Cultures of Trust: Legal, Technical and Archival Perspectives on the Use of Digital Signature Technologies

Fiorella Foscarini

School of Library, Archival and Information Studies
The University of British Columbia
1961 East Mall
V6T 1Z1 Vancouver, BC (Canada)
fiore@interchange.ubc.ca

Abstract: After examining some of the findings of two InterPARES 2 case studies involving the use of cryptographic technologies in e-government initiatives, the author reflects on the different ways in which the issues related to the preservation of digitally signed records and the concept of "electronic authenticity" are perceived, and put into practice, by the various interested professional groups, i.e., legislators, IT experts and archivists.

1 Introduction

The InterPARES (International Research on Permanent Authentic Records in Electronic Systems) Project is an international collaborative project that was established in 1999 with the objective of developing the theoretical and methodological knowledge necessary to ensure the long-term preservation of authentic electronic records. In its second phase, which started in 2002 and ended in 2006, its purpose was to address the issues of reliability, accuracy, and authenticity of records created and maintained in the context of artistic, scientific and government activities that are conducted by means of experiential, interactive and dynamic computer technology.[1]

Two of the case studies carried out in the course of InterPARES 2 involved e-Government initiatives – one in France and one in Ireland – which were both relying on the use of public key infrastructure (PKI) services for purposes of data integrity, security, and authentication. Due to the different goals, types of actors, and legislative frameworks involved, the PKI solutions adopted in the French and the Irish case respectively show quite diverse characteristics in terms of their features and underlying philosophies. At the same time, however, a striking similarity emerges from an analysis of the findings of the two case studies: the issues of maintaining the evidential value of digital signatures through technological evolution and preserving digitally signed documents over time have not been addressed by either project.

[1] For more information on the InterPARES Project, see at http://www.interpares.org (last accessed 30 June 2008).

Being short-sighted seems to be a characteristic of our times. National and supra-national laws and regulations do not make any exceptions in this respect, as an InterPARES 2 general study on records-related legislation demonstrates [SFC05]. The problems arising from the different life cycles of electronic records on the one hand and cryptographic signatures on the other have also received uneven consideration from the IT research community. It seems, as others have pointed out [Bl06], that both law-makers and IT experts share an understanding of "electronic authenticity" that is fundamentally different from the meaning that archivists attach to it.

From an analysis of the technical and archival literature on this topic, as well as of the legislative provisions that have been enacted in various countries in Europe following the 1999 EU Directive on e-signature [EU99], it will emerge that different "cultures of trust" exist, not only at the level of national cultures but also as far as professional groups, or "communities of practices", are concerned.

2 Findings of InterPARES 2 Case Studies

2.1 The Alsace-Moselle's Land Registry Case Study[2]

One of the two InterPARES 2 studies regarding the use of digital signature technologies investigated the computerisation of the land registry of Alsace-Moselle, a French regional administrative entity. The aim of the Alsace-Moselle's project, whose implementation was carried out between 2002 and 2006, was that of designing a dynamic information system for the online registration, authorisation, and publication of real estate transactions, according to the French civil law evidence system. The whole project involved, on the one hand, the transfer of 40.000 paper-based registers to a computer database, and on the other, the deployment of a region-wide PKI which would enable judges to digitally sign each new entry into the database. The infrastructure was meant to integrate a number of state-of-the-art security technologies and methodologies, including a biometric identification system for authenticating the judges' digital signatures.

All parties involved[3] had the strong belief that the computerisation process would maintain the high standard of efficiency and reliability of the paper-based land registry, while taking advantage of the enhanced access capabilities offered by the information and communication technologies. The project was in line not only with the European Union's push to break down national barriers and instil transparency in markets, but also with a major reform of evidence law that, beginning in the mid-1990s, affected most European countries including France. Thanks to the recognition of the legal value of

[2] The final report of the Alsace-Moselle's Land Registry Case Study will be available in the forthcoming book on the InterPARES 2 findings [DP08].

