UNIVERSITETET I OSLO

# Krav på sikkerhet i betalingssystemet

Sikker autentisering med bruk av eID til å gjennomføre internettbetalinger

Ellen Bennin Brataas
Vitenskapelig assistent
UiO

1. desember 2022

1

## Tema: Sikkerheten til bruk av eID

| Steg 1: | Steg 2: | Steg 3: |
|---|---|---|
| eID-løsningen godkjennes av nasjonale myndigheter | Kunden identifiseres ved utstedelse av eID | Krav til sikker autentisering av kunden ved bruk av eID |
| eIDAS-forordningen | 5AMLD | 5AMLD + PSD2 |



2

# Tema: Sikkerheten til bruk av eID

| Steg 1: | Steg 2: | **Steg 3:** |
|---|---|---|
| eID-løsningen godkjennes av nasjonale myndigheter | Kunden identifiseres ved utstedelse av eID | **Krav til sikker autentisering av kunden ved bruk av eID** |
| eIDAS-forordningen | 5AMLD | **5AMLD + PSD2** |

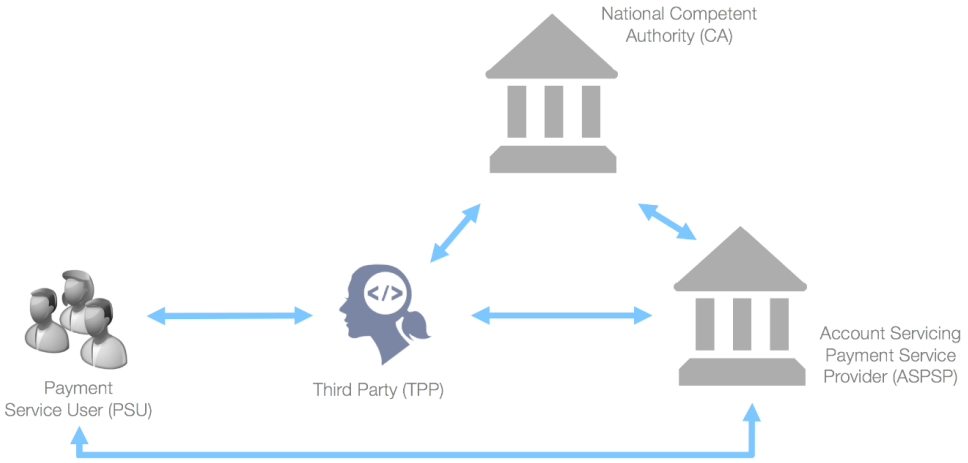


# Oversikt

- Gjennomføring av internettbetalinger
- Risikoer ved bruk av eID til å autentisere kunden
- Sikkerhetskrav i PSD2 og 5AMLD


# Om internettbetalinger

«Arkitekturen» til PSD2 ved autentiseringen av internettbetalinger




UNIVERSITETET I OSLO

Side 5

5

# Om TPP/PSP

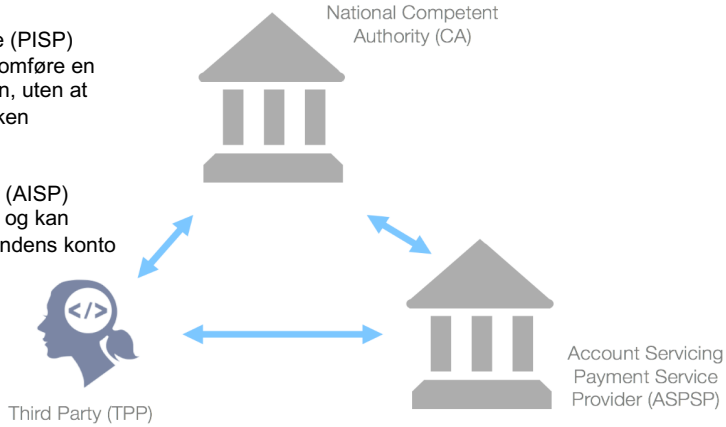
Third party provider/Payment service provider

TPP = en PSP som har tillatelse fra nasjonale myndigheter til å få tilgang til bankens «application programming interfaces» (API)

To typer TPP:

(i) Payment initiation service (PISP)
Tredjeparter som kan gjennomføre en betaling på vegne av kunden, uten at kunden logger inn i nettbanken
Eks. Zalando

