Secure Electronic Transcripts of Student Records

Mikael Berglund[1]

[1]Ladok Division, Umeå University, S-901 87 Umeå, Sweden, mikael.berglund@ladok.umu.se

Keywords
Security, transcripts, student services, pdf, pki

1. EXECUTIVE SUMMARY

A central part of education is to be able to see the progress in terms of finished courses and issued diplomas. This information is not only needed for the student, but also for possible future employers and other interested parties. A convenient, effective and secure way to accomplish these tasks is needed.

1.1. Background

Ladok is the national system used for documentation of academic information at higher education institutions in Sweden. It is jointly owned by these through a consortium. Each institution has its own separate installation of the Ladok system.

The ability for students to produce PDF transcripts has been in use since 2003. In 2007, this service was revised to include the higher security features which this paper will describe in greater detail.

1.2. Conclusions

In the Ladok system, the student can download a stand-alone PDF document which can be verified by the recipient of the document. This solution has the possibility of increasing security by purchasing a hardware module for storing of private keys and signing of documents or by using a self-signed certificate. One drawback is the possibility of distributing the transcript without the sender being aware of who will read it. One advantage is the rich way of formatting the transcript to make it look very similar to an actual transcript.

The option to increase security and convenience for recipients of a transcript is possible today with new technical solutions available with hardware signing. The benefits must be weighted against the resources required and the solution in place. For large institutions which can use economics of scale, the increased security can be a compelling argument. The downsides are increased costs and the dependency of a single vendor.

The Ladok system offers a solution implemented with open source tools and the possibility to add increased security if so required.

2. THE LADOK SYSTEM

As a result of co-operation among Swedish higher education institutions there are two common national computer based systems used in student administration in Sweden. NyA is the national system for student admission and Ladok is the national system for study documentation. Ladok is used by nearly all universities and university colleges in Sweden. All institutions co-operate in student administration and own the Ladok system portfolio through a consortium, but every institution has its own Ladok application and Ladok database.

Ladok contains and produces data regarding courses, admission conditions, examination, etc. All data regarding every student; application, admission, course registrations, study performance, diplomas, etc. is also stored in Ladok. Ladok is a central and very crucial system for institutions (Bergström, Berglund, Forutan-Rad, 2007).

3. SECURE TRANSCRIPTS

The traditional way of distributing a student's transcript of records is to print the records on paper and to stamp or sign it. This requires extensive manual handling and the resulting transcript is subject to forgery and is difficult to send in an electronic way to interested parties.

Transcripts have historically been sent to students after each semester, the exact time depending on the institution. This was very expensive for institutions and inconvenient for students. For students to receive transcripts outside of the normal frequency, special attention is required by the student office to print and send a separate transcript. This was even more costly for the institutions. To serve the increased demand for online services, an online web transcript was created. This reduced the need for separate handling of students.

4. FIRST VERSION

The first version of this service was based on PDF documents which were generated on the server and made available for download. To verify a transcript, the recipient of the PDF file accessed an URL specified in the file itself. In this web page, the recipient entered a verification code in the transcript. This presented the recipient with the original transcript issued by the institution. Through manual examination of the two documents, the recipient can verify the authenticity of the transcript. This solution has several security implications. PDF files are easily manipulated and a phishing website can be set up which returns the forged transcript. The usability is also limited since the recipient has to manually review the document. See Figure 1 for an image of the transcript. The name of the student is incomplete in this picture to protect the student.

This service is part of the subsystem Ladok on Web, which is a collection of SOAP services for the Ladok system. These services are used in student portals to present student information online and for students to perform administrative services online.

