen af undtagelser er stigende.

Brugen af undtagelserne er behandlet nærmere i afsnit 3.3.3.

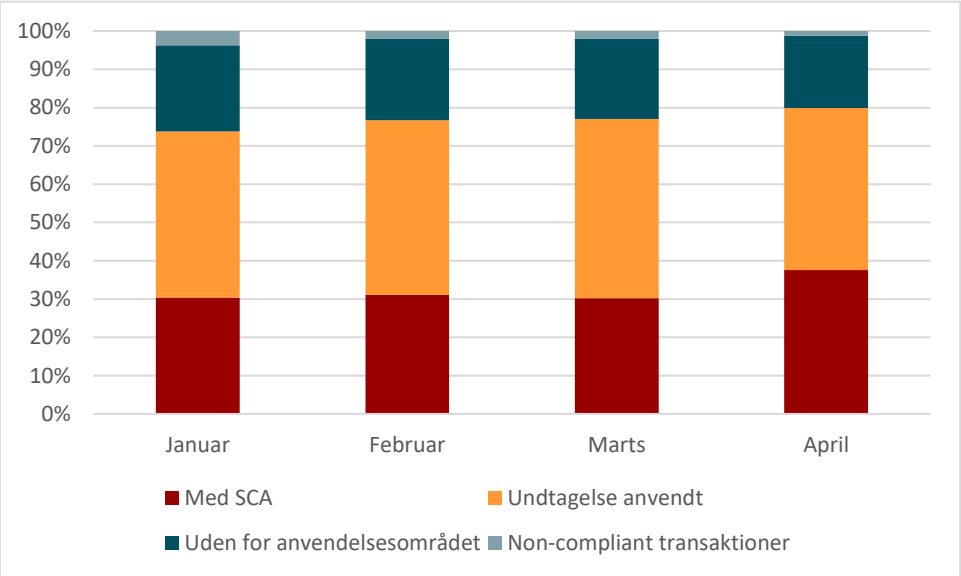
Hovedkonklusioner

- Næsten alle netbutikker havde foretaget den nødvendige migration, inden reglerne trådte i kraft.
- Netbutikkernes arbejde med at anvende undtagelser fra brugen af SCA er i gang, og brugen af undtagelserne er stigende.

3.3 Konklusioner fra analyse af transaktionsdata

Brugen af SCA er steget i løbet af den undersøgte periode, mens andelen af non-compliant-transaktioner er faldet. Andelen af non-compliant-transaktioner var i april 2021 ca. 1,3 pct[9]. Det fremgår af figur 4.

Figur 4: Fordeling af typer af transaktioner



I det følgende gennemgås forholdene omkring de forskellige typer af transaktioner nærmere.