(ii) Account service provider (AISP)
Tredjeparter som får tilgang og kan innhente informasjon om kundens konto
Eks. Experian




Bankens API legger til rette for informasjonsdeling med TPP

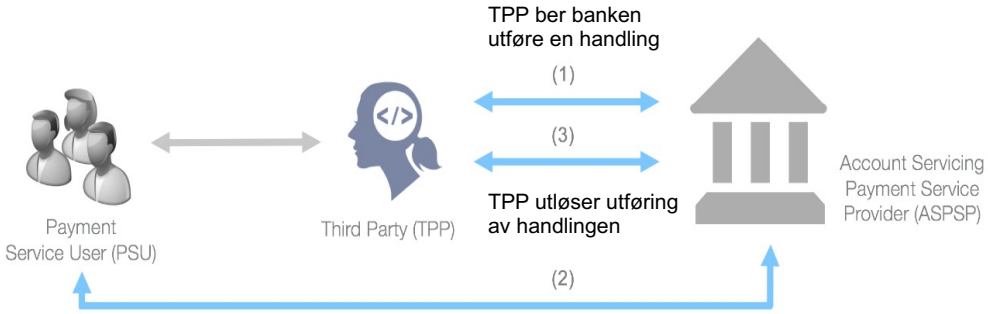
UNIVERSITETET I OSLO

Side 6

6

# Gjennomføring av internettbetalinger etter PSD2

Samspillet mellom kunden, tredjeparten og banken med betalingskontoen




Banken autentiserer kunden, og får kunden til å «signere» handlingen

eks. med eID



7

# «Open banking»

Fordeler:

"The continued development of an integrated internal market for safe electronic payments is crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market."

Fortalen til PSD2, avsn. 5

Ulemper

- Kompleks sikkerhetsmodell
- Autorisasjonen av betalingsorderen og autentiseringen av kunden gjøres at to forskjellige finansinstitusjoner



8

# Risikoen med eID i «open banking»

Risikofaktorer:

- Svært høy hastighet
  - eks. Instant payments
- «non-face-to-face»-transaksjoner
  - Tradisjonelt ansett som høyrisko kundeadferd for hvitvasking (FATF 2012)
- Vanskelig å spore opphav av midlene
- Vanskelig å straffeforfølge underliggende kriminell handling

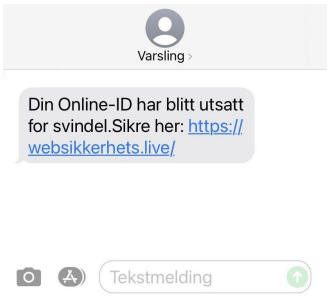
Rettsutvikling

- 5AMLD modifiserer 4AMLD etter anbefaling fra FATF (2020-rapport)
  - Integrerer eIDAS
- «non-face-to-face»-transaksjoner med eID ikke lenger ansett som høyrisiko
- OBS: forutsatt at

  1. eID-løsningen overholder eIDAS-forordningen

  2. på plass hensiktsmessige sikkerhetsmekanismer






# Den særlige risikoen med eID


I trusselvurderingen presenterer Økokrim det som forventes å bli de største truslene innenfor våre ansvarsområder de neste årene. Samtidig gis det et oppdatert kriminalitetsbilde og innblikk i forventet utvikling.

Sak om «Olgasvindel» og forsettbegrepet i finansavtaleloven til Høyesterett

Bakgrunnen for saken som skal behandles av Høyesterett onsdag 23. august er at en eldre kvinne ble lurt til å oppgi passord og kode for BankID til en hun trodde representerte banken. Det sentrale spørsmålet i saken er forsettbegrepets innhold i finansavtaleloven.


A man looks at posters from an international campaign to support Ukraine in Kiev, March 12. Commentary contributor Alec Ross writes: 'The absence of a set of broadly held norms and treaties governing the use of cyber weapons has not led to the firing of guns or launching of missiles, but this will not always be the case. We need something more than playground rules.'

GLOBAL VIEWPOINT

## Russia's cyber weapons hit Ukraine: How to declare war without declaring war

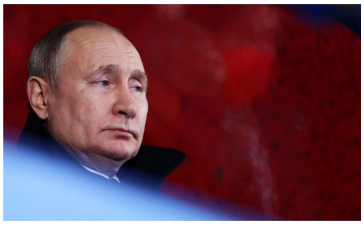
By targeting the Ukrainian government with a cyber weapon, the Russians are able to effectively engage in an aggressive, kinetic act without actually declaring war, or other countries reacting like it is an act of war. This will not last forever.

