GÉANT
Networks • Services • People

Logging and Monitoring for Digital Assessment

Best Practice Document

Produced by the UNINETT-led eCampus Digital Assessments working group

Authors: Ingrid Melve (UNINETT), Magnus Strømdal (UNINETT)

December 2015

Document No: GN4-NA3-T2-UFS149
Version / date: V1.0, 11 November 2015
Original language : Norwegian
Original title: UFS 149 Digital eksamen, logging og overvåkning
Original version / date: V1.0, 11 November 2015
Contact: Magnus Strømdal, Ingrid Melve (UNINETT)

UNINETT bears responsibility for the content of this document. The work has been carried out by the eCampus Digital Assessments working group.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Table of Contents

Table of Figures

Summary

This document contains recommendations for logging and monitoring in connection with digital assessment. It forms part of a series of documents recommending solutions for holding digital assessments.

The recommendations may be summarised as follows:

- **Only log what you need.**
- **Delete logs you don't need after the assessment is done.**
- **Remember to store and archive data safely and securely.**

1 Introduction

This document describes the best practices for logging and monitoring digital assessments, and reviews what may be logged for what purposes. The document also describes the distinction between logging and monitoring in the context of digital assessments.

Best practice documents (BPDs) have been developed to describe recommended solutions for carrying out digital assessment in the universities and colleges sector. The recommended solutions are based on experience from the pilot programmes for digital assessments.

Guidance on laws and official regulations has been taken from the legal report on digital assessment [LegalReport] – referred to as the "Legal Report". This was elaborated by representatives of the University of Agder (UiA), the University of Bergen (UiB), the University of Oslo (UiO), the University of Nordland (UiN), Sør-Trøndelag University College, Trondheim (HiST), the University of Tromsø (UiT), the Arctic University of Norway and the Norwegian University of Science and Technology, Trondheim (NTNU).

The series of Best Practice Documents listed in References are intended as working tools for planning and preparing the holding of digital assessments. The intended readership is the technical staff and advisors responsible for these tasks.

This document does not recommend a particular software solution for holding digital assessments. It simply focuses on the logging and monitoring requirements for digital assessments. Requirements concerning software, servers, virtualisation solutions, firewalls and monitoring solutions follow from the chosen software solution for holding digital assessments.

2 Recommended Process

A short recommended checklist has been drawn up for logging and monitoring. This is organised using the same phases of implementation that were used in [UFS148].

The following list describes the steps that should be taken for logging and monitoring in connection with the completion of a digital assessment. Some of the items in the preparation phase will only need to be done once depending on the choice of implementation solution, other items will have to be done for each assessment period or each time the solution is updated.

Prepare

- Review the logging and monitoring functionality in the implementation solution, infrastructure and clients.
- Categorise the information that is logged.
- Identify what should be monitored and/or logged.
- Carry out a legal assessment of the planned monitoring.
- Set up monitoring and logging.
- Test the monitoring and logging.
- Document the operation of monitoring and logging.
- Document monitoring and logging in connection with cheating.
- Set up data-processing agreements for parties logging information.
- Carry out a risk assessment for logging and monitoring.

Carry out

- Carry out operational logging and monitoring.
- Log and monitor cheating.
- Make active use of logs and assess the level of logging and monitoring.
- Collate information for further use.
- Retrieve information from the client.

Grade

- Collate information for further use in a possible report on cheating.

Finalise

- Delete information in the client.

- Delete information from the client.
- Delete information from the infrastructure.
- Store relevant operational logs (i.e. Implementation log, Experience log).
- Compile a possible report on cheating and send it to the case/archive system; delete information.

Note that these recommendations do not deal with questions concerning the procurement process (i.e. administrative and contractual provisions, the contracting process, tender evaluation or operating and service agreements).

3 Delimiting the topic

The focus of this recommendation is on digital assessments that replace traditional pen-and-paper-based written in-class assessments. It covers assessments both with and without permitted aids.