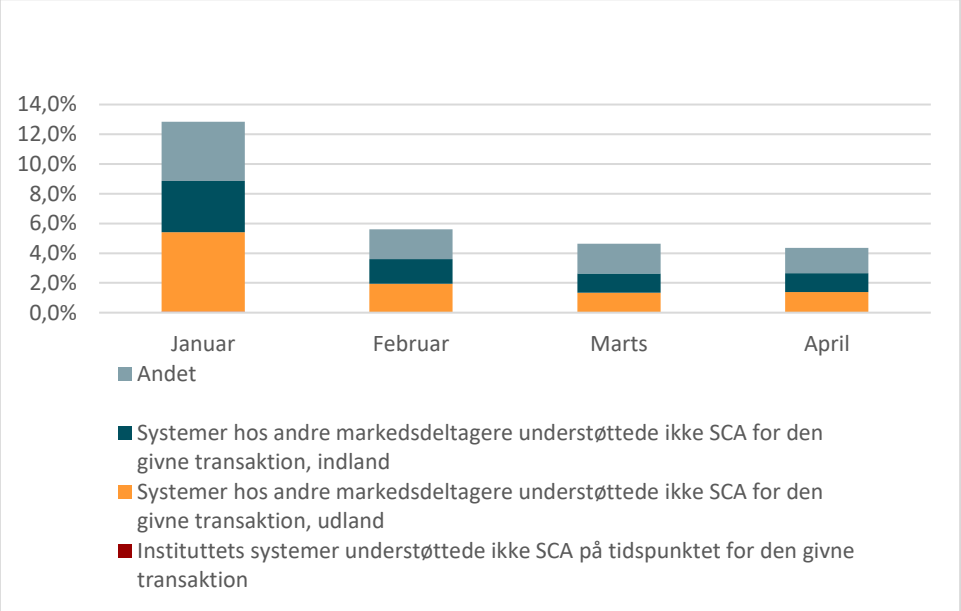
3.3.1 Afviste transaktioner

Når transaktioner afvises af kortudstederen, vil kortholderen opleve, at en betaling i en netbutik ikke kan gennemføres, og at købet må afbrydes. Det kan enten skyldes, at kortudstederens eller kortindløserens systemer ikke var klar til at understøtte SCA på det givne tidspunkt, eller at kortindløseren ikke har markeret transaktionen på en måde, der stemmer overens med kortudstederens systemer.

[9] Transaktioner, der ikke efterlever reglerne om SCA. Kortudstederen skal afvise disse transaktioner. I forbindelse med overgangen til SCA har nogle kortudstedere valgt at gennemføre transaktioner, der ikke lever op til reglerne, for at undgå, at kortholderen får afvist sin betaling. Finanstilsynet er i dialog med kortudstederne om, hvordan alle transaktioner bringes i overensstemmelse med reglerne. Situationen omkring disse transaktioner er nærmere behandlet i afsnit 3.3.2.

Andelen af afviste transaktioner faldt fra 12,8 pct. i januar til 4,4 pct. i april. Det fremgår af figur 5.

Figur 5: Afviste transaktioner



Note: Tallene over afviste transaktioner er et estimat. I tallene er der fraregnet tilfælde, hvor udsteder i første omgang afviser en fejlbehæftet betaling og beder indløser igangsætte betalingen på ny med korrekte oplysninger, hvorefter indløser igangsætter betalingen korrekt. Beregningen forudsætter derfor, at udsteder kan identificere den tilsvarende betaling, der igangsættes i anden omgang. Kategorien "Andet" dækker hovedsageligt over situationer, hvor kortindløseren ikke har igangsat transaktionen korrekt og videresendt de oplysninger kortudstederen skal bruge for at sætte betalingen igang. Det vil sige, at både udsteder og indløser i sig selv er klar til at understøtte SCA, men at udformningen af den enkelte transaktion ikke er korrekt.

Størstedelen af de tekniske problemer, der har forårsaget afviste transaktioner, opstod i forbindelse med overgangen til SCA i januar. Problemerne synes nu til dels at være bragt i orden, men Finanstilsynet mener, at markedsdeltagerne fortsat bør samarbejde om at få alle deltageres systemer til at fungere optimalt sammen.

Særligt har kortudstederne oplyst, at de oplever, at nogle betalingsmodtagere fortsat ikke er i stand til at gennemføre betalinger korrekt med SCA. Det gælder særligt for betalinger igangsat via en betalingsmodtagers app fremfor betalinger igangsat via løsninger baseret på en internetbrowser.

Finanstilsynet opfordrer kortudstederne til at arbejde på en passende løsning på de resterende problemer med app-baserede betalinger, herunder at indgå i et samarbejde med de relevante kortselskaber såsom VISA og Mastercard.

Bemærk, at statistikken i figur 5 ikke medregner tilfælde, hvor betaleren opgiver at benytte SCA, f.eks. fordi betaleren har glemt sin kode. Netbutikker kan derfor have oplevet et større antal afbrudte køb, end hvad denne statistik afspejler. Det er dog ikke muligt konkret at sige, hvorfor sådanne køb afbrydes. Det kan skyldes tekniske problemer med at gennemføre SCA, at betaleren fortrød sit køb, ikke var i stand til at gennemføre SCA, eller at de ektra skridt fik betaleren til at afbryde købet.

