Digitally signed reports and diplomas for the students of the University of Applied Sciences Berne (BFH)

the idea

- Already some years ago, someone had the idea to handout in the future reports and diplomas to bachelor students not only in the classical form as a document, but also in a digitally signed electronic form
- A couple of month ago a member of a bologna committee in our 'department of technique and informatics' asked me, if I would have a solution and if it would be possible to be realized in October 2006
- A couple of days ago, they invited me and another professor in cryptography to a meeting to present our solutions

the requirements

- It should be a publicity event
- It should be realized without big effort (work and costs)
- The electronic document must be tamper proof and the used key must be strong enough to be secure up to 10-20 years
- We should use preferably a simple technique to produce and deliver these documents
- A human resource department of a company should be able to verify this document in a simple way
- The electronic document should be verifiable in 20 or more years after the date of issuance
- Applications for an employment will take place increasingly in electronic form. The verification must be guaranteed, to avoid bad reputation of our institution in the future

the proposed solutions

the hash value solution

- Diplomas and reports will be - as usual - hand out in paper form, but with a 128-Bit truncated hash value printed on it
- The University must provide a verification page on a website
- Everyone who knows the hash value of a diploma can simply verify it, by entering sixteen characters or numbers (similar to a pgp-fingerprint)
- The student can generate a pdf-file (or what else) by his own, and send it in his electronic application for an employment

the digital signature solution

- Diplomas and reports will be hand out in paper form and additionally sent by e-mail to the student with a digitally signed pdf-file attached
- The student can send the diploma as pdf-file whenever he wants in his electronic application for an employment
- Everyone can verify the authenticity of the diploma by verifying the certificate of the signing person or institution
- The certificate issuer and the used certificate must be as confidential as possible to guarantee the verification

the open questions

- Do we need ZertES compliant certificates, or is a self registered certificate (e.g. SwissSign Silver/Gold) enough for this purpose?
- Contains the subject name in the certificate the signing person or the name of the institution?
- How should the enrollment of the keypair to be done? How should be the personal security environment (e.g. security token)?
- How can we guarantee a simple verification of the signed document, if the certificate of the authenticated person must have been revoked, because the signing person has left the institution?
- What if the pdf-file cannot be read anymore in 20 years, because the file format is not supported anymore?
- How can we sign diplomas and reports for more than 1000 students per year efficiently?

the decision

- The bologna committee decided to implement - when ever possible - the digital signature solution, but not already for October 2006
- Because this solution should be implemented at a higher level (not only in the ‘department of technique and informatics’), they now first want to bring this proposal into the school leadership of the BFH
- Main reason for this solution is the publicity. There is no need to use digitally signed diplomas, but it’s a good idea - realized with a forward-looking technology!