START REPORT

A report on the current state of online proctoring practices in higher education within the EU and an outlook for OP4RE activities

OP4RE Online Proctoring for Remote Examination

Improving Access to Higher Education through State-of-the-Art Assessment Technology and Procedures

Erasmus+ erasmus+
meer perspectief

Version May 9, 2017

Table of Contents

1 Introduction

This report contains the findings and conclusions of the preliminary desk research phase and the first experiments of the Erasmus+ KA2 Strategic Partnership project *Online Proctoring for Remote Examination* (OP4RE). This report offers a state-of-the-art review in early 2017 of *online proctoring* or *online remote examination*.

The importance of this topic is very clear in relation to several goals of the EU (European Union) and institutions of Higher Education (HEI) in general. Concerning the EU, this project specifically considers the Erasmus+ priority of 'supporting the implementation of the 2013 communication on opening up education' along with the directive on 'open and innovative education, training, and youth work in the digital era'. The priorities of Erasmus+ address the ultimate objective of using the current strides in technological advancements to increase access to higher education for citizens. Finally, by focusing on technological advances, the current findings as presented firmly promote the Erasmus+ general objective of 'modernizing education, training and youth work'. It is expected that online proctoring will contribute to increasing access to Higher Education for various groups of (prospective) students. Online proctoring is expected to increase the opportunity for 'anytime, anyplace' examination processes.

The prevailing European cultural view is that summative assessments are an integral part of accredited education courses and programmes and that secure exams are needed in several circumstances to assess student achievement. HEIs and society at large place a strong emphasis on trustworthy examination processes. When HEIs are exposed to and confronted by (suspicions of) non-academic, unethical or simply fraudulently acquired certifications, diplomas or degrees, serious consequences can occur, such as declining numbers of students, damaged reputations and nullifying awarded diplomas. Exams must therefore be conducted in a manner in which high personal and academic standards of behaviour from all stakeholders involved in the examination process are employed. These stakeholders include students, academic faculty members, examiners, exam boards and proctors as well as IT-staff and administrative staff. Cheating, collusion and/or fraudulently acquiring assessment results are the core phenomenon that proctoring must prevent during the examination process.

To investigate these topics, this report lays the groundwork for further activities in the OP4RE project. It begins by defining and describing online proctoring. Secondly, it outlines the current practices of online proctoring in selected countries in the EU and outside of the EU. Thirdly, issues regarding security and privacy are discussed. In addition, some highly preliminary findings regarding online proctoring and accreditation are described.

This Start Report is a living document. As the OP4RE project continues to progress, this document will be amended and expanded, eventually leading to a set of Intellectual Outputs as main output for the OP4RE project.

This project is a collaboration of HEIs across Europe. The extensive cooperation for this project signifies the importance attached to access to education, especially remote education and assessments, in an increasingly globalised Higher Education system. The collaboration further allows for the exploration of a variety of perspectives regarding security, privacy, fraud prevention and detection and applications whilst reviewing the diverse needs and experiences of a broad platform of users.

The public website of the project is http://www.onlineproctoring.eu.

2   What is Online Proctoring?

2.1   The Examination cycle

Before discussing online proctoring, the concept of the test cycle is introduced. In general, for exams, a test cycle describes the process of (1) determining the goal of a test, (2) designing a blueprint describing the distribution of test items across the content of the goal of the test, (3) designing the test items and test, (4) administering the test and (5) analysing, scoring and evaluating the test. This is shown in Figure 1.

Figure 1 Examination Cycle
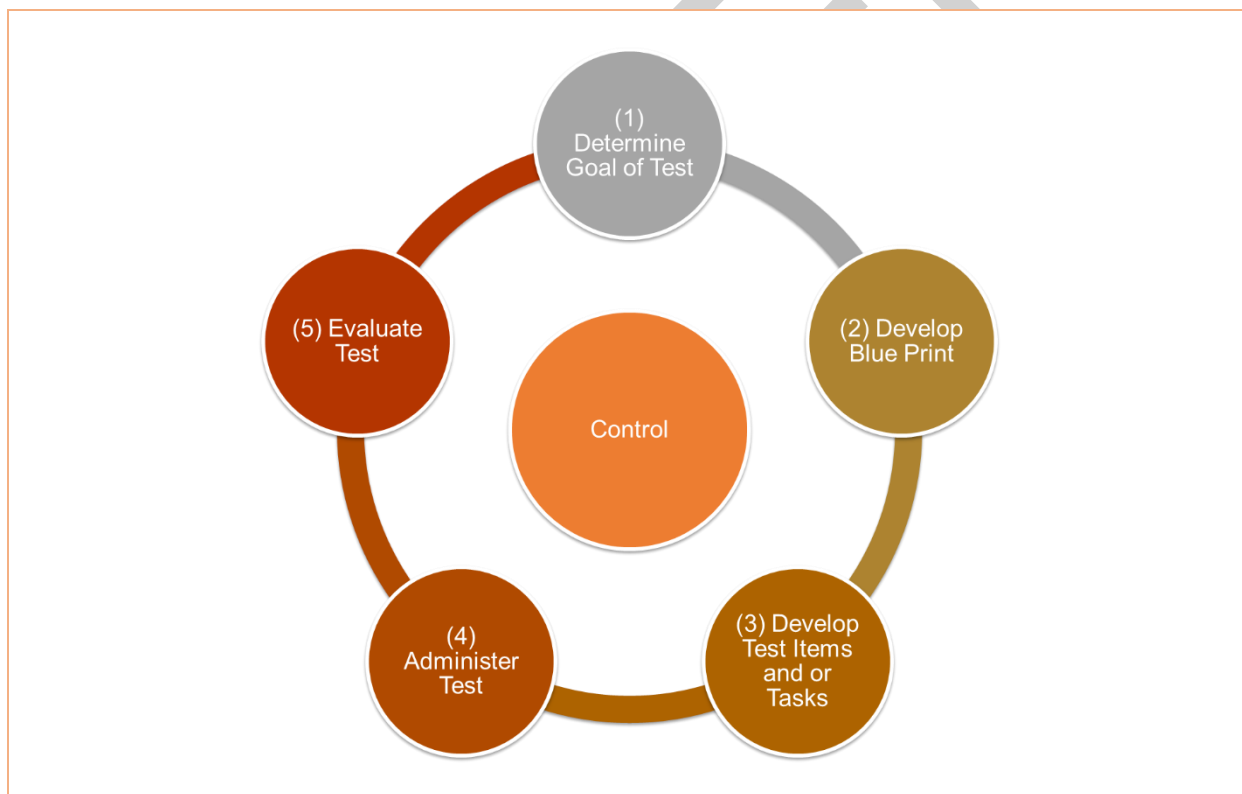
This report focusses on the process of administering and evaluating tests in which proctoring and results of proctoring play a primary role.

In the examination cycle, cheating or fraud can occur at various steps of the cycle. Test items can be stolen or harvested by test-takers, teachers can accidentally publish the correct answers to an upcoming exam, examiners can increase passing rates in an unethical manner, hackers can change grades, etc. In this report, these forms of fraud or cheating are not taken into account. Instead, the proctoring process is the focus.

Remark 1

Throughout this report, the term *examination* is used as well as *test* or *assessment*. These terms are used to denote a specific category of assessments, namely assessments in written form, with tasks or with selected response questions (test items). These assessments have a summative goal, meaning that the stakes of these tests are high, as they are used for selection, certification or achievement testing. Also, the assessments are intended to measure individual achievement.

This means that when administering a test, individuals must take the test without cheating. Cheating in general means that the test-taker used unpermitted means to answer a test question, such as by using materials including cheat sheets, other individuals or digital sources.

For each exam, various exceptions can be made to this general rule, such as formula sheets, calculators, books and computer programmes that are permitted when taking an exam.

2.2 Proctoring

Proctoring (or invigilation) plays an important role in the administering process. Proctoring is the process of watching people take an exam to ensure that they do not cheat. In a physical on-site examination situation, test-takers take the test in a confined space in which human proctors perform 'live' invigilation. Usually, a number of test-takers take an exam at exactly the same time and take the same test. Proctors do their invigilation work concurrently with the test-takers taking the exam.

Based on clear instructions, invigilators oversee test-takers to visually establish whether a test-taker commits an action regarded as cheating or malpractice. The exam space

itself is organised in such a manner that there are minimal opportunities for test-takers to see each other's exam papers or answer sheets. When these exams are administered via computers in a confined space, measures are taken so that test-takers cannot see one another's screens, or the order of questions is scrambled.

Figure 2 Illustration of physical on-site digital exam facilities[1].

During the proctoring process, clear demarcations are made with respect to the responsibilities of the invigilators on the one hand and examiners on the other hand. In general, invigilators have two important tasks. First, invigilators have the task to prevent cheating (by their presence and continuous supervision). Second, invigilators have the task to signal and report (suspicious) cheating behaviours.

Preventing cheating by continuously supervising a test-taker is the most impactful result of invigilation. Based on the psychological mechanism of the placebo-effect (Alderson, 2016), test-takers diminish their consideration for cheating if they are supervised or when they are under the assumption that they *can* be watched *at any time*.

Identifying cheating and taking actions when cheating is suspected is in fact the last

---

[1] Left: Digital exam hall, Vrije Universiteit Amsterdam
Right: Testing Centre at Indiana University - Purdue University Indianapolis

resort to prevent cheating. Invigilators must be trained to decide when interrupting the test-taking process of individuals is appropriate. For example, invigilators must follow procedures that describe whether they first should warn a test-taker before further actions can be taken or whether they can take action directly. Also, local procedures will lay down whether/when an invigilator should call in the examiner during the process to decide on the course of action or whether the invigilator can act on his/her own. Typically invigilators will write up a report describing the suspected cheating situation.

It is then the responsibility of the examiner, who in HEIs in general will be the teacher of a specific module, to decide on appropriate measures based on the invigilator's report. The examiner evaluates the seriousness of the suspected fraud and determines which penalties should accompany that fraud. These penalties can be limited (removal from the exam or nullifying the test attempt) or extensive (removal from a degree programme or fines). The examiner usually submits the decision as advice to an exam board. The exam board in general is the official body of the HEI with the jurisdiction to impose a range of penalties; however, a process is often begun in which the exam board or academic conduct officer invites the suspect of fraud to an adversarial process. During this process, the report serves as an important document for discussion and decision making.

Figure 3 Flow chart cheating and malpractice determination.
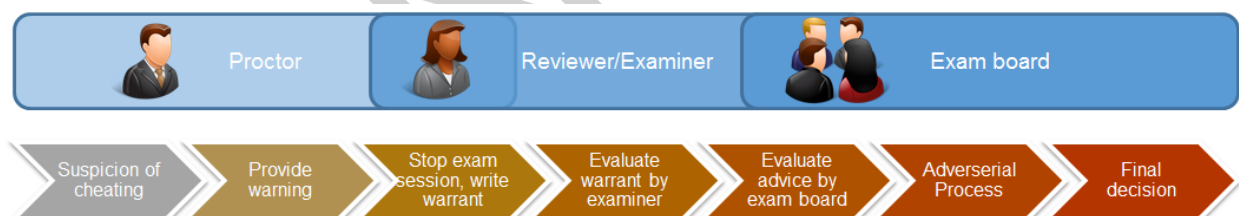
2.3   Online proctoring

For online proctoring, the process described is essentially very similar; however, due to the technology and additional actors involved, this process is more complex.

First, in an online proctoring situation, clear demarcations between the human actors, systems and procedures must be established. Many systems and procedures are already present at universities, but others are entirely new. The necessary systems are outlined in the next section.

2.3.1   E-assessment system

A widely used system in an online exam process is the *assessment (management) system*. An e-assessment system in general comprises functions for the following:

(1) creating and storing tasks and test items in a question-bank
(2) drawing test items from the question-bank, to form a test based on the assessment design
(3) presenting the test and items to the test-taker on the screen usually via a web browser
(4) receiving the students' answers
(5) scoring the test and performing psychometric analyses.

An assessment management system can also be part of a Managed Learning Environment (MLE). MLEs are used throughout HEIs worldwide.

2.3.2   LockDown browser or LockDown OS

In some instances, the e-assessment system also uses software known as LockDown™ browser. A locked down browser is a separate browser application or browser extension that has restricted capabilities. For example, a locked down browser only admits the test-taker to access a particular website (generally the e-assessment website), and it prohibits access to running programmes from a local computer.

Another approach is to have an operating system configuration in place that restricts access to any type of prohibited sources. These configurations can be enforced using Object Policies in Windows™, for example, or by booting from specially prepared USB-sticks. For online remote examinations, these approaches are normally deemed to be impractical.

2.3.3   Simple digital assessment system

An e-assessment system is not a necessary tool for an online exam. Test-takers can also be instructed to download an empty Word or PDF document, type in the answers to the questions and upload the completed file to a repository.

2.3.4   Pen-and-paper assessment

A test-taker can also be instructed to write answers to tasks or test items on a sheet of paper, scan it and send it via e-mail to a specific address.

2.3.5 Proctoring system and process

The proctoring system is in place during an exam along with the assessment system.

There are several administrative steps that precede remote live or recorded proctoring. First, the HEI will create an exam within the e-assessment system that must include correct settings regarding exam instructions, screen lay-outs, dates, times, access to information and the examination rules of conduct. Second, the HEI will include proctoring session information in the proctoring system. This session must be aligned with the settings in the e-assessment itself with respect to dates, times and examination rules of conduct. Specific details in the examination or proctoring process require careful communication and training.

In principle, two forms of proctored exam sessions are possible. The first, *live proctoring* includes exams in which all test-takers take the test at exactly the same time.

Live Proctoring. With *Live proctoring*, an actual proctor is present and proctoring simultaneously with the test-takers. With the current design of ProctorExam's assessment support products, one proctor can proctor seven to eight students simultaneously; however, the technology available allows universities to draft their own preferences. *Live proctoring* implies that the planning of exams and proctors must be closely aligned. Second, there are exams for which time windows are set for test-takers to begin an exam based on their preferences. This is called ***Record and Review***. The flexible exam can be taken 24 hours a day and seven days a week within the given time window. With *Record and Review* proctoring, which is much more automated, students can take an exam without a proctor present at the time the test is taken. Therefore, any number of students can begin an exam at a given time.

