Strong Authentication in the .eu ADR Rules

Report by Chris Reed
Professor of Electronic Commerce Law

Queen Mary
University of London

This Report has been prepared for the Czech Arbitration Court. Its purpose is to analyse the proposed introduction of the concept of Strong Authentication in the .eu ADR Rules to determine whether the implementation of the concept will provide authentication of submitted documents which is at least as good as the authentication provided by hand-written signatures. For the sake of completeness this Report also compares Strong Authentication with advanced electronic signatures based on qualified certificates.

1 Hand-written signatures

A hand-written signature authenticates a hard copy document in three respects:

1. It provides evidence of the identity of the person who signed the document, on the assumption that hand-written signatures are unique to each signatory. If a hand-written signature is alleged to be a forgery, expert examination of the signature can provide an assessment of how likely it is that the signature was forged.

   It is relevant to note that, unless the signature is already known to the recipient of the document, the recipient is in fact relying on the sender's self-certification of his or her identity. If the person who is asserted to have sent the document denies that he or she did so, the signature provides a mechanism for checking that matter at a later date.

2. It provides evidence that the signatory agrees to and intends to be bound by the content of the document. This evidence derives from the law's assumption that all signatories are aware of the convention that signing a document shows their agreement to it and intention to be bound by it.

3. It provides evidence that the document has not been altered since it was signed, on the basis that alteration of the text would be detectable as it would make physical changes to the hard copy. This evidence is weaker in the case of multi-page documents unless each page is signed.

It is important to note that a hand-written signature does not prove any of these matters conclusively. However, it provides sufficiently good evidence that the hand-written signature has been accepted for hundreds of years by courts, public bodies and private individuals as an appropriate authentication method for documents.

2 Strong Authentication

The concept of Strong Authentication in the proposed change to the ADR Rules is based on well-known concepts of strong authentication in computer security. It is standard practice to achieve strong authentication by requiring the communicating party to provide two different pieces of authentication of different types: in this case these are the user password (something known) and the one-time password generated via the Bingo card (something possessed). The Bingo card is functionally equivalent to the electronic tokens commonly used for applications such as electronic banking, and if produced in a secure manner is capable of producing an equally secure one-time password.

Strong Authentication as proposed would produce the following evidence:

1. Evidence of identity will be derived from the combination of the self-identification of the document sender when registering, coupled with receipt of the Bingo card by a secure method at the registered address. If the secure delivery method for the Bingo card requires a hand-written signature from the recipient, that hand-written signature will be further evidence of identity.

   If, as is likely in many cases, the party to ADR proceedings is an organisation rather than an individual, the signature on receipt of the Bingo card may not be that of the individual who is conducting the proceedings. However, the combination of delivery to the organisation's address with the hand-written signature of a person authorised by the organisation to sign for deliveries will be strong evidence that the organisation is the originator of communications using Strong Authentication. The legal question in these cases is whether the organisation is responsible for the communication, not whether a particular individual can be identified, and Strong Authentication provides good evidence of the identity of that organisation.

   Just the same as for hand-written signatures, as explained in section 1 above, Strong Authentication does not establish the identity of the communicating party in advance, but provides an equivalent method to confirm that party's identity in the event of later dispute. It might be possible to derive evidence in advance by making a check from third party sources that the registered address corresponds to the individual or organisation identified during registration – such evidence might come from e.g. trade or telephone directories. However, a system to collect such evidence would be difficult to implement across national boundaries, and is not necessary if the aim is to provide equivalent identification to that provided by hand-written signatures.

2. Evidence that the communicating party agrees to and intends to be bound by the content of the document is derived from the process which requires the communicating party to log in to the online platform and confirm the accuracy of

the documents previously uploaded. This is an express confirmation of these matters by the signatory, and is thus stronger evidence than the implied confirmation provided by signing a document with a hand-written signature. Most countries' laws permit in some circumstances a signatory to deny that a hand-written signature procured by e.g. deception was a valid demonstration of agreement or intention to be bound.

3. The confirmation process also provides evidence that the document has not been altered since it was uploaded, or that the correct document was uploaded, or that the upload was not made by some other person. The communicating party is stating expressly, as set out in the ADR Rules, that he or she has checked the document content. Even if this statement is untrue, and no check was in fact carried out, the law in common law countries would estop the communicating party from denying that the check was made. I am not competent to comment on the laws of other countries, but would expect that similar legal principles would apply.

   Requiring the confirmation in a two-stage process via separate SSL sessions is a useful precaution against interception by hacking, and is thus stronger evidence on these points than would be derived from the single-stage process of applying a hand-written signature.

3 Advanced electronic signature

Advanced electronic signatures based on qualified certificates as defined in Directive 1999/93/EC on a Community framework for electronic signatures provide stronger evidence than either hand-written signatures or Strong Authentication in two respects:

1. The identity certification process is conducted by an independent third party in advance, and based on reliable third party documents such as identity cards or passports. It thus provides reliable evidence in advance as to the identity of the electronic signatory.

2. Evidence that the document has not been altered derives from the strength of the encryption processes involved, and it is certainly easier to alter a document signed by hand than to alter a document signed with such an electronic signature. Strong Authentication requires the communicating party to check the document content, and in my opinion this provides evidence which is nearly as strong as, perhaps even equivalent to, that provided by electronic signature.

Electronic signatures provide exactly the same evidence that the communicating party agrees to and intends to be bound by the content of the document as do hand-written signatures, being based on the assumption that every signatory knows the consequences of signing. Because Strong Authentication requires a communicating party to confirm

these points expressly, it is even stronger evidence than an electronic signature on these matters.

4 Conclusions

From the analysis above, I have formed the opinion that Strong Authentication provides authentication evidence that is at least as strong as that provided by documents signed with a hand-written signature. Evidence of identity is perhaps a little weaker in the case of private individuals, but rather stronger in the case of organisations. Evidence of agreement and intention to be bound, and that the document is unaltered, is distinctly stronger in the case of Strong Authentication.

If the technical and operational procedures adopted for Strong Authentication comply with standard practices in the computer security field, my view is that Strong Authentication is functionally equivalent to, or even better than, hand-written signatures for the purpose of authenticating documents.

Although advanced electronic signatures provide stronger authentication, the difficulties for parties to ADR in obtaining and managing such signatures are substantial. In my opinion, it would be entirely appropriate for the .eu ADR Rules to adopt Strong Authentication as an approved method for authenticating documents uploaded for ADR proceedings.

Professor Chris Reed, 25 January 2008