

EUNIS 2009: A comparison of certified PDF and Digitary for secure graduation documents

Andy Dowling¹, Jonathan Dempsey²
Digitary, Invent Building, Dublin City University, Glasnevin, Dublin 9, Ireland.

¹ andy.dowling@digitary.net

² jonathan.dempsey@digitary.net

Keywords

Bologna Process, European Diploma Supplement, authentication, secure, electronic signature.

1. EXECUTIVE SUMMARY

Certified PDFs are used by some higher education institutions in the United States for the delivery by graduates of “eTranscripts” to employers. Digitary is used by higher education institutions in Europe for the delivery by graduates of award certificates, European Diploma Supplements, Official Transcripts of Results and other documents to employers, higher education institutions and others. This paper assesses how each approach meets the technical and security requirements for trust and usability and how each approach can be used to meet the additional requirements for the creation, management, distribution and authentication of electronic graduation documents.

1.1. Background

Graduation documents are used by graduates for the duration of their careers. Electronic graduation documents should therefore offer a career-long secure record of the graduate’s achievement. In addition, issues such as document distribution, access control, data protection, auditing, document revocation, and standards compliance must be addressed when implementing a secure graduation document solution.

1.2. Alternatives

After identifying the requirements for secure graduation documents, two alternative approaches to implementing secure graduation documents are discussed in this paper: certified PDF and Digitary. Both approaches are compared against these requirements.

1.3. Conclusions

This paper draws the conclusion that certified documents alone are not enough when implementing a comprehensive secure graduation document solution. We conclude that three core elements are required in order to address all of the requirements identified:

1. The means to create digitally-signed, standards-compliant documents
2. An online facility for the secure long-term archival of signed documents
3. Online services for the verification of documents within the archive

These three elements are already present by design with the Digitary model, and such a model can be implemented using certified PDF technology.

2. INTRODUCTION

2.1.Overview

In this paper, we compare two approaches to securing electronic graduation documents. The first approach involves the use of Certified PDF technology. The second uses the Digitary model.

Both approaches make use of digital signature technology to authenticate document content, although to differing levels and standards. Our discussion starts with a brief overview of the requirements for secure electronic graduation documents. We then briefly discuss digital signature technology and the technical requirements for the maintenance of digital signatures as long-term records. We observe that digital signatures alone are insufficient to address the wider issues of document distribution, access control, auditing, and comprehensive verification.

Based on these observations, we identify the technical elements required for the generation, maintenance, and secure access to standards-compliant electronic graduation documents in the long term.

2.2.Requirements for secure electronic graduation documents

Graduation documents are typically issued to a graduate upon successful completion of a course of study at a particular Higher Education Institution (HEI). Graduation documents are intended to represent a secure record of the graduate's qualifications/achievement at the HEI, and can last for the lifetime of that graduate. A graduate can present their graduation documents for verification by a recruiter or other third party should the need arise. In certain exceptional cases, a graduation document may be revoked by the issuing HEI (in the case of administrative error or plagiarism, for example).

With this overview in mind, we can define some fundamental requirements of a secure electronic graduation document. An ideal secure electronic graduation document:

- must be authentic and tamper-evident
- must be comprehensively verifiable by authorised parties
- must be a life-long electronic record (i.e. a “snapshot” equivalent to original paper) and remain valid for (at least) the career of the graduate to whom it refers
- must be available only to the graduate, and to third parties authorised by the graduate in a controlled and auditable manner
- may be revoked by the HEI after the document has been issued

In addition, an ideal secure electronic graduation document:

- must adhere to appropriate technical and security standards
- must be represented in a standards-compliant manner for interoperability with other systems

3. SECURE ELECTRONIC DOCUMENT TECHNOLOGY

3.1.Introducing certified PDF

PDF documents have been in widespread use for many years and are regarded by many as an excellent means for distributing document content.