[3] The project was under the responsibility of a specifically dedicated administrative body created in 1994, the GILFAM (Groupement pour l'Informatisation du Livre Foncier d'Alsace-Moselle). In 2002, GILFAM granted IBM and Parker Williborg, a consulting firm, a 60 million EUR contract to oversee and implement the computerisation of the registry.

electronic documents, the computerised land registry would continue to hold information admissible in court as evidence. Additionally, in response to the 1999 EU Directive on e-signature, the reformed legislation granted a special evidential status to a specific electronic signature technology, i.e., that based on public key cryptography, through a presumption of trustworthiness automatically met by such signatures. Technically, by verifying and digitally signing each document concerning a real estate transaction (so-called "ordonnance") submitted to his/her attention by one of the land registry offices, the judge would create a signed XML document considered "authentic" in the sense of the French law on e-signature.

The project now briefly summarised achieves the goals of interoperability, security and authentication that underpin any e-government initiatives involving electronic transactions. However, the approach taken by GILFAM, the body administering the land registry system, goes beyond the function that should be attached to a signature, i.e., to perform the one-time service of demonstrating the authenticity of an ordonnance at the very moment the judge signs it. By means of a control mechanism embedded in the software, which ensures that the content of the database remains consistent with the one of the signed ordonnance[4], the system uses the digital signature to provide continuous authentication service, that is, regularly performed declarations of the integrity and origin of the data.

Digital signatures have the property of fixing and making the bit representation of electronic documents non modifiable. Thus, they provide an extreme assessment of the integrity of the data: if just a single bit of the signed document is modified (whether intentionally or unintentionally), the signature fails. However, "an authentication failure does not necessarily mean that the document is no longer reliable" [Bo07]. Even when the physical integrity of digital materials (e.g., the proper number of bit strings) is compromised, the articulation of the content (i.e., the meaning and function of the document that, in diplomatic terms, are conveyed by required elements of documentary form) can still be intact. The bit strings within the land registry database will most likely undergo some modification through, for instance, system migration, which at present is the most viable strategy to counteract the decay of electronic media and technology obsolescence. While such an event will not alter the conceptual integrity of the data, it will unavoidably undermine its physical integrity.

GILFAM, which is entrusted with the legal responsibility to provide access to the land registry in a fashion that preserves its evidential value "regardless of technological change", claims that the control mechanisms embedded in the software guarantee the necessary flexibility for any future system upgrades. However, at the time the case study was carried out, it was still unclear how that was supposed to happen without breaking the "digital seal" attached to each document stored in the system. In addition, the issue of preserving the functionality and, implicitly, the evidential value of digital signatures

[4] The control mechanism consists of two parallel, automated processes: 1) a top-down process, which traverses sequentially all of the ordonnances, verifying each digital signature and comparing each ordonnance with the relevant data registered in the system (the so-called "inscription"); and 2) a bottom-up process, which performs a similar function but proceeds from the inscriptions.

through technology evolution had not been addressed by the system administrators in any existing policy.

2.2 The Revenue On-Line Service Case Study[5]

The second InterPARES 2 case study dedicated to the analysis of a specific PKI environment refers to Revenue On-Line Service (ROS), the Irish Revenue's interactive application allowing tax agents, companies and other interested customers to file their tax returns online by means of a secure site facility. ROS is a pioneer in European Internet applications and has been championed as a high profile e-government product, receiving several national and international awards. It was promoted at the end of the 1990s as a means to reduce errors in tax returns and to contribute to the development of e-commerce, whose importance for the Irish and European economies has been strongly emphasised by the Irish government.

All correspondence between Revenue and its customers is encrypted by means of a PKI technology which involves a "key pair" consisting of a "private key", used by the ROS customers to create their digital signatures, and a "public key", used by Revenue in an asymmetric cryptosystem to verify the digital signatures thus created. ROS customers are identified by their digital certificates, whose function is also that of ensuring the identity, integrity and confidentiality of any submitted data.[6]

All of the ROS application's components, including its security system, were built using, to the degree possible, open industry standards (e.g., HTML, XML, UNIX) and off-the-shelf products, in order to: 1) minimize the footprint from the users' perspective (e.g., system is accessed via a standard web browser); 2) increase the interoperability of its components; and 3) facilitate the reuse of Revenue's existing frameworks and systems.[7]

In order to guarantee the highest possible level of security, Revenue has implemented stringent technological, physical and procedural security controls and obligations to minimize threats to its PKI. As to its employees, Revenue provides for an extensive Access Control System which, inter alia, restricts staff access to any submitted data and system components based on job responsibilities. Revenue has also declared the area

---

[5] The final report of the Revenue On-Line Service Case Study will be available in the forthcoming book on the InterPARES 2 findings [DP08].

