Technische hulpmiddelen bij tentamens
hoe kun je veilig blijven toetsen?

Opgesteld door Chris Rouwenhorst & Cornelise Vreman
(beide werkzaam bij CES-CELT)

Aanleiding voor dit document

Vanuit de examencommissie ST werd de vraag gesteld hoe de opleiding (docent, examencommissie) om moet gaan met de technische hulpmiddelen bij tentamens. Technische mogelijkheden van de meeste apparaten (telefoons, ipads, PCs, notebooks) zijn zeer ruim en groeien allemaal naar elkaar toe. "Open boek" betekent tegenwoordig dat velen graag een laptop of tablet meebrengen met leesmateriaal. In hoeverre is het dan te voorkomen dat studenten ook op internet gaan of met elkaar communiceren via internet.

Wat is er technisch mogelijk om internet toegang onmogelijk te maken in examenruimtes en hoe kun je regels hierover op een homogene manier controleren?

In de beantwoording van de vraag gaan we eerst in op 'veilig toetsen – wat versta je eronder'. Vervolgens behandelen we een aantal risico's en een aantal mogelijkheden om met die risico's om te gaan. We sluiten af met een aanbeveling om deze vraag op UT-niveau op te pakken, omdat dit niet iets is dat individuele examencommissies op kunnen lossen.

1. Veilig toetsen en risico's - een inleiding

Veilig toetsen is een issue van alle tijden. 'Vroeger' werden spiekbriefjes gebruikt, probeerden leerlingen bij elkaar op het papier te kijken of werd er van alles in de grafische rekenmachine geprogrammeerd. Nu, met de komst van technische hulpmiddelen, is het repertoire aan 'spiekmogelijkheden' vele malen groter. En als je dan met deze technische hulpmiddelen kunt 'spieken', heeft de student ook toegang tot veel meer informatie.

Voorbeelden van 'hedendaagse' risico's:

- Student maakt via WIFI connectie met internet.
- Student maakt verbinding met internet op de laptop via telefoon.
- Student maakt verbinding met notebook via telefoon om met andere studenten te communiceren.
- Bluetooth, infrarood, of het opzetten van een eigen netwerk kan gebruikt worden om met andere studenten te communiceren.
- Studenten gebruiken een 'messenger' om onderling te kunnen communiceren.
- Student zet bestanden klaar in programma, zodat ze die kunnen gebruiken op laptop (bv in Matlab al wat programmatuur klaar hebben staan).
- Het gebruik van een USB stick met opgeslagen data.
- Een speciaal soort muis waarin data is opgeslagen die beschikbaar gesteld kan worden op de laptop.

2. Inventarisatie van SURF

Veiligheid heeft een prijs. SURF (De ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland) geeft als advies mee om onderscheid te maken tussen formatieve (tussentijdse) en summatieve (eind) toetsen. Sietses [1] geeft bijvoorbeeld deze rangschikking weer van het belang van veiligheid bij diverse soorten toetsen:

Belang van veiligheid:

- Low: formatieve toetsen en tentamens, of online courses waar geen grote maatschappelijke waarde aan wordt gehecht.
- Medium: toetsen die niet direct (significant) bijdragen aan de cijferlijst, maar waar wel consequenties aan vastzitten.
- High: tentamens die direct significante invloed hebben op het behalen van studiepunten.
- Very high: specifieke vakken of toetsmomenten die door de aard van het vak, of de (juridische) consequenties nog hogere eisen stellen aan fraudepreventie. Denk hierbij aan toetsen met direct civiel effect zoals het halen van een BIG-registratie of de eindscriptie.

Daarnaast kun je ook een inschatting maken van de diverse risico's ten aanzien van fraude die de opleiding aangaat, bij de diverse toetsvormen [1].

- Low: een toetsmoment waarbij de student volledig uniek werk inlevert. Denk hierbij aan scripties, essays en een mondeling examen, maar ook aan praktijkopdrachten.
- Medium: een toetsmoment waarbij antwoorden uniek zijn, maar het geen volledig eigen werk betreft zoals bij een scriptie of essay.
- High: tentamens waarbij slechts één antwoord mogelijk is en studenten per vraag dus nauwelijks uniek van elkaar kunnen antwoorden.

Voor diverse toetsvormen kan in kaart worden gebracht wat het belang van veilig toetsen is en welke mate van risico de opleiding loopt op fraude.

		BELANG			
		Laag	Middel	Hoog	Heel hoog
RISICO	Laag	Formatieve toets, tussentoets	Mondelinge tussentoets	Essay of betoog, praktijkopdracht	afstudeerwerk
	Middel	MOOC: open vragen	Tussentijdse toets met open vragen	Tentamen met open vragen	
	hoog	MOOC met gesloten vragen	Tussentoets met gesloten vragen	Tentamen met gesloten vragen	

Tabel 1: Voor diverse toetsvormen een overzicht van de belangen van veilig toetsen en de risico's op fraude. (Sietses [1]).