The document takes into account that a range of solutions are available for holding digital assessments and therefore does not discuss details concerning software, servers or virtualisation solutions. An attempt has been made to cover the use of firewalls and related monitoring solutions.

Digital-assessment client solutions intended to support oral assessments or take-home assessments with digital tools are not dealt with in this recommendation. However, parts of the specifications and tools may also apply to other examination forms than written digital in-class assessments with proctors present in an examination hall.

4 Definitions and terminology

4.1 Logging

By *logging* we mean a process in which information is gathered from systems, processes and routines, and in which the information gathered is stored for a shorter or longer period.

Logging related to digital assessments takes place in many systems and on many levels, which together form a complete logging environment for the chosen assessment solution. Logs may vary widely in format and may stem from many sources. Since logs are gathered from multiple sources, they may contain overlapping information.

Figure 4.1 shows a schematic overview of sources of log information on the examination day. Sources include:

- The assessment system or solution.
- The infrastructure tied to a specific examination Hall (power supply, network, etc.).
- The Clients that students have access to (marked with a “C”).
- The assessment unit tied to the Course (aids, times, etc.).

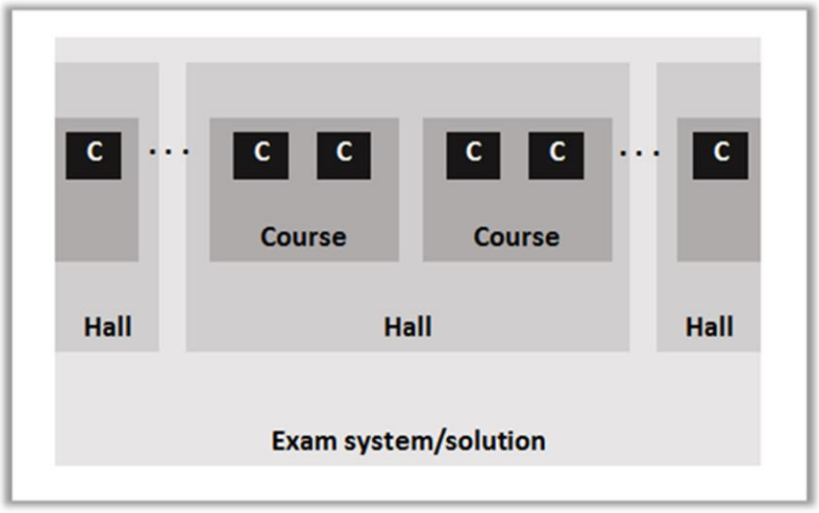

Figure 4.1: Sources of log information on the examination day

What Figure 4.1 shows is that there will be many **Clients** for the same **Course**, there may be several **Courses** in the same **Hall**, and that there may be several **Halls** using the same **Assessment system/solution**.

4.2 Monitoring

By *monitoring,* we mean automatic or manual systems for showing "status information" from systems, processes or procedures. Automatic system monitoring is often based on analysis of information gathered via logging. The main purpose of this status information is to show the progress and health status of systems and processes.

4.3 Logs and reports from external parties

Several implementation solutions are offered as cloud services. The content, design and regulation of agreements with the cloud provider is the subject of [UFS150].

The cloud solutions will produce logs, generate incident reports and trigger alerts of potential cheating. Logs and messages from the cloud service must be handled in the same way as logs produced in local systems.

When cheating is suspected, it may also be relevant to retrieve logs from infrastructure elements (from, for example, UNINETT). Normal procedures for security incidents should be followed in order to safeguard confidentiality and integrity, and to control access to the information.

4.4 Logs for other purposes

In connection with new assessment models, it may be relevant to retrieve logs from assessment solutions for other purposes than before. For example, logs from the assessment solution may be used for learning analysis, both individually and on a group level. In multi-phase assessment models, log analysis may provide the student with individual feedback on his/her progress and the focus of further study.

4.5 What is meant by cheating?

Various forms of cheating have been identified (see [HiHmReport]):

- Use of *aids* that are against the rules.
- *Communication* with others against the rules.
- False *authentication*, where a person other than the student has shaped the contents of the paper or where the student who should be sitting the assessment has been impersonated.