[6] To ensure the integrity and security of all interactions with its customers, Revenue operates a PKI in association with LanCommunications/RSA Security that is in conformance with Recommendation x.509, a standard specification for digital certificates published by the ITU-T (International Telecommunications Union – Telecommunication). The entity responsible for managing the whole PKI is Revenue Certificate Authority (ROS CA), which is a self-signing certification authority. Thus, ROS CA acts as the highest point of trust in the Revenue PKI.

[7] The technical components play a critical role in ensuring the accuracy, reliability and authenticity of the records generated by the system. It would therefore be worth describing more in detail the technical characteristics of digital certificates, digital signatures, tax forms and debt instruction forms. However, for the purposes of this paper, it will be enough to mention that, despite the adherence to existing standards and use of open formats and off-the-shelf applications, the digital certificate is a proprietary file with structured data and a unique hash key.

where the servers and work stations are located "no lone zone", which means that all tasks carried out within this area require oversight from at least two PKI services employers.

From an analysis of formal statements of Revenue, it emerges that its PKI is mainly understood to provide a twofold protection of the authenticity of ROS digital entities, by ensuring, on the one hand, the identification and authentication of all communicating parties, and on the other, the non-repudiation of transmissions. Revenue regards the digitally signed records captured by ROS as acceptable as evidence in court, thanks to a "chain of authenticity" that involves the following steps: 1) users' identification and authentication by means of digital certificates; 2) validation by ROS of all submitted data; 3) retention, logging and archiving of all actions within ROS; 4) prevention of deletion or modification of data; and 5) time/date stamping of all actions within ROS.

What happens, though, when digital certificates – which have a fixed operational life of two years – expire? Revenue requires the expired certificates and relevant metadata to be retained for a minimum period of ten years, after which time they are transmitted to an external facility that is supposed to offer "secure archiving". However, the issue of technological change is never addressed in any of the ROS records management policies and procedures. Not only is there a need to establish a coherent strategy for the treatment of digital signatures, taking into account both legal and technical perspectives, but it also is unclear whether later ROS releases are technically backward-compatible, such that the system will, for instance, accept earlier versions of tax forms.

One of the conclusions reached by this case study is that while ROS does capture documentary evidence, Revenue has not, as yet, articulated a process for ensuring the adequate medium- to long-term preservation of its data and records. Revenue seems to concern itself exclusively with the initial phases of a record's life cycle, which, in this specific case, correspond to the phases of records generation and transmission. In other words, Revenue PKI certainly facilitates the transmission of authentic data into ROS but cannot be used to continue to confer authenticity. Back-end systems require additional elements to ensure that electronic records remain authentic through time, such as, for instance, internal controls and procedures illustrating the mechanisms by which data are removed from the "security wrapper" (i.e., an XML-based component that includes the entire transaction dataset received from the customers by ROS), ingested into ROS and processed. As the findings of other InterPARES research work have proved, the lack of a comprehensive recordkeeping policy is a rather common trait of numerous e-government initiatives as well as of the majority of today's record-related legislation in the world [DST08].

3 The Legislator's Approach

Between 2004 and 2005, the InterPARES 2 Policy Cross-domain carried out a study which examined the barriers and enablers to the preservation of electronic records found

in the legislation of a number of countries in Europe, North America and Asia [SFC05].[8] With reference to the European Union, the study focused on a set of laws classified as ICT/Information Society Legislation and including the directives on e-signature, data protection, e-invoicing, as well as another five ones relevant to "electronic communications networks and services". These directives – all issued under the aegis of European standards organizations – have the purpose of "establishing a legal framework to ensure the free movement of information society services between Member States", by removing fragmentation and enabling interoperability both internally and at the EU level [EU04a].

