

# Certify Identity

---

## Creating an inter-connected network of digital signatures

IMERGE Consulting, Inc

---

*Jim Minihan*

*June 12, 2009*

*Jm@imergeconsult.com*

*As Appeared in Document Magazine*

*www.imergeconsult.com*

Sometimes, events are such a long time in coming that they seem to not exist one moment and then suddenly, after years of promise, they appear as if they have been there all along. So it seems to be with the paperless office. Not that I think this long-awaited technology has officially arrived, but there is no longer much left in its way. The ability to sign a document that represents a transaction is just another impediment starting to crumble.

Increasingly, organizations come to understand that the documents they use to conduct business are not only created electronically but distributed and used electronically as well. In fact, users prefer the speed and convenience of electronic and no longer make the "conversion" to paper. At the same time, they are also learning that conversion to paper is no relief for having to maintain the electronic version of their records. Records management policies will provide no reprieve when they are driven by regulatory compliance that view electronic originals as more important than paper. The holdout issue for those that insist on the need for paper, however, is the requirement of a signature. How else can a formal transaction occur? they will ask. But this reasoning is starting to meet the classic definition of an excuse a reason not good enough.

### **Understanding the Medium**

Previously, we discussed the basics of electronic signature and the many forms it can take. They can range from nothing more than your name typed at the bottom of an email to a bit-mapped picture of your signature, to the use of a digital signature issued in the context of a sophisticated public key infrastructure (PKI) intended for such purpose. Each has its use, but it is the value and seriousness of the transaction that ultimately defines which should be used based on the need for more or less integrity. However, the more important factor is to deal with the common belief that the only problem created by clinging to paper and ink is the resulting need to manage the paper, something we have centuries of experience with. After all, paper is tried and true... but so it was with rotary telephones and ox-carts. While companies have grappled with the common hurdles of paper production, such as the overhead expense, glitches in efficient operations, customer convenience and possibly your system architecture, it is now possible that even a signed piece of paper will not hold up in court in favor of its electronic counterpart.

Under the revised Federal Rules of Civil Procedure (updated to address electronic discovery), a number of cases have already occurred where a signed paper document is bypassed in favor of an electronic one. An example is an instance where a portion of a hospital's medical record was modified. A signed nurse's record on paper indicated a certain course of events in treatment. But the electronic system that generated that record had additional, relevant information and was allowed into the case in spite of the existence of the signed paper. More and more, electronic documents are becoming a preferred medium and, in some instances, are considered a more valuable and reliable representation of a record than even a signed paper document.

### **Credentials of Identity**

The use of digital credentials in the form of digital certificates (the same used for digital signatures) are becoming popular in applications, such as online banking and stock trading, where non-repudiation of the transaction is essential and there is the need for a level of integrity and security that can no longer be addressed by just a user name and password. The foundation of these applications is the establishment of your identity. Both the bank and the electronic broker want to know that it is you at the other end of the transaction. When they establish your identity in the course of opening the account by requiring proof of who you are, they connect that proof to the digital credential. This works in a number of narrow one to one transactions where the relying party (the bank or broker in this case) is also the issuer of the credential. But this approach is limited as a tool and would require everyone to have many one-to-one agreements. In essence, it is similar to having a phone line between two houses. This might be nice for house-to-house

communications but not very valuable for much else. As a network, this one-to-one communication is limited, as networks become more valuable as you increase the number of useful nodes. Therefore, having a digital signature issued by a trusted party that many others can rely on from a networked infrastructure is like having a phone in the telecom world of many users.

### **Networking Into the Digital Age**

The bottom line here is that we are rapidly learning the value of such a tool. Just as the telephone transformed from a tool of point-to-point communications for the wealthy before it networked into what we have today, a tool for everyone that has adopted functions beyond simply talking, so it will be with digital signatures.

Rather than needing multiple credentials for every transaction consumers might have to make, the public should have the ability to network their identity. In fact, this is exactly what the federal government has done under Homeland Security Presidential Directive 12 (HSPD-12). Already, the government has issued tens of thousands of digital credentials with every agency of the federal government mandated to accomplish issuance to all federal employees and contractors. This credential is meant to be used for all manner of proof of identity, from entering the building to accessing the data system and for digital signings. The federal government has created a networked identity where that one credential can be used across a spectrum of uses and agencies. In effect, they have adopted one phone that can call any other phone in the federal government. Now, what if the bank or broker that federal employee works with decides to accept that credential also? Suddenly that credential (like the phone) has more value.

To work properly, a digital signature would be issued from a recognized (and trusted) certificate authority, such as a state or government agency in a PKI. It would then be given to a properly vetted entity (person, organization or even a computer) whose identity is established to the satisfaction of the trusted issuer. This is similar to how your driver's license is issued in that the process of issuing the license is subsequently relied upon by other users. Once granted, this forms the basis of an identity that can be federated.

A number of states, Pennsylvania, North Carolina and Colorado among them, have begun issuing e-notary digital signatures to the notary public to support the growing use of electronic filing of deeds of trust. Kansas, one of the early adopters of digital signatures, has used them in conjunction with car dealerships to sign motor vehicle title liens where they reside in a database. Recently, the state's Board of Technical Professions modified their rules on signatures and seals to allow for digital variants, and already, a number of private engineering firms are looking to acquire a state-issued digital signature for use on engineering digital documents. In cooperation with the Hague Conference on Private International Law, Kansas was the first state to issue an e-Apostille, which is used by the Kansas Secretary of State for notarizing documents used in international transactions.

Growing acceptance by the public and financial institutions for digital signings represents a sign of things to come. It seems that digital signatures are here to stay.