Hovedkonklusioner

- De indledende tekniske problemerne synes nu til dels at være bragt i orden, men Finanstilsynet mener, at markedsdeltagerne fortsat bør samarbejde om at få alle deltageres systemer til at fungere optimalt sammen. Det gælder særligt for app-baserede betalinger.

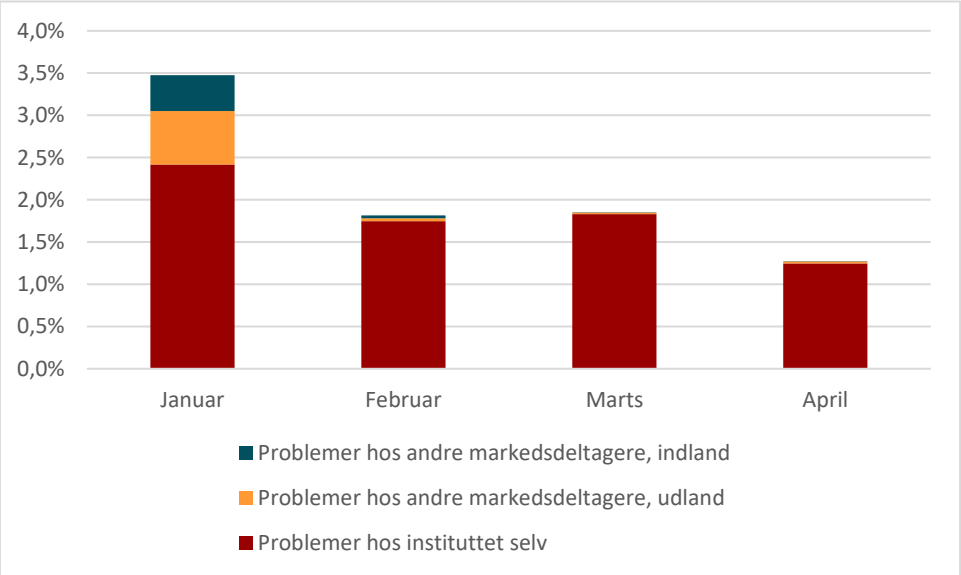
3.3.2 Non-compliant-transaktioner

En transaktion, som er iværksat af betaleren uden brug af SCA og uden en tilladt undtagelse fra kravet, er i strid med lovgivningen.

Ca. 3,5 pct. af transaktionerne i januar 2021 blev gennemført uden SCA eller en tilladt undtagelse. Det skyldtes primært problemer hos kortudstederne men også hos andre markedsdeltagere. I april 2021 var omfanget ca. 1,3 pct. Det fremgår af figur 6. De 1,3 pct. svarer til ca. 295.000 betalinger. Kortudstederne har oplyst, at de sidste problemer i kortudstedernes egne systemer var bragt i orden 20. april 2021.

De indledende vanskeligheder synes således at være håndteret, og stort set alle transaktioner gennemføres nu med SCA eller en tilladt undtagelse. En kortudsteder har oplyst, at man fortsat tillader, at visse app-baserede transaktioner (som også omtalt i afsnit 3.3.1) gennemføres uden korrekt brug af SCA for at undgå, at kortholderne får afvist deres køb. Finanstilsynet er i dialog med udstederen om, hvordan transaktionerne kan bringes i overensstemmelse med reglerne hurtigst muligt.

Figur 6: Non-compliant-transaktioner



Det er væsentligt at understrege, at kortudstederen hæfter for ethvert misbrug, når der ikke bruges SCA, og at kortholderen dermed ikke i udgangspunktet kan blive ansvarlig for misbrug for disse transaktioner.

