Authentication and Digital Signatures

Message posted to the Temple University School of Law E-mail List on Digital Signatures
By Daniel Greenwood
Thursday, 27 March 1998

Chas (and the members of the list)

I frankly don't have a strong opinion about what definitions end up being generally used in law and practice - but I certainly agree that the concepts of technical authentication and legal signatures need to be kept separate (though they become related in real deployments). For this post, I will use the definition of authenticate that you put forward and the definition of signature used in the November Uniform Electronic Authentication Act ("Signature means any symbol, sound, process or encryption of a record in whole or in part, executed or adopted by a person or the person's electronic agent with intent to (i) identify the party; (ii) adopt or accept a term or a record; or (iii) establish the information integrity of a record or term that contains the signature or to which a record containing the signature refers.").

You said:

>I think it is useful in drafting rules and talking about the subject, to keep the concept of intent consciously separate from the
>more *objective* concept of "authentication". To me, "authenticate" without expressing an object means to "authenticate
>identity". I also think that with an express object provided, the word tends to fit well with "authenticate identity of the
>signer," or "authenticate integrity of a message or record".

Given the fact that this list relates to digital signature law, I would like to further explore your point about making rules. While I have participated in the construction of technical systems that require the objective capacity to authenticate identity of a network user or device, I have frankly not seen any advantage in drafting rules (either statutory, regulatory or contractually based) that presume to bind or hold a party to the contents of a message without direct reference to the second definition of signature from the ETA draft. Here is what I am getting at: what is the definition of the term "digital signature?" If it merely comprehends authentication, then no rule based scheme that would create a binding presumption or attribution of intent on the purported signer to be bound by particular terms or records would seem logical or fair. If, on the other hand, the term includes the concept of agreement to be bound or to accept a term or record, then:

1. would the mere presence of authentication technology in any way assure the intent needed for a signature (using the second ETA definition), and

2. would not the presence of UDAC type contextual cues, direct notice of implications and gravity prompts be a welcome and important functional addition to the use of PKI-based digital "signature" systems for the creation of legally enforceable signatures?

The definition of a digital signature in the Utah Act, for example, reads:

"a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether:

(a) the transformation was created using the private key that corresponds to the signer's public key; and

(b) the message has been altered since the transformation was made."

This seems to be a very good example of the narrow concept of authentication that you mention in your post. Looks a bit weak in the signature (definition two) department though . . . Are we sure we want to bind people to that alone? Or, is it necessary to look to other interface and/or extrinsic contextual factors in order to assure the *subjective* element of intent is present? Relegating the term intent to the category of "subjectivity" should not mean ignoring the fact that it is legally required, commercially important, and socially valued for many of the online interactions digital signatures claim to enable.

A good point regarding the GSA procurement was made on this list, distinguishing between authentication for access control and authentication meant to form part of a binding signature. In my experience, using authentication for access control is usually bounded merely by a requirement for the first and sometimes the third) signature definitions of the ETA draft. The intent portion the under girds the authentication for access control occurs on the part of the controller at the time when a decision is made to permit a given user or device entry access (often premised upon organizational role, authorization, or legal right to data). But again, this does not let digital signatures off the hook. Use of PKI for access control in implementations like SSL3 do not really use a digital signature. Rather, it merely checks a certificate against a pre-approved list of access enabled entities and allows or rejects access thereupon. S/MIME comes a lot closer.

My questions for Chas, and the list as a whole, are this:

what technical protocols and other application or practical elements need to be present to assure intent for purposes of creating a valid, binding enforceable electronic signature? There are, for example, some notice screens that are tripped by use of S/MIME in Netscape. Is that really enough? How do we need to do better in order to create implementations that rise to the real business challenge of signatures in cyberspace? What is the relevance of the proposed UDAC in this regard? Does it respond to the need well or is it missing something? In short: What is missing, how can it be deployed and how well does it scale to an infrastructure solution?