- *Plagiarism*, where contents of the text have been copied from other sources without following the applicable rules.

Digital assessments open up new possibilities in all four areas. The technology also opens up new possibilities for the detailed monitoring of each individual student, and allows for a later review of the paper in order to uncover plagiarism. Most assessment-cheating cases involve plagiarism, which may be due to the fact that plagiarism is comparatively easy to detect in a digital context.

Measures against cheating include:

- Clear regulations and good information.
- Training the proctors, e.g., to move to the back of the examination hall so they can see the screens.
- Reducing physical peeking by other examinees.
- Activities on the device or account and network must be logged and must be available for later review.
- Provision of a virtual workspace (for example, VDI or LockDown Browser (LDB)) for control with the client device.
- An option to check for plagiarism after the paper is handed in.
- Disconnection of the network if no aids are permitted.

4.6 Personal data

Logging and monitoring inevitably entails the processing of personal data. The processing of personal data is regulated by the Personal Data Act and the associated regulation.

Chapter 6 of the Legal Report [LegalReport] reviews the definitions and how the Act and regulation relate to digital assessments. In brief, personal data is defined as follows:

- Personal data includes all information and assessments that can be tied to an individual.
- Sensitive personal data is information that requires extra protection.
- Anonymised personal data is personal data from which names, personal identification numbers and other characteristics directly identifying persons have been removed.
- De-identified personal data is similar to anonymised data, but there exists a key that allows the discovery of an individual author.

5 Logging and Monitoring

In order to assure the quality of digital assessment, the various solutions provide tools for monitoring and logging while holding assessments. As documented in the Legal Report, one is required to document what is logged, the legality of the logging, and to justify the validity of using the log.

If a solution is procured from an external service provider, it must be made clear what the service provider is logging and monitoring. How these logs are to be used and possibly stored must be specified in the data processing agreement drawn up between the institution and the service provider. The data processing agreement must be followed by a risk analysis, assessing whether the service provider is actually capable of fulfilling the requirements in the agreement.

Besides logging within the application solution, logging is required in the surrounding ecosystem of infrastructure and services. Digital assessments will be critically dependent on:

- Routers.
- Switches.
- Domain Name Servers (DNS).
- Wireless base stations.
- Wireless base-station controllers.
- RADIUS.
- eduroam.
- Feide (the Norwegian Federated Identity management for Education).
- The user database.

The list of systems on which the various digital-assessment solutions may depend is not exhaustive. The relevant list for each solution will emerge as a result of the risk-and-vulnerability analysis of the solution.

6 Operational Logging

An institution is always allowed to log activities in its ICT resources for purely technical purposes, providing these logs are only used to uncover technical errors and deficiencies in the solution. This also means that logging is permitted in order to be able to investigate and document what happened if a paper "disappears" in the system or if a candidate failed to hand in or was not allowed to hand in his or her paper (Section 6.3.1 of the Legal Report [LegalReport]).

Operational logging will also have a security aspect, since many different error situations can arise when students use their own device for assessments (BYOD). One example is inadequately configured or misconfigured clients that take down or disturb the wireless network, so that parts of it are experienced as broken or unstable. Institutions must also be prepared for examinees or external performers seeking to sabotage certain digital assessments by e.g. paralysing the wireless network in the examination hall or carrying out denial-of-service attacks (DDOS) against the institution or the infrastructure of the service provider. Motives may vary, but the problem is present and the institution needs to be prepared for such a situation.

In operational logging mainly anonymised and de-identified personal data is used.

Note that logs gathered for operational purposes cannot be used to uncover cheating, because the monitoring and the resulting logs have a different purpose (Section 6.3.1 of the Legal Report).

6.1 Who logs and monitors what?

The institution logs infrastructure:

- Local network components.
- Local power solutions.
- DNS.
- RADIUS.
- Wi-Fi.
- eduroam.
- The user database.