The preliminary process that ensures appropriate proctoring is to inform test-takers about the procedures regarding the proctoring process and the actual exam. Therefore, beginning weeks before an online exam, the test-taker must enrol for the exam via an institutional subscription system, e-assessment system or MLE. The student then receives an e-mail from the proctoring system or directly from the examiner to prepare for the remote exam at home.

At the appointed time the test-taker logs on to the proctoring website, after which the proctoring website takes the test-taker through several steps. During these steps, the student is instructed to install a proctoring software extension for the Chrome browser, or to install an app for the proctoring software (for Android or iPhone smartphones or tablets) and to test the internet quality (bandwidth, stability), webcam, screen sharing and camera of the smartphone. After all these tests have been executed successfully, the test-taker will be able to take part in the actual proctored exam. A confirmation e-mail is sent to the test-taker for confirmation.

Figure 4 Flow chart checks technical operation proctoring software test-taker side.

When the exam is due, a test-taker logs on approximately 10 minutes before the actual start time of the exam for the proctoring session. The main steps in the proctoring session are (1) to login to the proctoring system and begin a proctoring session, (2) to login to the e-assessment system and begin the exam, (3) to finish the exam and (4) to finish the proctoring session as shown in the figure below.

Figure 5 Flow chart proctoring and assessment process.
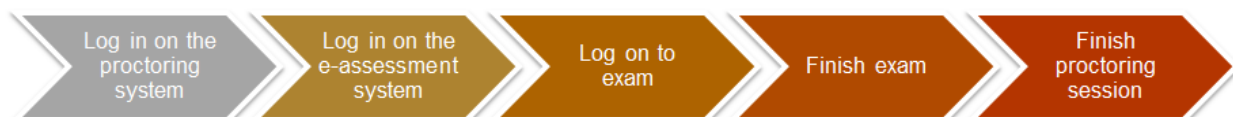
First, students are required to give consent for the fact that video footage of the student will be recorded and stored.

Second, the proctoring system completes all steps through which the student gives access to various computer/tablet functions that the proctoring system needs to begin visual proctoring. In particular, these steps include access to (1) sharing screen activities with the proctoring system, (2) sharing webcam video streams with the proctoring system and (3) sharing video streams from the webcam of the tablet or smartphone with the proctoring system. The various streams are then ready to be streamed to central servers of the proctoring system for 'live' monitoring by a proctor when the exam begins.

Third, the proctoring system automatically instructs and leads the test-taker through the steps to show that the room (ceiling, walls, tables, chairs, computer casing etc.) is free of unpermitted materials and cheating possibilities. The test-taker therefore must film and record the entire room before beginning the actual exam. Also, test-takers are instructed to film and record whether they have prohibited ear-pieces in their ears, or extra notes under the keypad, etc.

Fourth, the proctoring system automatically completes the steps to identify the test-taker. The test-taker shows the requested form of ID (usually a national ID card or student ID card) in front of the webcam, and a picture is taken with the webcam. This picture is then stored on the proctoring servers. In some instances, the ID is only checked by the proctor, and ID information is not stored on the proctoring servers.

Figure 6 Flow chart start of proctoring and examination process.
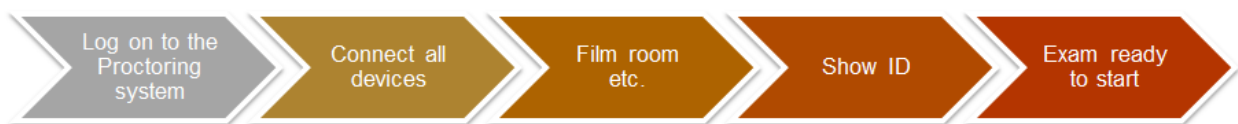
After the initial checks have been completed, the test-taker is ready to begin the actual exam. The test-taker logs in to the e-assessment system with his or her own credentials that are provided via the proctoring system (though not by the proctor) or via email or regular mail.

Once the exam begins, the proctor will monitor the student's desktop, physical environment (for example, sound and video) and conduct. Any unusual behaviour is logged and a response is made in accordance with the specifications provided by the examiner. Typically, with live proctoring, a student first receives a warning so that they may rectify their behaviour. If the behaviour continues, proctors can use their own judgment to gather enough evidence (e.g. video material) to report to the examiner.

During the exam, two-way communication between the test-taker and the proctor is possible, although *only in a very limited way*. First, with ProctorExam, communication is limited because only text chat can be used rather than two-way video/audio. Second, the proctor cannot help the student with logging in to the e-assessment platform, as the proctor does not have the login credentials. Third, the proctor cannot help with any issues related to technical problems of the e-assessment platform or issues related to the

content of the test itself. This limitation in communication implies that a proctor in practice cannot help a test-taker in most cases in which the test-taker encounters a problem. After the test-taker has submitted all answers to the test (or uploaded the answering file), the proctoring session is finished, and the test-taker closes the proctoring window.

Figure 7 Flow chart assessment process.

After 'live' proctoring has taken place, a first review round will be conducted. The first reviewer is in general the reviewer of the proctoring service, but the first review cycle can be performed by the HEI. This review process results in an initial scan of any potential situation that requires specific attention, such as suspicion of fraud or other circumstances. In the timeline of the video material, 'flags' are set.

After this process is completed, the videos are stored and combined into one video with video streams of webcams, phones and screen recording synchronised and compressed. This video can be stored on Amazon cloud storage or on local storage facilities of the HEI, for example. The compressed video can then be streamed to a reviewer, examiner or someone on an exam board for inspection. The reviewer or examiner can inspect the ID verification information or the uploaded exam answer papers (e.g. Word files). The reviewer can also check instances in the video in which flags have been set. To complete the review process in a timely manner, videos can be played with increased speed.

The described processes and systems are in line with the current functionality (2017) of the ProctorExam system. To read more about the functionalities of ProctorExam, visit the website www.proctorexam.com.

To learn more about proctoring vendors and other features offered for proctoring, please refer to this website: http://www.onlineproctoring.eu/en/online-proctoring-providers/.

Some examples of additional features could be automatic facial recognition using biometrics data, voice recognition or keystroke patterns.

Remark 2

Figure 8 Flow chart review process.
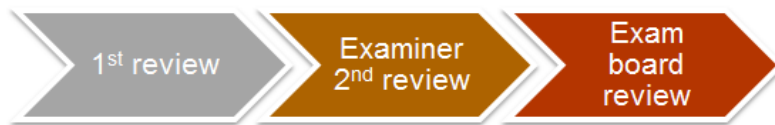
All video material is deleted from the store after a fixed number of weeks and when no suspicion of fraud has been raised for a stream. Limiting storage and access to data is of great importance in view of privacy and data protection regulations.

### 2.3.6 Who undertakes the proctoring and reviewing?

Currently, the question about which party is best able to perform the first review of recorded proctoring sessions is in debate in the OP4RE project.

First, the current proctoring service providers offer pools of remote proctors. These individuals are in principle remote from the HEI for which the proctoring process is conducted, and there is no control over which proctor supervises which exam. Setting agreed and executable procedures for the way these proctors should conduct proctoring is not straightforward. Procedures could be very specific and it requires training and accumulating shared experiences to get procedures workable.

Second, an HEI could also opt to create a local pool of proctors at its own institution. Often, HEIs already have local pools of proctors that conduct regular face-to-face proctoring in physical exam locations. This local HEI proctoring personnel could be trained to use the proctoring system and to perform the initial review. In this case, because of the closer proximity, it is easier to report findings of proctoring sessions to the local examiners and exam boards. Due to the current novelty of online proctoring, using local proctors seems desirable. However, this also implies that it is complex to outsource the online proctoring process to a third party and that the internal organisation must first be convinced that using online proctoring with its own proctoring personnel is preferable and feasible.

All-in-all, given the description of the online proctoring process in this Chapter, Figure 6 shows an overview of the main parts and actors in an online proctoring situation.

Figure 9 Diagram showing main parts and actors in an online proctoring situation.
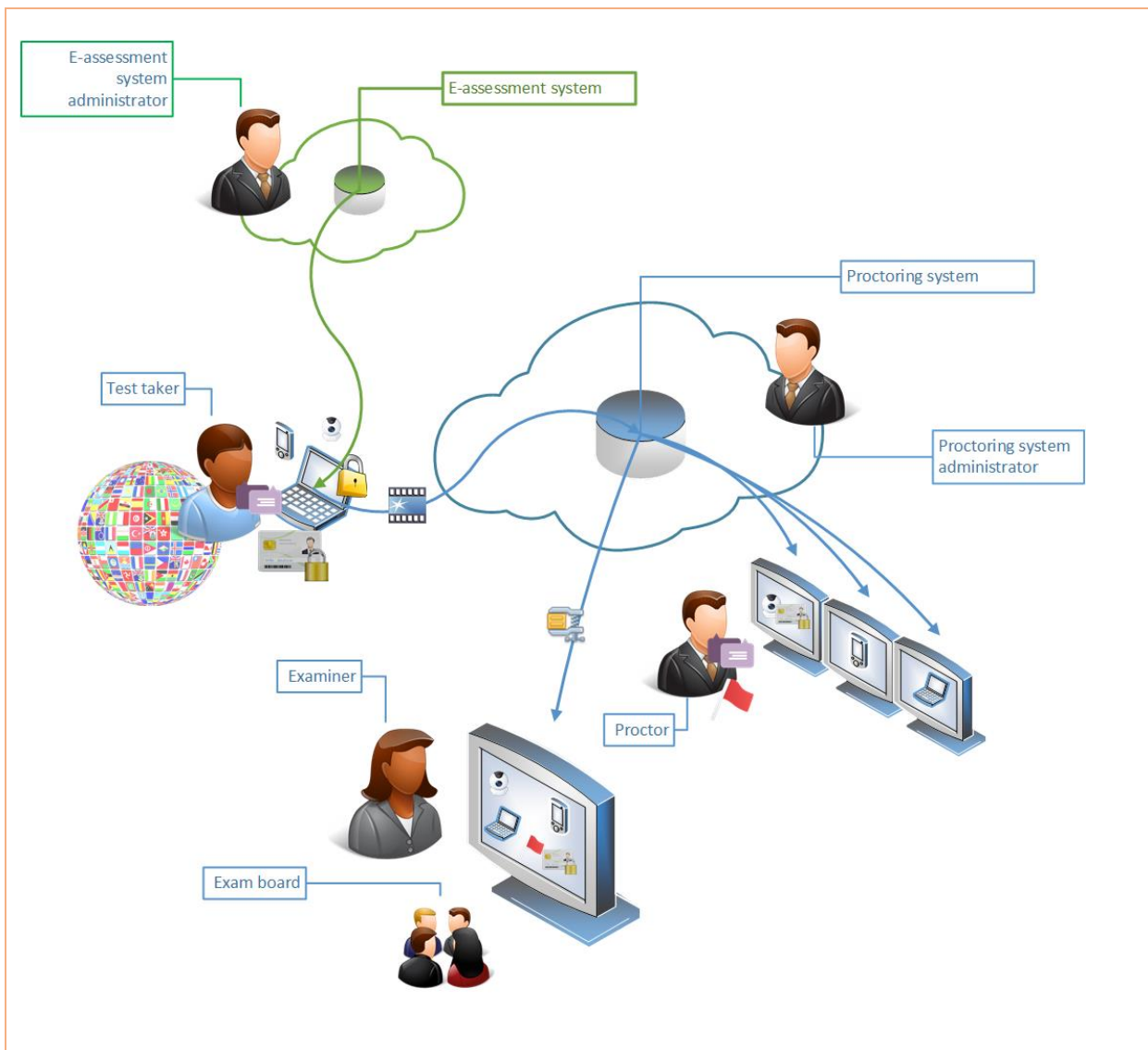
Overall, for successful online proctoring, systems and actors must perform a precisely orchestrated and synchronised process that requires closely aligned procedures and protocols.

Although a considerable amount of technology is already involved, the proctoring process still heavily relies on human effort and expertise for visual inspections and reviews of the test-taking process. This implies that proctoring large cohorts of students in a physical face-to-face location (on-site) is still more effective for residential degree programmes. For example, a ratio of one proctor to 25-50 test-takers is common practice in physical on-site proctoring. In setting up a contract for *Live proctoring*, one proctor to seven to eight students is currently recommended by ProctorExam as the maximum. With *Record and Review* proctoring, which is much more automated, a student can take an exam without a remote proctor present at the time the test is taken. Therefore, any number of students can begin an exam at a given time. For the latter process, proctoring is only executed in the form of reviews of recorded test-taking sessions. This lowers the cost of online proctoring, but it still requires significant effort because all test-takers are reviewed individually.

3   Current Practices and Research

In this chapter, based on desk research and a focus on the experiences of the partners of the OP4RE project, current practices with online remote examination in higher education are described. This is not an exhaustive or wholly systematic description of the state-of-art of online proctoring in higher education. It is rather based on data collected from our own networks and associates. Some notions about the rate of the use of online remote proctoring, other relevant projects and some current implementations and experiences in various countries in both online distance education and campus-based education are described.

3.1   A brief history of online proctoring

Remote examination by means of online proctoring is a field that has been evolving in the last five-seven years[2]. Beginning notably with the US-based firm Kryterion[3], a spin-off of American College Testing (ACT) offering the first methods for online proctoring, the field has expanded rapidly. New service providers have entered the marketplace, new technologies have emerged and new business applications in many fields of education, training and certification have been developed. The OP4RE public website offers an overview of many online proctoring services.

Recent developments have taken place in skills training, certification and licensure for the professional market. Most notably, online proctoring in areas such as computer and programming skills and project management has grown substantially. In addition, online university offerings, such as the Western Governors University[4] (US) and VIVES (Belgium), have incorporated online proctoring to administer secure large-scale remote exams. As of early 2017, the market has been evolving and seems to be in a phase of slow maturation.

