UNINETT, the Norwegian NREN, in collaboration with Norwegian higher education, has run a project (2015–2016) on digital assessment: eCampus Digital Exams.

The project has established current best practice for digital assessment, publishing this in the form of six GÉANT Campus Best Practice documents.

Best Practice Documents on Digital Assessment

The Six Campus Best Practice documents are:

- **CBP 42: Physical infrastructure for digital assessment**
- **CBP 43: Clients for digital assessment**
- **CBP xx: Integration for digital assessment** (forthcoming)
- **CBP 44: Architecture for digital assessment**
- **CBP 45: Logging and Monitoring of digital assessment**
- **CBP xx: Legal issues regarding use of cloud services** (forthcoming)

Documents that have a CBP number are translated and available in English. The two remaining documents are works in progress and will be translated to English after they are finalised in Norwegian.

CBPs are free, openly available documents available from the GÉANT website (http:services.geant.net/cbp/Knowledge_Base/Pages/Home.aspx)

CBP 42: Physical infrastructure for digital assessment

(UFS 145, Norwegian version)

In CBP 42, the working group makes recommendations for physical infrastructure in both permanent and temporary locations. The document is a guide for planning and hosting digital assessment at your own institution.

Recommendations for wired and wireless network infrastructures are described in other Best Practice documents available on the GÉANT website.

The document is relevant to technical staff with responsibility for planning and hosting digital assessment at Universities.

CBP 43: Clients for digital assessment

(UFS 146, Norwegian version)

The working group looked at available client solutions for digital assessment, including the use of BYOD compared to institutionally-owned equipment.

CBP 43 does not list the various assessment solutions available, but focuses on requirements and the pros and cons of client solutions.

The document is relevant to technical staff with responsibility for planning and hosting digital assessment at Universities.

CBP xx: Integration for digital assessment

(UFS 147, Norwegian version)

The two working groups associated with CBP44 identified key integrations. Data from existing systems should be reused in the assessment solution.

This CBP document identifies six existing systems, defining which system is an authoritative data source, and describes integrations for the exchange of data to/from the assessment systems.

The document is relevant to developers, system integrators and technical staff.

CBP 44: Architecture for digital assessment

(UFS 148, Norwegian version)

This CBP document is the combined work of two working groups, one on workflow for digital assessment and one on ICT architecture for digital assessment.

The CBP documents describe an ICT architecture for a national solution for digital assessment and the consequences for the workflow at the University.

The document is relevant to management and staff with responsibility for planning assessments at Universities.

CBP 45: Logging and Monitoring of digital assessment

(UFS 149, Norwegian version)

While working with digital assessment, we discovered that the vendors of digital assessment solutions have different approaches to logging and monitoring.

CBP 45 defines and lists requirements for logging and monitoring, and describes policies for how to do logging and monitoring during digital assessment.

The document is relevant to management and technical staff with responsibility for planning and hosting digital assessment at Universities.

CBP xx: Legal issues regarding use of cloud services

(UFS 150, Norwegian version)

Several of the digital assessment software solutions are designed to be run as cloud services (in a private or public cloud). This CBP document examines the legal considerations and the steps to be followed for successfully using public cloud services for assessment solutions.

This CBP document applies to cloud services for the University sector in general.

The document is relevant to management and security staff with responsibility for services moving to the public cloud.