An Ideal Anonymous E-exam System

Andrea Huszti and Péter Pleva

As electronic assessment forms an essential part of e-learning environments and, ideally, trustworthiness is of key importance in such systems, the design principles of e-exam schemes must be considered carefully. We propose a protocol that, above all the basic security requirements that traditional paper-based exams meet (such as secrecy, correctness and authenticity), provides anonymity for both examinees and examiners. From examinees' point of view, being anonymous not only ensures objectivity in determining their grades but also prevents partiality. On the other hand, examiners are also protected against bribing and threatening attacks with the help of anonymity.

Participants of our scheme include examinees, examiners, an Examination Board and an Administration Authority but the involvement of a Certification Authority and Timestamp Service Provider is also necessary. Examinees and examiners register for taking and correcting the exam, respectively, at Administration Authority. Examination Board receives e-exams and forwards them to examiners chosen randomly. Certification Authority and Timestamp Service Provider is responsible for managing digital certificates, issuing timestamps and also for controlling anonymous servers that replace senders' IP addresses to their own ones and perform some cryptographic operations. We assume honest behaviour on the part of the Certification Authority and Timestamp Service Provider, solely.

Acknowledgements

This work is supported by the national Economic Operative Programme (GOP-2007-1.1.2).

References

[1] Jordi Castella-Roca, Jordi Herrera-Joancomarti, Aleix Dorca-Josa: A Secure E-Exam Management System, ares, pp.864-871, First International Conference on Availability, Reliability and Security (ARES'06), 2006

[2] Andrea Huszti, Attila Pethö: A Secure Electronic Exam System, to appear

[3] ExamSoft Worldwide, `http://www.examsoft.com`