---

[2] http://articles.latimes.com/2013/may/01/local/la-me-online-cheating-20130502
[3] https://www.kryteriononline.com/
[4] http://www.wgu.edu/blogpost/innocent-red-flags-caught-by-online-exam-proctors#

3.2 Higher education

Online proctoring is currently used most by educational organisations that offer distance, flexible or online education. In the traditional and typically larger universities, the use of online proctoring is more experimental. This is probably due to the more urgent need for secure, reliable online proctoring in distance, flexible or online education, whereas the reliance on online proctoring in traditional education is less evident. Further research into engagement in online proctoring across European universities is ongoing as discussed below.

There are several possible reasons that the adoption of online proctoring is much slower for traditional universities than for HEIs in the distance education market.

Firstly, traditional HEIs seek to carefully protect their reputations. Institutions of Higher Education are keen to ensure that their names will not be associated with lower standards by being the unintended victim of (un)detected fraud or malpractice in examination procedures or with potential unequal treatment of students in the examination process. It could be said that there is a general conservatism in higher education towards online services in the examination process. There is a fear of reputational damage and damage with respect to accreditation. This makes traditional HEIs reluctant to embrace online proctoring very quickly.

Secondly, institutions of higher education are pressed to fully comply with privacy and data protection legislation. Legislation demands regarding privacy and information security have become increasingly strict within and outside Europe in the recent decade. Institutions of higher education must be cautious when collecting data employing any service providers, data processors and technologies if the HEI cannot oversee the possible consequences that these legislative rules imply. In particular, this includes the required rules of conduct (in detail) and potential high fines that data authorities can issue when there is a failure to comply and a data breach ensues (see Chapter 5 for more details).

Thirdly, institutions of higher education need to become familiar with the concept and required procedures and protocols when utilising online proctoring as described in Chapter 1). It is essential to determine who is responsible for which part of the process in the institution, in terms of execution, governance, administration, finance, legal

issues, exam procedures, etc. Implementing online proctoring in a traditional HEI most likely will also require organisational change and development.

Additionally, but of less interest for the current OP4RE project, is the issue of cost. As budgets become increasingly tighter in Higher Education, introducing new systems with their additional associated costs for training and licensing are under scrutiny. HEIs call for watertight business cases from their business departments. In this respect, little financial relief can be expected if HEIs manage to attract students from the European Economic Region (EER), although this will vary per country. For example, legal regulation in the Netherlands does not allow HEIs to charge students any additional costs for exams, as these costs are supposed to be included in the general higher education admission fee. This is also the case in the Netherlands for international EER students who want to enter the Dutch HE system; however, HEIs in several countries are taking steps to gain experience with online proctoring and study the conditions for its successful use and potential benefits.

For those countries in which the participating institutions in the OP4RE project are located, an overview of the current use of online remote proctoring is provided in sections 3.4 and following, to the end of the chapter.

3.3   The TeSLA project

The OP4RE project exchanges information with the TeSLA project[5]. The TeSLA project is a European funded project scheduled to run from January 2016 to December 2018. The TeSLA project aims to develop an *Adaptive Trust-Based e-Assessment System for Learning*. The TeSLA project goal is to provide an adaptive trust e-assessment system for e-assessment processes in online and blended environments to educational institutions. It will support both continuous and final assessments to improve the trust levels across students, teachers and institutions. One of the main means to achieve this trust-based process is by improving the authentication process of the test-takers by linking personal profile data to assessment system identification processes. The system will be developed in conjunction with quality assurance agencies in education, and through careful consideration of privacy and ethical issues and educational and technological requirements throughout Europe.

---

[5] http://tesla-project.eu/ , https://drive.google.com/file/d/0B-YJl0K9qtsGaVZTNzJsNl9CZG8/edit

Given the innovative action of the project, the current gap in e-assessments and the growing number of institutions interested in offering online education, large-scale pilots will be conducted during the project to evaluate and assure the reliability of the TeSLA system. The TeSLA system could become an integral part of future online proctoring systems and services to support transparent, robust and reliable identification of test takers. Developments of the TeSLA project will be closely monitored by the OP4RE project.

3.4   Practices in France

HEIs are increasingly developing flexibility in their educational offerings by creating online distance education in addition to traditional face-to-face education. Each university is responsible for its own distance learning programme. The situation is quite similar to that in the UK, but an important role is fulfilled by La FIED (Fédération Interuniversitaire de l'Enseignement à Distance) which is one of the OP4RE partners. FIED is an association of 38 higher education institutions involved in online and distance learning, including 35 French universities, or COMUE (Communautés d'universités ou d'établissements, Institutions or University Communities), one national Institution, INTS (National Institute for Blood Transfusion) and two non-French universities, Laval at Québec and Unidistance in Switzerland. FIED is an association of the Ministry of Education and Research but is independent as an emanation of the universities.

Amongst others, FIED represents French distance learning both nationally and internationally, informing the members of innovations in its field and sharing good practices.

3.4.1   The state-of-the-art for online proctoring in France

For almost all French higher education e-learning programmes, students still need to be physically present (on-site) at their host institute or university (or a partner examination facility) to take exams. Since 2015, FIED has been experimenting with online proctoring on a small scale. These experiments (still in progress) are undertaken under the supervision of the Mission for Pedagogy and Digital Technology of the French Ministry of National Education (MiPNES), Higher Education and Research. The goal is to offer authentic tests of the proctoring service ProctorU (see Appendix 1 for more information about this vendor) with currently enrolled students who will remotely take their

examinations from their homes.

The online proctoring experiments have mainly been managed in MOOC (Massive Open Online Course) programmes on the FUN (France Université Numerique) MOOC website (https://www.fun-mooc.fr/), such as by Ecole Centrale de Lille or Paris 2 Assas University. A partnership between FUN MOOC and the US-based proctoring service provider ProctorU (https://www.proctoru.com/) was established for this goal.

3.4.1.1   First experiment: Certificat Informatique & Internet

The University of Caen began two experiments in 2015[6]. The first experiment involved *Live proctoring* of a relatively large number of geographically remote students taking multiple-choice exams administered using an e-assessment system. From January 2016 to June 2016, the experiment involved students voluntarily enrolled in a distance certification of digital skills (C2i Level/Niveau 1: Certificat Informatique & Internet[7]) at the University of Caen.

The main findings of the experiment were primarily related to the practical aspects of the online proctoring process. The first practical experience was related to the limitation in successful test-taking sessions. Several students who were invited to participate did not want to participate after an inspection of the ProctorU information. Some students who agreed to take the test online did not attend the sessions. Finally, eight of the 31 students who had agreed to take the test remotely had technology issues due to hardware problems, low connection speeds or blocked software. The second practical experience was related to the quality of the proctoring itself. A number of situations that should have been noted as suspicious, fraudulent or prohibited behaviour were not registered by the ProctorU proctors. Different expectations regarding the specificity of the proctoring procedures seemed to exist between the examiners and ProctorU. This was an indication that more precisely aligned procedures and the demarcation of responsibilities are needed for the process. A final survey that focused on student

---

[6] More information and details can be found on the website of SUP-Numerique
http://www.sup-numerique.gouv.fr/cid95454/protocole-experimental-telesurveillance-epreuves-universite-caen.html
http://www.sup-numerique.gouv.fr/cid94566/telesurveillance-d-epreuve-une-experimentation-en-formation-a-distance.html
http://www.sup-numerique.gouv.fr/cid100211/premiers-resultats-de-l-experimentation-de-telesurveillance-d-epreuves.html
[7] https://c2i.enseignementsup-recherche.gouv.fr/

experiences showed that students found online remote examinations *attractive* for the following reasons:

- More comfortable due to the absence of noise or other distractions
- Calmer
- Less stressful
- Makes concentration easier

The students found it *unattractive* due to:

- Unstable web speed
- Non-French speaking proctor

3.4.1.2   Second experiment: Health professional programme

The second experiment is currently taking place for the academic year 2016-2017. FIED invites students enrolled in a distance learning health professional programme to complete their exams using online proctoring. This programme is mainly offered to students seeking further professional training. These students both work and attend classes during the programme and choose a distance learning programme for that reason. It is highly likely that students in a professional training course represent the principal type of target group for the OP4RE project. This group of students are most likely to benefit from online remote examinations and hence increase their access to higher education.

Currently, 50 students have each taken between two and five exams of a two-hour duration with *Live proctoring*. Of the students, 91% said they would agree to repeat these types of exams and would advise a friend to do the same.

3.4.2   Conclusion of the experiments thus far

The general finding of FIED at this point is that online proctoring has clear potential to be a broadly applicable service for online education; however, the practicalities involve a number of issues that need much more attention. Relatively simple processes/IT problems become hurdles for candidates who take this type of exam, thus inducing unfairness for students during the examination process.

3.5   Practices in the Netherlands

In the Netherlands, a limited number of institutions are specialised in distance education, including the Open Universiteit of the Netherlands and a few private

Universities of Applied Science (LOI, NCOI). The Open University of the Netherlands is involved in the TeSLA project.

Traditional Dutch universities offer campus-based education, only adding aspects of online education through a blended-approach or specific online programmes; however, institutions are increasingly developing flexibility in their degree programmes by offering distance training in addition to traditional face-to-face education. A few research universities have active policies in designing and delivering online programmes via MOOCs or SPOCs (Small Private Online Courses). These include Delft University of Technology, University of Amsterdam, University Leiden, Utrecht University, Erasmus University and Wageningen University. An online master programme at Wageningen University[8] and an online pre-master programme at the University of Amsterdam are well-known examples. Several Dutch universities and Universities of Applied Science have entered the MOOC arena, in particular via the platforms Coursera, EdX and FutureLearn[9].

3.5.1 Online proctoring

The Netherlands has experienced an increasing demand for online remote examinations in the last three years, mostly because the Netherlands have a Dutch Amsterdam-based company that offers services for online remote examinations (ProctorExam – a partner of the OP4RE project). As a start-up company, they have been heavily involved in the process of raising awareness for online remote examination possibilities in the Netherlands. ProctorExam has offered its system and proctors for several experiments.

In April 2017, a new proctoring facility in Amersfoort, The Netherlands, opened for the sole activity of administering live proctored exams using the ProctorExam system. With a dedicated pool of approximately five to 10 proctoring staff, the live proctoring centre will first focus on providing the European continent with live proctors. The live proctoring centre will be operated by the Dutch 'Association for Exams'.

Furthermore, SURFnet[10] has participated in the online proctoring field in recent years.

---

[8] http://www.wur.nl/en/Education-Programmes/master/Online-Masters-at-Wageningen-University.htm

[9] https://www.mooc-list.com/countries/netherlands

[10]SURFnet is the Dutch association of educational institutions in the Netherlands focussing on boosting the quality of education and research through the support, innovation, development and operation of an advanced, reliable and interconnected ICT infrastructure.

SURFnet has paid particular attention to upscaling safe and trustworthy digital examination procedures and online remote proctoring. With respect to online remote examination, an influential white-paper[11], published by SURFnet, provided an overview of privacy and security issues related to online remote proctoring. The authors of this paper presented an overview of the state of the field at the first meeting of the OP4RE team on October 22nd and 23rd 2016 in Amsterdam[12,13]. This white-paper, in addition to broader interest amongst higher education institutions, clearly indicates the growing interest in the field of secure online examinations and the possibilities therein across The Netherlands.

3.5.2   University of Amsterdam

ProctorExam has worked closely with the University of Amsterdam (UvA) to develop their product and services from 2013 onwards[14]. In particular, the deployment of online proctoring in the UvA online Pre-Master Programme of Information Studies is an exemplar programme[15]. Based on the preliminary findings, they have further developed the product and application area.

With respect to protocols, the UvA has developed a limited set of guidelines with practical information for teachers who are considering using online proctoring[16]. Up to now, most expertise and the capacity to employ online proctoring resided with one officer within the university. This officer was in charge of all communication and practical issues regarding the online proctoring. The officer worked in close collaboration with teachers and e-learning support officers.

These latter experiments were not geared towards collecting experience or data with respect to privacy and security though a light test against privacy and security issues was conducted.

The reports of the UvA provided insights into students' opinions regarding online proctoring[17]. The experiences of both students and teachers were positive according to

---

[11] https://www.surf.nl/en/knowledge-base/2016/white-paper-online-proctoring.html
[12] https://cloud.swivl.com/v/ee5048f14859f5f145cc26fb99ade7ee
[13] https://cloud.swivl.com/v/97092479f18197382e04545765f38efb
[14] https://ictofnwi.wordpress.com/2014/10/13/digitale-tentamens-op-afstand-met-proctoring/
[15] https://www.surfspace.nl/artikel/1662-uva-succesvol-pilot-online-proctoren/
[16] http://starfish.innovatievooronderwijs.nl/information/753/
[17] http://starfish.innovatievooronderwijs.nl/goodpractice/750/

the UvA (Brouwer, Heck, & Smit, 2017).

3.5.3 Delft University of Technology

Delft University of Technology (TU-Delft) is an associate partner of the OP4RE project that shared its experiences during the first transnational meeting of the OP4RE project to improve its practices. In particular, Delft seeks additional information regarding privacy and security related issues.

TU-Delft has been experimenting with online proctoring in their Extension School (online courses with a limited number of participants) and in some cases for campus students. During the central selection tests for prospective students of the Faculty of Aerospace Engineering in 2016, 500 students were proctored online in a record-and-review mode. TU-Delft uses ProctorU as their proctoring platform.

Initially, TU-Delft staff struggled with the robustness and limited user friendliness of the ProctorU system, but it optimised the procedures. Although the Extension School has set up a workflow, no formal protocol for online proctoring has been established yet. It is expected to be developed at the end of 2017. At this point, exam committees are closely involved.

TU-Delft considers online proctoring an extension of its service to on-campus students. For online students, it is considered a logical step; however, as the university is unable to use live proctoring, it is difficult to overcome several practical procedural and technical problems. Without a live proctor present, questions remain as to which actions to take when there are actual suspicions of fraud or when students are unable to begin the proctoring or examination process. The reported problems of TU-Delft appear to be comparable to the experiences and problems that FIED has reported.