3. Beleid in den lande

Het beleid op het gebied van veilig digitaal toetsen staat in Nederland nog in de 'kinderschoenen'. In Maastricht is men van plan om vrij ver te gaan, ze scannen WIFI in de examenzaal en bij de WC wordt gecontroleerd met scanners. In Maastricht is dus veel 'afgeschermd'. De TUE heeft een risico analyse laten maken, waarbij de diverse risico's bij verschillende toetsvormen in kaart zijn gebracht (tabel 1 dus

veel verder uitgewerkt). Naast die matrix zijn er oplossingen geformuleerd om fraude tegen te gaan. (dit document is niet vrij toegankelijk om zo te voorkomen dat studenten zicht krijgen op de technieken die ingezet worden om fraude tegen te gaan).

4. Welke opties zijn er om de veiligheid van toetsen te bevorderen?

SURF gaf eerst aan dat de optie van Bring Your Own Device (BYOD) niet veilig genoeg zou zijn. In de loop van de tijd is SURF daar toch op terug gekomen, omdat er nu meerdere projecten lopen met **USB's sticks** (en andere oplossingen die een toetsomgeving creëren op operating system niveau van het eigen device). In die projecten draait het erom dat de student de laptop start vanaf de USB stick (of netwerkboot). Na deze opstart vanaf USB is er een veilige omgeving gecreëerd waarin de student nergens anders bij kan dan wat er op de USB staat. De student werkt dan nog wel met de eigen hardware, maar kan niet meer bij de eigen programmatuur. Het grote voordeel van deze oplossing is ook dat er andere software pakketten (bv Matlab) ter beschikking kunnen worden gesteld. Dit kan ook zorgen voor een authentiekere toetsafname. De UT doet mee met pilots op dit gebied, mede omdat een UT-student zo'n 'veilig toetsen USB stick' heeft ontwikkeld.

Een andere optie is de **Lock-down browser**. Een docent kan bv op Blackboard een toets klaar zetten. Als de student die toets opent, kan alleen de toets op het getoond worden, totdat de student klaar is met de toets. SURF geeft echter aan dat deze 'lock down browser' nog te omzeilen is en dus niet geschikt is voor een toets waarbij het belang van veilig toetsen erg hoog is.

5. Conclusies

Vooralsnog lijkt het erop dat de USB stick de meest geschikte optie is in de race voor 'veilig digitaal toetsen', maar dit project is nog in de pilot fase. SURF gaat binnenkort wel meer projecten starten om dit verder te ontwikkelen, maar het eerste jaar hebben we er nog niet echt wat aan. Bovendien: Om studenten met zo'n USB stick veilig toegang te geven tot een e-book (zoals in aanleiding vermeld stond) haal je je als docent wel een hoop werk op de hals (bv USB stick werkt nog niet op alle soorten laptops, dus je moet reserve laptops hebben; een ruimte met voldoende stroompunten etc.).

Tot die tijd zou je als docent kunnen kijken naar toetsvormen waarbij het risico op fraude niet zo hoog is, en dus goed surveilleren. Wellicht kan de examencommissie nog eens kijken (en docenten wijzen op) de regels die er zijn voor het veilig afnemen van papieren toetsen.

Kijken we naar de meer lange termijn dan is onze aanbeveling dat de UT gaat werken aan een digitaal toetsbeleid, omdat veilig digitaal toetsen wat meer behelst dan een paar regels. Een eerste stap zou een risicoanalyse per toetsvorm kunnen zijn (waartoe Sietses dus al een aanzet heeft gegeven), waarbij per toetsvorm advies wordt gegeven ten aanzien van de veiligheidsmaatregelen.

Referentie:

1. Sietses, L. (…) Keuzemodel toetsveiligheid. Een hulpmiddel voor een onderbouwde keuze. Presentatie bij SURF. https://www.surf.nl/binaries/content/assets/surf/nl/2015/20151211-presentatie-keuzemodel-toetsveiligheid---lex-sietses.pdf

Vragen over of naar aanleiding van deze notitie? Ideeën of suggesties voor verdere acties?

Op de UT houdt het team voor Technology Enhanced Learning and Teaching (TELT) zich met thema's zoals in deze notitie beschreven bezig. In het team zijn zowel onderwijskundigen van CELT als medewerkers van de afdeling ICTS vertegenwoordigd. https://www.utwente.nl/telt/

Heeft u vragen of opmerkingen naar aanleiding van deze notitie of ideeën of voorstellen met betrekking tot het thema "digitaal toetsen", neem dan contact op met:
Chris Rouwenhorst, c.rouwenhorst@utwente.nl, +31534891034.