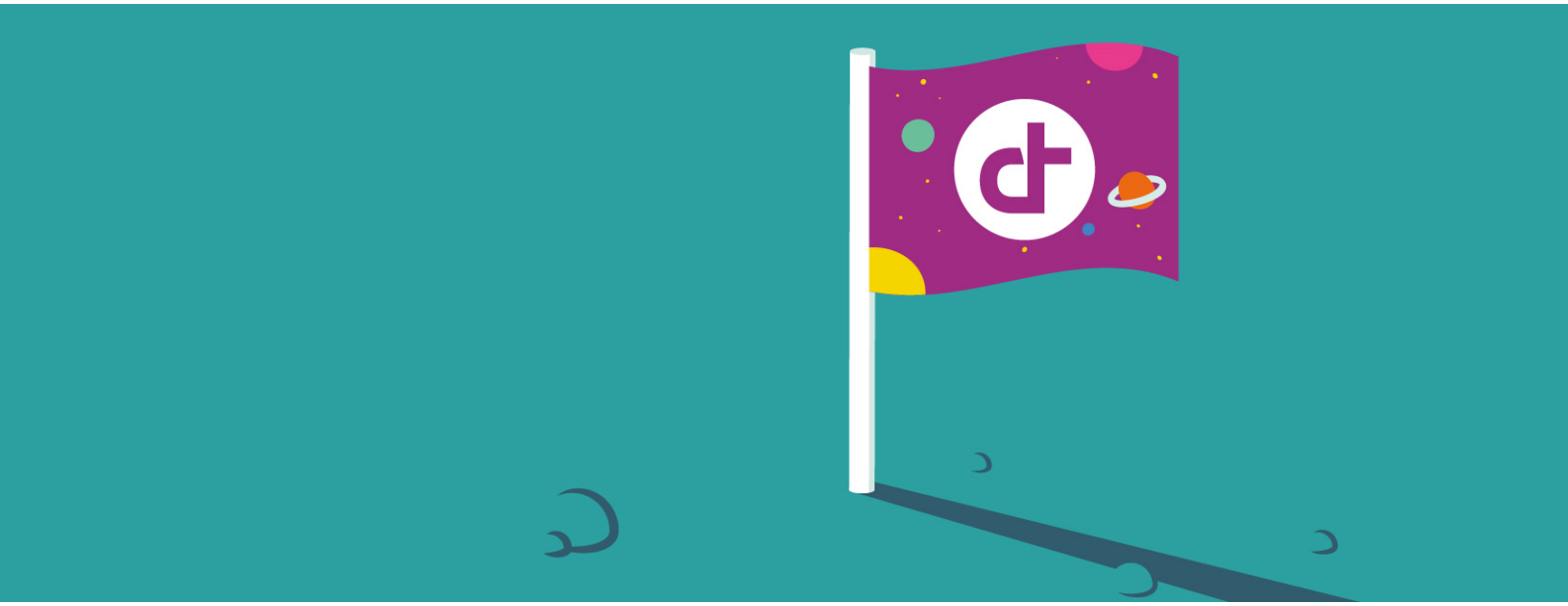
devoteam

Innovative technology consulting for business



Imødegåelse af snyd ved eksamen

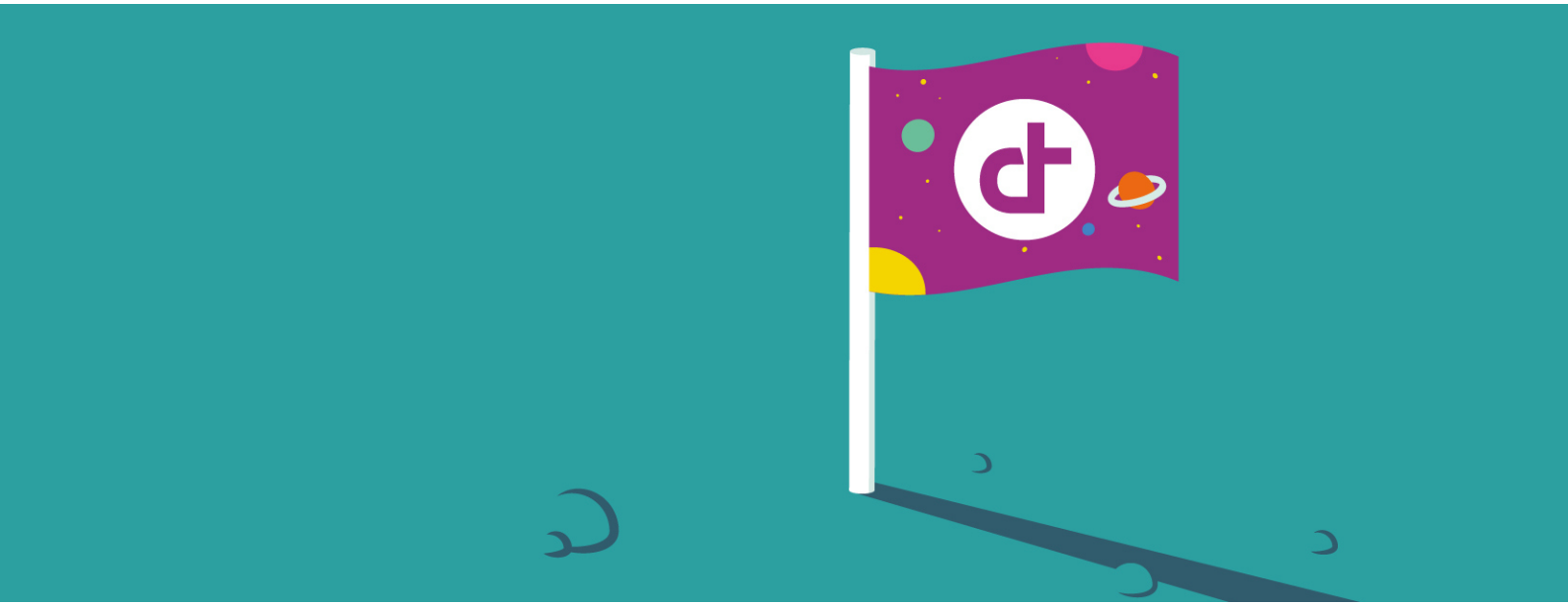
Rapport om de tekniske muligheder for at imødegå snyd ved eksamen

17. august 2016

MINISTERIET FOR
BØRN, UNDERVISNING
OG LIGESTILLING

devoteam

Innovative technology consulting for business



devoteam

Indholdsfortegnelse

1 Resumé og læsevejledning

1.1 Resumé

Styrelsen for Undervisning og Kvalitet (herefter STUK) har bedt Devoteam analysere, hvilke tekniske muligheder der er for at begrænse snyd ved eksamen. Denne rapport udgør Devoteams samlede analyse. Analysen er gennemført som en eksplorativ analyse baseret på interviews og internet-research. Interviewene har opfattet elever og ledere på de gymnasiale uddannelser samt interviews med repræsentanter for universiteter og professionshøjskoler, for skolemyndigheder i Norge samt for leverandører af løsninger til at imødegå snyd.

Analysen beskriver erfaringerne med at begrænse snyd, og giver et overblik over de tekniske muligheder for at begrænse snyd. Devoteam har ikke analyseret omfanget af snyd, afprøvet konkrete løsninger til at imødegå snyd eller vurderet effekten eller legaliteten af de midler, som i dag anvendes til at imødegå snyd.

Analysen fokuserer på snyd under eksaminandens besvarelse af opgaven ved de centralt stillede skriftlige stedprøver. Analysen ser på muligheder for at imødegå snyd gennem initiativer *før* (fx ved at vejlede eller ved at etablere netværksfiltre), *under* (filtrering og logning af internettrafik) og *efter* besvarelse (fx plagiatkontrol).

Erfaringer

Erfaringerne med snyd og imødegåelse af snyd i Danmark viser, at snyd kan ske ved

- Ikke-tilladt brug af den tilladte internetadgang, fx ved at bruge redigeringsfunktionen i Wikipedia til at kommunikere med andre
- Brug af ikke-tilladt elektronisk kommunikation, fx smartphones
- Brug af andre, ikke elektroniske kanaler, fx brug af ikke-tilladte noter gemt på elektroniske eller ikke-elektroniske medier.

Mulige tekniske midler til at imødegå snyd

Devoteam har identificeret en række forskellige tekniske muligheder for at imødegå snyd. De enkelte muligheder er vurderet op mod følgende kriterier:

Kriterium	Beskrivelse
BYOD	Kan løsningen understøtte, at eksaminanderne bruger deres egen computer (evt. begrænset til udvalgte typer af devices)
BYOA	Kan løsningen understøtte, at eksaminanderne bruger deres egne programmer
Data på egen computer	Kan løsningen understøtte brug af kun tilladte data/programmer på egen computer
Kommunikation	Kan løsningen forhindre kommunikation med andre
Tilladte/Ikke-tilladte kilder	Kan løsningen forhindre adgang til ikke-tilladte kilder på tilladte netsteder
Tilladte/Ikke-tilladte netsteder	Kan løsningen forhindre adgang til ikke-tilladte netsteder
Omkostninger	Hvilke særlige omkostninger vil der være ved løsningen
Sårbarheder	Hvilke sårbarheder har løsningen

Egenskaberne ved de mest relevante løsninger mod snyd, sammenlignet med det almindelige tilsyn, kan sammenfattes således:

Løsning	Eksempel	Effekt						Forudsætninger	Omkostninger	Sårbarheder
		BYOD/ BYOA	Data på egen computer	Ikke tilladt kanal	Kommu-nikation	Tilladte/ Ikke tilladte kilder	Tilladte/ Ikke tilladte netsteder			
Tilsyn	Forbedret praksis	Ja/Ja	Kan afsløre	Kan måske afsløre	Kan afsløre	Kan afsløre	Kan afsløre	Ingen særlige	Opgradering af tilsyn	Manglende it-kompetencer
Filtrering	Forbedret praksis	Ja/ja	Ingen effekt	Ingen effekt	Kan vanskelig-gøre	Ingen effekt	Kan skelne med usikkerhed	Eksamen i egne lokaler	Server Content filtre Opsætning af filtre/server	Store kompetencekrav Andre net Mange muligheder for fejl
Logning	Som visse it-centre	Ja/Ja	Ingen effekt	Ingen effekt	Kan afsløre	Ingen effekt	Kan afsløre	Eksamen i egen lokaler	Analysesystem Manuel gennemgang af log	I praksis skal der foreligge mistanke før gennemgang af log Andre net
Secure Browser	FLOWlock	Ja/Nej	Forhindrer	Forhindrer	Forhindrer	Ingen tillades	Ingen tillades	Ingen særlige	Licens, opsætning	Internationalt hackermål
Exam Monitor	Exam Monitor	Ja/Ja	Kan afsløre	Kan afsløre	Kan afsløre	Kan afsløre	Kan afsløre	Ingen særlige	Licens Opsætning Gennemgang af log	Afhængig af netforbindelse Kompetencekrav Behov for løbende opdatering

Devoteam vurderer, at en løsning som Exam Monitor giver en stor chance for at afsløre misbrug, der dog forudsætter, at uddannelsesstedet afsætter ressourcer til fx en omfattende opsætning af systemet eller til gennemgang af eksamensloggen. Hvis Exam Monitor suppleres med spærring af andre af skolens net, opdaterede eksamensregler samt et aktivt tilsyn, som kan kende forskel på tilladte og ikke-tilladte hjælpemidler (og fx inddrage smartphones og lign.), kan der opnås en pæn sandsynlighed for at afsløre snyd. Hvis hertil føjes en præcis og passende alvorlig vejledning, vurderer Devoteam, at der kan nås meget langt i retning af at imødegå snyd.

1.2 Læsevejledning

Rapporten er struktureret således:

I afsnit 2 redegør vi for baggrund og rammer for analysen, herunder for analysens emner og afgrænsning, samt for hvordan vi har gennemført analysen.

I afsnit 3 redegør vi for den undersøgelse, som vi har foretaget blandt gymnasieelever og eksamensansvarlige ved gymnasierne af mulighederne for snyd, og af hvilke foranstaltninger skolerne træffer for at imødegå snyd.

I afsnit 4 redegør vi for de yderligere undersøgelser, som vi har gennemført for at belyse emnet fra flere vinkler og for at søge information om, hvordan andre lande håndterer truslen om snyd ved digitale eksamener.

I afsnit 5 gennemgår vi de tekniske midler, som vi har fundet og behandlet i relation til de aktuelle danske eksamensformer.

I afsnit 6 samler vi analysens resultater og giver vores anbefalinger og forslag til imødegåelse af snyd ved eksamen i de gymnasiale uddannelser.

Afsnit 7 perspektiverer analysens resultater til eksamener i folkeskolen.

I bilag 1 resumerer vi erfaringer med imødegåelse af snyd ved eksamen ved de gymnasiale uddannelser i Norge.

Bilag 2 indeholder omkostningsskøn for nogle af de tekniske midler til imødegåelse af snyd.

2 Indledning

2.1 Baggrund og opdrag

I forbindelse med folkeskoleprøveinitiativerne i efteråret 2014 blev det tilkendegivet over for folkeskoleforligskredsen, at Undervisningsministeriet ville igangsætte en analyse, der skulle se på muligheden for at begrænse snyd ved eksamens- og prøveafholdelse. Det skal bl.a. ses i sammenhæng med, at den teknologiske udvikling gør elevernes adgang til internettet og andre it-baserede hjælpemidler lettere, og at prøver med adgang til internettet bliver benyttet i større og større grad.

Styrelsen for Undervisning og Kvalitet (STUK) har derfor bedt Devoteam om at gennemføre en analyse, der skaffer viden om og overblik over, hvilke erfaringer med at bekæmpe snyd der findes hos de gymnasiale skoler, og hvilke tekniske muligheder der er for at bekæmpe snyd ved eksamen, herunder for at sikre, at opgavebesvarelserne er elevernes egne produktioner ved prøver og eksamener. Tekniske muligheder kan både omfatte konkrete tekniske blokeringer og indsatser som overvågning mv. I sammenhæng hermed skal gives en vurdering af økonomiske, praktiske og formelle muligheder og begrænsninger.

2.2 Analysens emner

2.2.1 Snyd ved eksamen

Analysen skal se på tekniske muligheder for at imødegå snyd ved eksamen i de gymnasiale uddannelser.

De "gymnasiale uddannelser" omfatter ca. 150.000 elever, jf. Tabel 1 nedenfor, ved 225 institutioner (skoler).

"Eksamen" er i denne analyse de eksamener, hvor opgaverne stilles af Ministeriet for Børn, Undervisning og Ligestilling. Hovedfokus er på skriftlige stedprøver, men analysen omfatter også observationer om forberedelsestiden på skolen til mundtlig eksamen, hvor en sådan forekommer. Analysen omfatter således ikke de lokalt stillede terminsprøver, og heller ikke de store skriftlige opgaver, SSO og SRP, der ikke afvikles som stedprøver. Der afholdes årligt ca. 215.000 skriftlige eksamensbegivenheder, dvs. ca. 215.000 gange sidder der en eksaminand til stedprøve i et eller andet gymnasiefag. Antallet inkluderer sommer-, syge og vintereksamen. (Se Tabel 1 nedenfor.)

Tabel 1. Antal elever og antal skriftlige prøvebegivenheder ved de gymnasiale uddannelser[1]

	Antal elever 2014	Eksamener 2015-2016
Almengymnasiale uddannelser	108.305	164.193
Erhvervsgymnasiale uddannelser	40.451	52.673
Total	**148.756**	**216.866**

"Snyd" skal i denne analyse forstås som benyttelse af ikke-tilladte hjælpemidler - herunder bistand fra andre personer - under eksamen.

[1] *Bestand: Styrelsen for IT og Læring på data fra Danmarks Statistik. Eksamener: Styrelsen for Undervisning og Kvalitet.*

2.2.2 Faktisk registreret snyd ved eksamen[2]

Styrelsen for Undervisning og Kvalitet har gennemført en landsdækkende undersøgelse af snyd ved de mundtlige og skriftlige prøver i de gymnasiale uddannelser under prøveterminerne maj/juni og august 2014 og december/januar 2014/15. I alt er der i perioden aflagt ca. 550.000 prøver ved de 225 gymnasiale institutioner. Resultatet fremgår af nedenstående Tabel 2.