3.5.4 Fontys University of Applied Science

Fontys Academy for Creative Industries (Fontys ACI), one of the OP4RE partners, provides campus-based degree programmes in the Netherlands. With respect to remote online examinations four pilots were conducted in 2015 to test both digital examinations using QuestBase as the e-assessment system and to test online proctoring using ProctorExam (using both *Record and Review* and *Live proctoring*).

The first experiment was a digital on-campus exam with approximately 40 students using a Bring Your Own Device (BYOD) approach. Students were required to connect to the internet using wi-fi at the campus. Although the e-assessment system functioned as expected, the wi-fi connection was not stable enough to support connectivity for the number of students. Thus the exam session failed. The second experiment was also an on-campus exam with ProctorExam enabled (Record only). A proctor was physically present during the exam. This experiment had no technical problems. The third experiment was on the exam for the Big Data Marketing course in which approximately 40 students answered 13 open-ended questions. The exam was administered at home with ProctorExam using *Live proctoring*. A small number of students took the exam on campus, mostly due to claims regarding an insufficient capacity or reliability of an internet connection at home. During the exam, the campus internet connection failed completely due to a faulty fibre optic cable, which was a cause for great consternation. The fourth pilot, a small scale re-sit (5 students, remotely located using ProctorExam Record and Review), was executed without a single technical or procedural problem.

Additional pilots are planned within the context of the OP4RE project. If successful, there is a possibility that the DBC-programme could switch completely from pen-and-paper to digital exams (with remote proctoring). Fontys is still undertaking its own investigations into privacy and protocols and bring in their findings in the OP4RE project.

The experiences of Fontys University of Applied Science are mixed. On the one hand, online remote proctoring seems a viable means of conducting online exams. On the other hand, there is still a large number of practical and technical issues that negatively affect exams. Some questions arose including:

- How should extraordinary situations in which technology fails for several students at the same time be addressed?
- Who is responsible for informing the stakeholders?
- What default measures should be in place when the internet fails?
- Should we expect a BYOD exam on campus to be technically faultless?

The conclusion of the Fontys cases are that comparable to FIED and TU-Delft, practical issues in online remote proctoring are eminent and must receive ample attention because the procedures and technologies currently result in too many flaws and failures and backup procedures are not clarified

3.5.5 Erasmus University Rotterdam - Rotterdam School of Management, Leiden University and University of Groningen

Rotterdam School of Management, RSM, ran one pilot with online proctoring on a small scale. The first pilot was based on an ICT exam (using Microsoft Office™-Word, Excel), where students were already familiar with the use of a computer for the exam. The group size was 20 students who used their own devices to answer the test questions administered via an e-assessment system on campus using *Live proctoring*.

The evaluation results showed that the students found using their own devices to be positive because they were familiar with their own computer settings (for the use of Microsoft Office™-PowerPoint, Excel, and Word); however, students had difficulties connecting to the university wireless network.

The Faculty of Medicine at Leiden University (LUMC) is currently conducting a pilot with online proctoring. The pilot is taking place in their medical extension school with online proctoring for a course with 25 students. Candidates who want to enter the extension programme are required to complete an online entrance course which is concluded with a final achievement test. The online proctoring solution that they will use is TestReach[18]. TestReach is both a proctoring solution as well as an e-assessment tool capable of administering exam questions. No evaluation results are available yet. Because these pilots are still in an early phase, no protocols or accreditation forms have been developed for the online proctoring process.

There is one Dutch university that explicitly does not use online proctoring, which is the University of Groningen. Groningen has expressed grave concerns about the risk of students cheating during examinations. It has noted that with written paper-and-pen exams on campus, the risk of cheating may already be high, and with the use of online proctoring, it fears this risk will become even higher. While it acknowledges the benefits of online proctoring, it is not convinced of the trustworthiness of the online proctoring process and current systems as a whole. It prefers to wait for other institutions to take the lead in research and in gaining experience.

---

[18] https://www.testreach.com/

3.5.6 Vrije Universiteit Amsterdam

The Vrije Universiteit Amsterdam (VU), one of the OP4RE partners, has heavily invested in an on-campus digital exam facility in recent years[19]. About 50,000 digital exams are administered annually in this facility. About 30,000 use the e-assessment system Questionmark Perception (QMP). About 10,000 exams use Microsoft™ Word or pdf files as answering sheets as well as professional software such as SPSS, Microsoft™ Excel and Matlab. Combinations of these three forms of exams are also administered. In the exam facility, online proctoring is explicitly prohibited, as the facility uses a separate and secured VLAN and restricts access to any prohibited file sharing or web resource using Windows™ Object Policies.

VUA does acknowledge and make use of several potentially valuable applications for online remote examinations outside of the exam facility, including:

(1) Selection tests for Bachelor and Masters Programmes with *numerus fixus*
(2) Re-sit tests for foreign students staying only a limited time at the institution
(3) Re-sits for students studying abroad for a limited time
(4) Students with disabilities
(5) Foreign students who want to enter VU University Bachelor and Master programmes who lack appropriate certifications for basic skills, such as maths, statistics and English.

These additional applications provide concrete support for the Erasmus project's overarching goal to increase students' access to higher education. In particular, providing foreign students the option to take online remote assessments to gain legibility to enter the University are regarded as an important mechanism to achieve that goal.

Small-scale experiments with online remote proctoring at the VU were conducted in the first two months of 2017 for central selection purposes for two Bachelors programmes. The first experiment involved seven test-takers, and the second experiment involved three test-takers. The *Live proctoring* options of ProctorExam were used.

Good communication with students was identified as an important conditional aspect

---

[19] In the Netherlands, a growing number of research universities have large-scale digital exam facilities: Rijksuniversiteit Groningen, Universiteit van Amsterdam, Delft University of Technology, Vrije Universiteit Amsterdam and Universiteit Utrecht. Other universities are in the planning stages.

for successful online proctoring. In line with the experiences of FIED and others, there is a strong need for eminent clarification and reinforcement of guidelines for students on the exact procedures for online remote examinations. The URLs, times and time zones, the steps, the type of communication, what is (not) allowed during an exam (calculator, notes, pens, phones, watches, clean desks, etc.), the logins and passwords and other information relevant to the exam must be provided to students. In particular, students' first online remote exams can be highly stressful, and clear guidance and coaching is necessary. The VU sent out several emails and phone-calls to the students to make absolutely sure that everything would be technically and procedurally ready at the moment the exams began.

The data obtained from the pre- and post- examination surveys by the VU showed that once the students were able to get the proctoring software up and running, how to use it was clear, which was highly encouraging.

With respect to fraud detection, it was clear from a 'holistic perspective' when reviewing the video footage that fraud did not occur. The software allows for easily tracking the behaviour of the students and determining whether they made *obvious* attempts to find answers to test questions in a fraudulent manner. That behaviour was not detected but any hidden or subtler attempts at potential fraud seemed difficult to detect. The impression of VU staff is that it requires thorough training for proctors to be able to spot subtle fraudulent behaviour.

Further, it was found that some facets of the remote proctoring software need improvement. For example, the live proctors have access to the raw video stream, which has a relatively good image quality; however, reviewing the combined compressed video stream appeared difficult for the examiner, as there was a significant loss of video quality, streams were not completely in sync yet and some compressed streams showed glitches. This led to questions concerning what steps should be taken if video footage (front and back camera, and screen capture) is hampered or of low quality. For example, what should be done if the test-taking process has taken place in a room with too little light and with intermittent captures of video images with a low resolution? Policies and rules of conduct for these cases that are comparable to current policies and rules of conduct for physically proctored exams, should be established in the opinion of the VU.

VU took its first steps in raising awareness at the university regarding privacy and

protocols. Currently, the VU privacy officers, VU Security officers, VU legal officers and other officers are becoming involved. Based on the preliminary discussions, procedures that need to be followed to conduct online remote examinations are being developed to address privacy and security concerns.

Based on VU experience, a diagram was developed for internal communication regarding how online proctoring could become part of the regular university educational processes. This diagram will be worked out in the final intellectual outputs.

Figure 10 Diagram showing phases through which a HEI that wants to implement online proctoring, will likely go through.
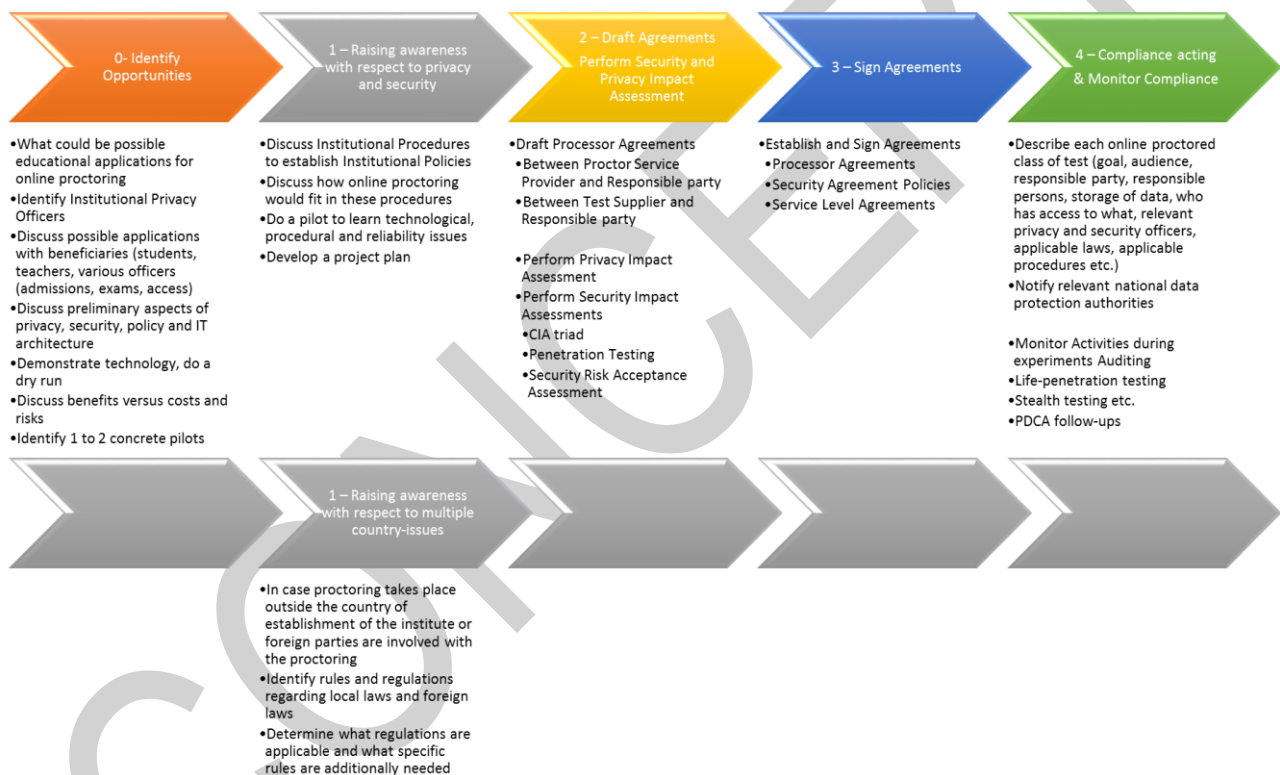
3.5.7 Wageningen University

Wageningen University and Research centre (WUR) offers two distance learning Masters programmes[20]. For these degree programmes, they use ProctorExam *Record and Review*

---

[20] http://www.wur.nl/nl/Onderwijs-Opleidingen/Master/Online-Masters-aan-Wageningen-University.htm

and *Classic*. Students from all over the world participate in these programmes, which is why online proctoring is used since two years.

Previously, Wageningen University used multiple choice questions, and all students were administered the same questions using an e-assessment system; however, Wageningen University was concerned that this might create opportunities to commit fraud using online proctoring. To prevent this type of fraud, the WUR began using essay questions that require the students' own knowledge to answer. No protocols, formal evaluation data or security and privacy data are shared by the WUR yet.

3.6   Practices in the UK

3.6.1   The UK online assessment landscape

UK HEIs have extensively invested in Managed Learning Environment (MLE) systems in the past 15 years to support the online and blended delivery of teaching and learning. In the UK alone, there were over 2,600 HE level online and distance learning courses offered by or on behalf of UK HE and FE (Further Education) institutions in 2010 (source: Higher Education Funding Council for England, HEFCE).

In recent years, the investment in MLEs has led to a growing interest in e-submission and e-assessment opportunities. Based on a survey conducted by the University and Colleges Information Systems Association (UCISA) from 2001 to 2016[21], about half of the 110 responding HEIs are planning to review their e-assessment facilities within the next two years.

Along with the developing interest in tools for e-assessments, there has been increased interest and engagement in the design and delivery of MOOCs since 2011; several British universities are participating in the FutureLearn project led by the Open University as well as with other major international online learning providers, including Coursera (University of Edinburgh) and EdX (University of Oxford and Imperial College London).

How does this widespread online activity contribute to the use of online examinations when students are remote from the HEIs location? E-assessments and online e-submissions are clearly on the agenda for several HEIs. In response to information requests made by the UH Online team to colleagues across the UK engaged with learning

---

[21] https://www.ucisa.ac.uk/publications/tel_survey2016

technology and policy development, there was clear interest and evidence of some initial engagement through their existing MLEs. Thus far (early 2017), there has been little evidence that the use of e-assessment features extends to the use of remote proctoring to support online examinations.

A small number of HEIs are actively exploring and using online remote examinations, which are accessible securely via their own MLEs. This figure is expected to increase rapidly, if the perceived vulnerabilities in the security of remote online examinations can be sufficiently addressed through the outcomes of this OP4RE study and other national studies.

In conclusion, many of the universities across the UK are already actively investing and researching ways to use technology to enhance the many online and distance learning programmes offered. The outcomes from the OP4RE project are expected to ensure that current expectations for systems that offer a secure and private solution to remote assessments and proctoring can be fulfilled.