Digital signature support was introduced into the PDF format to enable the creation of authentic and tamper-evident PDF documents. PDF documents support two types of digital signature – a “standard” digital signature and a “certification signature”. Both signature types provide a means to cryptographically ensure the authenticity and integrity of a PDF document. However, the certification signature is regarded as a higher form of signature (as it places additional restrictions on the signed document), and results in a “blue rosette” appearing on the PDF document when it is opened in a compatible PDF reader. We refer to such a PDF as a “Certified PDF” in this paper.

3.2.Introducing Digitary

Digitary's secure electronic document solution was developed over a number of years with document security and data protection as fundamental principles, using input from stakeholders within the European Higher Education sector.

The Digitary model is based around the secure *online archival* and long-term storage of digitally-signed, standards-compliant XML documents at a website *controlled by the issuing institution*. All access to the document (including document verification) is through a secure and monitored web environment, where access permissions for a given document are granted by the graduate to whom that document refers.

4. LONG-LIVED DIGITAL SIGNATURES

Both Certified PDF and Digitary approaches use digital signature technology to ensure the authenticity and integrity of document content. Typical digital signatures are only valid in the short term (usually until the validity period of the signer's digital certificate has expired), which is why additional technical approaches now exist to address the long term validity of a digital signature. A long-lived digitally signed document is built in a number of ordered stages, as follows:

Order	Stage	Description	Document Attributes
1	Digital signature (-BES)	The document signatory applies a digital signature to the document.	<ul style="list-style-type: none">● Authenticity● Tamper-evidence
2	Timestamp (-BES) + (-T)	A third party, called a Time Stamp Authority (TSA), certifies that the digital signature existed on or before a point in time. The time stamp is included in the document	<ul style="list-style-type: none">● Authenticity● Tamper-evidence● Certified signature time● Comprehensive non-repudiation¹

¹ Comprehensive non-repudiation is achieved through timestamping, as a document signer cannot deny having signed a document when their certificate was deemed to be valid. The timestamp provides a certified source of time.

3	Complete validation information (-BES) + (-T) + (-C)	Long-term validity information for the document signatory is gathered to prove in the long term that the signature was valid at the time of signing (i.e. certificate chains and CRLs/OSCP responses). These items are included with the document.	<ul style="list-style-type: none"> ● Authenticity ● Tamper-evidence ● Certified signature time ● Comprehensive non-repudiation ● Complete validation information
4	Archive timestamping (-BES) + (-T) + (-C) + (-A) (recurring)	<p>Archive timestamping creates a digitally signed timestamp over the original document signature, timestamp, long-term validation information, and any previous archive timestamps. The resulting archive timestamp is included with the document.</p> <p>The archive timestamp ensures the authenticity and integrity of the document, the signature, all validation information and timestamps in the long term. This step is performed periodically (i.e. every 10 years), and maintains adequate “cryptographic cover” over time through the use of up-to-date algorithms.</p>	<ul style="list-style-type: none"> ● Authenticity ● Tamper-evidence ● Certified signature time ● Comprehensive non-repudiation ● Complete validation information ● Long-term cryptographic authenticity and integrity

This approach to long-term validity of documents has been standardised by the European Telecommunications Standards Institute (ETSI) in standards TS 101 903 (XAdES) [ETSI-3] and ETSI TS 101 733 (CADES) [ETSI-1].

Observation #1

*In order to maintain long-term legal validity and cryptographic integrity of a digitally signed document, the document must be **securely archived and periodically timestamped** once it has been created.*

4.1.PDF Digital Signatures

A PDF document is stored in .PDF format according to the PDF language syntax (at the time of writing, version 1.7 is the most recent version of PDF).