Tabel 2. Antal formodninger om snyd og antal bortvisninger som følge af snyd

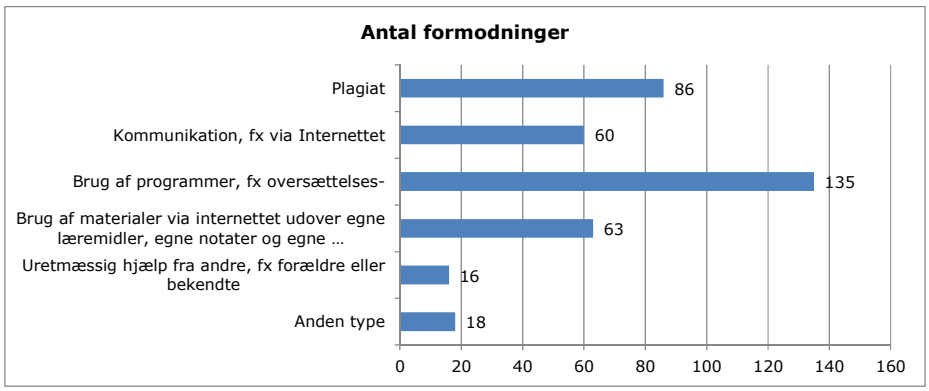
Formodninger om snyd ved prøver og bortvisninger fra prøver		
	Formodning om snyd	**Bortvisning**
Mundtlige prøver	25	14
Skriftlige prøver	304	129
I alt	329	143

Prøverne i studieretningsprojektet (SRP) og større skriftlig opgave (SSO) er ikke indgået i undersøgelsen.

218 ud af 225 institutioner har besvaret undersøgelsen. Der har været formodning om snyd på 124 af landets gymnasiale uddannelsessteder, mens der ikke har været formodninger om snyd på 94 institutioner. Ved 18 af skolerne var der tale om mere end fire formodninger, og tre skoler havde mellem ti og 17 formodninger.

Institutionerne blev i undersøgelsen bedt om at angive, hvilke årsager der har været til de formodninger om snyd, som de har registreret i de betragtede prøveterminer. Institutionernes svar er opsummeret i nedenstående Figur 1.

Figur 1. Fordeling af antal formodninger om snyd på årsager



Note: Under kategorien "Anden type" har institutionerne eksempelvis angivet brud på institutionens eksamensreglement, fx uretmæssig brug af mobiltelefon, forsøg på at anvende hjælpemidler ved prøver, hvor dette ikke er tilladt, og kommunikati-

[2] *STUK, 160203 Notat om undersoegelse af snyd ved proeverne i de gymnasiale uddannelser i 2014 15*

on mellem eksaminander under prøverne via ombytning af fysiske sedler eller USB-stik.

Det ses, at brug af elektroniske programmer, fx oversættelsesprogrammer, hvor det ikke er tilladt, ifølge institutionernes svar er den hyppigste årsag til formodninger om snyd ved prøverne. Brug af materialer fra internettet eller kommunikation via nettet ses hver især at være ca. halvt så hyppigt som brug af ikke-tilladte programmer og tilsammen at have omtrent samme omfang. Forsøg på plagiat kan meget vel omfatte illegal brug af nettet for at finde frem til en egnet kilde til plagiering. Formodninger om snyd handler kun i mindre grad om uretmæssig hjælp fra andre, fx forældre eller bekendte.

Devoteam formoder, at omfanget af observeret snyd dels afhænger af den faktiske forekomst af snyd, dels af omfang og karakter af den imødegående indsats. Devoteam har derfor valgt i den fortsatte undersøgelse at rette henvendelse til nogle af de institutioner, som har indrapporteret flest tilfælde af snyd (Se afsnit 2.3)

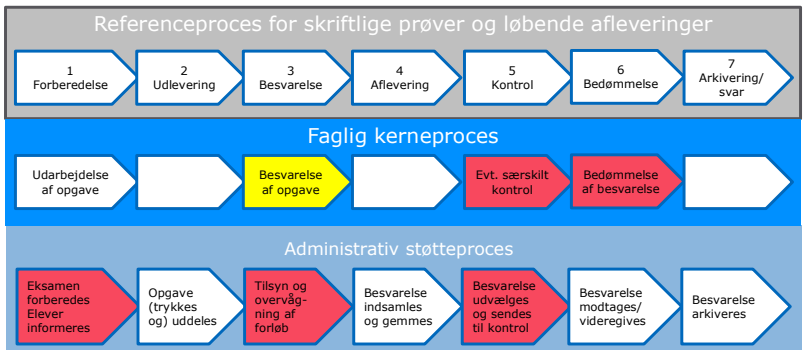
2.2.3 Eksamensprocessen

Analysen fokuserer på snyd under eksamen. Figur 2 nedenfor viser en referenceproces for eksamen. Det fremgår af figuren, at eksamensprocessen kan deles op i en række delprocesser. Centralt (markeret med gult) står eksaminandens besvarelse af opgaven. Det er snyd under denne aktivitet, der er analysens fokus.

Snyd kan i princippet også forekomme under de øvrige aktiviteter. Fx kan eleven hypotetisk skaffe sig adgang til at se opgaven, inden den udleveres eller til at rette i besvarelsen, efter den er afleveret. Snyd uden for besvarelsesprocessen er imidlertid ikke omfattet af nærværende analyse.

Imødegåelse af snyd kan til gengæld foregå både før, under og efter selve besvarelsesprocessen. Dette er markeret med rødt på figuren.

Figur 2 Referenceproces for eksamen



Figur 3 nedenfor viser nogle eksempler på muligheder for at forebygge, forhindre eller afsløre snyd før, under og efter besvarelsen (Bemærk, at disse eksempler ikke skal forstås som anbefalinger.)

Figur 3. Eksempler på imødegåelse af snyd før, under og efter besvarelsen

Før	Under	Efter
• Vejledning • Tilpasse eksamensreglement • Etablering af netværksfiltre	• Filtrering og logning af internet-trafik • Overvågning (eksamenstilsyn)	• Inspektion af log • Plagiatkontrol

2.2.4 Eksamensformer og lære- og hjælpemidler

De centralt stillede skriftlige stedprøver afvikles i dag i overvejende grad som digitale eksaminer, hvor eksaminanderne selv medbringer en computer (BYOD) og kan anvende de programmer (fx til tekstbehandling), som de er vant til fra dagligdagen. I mange tilfælde benyttes skolens interne studieadministrative system og netværk til digital udlevering af opgaven og digital modtagelse af besvarelsen. Efter introduktionen af Netprøver.dk vil digital udlevering af opgaven og digital aflevering af besvarelsen varetages af dette system.

De grundlæggende regler om brug af hjælpemidler ved eksamen fremgår af nedenstående § 15 i bekendtgørelse om prøver og eksamen i de almene og studieforberedende ungdoms- og voksenuddannelser, nr. 343 af 8. april 2016:

> § 15. Under prøverne er anvendelse af hjælpemidler, herunder elektroniske, tilladt, jf. dog stk. 2, medmindre der i reglerne for den enkelte uddannelse er fastsat begrænsninger.
> Stk. 2. Eksaminanden har under prøver, der er underlagt tilsyn, alene adgang til internettet, for så vidt angår egne læremidler, egne notater og egne arbejder.

Formuleringen i § 15 skal forstås således, at anvendelse af internettet som hovedregel ikke er tilladt ved eksamen. Men i praksis er der omfattende undtagelser fra denne hovedregel. Dels i medfør af bestemmelsen i stk. 2 om egne læremidler, egne notater og egne arbejder, dels i medfør af en række forsøgsordninger med eksamener med adgang til internettet.

Ministeriet har i en vejledning[3] til § 15, stk. 2, præciseret, at

> det ikke er eksaminanden, men skolen, der inden for de givne rammer beslutter, hvad der ved den enkelte prøve, hvortil der ellers ikke er netadgang, er "egne læremidler". Der skal være tale om et bestemt, konkret læremiddel, herunder i- og e-bøger, som et hold/en klasse på skolens foranledning har benyttet i undervisningen. Bestemmelsen giver ikke adgang til brug af hjælpemidler ud over det, der er tilladt i den konkrete læreplan. Eksaminanderne får således ikke flere hjælpemidler til rådighed end tidligere – mediet for hjælpemidlerne/adgangen hertil er blot anderledes. Det er forudsat, at det pågældende hjælpemiddel i øvrigt er tilladt ved prøven, og at skolen kan sikre prøveforhold, der er egnede til at udelukke, at eksaminanden kommunikerer utilsigtet.

Ministeriet giver bl.a. følgende eksempel på, hvad der kan være egne læremidler på nettet:

> Elever på et hold har i undervisningen benyttet Infomedia (en ganske bestemt artikel). Derved har eleverne under prøven og i forberedelsestiden kun online adgang til at benytte denne bestemte artikel. Det giver dem ikke retmæssig adgang til at benytte andre artikler i Infomedia.

[3] *140414 Vedroerende fortolkningen af § 15 stk 2 i den almene eksamensbekendtgoerelse*

Forsøgsordninger med adgang til internettet tillader som regel alle hjælpemidler. *I ingen tilfælde er det tilladt at kommunikere med andre personer under eksamen.*

I praksis betyder det for denne analyse, at der findes nedenstående tre eksamensformer med hensyn til brug af internettet:

A. Eksamen uden hjælpemidler (evt. som del af toleddet eksamen)
B. Eksamen med adgang til egne læremidler, egne notater og egne arbejder via internettet
C. Eksamen med fuld adgang til internettet

Ved eksamen uden hjælpemidler må eksaminanden heller ikke benytte filer eller programmer på sin egen computer (bortset fra tekstbehandlingsprogrammet). Ved de øvrige eksamensformer må der kun bruges evt. hjælpemidler på computeren, hvis de er godkendt i henhold til reglerne.

2.2.5 Imødegåelse af snyd

Snyd ved eksamen har formentligt altid forekommet, også før introduktion af computer og internet ved eksamen. Denne analyse vil da også nævne nogle eksempler på snyd, som ikke anvender tekniske midler og ikke kan imødegås med tekniske midler.

Den centrale opgave med hensyn til snyd er imidlertid at forbygge, forhindre eller afsløre snyd i form af:

- Kommunikation med andre
- Misbrug af andre end tilladte materialer på internettet
- Misbrug af materiale eller programmer på eksaminandens computer

Skolen skal altså kunne skelne mellem brug af internettet som tilgang til tilladte hjælpemidler hhv. som kanal for kommunikation med andre, fx besked- eller filudveksling. Skolen skal også kunne skelne mellem adgang til et tilladt hjælpemiddel, fx en artikel i Infomedia, og til et andet, ikke-tilladt hjælpemiddel, fx en anden artikel i Infomedia (jf. eksemplet i afsnit 2.2.4).

Det er det centrale formål med denne analyse at skaffe viden om hvilke tekniske muligheder, der er for at løse ovenstående udfordring.

2.3 Tilrettelæggelse af analysen

Devoteam har løst opgaven i perioden februar til juni 2016.

Devoteam har tilrettelagt opgaven som en eksplorativ analyse, baseret på en kombination af interviews og internet-research:

- Der er gennemført telefon-interviews med otte elever. Devoteam rettede henvendelse til henholdsvis Landssammenslutningen af Handelsskoleelever og Erhvervsskolernes ElevOrganisation, der udpegede hhv. tre HHX-elever og to HTX-elever til at deltage i interviews. Devoteam rettede også henvendelse til Danske Gymnasieelevers Sammenslutning, DGS, der desværre ikke kunne finde elever, der ville deltage i interviews. Kontakten til tre STX elever blev i stedet formidlet af Ørestads Gymnasium.
- Der er desuden gennemført telefon-interviews med ledere, eksamens- eller it-ansvarlige ved 11 skoler og et fælles it-center. Interviewene omfatter skoler med erhvervsgymnasiale og almen gymnasiale uddannelser, men interviewene afdækker selvfølgelig ikke forholdene ved alle landets 225 gymnasiale institutioner. Devoteam har udvalgt skolerne blandt de skoler, som har indrapporteret flest tilfælde af mistanke om snyd til STUK's undersøgelse (omtalt i afsnit 2.2.2)

- Der er gennemført telefoninterviews eller besøg ved de danske universiteter og et fælles It-center for professionshøjskoler og gymnasiale skoler.
- Der er ført drøftelser med udbyderne af Exam Monitor og WISEflow (se afsnittene 5.2.4 og 5.2.5)
- Der er gennemført telefon-interviews med repræsentanter for Utdanningdirektoratet i Norge og for et fylke (Se Bilag 1 – Erfaringer fra Norge)
- Devoteam har gennemført en internetbaseret analyse af status og udvikling inden for digital eksamen i globalt perspektiv

Det bemærkes, at Devoteam ikke har:

- Undersøgt omfanget og arten af snyd ved eksamen
- Afprøvet eller verificeret funktionen af de omtalte midler til imødegåelse af snyd
- Vurderet effektiviteten eller legaliteten af de midler, som nogle skoler har oplyst, at de tager i anvendelse

3 Erfaringer med snyd og imødegåelse

Devoteam har gennemført telefoninterviews med elever (3 HHX-, 2 HTX- og 3 STX-elever) og ledere/eksamensansvarlige ved 11 gymnasiale skoler og et it-service-center med henblik på at indsamle erfaringer med snyd og - ikke mindst – imødegåelse af snyd. Erfaringerne er gengivet i afsnit 3.1 .

Devoteam har også indhentet erfaringer med imødegåelse af snyd fra universitetssektoren. Resultatet er gengivet i afsnit 3.2 . Devoteam har samtidigt undersøgt, hvilke erfaringer der er indhentet i Norge ved tilsvarende uddannelser. Observationerne herfra er gengivet i Bilag 1 – Erfaringer fra Norge og resumeret i afsnit 3.3 .

3.1 Erfaringer fra de gymnasiale uddannelser

I det følgende gennemgås de indhentede erfaringer fra de danske gymnasiale uddannelser. Først erfaringer med snydemuligheder, dernæst erfaringer med imødegåelse af snyd.

3.1.1 Snydemuligheder

De adspurgte elever tog snyd alvorligt. De gav udtryk for, at det ikke kun er skolen, der bliver snydt, men også kammeraterne. På den anden side mente de ikke, at snyd forekom særligt ofte på deres skole eller blandt deres kammerater. Vi bad dem alligevel om at fortælle om snyd, som de kendte til eller havde hørt om, at nogen gjorde. Da der kun er interviewet et relativt lille antal elever, og da eleverne antageligt kun har haft andenhånds kendskab til snyd, kan der være måder at snyde på, som ikke er afdækket.

De eksamensansvarlige på skolerne mente generelt, at snyd kun forekom i meget ringe omfang på deres skole. Hyppigheden er belyst i ministeriets undersøgelse, som er refereret i afsnit 2.2.2 Der var forskellige opfattelser af, om snyd var mere eller mindre udbredt end den alminidelige forestilling. Ingen havde dog lyst til at gætte på mørketallene, og alle traf deres forholdsregler for at forebygge, forhindre eller afsløre snyd,

I det følgende resumeres de oplysninger om snydemuligheder (kanaler) og efterspurgte videnskilder. De identificerede kanaler kan deles op i hhv.:

- Ikke-tilladt brug af den tilladte netadgang
- Ikke-tilladt elektronisk kommunikation
- Andre, ikke elektroniske kanaler

3.1.1.1 Snyd via ikke-tilladt brug af den tilladte netadgang

Når eksaminanden får stillet en internetadgang til rådighed til fx egne hjælpemidler, kan denne adgang også misbruges til snyd i form af adgang til ikke-tilladte videnskilder på nettet eller til kommunikation med andre.

Skolerne nævner, at snyd ved brug af Google Translate er det hyppigst forekommende, uden nogen klar nummer to blandt de øvrige internetkilder, jf. også afsnit 2.2.2 og Figur 2 ovenfor. (Nogen skoler mener, at brug af Google Translate burde opfattes som uagtsomt snyd. De mener, at Google Translate er så indarbejdet i elevernes daglige it-brug (og opfattes som bedre end ordbøger), at eksaminanderne ikke opfatter det som forbudt område.)

Den tilladte internetadgang kan også bruges til udveksling af tekster med andre eksaminander eller udenforstående, fx gennem sociale medier eller samarbejdsværktøjer som OneNote, DropBox o.l. samt fora på skolens eget intranet/studienet. Tjenester som Spotify og Wikipedia har også været nævnt, fordi man kan bruge indbyggede funktioner til indbyrdes kommunikation.

Wikipedia kan illustrere problemet. Wikipedia er et hjælpemiddel, der kan være aktuelt i mange tilfælde. Men Wikipedia åbner desværre – gennem redigeringsfunktionen - også op for kommunikation mellem to eller flere eksaminander eller udenforstående, der på forhånd har aftalt at bruge redigeringsfunktionen for et bestemt, upåfaldende opslag som kommunikationsforum, dvs. aftalt, at de via redigeringsfunktionen skriver spørgsmål og svar ind i teksten for opslaget.