3.6.2 Examples from the University of Hertfordshire

UH Online is the University of Hertfordshire's centre for online distance learning. Established in 2012 to extend the university's online provision, it now forms part of the Learning and Teaching Innovation Centre (LTIC). UH Online works with schools and departments to develop, market, administer, support and deliver online distance learning courses. They also provide expertise and consultation on best practices for online distance learning.

At the University of Hertfordshire, the online distance learning programme has been offering the BSc Computer Science and other Bachelor and Masters Programmes for over 10 years. In line with technology developments at the University of Hertfordshire, the LTIC have been pioneering and piloting the use of remote online proctoring through the UH Online team.

The use of remote proctoring will allow for greater flexibility in the assessment formats used in online distance learning programmes. For example, it would make it feasible for online distance learning students to take timed practical programming tests under supervised conditions. It is highly likely that students in the current online distance courses of UH represent the principal type of target group for the OP4RE project.

The following excerpts from a journal article co-written by UH Online and School of Computer Science colleagues: Lilley, Meere and Barker (2016) reflects on the initial pilot study that they developed for remote online proctoring. The paper describes the landscape and the decisions made regarding remote proctoring, which is summarised below.

> [..] *This work reports on a small-scale pilot study where a group of 17 online distance learning computer science students from 7 different countries (Egypt, Kenya, Saudi Arabia, Slovakia, Trinidad & Tobago, United Kingdom, Zambia) took part in an online test using remote live invigilation. Some examinees expressed concerns about data security and privacy. Furthermore, some examinees expressed concerns about the extent to which the remote live invigilation process would be intrusive and negatively impact their online assessment experience. Overall, findings from this study suggest that the remote live invigilation did not affect the assessment experience of the examinees in any way, with some examinees reporting that knowing that a live proctor was present gave them 'peace of mind' in case technical problems occurred during the online test. Additionally, examinees suggested that remote live invigilation should be used more widely in online distance learning programmes as a means to enhance credibility.*

The results indicate that remote online proctoring presents a potential solution to the issue of student authentication and the prevention of cheating in online examinations. Furthermore, despite some initial concerns about data protection and the impact that feeling 'watched' might have on their online assessment experience, participants' feedback on the use of the remote proctored examination was positive overall, with some even suggesting that the presence of a proctor might reduce stress if problems arise.

Whilst it may not be possible to ensure that an online examination system is totally secure or fraud-free, it is the view of the authors that remote live invigilation does provide assurance that the person taking the exam is indeed the candidate, and to a greater extent, that they are working alone and unaided.

The University of Hertfordshire is collaborating with its European partners in OP4RE to develop, test and ensure secure and private access for students taking university assessments remotely, with lessons to share with the project's Associate Partners and

others interested in realising the potential of this technology.

3.7   Practices in Germany

Proctoring for remote exams is virtually unknown in Germany. Some universities have already implemented electronic assessments (E-Klausuren), but these exams are on-site exams monitored physically by university staff[22]. In most cases, exams are conducted in the traditional pen-and-paper format.

The Network of Lower Saxony for e-Assessment and e-Exams has conducted a survey that indicates that most universities in Lower Saxony utilise some methods of e-learning[23]; however, if any form of electronic exams has been implemented, it has always been an exam that is conducted on-site with physical proctoring.

Wilhelm Buchner University of Applied Science (WBUAS), one of the OP4RE members, has no experience yet with online examination or online proctoring; however, WBUAS acknowledges the many potential benefits for their distance programmes in terms of accessibility to higher education. From WBUAS' perspective, full compliance with strict German and EU privacy regulations and full trust in cheat deterrence and cheat detection options are of great importance.

To underline the importance of full compliance and fraud deterrence, most recently, the International University of Applied Sciences (IUBH) in Bad Honnef[24], North Rhine-Westphalia (Germany), performed a series of test exams with volunteers from the university. Instead of a specific proctoring software solution, the university utilised a web conferencing system called MegaMeeting[25] to proctor the exam and another remote desktop software solution called Bomgar[26] to monitor the examinee's desktop. IUBH further stipulated a set of rules and required the students to agree to several contracts, agreements and the set of rules. A third-party company was hired to conduct the actual online audiovisual proctoring. Examinees were identified by a photo ID and had to present their room from all angles by moving the camera(s). They were allowed to go to

---

[22] cf. http://www.elearning.uni-mainz.de/e-klausuren/
[23] cf. https://www.openeducationeuropa.eu/sites/default/files/legacy_files/asset/Use-of-eLearning.pdf
[24] http://www.iubh-fernstudium.de/
[25] http://megameeting.com/
[26] https://www.bomgar.com/

the restroom in case of emergencies, but the proctor was required to include a note about the event. After returning to the exam, the student had to present the room again from all angles. The IUBH made an effort to act accordingly with the German Federal Data Protection Act (Bundesdatenschutzgesetz)[27]. The pilot seemed to be successful.

However, the proctoring experiences at the IUBH were also reviewed by the German magazine *Der Spiegel*[28]. In a spoof-attempt to take part in a proctored exam, it turned out that the key issues of proctoring, i.e. security, privacy and exam experience, were far from resolved. Beginning with *privacy*, the test person felt uncomfortable showing the ID card knowing that it would be stored somewhere in the US without any guarantee (with respect to *security*) that it would not be hacked and sold for the highest price. In addition, the test person could not take the proctored exam seriously because all simple fraud trials were successful (cheating was 'easier than ever'). This raised the question of whether an *accreditation* agency would approve a Bachelor course of studies that uses this type of proctored examination as well as which remote examination companies may be used. Further, the undercover participant from *Der Spiegel* criticised the exam proctor for not being fluent in the native language. Hence, for Germany and WBUAS, it is imperative that the quality of the proctoring software solution and its proctoring staff, including privacy and security are two key issue to make online remote examination an acceptable practice.

The German proctoring example could be considered a 'lesson learned'. Due to the grave problems that arose during the first test case at the IUBH and given the fact that no other test cases for proctoring in Germany exist thus far, it is paramount to establish a solid groundwork for operational and legal challenges related to online proctoring for it to become an accepted and common practice in Germany. Key issues that must be faced are data protection and privacy policies, cheating prevention, quality of exam supervision, transparency of progress and data handling and stability of the proctoring solutions. WHBUA expects that the IOs that will be developed within the OP4RE project will investigate these issues and will try to provide best-practices to resolve these issues.

3.8 Practices in Belgium

---

[27] cf. https://www.fernstudium-infos.de/forums/topic/15022-mein-test-der-iubh-online-klausur/
[28] http://www.spiegel.de/lebenundlernen/uni/iubh-fuehrt-on-demand-online-klausuren-ein-so-einfach-war-schummeln-noch-nie-a-1129916.html

VIVES[29] is the first and only institution of Higher Education in Belgium to use online exam proctoring. VIVES has a long tradition of distance learning. About 10% of the students follow a distance learning programme (of a total of approximately 13,000 students).

Students in distance programmes at VIVES can take their exams in the exam centre in Kortrijk or online via proctoring. For the proctoring, VIVES works with ProctorExam, one of the partners of the OP4RE project. It uses ProctorExam *Record and Review*, which means that proctoring runs via a webcam, mobile camera and screen sharing, but there is no live proctor present during the exams. ProctorExam manages the proctoring of the recorded materials within a reasonable period of 4-6 days. Initially, taking proctored exams was only meant for students taking distance learning courses, but currently, an increasing number of students with special circumstances, such as elite athlete students and students with disabilities, take proctored exams.

The introduction of *distance exams* (this is the term VIVES uses) met with resistance, mostly from teachers and staff. Students were however immediately enthusiastic, and this enthusiasm continues to grow. Since November 2015, almost 2,000 proctored exams have been taken, and staff members and teachers are increasingly beginning to 'trust' the distance exam system.

One of the issues VIVES encountered was the identification of the students; VIVES wanted to be 100% sure the correct student was taking the online remote exam. VIVES trusts the procedure in which students must photograph their identity card and themselves at the beginning of an exam. This gives VIVES the opportunity to compare both pictures, which VIVES considers sufficiently trustworthy. In addition to this built-in security, VIVES only provides access to an exam (after logging in to ProctorExam) after a personal identifier and password are given.

Regarding cheating, VIVES believes that there are fewer fraudulent exams with online remote proctoring than with 'classic' exams on site; however, VIVES feels that research should be conducted to provide concrete evidence about occurrences and detection.

The fast and large uptake for online remote examinations according to VIVES is made possible because VIVES has a dedicated e-learning team consisting of two full-time staff

---

[29] https://www.vives.be/

members, including individuals who manage the e-assessment process and the online proctoring process. The OP4RE project is in contact with the responsible officer at WGU to inform the project.

Although Hasselt University, one of the members of the OP4RE project, has some distance learning programmes (such as the Master of Statistics and the Master in Transportation Sciences), remote online proctoring for exams is not yet established. Students from abroad who are enrolled in a distance programme at Hasselt University travel to Belgium to take the exams. In some cases, students can take their exams at partner universities. To lower the travel costs and for organisational reasons, Hasselt University wants to provide students in distance programmes with the opportunity to take the exams at home via online proctoring, hence the participation of UHasselt in the OP4RE project. The experiences of a university that has little experiences with e-assessment and online assessment will help inform the OP4RE project to deliver IOs that are useful for both beginning and more experienced HEI institutions in the field of online proctoring.

3.9   A brief overview of the situation regarding online proctoring in the United States

The rapid growth of online proctoring within VIVES can be compared to other distance or online education based schools, specifically Western Governors University (WGU) in the United States of America (USA), which has recently administered its one millionth online proctored exam. In both universities, dedicated staff manage online proctoring to streamline the process and to follow educational procedures regarding online proctoring. Both universities also have their own customized and detailed rulebooks for the online proctoring process and continuous monitoring. Furthermore, their experience with e-assessments and online assessment systems provides important knowledge and experience that has enabled them to successfully implement online proctoring in their educational practices. The OP4RE project is in contact with the responsible officer at WGU to inform the project.

An important difference between the USA and the EU in general regarding online proctoring are the completely different legal requirements regarding sensitive personal data. In the USA, data protection guidelines are much more permissive than in the EU and the significant growth and impact of Kryterion and ProctorU in the online proctoring market can be explained to a large extent from that perspective.

3.10 Conclusions

Across Europe, some general observations can be made. First, a clear difference exists in the use of online proctoring between HEIs that are more dedicated to distance, flexible or online education and HEIs with a more traditional outlook and focused on face-to-face education. For the latter, moving towards using online proctored exams will require a greater shift in mind-set and opinions regarding organising and appraising online proctoring.

Second, differences exist between countries, in both the rate of use and level of experimentation. This partly depends on national bodies that actively support research and experimentation with online proctoring.

Third, aspects of privacy and security have received only limited attention in the described practices in HEIs. Therefore, the investigation of the OP4RE project into these issues is timely and appropriate.

Fourth, from a practical perspective, a flawless course of conduct for examinations (be it pen-and-paper, digital or remotely proctored) is imperative to ensure the acceptability of any exam. In the experiences described thus far, several problematic issues arose in the proctoring and examination process, hindering quite a number of test-takers in their attempt to actually take an exam. This is very stressful and feeds negative perceptions about online proctoring. It induces unfairness in the test taking process which is almost as grave as cheating. It could be said that the strength of the entire e-assessment and proctoring process *is defined by the weakest link*. It is not possible to rely on the proctoring system or proctoring personnel alone to ensure a flawless process. It requires close cooperation, communication and alignment of procedures and technologies for online remote proctoring to meet the needed standards. Even then technology can fail, and it is important to also have procedures in place in cases of failure. Precisely because

of this, the OP4RE project will develop best practices and rulebooks incorporating issues related to these problematic issues.

Given the complexity of the processes, the number of people and the techniques involved in proctoring, it will take quite some time for each individual HEI to reach an acceptable level of maturity to deploy online proctoring on a large scale according to their individual goals for its introduction.

The goals of the OP4RE project, which include developing Intellectual Outputs that contain rule books, rules of conduct, templates for examinations and proctoring procedures, are timely and appropriate in this sense as well.

4 Security

One of the foci of the OP4RE project is related to the security of the test-taking process, particularly the technical security of the online proctoring process and systems. Security issues involve the extent to which technical problems can be related to flaws in the examination process or potential ways to commit fraud, such as identity fraud (someone taking the test other than the intended candidate) or fraud by providing a different video stream or a different e-assessment stream to the proctor. A failure of the entire e-assessment system and proctoring service could also prevent a flawless examination process, and this could provide test-takers with the opportunity to accuse the HEI of not delivering services as expected, resulting in negative consequences for the institution. These types of fraud can be referred to as 'attacks of the system'.

This chapter explains the key modes of attack that need to be taken into account in the development, maintenance and evaluation of a secure assessment and proctoring environment. These modes of attack include identifying types of potential hostile software attacks on the provider of the proctoring service and/or on the host institution. The key modes of attack presented in 4.1 will be used in security evaluation approaches, which are later described in section 4.2. In the development of the Intellectual Output for OP4RE regarding security, these modes of attack and ways to evaluate security will take the ProctorExam system as an exemplar. This exemplar can then be used by HEIs to compare their own approaches to security testing and security standards.

4.1 Attack vectors

There is a distinction between student-generated attacks and non-student generated attacks. For non-student generated attacks, the most common attack patterns related to this project are:

- Web servers and web application attacks
- Privilege misuse
- Crimeware and ransomware
- Network attacks
  - o Denial of Service (DoS)

- o M-i-M
- o SSL – brute force
- o DNS attacks
- For student-generated attacks, those related to this project are:
  - o Fraud through the use of virtualisation
  - o DoS

The above lists are not meant to be exclusive. The next section describes approaches used to thwart non-student generated attacks.

4.2   Web servers

Several web applications expose information that may seem trivial to a developer or administrator but may often be quite useful to an attacker. An example could be the host institution's web server and module versions being disclosed through the HTTP headers. This may initially seem trivial but for an attacker this may provide enough information to compromise the web server.