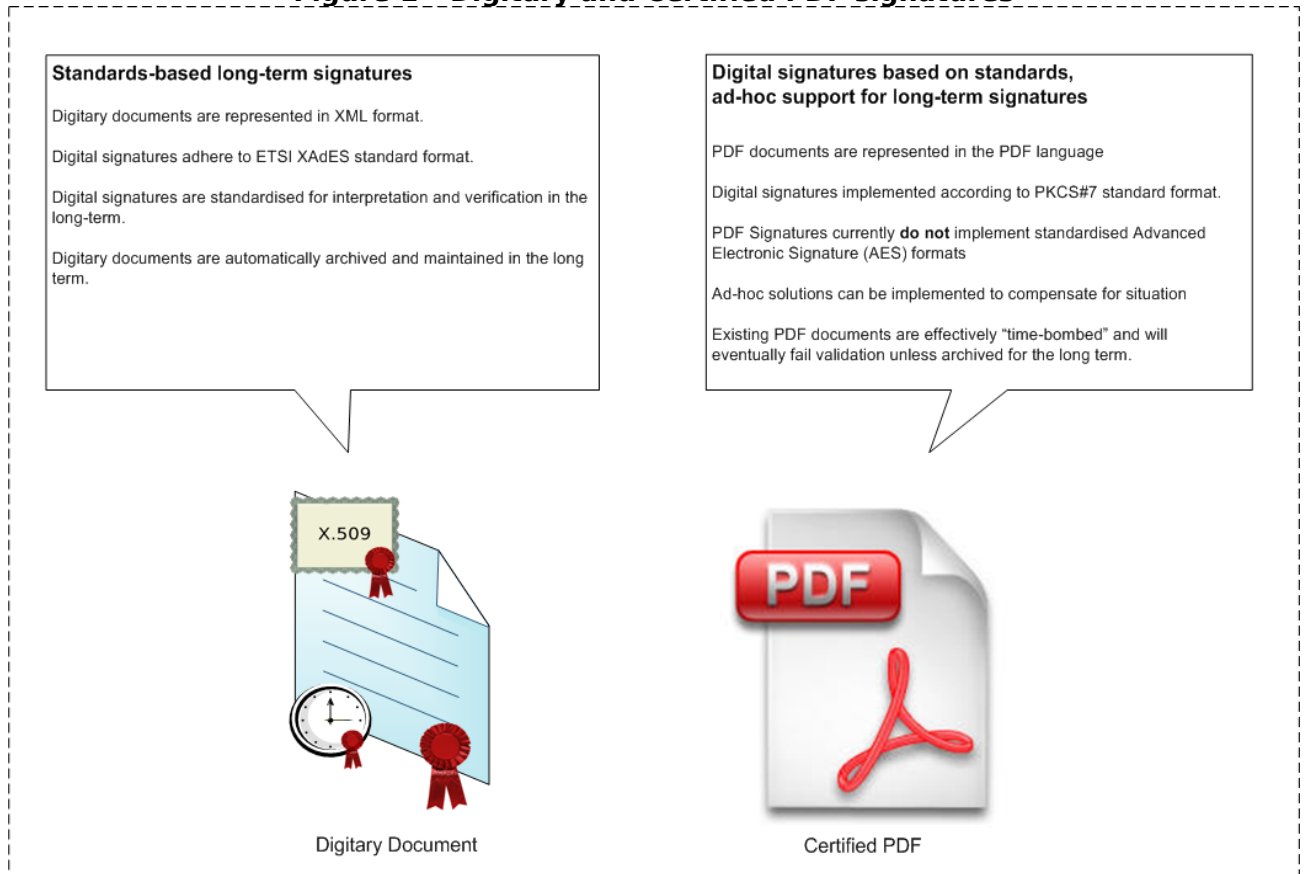
PDF v1.7 digital signatures provide digital signature and timestamping support. *However, there is currently no **standard** support for **long-term** signatures in PDF documents.* In order to implement long-term validity for PDF documents, non-standard mechanisms must be employed in order to maintain signature validity in the long term.

