NR_key_name:	8AAFC0D2F73B50A1852564740071B2D2
SendTo:	jrmilch @ kodak.com ("MILCHJAMES") @ INTERNET @ WORLDCOM
CopyTo:	
DisplayBlindCopyTo:	
BlindCopyTo:	CN=R ecord/O=ARRB
From:	CN=David Marwell/O=ARRB
DisplayFromDomain:	
DisplayDate:	04/09/1997
DisplayDate_Time:	4:42:44 PM
ComposedDate:	04/09/1997
ComposedDate_Time:	4:41:53 PM
Subject:	Re: Query

Body:

Many thanks, Jim. I look forward to getting the fax.To:David_Marwell @ jfk-arrb.gov @ Internetcc:(bcc: David Marwell/ARRB)From:jrmilch @ kodak.com ("MILCHJAMES") @ INTERNET @ WORLDCOM Date:04/09/97 04:06:32 PM CDTSubject:QueryTo: DAVIDMA7--INTERNET
*** Reply to note of 04/08/97 18:06 From: Jim Milch ISD LXJ600 ext. 89400 1/65/RL Subject: Query Thanks for your note. I will fax to you a nice description of the differences among "privacy" "authentication" "non-repudiation" and "integrity" which was written by Northern Telecom. This will give you a sense of the different kinds of digital security. The essential aspect of authentication is the concept of a "hash" or "digest" of a digital file. It is a short message (for example, 16 bytes) which is uniquely determined by the entire content of the file. If any bit is changed in the file, the digest will change. It is very difficult to find a set of bits to change in the file which will restore the digest to its previous value. There are standard/proven methods of calculating the digest of a file. Now the challenge is to deliver the digest reliably to the user.One method is discussed in the NT brochure--use public/private key encryption to encrypt the digest and attach it to the file itself. Another way is to store the digest in a public place (like a web server) which everyone can get to without uncertainty.The first method is preferred if the file has a long lifetime and a self-contained solution is needed. In both cases, Joe can authenticate the file in his hands by using the standard method of calculating the digest and comparing it to the stored/ published digest.
I have asked for a more complete description of this from our experts--if I get more, I will send it to you.
::: Regards, Jim
:::

recstat:	Record
DeliveryPriority:	N
DeliveryReport:	B
ReturnReceipt:	
Categories:	