Traces and events: On the evidential value of electronic records and signatures

Jean-François Blanchette
Department of Information Studies
University of California, Los Angeles
Los Angeles, CA 90005-1520
Tel: +1 310 267 5137; Fax: +1 310 206 4460
Mél : blanchette@ucla.edu
http://polaris.gseis.ucla.edu/blanchette/

Bruno Bachimont
Université de Technologie de Compiègne
UMR CNRS 6599 Heudiasyc
BP 20259 60205 Compiègne cedex
Tél : 33 3 44 23 49 74 /
Mél : bruno.bachimont@utc.fr
http://www.utc.fr/~bachimon.html

Presentation: Verbal presentation with Powerpoint
Keywords : Authenticity, integrity, evidential value of electronic documents, electronic signatures, cryptography.

The very fluidity that makes e-commerce potentially so enormous, its ability to seamlessly cross over borders and traditional market boundaries, is also its greatest liability: How can parties establish trustworthy relationships in shifting environments, characterized by the absence of traditional methods for establishing identity, commitment, evidence, and trust? In the world of paper-and-ink contracts, these objectives are typically achieved through the use of a most mundane technology, handwritten signatures.

A primary purpose of signatures, be they traditional, handwritten, ones, or based on esoteric mathematical algorithms, is to serve as instruments of law, as the preferred instrument for parties to manifest their consent and provide a mechanism for establishing intent. Signing is, of course, within most legal texts, understood to be concomitant with the use of paper as the instrumentum, the physical means whereby contractual agreements are inscribed, preserved, and, most importantly, exhibited during disputes. The last 10 years have thus seen an enormous amount of doctrinal, technological, and legislative activity aimed at designing a proper electronic equivalent to handwritten signatures and ensuring the authenticity of electronic records — in the US alone, the Food and Drug Administration, the Securities and Exchange Commission, the Environmental Protection Agency, the Federal Government and most States have reforming the rules governing admissibility of electronic records as evidence.

One proposed design, that of electronic signatures founded on cryptographic techniques, has succeeded over other solutions to the point where, in certain legal systems, such as those of the Member States of the European Union, electronic signatures are almost exclusively understood to be inevitably "digital signatures", that is, based on cryptological solutions, more specifically, public-key (or asymmetric) cryptography.

However, the efforts of the legal and technological community at enshrining digital signatures as the exclusive substitute for handwritten signatures has not met with its expected success on at least two fronts: on the one hand, predicted markets for digital signature technologies and public-key infrastructures have largely failed to materialize; on the other hand, the archival community, the very community historically entrusted with the care and preservation of documentary evidence, has expressed profound ambivalence at the prospect of preserving digitally signed records.

This paper argues that discrepancies between technical, legal and archival responses to the problem of long-term preservation of digitally signed documents are founded on diverging understandings — *physical* vs. *contextual* — of electronic authenticity. The paper reviews the evolution of these two divergent notions of electronic documentary evidence as they have been expressed through various laws, and regulations. It argues that, as archivists have long known, *no evidence is ever self-intelligible*, and that in order to be a "competent witness" of a juridical fact (commitment to obligations), electronic writing must be accompanied by the traces recording all of the operations which a document is susceptible to incur: creation, modifications, annotations, signature, conversion, transmission, etc. Likewise, digital signatures are unable to testify *in and of themselves* of the identity and integrity of a document, and to be effective, must also be accompanied by numerous traces that testify to their own identity and integrity as evidence — revocation lists, certificate chains, audit trails, etc.