BlackEnergy, its first version shortened as BE1, started as a crimeware being sold in the Russian cyber underground as early as 2007. Initially, it was designed as a toolkit for creating botnets for conducting DDoS attacks. It supported a variety of flooding commands including protocols like ICMP, TCP SYN, UDP, HTTP and DNS. Among the high profile targets of cyber attacks utilising BE1 were a Norwegian bank and government websites in Georgia three weeks before Russo-Georgian War.

On 23 December 2015, attackers behind the BlackEnergy malware successfully caused power outages for several hours in different regions of Ukraine. This cyber sabotage against three energy companies has been confirmed by the Ukrainian government. The power grid compromise has become known as the first-of-its-kind cyber warfare attack affecting civilians.

## US, UK detail malware tied to Russian hacking group Sandworm that targets Linux

Derek B. Johnson February 23, 2022



*Agencies from the US and UK detailed a new piece of malware they say has been leveraged by the Russian Sandworm APT group since June 2019. (Photo by Matthew Stockman/Getty Images)*

As Russia begins its invasion of Ukrainian territories and Western governments continue to warn about the potential or Russian cyberattacks in response to sanctions, U.S. and UK agencies have detailed what they claim is another malware tool used by Russian APT hacking group Sandworm.

BANKS JUNE 27, 2017 / 6:39 PM / UPDATED 5 YEARS AGO

## Cyber attacks affect some radiation checks at Ukraine's Chernobyl site

By Reuters Staff 1 MIN READ

A New Safe Confinement (NSC) structure over the old sarcophagus covering the damaged fourth reactor at the Chernobyl nuclear power plant is seen from Ukraine's abandoned town of Pripyat, Ukraine, April 5, 2017. REUTERS/Gleb Garanich

UNIVERSITETET I OSLO

Side 11

11

"Money generated by criminal activities is difficult to hide; it sometimes constitutes primary evidence of the crime. Transfer of criminal funds in financial systems can be identified, if proper alert mechanisms are in place."

FN, UNDOC Program, "Money Laundering and the Financing of Terrorism: The United Nations Response", s. 3

UNIVERSITETET I OSLO

Side 12

12

# Sikkerhetskrav ved internettbetalinger

| «Sterk kundeautentisering» (SCA) | Transaksjonsovervåkningen | Rapporteringsplikter |
|---|---|---|
| PSD2 | PSD2 + 5AMLD | 5AMLD (+ PSD2) |



# Sikkerhetskrav ved internettbetalinger

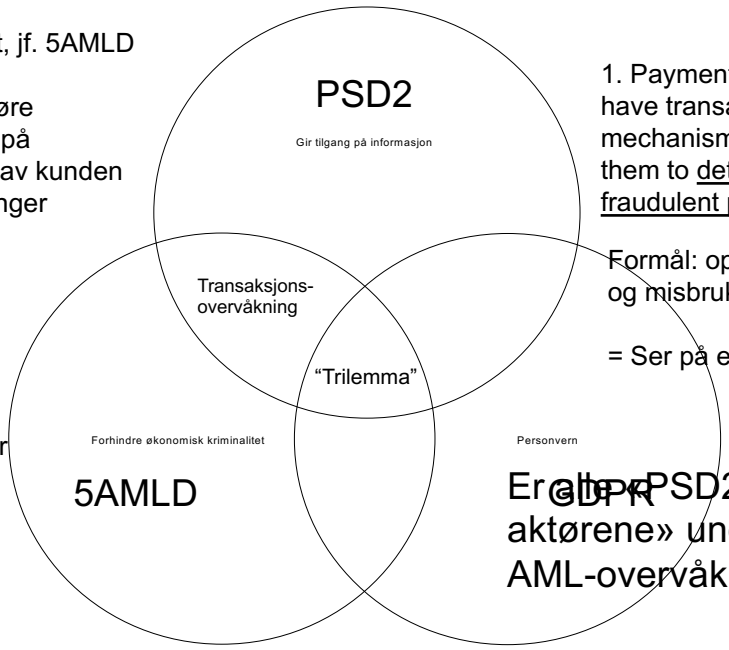
| «Sterk kundeautentisering» (SCA) | **Transaksjonsovervåkningen** | Rapporteringsplikter |
|---|---|---|
| PSD2 | **PSD2 + 5AMLD** | 5AMLD (+ PSD2) |

Undersøkelsesplikt, jf. 5AMLD

Plikt til å gjennomføre kundetiltak, basert på risikoklassifisering av kunden og kundens handlinger

Formål: Oppdage hvitvasking

= Ser etter mønster og avvik




RTS Article 2

1. Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions

Formål: oppdage svindel og misbruk

= Ser på enkelttransaksjoner

Er alle «PSD2-aktørene» underlagt AML-overvåkning?



