FINANSTILSYNET

Drøftelse af brug af digitale identiteter

Tobias Thygesen
Kontor for Fintech, Betalingstjenester og Governance

Finantilsynets redegørelse om Estland-sagen - idékatalog

- Myndighederne vil understøtte den finansielle sektors igangværende bestræbelser på at opbygge en fælles infrastruktur i forhold til at styrke de finansielle virksomheders processer for kundekendskab
- Fokus på
  - Danske styrkepositioner
  - Fælles infrastruktur
  - Offentlige data og løsninger
  - PEP-register
  - Bandit-register
  - …
- Udgangspunktet er, at teknologi kan være WIN-WIN-WIN – Bedre, billigere og lettere

Styrkelse af indsatsen mod hvidvask…

- *Finanstilsynet understøtter den finansielle sektor med at opbygge fælles infrastruktur, der kan styrke virksomhedernes processer for kundekendskab.*

- Finanstilsynet og øvrige relevante myndigheder vil deltage i den finansielle sektors arbejde med at opbygge en fælles infrastruktur, der kan styrke de finansielle virksomheders processer for kundekendskab. Det skal ske underhensynstagen til kundernes retssikkerhed med henblik på at undgå unødig deling af data, og at kunderne risikerer at blive "blacklisted" på usagligt grundlag.

Aftale mellem regeringen (Venstre, Liberal Alliance og Det Konservative Folkeparti) og Socialdemokratiet, Dansk Folkeparti, Radikale Venstre og Socialistisk Folkeparti

om

STYRKELSE AF INDSATSEN MOD FINANSIEL KRIMINALITET

Af 27. marts 2019

Er skrevet lidt meget op mod "banditregister"

Projekt AML/TEK

- Finanstilsynet beskriver fordele og ulemper ved en række initiativer, men beslutningen om videre skridt er i sidste ende politisk
- Forankret i fintech-teamet – men tæt samarbejde med HVID og JURA
- Skal belyse muligheder og udfordringer,

herunder særligt i forhold til databeskyttelse, m.m.

- Nogle ting vil vi selv kunne gå videre med – herunder vejledning om brug af eID…
- God dialog med FIDA og Digst herom!

FINANSTILSYNET

Identitet er ikke CDD – og FATF guidance går kun på 10(a)

- 10. Customer due diligence *
- Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.
- Financial institutions should be required to undertake customer due diligence (CDD) measures when:
- (i) establishing business relations;
- (ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
- (iii) there is a suspicion of money laundering or terrorist financing; or
- (iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.
- The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.
- The CDD measures to be taken are as follows:
- (a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
- (b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.
- (c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
- (d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

FINANSTILSYNET

Udviklingen i rammeværket

- ”Hvis kunden ikke har været fysisk til stede for at legitimere sig, pålægger medlemsstaterne disse institutter og personer at træffe særlige, passende foranstaltninger til at opveje den højere risiko.”

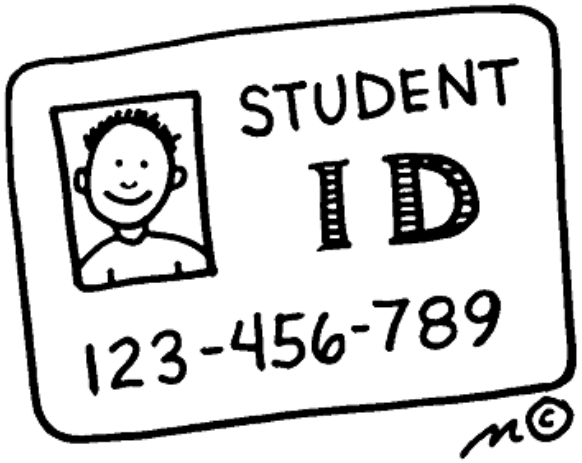
AMLDIII

- virksomhederne skal tage tilstrækkelige skridt for at sikre:
  - at den angivne identitet og den faktiske person er den samme,
  - **at virksomheden forholder sig til**, om det giver anledning til øget risiko, at kundeforholdet ikke etableres fysisk, samt
  - at der gennemføres skærpede kundekendskabsprocedurer, herunder vurderes om det er nødvendigt med skærpede legitimeringsprocedurer, hvis kundeforholdet er forbundet med en øget risiko.

