Interface Infrastructures: More Than a Digital Signature

Message posted to the Temple University School of Law E-mail List on Digital Signatures
By Daniel Greenwood
Thursday, 26 March 1998

Based upon Ben Wright's recent postings on the proposed Uniform Document Authentication Component (UDAC), this list has begun an exploration of the softer but no less important issues of context, cues and agreement that surround usage of electronic authentication. Ironically, perhaps, I think the best application of this type of ceremonial technical component would be coupled closely with PKI based authentication mechanisms. For those applications that require agreement to terms (any contract, license, filing, application, registration, etc.) such a component would greatly enhance the effectiveness of a raw digital signature. I posit that merely including links to pages of disclaimers and volumes of notices is not sufficient. Rather, we need a simple, comprehensible interface environment to support the human element of electronic interactions. I believe that the legal issues flow from the human behavior - not the other way around. (at the end of this message is an excerpt from an article I wrote last November on this topic)

There are a number of transactions where a solemnity requirement is "built in" legally. Enfeoffment (passing the twig to signify the purchase of land) was a great example. Some on this list have also cited things like marriage agreements, wills and "Kevorkian agreements" (is there a connection here? ;) Lets take all those applications as clear cases of the helpfulness of Ben's proposed ceremonial technical component. In addition to all of those clear cases, I think there is a broad range of other non solemn or less high value electronic interactions where such a component would be really useful - perhaps even necessary.

To my mind, one of the major difficulties remaining for electronic commerce and online government is the absence of intuitively comprehensible methods for knowing "where" we are, "what" we are doing and "who" we are doing it with in cyberspace. The book "City of Bits" by William Mitchell does an excellent job of detailing the rich combination of environmental cues, clues and general context that surrounds most human activity in physical space. When we are in a bank we know we are in a bank. When we sign a contract, it is clear that something important is happening. When we are in a government office getting information, or walking into a pub to order a beer and so on, the behavioral expectations and predictability of outcomes are quite well established. The current state of the art in electronic interaction systems is crude indeed by comparison. I co-teach a course Bill Mitchell that deals with some of these issues called "Designing Electronic Commerce and Online Government." The URL is for this semester is: http://architecture.mit.edu/class/4.195/ Interestingly, this course deals with legal and policy issues - but it is situated within the School of Architecture and Planning at MIT (however, so is the MIT Media Lab - so the multidisciplinary effort is not unprecedented).

Most behavior is self regulating and not forced by rule of law or other external compulsion. People need context and experience in an environment in order to interact effectively. The act of submitting a form or agreeing to terms or communicating on a list are all small expressions of a wider contextual set of transactional expectations and behavioral norms. When dealing with people in an online environment, it can be helpful to consider the "space" in which the interaction is taking place. By today's usual computation methods, we are probably talking about a physical restriction of a screen on a monitor. Beyond that, we quickly get into issues of User Interface design. The psychological aspects of this type of design are complex. It can be hard to know what people are thinking when they use a given system. What do they think the buttons do? What do they think the point of the system is supposed to be?

When we speak with people face to face, several misunderstanding can occur, without the benefit of body language and other such cues, the incidence of systems and users "talking past" each other spikes up. What does the button "OK" mean? What might be the result of selecting one of several items from a pull down menu and hitting something that says "submit" (will it mean I submitted a request for information with no obligation or that I submitted to the will of some powerful party that will now send me bills or otherwise hassle me?).

The discipline of architecture and planning has long dealt with these types of issues. The design of physical space has a serious component of psychology. The space is designed and built for the users who will traffic it. The users who create network traffic into an online system are seldom so lucky. We need more creative tools like the one Ben Wright is proposing to help us build the types of electronic commerce and other online environments that will be necessary to support the important activity people would like to carry on in cyberspace.

In my view, important activity is not restricted to such items as wills and sales of land. The sum of fifty smaller transactions, like subscriptions, orders of products and transmittals of government forms are all important enough to warrant a closer examination of the interface infrastructures that support them. I use the term "interface infrastructure" because I hope it conveys the idea that disputes will not only be based on the question "was it YOU who pressed this button" but will also (perhaps more often) derive from the assertion "I remember being on your site, but I never agreed to X!" The meaning of unfair and deceptive practices in the physical world is still subject to significant dispute. How much worse do we expect it will become via online channels unless our interface infrastructure is based upon widely accepted and understood mechanisms representing agreement to terms, personal identity, indication of "where" one is (e.g. what organization runs this server? Is this Fleet Bank or Microsoft?) including an indication of what jurisdiction one is operating (if I fly to Iran, and say or buy or do something, then I have a good idea under what jurisdiction and norms I am operating -

how do I get that information in a reliable, simple to understand method from my online environment?). I use the term infrastructure because I believe that ubiquitous usage of online technologies in open network environments will require widely accepted Interface norms - such as a UDAC. The gravity prompts and other systemic functions built into this component can provide a sound starting point for getting to the next level of wide spread deployment of interactions online.

==========

The following is an except from the short article: "Federal Case Indicates the Need for Information Age Reforms in Business, Policy and Law " available at: http://www.tiac.net/biz/danielg/kaspar9.htm

As more transactions take place electronically, including transaction that will require some solemnity, the question should be: how shall we express enfeoffment electronically? Enfeoffment was the act of going to the land and handing over a twig ceremonially in front of witnesses to signify the purchase and sale of land. This act was done to solemnify the transaction. The policy behind this solemnification was, in part, to assure there was no mistake about the nature and gravity of the transaction. How should such solemnity be achieved via communication technologies that allow for remote parties to transact business?

When some people indicate that this is a security issue I feel that is like saying: building a house is a hammer and nails issue. In the first place, we have an architectural question: what design requirements exist to create a structure that serves the purpose and won't fall down when pushed? Then we use the available tools to construct it. In this case, we construct an interface, application, network and records management environment that is replete with appropriate practices and agreements). What are the minimum requirements of this environment? There will almost certainly be a need for security dimensions as well. However, here, the mere "signature" and "writing" requirements are not met by secure systems but by understandable systems.

=========

Link to a paper on the Uniform Document Authentication Component (UDAC)
http://ourworld.compuserve.com/homepages/Ben_Wright/ceremony.htm