4.3   Poor error handling

If an attacker is able to force the web server into producing an error, it is quite common for these error messages to contain information related to the underlying operating system, web server, database or application. This information can then be used either to directly attack the system or to allow other attacks to be directed more accurately. Default error messages produced by a misconfigured web server generally leak information related to the type and version of the web server. This is commonly found in 404 error messages, where the page footer reveals detailed version and web server configuration information, for example.

4.4   Misconfiguration

A web server that is not configured securely can leak large amounts of information and can leave it vulnerable to various attacks. Default web server configurations generally have several insecure settings. By default, Apache is a relatively secure web server; however, it still requires a little tweaking. Default web server configurations allow for creating directory listings, enabling the web server directory structure to be enumerated and additional default files and directories to be browsed.

Furthermore, Apache has a default allow access control methodology, which means that by default, all files within the web server's web space will be accessible through the web

service. It is quite common for sensitive, private or confidential files and information to be stored within the web space of web servers, and by default, these are exposed to the Internet. Unreferenced files and directories, including various web application configuration files, backup and temporary files and unreferenced web applications and administrative interfaces, are commonly available to the Internet due to the lack of access controls implemented on the web server. These unreferenced files can cause a large number of security issues, ranging from enumerating internal system information, discovering insecure configuration files, downloading web application source code and brute-forcing access to administrative web interfaces, leading to serious breaches of confidentiality agreements.

4.5 Network attacks

4.5.1 Man-in-the-middle

On a switched network, ARP spoofing (or ARP cache poisoning) is used to perform man-in-the-middle (MITM) attacks, allowing data to be transferred across the network to be captured, analysed and modified. The *dsniff* package on Linux contains several programs that enable MITM attacks to be carried out, including *arpspoof, dnsspoof, webmitm, dsniff* and *webspy.*

4.5.2 DNS spoofing

When a user requests a website via the web browser, say http://bt.example.com, a DNS request is sent to the configured DNS server, which then sends a DNS reply containing the IP address corresponding to the URL. The web browser then connects to the IP address and downloads the requested web page. Let us assume that an attacker has set up a spoofed version of this website on the attack machine on the local network, which mimics the real website that the user has requested. By performing an ARP spoofing attack, the attacker will see these DNS requests in the network traffic and will be able to send a spoofed DNS reply to the user containing the IP address of the attacker's machine. The user's web browser will then connect to the attacker's machine and download the spoofed web page. The user may then attempt to log in to the web mail application, allowing the attacker to capture the user's authentication credentials and giving the attacker access to the real web mail application. To ensure that the attacker's spoofed DNS reply reaches the user before the actual DNS server's reply, the attacker could use ARP spoofing to perform a denial of service attack by redirecting the DNS server's

replies to a non-existent machine. This would stop any intermittent issues, allowing the attack to be carried out much more reliably.

4.5.3   Brute force

Brute force attacks aim to obtain access to a system by repeated attempts at authentication. Most services that require a username and password and have no facility for account lockout are vulnerable to this type of attack.

Brute force methods are commonly used to crack password files, as this can be done reasonably quickly on a local system. Common tools used in this case are:

- crack - a Unix based programme
- medusa
- Hydra
- Cain and Abel

Attacking network-based services can be more time consuming, as the response time will depend heavily on the network load.

To improve the chances of a successful brute force attack, one part of a two-part authentication is needed. This can be obtained from other network or system vulnerabilities, e.g. finger or null sessions, or by 'dumpster diving' and other intelligence gathering methods.

4.5.4   Denial of service

Denial of Service, or DoS, attacks result in a specific service being made unavailable to legitimate users. These attacks typically have one of three targets:

- The network connection providing access to the service
- The operating system hosting the service
- The application level programme providing the service.

By flooding the network with traffic, less bandwidth is available for use by the service. If enough bandwidth is consumed in this flood, access to the service could effectively deny service to legitimate users. A typical example of this is the 'Smurf' attack, where data is sent to the broadcast address of a network, and the source address of the traffic is specified as that of the target machine. This results in all the systems on the network responding to the supposed source at the same time, thereby generating huge amounts of traffic.

Operating systems have been found to be vulnerable to denial of service attacks. For network-based attacks, this is caused by the operating system's specific implementation of the networking stack. A bug in this stack can cause the entire operating system to hang or reboot when anomalous network traffic is encountered.

Network applications can be vulnerable to denial of service attacks in the same way that operating systems are. If no allowances are made for unexpected traffic or other input, the application could encounter a condition in which it hangs and can no longer provide the service it was designed for. Poor error handling in the code could lead to the same result. If the operating system does not take adequate precautions for extreme conditions, it could be vulnerable to an attack that attempts to exhaust the physical resources available on the system. Several such attacks have been released, which push the CPU to 100 per cent utilisation and thereby deny access to other services.

4.6 Security evaluation approaches

For all possible cybersecurity vulnerabilities, the OP4RE project has three specific aims to accomplish. The first of these is to provide the reader with a report analysing the threats against the assessment platform, which links identified system asset vulnerabilities to methods of exploitation, user capabilities and projected impact should threats be realised. Second, a comparative study/report of the efficacy of online and offline examination security will be produced. Third, a threat assessment on proctoring services and its supporting environment will be conducted. To accomplish these goals, the team will use the TAME methodology (Vidalis, Jones, & Blyth, 2004).

4.7 Threat assessment methodology

For the OP4RE project, the Threat Assessment Model for Electronic Payment Systems (TAME) is the methodology selected to assess the security level of an online proctoring system. TAME is a 3rd Generation threat assessment methodology that is based on an organisational analysis of a customer's business. The ultimate goal of TAME is to help customers decide how much security is necessary and where it should be applied. Figure 8 illustrates the high-level phases of TAME.

Figure 11 Phases of TAME methodology.
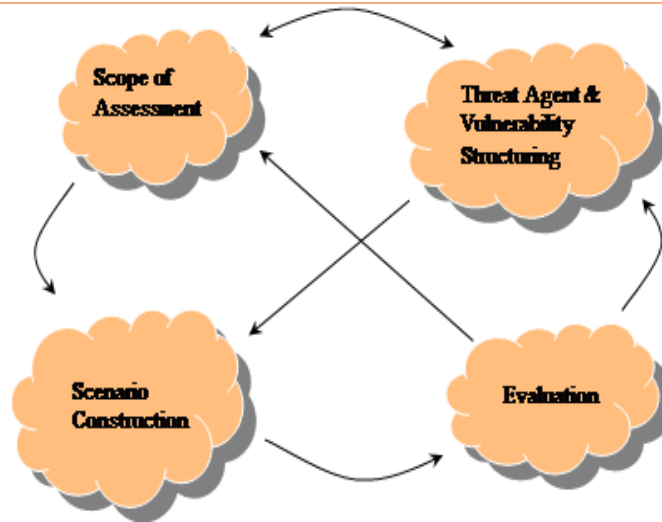
The TAME model will be used for managing the testing process and generating the needed inputs and outputs, for determining the threats and their impact and for generating the final report. The infrastructure penetration test will be based on PTES (Penetration Testing Execution Standard), and the Web App penetration test will be based on OWASP (Open Web Application Security Project).

4.7.1 TAME phase 1

In phase 1, the operational area of the organisation is identified and interrogated. This allows for the different parties that have a stake in the organisation to be identified. The information gathered can be used to identify the boundaries of the system. These boundaries must be protected from the threat agents, which leads to another process. Threat agents that are either active or inactive are identified. These threat agents will target assets. From the previous processes of the methodology, the assessor has the required information to perform asset identification.

4.7.2 TAME phase 2

In phase 2, the threat agents identified in phase 1 are examined, and their attributes are analysed. This allows for preference structuring based on their importance for the organisation. Having acquired enough information to perform vulnerability identification leads to the analysis of their exploitation complexity. The capabilities of the agents are also considered.

4.7.3 TAME phase 3

In phase 3, information gathered from phase 1 and phase 2 can be used to create threat scenarios (identified in phase 1, analysed in phase 2) by exploiting one or more of the vulnerabilities (identified in phase 1, analysed in phase 2). The output of this phase can be considered a second set of security requirements that must be met.

4.7.4 TAME phase 4

In phase 4, the organisation evaluates the results of each process, the impact of each threat identified in phase 3 is calculated and the risk assessment is generated for the information of both the proctoring organisation and the educational institutions.

4.8   Conclusion

In this section, some of the potential security issues that can arise before and during the implementation of online proctoring have been identified. Further, the use of the TAME methodology, a process by which institutions can assess the security risks that are posed by the online proctoring systems that they consider implementing, has been outlined. During the course of the OP4RE project, a trial assessment will be run on the vulnerabilities of online proctoring systems using ProctorExam (version beginning 2017), and the possibilities of eliminating the vulnerabilities for future users and organisations will be discussed.

5 Privacy and data protection

Some of the hurdles for the large-scale implementation of online proctoring are related to privacy, data protection and privacy legislation. It must be emphasised that online proctoring in which all types of ID and video data are recorded and stored is a form of *data collection*. Data collection is a central concept related to data protection and privacy.

Regulations and laws regarding data protection change frequently and may differ from one country to another and even within the EU. It may be difficult to determine as an HEI which specific rules and processes must be in place to ensure the HEI is compliant with regulations, which is the reason that the privacy aspects of online proctoring are one of the foci of the OP4RE project.

5.1 Personal highly-sensitive data

Online proctoring in general requires the storage and the processing of personal data. The personal data stored for online proctoring contains the personal information of a test-taker (for example, the ID card shown and photographed with the webcam) or the examinee's home interior. Camera images and video footage also fall into a separate category under the EU's Data Protection Directive: namely, that of *sensitive* personal data[30]. In particular, camera images can be used to track medical data (e.g. 'wears glasses'), race and ethnicity. This personal data may in principle not be processed unless the law provides specific or general exceptions.

The legislation can be more or less restrictive on these points in different countries. In France, for instance, the national institution for personal data protection and individual

---

[30] Sensitive personal data are:
- Religion or belief (crosses or head coverings)
- Race
- Political affiliation
- Health (videos showing illnesses, wearing glasses, health equipment)
- Sexual life
- Union membership
- Criminal data and personal information on unlawful or objectionable behaviour for which there is a ban.

liberties (CNIL) allows an HEI to store identity information and full video recordings using a webcam, but it does not allow the use or storage of biometric data. Being knowledgeable about these rules and guidelines is of great importance for HEIs to go forward implementing online proctoring. As of 2016, data authorities can issue large fines to institutions that do not comply with these rules.

Yet, despite the unclearly demarcated legal rules that may apply, several aspects related to privacy will likely be the same across EU countries. The EU rules, of which on 25 May 2018 the new General Data Protection Regulation (GDPR) will be implemented, are the strictest in the world. Complying with these rules is a firm (and necessary) first step in being allowed to use online remote examinations. In the next section a general overview of the legal frameworks that may apply will be given rather than a comprehensive review. This approach will be used in the OP4RE project to develop legal case studies that can serve as exemplars for remote online examinations applications in the future for HEIs.

5.2   Basic legal terms, rules and legal bases for collecting proctoring data

First, for data protection, it is important to know who the key actors are and how they are denoted:

- The Concerned person or Data subject (the test-taker providing data)
- The Data Controller (the HEI collecting data)
- The Data Processor (a third party collecting and processing the data on behalf of the Data Controller—with online proctoring this is the online proctoring system provider)
- The Privacy Officer or Data Protection Officer of the HEI (responsible for the data protection issues of the HEI[31])
- The Data Protection Authority (the national authorities to which Responsible parties need to report to in case of, for example, data leaks or complaints by Concerned persons).

The *main rules* that apply to data protection are as follows. These rules are in place to ensure that Responsible parties do not collect unnecessary data:

- Legality, propriety and transparency
- Goal binding
- Data minimisation
- Correctness
- Storage limitation

---

[31] http://tesla-project.eu/gdpr-come-data-protection-officer/

- Integrity and confidentiality > Security

To collect data, *a legal basis* is conditional. The legal basis forms the rationale for data collection and storage by a HEI or Processor.

- *Unambiguous* consent of the Concerned person is needed. The Concerned persons must be given full and clear information regarding the purpose of collecting the data (in view of the Goal Binding rule), their rights with regards to the ownership and correctness of the data and their right to demand deletion of the stored data.
- With respect to collecting the data, the HEI must show that collecting the data is *necessary for one of the following reasons*:
  - for the execution of a contract
  - for compliance with a legal obligation
  - to protect vital interests
  - for the performance of a public task
  - for the purposes of a legitimate interest, unless the privacy interests of the individual outweigh this legitimate interest

5.2.1 Consent

With respect to consent, permission to collect and store data must be given *freely* by the Concerned person; a student must therefore be able to refuse permission without suffering any negative consequences. This can have some far-reaching consequences for online proctoring applications. If students are dependent on their education institution to acquire a diploma, it can be argued that students' permission has not been given freely. After all, if they do not participate in an online proctoring session, their diplomas may be withheld. This implies that the HEI must always offer students the option to take a physically proctored exam at the HEI or without storing data. HEIs must be fully aware of this and may not in any way attach consequences to a refusal of permission for storing proctoring data. As a result, online proctoring cannot be compulsory. The HEI must always offer the student a non-recorded alternative as well. This may imply live proctoring without recording or physical proctoring on-site. No jurisprudence for these issues has been recorded as yet.

HEIs must also ensure that the consent request is as clear as possible and that it indicates *what data* will be processed, for *what purpose*, *who* will be able to *access* or *change* the data, *how long* the data will be stored and *what* will subsequently *be done* with the data. This must be formulated clearly and be stated *in the place* where the student gives permission. It may not be hidden and may not be contained in a privacy statement. In the OP4RE project, examples of consent statements will be developed and be part of the intellectual outputs.

5.2.2   Necessity

With respect to necessity, a Data Controller must be able to provide arguments for the necessity of collecting personal data, even more so in the case of highly sensitive data. A Data Controller must therefore document the arguments for necessity based on one or more of the five arguments for necessity as listed above. For specific classes of online remote proctoring, this will be explained in more detail in the final Intellectual Output that then can be used as exemplars by other HEIs.