Samtidigt er Wikipedia et eksempel på en tjeneste, som bruger krypteret kommunikation med sine brugere (https-protokollen), hvilket gør det muligt for eksaminanden at skjule indholdet af sin kommunikation som modtræk til evt. overvågning af nettrafikken.

Eleverne nævner i øvrigt, at de kan være i tvivl om fortolkningen af de "whitelists" over tilladte hjemmesider, som de får udleveret. Er det fx tilladt eller ikke tilladt at klikke videre til en underside til den tilladte side?

3.1.1.2 Snyd via ikke-tilladt elektronisk kommunikation

Eksaminanden kan skaffe sig adgang til illegal elektronisk kommunikation på flere måder. Den mest nærliggende måde er brug af en smartphone, der kan fungere som telefon, som net-book, eller som middel til at oprette en peer-to-peer-forbindelse til en anden eksaminand eller en hjælper. På denne måde bruges forbindelsen formentlig kun til udveksling af beskeder og ikke til tekstimport.

Den ikke-tilladte forbindelse kan imidlertid også oprettes til brug for eksaminandens tilladte computer, fx ved at koble computeren til andre net, eller ved at bruge mobiltelefonen som WiFi-hotspot. I så fald vil der kunne opnås samme muligheder som ved misbrug af den tilladte internetforbindelse (dog afhængigt af evt. begrænsninger i de alternative net, der benyttes).

Brug af Apple Watch el. lignende kropsbåret udstyr kan give samme muligheder som en smartphone, men bedre skjult.

En mere eksotisk, men ikke urealistisk, snydekanal er et "spion-sæt" med mikrofon/øresnegl, der kan bruges til kommunikation med en hjælper

3.1.1.3 Snyd via andre, ikke elektroniske kanaler

Indsamlingen af erfaringer blandt skoler og elever har også identificeret nogle snydemuligheder, der ikke er afhængige af elektronisk kommunikation.

Der er dels tale om følgende metoder baseret på de ovenfor nævnte devices, men ikke kommunikation:

- Brug af materiale, som er gemt på egen computer
- Brug af noter, lagret på mobiltelefonen
- Noter, indtalt i musik-stream på iPod o.l.

Dels er der tale om følgende metoder, baseret på ikke-elektronisk kommunikation:

- Udveksling af USB-sticks i lokalet eller på toiletterne
- Udveksling af noter på papir
- Bytte udprint med anden elev (print under eksamen kan være tilladt)
- Aflæsning af andre eksaminanders skærme
- Tegn og fagter
- Bytte plads under forløbet (via koordinerede toiletbesøg, hvis tilsynet ikke kender hver enkelt eksaminand)
- Hvisken
- Samtale på toilettet eller forberedelseslokalet (når der ikke er tilstrækkeligt tilsyn)

3.1.2 Imødegåelse af snyd

En række af interviews med ledere, eksamensansvarlige og it-chefer ved 11 gymnasiale institutioner og et it-fællesskab har vist os, at skolerne i dag foretager en række forskellige teknisk orienterede foranstaltninger for at imødegå snyd ved eksamen. I det følgende beskrives disse metoder, fordelt på placering i eksamensforløbet, dvs. *før*, *under* eller *efter* eksamen.

3.1.2.1 Imødegåelse

De adspurgte gymnasieskoler bestræber sig på at imødegå snyd ved forskellige kombinationer af de nedenfor beskrevne følgende indsatser.

Før eksamen

- I en længere periode før såvel som lige op til eksamen gives skriftlige og mundlige vejledninger om generelle og lokale eksamensregler. I disse vejledninger gives også tydelige advarsler mod snyd og beskrivelse af de mulige konsekvenser heraf. I denne kampagne kan nogle steder indgå, at nylige, lokale eksempler på episoder (fx fra med opdaget snyd fra terminsprøverne) trækkes frem til skræk og advarsel.

- En skole giver eksaminanderne påbud om at gemme links til de tilladte hjælpemidler som bogmærker på forhånd, og forbyder dem i øvrigt at søge på nettet under eksamen.

Under eksamen

- Udover generelle regler om forbud mod brug af sociale medier, fildeling, chat og messenger-tjenester mv., kan der være fastsat lokale regler med forbud mod at medbringe mobiltelefoner, musikafspillere og spil til eksamen.

- Opkvalificering eller supplering af eksamenstilsynet, så det er mere it-kyndigt. Eleverne synes p.t. at eksamensvagterne er dårligt rustede til opgaven. Nogen skoler er gået over til at hyre yngre studerende med it-kundskaber, evt. gennem et vikarbureau, som har specialiseret sig heri.

- En skole giver eksaminanderne påbud om at bevare browser-historik på computeren og ikke benytte sig af anonym browsing. Skolen forbeholder sig retten til at inspicere browserhistorikken, som skal bevares på eksaminandens computer indtil karakteren foreligger.

- Hvis der opstår mistanke om snyd under eksamen, praktiserer nogle skoler en umiddelbar gennemgang af eksaminandens computer for ikke-tilladte aktiviteter og ikke-tilladte links.

- Flere skoler oplyser, at de benytter sig af forskelige former for filtrering af internettrafikken. Der kan være tale om et særligt elevnet eller eksamensnet, der kun giver adgang til skolens egne servere, hvor man har anbragt opgaverne og de hjælpemidler, som man har valgt at stille til rådighed. Der kan også være tale om at give adgang til internettet, men kun til visse IP-adresser. Dette angives dog at fordre en større indsats i forhold til vedligehold mellem hver eksamen, og være meget vanskeligt, hvis man har flere eksamener samlet i samme lokaler.

- Andre skoler oplyser, at de logger nettrafikken med henblik på kunne afsløre og dokumentere snyd i form af illegal nettrafik. Skoler tilknyttet it-fællesskaber er typisk bedre stillede, fordi de fællesskaber, som vi har kendskab til, har udviklet analyseprogrammer, der kan vise nettrafikken for hver eksaminand på en overskuelig måde. Log-gennemgangen aktiveres som regel kun, hvis der er opstået mistanke under eksamen eller hvis censor retter henvendelse om snyd.

- Nogle skoler lader lejlighedsvis it-personale scanne i eksamenslokalet for åbne hot-spots. Dog, efter det oplyste, uden derved at have afsløret snyd.

- En enkelt skole har gennemført et forsøg med elektronisk overvågning af skærmene på eksaminandernes computere (Op til 16 skærme kunne overvåges af en person). Skolen har vurderet, at en sådan overvågning krævede for meget personale (en vagt pr. 16 eksaminander.)

- En skole oplyser, at man af hensyn til sikkerheden under forberedelsestiden til mundlig eksamen vælger at forbyde medbragte computere og i stedet stiller en af skolens computere til rådighed.

Efter eksamen

- De fleste af de adspurgte skoler anvender en eller anden form for plagiatkontrol ved interne prøver. De angiver, at de forventer sig meget af den plagiatkontrol, der forventes at være en del af Netprøver.dk.

- En skole har i et tilfælde af mistanke taget en eksaminand ind til "Supplerende overhøring" under deltagelse af den eksamensansvarlige og en lærer for at validere, om eksaminanden kunne præstere som i prøven.

3.1.2.2 Barrierer for imødegåelse

Udtalelserne fra skolerne har også omfattet en række udsagn om barrierer for bedre imødegåelse af snyd ved eksamen, som kan resumeres således:

- Flere skoler anfører, at tilsynet ikke har de fornødne kompetencer og/eller, at det er vanskeligt at rekruttere vagter, som har tilstrækkelige kompetencer til at afsløre snyde hos eksaminanderne.

- Nogle skoler peger på vanskeligheder med at etablere overvågning og logning af nettrafikken under eksamen. Der kan dels være tale om, at skolen ikke benytter personligt log-on til lokalnettet eller at en elev kan låne log-in-id fra en anden. I så fald kan eksaminandens nettrafik ikke identificeres, overvåges eller logges. Hertil kommer, at mange skoler holder eksamen i lånte/lejede faciliteter, fx Bellacenter, hvor de ikke har mulighed for at etablere overvågning af nettet.

- En skole peget på, at det vil være vanskeligt at lukke for adgangen til internettet, når Netprøver.dk introduceres. Dette system forudsætter at eksaminanderne har adgang til internettet, i hvert fald ved eksamens begyndelse og når den enkelte eksaminand ønsker at aflevere.

- Skolens organisering af netværket på skolen kan stille sig i vejen for anvendelse af filtrering i praksis. Hvis man ikke kan etablere et særligt lukket eksamensnet, kan nettet ikke filtreres til eksamensformål, hvis nettet på samme tid skal benyttes af andre elever på skolen, der fx forbereder sig til en kommende eksamen. Tilsvarende er filtrering uden virkning, hvis andre netværk er tilgængelige for eksaminanderne.

- Skolerne peger i øvrigt på, at de ikke kan spærre for andre, fremmede netværk (fx et mobil-hotspot uden for eksamenslokalet eller peer-to-peer forbindelse mellem to computere).

- Endeligt peger en skole på, at grænserne mellem tilladt og ikke-tilladt brug af internettet smuldrer. Som eksempet nævnes, at Apple stavekontrol slår op i Wikipedia.

3.1.2.3 Forslag til bedre imødegåelse af snyd

Skolerne har også i nogle tilfælde givet forslag til reduktion af problemet med snyd eller bedre imødegåelse. Devoteam har ikke taget stilling til de enkelte forslag, som resumeres nedenfor:

- Først og fremmest efterlyses udvikling af eksamensformer, der tillader fuld adgang til internettet (bortset fra kommunikation med andre).
- I øvrigt foreslås, at den skriftlige eksamen suppleres med en mundtlig overhøring. (Dette forslag er måske mest inspireret af problemer med snyd ved SSO og SRP.)

Vi har også bedt *eleverne* om forslag til, hvordan indsatsen kunne forbedres:

Før eksamen
- Mere dybtgående forklaring om eksamen, herunder bedre vejledning om, hvilke netkilder der er tilladte og om konsekvenserne om snyd. Vejledningen bør gives i flere omgange, både før eksamensperioden og i forbindelse med introduktionen til den enkelte eksamen
- Klare(re) retningslinjer fra ministeriet
- Udlevering af en vejledning på en enkelt side med gode råd til at undgå at snyde umiddelbart før eksamensstart og en vejledning med en whitelist over de tilladte kilder.
- Gøre undervisningen bedre, så der ikke er behov for at snyde

Under eksamen
- Mere kvalificeret, it-kyndigt tilsyn
- Filtrer og overvåg internettrafik gennem portal
- Mere konsekvent kurs fra skolerne ved mistanker om snyd

Uden for eksamensprocessen
- Fjern skolernes incitament til at undgå opdagelse af snyd for at bevare indtægter
- Reducér betydningen af eksamenskarakterer (fx ved at reducere betydningen af eksamenskarakteren ved optagelse på videregående uddannelser, eller ved kun at vægte de relevante fag.)

Hertil kommer naturligvis en række forslag om direkte imødegåelse af de muligheder for snyd, som har været nævnt (fx forbyd brugen af Onenote online, Online Evernote, Online Spotify).

3.1.3 Opsummering af erfaringerne fra de gymnasiale uddannelser

På baggrund af ovenstående gennemgang kan Devoteam konkludere, at såvel de adspurgte elever som de adspurgte skoler er opmærksomme på problemet snyd under eksamen. Begge parter har dog den opfattelse, at problemet ikke er videre udbredt, hvilket også understøttes af STUK's undersøgelse af forekomsten, som er omtalt i afsnit 2.2.2 .

De angivne eksempler på muligheder for snyd viser samtidigt, at snyd formentlig ofte har karakter af uplanlagte strejftog ind på forbudt område, enten ved et akut opstået behov, eller af usikkerhed på, hvad der faktiske er tilladt. Men de viser tillige, at snyd også kan være velforberedt og gennemtænkt, alene eller sammen med en med-eksaminand eller en udenforstående, med mere eller mindre sofistikerede metoder

Ved de uplanlagte tilfælde af snyd synes eksaminanderne typisk at misbruge den tilladte netadgang til at besøge ikke-tilladte steder (fx Google Translate) eller ikke-tilladte kilder på de tilladte netsteder. Evt. bruges mobilen til i smug at besøge en netside eller udveksle sms-beskeder med en ven.

Det planlagte forsøg på snyd kan naturligvis også basere sig brug af de samme metoder. Men de mere velforberedte snydeforsøg kan omfatte forsøg på at omgå eventuelle spærringer i skolens netværk eller brug af en smartphone til et etablere en alternativ netforbindelse. Andre forsøg, som at etablere et hot-spot uden for lokalet eller at aftale at udveksle beskeder med en hjælper på et aftalt sted på wikipedia, vil forudsætte en klar intention og en forudgående involvering af en medsammensvoren.

De adspurgte skoler gør alle forsøg på at forebygge, forhindre eller afsløre snyd. Der anvendes forskellige tekniske midler, der kan sammenfattes i følgende:

- Filtrering af internettrafik
- Logning af internettrafik og gennemgang af loggen ved mistanke
- Scanning for ikke-tilladte hot-spots

Skolerne anvender også forskellige ikke-tekniske midler for at imødegå snyd med tekniske midler:

- Opstramning af eksamensreglement, fx med forbud mod at medbringe mobiltelefoner
- Vejledning (indskærpelse) af eksamensregler
- Eksamenstilsyn, nogle steder opkvalificeret eller suppleret med it-kompetencer
- Inspektion af eksaminandens computer ved mistanke om snyd
- Påbud om at, at eksaminanderne skal gemme links til alle tilladte netsteder som bogmærker inden eksamen, og kun må besøge de pågældende steder

De adspurgte har dog samtidigt peget på, at filtrering, logning og overvågning er kompliceret at implementere, og derfor ikke altid fuldkomment. Anvendelsen er øjensynligt præget af, hvilke kompetencer der er til rådighed på skolen eller i et evt. it-fællesskab

Det er Devoteams vurdering, at skolerne med de tekniske midler, filtrering og logning, når et langt stykke ad vejen med at forhindre (og evt. afsløre) den lejlighedsvise snyd ved besøg på ikke-tilladte netsteder. Og at skolernes indsatser også har en forbyggende (afskrækkende) effekt. Det er imidlertid samtidig Devoteams vurdering, at de tekniske midler ikke er tilstrækkelige til at imødegå planlagt snyd. Tilsynet er således det bedste forhåndenværende middel til at forhindre eksaminanders brug af alternative netforbindelser. (Se afsnit 5 om midler, der kan tages i anvendelse.)

Samtidig må det konstateres, at de tekniske midler ikke vil kunne forhindre eller afsløre brug af ikke-tilladt materiale på tilladte netsteder eller fra egen computer, hvad enten dette er utilsigtet, tilsigtet eller endog planlagt.

Det skal erindres, at der også nævnes en række ikke-tekniske metoder til snyd, fx udveksling af noter på papir eller USB-sticks. Disse metoder imødegås af tilsynet.

3.2 Erfaringer fra de videregående uddannelser[4]

3.2.1 Universiteterne

Som led i undersøgelsen har Devoteam undersøgt, hvilke foranstaltninger der foretages ved universiteterne for at imødegå snyd ved skriftlige stedprøver.

Hovedindtrykket er, at indsatsen mod snyd udgøres af en kombination af tre elementer:

- Retningslinjer, som tydeliggør, at snyd, fx ved anvendelse af mobiltelefon eller PC til adgang til ikke-tilladte hjælpemidler, er bortvisningsgrund
- Forstærket tilsyn med kompetencer til at identificere teknologisk snyd
- Plagiatkontrol – Der arbejdes med at forbedre bedømmernes udbytte af plagiatkontrol, fx med præcise retningslinjer for, hvordan bedømmerne skal agere, hvis systemet finder mulig plagiering – hvornår er det "alvor" og hvornår er det helt naturligt (fx kilde-citater) eller falsk positive. En enkelt institution anvender to supplerende systemer til plagiatkontrol

På flere institutioner vælger man at supplere ovenstående med ændringer af eksamensordninger, sådan at de i højere grad afprøver den studerendes færdigheder i et teknologisk åbent setup – og på den måde nedbringe behovet for stærkt tilsyn til de få eksamensformer, hvor prøven skal omfatte indlært viden og færdigheder.

Universiteterne har dog også taget initiativer til teknisk at forhindre, at eksaminanden kan tilgå ikke-tilladte hjælpemidler.

