

TECHNOLOGY


 Timothy Perrin

Signing Your Life Away

A few weeks ago, I went to the local Purolator office to pick up a package. Rather than signing a piece of paper, they wanted me to sign on an electronic pad that would capture a digital image of my signature. Much to the surprise of the woman behind the counter, I refused.

"I won't digitize my signature," I told her.

"What?"

I explained that by signing her little pad, Purolator would then own a perfect copy of my signature, right down to stroke timing, pen pressure, and all the other little nuances that truly distinguish my signature—the touches that no forger can ever really duplicate.

"But nobody's ever refused before," she told me.

"Perhaps they should have."

She called her supervisor. I explained things again.

"Our lawyer says we don't have to release the package if you don't sign."

"Three years of law school and seven years of practice tell me that you do," I replied. "It's very simple. The package is my property. You have been paid for its delivery. I have proved my identity. You must release the package to me."

The stare-down lasted about 30 seconds until she reached under the counter, pulled out a clipboard, wrote the waybill number on line 47, passed it across the counter, pointed, and said, "Sign here."

I signed, said thank you, took my package, and left.

Why the big ruckus? As any victim of identity theft will tell you, once something gets out there in cyberspace, you cannot get it back. You completely lose control of it. Something as precious as a perfect rendering of my signature—a copy so accurate that the world's best experts would not be able to say it was not mine—is not something I want anyone to own.

As any victim of identity theft will tell you, once something gets out there in cyberspace, you cannot get it back.

Well, what about your signature on fax letters? I hear you ask. That is a low-resolution image of my signature, not the digitalization of it. It's the difference between a scratchy 78 rpm recording—for those of us who can even remember them—and the near-perfection of the new DVD audio recordings, which put to shame even compact discs. Take a blind man into the Orpheum, sit him down in the centre of row 13, and he could probably not tell whether he was listening to the Vancouver Symphony live or to a DVD recording on a very high-end sound system.

So, a digitized signature is a bad thing.

But it's not to be confused with a **digital signature**, which is a very good thing.

A digital signature is an electronic

method for you to verify you are the sender of a particular message or verify a particular message has come from the person who has purported to send it. At its simplest, it's a form of electronic encryption—secret codes.

Virtually all digital signature systems rely on what is called **public key-private key** technology. With public key-private key systems, there are two keys to every encoded message: one you make available to the public; the other you keep a secret. Anyone can encrypt a message using your publicly available key. Once encrypted, only *you* can decrypt it using the secret key.

Alternatively, to prove that you, and only you, are the originator of a particular message, you encrypt it with your private key. The fact that it decodes with your public key proves you were the source. It also creates a situation in which you cannot repudiate the message, claiming someone else sent it.

When you encode a message with your private key, you have digitally "signed" it.

Public key-private key systems are really quite simple in theory. They rely on what are called "trap door" mathematical functions, problems that are very easy to do in one direction—like falling through a trap door—but hard to do in the other direction—like climbing back up through the trap door.

Here's a super-simplified example. It's very easy to multiply two six-digit numbers together, say 190,208 and 295,009. The product is 56,113,071,872. (Everyone who double-checked my math, go to the special class

BC Decision-Makers Read *The Scrivener!*

This magazine reaches the following spheres of influence, quarterly.

- BC Notaries
- Land Appraisers: R.I.(B.C.) designates
- Land Surveyors of BC
- Lawyers
- Real Estate Professionals
- Real Estate Boards and Associations
- Provincial/Federal Court Judges
- Registrars
- MLAs and MPs
- Life Insurance Brokers and Agents
- Accountants
- Managers of Financial Institutions
- Mayors
- Government Ministries
- Libraries: Public and Private, including Law Society, Legal Services, Educational Facilities
- Investment Management Agencies
- Chambers of Commerce
- BC Housing
- BC Assessment
- BC Buildings Corporation

**Advertising Deadline for
Spring Issue: Feb 15, 2004**

**Promote your
services to our
prequalified
audience of allied
professionals!**

**Call: 604 985-9250
Fax: 604 985-0900
scrivener@notaries.bc.ca**

for keeners down the hall, please.) But, now that we've got that nice, big 56 billion more-or-less number, can you tell me the two numbers I used to generate it? Obviously, there are many, many combinations that would produce that same result—billions of them, in fact. Without knowing one of the two numbers, you can't tell me the other one.

That's a trap door. It's easy to multiply the two numbers, difficult to factor the result back to where we started.

Commercial encryption systems start with 128-digit prime numbers (the ones that can only be divided by one and by themselves). They then throw in a couple of other things like some cubing and a Calculus function here and there. The result is a function where you need know only one of the factors to go one way, but both of them to undo it.

Oh, in theory a highly motivated opponent could come up with a solution by brute force, using huge computers to try every possible combination until one worked, but the beauty of a trap door function is that it would take years to successfully force your way back through the trap door. By then, whatever you learned would be useless.

If you bank online, you are using public key-private key encryption all the time. Actually, to make things doubly secure, you are using either double public key-private key encryption or a combination of public key-private key encryption and old-fashioned secret-key encryption where both parties need to know the same key.

In the first, your computer sends the bank your public key. Everything the bank sends to you is encrypted using your public key, then is unjumbled at your end by your computer using your private key. Everything you send to the bank is encrypted using the bank's public key.

An even more secure system is to have your computer generate a new, unique 128-bit secret key. Your computer then encrypts this secret key using the bank's public key and sends it to the bank's computer. Now, both computers know the same completely secret key. Secret-key

encryption—where both sides are using the same key—is a totally secure method of encryption. To eavesdrop on your transactions, someone would first have to intercept that very quick transmission of the key, then decrypt it before he or she could use it. That's highly unlikely.

With public key-private key systems, there are two keys to the every encoded message: one you make available to the public; the other you keep a secret.

It will be public key-private key technology you will be using with the Land Title Office's electronic registration system when it comes online later in 2004.

The implications of digital signatures go beyond commercial transactions and legal undertakings. As the cyber universe matures, we will each be able to assume a single electronic identity rather than being "tperrin" with password "pword1" on this Website and "timperrin" with password "pword2" on that Website.

Further, this idea easily spills over into the physical world. We could easily use a single identity card similar to a bank card. Even better would be a keyring radio-frequency chip that need only be held close to a sensor. Then, when I need to "sign" for a package at the courier's office, I would use the combination of the card or r.f. chip and a PIN number.

The technology exists. The question is, how willing are we to adopt it? ▲

Timothy Perrin, a former lawyer, is a technology writer for a variety of magazines. He teaches writing in the Professional Writing program at Okanagan University College in Kelowna; online for the Community College of Southern Nevada; and through his own school, WritingSchool.com.

www.TimothyPerrin.com