Revised EBA guidelines on money laundering and terrorist financing risk factors

Anvendelsesområdet for digitale signaturer

- Primært relevant for legitimering af kunder identitet, der onboardes uden fysisk fremmøde (distancekunder) (?)
- Historisk har hvidvaskreglerne per definition forbundet distancekunder med øget risiko, men det har ændret sig:
  - Specifikke krav om EDD for distancekunder bortfaldt med AMLDIV
  - eIDAS opstiller rammeværk for sikre digitale identitetsløsninger
  - Både AMLDIV og EBAs vejledning (pt. i høring) fremhæver, at digitale identitetsløsninger kun skal kunne bruges, hvis de er sikre nok (eIDAS)
  - FATF understøtter denne holdning, og fremhæver endvidere, at brugen af gode digitale identitetsløsninger kan mindske risikoen for misbrug.
- Finanstilsynet ser i lyset deraf nærmere på, om MitID skal kunne anvendes bredere til legitimering af kunder under hvidvaskloven

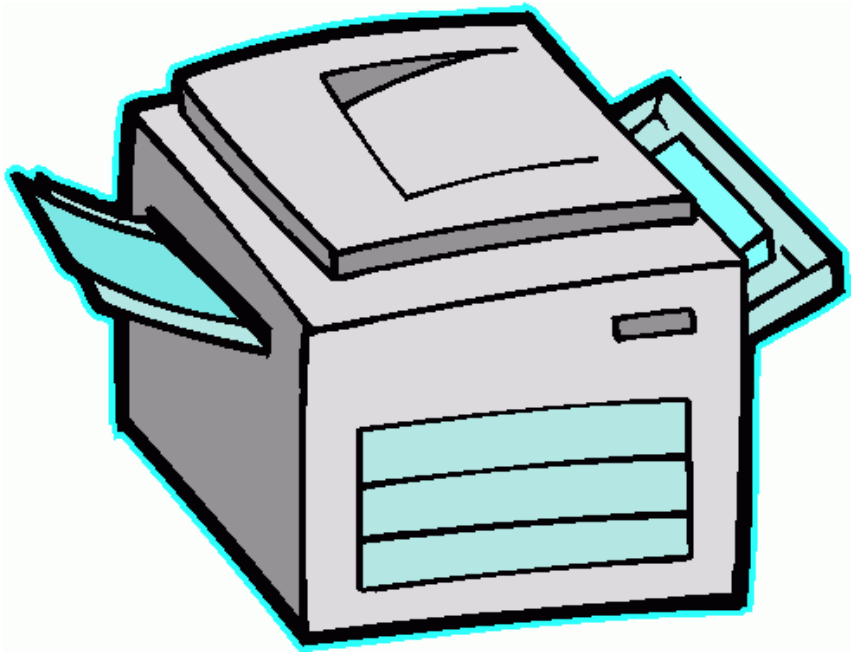


Finanstilsynets vejledende fortolkning om NemID (2013)

- NemID med tilknyttet OCES-certifikat kan anvendes som eneste kontrolkilde for kunder med lav risiko, hvis:
  - Kunden underskriver dokumenter ved anvendelse af NemID som bekræftelse på kundens navn (identitet), og
  - virksomheden sammenholder de fra kunden modtagne oplysninger med oplysningerne i CPR-registret, som bekræftelse på kundens adresse og CPR-nr.
- Finanstilsynets fortolkning var mere lempelig end foreskrevet i AMLD3, der per definition forbandt distancekunder med EDD

Men hvad så efter AMLDIV?

- At fortolkningen blev fastholdt efter AMLDIV skyldes, at sikkerheden omkring NemID løsningen historisk ikke har været høj nok:
  - Kvaliteten af indrullering var potentielt ikke høj nok
  - Nøglekortet for ”let” at videregive sammen med brugernavn og kode
- Man kan, populært sagt, sende sin identitet i en mail…



Kan MitID bruges til mere?