Most of the EU Member States have by now adopted new laws or amended existing ones according to the EU directives. In particular, the concept of an "advanced electronic signature"[9], which implies the use of cryptology-based technologies, has been adopted with no reserves, as the above examined InterPARES 2 case studies show. One may blame the pressure of the market on the administrators, the lack of knowledge on the part of the legislators, or the incapacity of the archival community to communicate effectively the risks deriving from adding to a record a digital component (the signature) that has a lifespan which is limited by the security of the technology used and may, therefore, differ from that of the record to which it is attached. The fact is that none of the laws examined by the InterPARES 2 Policy Research Team addresses this asymmetry [Fo07]; in fact, some, by imposing specific technical solutions that inevitably complicate the already difficult life of an electronic record, act as a real barrier to the long-term preservation of digital entities.[10]

The current Italian legislative framework concerning the management and preservation of digital records may provide an interesting example of the above. In order to facilitate the practical implementation of new dispositions conferring legal value to the records created or maintained in electronic systems [IT00], the body responsible for, inter alia, guiding and coordinating major e-government initiatives in Italy, called CNIPA[11], has issued "Technical Rules" that explain in detail how to preserve, "authentic copies" of electronic records, including signed ones [IT04]. On the one hand, in its deliberation, CNIPA acknowledges the fact that in the digital world one cannot preserve "original" documents but only copies, and that, because processes of migration occur constantly,

---

[8] The countries involved in the InterPARES 2 study on legislation were Australia, Canada (at the level of both national and sub-national jurisdictions), China, Hong Kong, Singapore, the United States, and, in Europe, France and Italy, as well as the European Union itself as a supranational entity. For more information on the InterPARES 2 Policy Cross-Domain, see at http://www.interpares.org/ip2/ip2_policy.cfm (last accessed 30 June 2008).

[9] According to the 1999 EU Directive on e-signature, an "advanced electronic signature", is an electronic signature that meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control; and
- it is linked to the data to which it relates in such a manner that any subsequent change of data is detectable.

[10] One of the policy recommendations formulated by InterPARES 2 refers to the necessity for laws, policies, strategies and standards to be "technologically neutral", in order to be effective and not to become a hindrance to the long-term preservation of digital materials [DST08].

[11] Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA).

archivists have to learn how to make adequate "substitute copies" of the records transferred to their custody. However, in practice, when it comes to prescribe the way for archivists to proceed in order to provide evidence of the correct execution of all these processes (i.e., transfer, migration, reproduction, etc.), instead of referring to any forms of annotation or descriptive metadata, CNIPA technical rules provide for digitally signing, and affixing a time stamp to, the entire sets of records that are subject to such processes. It is easy to predict that Italian archivists will soon realise how this authentication method is indeed an obstacle to their preservation duties.

4 Technical Responses

Although technological solutions to the problems raised by digital preservation are not always directly part of legislative provisions, technical specifications, requirements, standards and the like have often a considerable impact on the choices made by law- and policy-makers as well as on the practice of public and private record creating entities.

"Digital signatures are a solution that is predominantly based on technology" [Bo07]. The hashing of bit streams and encryption of hash codes depend on specific algorithms and software. Both are subject to technological obsolescence; however, they are both necessary for future validations of the digital signatures. Likewise, the digital certificates that are issued by Certification Authorities have a limited lifespan (e.g., two years, as we have seen with the Irish ROS) and may as well be revoked before they expire. Because records – even temporary ones – may be retained for a period of time that exceeds such validity time, authentication by means of a digital signature may become problematic. The "validation chain" that is implied by any PKI must remain available [DV02]. These are some of the "physical" issues that usually concern the IT research community.

In other words, IT and cryptology experts mainly perceive the threats to the long-term preservation of digitally signed documents to be, firstly, the unavoidable decay of signing algorithms due to scientific advances in cryptanalysis, and secondly, the availability over time of some signature verification software. As illustrated through the analysis of the InterPARES 2 case studies, this type of approach originates from a "physical" understanding of records' identity and integrity (i.e., the qualities of an authentic record) which has nothing to do with the "contextual" understanding of these issues that characterises the archival approach.

This "clash between two differing conceptions of electronic authenticity" [Bl06] makes any technical "solution" hardly satisfactory to the archival community. Archivists know – and not only with reference to electronic records – that the authentication function provided by a signature at "a point in time" cannot ensure authenticity "over time". In order to assess and protect the authenticity of a record, one must be able to establish its identity and to demonstrate its integrity by means of contextual elements, such as a set of rigorous procedural controls and a rich documentation (whether human- or computer-based) of the totality of the relationships entertained by the record throughout its life cycle.