# Hvorfor betyr forskjellen noe?

5AMLD Article 8

1. Member States shall ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those *relating to their customers, countries or geographic areas, products, services, transactions or delivery channels.* Those steps shall be proportionate to the nature and size of the obliged entities.

| **Transaksjonsovervåkningen** | Rapporteringsplikter |
|---|---|
| **PSD2 + 5AMLD** | 5AMLD |

# Hvorfor dette er så viktig:

= sentralt for å fastslå rekkeviddene av institusjonens plikter til å avdekke utnyttelse av det finansielle systemet

PSD2

Article 96

1. In the case of a **major operational or security incident,** payment service providers shall, without undue delay, **notify the competent authority** in the home Member State of the payment service provider.

5AMLD

Article 33(1)(a)

**All suspicious transactions**, including attempted transactions, **shall be reported**.

**Rapporteringsplikter**

**5AMLD**



# Er alle «PSD2-aktørene» underlagt AML-overvåkning?

PSD2 aktørene:

- ASPSP (account servicing payment service providers)
- PISP (payment initiation services)
- AISP (account information services)

5 AMLD Article 2

1. This Directive shall apply to the following **obliged entities**:

…

(2) **financial institutions**;

# Er TPP-ene underlagt 5AMLD?

Consultation paper, EBA JC/2019/87 s. 133

18.11.Monitoring:

As part of their CDD processes, PISPs and AISPs should ensure that their AML/CFT systems are set up in a way that alerts them to unusual or suspicious transactional activity. Even without holding significant information on the customer, PISPs and AISPs should use their own, or third party typologies, to detect unusual transactional activity.

ETPPA svar på EBA AML guidelines, 07/2020

«PISPs do not themselves execute payment transactions.»

«AISPs do not have any relation to financial transactions, they do not conduct financial activities. Therefore, they should not be subject to AML obligations.»

- Tilbyr ikke betalingskonto
- Er ikke del av den faktiske pengeflyten
- Overvåkningen bør utføres av banken som har betalingskonto



# Er TPP-ene underlagt 5AMLD?

Formålsbasert tolkning:

PSD2:

- Åpne opp betalingsmarkedet innad i EU
- Sikre innovasjon
- Minske hindringer

AML-reguleringen

- Beskytte mot utnyttelse av det finansielle systemet

På den ene siden:

- TPP-ene som «gatekeepers» i det finansielle systemet

På den andre siden:

- Fragmentert API-system (ikke standardisert i EU)
- Overholdelse av AML-reguleringen er dyrt (særlig for mindre TPP-er)
- Ansvarsfraskrivelse?

# Mulige løsninger

Skal man veie formålet med AML-regulering opp mot praktiske hensyn?

- Anlegge proporsjonalitetstankegang?
  - Avvist av EBA (EBA/Op/2022/06)
- Standardisere API-systemene
  - Arbeid i gang i EU – foreslått av EBA i juni i år
- Foreslått av næringen å sette krav til hvilken informasjon som skal deles mellom TPP-ene og banken
  - Fulgt opp i forslaget til EBA
  - Mulige gnisninger med GDPR?



# Transaksjonsovervåkningen

Regulatory Technical Standard til PSD2

RTS til PSD2

Article 2

General authentication requirements

1. Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions

Minimumskrav

Article 2

General authentication requirements

2. Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:

(a) lists of compromised or stolen authentication elements;

(b) the amount of each payment transaction;

(c) known fraud scenarios in the provision of payment services;

(d) signs of malware infection in any sessions of the authentication procedure;

(e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

# Gjennomføringen av transaksjonsovervåkning – privatrettslige følger?

- Forholdet til tilbakeføringsplikten
- Betydning for vurdering av kundens aktsomhet ved phishing/sosial manipulasjon



# Overvåkning og tilbakeføring

*Article 73*

1. Member States shall ensure that, without prejudice to Article 71, in the case of an unauthorised payment transaction, the payer's payment service provider refunds the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing.

