Authentication and security integration for eCampus services at the University of Applied Sciences Harz using the German Electronic Identity Card/eID and eGovernment Standards

Hermann Strack

Fachbereich Automatisierung und Informatik
University of Applied Sciences Harz / Hochschule Harz
Friedrichstr. 57-59, D-38855 Wernigerode, Germany
hstrack@hs-harz.de

Abstract: A eCampus security shell architecture was developed and deployed to improve the security of existing university management systems (legacy UMS), integrating innovative eGovernment Standards e.g. the German Electronic Identity Card (GeID), the eGovernment Protocol OSCI and qualified Signatures (QES).

1 Problem and requirements

The challenge was to improve the security of an existing university management systems (legacy UMS/HIS), by satisfying of particular interoperability requirements (INTOP) and by integrating innovative eGovernment Standards e.g. the German Electronic Identity Card (GeID), the eGovernment Protocol OSCI [www.xoev.de] and qualified Signatures (QES). Especially, these security requirements should be satisfied: privacy and data protection, integrity, (multi factor) authentication. The additional INTOP requirements included particular boundary conditions and restrictions for the security implementations as follows: no changes of existing (legacy) UMS interfaces and GUI; no discrimination of applicants or students without GeID.

2 The eCampus security shell architecture

To achieve the above requirements and conditions, the following eCampus security components must be integrated in an additional security shell for the legacy UMS (as a sort of "security satellite systems"): the eCampus registry to store/check additional security credentials for users (e.g. GeID Pseudonyms, QES certificates, OSCI certificates); the eCampus Server to host additional eCampus secured applications; the eCampus Mediator as a trusted Security Gateway between OSCI based secure communications (incl. signed data) and the legacy http based web interfaces of the

legacy UMS (incl. OSCI client for signed/encrypted data transfer); a U-M-converter service to translate between public and confidential user id attributes in a trusted manner.

To achieve the above requirements and conditions, the following eCampus security components must be integrated in an additional security shell for the legacy UMS (as a sort of "security satellite systems"): the eCampus registry to store/check additional security credentials for users (e.g. GeID Pseudonyms, QES certificates, OSCI certificates); the eCampus Server to host additional eCampus secured applications; the eCampus Mediator as a trusted Security Gateway between OSCI based secure communications (incl. signed data) and the legacy http based web interfaces of the legacy UMS (incl. OSCI client for signed/encrypted data transfer); a U-M-converter service to translate between public and confidential user id attributes in a trusted manner.

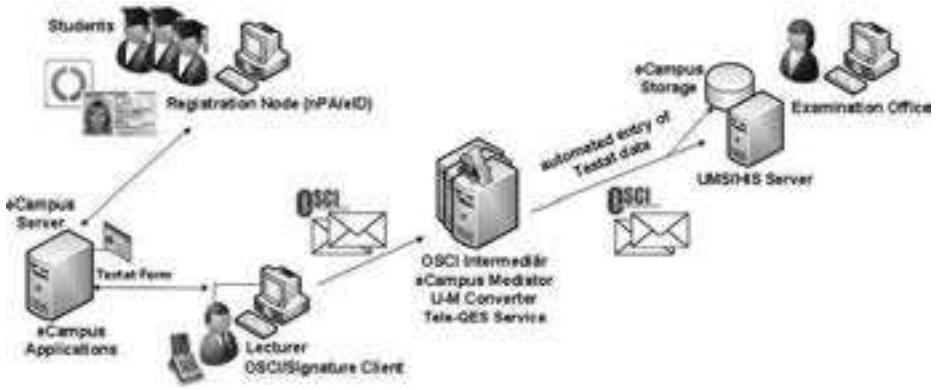

Figure 1: An overview - eCampus architecture, eGov. components, examination data flow (Testat)

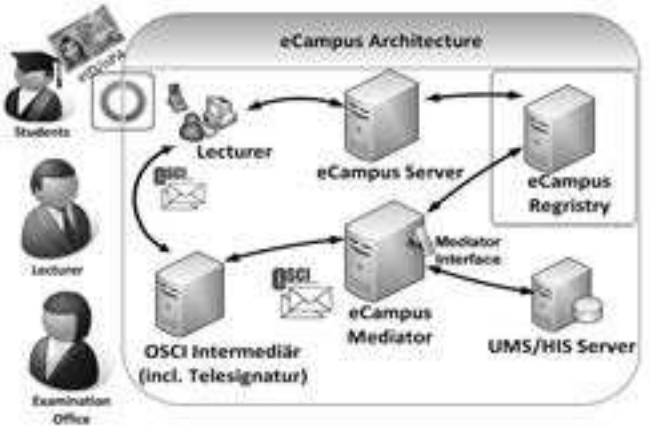

Figure 2: The eCampus security shell architecture, integrating GeID, OSCI, QES standards

References

[BKM+08] Bender J., Kügler D., Margraf M., Naumann I.: *Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis*, DUD, 3/2008

[StBr12] Strack H., Brehm N., et al.: *eCampus – Services & Infrastrukturen für elektronische Campusverwaltung mit verbesserter Sicherheit auf Basis von eGov.-Standards/Komponenten*, eGovernment Review, 2012

[BMI13] BMI eGov. Init. (ed.): *Hochschule Harz - eID-Anwendungskonzept (eTestate)*, http://www.personalausweisportal.de

[EuCo12] European Commission (ed.): *Public Services Online, Centric eGovernment performance in Europe – eGovernment Benchmark 2012*: HS Harz, pp. 47