- Nogle bruger således FLOWlock, som er en aflåst browserløsning, hvori eksamen afvikles (Se bl.a. afsnit 5.2.4 .)
- Flere universiteter anvender Exam Monitor, som er et system (udviklet af Syddansk Universitet), der kan overvåge og logge aktiviteten på hver eksaminands computer. (Se afsnit 5.2.5)
- Der vælges også i nogle tilfælde en løsning med et "eksamenshus", hvor institutionen stiller udstyr til rådighed for eksaminanderne til eksamen. Derved opnås, at institutionen kan kontrollere udstyrets muligheder, fx med hensyn til, hvilke netsteder, der kan besøges.

Med forskellig grad af sikkerhed – og omkostninger - kan disse løsninger forhindre, at den studerende tilgår internettet og søger ikke-tilladt hjælp. I varierende grad kan de forhindre brug af hjælpemidler, der måtte befinde sig på computerens harddisk.

Smartphones vurderes dog at være en mere udbredt adgangskanal til ikke-tilladte hjælpemidler end eksaminandens egen computer. Der er undersøgt flere muligheder for at forhindre GSM-trafik under eksamener, ved enten at "jamme" eller placere eksaminanderne i et radiodødt rum. Disse tiltag er dog stødt på praktiske og lovgivningsmæssige barrierer. (Se afsnit 5.3).

[4] *Kilde: Interviews med centralt placerede kilder på de enkelte institutioner.*

Flere institutioner vælger derfor at styrke tilsynet – enkelte har gjort forsøg med supplerende retningslinjer om, at smartphones ikke må benyttes med varsling om, at der periodisk vil blive scanner for mobiltrafik i eksamensrummet. Andre forbyder helt smartphones og andre kropsbårne enheder og/eller kræver dem afleveret til tilsynet inden eksamen begynder. I forhold til Apple Smartwatch har et universitet udstyret deres supportere med sådanne ure, som opdager, hvis andre ure i nærheden prøver at kommunikere. Den bedste effekt af scanning synes ifølge de interviewede at være den afskrækkende virkning.

3.2.2 Professionshøjskolerne

Devoteam har drøftet imødegåelse af snyd ved professionshøjskolerne med it-afdelingen ved den største professionshøjskole, VIA University College. VIA er i øvrigt også driftscenter for en række gymnasier.

Man har i sektoren anskaffet WISEflow (Se afsnit 5.2.4), som er under indkøring til administration, opgaveudlevering, modtagelse af besvarelse og fordeling til bedømmelse. Man har ikke implementeret komponenten til snydekontrol, FLOWlock. Begrundelsen er efter det oplyste, at stedprøven uden hjælpemidler fylder meget lidt På VIA og de øvrige professionshøjskoler. Behovet for indsats mod eksamenssnyd ved sådanne eksamener er således yderst begrænset, og dermed også erfaringer hermed.

Som det fremgår af afsnit 5.2.4.5 er FLOWlock ikke egnet til andre typer eksamener.

3.3 Erfaringer fra ungdomsuddannelserne i Norge

Som det fremgår af Bilag 1 – Erfaringer fra Norge, har Devoteam kontaktet Utdanningsdirektoratet og en fylkeskommune i Norge for at undersøge, hvordan man i Norge forholder sig til bekæmpelse af snyd ved eksamen i ungdomsuddannelserne.

3.3.1 Organisering

Det norske uddannelsessystem er det uddannelsessystem, der ligner det danske mest. Det uddannelsesniveau, der svarer til de gymnasiale uddannelser i Danmark, hedder videregående oplæring. Der er også i Norge en skelnen mellem studieforberedende uddannelser og erhvervsforberedende uddannelser, men dette er uden betydning for imødegåelse af snyd ved skriftlig eksamen. Der skelnes derfor ikke i det følgende, hvor der fremhæves nogle træk af den norske model med relevans for nærværende undersøgelse.

Utdanningsdirektoratet under Kundskabsdepartementet står for centralt stillede opgaver og for centralt fastsatte rammer for eksamen. Det overordnede ansvar for gennemførelse af eksamenerne ligger hos de norske regioner (Fylkeskommuner), mens den enkelte skole har det praktiske ansvar. Det betyder bl.a., at det er regionernes it-afdelinger, der har ansvaret for en it-mæssige afvikling af eksamen, og dermed også for håndteringen af eksaminandernes adgang til internettet.

3.3.2 Eksamen og internet

Hovedreglen for eksamen i videregående oplæring er, at alle hjælpemidler er tilladt, bortset fra internet og hjælpemidler, som tillader kommunikation, samt oversættelsesprogrammer i Norsk og fremmedsprog.

Men, som i Danmark kan skolerne vælge at lade eleverne benytte netbaserede forberedelseselementer, læringsressourcer, opslagsværk eller ordbøger, som de har brugt i undervisningen, under eksamen, for-

udsat at skolerne er i stand til at isolere de aktuelle IP-adresser. Det er regionerne, der bestemmer hvilke hjælpemidler skolerne kan stille til rådighed, så skolerne kan stå inde for sikkerheden under eksamen.

I den kontaktede region bestemmes de tilladte hjælpemidler af regionen efter indstilling fra skolerne. Der har været hovedfokus på at åbne for ordbøger, opslagsværker, forlagenes netsteder og andre helt centrale fagnetsteder. Regionen har udviklet et system til styring af elevernes adgang til netressourcer, som også kan spærre for videre trafik ud på internettet, dvs. eksterne links, sociale medier, chat osv. (Efter beskrivelsen er systemet baseret på filtrering.) I de tilfælde, hvor regionen ikke har fundet det muligt eller sikkert at styre adgangen til et hjælpemiddel på denne måde, tillades det ikke at bruge netstedet under eksamen.

3.3.3 Sikker eksamen

Regionen forklarer, at sikring imod, at eleverne bruger computeren til ikke-tilladt kommunikation eller fildeling med andre, baseres på følgende tiltag:

a) Alle elever får uddelt en elev-pc ved skolestart. Det er kun denne pc, som kan bruges under eksamen.
b) Eleverne er tilknyttet regionens elevnet. IT-afdelingen i regionen har udviklet et adgangsstyringssystem, som kan styre adgangen til internettet for alle brugere, som er tilknyttet elevnettet. (Se ovenfor)
c) Scanning for ikke-tilladt elektronisk kommunikation i eksamenslokalet foretages stikprøvevis ved skolerne under eksamen.
d) Internettrafikken logges, men det føres ikke kontinuerligt tilsyn med loggen. Kun ved mistanke om snyd/brug af ikke-tilladte netsteder.
e) Der kan foretages inspektion af elevens computer for ikke-tilladte hjælpemidler (fx oversættelsesprogrammer) i form af stikprøver ved skolerne under eksamen.
f) Der er forbud mod at medbringe mobiltelefon og smartwatches. Musikafspillere er kun tilladt, dersom eksamensopgaven kræver det (f.eks. i musikfag). Elevene kan imidlertid bruge ørepropper/headset koblet til pc-en, hvis de har digitale hjælpemidler, som de vil bruge.
g) Eksamensvagterne (tilsynet) må også følge med på elevenes skærme under eksamen.
h) Til syvende og sidst er eleverne selv ansvarlige for at undgå at bruge hjælpemidler, som ikke er tilladte, dersom de skulle få mulighed for det.

Digital eksamen har medført ændring i opgaver og kompetencekrav for eksamenstilsynet. Eksamensvagterne skal have relativt god it-kompetence. De bør kunne skelne mellem tilladte og ikke-tilladte netsteder, og de bør kunne genkende teknisk udstyr som ikke er tilladt (f.eks. mobilt bredbånd osv.) Tilsynet skal også kunne hjælpe til med udskrifter, samt download og upload.

3.3.4 Snyd og plagiat

I Norge foretages ikke generel plagiatkontrol af eksamensbesvarelser, men censorerne kan scanne for plagiat i tilfælde af mistanke.

I Norge skelner man i øvrigt mellem snyd og plagiat. Snyd defineres som at kommunikere med andre, eller at bruge oversættelsesprogrammer i sprogfag. Konsekvenserne af snyd eller forsøg på snyd er, at eleven kan få eksamen i faget annulleret, og tidligst kan gå til ny eksamen året efter.

Plagiat betragtes ikke som snyd, da tekstgengivelse uden klar angivelse af kilde også kan være udslag af umoden brug af kilder. Plagiat kan dog føre til en lavere karakter (netop fordi det som minimum er udtryk for umoden brug af kilde).

3.3.5 Forsøg med eksamen med fuld adgang til internettet

Norge har i 2015 afsluttet et forsøg med eksamener, hvor eleverne havde fuld adgang til internettet, men ikke lov til at bruge nettet til kommunikation med andre. I 2015 omfattede forsøget otte fag og 56 skoler.

Formålet med forsøget har været at se, om internettet kan fungere som et hjælpemiddel på linje med andre hjælpemidler. Elever, der deltog i forsøget, har fået samme eksamensopgaver som elever, der ikke deltog i forsøget. Utdanningsdrektoratet vurderer, at forsøget har været vellykket, og at eksamen med adgang til internettet synes at være en eksamensordning, der fungerer godt under visse betingelser.

Utdanningsdirektoratet har gjort følgende observationer, som vurderes at have relevans for nærværende undersøgelse af snyd under eksamen.

- Det ser ikke ud til, at forsøget indebærer tekniske eller praktiske problemer
- Eksamensformen synes at påvirke undervisningen ved at øge fokus på faglig og pædagogisk brug af internettet, samt give større bevidsthed om og uddannelse i kildebrug og kildekritik.
- Der er få tegn på, at snyd og plagiat stiger som følge af eksamensformen.
- Evalueringen af forsøget viser imidlertid klart, at både blandt elever, undervisere og eksaminatorer til en vis grad er usikkerhed om grænserne for, hvad der er plagiat og snyd ved eksamener.
- Eleverne mener, at internettet er nyttigt ved eksamen, fordi det giver dem mulighed for at dobbelt-tjekke oplysninger, bruge opdaterede statistikker og aktualisere besvarelsen. Denne vurdering varie-rer dog fra fag til fag.
- Censorerne er de mindst positive over for eksamen med fuld adgang til internettet, men har kun i ringe grad observeret forskelle på besvarelser med og uden internetadgang.

4 Yderligere bidrag til analysen

4.1 Globale iagttagere

Som led i analysen har Devoteam indhentet informationer fra globale iagttagere, som formodedes at kunne bidrage til analysen af muligheder for at imødegå snyd ved eksamen.

4.1.1 OECD og Euridice

Devoteam har undersøgt litteratur, undersøgelser og rapporter om digital eksamen hos de internationale organisationer OECD og Euridice. Disse organisationer har imidlertid ikke udgivet noget, der beskæftiger sig med problemet snyd under digital eksamen.

4.1.2 Gartners teknologiovervågning

Sædvanligvis vil det globale konsulentfirma Gartner være en god kilde til et opdateret overblik over teknologien på et givent forretningsområde. Devoteam har derfor undersøgt, hvilke observationer Gartner har om digital eksamen og imødegåelse af snyd. Gartner har imidlertid ikke nogen observationer om snyd i forbindelse med digital eksamen.

I et studie om "digital assessment" konstaterer Gartner, at de amerikanske skoler (K-12) – på trods af en række forhindringer – er inde i en hurtig udvikling hen i mod digitale eksamener. Indsatsen ser imidlertid ud til at koncentrere sig om digital parathed i bredere forstand, dvs. digitale læremidler, digital infrastruktur og digitale færdigheder hos eleverne. Gartner peger også fremvæksten af fælles on-line prøver, men beskæftiger sig altså ikke med sikkerhed mod snyd under eksamen.

4.2 Metoder til sikring af eksamen mod snyd

Devoteam har gennemført en omfattende (internet-baseret) direkte søgning efter tekniske midler til at imødegå snyd ved digitale eksamener. Der er fundet en række eksempler på "Online proctoring services" og "Secure Browsers", som beskrives nedenfor. Dertil kommer en række tilbud om plagiatkontrol. Det har ikke været muligt at finde andre tekniske midler til at forebygge, forhindre eller imødegå snyd.

4.2.1 Online Proctoring Services

Online Proctoring Services er udbredte i forbindelse med it-træning og certificering, og i øvrigt i fjernundervisningsmiljøer. Bl.a. benytter Microsoft Training sig af sådanne services. Der findes flere forskellige udbydere, og online proctored exams anvendes også af nogle anerkendte uddannelsesinstitutioner.

Ideen er, at prøven aflægges som fjernprøve via en computer med videoforbindelse, således at en eksamensvagt (proctor) kan se, hvad eksaminanden foretager sig, og om eksaminanden benytte ikke-tilladte hjælpere eller hjælpemidler. Det er sædvanligvis et krav, at eksaminanden sidder alene i et aflukket lokale. Proctor kan formentlig overvåge et begrænset antal eksaminander samtidigt.

Under prøven anvender eksaminanden en "secure browser" af den slags, som beskrives i det følgende.

4.2.2 Secure Browsers

Ovenfor omtalte Online Proctoring Services anvender såkaldte ”secure browsers”. Disse kan være selvstændige programmer eller plug-ins til almindelige browsere. Ideen er, at browseren under prøven afskærer brugerens adgang til de fleste sædvanlige funktioner og programmer på egen computer. Der tillades kun trafik mod en bestemt server på internettet, og kun brug af de specielt tilpassede programmer, fx til tekstbehandling med begrænset funktionalitet, som servicen stiller til rådighed.

De fleste af disse secure browsers tillader således kun internetforbindelse til en enkelt server, mens nogen oplyser, at man på serveren kan opsætte filtre, der tillader gennemstilling til et større udvalg af URL’s/IP-adresser.

Secure browsers udbydes som kommercielle services, og benyttes af mange universiteter i USA. Der findes også secure browsers fra Australien og Europa. Der er fx et open source projekt ved navn ”Safeexambrowser”, der er baseret i Schweiz. Denne browser understøtter pt. kun et begrænset udvalg af klienter/styresystemer.

I Danmark indgår en secure browser i løsningen FLOWlock fra firmaet UNIwise, som er omtalt i afsnit 5.2.4 nedenfor.

4.2.3 Vurdering

Devoteam har som nævnt ikke kunnet lokalisere andre tekniske midler til at imødegå snyd, end de ovenfor omtalte.

Det er Devoteams vurdering, at online proctoring ikke er relevant ved eksamener i de gymnasiale uddannelser, så længe disse skal afvikles som stedprøver.

Som beskrevet i afsnit 5.2.4 om WISEflow og FLOWlock er det tvivlsomt, om Secure Browsers kan håndtere delvis adgang til internettet. Den danske leverandør, UNIwise, har indtil videre ikke villet implementere delvis adang til internettet i FLOWlock. Derfor anser Devoteam på nuværende tidspunkt kun secure browsers for en løsning, der kan bruges til at imødegå snyd ved eksamen uden adgang til internettet.

5 Mulige tekniske midler til imødegåelse

5.1 Vurderingskriterier

I dette afsnit gennemgås de mulige tekniske midler til imødegåelse af snyd, som Devoteam har identificeret gennem undersøgelserne beskrevet i afsnittene 3 og 4 med bilag.

Som beskrevet i afsnit 2.2.5 er den grundlæggende udfordring ved at imødegå snyd, at forbygge, forhindre eller afsløre snyd i form af:

- Kommunikation med andre
- Misbrug af andre end tilladte kilder på internettet
- Misbrug af materiale eller programmer på eksaminandens computer

De tekniske midler til imødegåelse, der skal overvejes, bør derfor vurdereres på deres effekt i forhold til disse mål. Vi har derfor vurderet dem ud fra følgende vurderingskriterier:

Figur 4 Oversigt over vurderingskriterier for tekniske midler

Kriterium	Beskrivelse
BYOD	Kan løsningen understøtte, at eksaminanderne bruger deres egen computer (evt. begrænset til udvalgte typer af devices)
BYOA	Kan løsningen understøtte, at eksaminanderne bruger deres egne programmer
Data på egen computer	Kan løsningen understøtte brug af kun tilladte data/programmer på egen computer
Kommunikation med andre	Kan løsningen forhindre kommunikation med andre
Tilladte/Ikke-tilladte kilder	Kan løsningen forhindre adgang til ikke-tilladte kilder på tilladte netsteder
Tilladte/Ikke-tilladte netsteder	Kan løsningen forhindre adgang til ikke-tilladte netsteder
Omkostninger	Hvilke særlige omkostninger vil der være ved løsningen
Sårbarheder	Hvilke sårbarheder har løsningen

Gennemgangen af snydemuligheder i afsnit 3 har vist, at snyd under eksamen dels kan foregå ad den internetforbindelse, som skolen stiller til rådighed, dels ad andre forbindelser. I det følgende ses derfor på de tekniske midler for imødegåelse af snyd under eksamen fordelt på disse to kanaler:

- Den tilladte kanal (internetforbindelse), som skolen stiller til rådighed
- Alternative kanaler

Dernæst gennemgås et middel mod snyd, som kan tages i brug efter eksamen, Plagiatkontrol.