Hovedkonklusioner

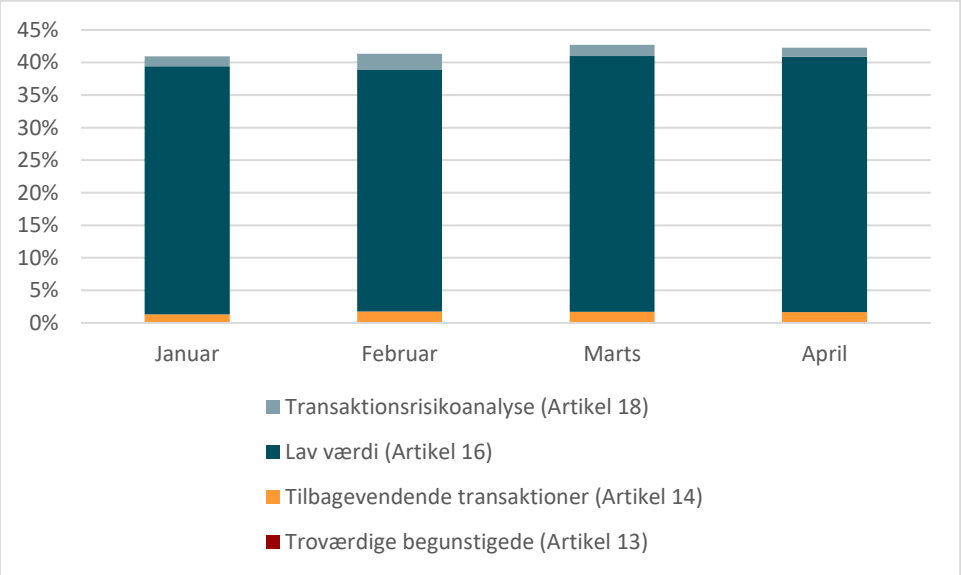
- De indledende tekniske vanskeligheder synes at være håndteret, og stort set alle transaktioner gennemføres nu med SCA eller en tilladt undtagelse.
- Enkelte transaktioner gennemføres fortsat i strid med reglerne. Finanstilsynet er i dialog med relevante parter om, hvordan transaktionerne kan bringes i overensstemmelse med reglerne hurtigst muligt.
- Når der ikke bruges SCA, hæfter kortudstederen for ethvert misbrug.

3.3.3 Brug af undtagelser

Reglerne om SCA indeholder en række muligheder for at undtage transaktioner fra SCA. Det gælder transaktioner til såkaldt troværdige begunstigede[10], tilbagevendende transaktioner af samme værdi og til samme modtager[11], transaktioner af lav værdi[12] og transaktioner, der vurderes at være forbundet med lav risiko på baggrund af en transaktionsrisikoanalyse[13].

Næsten alle transaktioner, der undtages SCA, er lavværditransaktioner. Det fremgår af figur 7. Af figuren fremgår også, at andelen af transaktioner, der var undtaget SCA, lå stabilt på omkring godt 40 pct. gennem den undersøgte periode.

Figur 7: Brug af undtagelser



Danske kortudstedere bruger ikke muligheden for at undtage transaktioner til såkaldt troværdige begunstigede.

Heller ikke undtagelsen baseret på såkaldt transaktionsrisikoanalyse bliver brugt aktivt i Danmark. Det fremgår af figur 7, at enkelte transaktioner er registreret af danske kortudstedere

[10] Kommissionens delegerede forordning (EU) 2018/389 artikel 13.
[11] Kommissionens delegerede forordning (EU) 2018/389 artikel 14.
[12] Kommissionens delegerede forordning (EU) 2018/389 artikel 16.
[13] Kommissionens delegerede forordning (EU) 2018/389 artikel 18.

som omfattet af undtagelsen. Ved disse transaktioner har udenlandske kortindløsere angivet, at de har foretaget en transaktionsrisikoanalyse og ønsker at undtage betalingen.