5.2.3   Rights of Concerned individuals

When data has been collected, Concerned individuals have some specific rights with respect to that data. Concerned individuals have right to:

● Information and access (they may at any time see what data is stored)
● Rectification (they may at any time ask for correction of possible faulty data)
● Restrict processing
● Object (they may oppose collected data)
● Erasure (they may ask for deletion of all data related to them)
● Data portability (they may have the data in a portable manner)
These terms and accompanying procedures will be worked-out in detail in the final Intellectual Outputs.

5.3   Rules of Conduct (access)

This section offers an initial small set of guidelines institutions, proctors, examiners and exam boards with regards to rules of conduct when working with a proctoring system and accessing information of that system. These guidelines will become part of the final Intellectual Outputs of the OP4RE project.

Identification

● Ask Concerned persons to cover any social security number and other identification numbers from their ID if they are not necessary for the purpose of identification
Viewing video footage

● Do not download video footage to a personal computer, USB stick or other unsafe storage
● Do not view video footage in such a manner that others can see this footage
    ● Do not view video footage in a public space
    ● Do not view video footage in such a way that other employees of the institution can see the footage

Access to proctoring system and data

- Maintain a full list of superusers (administators of online proctoring system) proctors, teachers and examiners who may access the proctoring system
- Log access-data of users accessing the proctoring system
- Do not share or store any passwords that enable access to the proctoring system
- Do not leave the computer unattended when working inside the proctoring system dashboard;
- Have an automatic log-out procedure in place when working within the proctoring system dashboard;
- Warn the Security Operations Centre of your institution if you find someone may have gained unauthorised access to the Proctoring System Dashboard

5.4   Proportionality and granularity

In principle, the bullet list in section 5.2 for *the rules* and *legal basis* should be considered for each separate form of online proctoring on a case-to-case basis. In this respect, proportionality also plays a role. As described by SURFnet (Sietses, 2016), does the end justify the means? At the most granular level, considerations could be required for each separate exam, which could lead to an unworkable situation; however, it is anticipated that in the OP4RE project, a set of most likely classes of cases for online proctoring can be described. For each of these classes, the rules and legal bases will be described in the Intellectual Outputs of the OP4RE project, which all HEIs in the EU can use as a template.

5.5   Transnational laws and regulations

It is not only the EU laws which need to be considered when dealing with privacy compliance; the local laws and regulations within each country can be even stricter or impose additional requirements. Here is an example of the complex cases which have already arisen within the OP4RE project:

> *The University X, located within the Netherlands, offers an online proctored exam for a Russian examinee (and the examination is also in Russia). The Russian law in general forbids the storing of personal data outside of Russia; the Dutch law does not. To perform the online proctored examination, X needs to store the personal data in Russia[32]; however, it is not clear whether the Russian government or legal*

---

[32] In reality, it is likely to be even more complex for Russian law; personal data may be stored in a different country but a copy must be stored on Russian soil.

officers can file charges against X if X does not comply with these rules. The exam poses an unknown risk for University X. The privacy officer of X advises against online proctoring for Russian candidates.

In such a case, all local laws apply in this transnational situation, and the Data Controller (University X) must comply with each of these jurisdictional rules. Thus, one unsatisfying solution from the example could be that X cannot offer online remote proctored exams with the storage of video footage in order to avoid the legal problems completely.

The example illustrates that in principle, for all relevant countries in the world, the legal position should first be evaluated. When the Data Controller's privacy officer has concerns about their responsibility, s/he can direct that the advice of a legal expert who specialises in and has full knowledge of the local data protection laws is needed, to provide a full interpretation of the specific rules, legal basis and rules of conduct for that country[33]. This would result in a consideration and comparison of the laws of roughly 194 countries/states (18721 combinations).

Within the OP4RE project, discussions have taken place to determine how to deal with this situation. One of the options is to involve the Associate Partners to use the combined network of legal officers to study this issue and to install a central knowledge repository. Also, a separate assignment is considered to be issued to Professor Arno Lodders of the VU. Prof. Arno Lodders is Professor of Internet Governance and Regulation, Head of Department of Transnational Legal Studies. He has proposed using his network of internet regulation experts to do some groundwork for this.

5.6   Risk assessment and risk acceptance

---

[33] This implies that general available information is insufficient. See sources general available sources such as:
- DLA Piper https://www.dlapiperdataprotection.com/
- Thomson Reuters Practical Law http://uk.practicallaw.com/2-502-1510?qaq=W_q2&qaid=3-502-4080&qaid=2-502-2227#
- "The Long-Arm of Data Protection and Data Production Laws" https://iapp.org/news/a/the-long-arm-of-data-protection-and-data-production-laws/
- "Data Protection Global Guide" http://uk.practicallaw.com/resources/global-guides/dataprotection-guide
- "Global Data Protection Q&A" http://iclg.com/practice-areas/data-protection/data-protection-2016

In summary the partners are not yet able to assure that online proctoring will be a risk-free endeavour from a legal point of view. HEIs should be aware that a number of risks are always involved and that processes of risk acceptance come into play. In the OP4RE project, based on prior experience and practice and knowledge gathered related to Data Classification, Privacy Impact Assessments, Security Impact Assessment, Security testing, Processor Agreements, Audit procedures and potential detected situations of fraud, the OP4RE project aims to deliver relevant and effective Intellectual Outputs. This will include examples of those assessments that can form an acceptable basis for HEI Security and Privacy Officers to inform and guide the various stakeholders through the identified risks and impacts with guidance about how to approach the anticipated risks.

6 Comparing Online and Offline Examinations - A Fraud and Cheating Perspective

6.1 Overview of online invigilation and proctoring

An important aspect of online proctoring is the remaining question of whether online proctoring is as secure a process as - or possibly more appropriately, 'not less secure than' - current physical on-site proctoring procedures and processes.

For physically proctored exams, in many institutions, detailed procedures and regulations regarding proctoring are established (see Appendix 2 in Section 9). Yet, despite the long tradition of face-to-face proctoring, academic misconduct still occurs. Students use both traditional and more technologically advanced means to cheat.

In a recent ten-day long examination period at a UK university, there were 14,000 individual occasions of examinations being taken, and in total, just five or six students were reported as potentially displaying suspicious behaviour (approximately 0.00043%). In the OP4RE project, more of these practical incidences will be gathered by local academic conduct officers and exam boards.

While academic misconduct as a concept is fairly well represented in professional and scientific literature, it seems that the use of (remote) invigilation in (online) exams and empirical findings regarding percentages of cheating in the UK and other countries is not well covered; in order for the OP4RE project to elaborate on this issue, an overview of collated research papers was conducted to provide a perspective of cheating in the examination procedure.

6.2 Literature overview of collated papers

A preliminary literature search investigated the use of online proctoring/invigilation in comparison with existing approaches to administering examinations. The outcomes of the review indicate that there is some equivocation about the incidence of cheating in the different approaches to assessments. For example, Harmon and Lambrinos (2008) found that students cheated more in un-proctored online tests than proctored tests, whilst Hollister and Berenson (2009) found no evidence of a difference in the incidence

of cheating between remote and face-to-face test contexts. Similarly, Ladyshewsky (2015) found that there was not a greater incidence of cheating in online tests when compared with traditional classroom-based pencil and paper tests.

Additional theoretical work has been conducted to identify risks associated with online tests. Ullah, Xiao and Barker (2016) undertook a piece of longitudinal research into the different types of fraudulent behaviour that students might use to cheat in online examinations. Types they distinguished included test-takers impersonated by intruders, examiners impersonated by test-takers, credential sharing, abetting or desktop sharing. There are elements of the paper's classification that are to be refined but it provides an indication of the potential value of a classification system. Research conducted into typologies and risks for this project would also likely be valuable contributions to classification efforts.

This area of research is as susceptible to problems in adopting a technical focus as other general research in educational technology. Curran et al. (2011) provided an account of the ways that different technologies were used to cheat, although it could be argued that advances in technology will materially change the threats posed. Thus, a classification system might consider the ease of execution of a given approach to cheating in an online test, and new technology might increase the ease with which that threat could be applied (even if it does not change its impact/severity). Hence, the classifications of threats must be sufficiently abstracted from their implementations.

King et al. (2009) presented an analysis of cheating in terms of the fraud triangle (Connolly, Lentz & Morrison, 2006; Ramos, 2003). Reproduced in Figure 9 below, the fraud triangle is comprised of *incentive*, *opportunity* and *attitude*. Without the presence of proctoring/invigilation, either in classroom exam environments or online exam environments, the likelihood of cheating increases. In terms of an online examination, this can be explained by the following reasons:

- Test-takers are under pressure to perform (incentive),
- Test-takers have unfettered access to a range of sources of support (opportunity)
- Test-takers may feel that other test-takers are behaving in the same way as they are (rationalization or attitude).

Figure 12 The fraud triangle based on Connolly, Lentz & Morrison (2006).
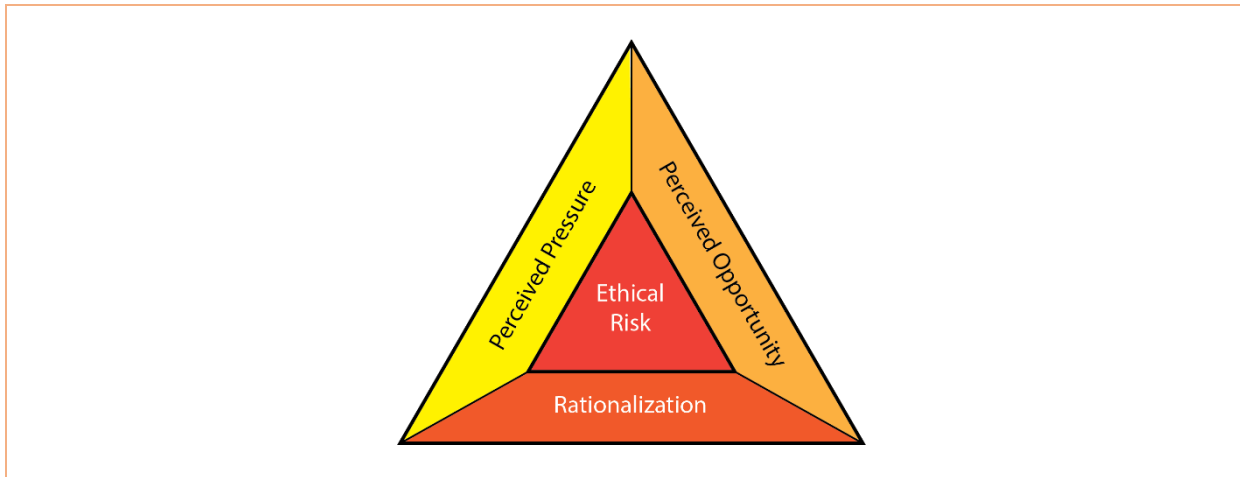
It is important to note that invigilation is not the only mitigating factor in counteracting cheating; test design can also be a mitigating factor (Ladyshewsky, 2015). For the latter, an example solution would include designing tests with scrambled questions or questions pertaining to students' specific previous individual work, a point recommended by Ullah et al (2016).

Considering the fraud triangle, online proctoring can most effectively influence the *opportunity* side.

6.3   Conclusion

Conole and Oliver (2007) outlined that the two main barriers to summative online assessments are: knowing if a student is 'who they say they are' and 'whether their work is their own'. There is no guarantee that traditional paper-based exams taken in invigilated exam halls (regardless of how the assessment is designed) are free from academic misconduct and the same is true for online remote examinations.

Proctoring/invigilation, including online proctoring, will never be a risk-free endeavour from a fraud point of view. HEIs should be aware that risks may always be involved and that the processes of risk acceptance come into play. Through experiments and further desk research, the OP4RE project aims to deliver relevant and effective Intellectual Outputs to provide HEIs with relevant information on which to base their decisions.

7 Regulations and accreditation

An important consideration of the OP4RE project is in which ways online proctoring can assist in improving access to Higher Education. It is expected that online proctoring will be included in future quality assurance regulations. In this chapter, an overview will be provided of the current accreditation regulations and the presence (or absence) of these specific rules.

7.1 European quality control and accreditation

7.1.1 ENQA: European Association for Quality Assurance in Higher Education[34]

Online proctoring and online learning are not included in the standards and guidelines for quality assurance in the European Higher Education Area (ESG). It does mention the importance of respecting and attending to the diversity of students and their needs, enabling flexible learning paths and the encouragement of a sense of autonomy for every learner. These are all points in which online proctoring can play a role. It also emphasises importantly that Assessors (or examiners) must be familiar with existing testing and examination methods. The NVAO, the Dutch-Flemish accreditation organisation, says that the accreditation of MOOCs will not be included in the future; however, it does use the National Qualification Framework from ESG to determine whether the learning outcomes of MOOCs are of good quality.

7.1.2 E-Xcellence: The European Quality Benchmark for Online, Open and Flexible Education[35]

The E-Xcellence report provides an overview of ways to assure the quality of an online course (e.g. open learning, distance learning, online learning, open accessibility, multimedia support and learning communities). It states that an online assessment should include the following aspects:

> *'For assessments that are essentially conventional in format, e.g. essays, but are submitted online, security in transit between student and marker, quality of the marking tools and detection of plagiarism are technical aspects that should be implemented and monitored'*

---

[34] http://www.enqa.eu/wp-content/uploads/2015/11/ESG_2015.pdf
http://www.enqa.eu/
[35] http://e-xcellencelabel.eadtu.eu/

(page 110).