5.2 Midler mod snyd via den tilladte kanal

5.2.1 Filtrering af nettrafik

Flere af de adspurgte skoler forsøger at imødegå snyd ved filtrering af internettrafikken, så besøg på ikke-tilladte netsteder, chat etc. forhindres.

Filtrering kan etableres på forskellige måder, bl.a. afhængigt af netværksopsætningen på skolen.

Det må antages, at alle skoler benytter trådløse netværk. Hvis filtrering kun skal berøre de aktuelle eksaminander, mens andre brugere ikke skal berøres af eksamensfiltreringen, skal der etableres et eller flere lukkede "eksamensnet" til lejligheden. Det er samtidigt nødvendigt, at adgangen til alle netværk på skolen er styret (netværkskode eller personligt log-in), således at eksaminanderne ikke kan koble sig på de forkerte netværk. (Vi har hørt om et tilfælde, hvor eksaminanderne uafvidende brugte skolens lærernet, fordi deres computere huskede nøglen til dette netværk fra en tidligere projektopgaveperiode.) Med personligt login vil det samtidigt være muligt at styre den enkelte elevs netværksadgang dynamisk, fx med eksamensopsætning om formiddagen og almindelig elevadgang om eftermiddagen.

Ved filtrering i skolens firewall kan der (afhængigt af model) foretages flere slags filtreringer, bl.a. af blokering af internetadresser eller af adgang til Domain Name Server (omsætning af www.-adresser til IP-adresser), blokering af e-mails, søgemaskinefiltre (dvs. fjerne links i fx en google-søgning). Med baggrund i opgavens omfang og variabilitet kan det i stedet være relevant at anvende nogle produktspecifikke content filters, som også kan blokere på andre objekt-niveauer.

Opsætning af filtre m.v. kræver dels en indsigt i, hvilke kilder der er relevante ved den pågældende eksamen (herunder egne læremidler, egne noter og egne arbejder), dels et højt kompetenceniveau i forhold til firewalladministration, hvilket skolerne kun sjældent vil kunne råde over, og som er kostbart at tilkøbe på servicebasis. Filtrering kan desuden være umulig at gennemføre på eksterne lokationer, fx ved eksamen i lejede haller, og vil som minimum forudsætte, at man kan medbringe og opstille et dedikeret udstyr.

Filtre vil ikke kunne skelne mellem tilladte og ikke-tilladte kilder på det samme netsted, fx Infomedia.

Løsningen er sårbar over for velplanlagte omgåelsesforsøg, der kan udnytte "huller" i filtreringen, fx ved at anvende direkte links gennem forud aftale netværksporte etc.

Løsningen er i øvrigt sårbar over for, om eksaminanden har mulighed for at omgå filtreringen ved at tilgå et andet af skolens andre netværk, fx ved at låne et log-in af en kammerat.

Vurdering:
Devoteam vurderer, at filtrering kan yde et væsentligt bidrag til at forhindre bevidst eller ubevidst tilgang til ikke-tilladte internetsteder. Men filtrering ikke er fuldstændigt effektiv, og kan ikke anvendes i alle situationer og på alle steder. Det kan grænse til det umulige at opsætte filtrene, så lige netop de tilladte netsteder kan tilgås. Og løsningen kan fx ikke afgrænse visse e-bøger fra andre, der udbydes af samme forlag, eller den ene underside fra den anden.

Løsning	Eksempel	Effekt							Forudsætninger	Omkostninger	Sårbarheder
		BYOD	BYOA	Data på egen computer	Ikke tilladt kanal	Kommu-nikation med andre	Tilladte/ Ikke tilladte kilder	Tilladte/ Ikke tilladte netsteder			
Filtrering	Forbedret praksis	Ja	Ja	Ingen effekt	Ingen effekt	Kan vanskelig-gøre	Ingen effekt	Kan skelne med usikkerhed	Eksamen i egne lokaler	Server Content filtre Opsætning af filtre/server	Kompetencekrav Andre net Kompleks opsæt-ning

5.2.2 Logning og kontrol af log

Afsløring af brug af ikke-tilladte internetkilder kan ske ved logning af trafikken til og fra den enkelte eksaminands computer og efterfølgende inspektion af loggen.

Logning med efterfølgende gennemgang af loggen for den individuelle trafik forudsætter i praksis, at skolen benytter individuelt login til netværket. Hvis der ikke benyttes individuelt log-in vil afkodningen af den enkelte eksaminands trafik være afhængig af oplysninger om eksaminandernes IP- eller MAC-adresser, som dels kan være vanskelige at indsamle, dels vil kunne ændres af eksaminanden.

Logningsdata skal opsamles på en passende server og efterfølgende gennemgås for uregelmæssigheder med et passende program. Dette kræver en vis teknisk indsats. For at hjælpe kunderne, tilbyder fx It-center Fyn og UC VIA, der hver servicerer et antal gymnasier, at foretage en sådan log-analyse i tilfælde af mistanke om snyd. I rapporten vil logningsdata være omsat på en sådan måde, at det er muligt at følge trafikken for den pågældende eksaminand. Vurdering af, om der har foregået ikke-tilladt trafik må foretages af personer med indblik i hvilke netsteder mv., der er tilladt ved den pågældende eksamen, herunder i relation egne læremidler, egne noter og egne arbejder. Gennemgang af loggen kan også gennemføres efter tilfældig udtrækning.

En løbende overvågning af loggen kunne være ønskelig, men Devoteam har ikke kendskab til redskaber, der på en effektiv og brugervenlig vis muliggør en sådan *realtidsmonitorering* af logningsdata (Se dog Exam Monitor, afsnit 5.2.5) Sådanne redskaber er tillige meget kostbare.

Bemærk, at løsningens effekt forudsætter, at eksaminanderne ikke har adgang til andre netværk end det overvågede. Som for filtreringen gælder det også, at det ikke er muligt at skelne mellem tilladt og ikke-tilladt trafik til samme netsted, specielt ikke, hvis netstedet bruger krypteret kommunikation (https).

Logning vil være vanskeligt at implementere ved eksamen i eksterne lokaliteter, og som minimum forudsætte, at man medbringer og opstiller et dedikeret udstyr.

Vurdering:
Devoteam vurderer, at logning kan være effektiv som dokumentation for en mistanke, der er opstået ad anden vej. Logning kan dog ikke anvendes i alle situationer og på alle steder. Administration af logningen kræver it-tekniske kompetencer, som nok primært findes ved it-centre. Logning kan ikke afgrænse visse e-bøger fra andre, der udbydes af samme forlag, eller den ene underside fra den anden.

Løsning	Eksempel	Effekt							Forudsætninger	Omkostninger	Sårbarheder
		BYOD	BYOA	Data på egen computer	Ikke tilladt kanal	Kommu-nikation med andre	Tilladte/ Ikke tilladte kilder	Tilladte/ Ikke tilladte netsteder			
Logning	Som visse it-centre	Ja	Ja	Ingen effekt	Ingen effekt	Kan afsløre	Ingen effekt	Kan afsløre	ID på netværk Eksamen i egne lokaler	Analysesystem Manuel gennemgang af log	Gennemgang af log kun ved mis-tanke Kompetencekrav Andre net

5.2.3 USB-boot

Der har tidligere været gjort forsøg med en løsning baseret på "boot fra en USB-stick". Ideen bag denne løsning var, at eksaminanderne nok medbragte deres egen computer, men skulle starte computeren op på et særligt USB-stick, som institutionen udleverede. Denne stick skulle indeholde et styresystem, som overtog kontrollen med computeren, herunder med internetforbindelsen, anden kommunikation og adgangen til egen disk.

En server skulle filtrere internettrafikken og/eller rumme relevante hjælpemidler, herunder eksaminandens egne noter, som vedkommende måtte uploade inden eksamen.

Pilotforsøg med udvikling af sådanne USB-sticks ved Aarhus Universitet viste imidlertid, at opsætningen var meget administrativt krævende, at løsningen stillede store krav til support, og at det i praksis var umuligt at opsætte styresystemet til alle i praksis forekommende computere, devices og drivere.

Forsøget blev derfor stoppet.

Vurdering:
Devoteam anser løsningen for urealistisk.

5.2.4 Secure Browser (FLOWlock)[5]

Det danske firma UNIwise udbyder et system til understøttelse af processen med administration og afvikling af digitale eksaminer fra planlægning, over opgaveudlevering og modtagelse af besvarelse til distribution til bedømmere og indsamling af bedømmelser. Dette system hedder WISEflow.

Sammen med WISEflow tilbyder UNIwise værktøjet FLOWlock til imødegåelse af snyd under eksamen. FLOWlock er en browser, der afskærer eksaminanden fra adgang til programmer og filer på egen computer, til kommunikationskanaler og til internettet (udover til WiseFlow-serveren). FLOWlock er baseret på Respondus, en secure browser, jf. også afsnit 4.2.2 om secure browsers)
Ved vurderingen af secure browsers tages udgangspunkt i FLOWlock/Respondus, som er tilpasset danske forhold af UNIwise.

5.2.4.1 Funktion

Eksaminanderne skal have downloadet den særlige browser inden eksamen. Eksaminanderne logger på WISEflow/FLOWlock med WAYF eller NemID. I princippet skal eksaminanderne være påloggede under hele besvarelsen. Hvis eksaminanden ønsker at gå før tid, skal tilsynet afgive en kode på eksaminandens computer.

[5] *Kilder til information om WISEflow og FLOWlock: Interviews, netvejledninger. Kilde til information om Respondus: Respondus netsider m.fl.*

FlowLock stiller en særlig tekstbehandler til rådighed for eksaminanden. Der kan også stilles multiple choice-opgaver og andre typer opgaver i et indbygget format. Men der er ikke adgang til eksaminandens sædvanlige applikationer, fx tekstbehandler og regneark, eller til egne noter på computeren eller udvalgte ressourcer på internettet.

WISEflow og FLOWlock betjener sig af servere i skyen. I tilfælde af netudfald kan eksaminanden arbejde videre, og resultatet bliver gemt krypteret på eksaminandens computer. FLOWlock understøtter Windows og Mac, og kræver Flash.

FLOWlock er baseret på en amerikansk secure browser kaldet Respondus. På internettet findes forskellige forslag til omgåelse af Respondus. De angivne metoder er dog komplicerede at implementere og tilsyneladende forældede, da Respondus efter det oplyste løbende udvikles til at imødegå disse omgåelsesmetoder. Det er således fx ikke længere muligt at omgå FLOWlock ved at installere en virtuel maskine på computeren.

Devoteam har ikke afprøvet sikkerheden mod omgåelse.

5.2.4.2 Udbredelse

UNIwise oplyser, at WISEflow anvendes ved mere end 50 institutioner og af mere end 600.000 studerende, undervisere og administratorer. I alt er mere end 2 mio. eksamener afviklet i WISEflow siden foråret 2013. (Disse tal omfatter ikke nødvendigvis anvendelse af FLOWlock.)

Hovedvægten ligger på videregående uddannelser i Skandinavien, men løsningen er også eksporteret til Korea m.fl. steder.

I Danmark anvendes FLOWlock i henhold til vores undersøgelse ved enkelte universitetsfakulteter. På professionshøjskolerne, hvor der er udbredt anvendelse af WISEflow, er der meget få skriftlige stedprøver og relativt sporadisk anvendelse af FLOW-lock.

5.2.4.3 Erfaringer

WISEflow og FLOWlock har været anvendt ved Aarhus Universitet, Fakultetet for Business and Social Sciences (AU-BSS) siden foråret 2014.

WISEFlow bruges til administration mv. af både skriftlige og mundtlige eksamener, herunder til udlevering af opgaver og modtagelse af skriftlige besvarelser. Ca. 90 % af alle skriftlige eksamener ved AU-BSS er digitaliserede, og ved alle disse anvendes elevens eget udstyr og WiseFlow.

AU-BSS opererer i princippet med to slags stedprøver: hhv. med og uden hjælpemidler. Stedprøver med begrænsede hjælpemidler forekommer ikke. (Dog tillades brug af computer uden tekniske begrænsninger til nogle eksamener uden hjælpemidler.)

WISEflow uden FLOWlock lægger ikke begrænsninger på eksamensformen. FLOWlock låser som nævnt computeren totalt, således at der ikke er adgang til internet, kommunikation, eller egen disk. Det betyder, at det fx ikke er muligt at give adgang til Karnovs lovsamling uden at åbne for alle hjælpemidler, dvs. at undlade at bruge FlowLock. Det betyder således, at eksamener enten er med FlowLock og helt

uden digitale hjælpemidler eller uden Flowlock og med alle digitale hjælpemidler. Dette vurderes dog ikke at have givet anledning til ændringer i valg af eksamensform, bortset fra enkelte tilfælde.

FlowLock stiller let forøgede krav til tilsynet, men letter også opgaven, fordi alle eksaminander nu vil sidde med samme skærmbillede, den indbyggede tekstbehandlingsapplikation.

FLOWlock har været anvendt til ca. 70 eksamener med ca. 6.000 deltagere i det seneste år. AU-BSS har ikke registreret noget tilfælde af omgåelse af FlowLock. Man vurderer i øvrigt, at eksaminander, der måtte forsøge omgåelse, som regel vil eksponere sig selv over for tilsynet. WISEflow og FLOWlock opleves at have en tilfredsstillende driftsstabilitet med kun få, kortvarige ikke-varslede nedetider.

5.2.4.4 Perspektiver

Efter dialog med UNIwise er det vores vurdering, at den videre udvikling af WISEflow i relation til imødegåelse af snyd vil følge tre alternative, men evt. samtidige, veje:

1. FLOWlock – Fortsat helt lukket af. UNIwise har efter det oplyste ikke planer om at åbne løsningen for et udvalg af internetkilde, idet man vurderer, at det ikke er muligt med sikkerhed at styre en tilladt adgang til netressourcer).
2. En overvågningsløsning, der lyder til at være i stil med Exam Monitor.
3. Ren WISEflow med plagiatkontrol, men uden FLOWlock eller lignende.

5.2.4.5 Vurdering

Det er Devoteams vurdering, at Secure Browsers, i form af FLOWlock, vil kunne gøre god fyldest i en eksamen uden digitale hjælpemidler. Vi anser det derimod ikke for realistisk, at Secure Browsers kan bruges til at skelne mellem tilladte og ikke-tilladte netsteder, eller til at give begrænset adgang til materiale på egen computer.

Det må anses for en fordel, at den anvendte secure browser løbende vedligeholdes af en international virksomhed. På den anden side gør den internationale eksponering også browseren sårbar som mål for alverdens hackere.

Løsning	Eksempel	Effekt							Forudsætninger	Omkostninger	Sårbarheder
		BYOD	BYOA	Data på egen computer	Ikke tilladt kanal	Kommunikation med andre	Tilladte/ Ikke tilladte kilder	Tilladte/ Ikke tilladte netsteder			
Secure Browser	FLOWlock	Windows og MAC	Nej	Forhindrer	Forhindrer	Forhindrer	Ingen tillades	Ingen tillades	Ingen særlige	Licens, opsætning	Løbende opdatering Internationalt hackermål

5.2.5 Exam Monitor[6]

Syddansk Universitet har udviklet et system til overvågning af aktiviteten på hver studerendes computer under eksamen. Systemet kaldes "Exam Monitor", og tilbydes nu til andre universiteter og til gymnasier m.v. SDU forbeholder sig dog, at skolen har en vis modenhed og erfaring med digital eksamen i forvejen.

6 *Kilde: Produktblad for Exam Monitor og interviews.*

5.2.5.1 Funktion

På SDU anvender de studerende deres egen computer i undervisningen. Exam Monitor muliggør, at de studerende også kan bruge deres egen computer til eksamen, samtidig med, at universitet kan sikre troværdigheden af eksamen ved at overvåge hver enkelt studerendes computer under eksamen.

Exam Monitor sætter ingen begrænsninger på, hvad eksaminanden kan benytte af programmer eller besøge af netsteder. Under prøveafviklingen overvåges netforbindelser og tages løbende snapshots af skærmbilleder, udklipsholderen og listen over kørende programmer. Tilsynet kan via systemet kigge rundt på de studerendes maskiner og log i systemet (ligesom vagtpersonale kigger rundt på overvågningskameraer i et supermarked.). Når prøven er slut, skrives en rapport ud med røde flag, hvis der er konstateret noget mistænkeligt, som skal kigges efter i loggen. De røde flag er bl.a. baseret på et katalog over, hvilke services der ikke må bruges (SDU fokuserer på Facebook og andre sociale medier, men der kan også sættes alarm op for andre netsteder). Når en rapport skal gennemgås, kan man lave maskinel billedgenkendelse, så man kan finde det sted i rækken af skærmdumps, hvor eksaminanden begynder at anvende en ny applikation, en ny hjemmeside eller lignende.