For aktivt at gøre brug af undtagelsen på baggrund af transaktionsrisikoanalyse, skal instituttet opfylde en række krav. Kravene dækker blandt andet, at instituttet skal implementere en tilstrækkelig mekanisme til transaktionsmonitorering. Det er også et krav, at instituttet beregner en udførlig rate for svig på den type transaktion som ønskes undtaget, her korttransaktioner. Instituttets grundlag for brug af undtagelsen, herunder blandt andet den beregnede svigrate samt ovennævnte mekanisme til monitorering, skal årligt revideres. De samme krav er ikke i udgangspunktet gældende for et institut som blot skal acceptere en anmodning om at anvende undtagelsen.

Finanstilsynet har den forståelse, at både danske indløsere og udstedere mener, at kravene for denne konkrete undtagelse gør den besværlig at bruge. Finanstilsynet vil inkludere disse erfaringer i forbindelse med en kommende revision af reglerne på området.

Påbud om korrekt brug af lavværdiundtagelsen
Undersøgelsen viste, at kortudstedere, der bruger SDC som datacentral, brugte undtagelsen for lavværditransaktioner forkert, da grænseværdierne for at bruge undtagelsen var sat højere end de maksimale beløbsgrænser tilladt i lovgivningen. Finanstilsynet påbød på den baggrund disse kortudstedere at efterleve § 128, stk. 1, nr. 2, ved at undlade at undtage transaktioner over de tilladte grænseværdier fra SCA. Institutterne har siden den 20. august brugt undtagelsen korrekt[14].

Hovedkonklusioner

- Undtagelsen baseret på transaktionsrisikoanalyse bliver ikke brugt aktivt i Danmark. Finanstilsynet vil inkludere erfaringerne i forbindelse med en kommende revision af reglerne på området.
- Kortudstedere, der bruger SDC som datacentral, brugte undtagelsen for lavværditransaktioner forkert. Institutterne har siden den 20. august brugt undtagelsen korrekt.

[14] https://www.finanstilsynet.dk/Tilsyn/Tilsynsreaktioner/Paabud/2021/kortudstedereSDC

4. Brug af delegeret autentifikation

Ved brug af såkaldte wallet-løsninger (f.eks. MobilePay Online, ApplePay og GooglePay) bruger kortudstederne såkaldt delegeret autentifikation, hvor SCA gennemføres i wallet-udbyderens miljø. Ved kortbetalinger gennem en wallet bruger kortholderen ikke de autentifikationselementer, der som udgangspunkt bruges til kortbetalinger på internettet (som nærmere beskrevet under punkt 3.1 ovenfor). I stedet bruges elementer, der er integreret i den pågældende wallet. Det kan eksempelvis være en talkode eller biometrisk løsning, der bruges som en del af den pågældende wallet[15].

Regler for udstedelse af autentifikationselementer
SCA skal gennemføres med de autentifikationselementer (også kaldet personlige sikkerhedsforanstaltninger), der er udstedt af brugerens udbyder af betalingstjeneste. Det følger af definitionerne i § 4, nr. 29-31, i betalingsloven.

I betalingsloven defineres autentifikation som "en procedure, der medfører, at en udbyder af betalingstjenester kan verificere identiteten af brugeren eller validiteten af anvendelsen af et specifikt betalingsinstrument, herunder anvendelsen af **en brugers personlige sikkerhedsforanstaltninger**" (Finanstilsynets fremhævning)[16]. En personlig sikkerhedsforanstaltning defineres som "Personaliserede elementer, som **udbyderen stiller til rådighed** for brugeren med henblik på at foretage autentifikation" (Finanstilsynets fremhævning)[17].

I forbindelse med en kortbetaling vil kortudstederen være udbyderen af betalingstjenesten.

Sikkerhedsforanstaltningerne kan som nævnt ovenfor omfatte elementer, der enten kan kategoriseres som viden (noget, kun brugeren *ved*), besiddelse (noget, kun brugeren *har*) eller en iboende egenskab (noget, kun brugeren *er*) [18].