To address this limitation in the PDF standard, ETSI has commenced work on the standardisation of XAdES and CADES digital signatures into ISO32000 (PDF 1.7 standard), and this work is scheduled for completion by mid-2010 [ETSI-2].

4.2. Digitary Digital Signatures

Digitary documents and digital signatures are represented in XML format. Digitary documents use ETSI XAdES-A signatures, and provide long-term validation by representing signatures, timestamps, complete validation information, and archive timestamps in the document according to this European technical standard, thus ensuring the long-term legal validity, cryptographic integrity, and standards compliance of electronic documents.

Figure 1 - Digitary and Certified PDF signatures



Observation #2

*As it currently stands, the digital signatures implemented inside PDF version 1.7 **do not follow existing standards for long-lived digital signatures**, and the legal validity of these documents is not guaranteed in the long term unless additional ad-hoc mechanisms are put in place to compensate.*

*The digital signatures implemented through Digitary are **standards-compliant (XAdES-A) long-lived digital signatures**.*

5. THE BIGGER PICTURE

When issuing electronic graduation documents, the creation of digital signatures (and timestamps) provides a legally recognised method to authenticate the signed content in the short term. Creating digital signatures and timestamps alone does not address a number of other key issues related to the management of graduation documents over the long term.

Certified PDFs are effectively self-contained “snapshots” of authenticated content that can be distributed and verified *independently of the issuing HEI and of the graduate*. These .PDF files can effectively become *standalone* documents. This has a number of side effects as shown below:

Issue	Side Effect	Action Required
Standalone, certified PDF file re-distribution does not require intervention of the graduate to whom the document refers	Standalone certified document distribution facilitates identity theft. (i.e. obtaining a standalone certified PDF file is the digital equivalent of taking an original paper document from its owner.) No audit trail for document access.	Need to provide means for graduate to control and monitor access to their document(s)
Standalone documents exist outside of a controlled archive environment	Long-term legal validity and cryptographic integrity of offline documents is not guaranteed, as there is no guarantee that archive timestamps will be periodically applied to these documents.	Need controlled document archive to store and periodically timestamp documents
Verification does not depend on contacting the issuing HEI	Issuing HEI does not have the ability to communicate with the relying party that the document has been revoked since it was issued	Need to check document revocation status at issuing HEI at time of verification ²
PDF Reader software performs only generic document validity checks	Additional application-level checks specific to the type of document are outstanding, for example: a) Authorisation of the signatory to sign <i>the type of document in question</i> on behalf of the organisation b) Number of signatures required for the type of document The verifying party may be left with an incomplete picture of the document's trustworthiness	Need to perform additional checks at time of verification

² This feature is available in PDF Reader, but may require additional Adobe Enterprise software (Policy/Rights Management Server) to be installed at the HEI and made publicly available to Adobe Reader clients outside the HEI

These issues can be addressed by implementing:

- a **secure document archive** for the maintenance of long-term digital signature validity
- a **set of secure online services** for managing document access control, verification, and for maintaining an audit trail

...to **complement** the digitally signed graduation documents.

Observation #3

The implementation of digital signatures alone is insufficient address the issues around long-lived graduation documents. Additional elements must be implemented, including:

- 1) A secure document archive to maintain long-term digital signatures*
- 2) A set of services for the distribution, access control, audit, and verification of documents*

5.1. Filling the gaps by building upon Certified PDFs

At the time of writing, the author is not aware of any standardised model that fills the requirements of Observation #3. Therefore, a HEI must implement these elements itself if all of the issues are to be addressed. This involves:

1. Implementation of certified PDF generation (i.e. using Adobe³ CDS/CTS, for example)
2. Implementation of a secure document archive for ad-hoc maintenance of PDF signature validity in the long-term
3. Implementation of a set of externally-available services for managing distribution, access control, verification, and audit of certified PDF documents

One example where Certified PDFs are combined with an online model is at Pennsylvania State University [PSU] (PSU) in the United States. Their model can be roughly described as follows:

1. PSU Graduates apply for transcripts via a secure website to be sent directly to recruiters
2. Certified PDF documents are issued through the Adobe Certified Transcript Service (CTS) by the Higher Education Institution (HEI - Penn. State, in this case)
3. The HEI distributes the resulting PDF documents to recruiters in a secure manner (i.e. via authenticated secure download)

Once the PDF document has been obtained, it can be saved and verified inside appropriate PDF reader software.