De studerende har adgang til efterfølgende at se den overvågning som institutionen har foretaget. Dermed er det helt transparent, hvad der sker. Både den studerende og institutionen kan afkræfte en mistanke om snyd ved tvivlstilfælde, og den studerende får også indsigt i sit eget eksamensforløb.

SDU oplyser, at Exam Monitor er godkendt til eksamensbrug af Datatilsynet, Kammeradvokaten og Styrelsen for Videregående Uddannelser.

Systemet består af følgende elementer:

1. En klient, der startes op på den studerendes computer, skaber forbindelse til en server og foretager en løbende logning af aktiviteten på computeren ved at lagre skærmdumps og proceslister på serveren. Klienten er en Javawebstart (den samme teknologi som bruges af NemId), og er dermed ikke et program, som skal installeres og afinstalleres igen efter eksamen.
2. En eller flere servere, som opsamler data, laver efterbehandling af data, og fremstiller en rapport for hver studerende. Administrator får adgang til server via unikt login.
3. Databehandlingssoftware, som bl.a. foretager forskellige former for billedbehandling af skærmdumps fra de studerendes computer.

Der er indbygget forskellige sikkerhedsforanstaltninger i løsningen. Således tjekkes fx, om der kører en virtuel maskine på eksaminandens computer, og om der er indhold i udklipsholderen.

Løsningen er en helt selvstændig komponent, der er uafhængig af, hvordan opgaven udleveres, og besvarelsen afleveres.

Exam Monitor afvikles på servere i skyen, hvorfor der skal være en aktiv internetforbindelse og et netværk i eksamenslokalet. Exam Monitor kræver i øvrigt ikke, at skolen har noget særligt installeret. Exam Monitor fungerer med WAYF[7] og Uni-Login, og understøtter Windows, Mac og Linux (men ikke iPads).

[7] *Universitetssektorens fælles login-facilitet ("Where Are You From")*

5.2.5.2 Udbredelse

Exam Monitor benyttes på nuværende tidspunkt, ud over på SDU, på to fakulteter ved Aalborg Universitet og på et fakultet ved Aarhus Universitet. Systemet er under overvejelse på flere universiteter og gymnasier. Det afprøves pt. ved et it-center, der servicerer flere gymnasier.

5.2.5.3 Erfaringer

SDU mener selv, at systemet fungerer tilfredsstillende og anvender det bredt på universitetet. Ca. 1 % af deres studerende kommer ud med rødt flag og skal ses efter. I disse tilfælde er der som hovedregel faktisk tale om ikke-tilladte aktiviteter.

Devoteam har ikke afprøvet systemet. Devoteam har kontaktet det gymnasium, som har afprøvet systemet for at høre om de foreløbige erfaringer.

Skolen fortæller, at systemet har kørt uden problemer. Man har haft adgang til administrator-login, og har via systemet kunnet overvåge de enkelte eksaminanders skærme og øvrige aktiviteter på computeren. Man har ikke haft adgang til at opsætte alarmer for særlige aktiviteter (jf.of.) , men det har ikke været et problem.

Skolen har oplevet, at intervallerne mellem screenshots var for store til, at skolen med sikkerhed kunne dokumentere, at en eksaminand faktisk anvendte et samarbejdsværktøj som Dropbox eller Skype. I det gældende eksamensreglement var det ikke forbudt at have sådanne redskaber kørende på maskinen, de måtte blot ikke benyttes. Ofte vidste eksaminanderne slet ikke, at de pågældende programmer kørte i bagrunden. Reglementet vil nu blive strammet, så disse tjenester ikke må køre på computeren.

Umiddelbart vurderer man fra skolen, at den præventive virkning på eksaminanderne er betydelig (”udgør 90 % af effekten”).

5.2.5.4 Vurdering

Det er Devoteams opfattelse, at Exam Monitor lever op til det lovede: at overvåge, logge og analysere den samlede aktivitet på eksaminandens computer. Systemet vil dog kræve en del opsætning i relation til den enkelte eksamenssituation (fx vedr. egne læremidler, egne noter og egne arbejder) for at kunne give de rette alarmer. Såfremt der ikke kan opsættes præcist virkende alarmer, skal gennemgang af loggen initieres ved mistanke, der er opstået ad anden vej (eller ved tilfældigt udtræk). Den løbende betjening og fortolkning af rapporter vurderes at stille krav til den eksamensansvarliges it-mæssige kompetencer, såvel som indsigt i tilladte og ikke-tilladte hjælpemidler ved den pågældende eksamen.

Exam Monitor er pt. ude i en tidlig version, og det må forventes, at SDU i den nærmeste fremtid vil opdatere og evt. yderligere forbedre systemet. Men med udbredelse af løsingen vil der blive et behov for vedvarende, løbende opdatering, bl.a. fordi løsningen må formodes at ville blive forsøgt hacket. På lidt længere sigt kan det imidlertid være et spørgsmål, om SDU fortsat selv vil have behov for at vedligeholde Exam Monitor, hvis SDU forlader konceptet med overvågede eksamener med begrænsede hjælpemidler, jf. omtalen af universiteternes holdning til imødegåelse af snyd i afsnit 3.2.1 .

Exam Monitors server(e) er placeret i skyen, og løsningen styres fra SDU. Det betyder bl.a., at løsningen er sårbar over for evt. nedbrud af internetforbindelsen til en skole.

Løsning	Eksempel	Effekt							Forudsætninger	Omkostninger	Sårbarheder
		BYOD	BYOA	Data på egen computer	Ikke tilladt kanal	Kommu-nikation med andre	Tilladte/ Ikke tilladte kilder	Tilladte/ Ikke tilladte netsteder			
Exam Monitor	Exam Monitor	Windows, MAC, Linux	Ja	Kan afsløre	Kan afsløre	Kan afsløre	Kan afsløre	Kan afsløre	Ingen særlige	Licens Opsætning Gennemgang af log	Netforbindelse Kompetencekrav Løbende opdate-ring

5.3 Midler mod snyd via alternative kanaler

Som beskrevet i afsnit 3.1.1.2 kan der snydes ved at bruge andre kanaler end den internetforbindelse, som skolen stiller til rådighed. Det kan enten ske ved, at eksaminanden kan få adgang til et andet af skolens net, som ikke er underlagt samme regulering som det autoriserede eksamensnet, eller ved at eleven selv sørger for at etablere en forbindelse, fx gennem et eksternt Wi-Fi-hotspot eller en 4G-mobiltelefonforbindelse.

Etableres en alternativ forbindelse sættes filtrering og logning ud af spillet. Secure Browser og Exam Monitor vil fortsat kunne imødegå denne form for snyd, hvis den ikke-tilladte forbindelse forsøges etableret fra den computer, som eksaminanden bruger til eksamen. Den ikke-tilladte forbindelse må imidlertid imødegås på anden måde, hvis skolen hverken anvender Secure Browser eller Exam Monitor, eller eksaminanden etablerer forbindelsen til fx sin mobiltelefonen i stedet for computeren. Teknisk set kræver det, at der gribes ind mod ikke-tilladt radiokommunikation.

Vi ser tre principielle muligheder, som gennemgås i det følgende.

5.3.1 Scanning og pejling

Radiotrafik kan detekteres ved såkaldt scanning, og ved pejling kan man i nogle tilfælde også identificere kilden. Men i praksis er der en række udfordringer, som gør det urealistisk at anvende scanning i bekæmpelsen af snyd ved eksamen.

- Eksamenslokalet må formodes at være opfyldt af intens Wi-Fi-trafik, både fra den tilladte nettrafik via det officielle access-punkt og fra en del hot-spots udenfor lokalet. Det vil ofte være umuligt at udskille aktivitet fra fx illegale hot-spots. Nogle skoler har dog haft held til at detektere åbne hot-spots i lokalet.
- Mobiltelefoni-netværkene vil være til stede i lokalet, selv om alle mobiltelefoner m.v. er slukket, og det er ikke muligt at detektere den enkelte telefon.
- Bluetooth, Air-drop o.l. har så kort rækkevidde, at der skal scannes tæt på hver plads. Dette kan ikke ske uden, at eksaminanderne bliver opmærksomme på det, og kan nå at slukke for den ikke-tilladte forbindelse, før den opdages.

Scanning anses derfor ikke for praktisk anvendeligt til generelt at afsløre forsøg på snyd. Skjult scanning med hensyn til bluetooth m.fl. kortrækkende radiolinks kan dog have en funktion ved at bekræfte en mistanke om brug af illegale forbindelser, opstået ad anden vej. Men scanningen må i givet fald supperes med en mere indgående søgning efter udstyr eller spor på computere i det mistænkelige område. Afskrækkelsesvirkningen kan dog være grund til at bruge scanning.

Vurdering:
Devoteam vurderer, at scanning ikke vil have nogen synderlig effekt i praksis.

5.3.2 Jamming

Der har tidligere været gjort forsøg med at benytte jamming til at forhindre ikke-tilladt digital kommunikation i eksamenslokalet, fx med mobiltelefoner. Jamming består i udsendelse støj på relevante radiofrekvenser. Devoteam har forespurgt i Energistyrelsen om jamming vil være lovligt.

Energistyrelsen har oplyst, at jamming i princippet er frekvensanvendelse, som kræver en tilladelse efter frekvenslovens (lov 475 af 12. juni 2009) § 6, stk. 1. Jamming af mobiltelefoner ville i så fald være frekvensanvendelse i de frekvensbånd, som Energistyrelsen allerede har tildelt mobilselskaberne. Derfor er det ikke muligt for Energistyrelsen at give tilladelse til yderligere aktivitet i mobilfrekvensbåndene.

Mere generelt gælder, at jammere vil være radioudstyr, og omfattet Lov om Radioudstyr og Elektromagnetiske Forhold; lov nr. 260 af 16. marts 2016. De væsentligste relevante bestemmelser vil være lovens § 17, stk. 1, nr. 2 og 3., hvorefter radioudstyr skal være konstrueret således, at det ikke frembringer kraftigere elektromagnetiske forstyrrelser, end at andre apparater, faste anlæg eller radioudstyr kan fungere efter hensigten, og således, at udstyret understøtter en effektiv anvendelse af radiofrekvenser, så uacceptable forstyrrelser forebygges.

Jammere vil i sagens natur ikke kunne overholde disse bestemmelser, idet der (som det er hensigten med jammingen) vil være radioudstyr, som ikke vil kunne fungere på grund af forstyrrelser, og jammerne ikke vil heller ikke udnytte frekvenserne effektivt. Det er ikke tilladt at markedsføre eller bruge sådant udstyr. Dette gælder også, selvom forstyrrelserne vil være af en mere begrænset karakter, som det fx er tilfældet i forbindelse med en eksamenssituation.

Vurdering:
Jamming vil ikke være lovligt efter gældende regler, og er derfor ikke et muligt middel i bestræbelserne for at imødegå snyd ved eksamen.

5.3.3 Radiodødt rum

Alternativt til jamming har det været foreslået at forhindre brug af smartphones ved at afholde eksamen i et radiodødt rum, fx en betonkælder eller et såkaldt Faraday's bur, hvor rummet er omgivet af en metalskærm eller et metalnet.

Det må dog anses for urealistisk i en praktisk sammenhæng og skala. Dels vil elektromagnetisk skærmning udgøre hhv. kræve meget omkostningsfulde bygningsforandringer, dels vil løsningen være praktisk umulig i lånte eller lejede lokaler (haller o.l.).

Vurdering:
Etablering af radiodøde rum vurderes at være uforholdsmæssigt dyrt som middel mod snyd ved eksamen i de gymnasiale uddannelser.

5.4 Andre midler

5.4.1 Plagiatkontrol[8]

Plagiatkontrol bruges allerede af de fleste skoler i forbindelse med skriftlige afleveringer. Det udbredte skoleadministrative system, Lectio fra Macom, tilbyder bl.a. plagiatkontrol i forhold til samtidige og tidligere afleveringer i systemet. Mange skoler bruger også andre systemer til plagiatkontrol, fx Urkund. Netprøver.dk omfatter plagiatkontrol (ved Urkund) af alle hovedbesvarelser.

Plagiatkontrol tilbyder en efterfølgende mulighed for afsløring af, om der har været skrevet af ved udarbejdelsen af eksamensbesvarelsen. Og man kan formode, at den blotte bevidsthed om, at besvarelsen vil blive underkastet plagiatkontrol, vil afholde de fleste eksaminander fra at plagiere de kilder, de måtte råde over.

Plagiat er dog ikke ensbetydende med snyd under eksamen i denne analyses forstand (dvs. brug af ikke-tilladte kilder). Om det er tilfældet vil afhænge af, hvilke hjælpemidler eksaminanden har haft tilladelse til at bruge. Plagiatkontrollen kan heller ikke afsløre, om eksaminanden har anvendt tilladte eller ikke-tilladte kilder til inspiration til strukturering af besvarelsen el. lign.

På grund af den store udbredelse af plagiatkontrol, er plagiatkontrol selv et mål for snyd under eksamen. Vi er da også i vores interviews om snydemuligheder(jf. afsnit 3.1.1) stødt på viden om snydemetoder over for plagiatkontrol. Den eksaminand, der ønsker at bruge en ikke-tilladt eller ikke-opgivet kilde som forlæg, kan på forskellig måde forsøge at sløre dette over for plagiatkontrol-systemet. Der er således på internettet talrige anvisninger på, hvordan tekster manipuleres, så de ikke opdages af plagiatkontrolsystemer. Nedenfor gengives et udvalg:

- Indsætte tegn med hvidt i stedet for mellemrum
- Udskifte med de latinske bogstaver med bogstaver med samme udseende fra andre alfabeter (fx e)
- Ombytning af ordrækkefølge, ændre tegnsætning, udskifte ord med synonymer, slette eller tilføje fyldord
- Udskifte tekstlaget i pdf-filen med volapyk, men bevare præsentationslaget i filen (pdf-afleveringer)
- Lægge tekst i macro'er, så de kun ses af den menneskelige læser, ikke af scanneren (word-afleveringer)
- Regulær omskrivning

Der findes også programmer, word-makroer o.l. på nettet, der kan udføre i hvert fald de fire første typer sløringsaktiviteter automatisk.

Derved opstår der en risiko for falsk negative, dvs. at plagiatkontrollen ikke fanger faktiske tilfælde af plagiat. Det modsatte fænomen, falsk positive, kan opstå, fx hvis eksaminanden ikke er omhyggelig med at markere citater. I alle tilfælde må omfanget af evt. plagiat derfor vurderes af en fagkyndig person.

5.5 Opsummering af tekniske midler

De væsentligste midler mod snyd via den tilladte internetforbindelse kan sammenfattes i følgende oversigt.

[8] *Analysen her baserer sig i vidt omfang på nettilgængelige arbejder af Prof. Dr. Debora Weber-Wulff, HTW Berlin.*

Figur 5. Oversigt over egenskaber ved tekniske midler til imødegåelse af snyd

Løsning	Eksempel	Effekt							Forudsætninger	Omkostninger	Sårbarheder
		BYOD	BYOA	Data på egen computer	Ikke tilladt kanal	Kommu-nikation med andre	Tilladte/ Ikke tilladte kilder	Tilladte/ Ikke tilladte netsteder			
Tilsyn	Forbedret praksis	Ja	Ja	Kan afsløre	Kan måske afsløre	Kan afsløre	Kan afsløre	Kan afsløre	Ingen særlige	Opgradering af tilsyn	Krav til it-kompetencer Skjult omgåelse
Filtrering	Forbedret praksis	Ja	Ja	Ingen effekt	Ingen effekt	Kan vanskelig-gøre	Ingen effekt	Kan skelne med usikkerhed	Eksamen i egne lokaler	Server Content filtre Opsætning af filtre/server	Kompetencekrav Andre net Kompleks opsæt-ning
Logning	Som visse it-centre	Ja	Ja	Ingen effekt	Ingen effekt	Kan afsløre	Ingen effekt	Kan afsløre	ID på netværk Eksamen i egne lokaler	Analysesystem Manuel gennemgang af log	Gennemgang af log kun ved mis-tanke Kompetencekrav Andre net
Secure Browser	FLOWlock	Windows og MAC	Nej	Forhindrer	Forhindrer	Forhindrer	Ingen tillades	Ingen tillades	Ingen særlige	Licens, opsætning	Løbende opdate-ring Internationalt hackermål
Exam Monitor	Exam Monitor	Windows, MAC, Linux	Ja	Kan afsløre	Kan afsløre	Kan afsløre	Kan afsløre	Kan afsløre	Ingen særlige	Licens Opsætning Gennemgang af log	Netforbindelse Kompetencekrav Løbende opdate-ring

I oversigten er for fuldstændighedens skyld medtaget det tilsyn, som udføres af eksamensvagter. De tekniske midler skal nemlig i alle tilfælde suppleres af dette tilsyn.

