CAC UDRP pilot project

Report by Chris Reed
Professor of Electronic Commerce Law, School of Law

1

This Report has been prepared for the Czech Arbitration Court ("CAC"). The views expressed are those of Professor Reed in his personal capacity.

The purpose of the Report is to provide an opinion on the legal compliance of the proposals in the pilot project with the formal requirements of the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules") and with general legal principles applicable to dispute resolution and evidence in such proceedings.

1 Simplified submission of hard copies of Complaints and Responses

Under the Rules, Complaints and Responses are required to be submitted to the Provider in hard copy form as well as in electronic form (paras 3(b), 5(b)), together with a declaration in the prescribed wording signed by the Complainant/Respondent or its authorised representative (paras 3(b)(xiv), 5(b)(viii)). These are the only requirements of form with which such submissions must comply.

The pilot project proposes that compliance with these rules should be achieved by electronic transmission of the relevant documents making up the Complaint or Response to a Service Center to be established by CAC. The Complainant/Respondent will check the accuracy of these documents online, and when satisfied will ask the Service Center to lock the document file and generate a signature page. That signature page will declare that each submitted document is accurate and contain the declaration required by para. 3(b)(xiv) or 5(b)(viii) as appropriate.

The Complainant/Respondent will then print out the signature page in the required number of copies, sign them, and send the signed copies to the Service Center. When they are received, the Service Center will print out the locked document file in the appropriate number of copies, attach to each set a signed signature page, and submit the whole to the Provider on behalf of the Complainant/Respondent.

In my opinion, submission of Complaints or Responses in this way will comply with the formal requirements of the Rules. The Service Center will as a matter of fact be the Complainant's/Respondent's agent for the purposes of printing out the documents and submitting them to the Provider, and for the avoidance of doubt could formally be appointed as such by an online agreement when the Complainant/Respondent first

submits documents to the Service Center online. The signature page containing the prescribed declaration will actually have been signed by the Complainant/Respondent, and there is no requirement under the Rules for any other document to be signed. Thus the requirements of the Rules for submission to be in the form of hard copy accompanied by a signed declaration will have been met.

2 Secure online filing and hard copy delivery

The proposal here is to accept online filing of document under Strong Authentication (as described in Annex 3 of the pilot project document), and then for the Service Center to print off, certify, sign and deliver hard copy.

In my opinion, the submission of documents electronically using Strong Authentication provides authentication evidence that is at least as strong as that provided by documents signed with a hand-written signature, as explained in sections 2.1 and 2.2 below.

Electronic submission is, however, incapable of meeting the requirement of the Rules that the appropriate declaration is delivered as signed hard copy. This would be overcome by the Service Center signing the hard copy as the authorised representative of the Complainant/Respondent. This *would* comply with the Rules if the Service Center were properly authorised to act as such a representative. Authority to sign in this capacity would be conferred by the online agreement referred to in section 1. In all the common law jurisdictions of which I am aware, such an online agreement would confer on the Service Center the necessary authority to sign as agent. I am not, however, able to state with certainty that the laws of other jurisdictions would necessarily allow authority to be conferred by means of an online agreement. This issue could easily be resolved by making the online agreement subject to the law of the jurisdiction in which the Service Center is established, which would be a natural choice of law for such an agreement, provided that the applicable law permits authority to act in this way to be conferred via an online agreement. On the assumption that the Service Center would be established in the Czech Republic, the relevant law would be Czech law. I am informed by the CAC that Czech law permits authority to be conferred in this way.

2.1 The limits of 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 such 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.

2.2 Strong Authentication

Strong authentication meets the most common legislative requirements to constitute an electronic signature[1] because it provides the necessary evidence of the identity of the signatory, intention to be bound and non-alteration of the document. It further provides evidence which is functionally equivalent to, or in some cases stronger than, the evidence provided by a hand-written signature.

The concept of Strong Authentication in the pilot project 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 PAC card (something possessed). The PAC 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.

[1] For example, it meets the requirements of the US Electronic Signatures in Global and National Commerce Act 2000 section 106(5) through being a "process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record". It also complies with Article 2(1) of the EU Directive 1999/93/EC on a Community framework for electronic signatures, which defines an electronic signature as "data in electronic form which are attached to or logically associated with [the document to be signed] and which serve as a method of authentication".

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 PAC card by a secure method at the registered address. Because the secure delivery method for the PAC 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 UDRP proceedings is an organisation rather than an individual, the signature on receipt of the PAC 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 2.1 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 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.

2.3 Conclusions on Strong Authentication

From the analysis above, I have formed the opinion that Strong Authentication provides authentication evidence that is equivalent to or better than that provided by documents signed with a hand-written signature. Evidence of identity is at least as strong in the case of private individuals, because the individual is required to give a hand-written receipt for the PAC card, and 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. I also take the view that it amounts to an electronic signature for the purposes of most e-signature laws, including the EU Directive which would be applicable to the CAC and the Service Center.

3 Status of the Service Center

The pilot project document states:

> The Service Center may be a department of the CAC or it may be a separate legal entity located at the CAC‘s premises.

This is a decision to be taken once the results of the pilot project are known.

If the favoured option is that the Service Center should be a department of the CAC, a number of potential issues will need to be considered. These issues would not arise if the Service Center were established as a separate legal entity.

1. **Liability.** There is a potential for liability claims by a Complainant/Respondent if the Service Center fails to submit the documents as authenticated (e.g. submitting an earlier version of some document because of system error). This liability would need to be defined and controlled by the agreement between the Complainant/Respondent and the Service Center. The question whether the

potential for liability claims creates a reputational risk for the CAC in its role as Provider also needs to be considered.

2. **Due Process.** The potential for liability claims discussed in the previous paragraph gives the CAC a theoretical incentive to allow the amendment of incorrect submissions rather than rejecting them, where a rejection might give rise to a liability claim. Such a potential conflict of interest might be contrary to the accepted principles of due process. Amendments to the constitution of the CAC, or appropriate language in the agreements between the CAC and the Complainant/Respondent, would need to be considered in order to address this issue.

3. **Rules compliance.** Paras 3(b) and 5(b) of the Rules require the documents to be submitted to the Provider in hard copy. If the Service Center is a department of the Provider, it might be arguable that printing out of hard copy by the Service Center and submission to a different CAC department is not a proper submission, because the documents will never have been received by CAC in hard copy as required by the Rules. This is not to say that such an objection would be valid, but thought needs to be given as to whether this issue needs to be resolved, and if so whether it can be addressed via the terms of the agreements between the CAC and the Complainant/Respondent.

Professor Chris Reed, 18 June 2008