The assessment-service operator logs the server side of the assessment solution:

- Examinee number.
- Assessment unit.
- Information on the assessment paper.
- Attendance.
- The server side of the assessment system.

The examinee's PC logs client data:

- LockDown Browser (LDB).

The NREN (e.g. UNINETT) logs infrastructure:

- Backbone components.
- Traffic volume.
- National-level DNS.
- National-level RADIUS.
- Feide.

6.2 Assessment-paper changelog

The assessment solution will normally log changes or save the entire assessment paper at least every five minutes to minimise the risk of work being lost.

7 Operational Monitoring

Operational monitoring in order to ensure the carrying out of digital assessments includes end-to-end monitoring of all the systems involved, from the examinee's own PC to the assessment system, which may reside with a cloud provider.

In operational monitoring, one mainly deals with anonymised and de-identified personal data.

7.1 Centre of operations

For digital assessments, it may be useful to either set up a separate ICT assessment team or to reinforce an existing centre of operations or helpdesk with new functionality. Staff with such functions must be covered by normal procedures for data access and processing. Local staff must be aware of how to contact upstream providers of networks, power, assessment solutions, etc.

7.2 The use of packet inspection and/or firewalls

Some of the assessment solutions will be provided as cloud services, so we must take into account that solutions may be provided by both domestic and overseas providers. With a cloud-based assessment solution, candidates need reliable Internet access to be able to take the assessment.

The use of Deep Packet Inspection (DPI) and/or firewalls to monitor the data traffic to and from an examination hall will help uncover attempts at cheating and literature searches or Internet lookups. The drawback is that such solutions are often resource expensive and may be experienced as a bottleneck for normal traffic connected to holding assessments.

In a situation where cheating is suspected or one which compromises the digital assessment, an escalation from packet inspection to logging may be needed to preserve evidence.

Packet inspection of Internet traffic in order to uncover cheating involves mainly de-identified personal data.

Note that when there is a suspicion of cheating, the individual will have to be identified and a switch to processing **sensitive** personal data is required.

8 Logging in order to uncover cheating

Logging on the examinee's PC during a digital assessment in order to uncover cheating will store the student's username and activities during the assessment. What is stored by the system will vary from one system to another, but in any case, this involves processing the examinee's personal data. In order to initiate the gathering of logs from examinees' PCs, there has to be a justified interest in monitoring the examinee's activity on the PC during the assessment, and it has to be documented that this interest outweighs the interest in protecting the examinee's privacy.

When logging in order to uncover cheating, mainly de-identified personal data is used.

Note that when suspicion of cheating arises, the individual will have to be identified and a switch to processing **sensitive** personal data is required.

Procedures must be established for the escalation and handling of logs in connection with suspected cheating. In order to preserve evidence, it is important to note the time when the suspicion arose and who it was that suspected the cheating. It must also be noted at what time the investigation of the case in question was concluded and who closed the case. A summary of the number of suspected cases and what triggered the suspicions is useful information for the implementation log and the experience database.

Logs in connection with suspected cheating can quickly reach a large volume, and may thus burden storage systems and archives with large amounts of data. It is important to have good procedures for reducing the volume of the relevant logs afterwards, both in order to conserve storage space and to make the logs of the incident in question more legible. Logs should be deleted as soon as they are no longer needed.

A LockDown Browser (LDB) entails extensive logging of transactions on the examinee's PC in the assessment period. The handling of such logs must be documented with specific procedures for starting, ending and storing them until deletion.

9 Monitoring in order to uncover cheating

Monitoring the examination hall, the assessment solution and the network traffic in order to uncover cheating differs from monitoring for operational purposes. Monitoring in order to uncover cheating has a narrower and more serious purpose, and is often based on procedures internal to the institution. As far as Norway is concerned, for example, there is currently no direct authority in Norwegian law covering monitoring when the purpose is to uncover cheating, when obtaining the consent of the examinee is not feasible. It is only when there is a justified interest in monitoring the examinee's activity during the assessment, and when this interest outweighs the examinee's interest in privacy protection, that such monitoring is permitted.