Filtrering kan yde et væsentligt bidrag til at forhindre bevidst eller ubevidst tilgang til ikke-tilladte internetsteder. *Logning* kan være effektiv som dokumentation for en mistanke, der er opstået ad anden vej. Budskabet om, at skolens etablerer filtrering og/eller logning vil også have en forbyggende (afskrækkende) effekt. Opsætning af filtrering og logning er imidlertid omstændelige og stiller krav til kompetencer, som skolerne ikke altid kan råde over. Dertil kommer, at ikke med sikkerhed kan adskille tilladt trafik fra ikke-tilladt trafik, og ikke adskille tilladte kilder fra ikke-tilladte kilder på et netsted. Logning kan afsløre den ikke-tilladte trafik, hvis loggen gennemgås minutiøst. Men man kan heller ikke se forskel på kilder på samme netsted. Hertil kommer, at disse løsninger er sårbare over for eksaminandernes evt. brug af alternative net.

Secure Browsers vil (som den er realiseret i form af FLOWlock) kunne gøre god fyldest i en eksamen uden digitale hjælpemidler. Vi anser det derimod ikke for realistisk, at Secure Browsers kan bruges til at skelne mellem tilladte og ikke-tilladte netsteder, eller til at give begrænset adgang til materiale på egen computer. Det er fordel, at den anvendte secure browser løbende vedligeholdes af en international virksomhed. På den anden side gør den internationale eksponering også browseren sårbar som mål for alverdens hackere.

Exam Monitor kan overvåge alle aktiviteter og al internetkommunikation til computeren, men der skal en vis eksamensspecifik opsætning til, før end den automatisk kan give alarm ved ikke-tilladte aktiviteter. Uden opsætning må man i praksis forudsætte mistanke(eller tilfældig udtrækning) før end loggen gennemgås og analyseres. Det kan være uhensigtsmæssigt at basere sig på en ikke-kommerciel, hvor der er risiko for, at udbyderen selv mister interessen for løsningen.

Secure Browser og Exam Monitor kan også forhindre, hhv. afsløre, snyd via en alternativ netforbindelse, hvis denne søges anvendt sammen med den tilladte computer. Eksaminanden kan dog i stedet anvende fx mobilens browser for at tilgå en ikke-tilladt kilde.

Den væsentligste indsats mod alternative kanaler er derfor at begrænse eksaminandernes mulighed for at tilgå andre kommunikationskanaler end eksamensnettet. Dvs. sikre skolens øvrige netværk med adgangskoder, der giver mulighed for at spærre adgangen til disse net for de aktuelle eksaminander, og at forhindre eksaminanderne i at benytte deres mobil som adgangsvej.

Plagiatkontrol kan efter eksamen afsløre forskellige former for snyd, og kan dermed – med de forbehold, der er anført i afsnit 5.4.1 - bidrage til den samlede indsats til imødegåelse af snyd under eksamen.'

I Bilag 2 - Omkostningsvurderinger, har vi samlet oplysninger om priser for Respondus Secure Browser og Exam Monitor.

6 Anbefalinger og perspektiver

6.1 Praktiske muligheder

Som det indtil nu er fremgået af rapporten, er der en række tekniske midler, som i et vist omfang kan imødegå snyd ved eksamen. Devoteam vurderer, at der reelt er tre virkningsfulde tekniske midler til rådighed:

- Exam Monitor giver en stor chance for at afsløre, hvis eksaminanden misbruger den tilladte internetforbindelse til at tilgå ikke-tilladte netsteder, eller hvis eksaminanden forsøger at tilgå et andet net fra computeren.

- Filtrering og Overvågning af nettrafikken kan være et alternativ til Exam Monitor. De mangler dog dokumentationen for, hvad der er foregået på computeren, og er dermed mindre effektive og bl.a. sårbare over for brug af alternative net. I lyset af de vanskeligheder, der vil være med at opsætte korrekte filtre, er Logning at foretrække.

- Secure Browsers kan være effektive ved eksamener uden hjælpemidler, men på nuværende tidspunkt ikke til eksamener med adgang til visse hjælpemidler på nettet eller egen computer.

Effektiviteten af imødegåelsen ved tekniske midler vil øges betydeligt, hvis disse suppleres med følgende andre midler:

- Reduktion af mulighederne for at etablere alternative net ved i det mindste at forhindre eksaminanderne i at logge på andre af de net, som skolen råder over.

- Forbud mod, at eksaminanderne medbringer udstyr, der kan anvendes til at etablere alternative net (fx mobiltelefoner). Det har den yderligere fordel, at det evt. alternative net i givet fald kun kan udnyttes af den officielle computer, hvor Exam Monitor i givet fald kan afsløre det.

- Forbud mod, at diverse faglige samarbejdstjenester og sociale medier kører i baggrunden på eksaminandernes computere. Det kan kræve en ikke ubetydelig supportindsats, da eksaminanderne i mange tilfælde ikke selv er klare over, hvad der kører på deres computer.

- Etablering af et aktivt og kompetent tilsyn, der kan kende forskel på tilladte og ikke-tilladte faglige hjælpemidler samt spotte ikke tilladte samarbejdstjenester, og evt. ikke-tilladt udstyr som mobiltelefoner, Apple-watches etc.

- Klar og præcis vejledning og formidling af reglerne for eksamensafvikling, herunder for hvilke netsteder og materialer, det er tilladt at benytte ved den enkelte eksamen. Leveret både i god tid inden eksamen, og umiddelbart før eksamensstart på en passende alvorlig måde.

Som det er også er fremgået af rapporten, har det ikke været muligt at identificere tekniske midler, som 100% effektivt kan forhindre snyd ved eksamen, når eksamen skal være med adgang til visse hjælpemidler på nettet. Ingen af de identificerede tekniske midler kan fx kende forskel på tilladt materiale på et netsted og ikke-tilladt materiale på det samme netsted eller på eksaminandens egen computer. Og ingen tekniske midler kan fuldstændigt forhindre kommunikation med andre, hvis kommunikationen fx er skjult som opdateringer af en allerede eksisterende tekst på et tilladt netsted.

Men hvis Exam Monitor, Filtrering og/eller Logning som beskrevet ovenfor suppleres med et aktivt og kompetent tilsyn, opdaterede regler for eksamensafvikling, samt en præcis og passende alvorlig vejledning af eksaminanderne, kan der efter Devoteams opfattelse nås meget langt i retning af at imødegå snyd. I den nuværende situation anbefaler Devoteam en løsning centreret om Exam Monitor eller et lignende teknisk middel. Alternativt anbefaler vi Logning.

Det skal erindres, at Exam Monitor forudsætter et relativt omfattende set-up og/eller en omfattende gennemgang af eksamensloggen. Det er på den anden side vores vurdering, at opsætning af filtre til Filtrering vil kræve samme arbejdsindsats som opsætning af Exam Monitor eller mere, og at gennemgangen af log i tilfælde af mistanke vil være mere omstændelig.

Som det er fremgået af afsnit 3.1.1.3 , kan snyd foregå med andre midler end tekniske. Ved overvejelser om ændringer i indsatsen mod snyd, skal man derfor også tage indsatsen mod disse snydmuligheder i betragtning. Indsatsen mod de forskellige snydemuligheder vil skulle balanceres, så resultatet er en samlet reduktion af snydemuligheder, og ikke kun en relativ forskydning af snyd fra en mulighed til en anden.

6.2 Tekniske perspektiver

I lyset af den globale betydning af digital eksamen må det anses for overordentligt sandsynligt, at der globalt set vil blive udviklet og markedsført andre systemer med omtrent samme funktionalitet som Exam Monitor. I Danmark kunne man også forestille sig, at forskellige aktører på markedet for uddannelsesadministrative systemer kunne være interesserede (som fx UNIwise, jf. afsnit 5.2.4).

For de gymnasiale uddannelser kan der være en fordel ved at vælge en national eller global kommerciel løsning. Man vil ikke i samme grad være afhængig af, om SDU fortsat kan og vil vedligeholde og videreudvikle Exam Monitor. Udviklingen hen imod andre eksamensformer på SDU kan reducere SDU's egen interesse i løsningen. Det kan også tænkes, at andre producenter kan have bedre teknologier og mere kapital til udvikling og vedligeholdelse.

Det er også muligt at gennemføre et åbent udbud af en løsning på opgaven. I den forbindelse kunne man efterlyse løsninger på de hidtil uløste problemer med at skelne mellem den tilladte trafik og den ikke-tilladte trafik på indholdsniveau.

Generelt forventer Devoteam, at alle tekniske midler vil blive forældede/miste effekt over tid, og derfor skal revitaliseres eller udskiftes med mellemrum. Bekæmpelse af snyd ved eksamen kan på mange måder sammenlignes med kampen mod computervirus. Man er altid "bagud", og der findes ikke én løsning, men en kombination af forskellige løsninger. Løsningerne er ikke udelukkende tekniske, men handler mange gange om "awareness".

6.3 Alternative løsninger

Undervejs i analysen er Devoteam stødt på en række forslag til, hvordan man kan imødegå snyd ved eksamen med andet end tekniske midler. Disse forslag har forskellig baggrund og forskellige mere eller vidtgående konsekvenser. Devoteam har samlet forslagene under tre overskrifter efter deres umiddelbare virkemåde. Nogle af forslagene er gensidigt udelukkende, mens andre kan kombineres. Det skal understreges, at Devoteam ikke har taget stilling til forslagene.

1. Reducer behovet for adgang til mange internetsteder og risikoen for snyd med adgang til ikke-tilladte undersider o.l.:
    a. Tillad kun egne hjælpemidler, som kan isoleres (jf. løsningen i Norge).
    b. Indgå evt. aftaler med forlagene om isolerede (ord-) bøger eller om tilladelse til at downloade de pågældende kilder til en eksamensportal
    c. Forlang, at alle egne noter og arbejder deponeres på portalen
    d. Etabler evt. en server, som kan viderestille trafikken til de udpegede steder (og spærre for andre steder).

2. Anvend andre eksamensformer, der er nemmere at kontrollere:
    a. Afskaf adgang til internettet
    b. Giv fri adgang alle hjælpemidler og internettet
    c. Brug multiple choice eksamener med kort tid til hvert spørgsmål
    d. Afskaf stedprøver
    e. Opgiv BYOD og indfør haller med eksamenscomputere

3. Brug skrappere sanktioner
    a. Kropsvisitering ved mistanke om ikke-tilladte kommunikationsmidler
    b. Inspektion af computer (systematisk, ved mistanke, tilfældigt udvalgt)
    c. Mundtlig overhøring (systematisk, ved mistanke, tilfældigt udvalgt)

7 Perspektivering til folkeskolen

Folkeskoleforligskredsen aftalte i november 2014 en række initiativer til udvikling af folkeskolens prøver. Heriblandt to initiativer, som indebærer prøver med adgang til internettet:

- Prøven i skriftlig dansk i 9. og10. klasse skal ændres, så eleverne fremover har adgang til internettet under prøveaflæggelsen. Det vil dog ikke være tilladt for eleverne at kommunikere med andre over internettet under prøveaflæggelsen.
- Der skal gennemføres forsøg i 9. klasse med prøve i skriftlig fremstilling i fremmedsprogene (engelsk, tysk og fransk) med adgang til internettet. Heller ikke her må eleverne kommunikere med andre over internettet under prøveaflæggelsen.

Hertil kommer, at dele af folkeskolens afgangsprøver afvikles om selvrettende prøver via nettet. Ved nogle af prøverne er visse materialer tilladte.

I det følgende vurderer Devoteam, i hvilket omfang denne rapports observationer og anbefalinger også er relevante for folkeskolen.

Umiddelbart må det konstateres, at der med de selvrettende prøver og de to nye initiativer forekommer prøveformer, der er sammenlignelige med de eksamener med delvis eller fuld adgang til internettet, som vi har betragtet i denne rapport. Det må derfor lægges til grund, at der forekommer de samme muligheder for snyd. Dermed må det også antages, at de identificerede tekniske midler mod snyd vil kunne tages i anvendelse med samme effekt og med de samme svagheder.

Der formodes dog at være fire forskelle i karakteristika, der kan have betydning:

- Alderen på eksaminanderne
- Prøvens betydning
- Organiseringen af prøver og it-understøttelse
- Kontrol med udstyret

Ad alderen
Der er muligvis en forskel i snydetilbøjelighed, it-kompetencer eller andre kompetencer mellem elever i 9. eller 10. klasse og elever i de gymnasiale uddannelser. Men der er formentlig tilstrækkeligt høje niveauer af alle tre faktorer i en 9. eller 10. klasse til, at man må iagttage de samme forholdsregler mod snyd som over for gymnasieelever.

Ad Prøvens betydning
Sædvanligvis antages det, at snydetilbøjeligheden øges med prøvens betydning. Dette ville tidligere føre til en antagelse om, at snydetilbøjeligheden ville være mindre i folkeskolens afgangsklasser end ved studentereksamen. Men med de seneste reformer af optagelseskravene ved ungdomsuddannelserne må man imidlertid antage, at snydetilbøjeligheden vil ligge på samme niveau som i de gymnasiale uddannelser.

Ad organiseringen af prøver og it-understøttelse
Både i folkeskolen og i gymnasiet er det den enkelte skoles ansvar at afholde prøverne. Forskellen ligger imidlertid i de enkelte skolers størrelse. Der er væsentligt færre afgangselever pr. skole i grundskolen (gnsn. ca. 55) end i de gymnasiale uddannelser (gnsn. ca. 220).

Dette forhold betyder, at en grundskole må formodes at have væsentligt færre ressourcer til rådighed til tilrettelæggelse af eksamen, herunder til at etablere et værn mod snyd. It-drift og service er organiseret på mange forskellige måder i de enkelte kommuner. Vi formoder derfor, at nogle skoler står med en meget lille it-organisation til at løse problemet med imødegå snyd ved prøverne. I andre tilfælde har hver kommune en fælles it-enhed (eller kan organisere en sådan), som kan stå for it-opgaven ved de digitale prøver. De private skoler vil kunne have et større problem.

Folkeskoler, friskoler, private grundskoler, efterskoler[9]
2014: ca. 108.000 elever i afgangsklasser fordelt på ca. 1.900 skoler
Gennemsnitligt 55 afgangselever pr. skole

Gymnasiale uddannelser[10]
2014: ca. 149.000 elever i alt. Heraf ca. 50.000 afgangselever (anslået).
2016: 225 skoler med gymnasiale uddannelser.
Gennemsnit: ca. 220 afgangselever pr. skole (anslået)

Ad kontrol over udstyret
I de gymnasiale uddannelser er prøveafholdelsen lagt an på, at hver elev medbringer sin egen computer. Derfor indgår der ikke forslag om at installere bestemte programmer på elevernes computere i denne rapport. I folkeskolen skal skolen i princippet stille udstyr til rådighed ved digital eksamen. Men en stor del af eleverne i afgangsklasserne anvender deres egen computer. Man må derfor lægge til grund, at prøverne skal kunne aflægges ud fra et BYOD-princip, ligesom i de gymnasiale uddannelser.

Sammenfatning
Sammenfattende er det vores vurdering, at

- Problemet med snyd ved folkeskolens prøver vil være det samme som med snyd ved eksamen i gymnasiet
- Imødegåelse vil kræve, at de samme midler tages i brug som i gymnasiet
- Hver folkeskole har – i gennemsnit - ringere mulighed for at imødegå snyd ved digitale prøver end en gymnasial institution
- Folkeskolerne må formentlig støttes af kommunerne (fx af kommunens skoleforvaltning og it-center) i arbejdet med at imødegå snyd ved de digitale prøver

[9] *Kilde: MBUL institutionsregister og MBUL's statistikbank*
[10] *Kilde: MBUL's statistikbank.*

8 Bilag 1 – Erfaringer fra Norge

Det norske uddannelsessystem er det uddannelsessystem, der ligner det danske system mest. Devoteam har derfor valgt at undersøge hvordan forholdene ved uddannelser på det gymnasiale niveau er i Norge med hensyn til imødegåelse af snyd.