Whilst the PSU implementation shows that it is technically possible to address some of these wider issues by building online services on top of Certified PDF technology, the following issues with this approach invariably remain:

- The digital signature representation inside PDF documents does not currently adhere to existing technical standards for long-lived digital signatures

³ Adobe is a registered trademark of Adobe Systems Inc.

- Lack of standard long-term signature support means that certified PDF documents issued using today's PDF technology are effectively “time-bombed” and will not validate after a certain point in time (to illustrate - simply open a working Certified PDF in Adobe Reader and set your system clock to the year 2020). This could possibly lead to documents being denied legal admissibility in the long term.
- At some point in the workflow, a certified PDF document can leave the control of the HEI and exist as a standalone document (.PDF file) outside of the HEI. This .PDF file could be copied and used for the purposes of identity theft, as it could be verified without the intervention of the graduate referred to in the document. This is the digital equivalent of being able to take a person's paper original and use it for the purposes of identity theft. This is arguably easier to accomplish digitally.

5.2. Filling the gaps with the Digital approach

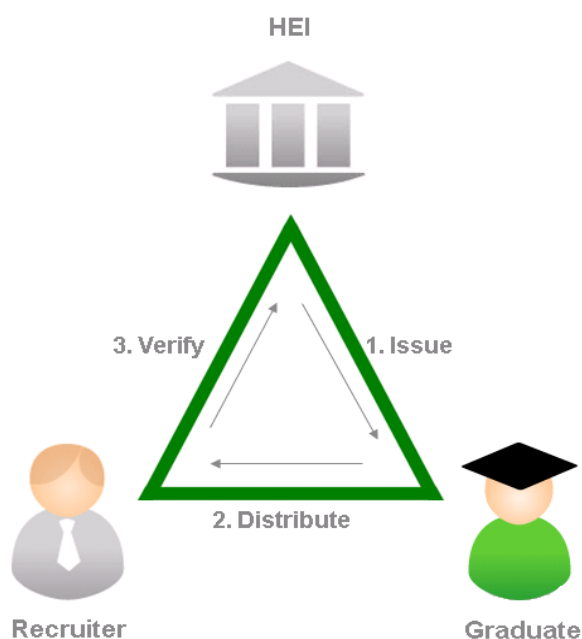
The Digital approach to secure graduation documents is a combination of:

1. A facility for the creation of long-lived digitally signed and timestamped documents compliant with the XAdES standard
2. A secure document archive for the management of digital document signatures compliant with the XAdES standard
3. A set of web-based applications that enable document distribution, access control, auditing, and comprehensive verification

The anatomy of the Digital workflow model is as follows:

1. The electronic document is created and digitally signed by officer(s) of the HEI. The signed document persists in a secure online electronic archive, which is under the control of the HEI.
2. The Document Holder (i.e. graduate) uses a secure web application controlled by the HEI to view their document(s) online, share their documents with third parties, and to control and monitor access to their online documents.
3. Relying Parties access and verify online documents via a secure web application controlled by the HEI. They can also maintain a secure audit trail of any documents that they have verified, and to determine if any previously verified documents have been revoked since they were issued or last verified.

Figure 2 - Digital Triangle Model



The Digitary approach is based around an entirely different model to that of the "traditional" method of electronic file distribution (i.e. .DOC, .PDF, etc.). With Digitary, the documents that are created and stored online on a secure server at the issuing HEI. The documents are *stored* and *verified* on the server, and are only *rendered* on the client. Standalone document files are not distributed to graduates and/or third parties, *secure hyperlinks to online documents* are distributed instead.

