On the End of Paper Based Communication

Perry Alexander, Director, Information and Telecommunication Technology Center (ITTC), University of Kansas

The post-PC world is upon us. On Christmas Day, 2011, the number of tablet computer owners in the world doubled. Apple consumes more silicon than any company on earth, yet it controls only 12% of the PC market. Physical media for music and video are antiques and printed media is next. I have not printed a single technical paper since purchasing my iPad a month after they came out. I have not visited a physical library in over 10 years.

We are consuming more information in more ways than ever in our history. Information is ubiquitous and always available. The industrial revolution snatched up our information infrastructure and made its products commodities. Specialized tools targeting specific types of information and consumers are replacing general purpose desktop PCs at a rapid pace. Truly, the post-PC world has arrived.

Yet…

Accounting still needs physical receipts for my trips. They will scan them and destroy them, but they need physical receipts. Wouldn't it be simpler for me to scan and send them myself? The "sign and return" two-step is still far too common - receive a document in email; print it; sign it; scan it; send it back; and throw the copy in the recycling bin. What if someone cuts a signature out of a previously signed document and "signs" the document without my knowledge? Contracts, POs, and the paperwork of business is still quite literally paper. Wouldn't it be simpler to never print them at all? Homework, projects, exams, and textbooks are still largely physical, linear, and expensive. Why is this? Whatever happened to the paperless office promised two decades ago? The technology is most clearly here and available. What's missing? What does paperless mean?

Paperless means literally less paper, lowering costs, and producing less waste. These are great things. However, there is another side to this coin that institutions are finally recognizing. What we are really doing is shifting, rather than eliminating consumption. Instead of reams of paper and stamps, we now consume terabytes of bandwidth and storage. Thus, we need more information technology. We need greater bandwidth and storage, new kinds of data archives, more software with far higher complexity, all with increased reliability and ubiquity requirements. We may need more people, or we may need less people, only time will tell. However, we certainly need *different* people or the same people with *different* skills. New skills for everyone. New protocols for information exchange. New mechanisms for decision-making. New classes of people who fix our technology

and make sure it is up-to-date and always there. Still, this will do nothing for the print-and-sign protocol because while the paper carries information we see, it also establishes trust. We need *new ways of establishing trust* that reflect our new ways of storing and transmitting information.

For a researcher who looks at high-assurance systems and security, *the need to shift trust from physical to virtual things* is fascinating. When we make things electronic, we eliminate the traditional places where we root our trust – the physicality of receipt or a contract, the ink of a signature, the weight of a book, or the authenticity of a homework submission or exam. All of these things definitely convey information and there are more efficient, more effective ways of transferring and storing that information. But trust is simply not keeping up – we need better models for establishing trust.

Certainly there is risk in paperless trust. There is also risk in physical artifacts of trust – that risk is simply obscured by familiarity. We have all heard "it's always been done this way", "I've never seen it done that way", or my personal favorite "the University of (your favorite rival here) does it this way." We all have Rasputin whispering in our ear about lawsuits, audits, FERPA, HIPAA, security and friends that surely enough paper will protect us from. But paper won't protect us. We know it won't because it never has. So, let's move forward.

A signature, a sealed envelope, and handshake are all physical things where we root our trust. When a trusted party signs a letter, the contents of that letter are trusted to come from the associated agent. When a letter is sealed in an envelope, the contents are trusted to be delivered in a confidential manner. Finally, when information comes from a trusted source through other trusted parties, the contents are trusted.

The tools of virtual trust are cryptographic functions for encrypting and signing messages and cryptographic protocols for exchanging information. Encrypting information with a key provides the same trust as a sealed envelope – no unauthorized agent may access transmitted information that is encrypted. Signing information with a key provides the same trust as a physical signature – no unauthorized agent may generate a signature over information. Protocols provide us methodologies for using encryption and signing to exchange information.

Exchanging information securely using encryption and signing incorporated into protocols will emerge as a viable solution for trust management. They key is asymmetric key encryption. In asymmetric key encryption one key is used for encrypting secrets while another is used to decrypt. If Alice and Bob want to communicate securely, they exchange their public keys and keep their private keys secret. If Alice wants to send Bob a confidential file, she simply encrypts it with is public key. Upon receipt, Bob can decrypt it with his private key. If Cindy intercepts Alice's message, without Bob's private key she cannot decrypt it. This guarantees *confidentiality* in communication.

Conversely, if Bob wants Alice to know it is he sending the file, he can create a cryptographic signature for the file. Bob creates a signature from his file using a hash function. That signature is then encrypted with Bob's private key. When Alice receives the file that Bob sent, she can decrypt the signature with his public key and check the fingerprint against the file she received. If Cindy sent the file posing as Bob, Bob's public key cannot decrypt the signature because Cindy's key created it. Thus, Alice would know that Bob did not send the file. This guarantees *integrity* in communication.

Asymmetric key cryptography gives us the tools to electronically replace envelops that guarantee confidentiality and physical signatures that guarantee integrity. *Protocols* then specify how those tools are used in practice. One such protocol example is S/MIME for sending privacy-enhanced email. S/MIME is incorporated in virtually every modern email client. It manages keys, ensures your messages are encrypted and signed, and decrypts and checks signatures on incoming email. It literally eliminates the sign and return protocol discussed earlier. There are far more sophisticated protocols for achieving a wide variety of security and privacy goals. We are seeing these protocols implemented in everything from software distribution systems to lab information maintenance.

Establishing trust electronically has its problems. Key management – particularly revocation of compromised keys – is an ongoing area of research and development. But the tools are there for us to use. The time is now for us to move forward and begin to put trust on equal footing with information in the electronic world.