Udbyderen af betalingstjenesten skal sikre, at sammenkædningen mellem kortholderen og elementerne, der benyttes til SCA, sker i et sikkert miljø[19], og at der bruges SCA ved tilknytningen, hvis sammenkædningen sker via en fjernkanal (f.eks. en smartphone)[20]. Når en kortholder vil benytte en wallet-løsning skal kortudstederen altså konkret bruge en af de SCA-løsninger, man allerede har knyttet til kortholderen, og kortudstederen skal sikre sig, at tilknytningen sker på en måde, hvor svindlere eller andre uvedkommende ikke kan få indsigt i eller manipulere med de oplysninger, der bliver udvekslet.

---

[15] Undersøgelsen omfatter ikke løsninger som Garmin Pay og Fitbit Pay, da de ikke bruges til at igangsætte kortbetalinger på internettet, men kun fysisk handel.
[16] Lov om betalinger § 7, nr. 29. I lov betalinger § 4, nr. 30, præciseres det yderligere, at SCA defineres som "En autentifikation, som er baseret på anvendelsen af to eller flere elementer, der er kategoriseret som viden, besiddelse og iboende egenskab, der er uafhængige, så brud på et element ikke svækker pålideligheden af de andre elementer, og er designet på en sådan måde, at fortroligheden af autentifikationsdata beskyttes."
[17] Lov om betalinger § 4, nr. 31. § 4, nr. 31, implementerer PSD2 artikel 4, nr. 31, hvor det fremgår, at der med "udbyderen" forstås en betalingstjenesteudbyder. Finanstilsynet vurderer, at betalingstjenesteudbyderen i dette tilfælde er brugerens betalingstjenesteudbyder.
[18] Lov om betalinger § 7, nr. 30.
[19] Kommissionens delegerede forordning (EU) 2018/389 artikel 24, stk. 2, litra a
[20] Kommissionens delegerede forordning (EU) 2018/389 artikel 24, stk. 2, litra b

Brug af token-løsninger
Wallet-løsninger fungerer som hovedregel ved, at kortudstederen ved indrullering af et betalingskort i wallet-løsningen udsteder en såkaldt token. Denne udgør en digital repræsentation af betalingskortet, som kun kan bruges i en bestemt sammenhæng (eksempelvis en specifik wallet-løsning på en specifik smartphone). Denne token er knyttet til og bliver opbevaret på kortholderens smartphone. EBA har i sit svar på Q&A 2019_4827[21] slået fast, at tokens, der repræsenterer et betalingskort, kan udgøre en valid autentifikationsfaktor, hvis kravene til beskyttelse mod kopiering i artikel 7, stk. 2, i den delegerede forordning og kravene til indrullering i artikel 24 i den delegerede forordning er overholdt. Finanstilsynet vurderer på den baggrund, at en token, der overholder disse krav, kan bruges som den ene autentifikationsfaktor i forbindelse med gennemførelse af SCA. Finanstilsynet vurderer også, at en sådan token kan anses som udstedt af kortudstederen.

Øvrige autentifikationsfaktorer ved delegeret autentifikation
Som den anden faktor ved gennemførelse af kortbetalinger gennem en wallet bruges ofte de biometriske elementer, der er knyttet til kortholderens smartphone, som f.eks. ansigtsgenkendelse eller fingeraftrykslæser. Alternativt bruges vidensbaserede elementer, som f.eks. en talkode.

Disse autentifikationsfaktorer er blevet knyttet til kortholderen af wallet-udbyderen og ikke af kortudstederen.

Finanstilsynet vurderer, at disse løsninger som udgangspunkt lever op til kravene om, at der ved autentifikation af kortholderen**,** i forbindelse med, at kortholderen igangsætter en betaling, skal bruges to autentifikationsfaktorer, der enten kan karakteriseres som viden, besiddelse eller en iboende egenskab[22]. Det er dog afgørende, at autentifikationsfaktorerne knyttes til kortholderen med en af de SCA-løsninger, kortudstederen allerede har knyttet til kortholderen.[23]

Outsourcing ved brug af wallet-løsninger
Bekendtgørelse om outsourcing for kreditinstitutter mv. (outsourcing-bekendtgørelsen)[24] finder anvendelse, hvor en leverandør udfører en proces, en tjenesteydelse eller en aktivitet, som outsourcingvirksomheden ellers selv ville udføre.