More specifically, the recommendations include (page 111):

- The assessment method is appropriate to the programme and topic
- Learners are informed about the conditions and outcomes of the assessment
- Data protection and privacy procedures are in place
- Feedback is relevant, contains appropriate depth and is timely
- Progress details are available to the individual involved

7.2   United Kingdom QAA: The Quality Assurance Agency for Higher Education[36]

This organisation utilises a broad range of accreditation tools that ensure quality within an educational institution. There are no specific tools that refer to online education or online proctoring. There is a potential for adapting the current policy to the future needs of students, such as online education, and the need to share experiences and knowledge between educational institutions is discussed[37]:

> *'Our assessment of the UK Quality Code has not identified barriers to innovation and to developing new approaches to teaching, such as providing online courses, or night-time learning and blending teaching with more practical aspects of learning'. An Effective Regulatory Framework for Higher Education, Competition & Markets Authority* (March 2015, page 6).

7.3   Belgium - The Netherlands

7.3.1   NVAO: Nederlands-Vlaamse Accreditatieorganisatie

7.3.1.1   MOOCs and online learning in higher education (2014)

The NVAO recently reported on the use of MOOCs in higher education[38]. In the future, it is not expected that MOOCs will be a subject for accreditation; however, it is believed

---

[36] http://www.qaa.ac.uk/assuring-standards-and-quality/the-quality-code/qualifications

[37] http://www.qaa.ac.uk/en/Publications/Documents/QAA-Response-to-Quality-Assessment-Review-15.pdf

[38]

https://www.nvao.net/system/files/pdf/NVAO%20MOOCs%20and%20Online%20HE%20A%20Survey%202014.pdf

that the parties concerned may in time develop a shared view of how to create a 'good' MOOC.

When a MOOC offers the opportunity to gain credits, the NVAO presents the following questions (page 6 of the report):

(a) What does the certificate state? What is its status?

(b) How do you know that the person whose name is on the certificate is the person who took the relevant exams?

(c) How do you know that the holder of the certificate did not receive assistance on the exams?

For the latter question, online proctoring, either live using a webcam or on the basis of a full recording, could provide justification. This is of course only viable if the assessment for the MOOC required the student to take an exam; many MOOCs require assessment by submission of pieces of coursework, which are more difficult to check for fraudulent behaviour.

Another point of interest for the accreditation of online proctoring could be the distinction between internal and external quality assurance. Internal quality assurance refers to the content of the examination in relation to the entire programme of the faculty/institution. External quality assurance refers to how the examination meets the standards of other faculty examination programmes in the same country or even worldwide.

7.3.1.2   NVAO's accreditation of online education (2015)

The NVAO clearly states that there should be no separate accreditation for online education but that it should be part of the programme/institute[39].

For the accreditation of online education, this report proposes two approaches. The first is an approach on an institutional level, where the focus will be on policy, teaching and learning. The second concentrates on a programme level, where the focus is on performance and the learning outcomes. When online proctoring is the focus, it makes sense to establish policies for how to use it and when, and at the programme level, for

---

[39]https://www.nvao.net/system/files/documenten/Bollaert%20NVAO%27s%20accreditation%20of%20online%20education%20Sept%202015.pptx_0.pdf

how it meets the learning outcomes.

The NVAO also describes when to reward credits in different scenarios:

Scenarios	
Credit recognition	Expertise panel; learning outcomes (A MOOC certificate)
Imported e-learning	Expertise panel; assessment and learning outcomes (who assesses?)
E-learning module	Expertise panel
E-learning programme	Expertise panel, assessment and learning outcomes

MOOC-based college credits[40] can be divided into three levels: single course credit, credit for a sequence of courses and fully fledged online degrees.

7.4   Conclusion

European accreditation agencies are poised to provide both online examinations and MOOCs with official status. An important takeaway from this section is that the accreditation agencies clearly state that eventual official status must be on the condition that the online examinations are just as secure as their offline counterparts. This means that before there can be a broad acceptance of online courses in which online achievement test are deployed as means of final measurement of achievement, there is a strong need for evidence concerning the security and fraud deterrence of online proctoring; however, it is clear from the information provided by the accreditation agencies that due to the broad use of these innovative technologies in educational environments, they are expected to be implemented and accredited in the future.

It is expected that the OP4RE project will be able to deliver both theoretical and empirical findings to speed up the process acceptance of online proctoring technologies within accredited and not-accredited education.

---

[40] https://www.class-central.com/report/mooc-trends-credit-credentials-degrees/

8   Appendix 1 - ProctorU

8.1   Uses of ProctorU in France and Europe

ProctorU (https://www.proctoru.com/) is a US-based company founded in 2008 and one of the most well-known proctoring services in Europe and the USA. To date, the company has supervised more than two million reviews in 129 countries[41]. In France, ProctorU has only previously been used for the University of Caen's experiments in MOOC certifications but not for diplomas.

Today, ProctorU has supervised roughly 20,000 exams in Europe (estimation in 2016). The breakdown of assessments is in two primary categories: education and professional/corporate. ProctorU currently has a rough breakdown of 85% exams in education and 15% in professional/corporate. The type of training completed using ProctorU' s services are typically in Human Resources, Pre-Employment, Associations, Fitness, Food Safety, IT, Healthcare, General Business and Project Management.

The development prospects in France and Europe are a mixture of education and corporate prospects through customer engagement, trade shows and referrals.

For ProctorU, one obstacle to market development is the slow decision process of European academic institutions (compared with other regions); this is generally due to bureaucratic procurement processes and six-month exam cycles. ProctorU identifies less commitment to online learning (and lifelong learning) in European countries than in other regions due to technical hurdles (computers and connections). ProctorU also stated that some institutions attempt to replicate a physical proctoring experience for online proctoring, though it is of the opinion that this replication is not suitable for computer-based learning and assessments. Finally, according to ProctorU, the lack of an 'online ECTS (European Credit Transfer and Accumulation System)' market that would allow students to take online courses and obtain ECTS credits towards their diplomas is

---

[41] http://www.bizjournals.com/birmingham/news/2016/04/20/proctoru-forms-two-new-partnerships-amid-huge.html

another obstacle.

9 Appendix 2 - Review of the typical security surrounding the pre-test and assessment phases in a campus-based assessment environment

9.1 Introduction

The Hertfordshire project team interviewed an Assistant Registrar (Exams and Awards) and the Examinations Officer, who were responsible for the security of assessments. In particular, assessments taken under controlled examination conditions in a campus-based, face-to-face environment were considered. This would normally include timed, previously unseen examinations taken in silence and supervised by a team of independent invigilators. The issue of the secure pre-exam environment was considered as well as the regulations for the conduct of examinations. Examples of close attention to detail to provide a highly secure environment for campus-based, face-to-face examinations from the pre-exam preparation onwards are evidenced through the sections below. Overall, the examples illustrate a challenge to the OP4RE project to demonstrate that the security of the remote online proctored environment and the conduct of the assessments are not breached by fraudulent activities.

9.1.1 The pre-exam preparation and regulations for the secure setting, checking and printing of on-campus, face-to-face examinations.

The course team that prepares the assessment for a timed examination designs, writes and moderates the paper electronically on the University's Document Management System. The paper resides on a File Exchange where a limited group of staff are permitted access to each paper, and the embryonic developing question paper is not shared by email. An electronic audit trail can identify those who open the document while it is being compiled and checked. The final moderated paper is sent via a secure online link to a 'locked down' printer with access authorised to a small number of Reprographic staff in a secure area. The printed papers are then placed in sealed, tamper-proof containers and transported to a secure office. The paper is handed to the invigilator from a tamper-proof pack, which is opened in the presence of the students taking the exam.

9.1.2 Guidelines for the secure conduct of a face-to-face (f2f) examinations

This section provides a summary of the guidelines for the secure conduct of a summative assessment, followed by a table that summarises the areas for vigilance and common ways to counteract suspicious of fraudulent behaviour.

I. All students must sign the attendance register upon entry to the exam room.

II. Seating plans will vary from one exam to another and from one room to another so it is more difficult for students to predict where they will be seated.

III. Invigilators pre-check all the desks for notes.

IV. Student photo ID cards, which show the student without headgear, are checked individually.

V. No hats /caps/ headphones can be worn in the exam rooms.

VI. If there is doubt about students' IDs, they will be asked to confirm their dates of birth and their addresses.

VII. Students may not share dictionaries; these are held by the invigilator.

VIII. Calculators cannot be shared.

IX. On the desk, only essential stationery is permitted with a transparent ruler.

X. A clear plastic pencil case is allowed.

XI. No spectacles cases or calculator lids are permitted on the desk.

XII. A clear plastic lidded box is provided for students in which to put their mobile phones, car keys, etc. and this is placed under their chair.

XIII. No sweets allowed, only an un-labelled clear plastic water bottle.

XIV. Toilet breaks are only allowed for exams over two hours.

XV. Students have a reminder before they sit down, that leaving the exam room during exams of less than two hours means they cannot return. Toilet breaks are supervised by a same-sex invigilator.

XVI. Students are invited to go to the toilet to wash off any notes written on their arms, hands, legs etc. before they sit down to avoid giving any cause for challenge.

XVII. The invigilators placed around the room will watch for suspicious behaviour during the exam, e.g. students trying to communicate, looking at their wrists/ cuffs/handkerchiefs, etc. for potential notes/body writing.

Table 9.1 A table for countering the risk factors in the conduct of f2f summative examinations

Risk Areas	Risk Limitation Actions
Person-to-person • Impersonation by another person • Swapping of identities • Reading another student's answers • Sharing with another student • Aided by a friendly invigilator	• Careful ID checks undertaken with university issued photo ID card • No talking permitted once they have signed in and sat down or collusion over answers • No swapping of seats allowed • No sharing of materials • Invigilators normally work in pairs or with a runner outside their door
Accessing unpermitted study materials • Materials hidden on person/clothes – most likely including written on skin, arms, legs, thighs, cuffs, water bottles, calculator lids • Audio notes through headphones, e.g. in hat • Access via e.g. Bluetooth technology to a recording or another person reminding student of key points expected • Prior sight of exam paper	Reminders are issued to students before they sit down to confirm there are no notes that could lead to them being challenged for cheating No headgear/headphones allowed It is near impossible to have prior sight of the exam paper apart from collusion or unlawful access to an academic's password-protected online areas
Location • Notes left in an exam room • Materials hidden in a remote location, such as the toilet	• Students cannot anticipate where they would be seated in a room with other cohorts • Toilets close to exam rooms are checked for hidden materials in situations of suspicious behaviours
Miscellaneous Electronic calculators	• Only 'University issue', non-programmable calculators are allowed

9.1.3 Recommended conduct for PC-based exams taken by students on campus

The same ID regulations are used as for face-to-face examinations. Students may take summative assessments in secure digital assessment rooms where the PCs are locked down to show limited access to programmes/software and, for example, the right click from the mouse is disabled to avoid copying and pasting from another document. There is a full log of each student's session available to subsequently check for fraudulent activity. USB sticks are not permitted. Typically, the password to access the online exam is only given at the beginning of the exam when all students are seated and ready to begin. A tight timescale is used to focus students on completion of the practical exam.

9.2 Conclusion

It is apparent from the typical pre-exam and invigilation procedures outlined above that protecting the summative assessment procedure right through from the point of the assessment being designed to counteracting fraudulent behaviour in an examination hall sets high standards for the setting and invigilation of remote online proctored exams to match.

10 References

Alderson, J. (2016, October 4). The Placebo Effect of Online Proctoring. Retrieved April 21, 2017, from http://www.eduventures.com/2016/10/placebo-effect-online-proctoring/

Brouwer, N., Heck, A., & Smit, G. (2017). Proctoring to improve teaching practice. *MSOR Connections*, *15*(2), 25–33.

Connolly, J., Lentz, P., & Morrison, J. (2006). Using the business fraud triangle to predict academic dishonesty among business students. *Academy of Educational Leadership Journal*, *10*(1), 37.

Conole, G., & Oliver, M. (Eds.). (2006). *Contemporary perspectives in e-learning research: Themes, methods and impact on practice*. London: Routledge Falmer.

Curran, K., Middleton, G., & Doherty, C. (2011). Cheating in exams with technology.

Harmon, O. R., & Lambrinos, J. (2008). Are online exams an invitation to cheat? *The Journal of Economic Education*, *39*(2), 116–125.

Hollister, K. K., & Berenson, M. L. (2009). Proctored versus unproctored online exams: Studying the impact of exam environment on student performance. *Decision Sciences Journal of Innovative Education*, *7*(1), 271–294.

King, C. G., Guyette Jr, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *Journal of Educators Online*, *6*(1), n1.

Ladyshewsky, R. K. (2015). Post-graduate student performance in "supervised in-class" vs. "unsupervised online"multiple choice tests: Implications for cheating and test

security. *Assessment & Evaluation in Higher Education, 40*(7), 883–897.

Lilley, M., Meere, J., & Barker, T. (2016). Remote live invigilation: A pilot study. *Journal of Interactive Media in Education, 2016*(1): 6, 1–5. https://doi.org/10.5334/jime.408

Ramos, M. (2003). Auditor's responsibility for fraud detection. *Journal of Accountancy, 195*(1), 28.

Sietses, L. (2016). *Whitepaper Online proctoring - Vragen en antwoorden bij surveilleren op afstand.* SURFnet. Retrieved from https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2016/whitepaper-online-proctoring_webversie.pdf

Ullah, A., Xiao, H., & Barker, T. (2016). A classification of threats to remote online examinations. In *Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 IEEE 7th Annual* (pp. 1–7). IEEE.

Vidalis, S., Jones, A., & Blyth, A. (2004). Assessing cyber-threats in the information environment. *Network Security, 2004*(11), 10–16.

11 Colofon

This Start Report is part of the Erasmus+ KA2 project 'Online Proctoring for Remote Examination'.

Project Manager

● Vrije Universiteit Amsterdam, NL, Silvester Draaijer
Project Management Group Members

● Universiteit Hasselt, BE, Gwendoline Somers
● Fédération Interuniversitaire de l'Enseignement à Distance (FIED), FR, Pierre Beust
● ProctorExam, NL, Daniel Haven
● University of Hertfordshire, UK, Amanda Jefferies and Karen Barton
● Risbo - Erasmus University, NL, Kris Stabel
● Wilhelm Buchner University of Applied Science, GE, Michael Fuchs
● Fontys University of Applied Science, NL, Michel Van Diesen