FINANSTILSYNET

Sikkerheden ved MitID

- Finanstilsynets analyse er fokuseret på sikkerhedsniveauet i MitID

- Finanstilsynet forventer, at det typisk anvendte MitID som minimum anmeldes på sikkerhedsniveau ”betydelig” under eIDAS.
  - Der er både krav til indrullering, autentifikationsmekanisme samt håndtering, organisering og governance.

- Om MitID kan stå alene som kilde til legitimering af en kundens identitet kan koges ned til to forhold:
  1. Hvorvidt virksomhederne kan være sikre på, at et MitID er udstedt til den person, det er registeret til, samt
  2. I hvor høj grad virksomhederne kan være sikre på, at det givne MitID ikke er videregivet (bevidst eller ubevidst) til en anden person.

FINANSTILSYNET

Andre myndigheders syn på sikkerheden

- FATF guidance til myndigheder og virksomheder:
  - Afgørende med klar forståelse af sikkerhedsniveauet i en given digital identitetsløsning, herunder i hvilket omfang løsningen er troværdig og en uafhængig kilde, samt
  - Givet sikkerhedsniveauet, vurdere om løsningen tilstrækkeligt mitigerer risikoen for hvidvask, terrorfinansiering og svindel.

- EBAs vejledning (i høring):
  - eID-løsninger med sikkerhedsniveau 'høj' giver i sig selv ikke giver anledning til øget risiko for hvidvask eller terrorfinansiering, men
  - sådanne løsninger kan potentielt øge risikoen, eksempelvis gennem svindel med identiteter.

- Primære problemstillingen fsva. MitID relaterer sig således til muligheden for videregivelse af en identitet (svindel eller tyveri).

FINANSTILSYNET

Videregivelsesproblematikken

- Uanset hvilke kontrolkilder der anvendes for (distance-)kunder, vil det altid være muligt at videregive identiteter, hvis den givne person indvilliger hertil, enten frivilligt eller under tvang
- Finanstilsynet vejledning lægger op til, at virksomheder anvender en eller flere kontrolkilder eller mitigerende tiltag
- Denne tilgang afspejler i høj grad, at man som minimum skal besværliggøre processen så meget som muligt for kriminelle
- Konsekvensen af bevidst videregivelse af en identitet kan dog være, at kriminel adfærd først identificeres i den løbende monitorering af kundeforholdet (eller aldrig)
- ODD og overvågning er vigtig – og her kan eID være bedre!