Som tidligere beskrevet er det kortudstederens opgave at udstede de faktorer, der bruges ved SCA. Ved brug af wallet-løsninger vil en token være udstedt og knyttet til kortholderen af kortudstederen.

I modsætning til dette vil det andet autentifikationselement typisk ikke være udstedt og knyttet til kortholderen af kortudstederen. Knytter kortudstederen ikke selv denne faktor til kortholderen med SCA, men i stedet forlader sig på den tilknytning af faktoren til kortholderen, som wallet-udbyderen har foretaget, vurderer Finanstilsynet, at det skal anses som outsourcing.

[21] https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4827
[22] § 127, stk. 1, nr. 2, og § 7, nr. 30, i lov om betalinger.
[23] Kommissionens delegerede forordning (EU) 2018/389 artikel 24, stk. 2, litra b.
[24] BEK nr. 877 af 12/06/2020

Det skyldes, at wallet-udbyderen her udfører den opgave, som udbyderen af betalingstjenesten ellers selv skulle udføre i medfør af artikel 24 i den delegerede forordning. Det er desuden en opgave, som udføres løbende i forbindelse med, at de enkelte kortholdere indrullerer sig. Det er samtidig en opgave, som kortudstederen selv vil kunne varetage, da kortudstederen udsteder andre autentifikationsløsninger til kortholderen. Kortudstederen skal i den forbindelse sikre sig, at wallet-udbyderen har overholdt kravene i artikel 24 i den delegerede forordning i forbindelse med tilknytningen. Det vil sige, at tilknytningen er sket i sikkert miljø med SCA. Kortudstederen bør desuden overveje, om der er tale om kritisk eller vigtig outsourcing.

Kortudstedernes praksis med indrullering i de anvendte wallet-løsninger
MobilePay Online
Ved brug af MobilePay bruges der ved indrullering af kortholderen og kortholderens betalingskort i løsningen de autentifikationselementer, der er beskrevet i afsnit 3.1. Løsningen overholder dermed reglerne i artikel 24 i den delegerede forordning, da kortholderen indrulleres med SCA.

Apple Pay og Google Pay
Ved brug af Apple Pay og Google Pay bruges to forskellige løsninger, henholdsvis indrullering via kortholderens mobilbank eller indrullering via wallet-appen.

Ved indrullering gennem mobilbanken autentificeres kortholderen med SCA gennem den løsning, der er indbygget i mobilbanken. Løsningen overholder dermed reglerne i artikel 24 i den delegerede forordning, da kortholderen indrulleres med SCA.

Ved indrullering gennem wallet-appen er det et krav i løsningen, at kortholderen er logget ind med sin Google-konto eller AppleID. Kortudstederen kan også vælge, at kortholderen skal autentificere sig med en SMS-engangskode sendt til det SIM-kort, som kortudstederen har knyttet til kortholderen. Er SIM-kortet knyttet korrekt til kortholderen, kan det udgøre en autentifikationsfaktor i form af besiddelse.

En række kortudstedere, der deltager i undersøgelsen, har angivet, at login på en Google-konto eller AppleID udgør et autentifikationselement i form af viden, da kortholderen har brugt et kodeord til at logge ind. Finanstilsynet vurderer, at et kodeord til en Google-konto eller et kodeord til et AppleID kun kan udgøre en autentifikationsfaktor, hvis kortholderen er korrekt knyttet til kodeordet med SCA. Har kortudstederen ikke selv knyttet kortholderen til kodeordet, vil der være tale om outsourcing af den opgave, kortudstederen er pålagt i artikel 24 i den delegerede forordning. Lader kortudstederen kortholderen autentificere sig ved brug af en Google-konto eller AppleID, er udstederen derfor forpligtet til at indgå outsourcingkontrakter med wallet-udbyderne. Kortudstederne skal i den forbindelse sikre, at wallet-udbyderen knytter kortholderen til de benyttede autentifikationsfaktorer i overensstemmelse med artikel 24 i den delegerede forordning.