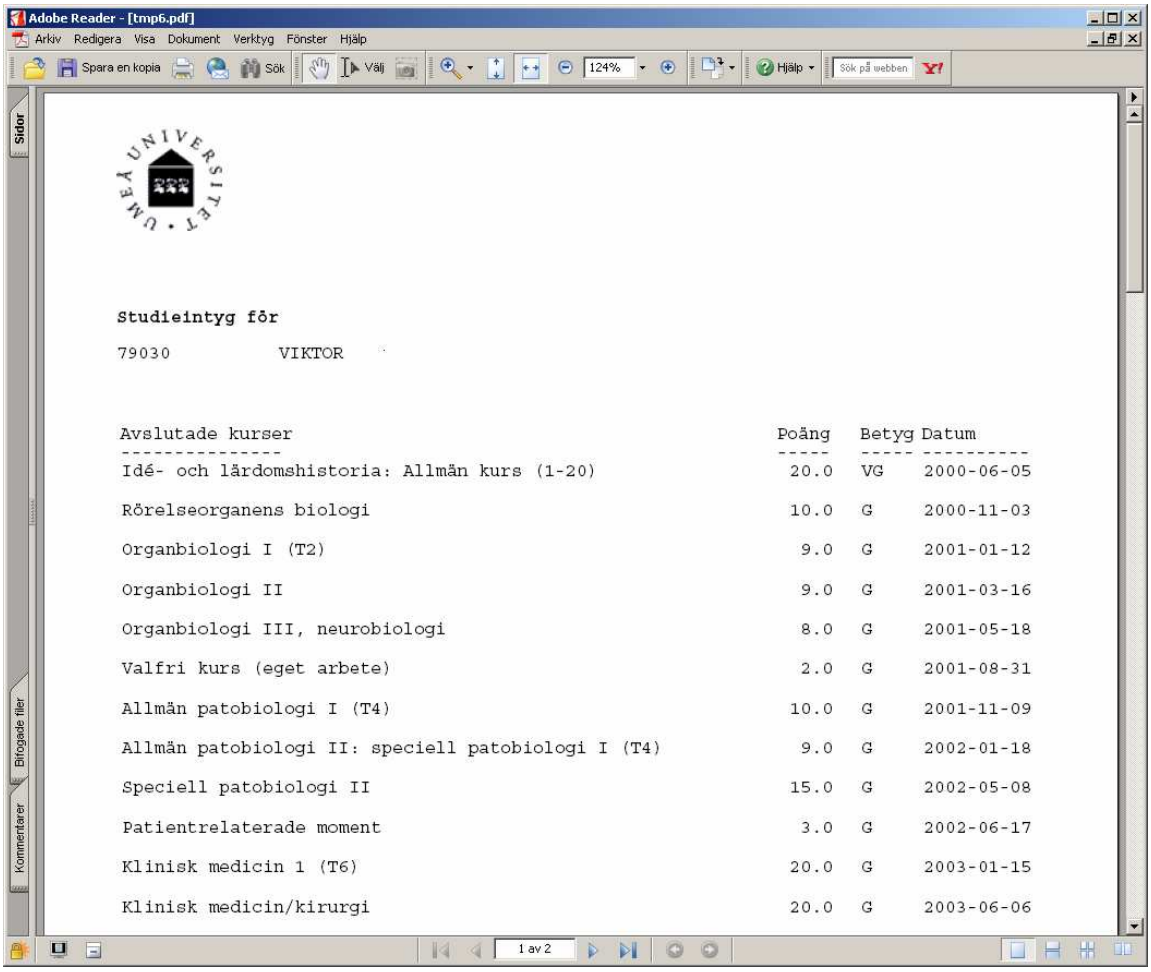

Figure 1. Secure transcript.

5. SECOND VERSION

The new version has a new method of securing the transcripts which rectifies these flaws and introduces higher security. This solution is based on the ISO 32000 PDF standard and public key infrastructure.

5.1. PKI solutions

In accordance with the PDF standard, a document can be digitally signed by a certificate authority. In Public Key Infrastructure terms, the recipient has to trust the certificate authority. As with Secure Socket Layer (SSL) the trusted certificate authorities is dependent on the application used. Microsoft Internet Explorer uses the certificate store on the local Windows machine. Mozilla Firefox uses an internal store. There is a large mental and practical step for a user to install a new trusted certificate authority.

In the new version a new feature was created which enables the institution to sign a transcript with either a self-signed certificate stored on the server or a hardware storage module (HSM).

A signed PDF file can be verified in Acrobat Reader. A self-signed transcript can't be verified in Acrobat Reader without importing the certificate authority's public key. This is shown in figure 2.