We will not dwell upon any detailed description of the numerous technical responses that have lately been put forward (from "late validation" formats and time stamping procedures, to canonicalization and other mechanisms that to-be-established "trusted service providers" should be able to offer in the near future). What may be worth mentioning here is that the various standardisation efforts that EESSI (European Electronic Signature Standardization Initiative), ETSI (European Telecommunications Standards Institute), IETF (Internet Engineering Task Force) and other web consortia have made to find a solution to the challenge of the long-term preservation of digitally signed records, have created such a multi-layered infrastructure that it does not come as a surprise if the European market for e-signature products and services has not been flourishing as expected.[12]

5 The Archivists' Dilemma

Because cryptographic techniques freeze the signed document in its original state, forever forbidding any modification that would entail the inevitable failure of the signature verification process, archivists face a dilemma when confronted with the preservation of both document and digital signature legibility over the long term. To ensure the first, at present, the most promising strategy seems to be migration, which necessarily alters the bitwise integrity of the document. Thus, various research projects (e.g., InterPARES), archival standards (e.g., the Dutch ReMaNo) and archival institutions (e.g., Library and Archives Canada, the United States National Archives and Records Administration, the National Archives of Finland) suggest the digital signature be detached from the document upon receipt and after verification of authenticity, thus well before the first migration occurs.

The position of InterPARES is clearly spelled out in its "Creator Guidelines", where recommendation no. 6 reads: "You should, when you receive a document with an attached digital signature, detach the signature whenever possible and add information to the integrity metadata to indicate that the document had an attached digital signature when received, and that the signature was verified, detached, and deleted"[13].

However, the process of detaching the digital signature presents a few difficulties. First of all, some argue that a procedure that removes signatures and only stores traces of the validation process may not be acceptable in all and every context [ØS02]. The level of trust existing between the counterparts in a transaction (e.g., a bank or some public service may be examples of environments requiring the archiving of the signed

[12] As one may read in a document regarding the "eEurope 2005 Action Plan", "a number of issues remain on the legal and market aspects of the application of the Directive [on e-signature]. Firstly, there is currently no market demand for qualified certificates and related services. Secondly, greater interoperability of e-signatures is called for by the Directive as necessary to achieve the wide spread-use of electronic signatures and related services" [EU04b].

[13] InterPARES 2 Project, Creator Guidelines. Making and Maintaining Digital Materials: Guidelines for Individuals", 2007. Available online at http://www.interpares.org/display_file.cfm?doc=ip2(pub)creator_guidelines_booklet.pdf (last accessed 30 June 2008).

document), the document typology (e.g., for legal reasons, the original signature must sometimes be preserved), the delegation of the archival function to some external party (e.g., outsourcing of the archives service may diminish the level of trust in the procedures employed) may be alleged as reasons for keeping the digital signature.

Second, when and how to proceed with removing the signature is not sufficiently described at present. Should the process occur when the document is first saved to a file or to a current record system? Or should it rather happen when the document is no longer active? Before migration or before transfer to a historical archives? To ensure that such removal will not undermine the trust of those who signed the document and those who will use it in the future, it is necessary to make clarity on all these aspects. This issue calls for further research from both a technical and a methodological perspective.

What is on the contrary quite clear, at least to the archival community, and should not therefore be questioned – as it happens to read in some more IT-oriented works – is the role of the archivist as "trusted third party" with reference to the preservation of authentic electronic records that have once been signed digitally, whether the digital signature will be kept or removed at some point in time. We believe that if the archivists, or better, "designated records preservers"[14], are up to their traditional role of trusted custodians (which implies that they must have the necessary expertise and equipment to perform their functions), there is no need to call for "services that offer 'electronic vaults', where users may deposit electronic documents that they need to archive", or to identify such a service with a notary [ØS02].