Whether there is a justified interest in initiating monitoring for the purpose of uncovering cheating, must be assessed, justified and documented by the individual institution for each venue and each assessment.

The grounds for the decision to monitor a particular digital assessment should be announced well before the day of the assessment and any alternatives for examinees who do not want such monitoring should be clear from the announcement. It is not sufficient for examinees to be informed when they arrive at the examination hall that monitoring will take place in order to uncover cheating.

In a monitoring situation, one will escalate from monitoring to logging if situations arise where evidence needs to be preserved or where the situation may have consequences for carrying out the digital assessment.

When monitoring in order to uncover cheating, mainly de-identified personal data is used.

Note that when a suspicion of cheating arises, the individual will have to be identified and a switch to processing **sensitive** personal data is required.

Procedures must be established before escalation takes place in connection with suspected cheating. In order to preserve evidence, it is important to note what time the suspicion arose and who it was that suspected the cheating. It must also be noted at what time the investigation of the suspicion in question was concluded and who closed the case. A summary of the number of suspicions and what triggered them is useful information for the implementation log and experience database.

9.1 Report on cheating

Based on information from logging and monitoring in order to uncover cheating, a report on cheating may be created as described in [UFS148]. The gathering of logs and monitoring data may form part of such a report. We recommend that the collation of data possibly containing sensitive personal data should be done in tools with support for confidentiality, for example, using approved tools for administrative casework. See the Legal Report [LegalReport] for more information on the requirements of such data.

9.2 Visual privacy

Proctors must be able to see what examinees are doing during digital assessments. Proctors should be placed at the back of the hall to facilitate monitoring.

The demand for visual-privacy measures will increase. While paper lies flat, screens stand upright, and individual students may need to magnify text, making it very easy to see from the neighbouring desk. This may lead to unintentional cheating, because it is too easy to read the text on the screen of the neighbouring examinee. This problem should be part of the assessment when planning the use of the examination hall. The biggest problem is with assessments held on desktop computers, which often have large screens (19–24 inches). Visual-privacy measures for screens are described in UFS 145: Physical Infrastructure for Digital Assessment [UFS145].

Solutions include installing screen privacy filters, reducing the capacity of the hall, or mixing examinees from multiple assessments in the same hall, so that neighbours do not take the same assessment. It may be necessary to seat candidates further apart than one usually does in paper-based assessments.

Visually impaired students may be placed at the back of the hall, so that others cannot peek at their screens, which may feature large text.

Peeking at screens and their contents when the examinee wishes to temporarily leave the examination hall, or when the examinee returns, is assumed to be a lesser problem, since the exposure time is short and the examinee is accompanied by a proctor in such cases.

The use of screen locks for examinees temporarily leaving the hall may lead to problems and screen-lock support must be checked in the various implementation solutions. If screen locks cannot be used, they must be deactivated on the devices of examinees, and proctors must be trained in alternative solutions to prevent peeking at empty seats, e.g. draping a newspaper across the screen.

9.3 Plagiarism checks

A growing number of educational institutions are using plagiarism checkers, where the assessment paper and metadata are sent to a central text-similarity server for checking. The service may be an integrated part of the solution for implementation of digital assessments, or it may have been purchased as a general service that is also used in connection with digital assessments. When using

such tools, the institution is transferring personal data in the metadata, along with the assessment paper being checked for cheating, to the service provider (data processing). Text similarity is to be assessed by qualified staff. Note that text identicality is not in itself proof of cheating, as correct quotations in compliance with good citation practice may result in hits.

Note that in cases where cheating is suspected, the examinee will have to be identified and the exam paper switches from containing personal data to containing sensitive personal data.

10 Documentation and Implementation Log for each Assessment

The infrastructure, client and implementation-solution set-up for each individual assessment should be documented, along with logs from the implementation and any incidents that may have occurred during the assessment.