*Fortale til PSD2*

(71) In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an *unauthorised transaction resulting from fraudulent behaviour by the payment service user* and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct, within a reasonable time, an investigation before refunding the payer.

# Overvåkning og kundens aktsomhet (phishing)

*Article 74*

(1) …

The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 69 with intent or gross negligence. In such cases, the maximum amount referred to in the first subparagraph shall not apply.

OBS: adgang til at medlemsstatene begrenser kundens ansvar ved «gross negligence»

*Fortalen til PSD2*

(72) In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties.



# Praksis

FinKN: tolkning av terskelen "grovt uaktsomt" (2022-59)

Nemnda har i sin tidligere praksis i saker om "phishing" vist til at det jevnlig advares mot falske e- poster, tekstmeldinger og telefonoppringninger som tilsynelatende kommer fra kjente avsendere, og hvor mottakeren blir bedt om å gi fra seg kortnummer og sikkerhetsopplysninger gjennom lenker eller på annen måte. Nemnda antar at advarsler mot å følge slike anmodninger og å gi fra seg sikkerhetsopplysninger er allment kjente. I nemndas tidligere praksis har det i de fleste sakene vært ansett grovt uaktsomt å følge slike lenker og å gi opplysninger. Det er likevel påpekt at vurderingen av kortholderens grad av skyld må foretas ut fra sakens individuelle omstendigheter. Det finnes i nemndas praksis flere saker hvor nemnda, enstemmig eller under dissens, på grunn av sakens spesielle omstendigheter har konkludert med at vilkåret om grov uaktsomhet ikke var oppfylt.

Nemnda kan ikke se at det foreligger slike spesielle omstendigheter i denne saken. Det er vanskelig å se en forbindelse mellom den falske tekstmeldingen og det brevet om barnas konti, som klageren tidligere hadde mottatt. Tekstmeldingen er lagt frem for nemnda. Den har et utenlandsk telefonnummer som avsender, og fremstår også ellers som amatørmessig og svært lite troverdig, uten logo eller andre kjennetegn som kan knytte den til banken. Heller ikke lenken inneholder noe som indikerer at den leder til en nettside som tilhører banken. Nemnda mener at kortholderen har opptrådt grovt uaktsomt ved å trykke på lenken for så å oppgi kortopplysninger, engangskoder og passord fra sin BankID. Hun kan holdes ansvarlig for egenandel på kr 12 000 som kortholderen må dekke ved grov uaktsomhet.

# EBA/Op/2022/06

293. … Relatedly, the EBA has observed that sometimes PSPs consider gross negligence to cover cases where the PSU is a victim of social engineering fraud since the latter were manipulated to hand over their PSU's credentials to a fraudster. The EBA sees such approaches as undesirable because *PSPs are also required under Article 2 of the RTS on SCA&CSC to carry out transaction monitoring mechanisms, including cases of well-known fraud scenarios, as well as expected to raise PSUs' awareness and provide assistance and guidance*

- Phishing/svindel ved sosial manipulasjon er det transaksjonsovervåkningen er ment å avdekke, og følgelig stanse
- I alle tilfeller skal ikke kundens handlinger ansees «grovt uaktsomt»



# TOSLO-2020-110915 – "Direktørbedrageri"

"Banken hadde et rutineverk for å forebygge og motvirke svindel. Hvorvidt disse interne rutinene er overholdt, er et viktig moment i aktsomhetsvurderingen.

…

Etter rettens syn innebar det vedvarende unntaket fra automatisert kontroll et avvik fra forsvarlig handlemåte, som en eller flere ansatte i banken kan bebreides for.

…

Det forelå følgelig mangler ved den manuelle vurderingen i svindelkontrollen, som innebærer avvik fra forsvarlig handlemåte som en eller flere ansatte i banken kan klandres for.

…

Retten mener at Edison Norge AS selv bør bære hovedansvaret for transaksjonene som skjer fra og med 2. oktober 2019.

…

Retten er kommet til at erstatningen bør settes ned med 75 %o av netto tapet (125 640 437,98 kroner) slik at erstatningen settes til 31 410 109 kroner."