This online approach to application hosting and data storage is becoming increasingly popular. The approach has been adopted by Google⁴ in their "Google Apps" offering. In a more general sense, the "Cloud" computing model is being embraced by stakeholders in the IT community at large.

The Digitary model can be used to address the issues that arise with the use of digitally-signed graduation documents. The Digitary model provides online archival, distribution and verification facilities to resolve the issues as follows:

Action Required	Digitary Solution
Need to provide means for graduate to control and monitor access to their document(s)	The Document Holder (i.e. graduate) uses a secure web application controlled by the HEI to view their document(s) online, share their documents with third parties, and to control and monitor access to their online documents
Need to check document revocation status at HEI at time of verification	Documents are verified online at a website controlled by the HEI. Revoked documents will fail to verify. Relying Parties who verified a document prior to its revocation can be identified from the audit trail and contacted, where permitted.
Need to perform additional checks at time of verification	Additional checks are performed upon verification through Digitary
Need controlled document archive to store and periodically timestamp documents	All documents are stored in Digitary online archive, and are periodically timestamped to guarantee long-term validity.

6. CONCLUSION

This paper compared two approaches for the implementation of secure electronic graduation documents. In doing so, we started by looking at how both approaches used digital signature technology and we made three key observations in this regard:

1. Digitally signed documents, regardless of their format, must be securely archived and periodically timestamped in order to preserve their validity in the long term
2. The current PDF format (version 1.7) does not implement existing technical standards for ensuring long-term document validity
3. Digital signatures alone do not address the issues of document archival, distribution, access control, comprehensive verification, and auditing.

We discovered that in order to address the issues properly, three ingredients are required:

1. A facility for the creation of long-lived digitally signed and timestamped documents compliant with an appropriate international technical standard

⁴"Google" and "Google Docs" are registered trademarks of Google, Inc.

2. A secure document archive for the management of digitary document signatures compliant with an appropriate international technical standard
3. A set of online services that enable document distribution, access control, auditing, and comprehensive verification

In addition to addressing the requirements for graduation documents, the combination of a standardised document representation and a set of online services *provides a platform for the HEI to integrate their graduation documents with other services in the future* (ePortfolio and life-long learning systems, recruitment portals, government statistics agencies, etc.)

A comprehensive secure graduation document implementation at a HEI can be implemented using one of two approaches:

1. Implement a combination of:
 - a) Certified document technology (PDF)
 - b) A secure “ad-hoc” digital signature archive using PKI technology
 - c) Online services for the distribution, access control, audit, and verification of certified PDF documents
2. Implement the Digitary solution, which by design contains all three components

The first approach will address the issues, but is complex to implement and the digital signatures are not currently standards compliant (PDF 1.7).

The Digitary approach is a unified solution that will address the same issues in a XML-based and standards-compliant manner that ensures legal validity for documents and provides wide scope for interoperability in the long term.

7. REFERENCES

[ETSI-1] ETSI Website (2008). *CMS Advanced Electronic Signatures (CAAdES) ETSI TS 101 733*. Retrieved November 2008, from: <http://portal.etsi.org>

[ETSI-2] ETSI Website (2008). *Terms of Reference for Specialist Task Force STF 364 (TB ESI) on “Advanced Electronic Signatures for PDF”*. Retrieved November 2008, from: http://portal.etsi.org/STFs%5CToR%5CToR364v11_ESI_PDF_ADES.doc

[ETSI-3] ETSI Website (2008). *XML Advanced Electronic Signatures (XAdES) ETSI TS 101 903*. Retrieved November 2008, from: <http://portal.etsi.org>

[PSU] Pennsylvania State University Website (2008). Information regarding of PSU eTranscripts system. Retrieved November 2008, from: http://www.registrar.psu.edu/transcripts/delivery_methods.cfm