Finally, instead of suggesting (like the above-mentioned Italian regulation does) that archivists should sign the sets of documents that are transferred to their custody by means of digital devices in order the preserve them authentically, policy-makers should better refer to a well-established archival method, that is, archival description. As InterPARES 2 has reminded us, it has always been a function of archival description to authenticate the whole of the documents transferred to an archives and to perpetuate their administrative and documentary relationships. In the digital world, this method has become even more critical, in that, given our inability to preserve an "original" document, the archival description is the primary source of information about the history of all the reproductions and changes that have affected the document over time and of the interrelationships among the records. The events of signature creation and use, as well as the traces of any validation process, including information on relevant digital certificates and certificate issuers, should be part of the contextual metadata accompanying the document throughout its active life. The latter (also known as recordkeeping metadata) should later be added to the archival description, which occurs in the archives and is to be seen as the "collective attestation of the authenticity of the documents and their relationships" in the context of the archival corpuses of materials to which the documents belong [DST08].

[14] According to the InterPARES definition, "the designated records preserver is the entity responsible for taking physical and legal custody of and preserving (i.e., protecting and ensuring continuous access to) a creator's inactive records" [DST08].

6 Conclusion

Records managers and records creators who are involved in e-government and e-business transactions, records preservers who are entrusted with the preservation of the evidence of those transactions, judges who have to assess the admissibility of digitally signed documents in courts, and notaries who are requested to decide on the formalities of a transaction often rely on different values, and thus have different perceptions of trusted situations. All of these diverse "cultures of trust" look for clear rules and best practices.

If it is true that, technically, the long-term storage of digitally signed documents cannot be relied upon for more than ten years [ØS02], it is also true that ten years may be enough for most practical purposes. Therefore, we cannot probably dismiss the currently available technologies nor, as archivists, ignore the attempts made by our IT counterparts with the aim of solving the problem of the long-term preservation of digital signatures.

A constructive dialogue between all involved "communities of practices" is indeed necessary and urgent, in order to avoid that the over-complexity of technical solutions and fragmentariness of legal instruments escalate to a point that the usefulness of the digital signature as a means of authentication is undermined.

Bibliography

[Bl06] Blanchette, J-F.: The Digital Signature Dilemma. Annales des Télécommunications, May-June 2006.

[Bo07] Boudrez, F.: Digital Signatures and Electronic Records. Archival Science, 2007; 179-193.

[DP08] Duranti, L.; Preston R. (eds.): InterPARES 2: Interactive, Dynamic and Experiential Records, Roma, ANAI, 2008 (forthcoming).

[DST08] Duranti, L.; Suderman J.; Todd M.: InterPARES 2 Project – A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records, 2008. Available online at http://www.interpares.org/ip2/display_file.cfm?doc=ip2(pub)policy_framework_document.pdf (last accessed 30 June 2008).

[DV02] Dumortier J.; Van den Eynde S.: Electronic Signatures and Trusted Archival Services. In: Proceedings of the DLM Forum 2002, Barcelona 6-8 May 2002. Luxembourg, Office fir Official Publications of the European Communities, 2002.

[EU99] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. In: Official Journal of the European Communities, L 13, 19 January 2000.

[EU04a] Communication from the Commission to the European Parliament and the Council on the role of European standardization in the framework of European policies and legislation, [SEC(2004) 1251] (Text with EEA relevance)/*COM/2004/0674 final*/.

[EU04b] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – eEurope 2005 Action Plan: An Update. [SEC(2004) 607-608] /* COM/2004/0380 final */.

[Fo07] Foscarini, F.: InterPARES 2 and the Records-Related Legislation of the European Union. Archivaria 63, Spring 2007; 121-136.

[IT00] President of the Republic Decree No. 445/2000 of 28 December 2000: Single Text of legislative and regulatory provisions regarding the administrative documentation [DPR

445/2000: Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa].

[IT04] CNIPA Deliberation No. 11/2004 of 19 February 2004: Technical Rules for the reproduction and preservation of documents on digital media which are suitable to guarantee the creation of authentic copies [Regole techiche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformita' dei documenti agli originali].

[ØS02] Ølnes, J.; Seip A.B.: On Long-Term Storage of Digitally Signed Documents. In: Proceedings of the Second IFIP Conference on e-Commerce, e-Business, e-Government (I3E). Kluwer Academic Publishers, 2002.

[SFC05] Suderman, J.; Foscarini, F.; Coulter E.: InterPARES 2 Project – Archives Legislation Study Report, 2005. Available online at http://www.interpares.org/display_file.cfm?doc=ip2(policy)archival_legislation_study_report.pdf (last accessed 30 June 2008).