Published on **The O'Reilly Network** (http://www.oreillynet.com/)
http://www.oreillynet.com/pub/wlg/5142

CAcert: Digital certificates become free

by Andy Oram
Jun. 30, 2004
URL: http://www.cacert.org/

Getting a digital certificate signed by a recognized Certificate Authority--and here I mean a well-known entity embedded in web browsers and other critical places, not a Web of Trust kind of thing or a hub on your LAN--used to be a major expense.

It was natural to think of Certificate Authorities as heavy-weight, bureaucratic, and expensive, like getting a domain name (a field dominated by the same firm that dominates Certificate Authorities--hmmm) or wireless Internet services.

Well, what's natural turns out to shift like the sand on a Cape Cod bayside beach when the tide goes out. You can get wireless Internet free, if you happen to live near one of the many municipal hotspots being installed around the world. Competition in domain names is growing, and costs are correspondingly coming just a bit closer to the costs of maintaining the DNS infrastructure (which is quite small). Now, thanks to CAcert, everyone can get a free digital certificate signed by a global player.

CAcert is a non-profit volunteer organization. Some of the volunteers turned up this week at Usenix in Boston, where I talked to them for some time. CAcert's marketing/PR director Adam Butler also put a long article in the June 2004 issue of Usenix's magazine *;login:* to explain their approach to security and their progress toward acceptance.

There are discussions going on at the Mozilla and Konqueror about including CAcert in their list of Certificate Authorities so that no extra steps are required to validate web sites that use CAcert certificates. Several valid concerns have been raised about the standards for determining whether CAcert itself is trustworthy, which I'll touch on later.

How CAcert works

CAcert's resourceful Australian originators took a hard look at the infrastructure that's really necessary to operate a Certificate Authority, and found that it was fairly small. Free software implementations of SSL, X.509, and similar secure technologies reduce technological costs to the price of the hardware. Organizationally, the service is driven by volunteers and donors who find a mission in providing authentication to the world.

Registering for a CAcert certification requires no money; the cost comes in time and trouble. You are asked to register online, perform some tasks by email, and then bring two forms of picture identification to a site where CAcert staff can determine whether you're legit. (At Usenix, I was not able to complete the sequence.) This provides enough friction to make cheating non-trivial.

As one volunteer explained, "You could forge or steal a passport, but then you're in much bigger trouble than you could ever be with us and our little certificate." He also pointed out that Verisign offers certificates on the basis of documents faxed to them. In short, like all CAs, CAcert leverages off the existing infrastructure for verifying identities. The processes for getting passports and drivers licenses have known vulnerabilities, but getting a digital certificate from CAcert isn't significantly more vulnerable.

Certificate Authorities recognize different levels of assurance, based on how hard it is to get a certificate. CAcert's process for average users is not very demanding, but it's probably adequate for exchanging email and other everyday online activities. I probably wouldn't use one to sign a million-dollar contract.

CAcert has also adopted a Web of Trust system to allow multiple sites to grant certificates. The criteria for reaching this higher level and becoming an Assurer is more rigorous.

The meaning of CAcert in context

Goods and services obey a kind of financial Parkinson's Law, expanding to fill the available space. Thus, when commercial Certificate Authorities defined a digital certificate as a rare item deserved only by large institutions, they could charge accordingly and the institutions felt privileged to have one. Meanwhile, the small group of computer hackers who recognized the value of digital certificates resorted to the Web of Trust or simple measures such as signing software with MD5 hashes that they posted in well-known places.

But in an era where we are drowning in malicious code, spam, and an increasing reliance on the Internet for critical activities, people are rising up to expose the Parkinson's Law. A comment on the Mozilla site from Glen Morris says, "Security should be a right not dependent on your ability to pay."

Critics of CAcert says it fails to follow industry standards. Defenders point out that these standards impose costs that can't fit in CAcert's service model, that many browsers fail to enforce standards, and that major Certificate Authorities fail even when they've been attested to by standards committees. (The famous incident where Verisign gave a Microsoft certificate to an unknown masquerader comes up a lot.) Furthermore, some experts such as Bruce Schneier are skeptical of the security claims Certificate Authorities make, on the basis that real life just isn't air-tight.

And here's where CAcert may actually represent that overused phrase, a paradigm shift. To judge CAcert fairly requires us to go beyond the accepted industry standards, to decide what we really want in a Certificate Authority, and to carry out the traditional analysis of risk, threat, and response that Schneier and others tell us to do whenever we deal with security issues. I bet that open-minded people can find a low-cost solution to everyday communications needs involving a free CA such as CAcert.

Andy Oram is an editor at O'Reilly & Associates, specializing in books on Linux and programming. Most recently, he edited Peer-to-Peer: Harnessing the Power of Disruptive Technologies.