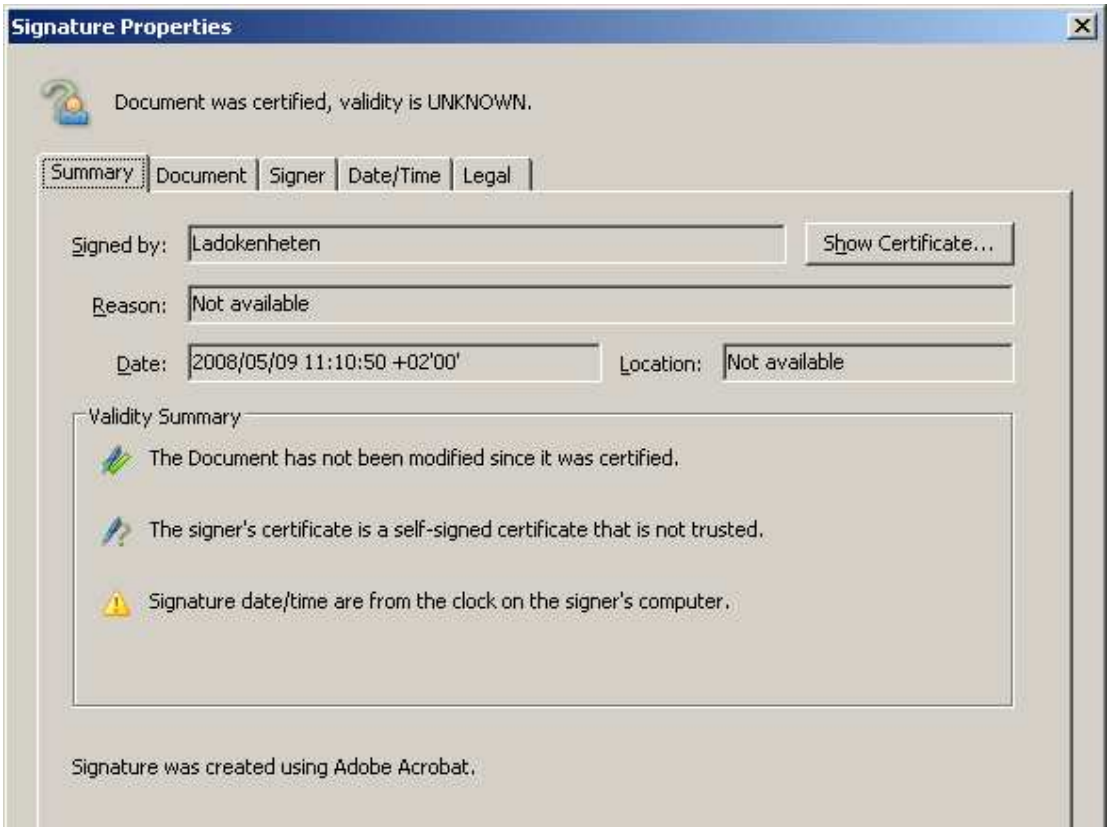

Figure 2. Self-signed certificate.

This is not optimal; however it is arguably more secure than omitting a signature. It is possible for the recipient of the document to install the public key of the signer.

Currently, the only way to generate a PDF document that is trusted out of the box in Acrobat Reader is to purchase a certificate from GeoTrust. This certificate is very expensive and has a list price of approximate €9000 for 100 000 signatures (TrustCenter, 2008). The certificate must also be installed on a Hardware Security Module (HSM). The level of trust is very high, together with the cost. The cost is not only for the purchase of a certificate, but also the cost of installing the hardware module and integrating a software system.

This gives a different user experience as shown in figure 3.