Up to one year may pass between the assessment and the final grading. Over this span of time, it is likely that the client set-up and the implementation solution have been updated and improved. It will therefore be important to have gathered documentation from each individual assessment in anticipation of complaints about how the assessment was held. Logs have limited archival value after the exam assessment becomes final: logs lacking archival value should be deleted at that point.

Digital assessments provide various built-in solutions for monitoring the holding of the assessment. How the monitoring is carried out, and what is being monitored/logged, must be documented and communicated to the examinees.

For the sake of security and quality, it is recommended that procedures for the implementation and incident logs from each completed assessment be established. These logs may be useful for uncovering weaknesses and security problems with the chosen infrastructure, client and application solution for digital assessments.

The Legal Report lists the following items for an incident log:

- What happened?
- Where did it happen?
- When did it happen?
- Who is involved?
- Who has been alerted?
- Possible reason for the incident.

11 Deletion of logs

Procedures for securing and deleting logs must form part of the tidying-up after assessments. All logs containing personal data and lacking archival value should be deleted. Logs with personal data that do have archival value should be secured in such a way that they cannot go missing or be misused at a later time.

The following procedures are recommended:

- The assessment software and attendant logs should be deleted from BYOD units in order to free up any licenses and minimise possible confusion as to which logs belong to which assessment.
- On institutionally-owned equipment, procedures must ensure that a new assessment will start without old data carried over from the previous assessment. One alternative is to reinstall all the software between each assessment, or to use solutions that delete assessment users and all logs related to these users.
- Assessment-related data should be deleted from the infrastructure. This applies, for example, to assessment users, traffic logs from assessments, network authentication logs that can connect those undergoing assessment with students, any downloaded materials, and generally all data that could cause confusion the next time an assessment is held.
- Logs related to carrying out the assessment are archived.
- Relevant operational logs are archived, for example, for statistical use.
- Incident reports and any reports on cheating are transmitted to the case/archive system; system data on incidents and cheating should be deleted.

References

References to relevant regulations and guides are freely available for download:

[LegalReport] ”Digital vurdering og eksamen, en juridisk vurdering” A collaborative project commissioned by the expert group on digital assessment and exams, Spring 2014, carried out by representatives of UiO, UiB, UiA, HiO, UiT, UiN, NTNU and HiST, Norway.

[HiHmReport] The survey of types of cheating is taken from work done at Hedmark University College, Elverum, Norway

UNINETT best practice documents are available from https://www.uninett.no/ufs

[UFS112] UFS 112: Recommended Security System for Wireless Networks.

[UFS122] UFS 122: Recommended ICT Security Architecture in the HE Sector.

[UFS127] UFS 127: Guide to Configuring eduroam using a Cisco Wireless Controller.

[UFS145] UFS 145: Physical Infrastructure for Digital Assessment.

[UFS146] UFS 146: Clients for Digital Assessment.

[UFS148] UFS 148: ICT Architecture for Digital Assessment.

[UFS150] UFS 150: Requirements for the Use of Cloud Services.

Glossary

BPD	Best Practice Documentation
BYOD	Bring Your Own Device
CBP	Campus Best Practice
DDOS	Distributed Denial of Service (attack)
DNS	Domain name Server
DPI	Deep Packet Inspection
eduroam	A global service that provides secure roaming connectivity
Feide	The Norwegian Federated Identity management for Education
HiST	Sør-Trøndelag University College, Trondheim
ICT	Information and Communications Technology
LDB	LockDown Browser. If a LDB is used during an online assessment, the candidate is unable to visit other URLs, switch applications, take screenshots, copy questions or print.
NTNU	Norwegian University of Science and Technology, Trondheim, Norway
RADIUS	Remote Authentication Dial-In User Service (server)
UiA	University of Agder, Norway
UiB	University of Bergen, Norway
UiN	University of Nordland, Norway
UiO	University of Oslo, Norway
UiT	University of Tromsø, Norway
VDI	Virtual Desktop Infrastructure
WiFi	Wireless Fidelity; generally any wireless local area network product based on the IEEE 802.11 standards