Editors Note: The e-health musings of Alan S. Goldberg, Goulston & Storrs, Boston, are a regular feature of E-Health Law & Policy Report.

Goldberg on E-Health: Security and Health Care: A Basic Introduction to PKI-Lite

By Alan S. Goldberg

Alan S. Goldberg is a lawyer at the Boston law firm of Goulston & Storrs.

Mention the words "encryption" and "decryption", or "public key infrastructure," to lawyers today, and the reaction often is a mixture of anxiety, confusion, and illusion. Anxiety because most lawyers and technology have not always gotten along well; confusion because the terms are neither generally understood nor appreciated by many lawyers; and illusion because some lawyers still believe that it is possible to practice health law today without embracing computer security technology.

Unfortunately for those lawyers who are challenged by all of this, providers, payers, and patients are moving ahead with electronic health care, and laws, rules, negotiations, contracts, and transactions will include more and more references to PKI and other privacy and security approaches, as HIPAA and related initiatives take hold. So, in an effort to provide a basic introduction to PKI for lawyers, here is a summary of what many are talking about but few understand.

In the old days, in order to hide a message, a system based upon single key encryption or coding was used. In other words, someone who wanted to hide a message would create a secret code that would make the message unintelligible; a key, perhaps in the form of a computer algorithm or computation, would be used to hide the message; and to decrypt or decode the message, that same key would have to be used. While the systems were far more complex than this simple example, basically the notion was that the coding feature and the decoding feature were substantially the same. This meant that if someone could get a hold of the single key or could figure out how to recreate that key, the code could easily be broken, and single keys could be lost while being transported to addressees of the coded message as well or stolen.

For thousands of years, the single key approach was used and no one was able to devise a better system. But fortunately for those believing that code is good, several decades ago the notion of two keys was realized. In other words, the creator of a message proposed to be hidden or encoded would use one key to encode the message, and the intended addressee of the message would use a different but mathematically related key to decode the message. This means that the creator of the coded message does not have to deliver to an addressee the key used to encode the message. Instead, the addressee gets the second key independently and the second key and the first key are two different keys. Get it so far?

This means that, for the first time, the risk of transporting and losing a key is not a major issue and the security of the message encoded is far greater than ever. The more complex the key (or, in other words, the longer the algorithm or computation), the more difficult it is to break the code used for the key.

Now, the two keys, under the public key infrastructure approach, are called the public key and the private key. The public key is a key created and intended to be made public. Everyone can get a copy of the public key, which the creator of the key either makes available on the Internet generally or gives to a central authority, trusted by the public, which will certify to the public that the public key is, indeed, the public key of a designated individual.

The same individual creates a private key, that only the creator can use, either because of a special password that only the creator knows or some other means of authentication. The private key is the only key in the world that can create a message that can be decoded by a particular public key that the creator of the private key created. And the public key is the only key in the world that can encode a message that only the creator's private key can decode.

Leaving aside issues involving authentication and trusted public authorities who verify that a particular public key is the public key of a certain individual, the public key and private key approach, known as PKI or public key infrastructure, has many benefits. First of all, there is the elimination of the risk of loss of a single key that encodes and decodes. Second, everyone can access anyone's public key. And third, no one can access anyone else's private key, unless someone's private key password is stolen or lost.

Here, simply and without lots of the details, is how all of this works:

1. If I want to encode a message that only a particular addressee can decode and read, I use that addressee's public key to encode the message.

2. Only the person whose public key I am using will be able to open that message. Thus, I will know that no one else in the world can read that message unless the addressee decides to show the message to others.

3. If I want to prove to someone else that a message I am sending is, indeed, from me and not from anyone else in the world, I use my private key to encode the message.

4. The only key that is able to decode a message encoded with my private key is my public key, that everyone can use to decode messages encoded with my private key.

5. A single message can be encoded with my private key and encoded again with someone else's public key, in order to send a message that is both encoded (to make it private) and authenticated (to prove its source) as coming from me.

I hasten to add that all the foregoing is a summary only and I have left out lots and lots of details. Therefore, please treat this as an approximation of how PKI works and not as the definitive guide to PKI. And there are different approaches to PKI as well, although in general they all rely at least on a public key and a private key.

See? It's not that bad, is it? PKI for you and me--it's the future of health care information and technology, and it will revolutionize commercial transactions generally and health care delivery and payment specifically. Now, if I can only figure out how to program my VCR without an eleven year old helping me, I will truly have embraced the new technologies.

Alan S. Goldberg maintains his own Web site at http://www.healthlawyer.com, and can be reached at (617) 482-1776 or at agoldberg@goulstorrs.com.