Finanstilsynet forventer på den baggrund, at kortudstederne enten indgår outsourcingkontrakter med Apple Pay og Google Pay eller afholder sig fra at indrullere kortholdere via wallet-appen. Kortudstederne bør i den forbindelse også overveje, om der er tale om kritisk eller vigtig outsourcing. Finanstilsynet vil indgå i en dialog med kortudstedere, der måtte ønske at

indrullere kortholdere via wallet-appen, om hvornår en outsourcingkontrakt skal være indgået. Finanstilsynet vil desuden drøfte på europæisk niveau, hvordan kortudstedere kan opfylde kravet om indgåelse af en outsourcingkontrakt med wallet-udbyderne.

Kortudstedernes praksis med den løbende brug af wallet-løsninger
Efter indrullering af kortholderen i en wallet-løsning vil kortudstederen i forbindelse med en konkret kortbetaling fra en wallet kontrollere, at kortholderen er i besiddelse af en valid token fra en smartphone, hvor kortholderen er korrekt indrulleret.

Kortholderen autentificerer sig i denne forbindelse med den udstedte token (noget, brugeren *har*) og med den indbyggede sikkerhedsforanstaltning i den pågældende wallet (typisk kode, fingeraftryk eller ansigtsgenkendelse, noget brugeren *ved* eller noget brugeren *er*). Finanstilsynet vurderer, at kortudstederen på egen hånd kan kontrollere validiteten af den udstedte token. Kortudstederen varetager derfor selv denne del af processen med SCA.

Finanstilsynet indgår på nuværende tidspunkt i drøftelser på europæisk niveau om, hvorvidt kortudstedere i tilstrækkelig grad kan kontrollere processen med validering af den anden autentifikationsfaktor, der er indbygget i wallet-løsningen. Finanstilsynet kan derfor endnu ikke konkludere, om den løbende brug af autentifikationsfaktorer til at gennemføre de enkelte betalinger, der er indbygget i wallet-løsninger, kan anses som outsourcing af forpligtelsen til at gennemføre SCA. Finanstilsynet vil inddrage de indhentede oplysninger i arbejdet på europæisk niveau og genoptage dialogen med kortudstederne om spørgsmålet på et senere tidspunkt.

Kortudstedere, der bruger disse autentifikationsløsninger, er dog under alle omstændigheder forpligtet til løbende at kontrollere, at løsningerne overholder de gældende krav[25].

Hovedkonklusioner

- Det er Finanstilsynets vurdering, at de undersøgte wallet-løsninger opfylder kravene om brug af SCA. Det er dog afgørende, at autentifikationsfaktorerne knyttes til kortholderen med en af de SCA-løsninger, kortudstederen allerede har knyttet til kortholderen.
- Knyttes kortholderen til wallet-løsningens autentifikationsfaktorer med autentifikationselementer, der ikke er udstedt af kortudstederen, skal det anses som outsourcing.
- Det er Finanstilsynets forventning, at kortudstederne enten indgår outsourcingkontrakter med Apple Pay og Google Pay eller afholder sig fra at indrullere kortholderen via wallet-app'en.
- Finanstilsynet kan på nuværende tidspunkt ikke konkludere, om den løbende anvendelse af autentifikationsfaktorer, der er indbygget i en wallet-løsning, kan anses som outsourcing af forpligtelsen til at gennemføre SCA ved betalinger igangsat af brugeren eller ej. Finanstilsynet vil inddrage de indhentede oplysninger i arbejdet på europæisk niveau og genoptage dialogen med kortudstederne om spørgsmålet på et senere tidspunkt.

[25] Kommissionens delegerede forordning (EU) 2018/389 artikel 3.