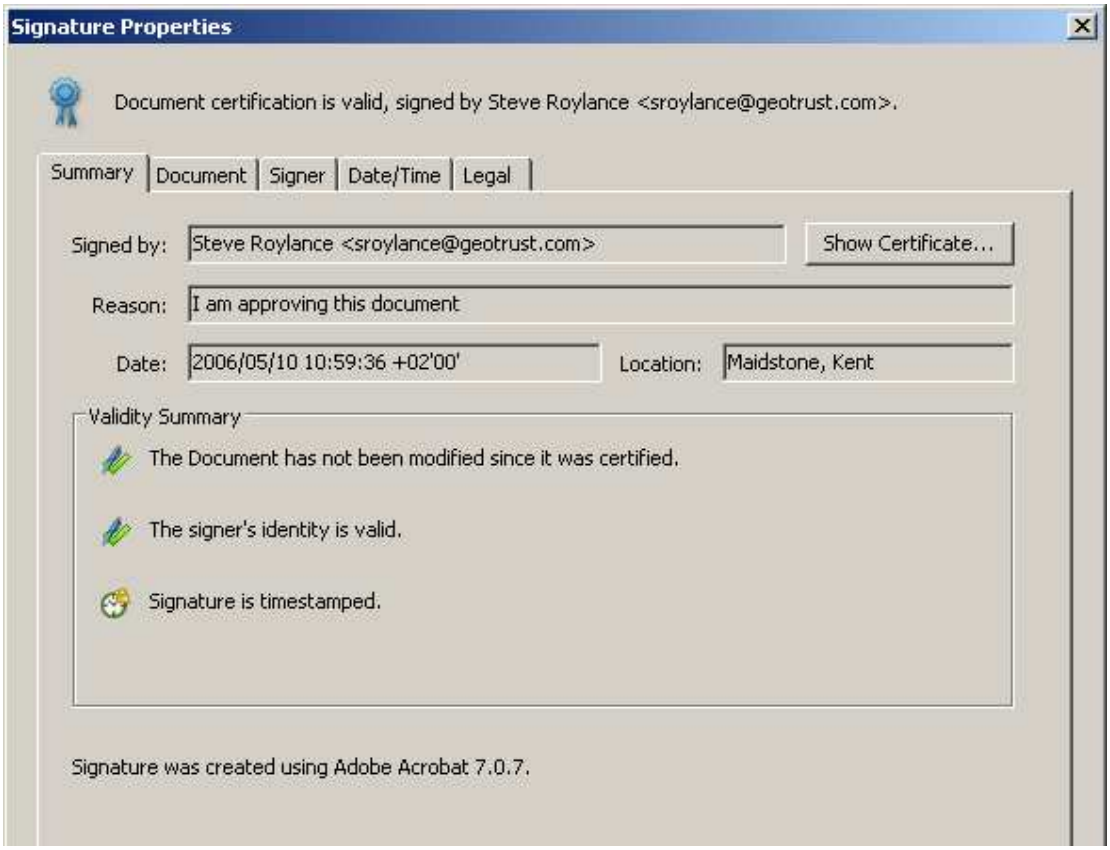

Figure 3. Signed PDF file.

5.2. The Ladok solution

The Ladok solution is built on the Ladok on Web SOAP framework and provides portal developers with a web service to fetch and verify PDF transcripts. The PDF files generated by the server can optionally be signed with a digital signature. This feature is fully pluggable and can either use self-signed certificates or a HSM module with a purchased GeoTrust certificate.

5.3. Alternatives

There are a number of alternatives in use today. The most successful alternative is made by the company Digitary with their product Workflow (Digitary, 2008). In Workflow, the student makes the information available on-line for the recipient with several advanced features for access control and support for audit trails. The transcript can be sent stand-alone, or fetched on demand. The same issues with forging an e-mail pointing to a fraudulent website exist in this solution.

6. CONCLUSIONS

Computer security is a broad and difficult subject with many facets. Strong ciphers and cryptography means nothing if we trust the wrong sources. There are, however, several effective security mechanisms which are in general use and trusted by general computer users. A website which uses a SSL certificate for encryption can usually be trusted to be the real one.

One must also consider the nature of the information to be secured. To be able to access a SSL secured web site on a trusted domain such as the issuing institution to verify a transcript is arguably more secure than paper copies.

The option to increase security and convenience for recipients of a transcript is possible today with new technical solutions available with hardware signing. The benefits must be weighted against the

resources required and the solution in place. For large institutions which can use economics of scale, this can be a compelling argument. The downsides are increased costs and the dependency of a single vendor.

The Ladok system offers a solution implemented with open source tools and the possibility to add increased security if so required.

7. REFERENCES

J. Bergström, M. Berglund, A. Forutan-Rad (2007). *National and local integration in the Swedish Ladok System*. EUNIS 2007, Grenoble, France.

TrustCenter website (2008). *TC Business ID for Adobe*. Retrieved May 15, 2008, from: http://www.trustcenter.de/en/products/tc_business_id_for_adobe.htm

Digitary website (2008). *Digitary*. Retrieved May 15, 2008, from: http://www.digitary.net/digitary.htm