8.1 Nationalt niveau[11]

8.1.1 Organisering

Den del af det norske uddannelsessystem, der svarer til de danske ungdomsuddannelser, hedder "videregående oplæring". Uddannelsestilbuddene er delvist opdelt i et " Studieforberedende utdanningsprogram" og et "Yrkesforberedende utdanningsprogram". Der er en del fag, der har samme målsætning og evt. læses sammen i det studieforberedende og det yrkesforberedende uddannelsesprogram. I relation til drøftelsen af imødegåelse af snyd har vi ikke skelnet mellem programmerne, men talt generelt om skriftlige stedprøver.

Ansvaret for de enkelte skoler er placeret i de 19 fylkeskommuner. Fylkeskommunerne har også det overordnede ansvar for afvikling af eksamen på den enkelte skole, herunder for imødegåelse af snyd. Fylkeskommunerne står selv for at stille en del opgaverne til de eksamener, der indgår i uddannelsesforløbet. På hver skole er rektor ansvarlig, og et antal medarbejdere står for den praktiske gennemførsel. På statsligt niveau er ansvaret for eksamen placeret i Utdanningsdirektoratet under Kunnskabsdepartementet. Direktoratet står for de centralt stillede eksamensopgaver. Inkl. eksamener i grundskolen har direktoratet udarbejdet ca. 400 opgaver om året. I 2015 deltog i alt ca. 167.000 elever og privatister i videregående oplæring i en central stillet eksamen. Vi har ikke fået oplysning om, hvor mange der var skriftlige stedprøver. I relation til imødegåelse af snyd forlader Utdanningsdirektoratet sig på de tiltag, som gennemføres af fylkeskommunerne.

8.1.2 Hjælpemidler ved eksamen

Hovedreglen for eksamen i videregående oplæring er, at alle hjælpemidler er tilladt, bortset fra

- Internet og hjælpemidler, som tillader kommunikation
- Oversættelsesprogrammer i Norsk og fremmedsprog

Siden foråret 2015 har det imidlertid samtidigt været gældende, at skolerne selv kan vælge at lade elevene benytte netbaserede forberedelseselementer, læringsressourcer, opslagsværk eller ordbøger under eksamen, forudsat at skolerne er i stand til at isolere de aktuelle IP-adresser. De tilladte hjælpemidler skal være nogen, som eleverne har brugt i undervisningen. Det er det lokale niveau (Fylkeskommune og skole), som har ansvaret for afviklingen af eksamen, og som dermed bestemmer rammer og begrænsninger for hvilke hjælpemidler eleverne må bruge, samtidig med at skolen varetager sikkerheden under eksamen.

Nogle eksamener er todelte, således at der er en første del, hvor hjælpemidler er begrænset til skrivesager, passer, lineal og vinkelmåler, mens anden del gennemføres med alle hjælpemidler tilladt som beskrevet oven for.

[11] *Kilde: Interview med Utdanningsdirektoratet og Utdanningsdirektoratets rapport til Kunnskabsdepartementet: «Erfaringer og vurderinger av eksamen 2015 og 2016», 10. maj. 2016.*

8.1.3 Plagiatkontrol

Eksamensbesvarelser afleveres som hovedregel digitalt (evt. scannet) til et landsdækkende system. Der anvendes ikke generel plagiatkontrol i tilknytning til dette system eller i øvrigt. Men Utdanningsdirektoratet giver censorerne mulighed for at plagiat-scanne i tilfælde af mistanke.

I Norge skelner man i øvrigt mellem snyd og plagiat. Det beskrives således på Utdanningsdirektoratets hjemmeside (i vores oversættelse):

> *Snyd*
> Det er snyd at kommunikere med andre. Desuden er det snyd at bruge oversættelsesprogrammer i sprogfag. I fag som har todelt eksamen, er det snyd at bruge hjælpemidler ved første del af eksamen.
>
> Hvad er konsekvenserne af snyd til eksamen? Det er meget alvorligt at snyde til eksamen. Konsekvenserne af snyd eller forsøg på snyd er:
> - Eleven kan få eksamen i faget annulleret.
> - Eleven som får eksamen annulleret, mister standpunktskarakteren i faget.
> - Elever i videregående oplæring og privatister kan tidligst gå op til ny eksamen et år efter.
>
> *Plagiat*
> Plagiat er at bruge andres tekster helt eller delvis uden at opgive kilden.
> Når alle hjælpemidler er tilladte til eksamen, er det ikke plagiat at bruge kilder. Dersom eksaminanden bruger kilder, skal disse opgives på en ansvarlig måde. Dette er omtalt både i eksamensvejledningerne og i informationsdelen til eksamensopgaven.
>
> Hvad kan være konsekvenser ved plagiat? Hvis en elev i stort omfang benytter copy and paste fra andres tekster, kan det være vanskeligt at se elevens individuelle kompetence. Dette kan føre til lavere målopfyldelse.

Denne skelnen har givet anledning til debat i Norge. Modstandere mener, at plagering til eksamen belønnes. Utdanningsdirektoratet udbygger begrundelsen således (i vores oversættelse).

> Hvis elevene bruger kilder til eksamen, skal disse opgives på en ansvarlig måde. Hvis de ikke gør det, fører det mest sandsynligt til en lav karakter, fordi eleven i så fald ikke demonstrerer en selvstændig kompetence. Når det alligevel ikke er en del af reglerne for snyd, handler det om, at det for censorerne vil være vanskeligt at skelne mellem en elev, som fortsat bruger kilder på en umoden måde, fra en elev, som bevidst har undladt at opgive kilderne.
>
> Ideelt set kunne vi ønske, at vi kunne se denne forskel i elevenes svar, men det kan vi ikke med en anonym censur. Konsekvenserne ved snyd er, at standpunktskarakteren slettes, og at eleven ikke må aflægge eksamen igen, før der er gået et år. Når vi ikke kan være sikre på, at der er tale om bevidst snyd, er det vores vurdering, at det vil være en for streng sanktion. At elevene har vist lav kompetence og dermed får en dårlig karakter, er en mere rigtig reaktion[12].

[12] Originalteksten fortsætter "for elever i grunnopplæringa", dvs. for elever i grundskolen. Sondringen mellem snyd og plagiat findes imidlertid også for eksamener i videregående opplæring.

8.1.4 Forsøg med eksamen med adgang til internettet

I årene 2012-2015 har Norge gennemført forsøg med eksamener med adgang til internettet. Forsøget startede med to fag og 15 skoler, men er hvert år blevet udvidet med flere fag og skoler. I 2015 omfattede forsøget otte fag og 56 skoler.

I forsøget har eleverne haft ubegrænset adgang til internettet, men ikke lov til at bruge internettet til at kommunikere med andre i forbindelse med eksamen. Formålet med forsøget har været at se, om internettet kan fungere som en hjælpemiddel på linje med andre hjælpemidler. Elever, der deltog i forsøget har fået samme eksamensopgaver som elever, der ikke deltog i forsøget.
Overordnet betragtet vurderer Utdanningsdrektoratet, at forsøget har været vellykket, og at eksamen med adgang til internettet synes at være en eksamensordning, der fungerer godt under visse betingelser.

Forsøget er nu afsluttet, og der er udarbejdet en slutrapport (Rambøll). I det følgende resumeres de af Utdanningsdirektoratets observationer, som vurderes at have relevans for nærværende undersøgelse af snyd under eksamen.

- Det ser ikke ud til, at forsøget indebærer tekniske eller praktiske problemer
- Eksamensformen synes at påvirke undervisningen ved at øge fokus på faglig og pædagogisk brug af internettet, samt give større bevidsthed om og uddannelse i kildebrug og kildekritik.
- Der er få tegn på, at snyd og plagiat stiger som følge af eksamensformen.
- Evalueringen af forsøget viser imidlertid klart, at både blandt elever, undervisere og eksaminatorer til en vis grad er usikkerhed om grænserne for, hvad der er plagiat og snyd ved eksamener.
- Eleverne mener, at internettet er nyttigt ved eksamen, fordi det giver dem mulighed for at dobbelttjekke oplysninger, bruge opdaterede statistikker og aktualisere besvarelsen. Denne vurdering varierer dog fra fag til fag.
- Censorerne er de mindst positive over for eksamen med fuld adgang til internettet, men har kun i ringe grad observeret forskelle på besvarelser med og uden internetadgang.

8.2 Lokal indsats mod snyd[13]

Som nævnt er ansvaret for afvikling af eksamen i Norge placeret hos de 19 fylkeskommuner. Disse har på forskellig vis forsøgt at løse udfordringen med at stille netbaserede ressourcer til rådighed, og samtidigt isolere de pågældende IP-adresser og spærre for kommunikation. Hovedparten af fylkeskommunerne opererer efter det oplyste med afgrænsede "elevnet", filtrering i forhold til positiv-lister ("white-lists") og nøje udvælgelse af netsteder, der ikke giver mulighed for viderestilling o.l. Enkelte bruger en citrix-løsning, hvor brugernes applikationer afvikles på en central server, og man dermed har fuld kontrol over, hvilke netsteder der kan besøges.

Vi har som led i undersøgelsen haft dialog med Østfold Fylkeskommnune (i det følgende benævnt ØFK) om, hvilke forholdsregler ØFK tager for at imødegå mulighederne for snyd, samt for at kunne stille hjælpemidler til rådighed med afgrænsede IP-adresser.

8.2.1 Digital eksamen generelt

Uddannelsesafdelingen i ØFK udarbejder og opdaterer de lokale retningslinjer for planlægning og gennemførelse af eksamen i skolerne. Retningslinjerne bygger på de nationale retningslinjer. Rektor på hver

[13] *Kilde: Korrespondance med Opplæringsavdelingen, Østfold Fylkeskommune.*

skole har hovedansvaret for at skolen overholder retningslinjerne. Hver skole har også en eller flere medarbejdere, der har ansvaret for den egentlige eksamensgennemførelse.

Sikring imod, at eleverne bruger computeren til ikke-tilladt kommunikation eller fildeling med andre baseres på følgende tiltag:

a) Alle elever i ØFK får uddelt en elev-pc ved skolestart. Det er kun denne pc, som kan bruges under eksamen.
b) Eleverne er tilknyttet ØFK's elevnet. IT-afdelingen i ØFK har udviklet et adgangsstyringssystem, som kan styre adgangen til internettet for alle brugere, som er tilknyttet elevnettet. (Se nedenfor)
c) Scanning for ikke-tilladt elektronisk kommunikation i eksamenslokalet foretages ikke kontinuerligt, men stikprøvevis ved skolerne under eksamen.
d) Internettrafikken logges, men det føres ikke kontinuerligt tilsyn med loggen. Kun ved mistanke om snyd/brug af ikke-tilladte netsteder.
e) Der kan foretages inspektion af elevens computer for ikke-tilladte hjælpemidler (fx oversættelsesprogrammer) i form af stikprøver ved skolerne under eksamen.
f) Der er forbud mod at medbringe mobiltelefon og smartwatches. Musikafspillere er kun tilladt, dersom eksamensopgaven kræver det (f.eks. i musikfag). Elevene kan imidlertid bruge ørepropper/headset koblet til pc-en, hvis de har digitale hjælpemidler, som de vil bruge.
g) Eksamensvagterne (tilsynet) må også følge med på elevenes skærme under eksamen.
h) Til syvende og sidst er eleverne selv ansvarlige for at undgå at bruge hjælpemidler, som ikke er tilladte, dersom de skulle få mulighed for det.

8.2.2 Udvælgelse af netbaserede hjælpemidler

Som nævnt ovenfor er adgang til internettet som hovedregel ikke tilladt. Men skolerne kan vælge at lade elevene benytte netbaserede forberedelseselementer, læringsressourcer, opslagsværker eller ordbøger under eksamen, såfremt skolerne er i stand til at isolere de aktuelle IP-adresser.

ØFK bestemmer dette for alle videregående skoler i ØFK efter indstilling fra skolerne. Der har været hovedfokus på at åbne for ordbøger, opslagsværker, forlagenes netsteder og andre helt centrale fagnetsteder.

ØFK's adgangsstyringssystem giver mulighed for at afgrænse de tilladte URL'er. I de tilfælde, hvor det ikke er muligt at styre adgang til et hjælpemiddel på denne måde, eller hvor ØFK er usikre, tillades det ikke at bruge netstedet under eksamen.

8.2.3 Adgangsstyringssystem

ØFK har som nævnt etableret et adgangsstyringssystem til styring af adgang til netressourcer. Systemet kan kort beskrives således:

> Eleverne er tilknyttet ØFKs elevnet. Adgangsstyringssystemet kan styre adgangen til internettet for alle brugere, som er tilknyttet elevnettet. Adgangsstyringen er koblet op imod ØFKs skoleadministrative system, således at enkeltelever eller undervisningsgrupper kan udelukkes fra internettet, eller eventuelt gives begrænset adgang til internettet. Systemet spærrer for videre trafik ud på internettet, dvs. eksterne links, sociale medier, chat osv. Systemet fungerer ved hjælp af "white lists" og opsætninger af filtre i firewall.

8.2.4 Virkninger for eksamenstilsynet

Ordningen har ført til ændring af opgaver og kompetencekrav for eksamenstilsynet. Eksamensvagterne skal have relativt god IT-kompetence. De bør kunne skelne mellem tilladte og ikke-tilladte netsteder, og de bør kunne genkende teknisk udstyr som ikke er tilladt (f.eks. mobilt bredbånd osv.) Hvis de er i tvivl, må der tilkaldes IT-teknikere eller den eksamensansvarlige på skolen.

Tilsynet skal også kunne hjælpe til med udskrifter, samt download og upload i forhold til Utdanningsdirektoratets digitale system for eksamen (PGS).

8.2.5 Erfaringer med eksamen med åbent internet

Tre skoler i ØFK deltog i forsøget med åben adgang til internettet (jf. afsnit 8.1.4).
I dette forsøg brugte ØFK ingen tekniske løsninger for at sikre, at elevene ikke fik adgang til ikke-tilladte hjælpemidler. Her baserede skolerne sig på udvidede tilsynshold og oftere inspektion med IT-teknikere i eksamenslokalet. Skolerne havde fokus på god undervisning af elevene på forhånd om, hvad som er tilladt og ikke tilladt på internettet.

9 Bilag 2 - Omkostningsvurderinger

I dette bilag gengives oplysninger om priser ved licenser til hhv. en Secure Browser og Exam Monitor.

9.1 Secure Browser

Devoteam har ikke drøftet priser med UNIwise.

Den amerikanske udbyder af Respondus har en standardprisliste for årlige site-licenser for uddannelsesinstitutioner, der begynder ved 2.400 USD (ca. 13.200 DKK) for op til 2.000 studerende og ender med 6.000 USD (ca. 40.000 DKK) for op til 40.000 studerende. For større studentertal oplyses priser på forespørgsel.

De danske gymnasiale uddannelser falder ind under den amerikanske kategori K-12. For sådanne institutioner gives priser efter individuel forhandling. For en ren secure browser-løsning vurderer vi, at priserne pr. studerende ikke vil overstige de ovenfor nævnte standardpriser.

Såfremt hver gymnasial institution skulle anskaffe sin egen Respondus-løsning til listepris, ville det således løbe op i 225*2.000 USD ~ ca. 3 MDKK).

Det må formodes, at der kan opnås bedre priser ved koordineret indkøb. Ud fra ovenstående amerikanske priser kan det anslås, at en national sitelicens for de ca. 150.000 elever i de danske gymnasiale uddannelser vil kunne erhverves for højst 150.000*1 DKK ~ 150.000 DKK.

Ved overvejelser om anskaffelse bør man medregne fordanskning, lokal supportorganisation m.v.

9.2 Exam Monitor

SDU har oplyst følgende om den aktuelle prissætning af Exam Monitor:

1. Licens: kr. 20,- pr. studerende pr. eksamensbegivenhed
2. Implementeringspakke pr. institution: 10.000 kr.
   Pakken indeholder:
   - 2 dages konsulentydelse
   - Egen hjemmeside, hvorfra de studerende kan hente information og softwaren
   - Test-setup, hvor de studerende kan teste deres egen computer
   - Uddannelse af administrator og IT-supporter
   - Rådgivning vedr. etablering af supportorganisation til digital eksamen (fx vedr. lånecomputere, eksamens-supportere, eksamensvagter)
3. Evt. yderligere konsulentbistand til 600 kr. pr. time

Det må formodes, at disse priser vil kunne være genstand for forhandling, og vil kunne reduceres, hvis Exam Monitor bringes i anvendelse i hele gymnasiesektoren.

devoteam.dk

Innovative technology consulting for business