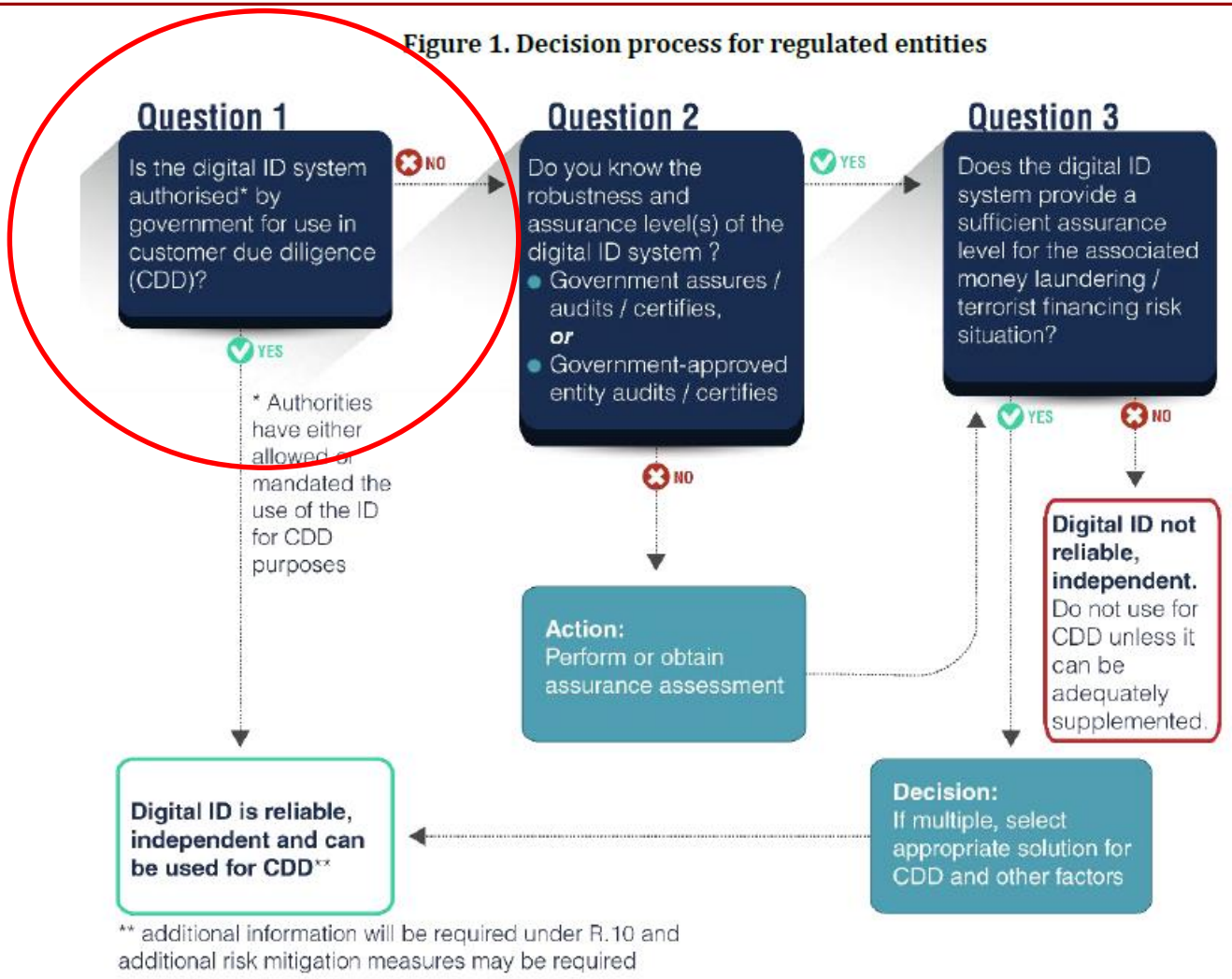
FINANSTILSYNET

Mulighederne for øget sikkerhed i MitID-løsningen

- Høje sikkerhedsmæssige krav til legitimeringen af personer ved udstedelse af MitID
- Finansielle virksomheder kan kun integrere til MitID-løsningen gennem en broker - NemLog-in eksempelvis broker for den offentlige sektor
- Broker modtager både autentifikationssvar og anden supplerende risikodata fra MitID-løsningen, når en kunde autentificerer sig ved brug af nøgleappen
- Spørgsmålene forbliver således:
  - I hvilket omfang disse risikodata kan anvendes til at mitigere videregivelsesproblematikken, samt
  - Hvor sikker skal man være førhen problematikken er tilstrækkeligt mitigeret?
- **Vejledning følger ☺**

FATF guidance – intet er givet her i verden!

Figure 1. Decision process for regulated entities



Hvis Finanstilsynet ikke giver svaret, så tænk selv…

FINANSTILSYNET

Grundlæggende budskaber

- I sidste ende drejer det sig om risici – og mitigerende tiltag – uagtet om det er digitalt eller analogt
- eID-løsninger kan være lige så sikre som papirbaserede – men man skal tænke sig om
- Der er forskellige sikkerhedsniveauer, også selvom et eID er udstedt af det offentlige!
  - Hvis der ikke er guidance fra myndighederne, må man selv vurdere som vanligt
- Det er Finanstilsynets forventning, at MitID sandsynligvis vil kunne anvendes bredere end NemID
- Husk at kundekendskabsprocedurer er MERE end identitet!

FINANSTILSYNET

Spørgsmål